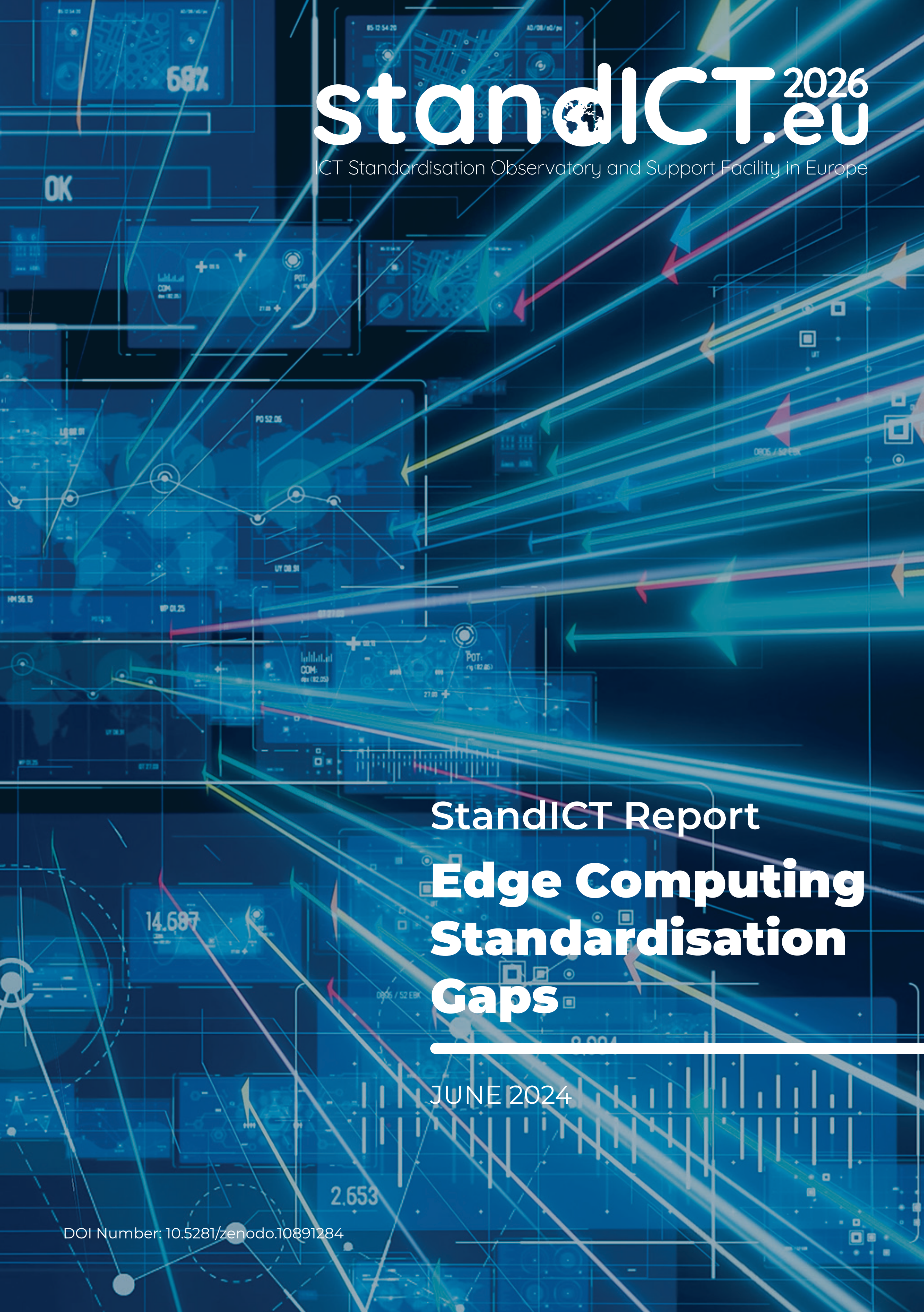


standICT.eu 2026

ICT Standardisation Observatory and Support Facility in Europe

StandICT Report

# Edge Computing Standardisation Gaps

JUNE 2024

DOI Number: 10.5281/zenodo.10891284

## Legal notice

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

## About StandICT.eu

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

JUNE 2024

# Table of Contents

# Executive Summary

This report presents an approach reported in AIOTI, for the definition and identification of key Edge Computing 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.

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

The purpose of this document is to promote a structured discussion within the EUOS and edge computing 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 Edge computing standardisation gaps in several initiatives.

# Foreword by the Editor

Currently, there are several definitions of edge computing, which are provided by Standards Development Organizations (SDOs) and industry associations, see e.g., the EUOS StandICT.eu Landscape of Edge Computing Standards report. Similar to IoT systems, there are several edge computing systems and edge computing applications being implemented and deployed in almost all vertical industry domains, such as Health, Industry & Manufacturing, Agriculture, Finance, Mobility, Energy, Public safety, Buildings and Cities.

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, Alliances and OSS (Open-Source Software) initiatives.

This report complements the EUOS StandICT.eu Landscape of Edge Computing Standards report by presenting an approach reported in AIOTI, for the definition and identification of key Edge Computing 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 Edge Computing standardisation gaps. In the context of EUOS, the synergy and integration of IoT/ IIoT and edge computing, is considered to be a part of the paradigm shift from centralised solutions to decentralised and distributed computing architectures, in which information processing is located close to the edge, where "things" (e.g. sensors/ actuators, devices, machines and humans) produce and utilise that information, knowledge and related experience.

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 edge computing 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 Edge computing standardisation gaps in several key SDO initiatives.

**By the Editor: Georgios Karagiannis**

# Foreword by the European Commission

In a new post-Covid era, IoT and Edge technologies are speeding up the transition paths for key sectors and helping industries that face overarching challenges, particularly linked to the side-effects of the Ukraine crisis. Leveraging emerging digital technologies like edge computing and decentralised intelligence help to tackle urgent societal needs such as addressing energy savings and resilience, and reducing the carbon footprint in key sectors like mobility and housing as well as of major industrial sectors.

Aligned with Europe's data legislation, the digital and green transition, and industrial strategies, significant investments are required to propel the development and deployment of next-generation edge computing components and systems. These investments are crucial for facilitating a swift transition to a computing continuum characterised by increasing computing capacities at the network edge , gradual integration of AI at the edge and a paradigm shift towards software-define systems.

In order to achieve Europe's Digital Decade targets for 2030, a unified strategy is needed. It is crucial that all stakeholders involved interact in a coordinated way to set the route on interoperability and data standards, weaving together diverse ecosystems and streamlining data flows, particularly within the energy sector and beyond the energy sector, to pave the way for a sustainable future.

Multi-standard interfaces, horizontal and cross-sector interoperability standards and the crucial importance of the upcoming pilots on emerging Smart IoT Platforms and decentralized intelligence emerged as key discussion points in the workshop on "Accelerating standardisation in the nexus of mobility, buildings and energy" organised in January 2024, underscoring the importance of open cross-sectoral standards in enabling orchestration and seamless integration and management across ecosystems within the cloud-edge-IoT continuum, operated by meta operating systems.

In this context, there are challenges in terms of adopting common reference architecturemodels (cloud-edge orchestration, data models and ontologies, cross-domain signals and messaging, containerization etc.), interfaces,and APIs, whilst ensuring compliance with existing and upcoming regulations.

We therefore acknowledge the work of initiatives like StandICT.eu, IPCEI Next Generation Cloud Infrastructure and Services, the Alliance for IoT and Edge Innovation (AIOTI) that help interact with relevant open source initiatives and standardisation communities to define complementarities around interoperability, data protection, portability of cloud services and security, fostering collaboration and coordination around inputs to new activities and spotlighting European strengths and leadership in international developments.

The present report valuably complements the EUOS StandICT.eu Landscape of Edge Computing Standards report by offering an approach, drawn from AIOTI, to define and identify key standardisation gaps in edge computing across various key Standard Development Organisations (SDOs).

Harnessing the power of IoT and Edge Computing technologies will unquestionably create positive spins to all industrial sectors of activity; as edge computing is triggering a paradigm shift ushering in the next industrial revolution by transforming system design processes to make them faster and more agile, alignment with legislative initiatives like the Data Act, Data Governance Act, and Cyber Resilience Act becomes increasingly pivotal for ensuring regulatory compliance and resilience.

**Rolf Riemenschneider**

**Head of Sector IoT, DG Connect, Unit E4, 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 |
| AI | ARTIFICIAL INTELLIGENCE |
| AIOTI | ALLIANCE FOR IOT AND EDGE COMPUTING INNOVATION |
| APIs | APPLICATION PROGRAMMING INTERFACES |
| AR | AUGMENTED REALITY |
| CEN | EUROPEAN COMMITTEE FOR STANDARDISATION |
| CENELEC | EUROPEAN COMMITTEE FOR ELECTRONICAL STANDARDISATION |
| CIM | COMPUTER INTEGRATED MANUFACTURING |
| DARPA | DEFENSE ADVANCED RESEARCH PROJECTS AGENCY |
| DLT | DISTRIBUTED LEDGER TECHNOLOGY |
| DNS | DOMAIN NAME SYSTEM |
| ESG | ENVIRONMENTAL, SOCIAL AND GOVERNANCE |
| ETSI | EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE |
| EUOS | EUROPEAN OBSERVATORY |
| GS | GROUP SPECIFICATION |

| | |
|---|---|
| HPC | HIGH-PERFORMANCE COMPUTING |
| ICT | INFORMATION AND COMMUNICATIONS TECHNOLOGY |
| IEC | INTERNATIONAL ELECTRONICAL COMMISSION |
| IEEE | INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS |
| IETF | INTERNET ENGINEERING TASK FORCE |
| IIOT | INDUSTRIAL INTERNET OF THINGS |
| INFOCOM | INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS |
| IOT | INTERNET OF THINGS |
| IRTF | INTERNET RESEARCH TASK FORCE |
| ISG | IMPLEMENTATION SPECIFICATION GROUP |
| ISO | INTERNATIONAL ORGANIZATION FOR STANDARDIZATION |
| ITU-T | INTERNATIONAL TELECOMMUNICATION UNION – TELECOMMUNICATION STANDARDISATION BUREAU |
| LCA | LIFE CYCLE ASSESSMENT |
| MEC | MULTI-ACCESS EDGE COMPUTING |
| ML | MACHINE LEARNING |
| NB-IOT | NARROWBAND INTERNET OF THINGS |
| NFV | NETWORK FUNCTION VISUALIZATION |
| NGNM | NEXT GENERATION MOBILE NETWORKS |
| NGSI-LD | NEXT GENERATION SERVICE INTERFACE - LINKED DATA |
| OAM | OPERATIONS, ADMINISTRATION AND MAINTENANCE |
| ONEM2M | ONE MACHINE-TO-MACHINE |
| OMA | OPEN MOBILE ALLIANCE |
| OPC UA | OPEN PLATFORM COMMUNICATIONS UNIFIED ARCHITECTURE |
| OPEX | OPERATING EXPENSES |
| OS | OPERATING SYSTEM |
| OSS | OPEN SOURCE SOFTWARE |
| OT | OPERATIONAL TECHNOLOGY |
| RAN | RADIO ACCESS NETWORKS |
| RIOT OS | REAL-TIME OPERATING SYSTEM FOR THE INTERNET OF THINGS |
| RDF | RESOURCE DESCRIPTION FRAMEWORK |
| REST | REPRESENTATIONAL STATE TRANSFER |
| SDO | STANDARDS DEVELOPMENT ORGANISATION |
| SFDR | SUSTAINABLE FINANCE DISCLOSURE REGULATION |
| SFWG | SUSTAINABLE FINANCE WORKING GROUP |
| SLA | SERVICE LEVEL AGREEMENTS |
| SSO | STANDARDS SETTING ORGANISATION |
| STF 505 | SPECIALIST TASK FORCE 505 |
| TR | TECHNICAL REPORT |
| TS | TECHNICAL SPECIFICATION |
| TWG | SECURITY TECHNICAL WORK GROUP |
| UALCMP | USER APPLICATION LIFECYCLE MANAGEMENT PROXY |
| VR | VIRTUAL REALITY |
| XR | EXTENDED REALITY |
| W3C | WORLD WIDE WEB CONSORTIUM |

# 1. Goal and motivation

This report introduces[1] an approach for the definition and identification of key Edge Computing standardisation gaps in several initiatives.

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

There are now  Edge Computing Standards Landscape reports available, including the work done by EUOS in "Landscape of Edge Computing Standards" and by AIOTI in "High Priority Edge Computing Standardisation Gaps and Relevant SDOs, Release 1.0" that have identified a number of standards that are available, i.e. which have reached a final stage (TS or TR, etc.) in a Standards Development Organisation (SDO) or industrial consortia, and can be used for the work and developments of the Edge computing community.

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

The purpose of this document is to start a structured discussion within the 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 Edge Computing 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 edge computing research and standardisation challenges included in following sections, have been described using the edge computing 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 Edge Computing challenges

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

The edge computing 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 edge computing 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 research and standardisation challenges, and provide a structure that will be essential to identify specific gaps. These categories of research standardisation challenges are:

- Data Models & Formats (Interoperability): Establishing standardized data models and formats to facilitate seamless data sharing and interpretation across different Edge computing systems.
- Data Exchange APIs (Interoperability): Developing APIs that enable efficient and compatible data exchange between various components in Edge environments.
- Provenance and Traceability (Interoperability): Ensuring the ability to trace the origin and history of data in Edge computing, enhancing data integrity and reliability.
- Identity Management (Trust): Implementing systems to securely manage digital identities in Edge environments, ensuring entities are authentic and trustworthy.
- Access and Usage Control/Policies (Trust): Establishing protocols for controlling access to data and regulating its use in Edge systems, maintaining data security and privacy.
- Trusted Exchange (Trust): Creating secure and reliable methods for data exchange in Edge computing to maintain trustworthiness in digital transactions.
- Metadata & Discovery Protocol (Data Value): Using metadata and discovery protocols to enhance the findability and utility of data in Edge computing environments.
- Data Usage Accounting (Data Value): Implementing systems to track and manage the usage of data in Edge computing, enabling accurate accounting and potential monetization.
- Publication and Marketplace Services (Data Value): Facilitating the publication and transaction of digital services and data in Edge computing marketplaces.
- Overarching Cooperation Agreement (Governance focusing on standardisation): Developing comprehensive agreements to govern cooperative efforts and standardization in Edge computing.
- Operational (e.g., SLA) (Governance focusing on standardisation): Setting operational standards like Service Level Agreements to ensure reliable and quality services in Edge environments.
- Continuity Model (Governance focusing on standardisation): Establishing models to ensure continuous and sustainable operation of Edge services and infrastructures.
- Device Certification: Certifying Edge devices for compliance with established standards, ensuring interoperability and quality.
- Solution Deployment and Maintenance Tools: Standardizing tools for deploying and maintaining Edge computing solutions efficiently.
- Scalable Device Deployment: Addressing the challenges in efficiently deploying devices at scale in Edge computing environments.
- Green Technologies: Focusing on environmentally sustainable technologies and practices in Edge computing to reduce ecological impact. Methodologies to measure carbon emissions are as well included.
- Usability (easy accessibility and usage to a large non-technical public): Making Edge computing technologies easily accessible and user-friendly, even for non-technical users.

- Security and Data Privacy: Prioritizing the protection of data and systems against unauthorized access and breaches in Edge computing.
- Social/Societal: Addressing the social and societal implications and benefits of Edge computing technologies.
- Digital/Digital Twin in the Context of IoT and Edge: Creating digital replicas of physical systems in Edge environments for real-time monitoring and simulation.
- Computing Continuum: Integrating Edge computing with other computing paradigms like cloud and fog computing for seamless data processing and services.
- Artificial Intelligence in the Context of IoT and Edge: Implementing AI algorithms and models in Edge environments to enhance IoT applications and services.

## 2.1 Digital for Green research challenges

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

Category: Green Technologies

### Description of research challenges

1. Define and evaluate approaches on increasing energy efficiency in communication infrastructures applied in IoT and edge computing solutions;

2. Develop and evaluate IoT and edge computing solutions that support monitoring and controlling energy and carbon footprint usage in EU Green Deal areas:

- Climate action
- Clean energy
- Sustainable industry
- Building and renovating
- Sustainable mobility
- Biodiversity
- From farm to fork
- Eliminating pollution;

3. Develop and evaluate security and privacy by design approaches required to secure the IoT and edge computing solutions applied to monitor and control energy and carbon footprint usage in EU Green Deal areas and which are as well able to protect any personal data lifecycle used by these solutions;

4. Develop (or reuse) and evaluate interfaces, data models and ontologies required by IoT and edge computing solutions that support monitoring and controlling energy and carbon footprint usage in EU Green Deal areas;

5. More research and innovation activities on standards or guidelines are required to define the Carbon footprint of ICT installations – in use but also incl. material production, assembling, recycling (LCA - Life Cycle Assessment);

6. R&I activities on “green AI”, developing strategies and implementation concepts;

7. R&I activities for reference designs and benchmark platforms;

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

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.2 Digital for Green standardisation challenges

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

Category: Green technologies

### Description of standardisation challenges

1. Specify (or modify existing) interfaces that help monitor and control of the energy usage in communication protocol layer stacks applied in IoT and edge computing solutions

2. Specify (or modify existing) IoT and edge computing related standards, interfaces, data models and ontologies to reduce the energy and carbon footprint (by e.g., monitoring and controlling energy and carbon footprint) in EU Green Deal areas:

- Climate action
- Clean energy
- Sustainable industry
- Building and renovating
- Sustainable mobility
- Biodiversity
- From farm to fork
- Eliminating pollution

3. Specify (or modify existing) security and privacy by design standards required to secure the IoT and edge computing solutions applied to monitor and control energy and carbon footprint usage in EU Green Deal areas and which are as well able to protect any personal data lifecycle used by these solutions.

4. 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

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

- Based on the AIOTI report “IoT and Edge Computing Carbon Footprint Measurement Methodology”, Release 1.1, see: https://aioti.eu/wp-content/uploads/2022/11/AIOTI-Carbon-Footprint-Methodology-Report-Final-R1.1.pdf

### Application/Industry domain

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

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

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

Category: Social, Societal

### Description of research challenges

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

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

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

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

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

These requirements imposed by this challenge can be divided in:

- Functional requirements
  - What infrastructure shall be in place to ensure the underlying technology, metrics and data are available and accessible?
    - ESG Data Taxonomy: Define a robust, comparable and reliable ESG data taxonomy. As per European Banking Federation: “Therefore, ensuring availability of high quality and comparable ESG data should be regarded as an EU strategic infrastructure project to meet the EU sustainability objectives both under the Action Plan on Sustainable Finance and the EU Green Deal”

  - What are the underlying connectivity requirements?: The overwhelming majority of IoT connections are likely to require some form of connectivity (cellular, WiFi, optical, cable, etc.) in the last mile, whether directly from terminal devices themselves or from aggregation hubs.
    - ESG related regulations to consider that IoT sensors, e.g., Smart meters, can be used as remote reading capabilities collectors from assets
    - Define Technology -driven ESG ratings as they are becoming increasingly influential, since they offer financial service institutions the ability to compare the ESG performance of companies, which is currently complex due to the low degree of standardised methods for ESG metric and data collection & monitoring.
- Non-functional requirements
  - Data-Security and privacy: These requirements are significant due to the fact that the ESG data and metrics that are collected and monitored can be considered to be sensitive and personal data related, where typically compliance to GDPR is required.
  - Avoid lock in and fragmentation and support of Interoperability: A large number of players in the IoT ecosystem (e.g., over 400 IoT platform providers) are driving the development and deployment of their own IoT platforms and solutions on supporting ESG. This can lead to lock in and fragmentation. Deploying Interoperable IoT and edge computing platforms and solutions for this purpose, can avoid the fragmentation challenge. This requires the use of standardized interfaces, protocols, data models and ontologies to support the collection and monitoring of ESG related metrics and data. Interoperability can as well enable cross-industry solutions to unlock mutual benefits and enable new monetization models.

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

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

### Application/Industry domain

ESG metrics and rating will be useful for:

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

## 2.4 Explainable AI using human argumentation research challenges

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

Category: Artificial Intelligence in the context of IoT and/or Edge

## Description of research challenges

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

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

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

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

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

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

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

## Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

According to DARPA:

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

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

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

### Application/Industry domain

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

## 2.5 Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge

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

Category: Digital Twin in the Context of IoT and/or Edge

### Description of standardisation challenges

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

### Description of the requirement:

Standards are needed in a number of areas:

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

### Types of Requirements:

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

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

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

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

### Application/Industry domain

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

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

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

Category: Computing Continuum & Data Models and Formats

### Description of edge computing challenge-research/standardisation requirement

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

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

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

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

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

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

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

## Description of the requirement:

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

Key Requirements:

- At the network level, the requirements are :
  - Ensuring interoperability across platforms, devices, and locations, enabling assets to be securely purchased and transferred between virtual and real-world locations, authenticated and validated using various consensus methods that support the validation of identity, ownership, and usage rights of any asset subject to relevant rights.
  - Enabling the interoperability of search, trade, transaction, trackability, and transfer of assets by and between users within and across physical or virtual locations across digital and physical supply chains.
  - Providing secure authenticated human identities and virtual identities and their relevant profile information, transaction, and location histories for representative agents and avatars.
  - Tracking location-based asset provenance, persistence, and validation
  - Allowing assets to maintain and prove their uniqueness, ownership, location and history.
- At a user level, the requirement is allowing a user to:
  - securely register, find, buy, sell, and transfer virtually anything between individuals within and across virtual web “spaces” (physical, cyber-physical or purely digital and immersive)
  - connect spaces together to organically grow a new internet space that both visitors and virtual and physical items can securely and reliably move between.
- At the context (meta-data) level, key requirements are:
  - New data meta-models and communication protocols need to define a common method to describe, express, share and update that notion of context between all the edges of a network. They also need to allow a secure and privacy preserving governance of people, places and things. This is not possible without having a network that is “context-aware”.
  - Context in this instance is the semantic, societal, situational and environmental meta-data model about people, places and things over time.
  - Context needs to be shared between networks of heterogeneous devices and applications empowering them to proactively offer enriched, situation-aware and usable content, instructions and experiences: a situational communal garden of context information if you will.

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

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

Its description also needs to:

- Be Stateful
- Be machine readable and executable
- Be shareable between heterogeneous networks, devices and applications

- Maintain coherence over time and space for all actors / edges involved in a use case

### Types of Requirements:

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

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

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

### Application/Industry domain:

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

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

## 2.7 IoT and edge computing in Digital service transformation

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

Category: Computing Continuum & Data Models and Formats

### Description of edge computing challenge-research/standardisation requirement

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.8 IoT and edge computing coexistence across sectors

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

Category: Computing Continuum & Data Models and Formats

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.9 AI/ML enabled Network and Services

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

Category: Artificial Intelligence in the context of IoT and/or Edge

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.10 Service discovery support

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

Category: Metadata & Discovery Protocol

### Description of edge computing challenge-research/standardisation requirements

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

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.11 Authentication of services and service providers

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

Category: Security and Data Privacy

### Description of edge computing challenge-research/standardisation requirements

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

## 2.12 Policy descriptions, rules, and constraints

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

Category: Social & Overarching cooperation agreement

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.13 Novel programming models and languages

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

Category: Scalable device deployment & Data Models and Formats

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.14 Devices and open device management

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

Category: Scalable device deployment

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.15 IoT and X-Continuum Paradigm

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

Category: Computing Continuum

### Description of edge computing challenge-research/standardisation requirements

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

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.16 Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models

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

Category: Security and Data Privacy & Data Models and Formats

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.17 IoT Swarm Systems

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

Category: Scalable Device deployment

### Description of edge computing challenge-research/standardisation requirements

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

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, "High Priority Edge Computing Standardisation Gaps and Relevant SDOs", see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

# 2.18 Federated Learning and AI for IoT Edge:

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

Category: Artificial intelligence in the context of IoT and/or Edge

## Description of edge computing challenge-research/standardisation requirements

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

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

## Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

## Application/Industry domain

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

# 2.19 OSs and Autonomous Orchestration Concepts

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

Category: Computing Continuum

## Description of edge computing challenge-research/standardisation requirements

- New orchestration paradigms to support distributed IoT edge based on internet-enabled automation concepts, virtualization, multi-state analytics, digital twins to improve end-to-end response time and swarm paradigms integration

## Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

## 2.20 IoT Systems integration

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

Category: Computing Continuum & Data models

### Description of edge computing challenge-research/standardisation requirements

- IoT intelligent systems integration through federation of platforms and distributed systems including many heterogeneous IoT devices and smart systems to provide resilience, security and trust for AI-based IoT edge applications. This will require a standardized reference architecture with new/modified interfaces.

## 2.21 IoT sectorial and Cross-Sectorial Open Platforms

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

Category: Computing Continuum

### Description of edge computing challenge-research/standardisation requirements

- These concepts will impose federated and distributed identity management for authentication, authorization policies, the access control mechanisms, and facilitates the exchange and coordination among several cross sectorial open platforms. Moreover, a common framework is needed for verification, validation, testing, and certification of different IoT implementations based on agreed performance requirements. Moreover, validation verification methods for task development of edge IoT intelligent multi-agent system architecture.

### Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

### Application/Industry domain

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

# 2.22 IoT and edge computing Platforms

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

- Category: Solution deployment and maintenance tools & Data Models & Formats (Interoperability)

## Description of edge computing challenge-research/standardisation requirements

- IoT platforms require interoperability at multiple levels and a federation of platforms will allow optimising the use of the resources, improving service quality and most likely reducing costs. Research on IoT platforms and integration of the functions of the platforms in the intelligent infrastructure as well as research on a layer-oriented approach and semantic interoperability in heterogeneous systems is required to address interoperability at all layers. The inclusion of a programmable, software defined network layer is critical for merging IoT and 5G and future architectures. Emerging industrial IoT applications, Tactile Internet, digital twin and autonomous/robotic systems solutions will require much faster reactivity at the edges of the networks as it becomes increasingly inefficient to extract insights from the cloud with growing numbers of IoT devices. These trends impose as well standardisation challenges such as modification of interfaces, data models, security, and privacy models.

## Source

- Copied from AIOTI report focusing on Edge Computing Gap Analysis, “High Priority Edge Computing Standardisation Gaps and Relevant SDOs”, see:

https://aioti.eu/wp-content/uploads/2022/04/AIOTI-High-Priority-Edge-Computing-Gaps-Final.pdf

## Application/Industry domain

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

# 2.23 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 edge computing 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

## 2.24 Simulation and Emulation Environments

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

- Usability

### Description of edge computing 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

## 2.25 Optimal Edge-based Lifecycle Management

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

- Operational

### Description of edge computing challenge-research/standardisation requirements

- Edge computing introduces new challenges for service and application lifecycle management. Traditional cloud-based lifecycle management techniques are not always suitable for edge computing environments, which often consist of smaller, distributed computing devices that operate outside of controlled data centers.
- To optimize edge-based lifecycle management, new management platforms and products have been developed that adapt cloud management technologies to the edge cloud. These platforms and products use NFV-like management and orchestration models to enable efficient service and application lifecycle management in edge computing environments.
- The challenge of optimal edge-based lifecycle management is therefore a critical issue for the successful deployment of IoT applications that leverage edge computing. By developing new management techniques and tools that are specifically tailored to the unique requirements of edge computing environments, it is possible to improve the efficiency, performance, and reliability of IoT applications, and unlock the full potential of the IoT.
- Managing the lifecycle of edge-based IoT devices and systems can be challenging due to the dispersed nature of these devices, which can be in remote or hard-to-reach locations. This can make it difficult to deploy, update, and maintain these devices, as well as to monitor and troubleshoot issues.

### Source:

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

### Application - Industry Domain

- Horizontal

## 2.26 Optimal Edge Organization and Federation

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

- Scalable device deployment

### Description of edge computing challenge-research/standardisation requirements

- In a distributed system, edge devices can come together and form clusters or hierarchies once they have been authenticated and discovered. The organization structure can range from centralized to peer-to-peer and may be closely linked to other systems or even form federations with remote clouds or other edge devices.
- To make this possible, there are several challenges that need to be addressed, including: 1) Scaling support, fault tolerance, and self-healing mechanisms: This can be achieved by using hierarchical organization or multicast methods to handle scaling challenges. 2) Integration of edge computing with virtualized Radio Access Networks (Fog RAN) and 5G access networks. 3) Resource sharing in multi-vendor or operator scenarios, which can optimize criteria like profit, resource usage, latency, or energy consumption. 4) Capacity planning, where the placement of infrastructure nodes is optimized to minimize delays, costs, energy consumption, etc. 5) Incentives for participation in peer-to-peer federation schemes.
- To address the gap for optimal edge organization and federation, it's important to have a comprehensive edge organization and federation strategy in place. This should include the ability to organize and group devices and systems based on their function, location, or other relevant criteria, as well as to federate devices and systems that are spread out across different geographic locations or networks. Additionally, it's important to have the ability to manage and analyze data collected at the edge, this can be achieved through the use of edge computing, which allows to process and analyze data locally on the device, reducing the need for communication with the cloud.
- The gap for optimal edge organization and federation in IoT refers to the challenge of effectively organizing and federating the large number of edge devices and systems that make up an IoT ecosystem. With the increasing number of IoT devices and systems, it can be difficult to manage and coordinate the data and information that is being collected and transmitted by these devices.

### Source:

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

### Application - Industry Domain

- Horizontal

## 2.27 Multi-Tenancy at the Isolation

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

- Solution deployment and maintenance tools

### Description of edge computing challenge-research/standardisation requirements

- IoT edge computing systems sometimes use virtualized resources for secure multi-tenancy at the edge. This creates "edge clouds" that have similar properties to the remote Cloud and can leverage some of its ecosystem. Standards activities such as ETSI NFV and MEC address virtualization function management to a large extent. There are also projects that focus on virtualization and its management in distributed edge computing environments.
- There are several related challenges to consider, including adapting cloud management platforms to the edge to account for its distributed nature, dealing with heterogeneity and customization using

intent-based management mechanisms, and working with limited resources. Additionally, minimizing the time and resources needed for virtual function instantiation is an important consideration.

- These technologies are designed to enable the creation of highly distributed systems that can support a wide range of applications and use cases. However, because of their distributed nature, they can also introduce security risks if not properly managed.
- The gap in multi-tenancy and isolation in IoT refers to the challenge of ensuring that different users, organizations, and applications that share IoT devices and systems have the ability to securely and independently access and use the data and resources of the system.

### Source

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

### Application - Industry Domain

- Manufacturing
- Horizontal

## 2.28 Efficient OAM (Operations, Administration, and Maintenance) at the Edge

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

- Operational

### Description of edge computing challenge-research/standardisation requirements

- Edge computing environments are typically distributed, heterogeneous, and located in remote or hard-to-reach locations, which can make OAM more challenging than in traditional data center environments
- The emergence of the Internet of Things (IoT) and the proliferation of edge computing have brought about a significant transformation in the way we interact with and manage our devices and networks. With the growing number of connected devices and the increasing demand for real-time processing and analysis of data at the edge, efficient OAM (Operations, Administration, and Maintenance) has become a critical challenge for organizations.
- Efficient OAM is essential to ensure the optimal performance, availability, and reliability of edge devices and networks. OAM encompasses a broad range of activities, including device and network configuration, monitoring, troubleshooting, and repair. At the edge, OAM is even more critical as devices may be distributed over a large area and operate in challenging environments, which makes them harder to manage and maintain.
- The challenge of efficient OAM at the edge stems from several factors. Firstly, edge devices and networks are often highly distributed, and traditional centralized OAM solutions may not be adequate to manage them effectively. Secondly, edge devices and networks may operate in remote or harsh environments, making it difficult to perform maintenance and repairs on-site. Thirdly, edge devices and networks may generate large volumes of data, which need to be processed and analyzed in real-time, making it challenging to detect and diagnose issues quickly.
- Moreover, inefficient OAM at the edge can have severe consequences, such as downtime, data loss, and security breaches. For example, a malfunctioning edge device in a manufacturing plant can cause significant production downtime, resulting in revenue loss. In a healthcare setting, a malfunctioning

edge device can compromise patient safety, leading to legal and reputational damage.

- Addressing the challenge of efficient OAM at the edge requires a holistic approach that takes into account the unique characteristics of edge devices and networks. This approach involves leveraging new technologies such as artificial intelligence, machine learning, and automation to streamline OAM processes and improve decision-making. It also requires the development of new OAM tools and techniques that can operate in challenging environments and provide real-time insights into device and network health.
- In conclusion, the challenge of efficient OAM at the edge is critical for organizations that rely on edge devices and networks to deliver real-time insights and services to their customers. Addressing this challenge requires a concerted effort to develop new technologies, tools, and techniques that can streamline OAM processes and ensure optimal performance, availability, and reliability of edge devices and networks.
- The OAM gap refers to a deficiency or a missing element in the current state of managing and maintaining the edge infrastructure. Specifically, it pertains to the need for more effective and streamlined OAM processes to ensure efficient operations, administration, and maintenance of edge devices and networks. The gap implies a discrepancy between the existing state and the desired state of OAM at the edge, which needs to be addressed for optimal performance and reliability of edge infrastructure.

### Source

- https://datatracker.ietf.org/doc/draft-ietf-detnet-oam-framework/
- https://www.ietf.org/id/draft-ietf-raw-oam-support-06.html
- https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

### Application - Industry Domain

- Horizontal

## 2.29 Edge Analytics

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

- Operational

### Description of edge computing challenge-research/standardisation requirements

- Ensuring that the data processing and analytics capabilities at the edge are sufficient to handle the volume and velocity of data being generated.
- One critical aspect of edge computing in the Internet of Things (IoT) is storing and processing data at the edge. This directly tackles the significant IoT challenges outlined in Section 3. Specialized hardware support on computing nodes can enhance data analysis, such as those required in artificial intelligence (AI) and machine learning (ML) tasks performed at the edge.
- There are several related challenges, including addressing resource usage, security, and privacy concerns when sharing, processing, discovering, or managing data. Some of the approaches to tackle these challenges include presenting data in views consisting of related data aggregation, protecting data communication between authorized peers, classifying data based on privacy, importance, or validity, compressing and encrypting data, and using homomorphic encryption to process encrypted data directly. Edge data discovery presents other challenges, such as siloization and the lack of standards in dynamic and heterogeneous edge environments like vehicular networks. Data-driven

programming models that handle naming and data abstractions, including event-based models, are also essential.

- Deploying machine learning at the edge requires addressing challenges such as limited resources, privacy, dynamic and heterogeneous environments. Lightweight and distributed machine learning models, shorter training times and simplified models, and compressed models for efficient communication are some ways to address these challenges. Furthermore, while edge computing can support IoT services independently of cloud computing, it can also be connected to cloud computing. Therefore, the relationship between IoT edge computing and cloud computing regarding data management is another potential challenge.
- The Gap of the Edge Analytics refers to the need for developing and implementing efficient techniques and tools for performing real-time data analytics at the edge of the network, where data is generated, collected, and processed. This gap is related to the challenge of extracting valuable insights from large and diverse data sources in a timely and efficient manner, without the need to transfer all data to the cloud or a centralized location for analysis. Edge Analytics aims to bridge this gap by enabling data processing and analysis to be performed closer to the source, reducing latency, bandwidth requirements, and enhancing the overall performance and scalability of IoT systems.

### Source

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

### Application - Industry Domain

- Horizontal

## 2.30 Edge-to-Cloud Integration

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

- Operational

### Description of edge computing challenge-research/standardisation requirements

- The Challenge of Edge-to-Cloud Integration arises from the need to effectively utilize the distributed computing resources of edge devices and cloud services in an integrated and coordinated manner. With the increasing adoption of the Internet of Things (IoT) and other edge computing applications, the need for processing, analyzing, and storing data in real-time at the edge of the network has become critical. At the same time, cloud services continue to play a significant role in providing high-level computation, storage, and analytics capabilities. To address these requirements, it is necessary to integrate and coordinate data processing and communication between edge devices and cloud services.
- Edge devices are often resource-constrained, with limited processing power, memory, and storage capacity, and are deployed in remote or harsh environments, making them challenging to manage and maintain. On the other hand, cloud services offer vast computing resources, high scalability, and sophisticated analytics tools but are located remotely, leading to potential issues such as high latency, limited bandwidth, and privacy concerns. Moreover, data generated at the edge is often time-sensitive, and decision-making needs to be done quickly and accurately, necessitating real-time processing and analysis.
- Edge-to-Cloud Integration addresses these challenges by providing a way to seamlessly integrate data processing and communication between edge devices and cloud services, ensuring the efficient utilization of computing resources, minimizing latency, and optimizing the overall performance of the system. It also enables the implementation of a distributed computing architecture that can handle

large volumes of data generated at the edge and support advanced analytics applications such as machine learning, predictive modeling, and anomaly detection.

- Overall, Edge-to-Cloud Integration is a critical challenge that needs to be addressed to realize the full potential of edge computing and IoT applications, enabling the development of innovative and efficient solutions to real-world problems.
- The gap of the Edge-to-Cloud Integration refers to the challenge of integrating and coordinating data processing and communication between edge devices and cloud services in an efficient and seamless manner. This gap is related to the need for designing and deploying hybrid architectures that enable data to be processed, analyzed, and stored both at the edge and the cloud, depending on the specific requirements of the application. Edge-to-Cloud Integration aims to bridge this gap by providing the necessary infrastructure, protocols, and standards for enabling secure and reliable communication, data sharing, and synchronization between edge devices and cloud services, while ensuring the optimal utilization of resources, performance, and scalability of the entire system

### Source

- https://datatracker.ietf.org/doc/html/rfc8568

### Application - Industry Domain

- Horizontal

## 2.31 Cost of Edge infrastructure

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

- Data Usage Accounting

### Description of edge computing challenge-research/standardisation requirements

- The deployment and maintenance of edge infrastructure can be a costly endeavor, especially considering the sheer volume of devices and systems that may be involved in edge computing environments. Therefore, optimizing the cost of deploying and maintaining edge infrastructure is an important challenge that needs to be addressed in order to make edge computing a more viable and cost-effective solution.
- One aspect of optimizing the cost of edge infrastructure is the selection and procurement of hardware components. Edge devices are often resource-constrained, meaning that they have limited processing power, memory, and storage capacity. Therefore, it is important to select hardware components that are optimized for edge computing workloads, while also being cost-effective. This includes selecting processors that are energy-efficient, yet powerful enough to handle edge workloads, and choosing storage devices that have a high capacity, yet are affordable.
- Another aspect of optimizing the cost of edge infrastructure is the management of software components. Edge computing environments often involve a large number of software components, including operating systems, middleware, and applications. It is important to manage these components in a way that minimizes software licensing costs, while also ensuring that the software components are compatible with each other and with the hardware components.
- In addition to hardware and software costs, networking costs are also an important consideration when deploying and maintaining edge infrastructure. Edge devices often need to communicate with each other and with cloud-based systems, which can result in high networking costs. Therefore, optimizing networking costs involves selecting networking technologies that are optimized for edge computing workloads, while also being affordable.

- Overall, optimizing the cost of deploying and maintaining edge infrastructure is an important challenge that needs to be addressed in order to make edge computing a more cost-effective and sustainable solution. This involves careful consideration of hardware, software, and networking costs, as well as the development of best practices and standards for managing and optimizing these costs in edge computing environments.
- The Gap includes the importance of addressing the economic aspects of edge computing, including the cost-effectiveness of deploying and managing edge devices, the return on investment for edge computing solutions, and the potential benefits of edge computing in various industries.

### Source

- "Samanta, Amit, and Yong Li. "Time-to-think: Optimal economic considerations in mobile edge computing." IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2018." https://ieeexplore.ieee.org/abstract/document/8406828
- Egwuche, O. S., M. Ganiyu, and M. A. Ibiyomi. "A survey of mobile edge computing in developing countries: Challenges and prospects." Journal of Physics: Conference Series. Vol. 2034. No. 1. IOP Publishing, 2021.
- https://iopscience.iop.org/article/10.1088/1742-6596/2034/1/012004/pdf

### Application - Industry Domain

- Horizontal

## 2.32 Edge Environmental Considerations

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

- Green Technologies

### Description of edge computing challenge-research/standardisation requirements

- As edge computing continues to gain traction, it is important to consider its impact on the environment. The increasing number of edge devices and systems can lead to significant energy consumption, which can in turn contribute to climate change and other environmental issues. Additionally, the disposal of electronic waste (e-waste) generated by edge devices and systems can create additional environmental concerns.
- To address these issues, it is important to consider environmental considerations in the design, deployment, and operation of edge computing systems. This may involve the use of energy-efficient hardware and software, the deployment of renewable energy sources, and the implementation of recycling and waste management practices for e-waste generated by edge systems.
- Therefore, the gap of Edge Environmental Considerations highlights the need for the development of best practices and standards for sustainable and environmentally responsible practices in edge computing. This includes considerations such as energy consumption, carbon footprint, and e-waste generation, as well as the development of tools and methodologies for measuring and managing the environmental impact of edge computing systems.
- Edge Environmental Considerations refer to the need to address the environmental impact of edge computing, including issues such as energy consumption, carbon footprint, and e-waste generation. This gap highlights the need for sustainable and environmentally responsible practices in the design, deployment, and operation of edge computing systems.

## Source

- https://www.ietf.org/id/draft-cx-green-ps-02.html

## Application - Industry Domain

- Horizontal

# 3 Standardisation Gaps

The previous section introduced the edge computing research and standardisation challenges that have been identified either from the edge computing 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 edge computing challenges in standardisation gaps.

## 3.1 Definition and classification of standards gaps

The definition of a Standard Gap are 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 edge computing standardization landscape
- Examples of standardization gaps are: missing standards or regulations, missing APIs, technical interoperability profiles that would clarify the use cases, duplications that would require harmonization.

## 3.2 Standardisation Gaps: Identification

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

The result of this brainstorming was to identify which edge computing 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 edge computing challenges that required more research before being standardised are the edge computing challenges:

- "2.4 Explainable AI using human argumentation research challenges"
- "2.7 IoT and edge computing in Digital service transformation"
- "2.18 Federated Learning and AI for IoT Edge"
- "2.31 Cost of Edge infrastructure"

The rest of the edge computing challenges can be considered to be standardisation challenges.

## 3.3 Standardisation Gaps: Prioritisation

This section provides a prioritisation of edge computing standardisation gaps in terms of their impact in the edge computing landscape. The method of prioritising the standardisation gaps is by investigating the standardisation activities in SDOs, such as 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 Edge computing 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 edge computing community, depending on the breadth and complexity of the gap.

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

## 4.2 EUOS identified edge computing challenges covered/worked out by SDOs

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

The EUOS "Landscape of Edge Computing 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 Edge Computing 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 Edge Computing 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 Edge Computing challenges covered/worked out by ETSI.

The rest of the tables that show how the EUOS identified Edge Computing 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 "Annex I Tables including EUOS edge challenges covered by SDOs"

*Table 1: EUOS identified Edge Computing challenges covered/worked out by ETSI*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GS MEC 010-1 V1.1.1 (2017-10): Mobile Edge Management; Part 1: System, host and platform management | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01001/01.01.01_60/gs_mec01001v010101p.pdf | The document defines the management of the mobile edge system, mobile edge hosts and mobile edge platforms. This includes platform configuration, performance and fault management, application monitoring, remote service configuration and service control, information gathering regarding the platform features, available services, and available virtualised resources. | S.20 (IoT systems integration)<br>S2.21 (IoT sectorial and cross-sectorial open platforms)<br>S2.22 (IoT and edge computing platforms) |
| ETSI | ETSI GS MEC-IEG 006 V1.1.1 (2017-01): MEC Metrics Best Practice and Guidelines | https://www.etsi.org/deliver/etsi_gs/MEC-IEG/001_099/006/01.01.01_60/gs_mec-ieg006v010101p.pdf | The document describes various metrics which can potentially be improved through deploying a service on a MEC platform. Example use cases are used to demonstrate where improvements to a number of key performance indicators can be identified in order to highlight the benefits of deploying MEC for various services and applications. Furthermore, the document describes best practices for measuring such performance metrics and these techniques are further exemplified with use cases. Metrics described in the present document can be taken from service requirements defined by various organizations (e.g. 5G service requirements defined by Next Generation Mobile Networks (NGMN) or 3rd Generation Partnership Project (3GPP)). An informative annex is used to document such desired and/or achieved ranges of performance which could be referenced from the main body of the present document. | S.2.23 (Need for real-time or near real-time processing and decision-making) |
| ETSI | ETSI GS MEC 016 V2.2.1 (2020-04): Multi-access Edge Computing (MEC); Device application interface | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/016/02.02.01_60/gs_mec016v020201p.pdf | The document contains the API definition for the lifecycle management of user applications over the Mx2 reference point between the device application and the User Application LifeCycle Management Proxy (UALCMP) in the MEC system. The document covers the following lifecycle management operations: user application look-up, instantiation and termination. In addition, a mechanism is specified for the exchange of lifecycle management related information between the MEC system and the device application. The intended key audience of the present document are the application developers for the MEC system, since this API provides them with a method to manage their applications. | S2.14 (Devices and open device management) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GS MEC 011 V2.2.1 (2020-12): Multi-access Edge Computing (MEC); Edge Platform Application Enablement | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/02.02.01_60/gs_mec011v020201p.pdf | The document focuses on the functionalities enabled via the Mp1 reference point between MEC applications and MEC platform, which allows these applications to interact with the MEC system. Service related functionality includes registration/deregistration, discovery and event notifications. Other functionality includes application availability, traffic rules, DNS and time of day. It describes the information flows, required information, and specifies the necessary operations, data models and API definitions. | S2.21 (IoT sectorial and cross-sectorial open platforms)<br>S2.22 (IoT and edge computing platforms) |
| ETSI | ETSI GS MEC 013 V2.1.1 (2019-09): Multi-access Edge Computing (MEC); Location API | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/013/02.01.01_60/gs_mec013v020101p.pdf | The document focuses on the MEC Location Service. It describes the related application policy information including authorization and access control, information flows, required information and service aggregation patterns. The document specifies the necessary API with the data model and data format. It is to be noted that the actual data model and data format which is functional for the present API re-uses the definitions in "RESTful Network API for Zonal Presence" and "RESTful Network API for Terminal Location" published by the Open Mobile Alliance. | S2.10 (Service discovery support) |
| ETSI | ETSI GS MEC 010-2 V2.1.1 (2019-11): Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01002/02.01.01_60/gs_mec01002020101p.pdf | The document provides information flows for lifecycle management of applications running on a MEC host, and describes interfaces over the reference points to support application lifecycle management. It also describes application rules and requirements, application-related events, mobility handling and MEC service availability tracking. The document specifies the necessary data model, data format and operation format when applicable. | S2.25 (Optimal edge-based lifecycle management) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GR MEC 035 V3.1.1 (2021-06): Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination | https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_mec035v030101p.pdf | The document studies the applicability of MEC specifications to inter-MEC systems and MEC-Cloud systems coordination that supports e.g. application instance relocation, synchronization and similar functionalities. Another subject of this study is the enablement and/or enhancement of functionalities for application lifecycle management by third parties (e.g. application developers). | S2.16 (Support of interoperability)<br>S2.30 (Edge-to-cloud integration) |
| ETSI | ETSI GS MEC 014 V2.1.1 (2021-03): Multi-access Edge Computing (MEC); UE Identity API | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/014/02.01.01_60/gs_mec014v020101p.pdf | The document focuses on the UE Identity functionality. It describes the related application policy information (including authorization, access control and traffic rule pattern format), information flows, required information and service aggregation patterns. The document specifies the necessary API, data model and data format, considering existing API(s) if applicable. | S2.11 (Authentication of services and service providers) |

# 5. Standards Gaps Analysis and Recommendations

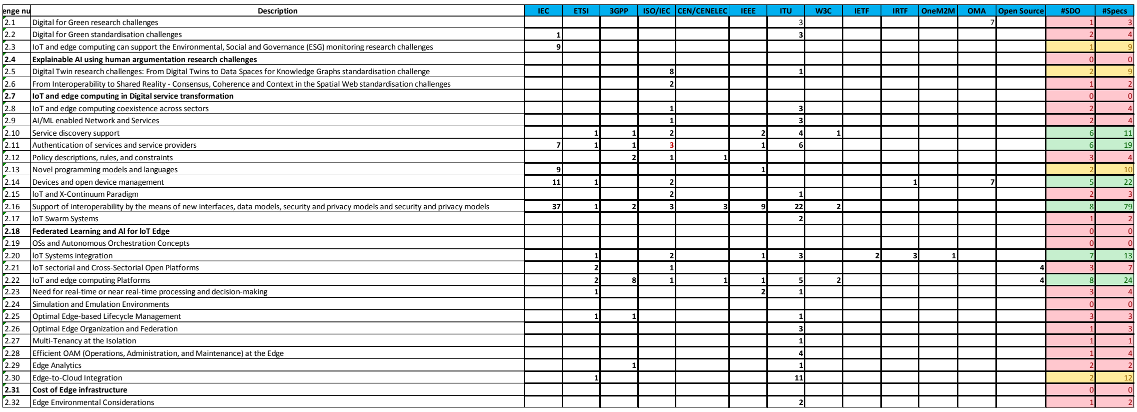
Section 4.2 of this report together with the **Annex I** provides an analysis on whether the 32 EUOS identified edge computing challenges, specified in Section 2 of this report are covered/worked out in the 230 SDO specifications that were listed in the EUOS "Landscape of Edge Computing Standards" report.

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 edge computing challenges.

- Based on a brainstorming with the EUOS community, it has been concluded that depending on the level of the intensity that an edge computing 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 edge computing challenges covered/worked out by SDOs*



| enge nu | Description | IEC | ETSI | 3GPP | ISO/IEC | CEN/CENELEC | IEEE | ITU | W3C | IETF | IRTF | OneM2M | OMA | Open Source | #SDO | #Specs |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.1 | Digital for Green research challenges | | | | | | | 3 | | | | | 7 | | 1 | 3 |
| 2.2 | Digital for Green standardisation challenges | 1 | | | | | | 3 | | | | | | | 2 | 4 |
| 2.3 | IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges | 9 | | | | | | | | | | | | | 1 | 9 |
| **2.4** | **Explainable AI using human argumentation research challenges** | | | | | | | | | | | | | | 0 | 0 |
| 2.5 | Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge | | | | 8 | | | 1 | | | | | | | 2 | 9 |
| 2.6 | From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges | | | | 2 | | | | | | | | | | 1 | 2 |
| **2.7** | **IoT and edge computing in Digital service transformation** | | | | | | | | | | | | | | 0 | 0 |
| 2.8 | IoT and edge computing coexistence across sectors | | | | 1 | | | 3 | | | | | | | 2 | 4 |
| 2.9 | AI/ML enabled Network and Services | | | | 1 | | | 3 | | | | | | | 2 | 4 |
| 2.10 | Service discovery support | | 1 | 1 | 2 | | 2 | 4 | 1 | | | | | | 6 | 11 |
| 2.11 | Authentication of services and service providers | 7 | 1 | 1 | 3 | | 1 | 6 | | | | | | | 6 | 19 |
| 2.12 | Policy descriptions, rules, and constraints | | | 2 | 1 | 1 | | | | | | | | | 3 | 4 |
| 2.13 | Novel programming models and languages | 9 | | | | | 1 | | | | | | | | 2 | 10 |
| 2.14 | Devices and open device management | 11 | 1 | | 2 | | | | | | 1 | | 7 | | 5 | 22 |
| 2.15 | IoT and X-Continuum Paradigm | | | | 2 | | | 1 | | | | | | | 2 | 3 |
| 2.16 | Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models | 37 | 1 | 2 | 3 | 3 | 9 | 22 | 2 | | | | | | 8 | 79 |
| 2.17 | IoT Swarm Systems | | | | | | | 2 | | | | | | | 1 | 2 |
| **2.18** | **Federated Learning and AI for IoT Edge** | | | | | | | | | | | | | | 0 | 0 |
| 2.19 | OSs and Autonomous Orchestration Concepts | | | | | | | | | | | | | | 0 | 0 |
| 2.20 | IoT Systems integration | | 1 | | 2 | | 1 | 3 | | 2 | 3 | 1 | | | 7 | 13 |
| 2.21 | IoT sectorial and Cross-Sectorial Open Platforms | | 2 | | 1 | | | | | | | | | 4 | 3 | 7 |
| 2.22 | IoT and edge computing Platforms | | 2 | 8 | 1 | 1 | 1 | 5 | 2 | | | | | 4 | 8 | 24 |
| 2.23 | Need for real-time or near real-time processing and decision-making | | 1 | | | | 2 | 1 | | | | | | | 3 | 4 |
| 2.24 | Simulation and Emulation Environments | | | | | | | | | | | | | | 0 | 0 |
| 2.25 | Optimal Edge-based Lifecycle Management | | 1 | 1 | | | | 1 | | | | | | | 3 | 3 |
| 2.26 | Optimal Edge Organization and Federation | | | | | | | 3 | | | | | | | 1 | 3 |
| 2.27 | Multi-Tenancy at the Isolation | | | | | | | 1 | | | | | | | 1 | 1 |
| 2.28 | Efficient OAM (Operations, Administration, and Maintenance) at the Edge | | | | | | | 4 | | | | | | | 1 | 4 |
| 2.29 | Edge Analytics | | | 1 | | | | 1 | | | | | | | 2 | 2 |
| 2.30 | Edge-to-Cloud Integration | | 1 | | | | | 11 | | | | | | | 2 | 12 |
| **2.31** | **Cost of Edge infrastructure** | | | | | | | | | | | | | | 0 | 0 |
| 2.32 | Edge Environmental Considerations | | | | | | | 2 | | | | | | | 1 | 2 |

**Figure 1** and **Figure 2.** provide a more detailed overview of the intensity that an edge computing standardisation challenge is covered/worked out by an SDO and by specifications, respectively.

The edge computing 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.

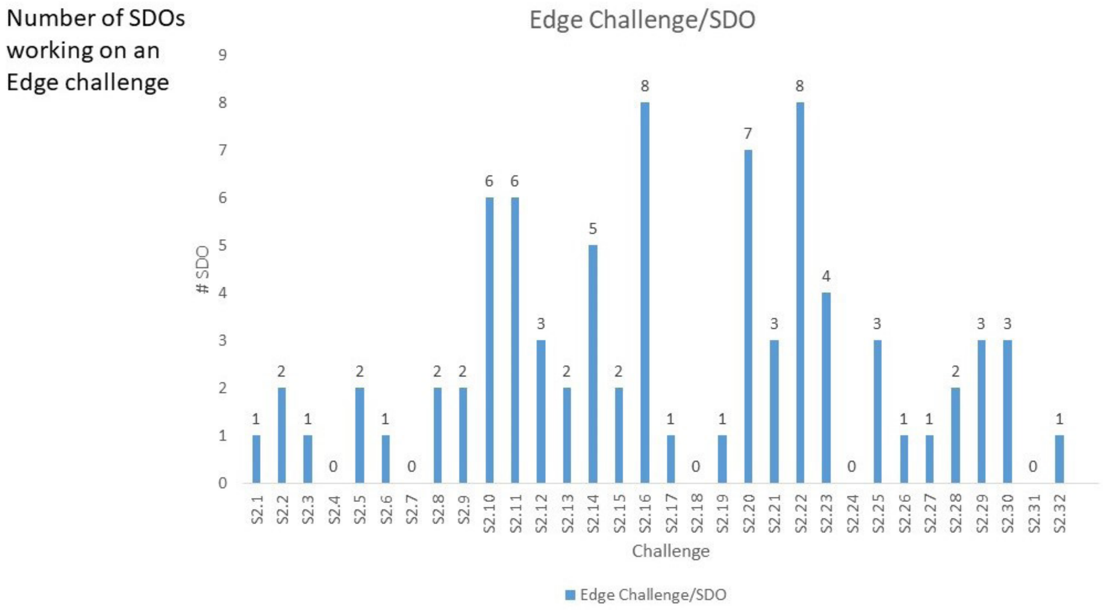


*Figure 1*

*Number of SDOs covering / working out an EUOS edge computing identified challenge*

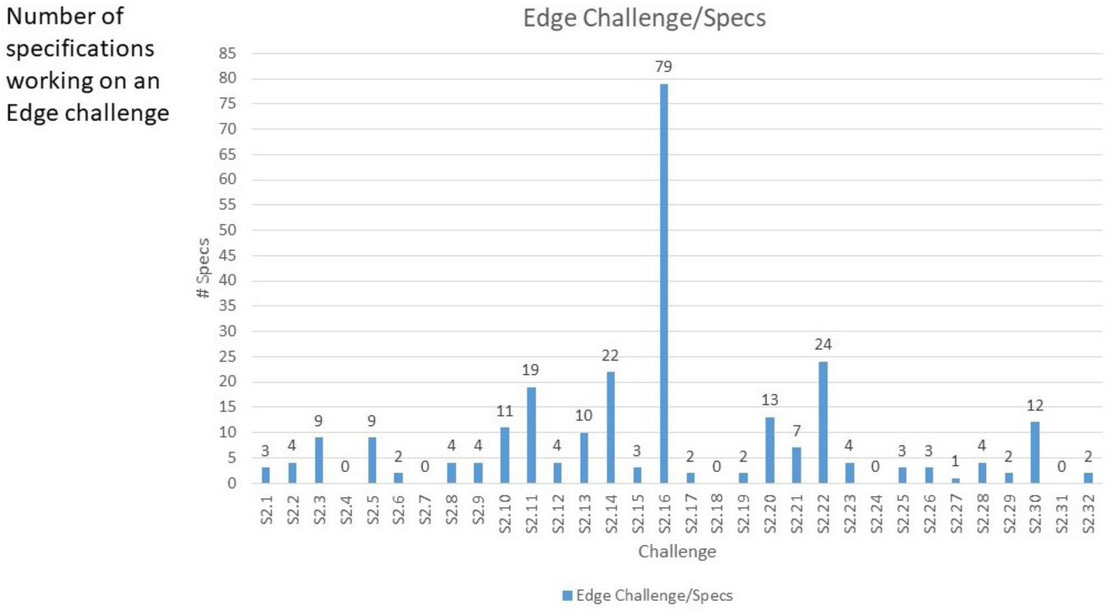


*Figure 2*

*Number of specifications covering / working out an EUOS edge computing identified challenge*

From this analysis it can be concluded that:

- the following edge computing challenges need more research before being standardised:
  - "2.4 Explainable AI using human argumentation research challenges"
  - "2.7 IoT and edge computing in Digital service transformation"
  - "2.18 Federated Learning and AI for IoT Edge"
  - "2.31 Cost of Edge infrastructure"
- the following edge computing standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - 2.1 Digital for Green research challenges
  - 2.2 Digital for Green standardisation challenges
  - 2.6 From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges
  - 2.8 IoT and edge computing coexistence across sectors
  - 2.9 AI/ML enabled Network and Services
  - 2.12 Policy descriptions, rules, and constraints
  - 2.15 IoT and X-Continuum Paradigm
  - 2.17 IoT Swarm Systems
  - 2.19 OSs and Autonomous Orchestration Concepts
  - 2.21 IoT sectorial and Cross-Sectorial Open Platforms
  - 2.23 Need for real-time or near real-time processing and decision-making
  - 2.24 Simulation and Emulation Environments
  - 2.25 Optimal Edge-based Lifecycle Management
  - 2.26 Optimal Edge Organization and Federation
  - 2.27 Multi-Tenancy at the Isolation
  - 2.28 Efficient OAM (Operations, Administration, and Maintenance) at the Edge
  - 2.29 Edge Analytics
  - 2.32 Edge Environmental Considerations
- the following edge computing standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
  - 2.3 IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges
  - 2.5 Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge
  - 2.13 Novel programming models and languages
  - 2.30 Edge-to-Cloud Integration

# 6 Conclusion

This report presented an approach for the definition and identification of key edge computing 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 Edge Computing 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 edge computing challenges, Section 3 describes the identification and prioritisation of the EUOS identified edge computing 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 230 SDOs specifications to the 32 edge computing challenges identified by EUOS and presented in Section 2. Based on this analysis it can be concluded that:

- the following edge computing challenges need more research before being standardised:
  - "2.4 Explainable AI using human argumentation research challenges"
  - "2.7 IoT and edge computing in Digital service transformation"
  - "2.18 Federated Learning and AI for IoT Edge"
  - "2.31 Cost of Edge infrastructure"
- the following edge computing standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - 2.1 Digital for Green research challenges
  - 2.2 Digital for Green standardisation challenges
  - 2.6 From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges
  - 2.8 IoT and edge computing coexistence across sectors
  - 2.9 AI/ML enabled Network and Services
  - 2.12 Policy descriptions, rules, and constraints
  - 2.15 IoT and X-Continuum Paradigm
  - 2.17 IoT Swarm Systems
  - 2.19 OSs and Autonomous Orchestration Concepts
  - 2.21 IoT sectorial and Cross-Sectorial Open Platforms
  - 2.23 Need for real-time or near real-time processing and decision-making
  - 2.24 Simulation and Emulation Environments
  - 2.25 Optimal Edge-based Lifecycle Management
  - 2.26 Optimal Edge Organization and Federation
  - 2.27 Multi-Tenancy at the Isolation
  - 2.28 Efficient OAM (Operations, Administration, and Maintenance) at the Edge
  - 2.29 Edge Analytics

    - 2.32 Edge Environmental Considerations
- the following edge computing standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
    - 2.3 IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges
    - 2.5 Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge
    - 2.13 Novel programming models and languages
    - 2.30 Edge-to-Cloud Integration

# Annex I Tables including EUOS edge challenges covered by SDOs

*Table* 1: EUOS indentified Edge Computing challenges covered/worked out by IEC

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 61406 ED1 | https://www.iec.ch/ords/f?p=103:38:401030832849310::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,104621 | IEC 61406-1:2022 specifies minimum requirements for a globally unique identification of physical objects which also constitutes a link to its related digital information. This identification is designated hereinafter as "Identification Link" (IL), with the encoded data designated as IL string. The IL string has the data-format of a link (URL). The IL is machine-readable and is attached to the physical object in a 2D symbol or NFC tag. The requirements in this standard apply to physical objects:<br>that are provided by the manufacturer as an individual unit,<br>and that have already been given a unique identity by the manufacturer.<br>This document does not specify any requirements on the content and the layout of nameplates/typeplates (e.g. spatial arrangement, content of the plain texts, approval symbols etc.<br>(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:<br>they are passive in that they contain no optoelectronic or other transducing elements;<br>they have two ports for the transmission of optical power and control of the transmitted power in a fixed or variable fashion;<br>– the ports are non-connectorized optical fibre pigtails, connectorized optical fibres or receptacles. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| | | | This document establishes generic requirements for the following passive optical devices:<br>– optical attenuator;<br>– optical fuse;<br>– optical power limiter.<br>This document also provides generic information including terminology for the IEC 61753-05x series. Published IEC 61753-05x series documents are listed in Bibliography<br>This fifth edition cancels and replaces the fourth edition published in 2012 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:<br>a) the terms and definitions have been reviewed;<br>b) the requirement concerning the IEC Quality Assessment System has been reviewed;<br>c) the clause concerning quality assessment procedures has been deleted;<br>d) Annex G, relating to technical information on variable optical attenuators, has been added.<br>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:<br>- they are passive, in that they contain no optoelectronic or other transducing elements;<br>- 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;<br>- 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:<br>- removal of terms and definitions for splitter, coupler, symmetric non-wavelength-selective branching device, asymmetric non-wavelength-selective branching device; | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| | | | - addition of terms and definitions for bidirectional non-wavelength-selective branching device and non-bidirectional non-wavelength-selective branching device, removal of assessment level.<br>Keywords: non-wavelength-selective fibre optic branching devices, uniform requirements for the optical, mechanical and environmental properties. | |
| IEC | IEC 61300-1:2022 | https://webstore.iec.ch/publication/67663 | 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.<br>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:<br>- addition of the information of measurement uncertainties in 4.2.1;<br>- change of the requirements for attenuation variation in 4.2.2;<br>- addition of the multimode launch conditions of other fibres than A1-OM2, A1-OM3, A1-OM4, A1-OM5 and A3e in 10.4;<br>- addition of the multimode launch conditions of the planer waveguide in 10.6;<br>- splitting Annex A for EF and Annex B for EAF;<br>- correction of errors in the definitions of encircled flux and encircled angular flux. | |

| SDO | Specification | | | Relevant EUOS identified Edge 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.<br>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:<br>a) definitions updated with new products: wall outlets, wall or pole mounted boxes, splices, ODF modules, street cabinets, hardened connectors and field mountable connectors;<br>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;<br>c) addition of Category I (Industrial);<br>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");<br>e) the height of category A changed from 3 m to ground level (0 m);<br>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;<br>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;<br>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; | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| | | | 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);<br>j) test severity of "Flexing of strain relief" test for connectors in categories C, OP and OP+ is reduced to 50 cycles;<br>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;<br>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);<br>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;<br>n) sealing performance criteria of sealed closures for categories G and A are reduced to 20 kPa overpressure.<br>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).<br>Keywords: performance standards for all passive fibre optic productsThe contents of the corrigendum of May 2019 have been included in this copy. | |
| IEC | IEC 61754-4:2022 | https://webstore.iec.ch/publication/29284 | IEC 61754-4:2022 is available as <a href="https://webstore.iec.ch/publication/74619">IEC 61754-4:2022 RLV</a> 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. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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.<br>Keywords: interface dimensions for type MPO connectors | |
| 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:<br>- addition of figures to show the interface between protective housing and fibre management system;<br>- addition of definitions for protective housing, closure, wall box, street cabinets and optical distribution frame modules;<br>- addition of table with dimensions of fusion splice protectors and mechanical splices;<br>- addition of method to identify the minimum bending radius for stored fibres;<br>- addition of clause for other factors relevant to fibre management systems;<br>- addition of annex A for example of calculating the minimum bending radius of stored fibres in a fibre management system.<br>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. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | |
| 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge 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:<br>- the (base) Device Model intended to provide a unified view of devices;<br>- the Device Communication Model which adds Network and Connection information elements so that communication topologies can be created;<br>- 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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| 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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge 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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| 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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62541-3:2020 | [https://webstore.iec.ch/publication/61112](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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| IEC | IEC 62541-4:2020 | [https://webstore.iec.ch/publication/61113](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. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| | | | 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: a) Added ability to resend all data of monitored items in a Subscription using the ResendData Method. b) Added support for durable Subscriptions (lifetime of hours or days). c) Added Register2 and FindServersOnNetwork Services to support network-wide discovery using capability filters. d) Removed definition of software certificates. Will be defined in a future edition. e) Extended and partially revised the redundancy definition. Added sub-range definitions for ServiceLevel and added more terms for redundancy. f) Added a section on how to use Authorization Services to request user access tokens. g) Added JSON Web Tokens (JWTs) as a new user token. h) Added the concept of session-less service invocation. i) Added a generic structure that allows passing any number of attributes to the AddNodes Service. j) Added requirement to protect against user identity token attacks. k) Added new EncryptedSecret format for user identity tokens. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62541-5:2020 | [https://webstore.iec.ch/publication/61114](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.<br>b) Added new data types: "Union", "Decimal", "OptionSet", "DateString", "TimeString", "DurationString", NormalizedString", "DecimalString", and "AudioDataType".<br>c) Added Method to request a state change in a Server. d) Added Method to set Subscription to persistent mode.<br>e) Added Method to request resending of data from a Subscription.<br>f) Added concept allowing to temporarily create a file to write to or read from a server in C.4.<br>g) Added new Variable type to support Selection Lists.<br>h) Added optional properties to FiniteStateMachineType to expose currently available states and transitions.<br>i) Added UrisVersion Property to ServerType. This version information can be used for session-less service invocation. | S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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:<br>• added JSON encoding for PubSub (non-reversible);<br>• added JSON encoding for Client/Server (reversible);<br>• added support for optional fields in structures;<br>• added support for Unions.<br>b) Transport mappings:<br>• added WebSocket secure connection – WSS;<br>• added support for reverse connectivity;<br>• added support for session-less service invocation in HTTPS.  c) Deprecated Transport (missing support on most platforms):<br>• SOAP/HTTP with WS-SecureConversation (all encodings).  d) Added mapping for JSON Web Token.<br>e) Added support for Unions to NodeSet Schema.<br>f) Added batch operations to add/delete nodes to/from NodeSet Schema.<br>g) Added support for multi-dimensional arrays outside of Variants.<br>h) Added binary representation for Decimal data types.  i) Added mapping for an OAuth2 Authorization Framework. | S2.11 (Authentication of services and service providers); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62541-7:2020 | https://webstore.iec.ch/publication/61116 | IEC 62541-7:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition.  IEC 62541-7:2020 defines the OPC Unified Architecture (OPC UA) Profiles. The Profiles in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs.<br>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. 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:<br>• profiles for global discovery and global certificate management;<br>• profiles for global KeyCredential management and global access token management;<br>• facet for durable subscriptions;<br>• standard UA Client Profile;<br>• profiles for administration of user roles and permissions.<br>b) new transport Profiles:<br>• HTTPS with JSON encoding;<br>• secure WebSockets (WSS) with binary or JSON encoding;<br>• reverse connectivity. | S2.11 (Authentication of services and service providers); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| | | | c) new security Profiles:<br>· transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy);<br>· securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15);<br>· securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP);<br>· user Token JWT (Jason Web Token). d) deprecated Security Profiles (due to broken algorithms):<br>· securityPolicy – Basic128Rsa15 (broken algorithm Sha1);<br>· securityPolicy – Basic256 (broken algorithm Sha1);<br>· transportSecurity – TLS 1.0 (broken algorithm RC4);<br>· transportSecurity – TLS 1.1 (broken algorithm RC4). e) deprecated Transport (missing support on most platforms):<br>· SOAP/HTTP with WS-SecureConversation (all encodings). | |
| IEC | IEC 62541-8:2020 | https://webstore.iec.ch/publication/61117 | IEC 62541-8:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-8:2020 is part of the overall OPC Unified Architecture (OPC UA) standard series and defines the information model associated with Data Access (DA). It particularly includes additional VariableTypes and complementary descriptions of the NodeClasses and Attributes needed for Data Access, additional Properties, and other information and behaviour. The complete address space model, including all NodeClasses and Attributes is specified in IEC 62541-3. The services to detect and access data are specified in IEC 62541-4. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:<br>a) added new VariableTypes for AnalogItems;<br>b) added an Annex that specifies a recommended mapping of OPC UA Dataccess to OPC COM DataAccess;<br>c) changed the ambiguous description of "Bad_NotConnected";<br>d) updated description for EUInformation to refer to latest revision of UNCEFACT units. | S2.11 (Authentication of services and service providers); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62541-9:2020 | https://webstore.iec.ch/publication/61118 | IEC 62541-9:2020 contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-9:2020 specifies the representation of Alarms and Conditions in the OPC Unified Architecture. Included is the Information Model representation of Alarms and Conditions in the OPC UA address space. Other aspects of alarm systems such as alarm philosophy, life cycle, alarm response times, alarm types and many other details are captured in documents such as IEC 62682 and ISA 18.2. The Alarms and Conditions Information Model in this specification is designed in accordance with IEC 62682 and ISA 18.2. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:<br>a) added optional engineering units to the definition of RateOfChange alarms;<br>b) to fulfill the IEC 62682 model, the following elements have been added:<br>- AlarmConditionType States: Suppression, Silence, OutOfService, Latched; - AlarmConditionType Properties: OnDelay, OffDelay, FirstInGroup, ReAlarmTime; - New alarm types: DiscrepencyAlarm, DeviationAlarm, InstrumentDiagnosticAlarm, SystemDiagnosticAlarm.<br>c) added Annex that specifies how the concepts of this OPC UA part maps to IEC 62682 and ISA 18.2;<br>d) added new ConditionClasses: Safety, HighlyManaged, Statistical, Testing, Training;<br>e) added CertificateExpiration AlarmType;<br>f) added Alarm Metrics model. | S2.11 (Authentication of services and service providers); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62714-1:2018 | https://webstore.iec.ch/publication/32339 | IEC 62714-1:2018 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition.<br>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.<br>This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision.<br>This edition includes the following significant technical changes with respect to the previous edition:  a) use of CAEX 3.0 according to IEC 62424:2016  b) improved modelling of references to documents outside of the scope of the present standard,  c) modelling of references between CAEX attributes and items in external documents,  d) revised role libraries,  e) modified Port concept,  f) modelling of multilingual expressions,  g) modelling of structured attribute lists or array,  h) a new AML container format,  i) a new standard AML attribute library | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEC | 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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 | IEC 63365:2022 applies to products used in the process measurement, control and automation industry. It establishes a concept and requirements for the digital nameplate and provides alternative electronically readable solutions (e.g. 2D codes, RFID or firmware) to current conventional plain text marking on the nameplate or packaging of products. The digital nameplate information is contained in the electronically readable medium affixed to the product, the packaging or accompanying documents. The digital nameplate information is available offline without Internet connection. After electronic reading, all digital nameplate information is displayed in a human readable text format. The digital nameplate also includes the Identification Link String according to IEC 61406-1 which provides additional online information for the product. This document does not specify the contents of the conventional nameplate, which are subject to regional or national regulations and standards.<br>(Under development) | |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 63278-2 ED1 | https://www.iec.ch/ dyn/www/f?p=103:38:731054763917753::::FSP_ORG_ID,FSP_APEX _PAGE,FSP _PROJECT_ID:1250,23,109017 | Asset Administration Shell for Industrial Applications – Part 2: Information meta model<br>(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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| 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:<br>- to define a common language for customers and suppliers through the publication of Lists of Properties (LOPs),<br>- to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations,<br>- to reduce transaction costs.<br>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.<br>This publication is to be read in conjunction with <a href=”http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/37363”>IEC 61987-1:2006</a>. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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". | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| | 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |
| 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 | Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 32: Lists of properties (LOP) for I/O modules for electronic data exchange<br>(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 | IEC 61987, Part 41: Generic structures of List of Properties (LOP) of Process Analyzer Technology (PAT) measuring devices for electronic data exchange<br>(Under development) | |
| 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. | S2.3 (IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.11 (Authentication of services and service providers); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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 | S2.11 (Authentication of services and service providers); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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). | S2.13 (Novel programming models and languages); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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. | S2.13 (Novel programming models and languages);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy 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. | S2.2 (Digital for Green standardisation challenges);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 63278-1 ED1 | https://www.iec.ch/ dyn/www/f?p=103:38:7310 54763917753::::FSP_ORG_ID,FSP_APEX _PAGE,FSP_PROJECT_ID 1250,23,103536 | IEC 63278-1:2023 defines the structure of a standardized digital representation of an asset, called Asset Administration Shell (AAS). The Asset Administration Shell gives uniform access to information and services. The purpose of the Asset Administration Shell is to enable two or more software applications to exchange information and to mutually use the information that has been exchanged in a trusted and secure way. This document focuses on Asset Administration Shells representing assets of manufacturing enterprises including products produced by those enterprises and the full hierarchy of industrial equipment. It defines the related structures, information, and services.<br>The Asset Administration Shell applies to:<br>any type of industrial process (discrete manufacturing, continuous process, batch process, hybrid production);<br>any industrial sector applying industrial-process measurement, control and automation;<br>the entire life cycle of assets from idea to end of life treatment;<br>assets which are physical, digital, or intangible entities.<br>(Under development | |
| IEC | IEC 63278-3 ED1 | https://www.iec.ch/ dyn/www/f?p=103:38:7310 54763917753::::FSP_ORG_ID,FSP_APEX _PAGE,FSP_PROJECT_ID:1250,23,109075 | IEC 63278-3 ED1: Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells<br>(Under development) | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 63339 ED1 | https://www.iec.ch/ dyn/www/f?p=103:38:7310 54763917753::::FSP_ORG_ID,FSP_APEX _PAGE,FSP_PROJECT_ID:1250,23,104329 | IEC 63339 ED1:2023 (EN) specifies the unified reference model for smart manufacturing (URMSM) using a terminology and structure, and establishes criteria for creating reference models, as specializations, that support smart manufacturing. The terminology and structure comprise a set of common modelling elements, their associations, and conformance criteria. These common modelling elements address aspects and perspectives of products and production and their lifecycle considerations.<br>The URMSM enables an approach for creating multiple models based upon a reference model that is sufficient for understanding significant relationships among entities involved in smart manufacturing (SM) and for the development of standards and other specifications.<br>(Under development) | |
| IEC | IEC 63376 ED1 | https://www.iec.ch/ dyn/www/f?p=103:38:7310 54763917753::::FSP_ORG_ID,FSP_APEX_ PAGE,FSP_PROJECT_ID:1250,23,104647 | IEC 63376:2023 specifies the functions and the information flows of industrial Facility Energy Management System (FEMS). Generic functions are defined for the FEMS, to enable upgrading traditional Energy Management System (EMS) from visualization of the status of energy consumption to automation of energy management defining a closer relation with other management and control systems. A generic method to classify the FEMS functions will be explained. The information exchange between the FEMS and other systems such as Manufacturing Operations Management (MOM), Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) will be outlined.<br>(Under development) | |
| | 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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). | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge 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.<br>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 | IEC 61987-31:2022 ED1: Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 31: List of Properties (LOPs) of infrastructure devices for electronic data exchange – Generic structures<br>(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 Edge 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:<br>· defining a system under consideration (SUC) for an industrial automation and control system (IACS);<br>· partitioning the SUC into zones and conduits;<br>· assessing risk for each zone and conduit;<br>· establishing the target security level (SL-T) for each zone and conduit; and<br>· documenting the security requirements. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC 62443-3-2:2020 | https://webstore.iec.ch/publication/30727 | IEC 62443-3-2:2020 establishes requirements for: a) defining a system under consideration (SUC) for an industrial automation and control system (IACS); b) partitioning the SUC into zones and conduits; c) assessing risk for each zone and conduit; d) establishing the target security level (SL-T) for each zone and conduit; and e) documenting the security requirements. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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).<br>As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs):<br>a) identification and authentication control (IAC),<br>b) use control (UC),<br>c) system integrity (SI),<br>d) data confidentiality (DC),<br>e) restricted data flow (RDF),<br>f) timely response to events (TRE), and<br>g) resource availability (RA).<br>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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEC | IEC TR 62443-2-3:2015 | https://webstore.iec.ch/publication/22811 | IEC TR 62443-2-3:2015(E) describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. This Technical Report recommends a defined format for the distribution of information about security patches from asset owners to IACS product suppliers, a definition of some of the activities associated with the development of the patch information by IACS product suppliers and deployment and installation of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however, it may also be applicable for non-security related patches or updates. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 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.<br>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. | S2.11 (Authentication of services and service providers); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEC | IEC 63237-1 ED1 | https://www.iec.ch/ dyn/www/f?p=103:7:602873313141987::::FSP_ORG_ID,FSP_LANG_ID:1275,25 | This part of IEC 63237 provides a method of standardizing the descriptions of household electrical appliances. The aims of this standard are: a) to define a common language for customers and suppliers through the publication of classes, represented by properties and their attributes; b) enable electronic data exchange by machines (including information technology systems, see M2M communication); c) to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations; d) to offer also a dictionary to legislators and; e) to reduce transaction costs.<br>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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

*Table 2: EUOS identified Edge Computing challenges covered/worked out by ETSI*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GS MEC 010-1 V1.1.1 (2017-10): Mobile Edge Management; Part 1: System, host and platform management | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01001/01.01.01_60/gs_mec01001v010101p.pdf | The document defines the management of the mobile edge system, mobile edge hosts and mobile edge platforms. This includes platform configuration, performance and fault management, application monitoring, remote service configuration and service control, information gathering regarding the platform features, available services, and available virtualised resources. | S.20 (IoT systems integration)<br>S2.21 (IoT sectorial and cross-sectorial open platforms)<br>S2.22 (IoT and edge computing platforms) |
| ETSI | ETSI GS MEC-IEG 006 V1.1.1 (2017-01): MEC Metrics Best Practice and Guidelines | https://www.etsi.org/deliver/etsi_gs/MEC-IEG/001_099/006/01.01.01_60/gs_mec-ieg006v010101p.pdf | The document describes various metrics which can potentially be improved through deploying a service on a MEC platform. Example use cases are used to demonstrate where improvements to a number of key performance indicators can be identified in order to highlight the benefits of deploying MEC for various services and applications. Furthermore, the document describes best practices for measuring such performance metrics and these techniques are further exemplified with use cases. Metrics described in the present document can be taken from service requirements defined by various organizations (e.g. 5G service requirements defined by Next Generation Mobile Networks (NGMN) or 3rd Generation Partnership Project (3GPP)). An informative annex is used to document such desired and/or achieved ranges of performance which could be referenced from the main body of the present document. | S.2.23 (Need for real-time or near real-time processing and decision-making) |
| ETSI | ETSI GS MEC 016 V2.2.1 (2020-04): Multi-access Edge Computing (MEC); Device application interface | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/016/02.02.01_60/gs_mec016v020201p.pdf | The document contains the API definition for the lifecycle management of user applications over the Mx2 reference point between the device application and the User Application LifeCycle Management Proxy (UALCMP) in the MEC system. The document covers the following lifecycle management operations: user application look-up, instantiation and termination. In addition, a mechanism is specified for the exchange of lifecycle management related information between the MEC system and the device application. The intended key audience of the present document are the application developers for the MEC system, since this API provides them with a method to manage their applications. | S2.14 (Devices and open device management) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GS MEC 011 V2.2.1 (2020-12): Multi-access Edge Computing (MEC); Edge Platform Application Enablement | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/02.02.01_60/gs_mec011v020201p.pdf | The document focuses on the functionalities enabled via the Mp1 reference point between MEC applications and MEC platform, which allows these applications to interact with the MEC system. Service related functionality includes registration/ deregistration, discovery and event notifications. Other functionality includes application availability, traffic rules, DNS and time of day. It describes the information flows, required information, and specifies the necessary operations, data models and API definitions. | S2.21 (IoT sectorial and cross-sectorial open platforms)<br>S2.22 (IoT and edge computing platforms) |
| ETSI | ETSI GS MEC 013 V2.1.1 (2019-09): Multi-access Edge Computing (MEC); Location API | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/013/02.01.01_60/gs_mec013v020101p.pdf | The document focuses on the MEC Location Service. It describes the related application policy information including authorization and access control, information flows, required information and service aggregation patterns. The document specifies the necessary API with the data model and data format. It is to be noted that the actual data model and data format which is functional for the present API re-uses the definitions in "RESTful Network API for Zonal Presence" and "RESTful Network API for Terminal Location" published by the Open Mobile Alliance. | S2.10 (Service discovery support) |
| ETSI | ETSI GS MEC 010-2 V2.1.1 (2019-11): Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01002/02.01.01_60/gs_mec01002v020101p.pdf | The document provides information flows for lifecycle management of applications running on a MEC host, and describes interfaces over the reference points to support application lifecycle management. It also describes application rules and requirements, application-related events, mobility handling and MEC service availability tracking. The document specifies the necessary data model, data format and operation format when applicable. | S2.25 (Optimal edge-based lifecycle management) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ETSI | ETSI GR MEC 035 V3.1.1 (2021-06): Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination | https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_mec035v030101p.pdf | The document studies the applicability of MEC specifications to inter-MEC systems and MEC-Cloud systems coordination that supports e.g. application instance relocation, synchronization and similar functionalities. Another subject of this study is the enablement and/or enhancement of functionalities for application lifecycle management by third parties (e.g. application developers). | S2.16 (Support of interoperability)<br>S2.30 (Edge-to-cloud integration) |
| ETSI | ETSI GS MEC 014 V2.1.1 (2021-03): Multi-access Edge Computing (MEC); UE Identity API | https://www.etsi.org/deliver/etsi_gs/MEC/001_099/014/02.01.01_60/gs_mec014v020101p.pdf | The document focuses on the UE Identity functionality. It describes the related application policy information (including authorization, access control and traffic rule pattern format), information flows, required information and service aggregation patterns. The document specifies the necessary API, data model and data format, considering existing API(s) if applicable. | S2.11 (Authentication of services and service providers) |

*Table 3: EUOS indentified Edge Computing challenges covered/workd out by 3GPP*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 3GPP | 3GPP TR 23.748 V17.0.0 (2020-12) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3622 | The Technical Report studies and performs evaluations of potential architecture enhancements to support Edge Computing (EC) in the 5G Core network (5GC). Specifically, two objectives are included: a) to study the potential system enhancements for enhanced Edge Computing support, and b) to provide deployment guidelines for typical Edge Computing use cases, e.g. URLLC, V2X, AR/VR/XR, UAS, 5GSAT, CDN, etc. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); S2.22 (IoT and edge computing Platforms) |
| 3GPP | 3GPP TS 23.558 V17.2.0 (2021-12) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3723 | The document specifies the application layer architecture, procedures and information flows necessary for enabling edge applications over 3GPP networks. It includes architectural requirements for enabling edge applications, application layer architecture fulfilling the architecture requirements and procedures to enable the deployment of edge applications. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); S2.22 (IoT and edge computing Platforms) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 3GPP | 3GPP TR 23.803 V7.0.0 (2005-09) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=883 | The document studies: a) the complete harmonization and merger of the policy control and flow based charging architecture and procedures; b) possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control; c) alternative solutions for binding bearers to services (provided today by the authorization token). This includes studying solutions for the network to control bearer usage by service flows. | S2.12 (Policy descriptions, rules, and constraints); S2.22 (IoT and edge computing Platforms) |
| 3GPP | 3GPP TR 23.758 V17.0.0 (2019-12) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3614 | The document is a technical report capturing the study on application architecture for enabling edge applications over 3GPP networks. The aspects of the study include identifying architecture requirements (e.g. discovery of edge services, authentication of the clients), supporting application layer functional model and corresponding solutions to enable the deployment of applications on the edge of 3GPP networks, with no impact to edge-unaware applications on the UE and minimal impact to edge-aware applications on the UE. | S.2.10 (Service discovery support); S2.22 (IoT and edge computing Platforms) |
| 3GPP | 3GPP TR 28.815 V17.0.0 (2021-12) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3758 | The present document studies the charging aspects of Edge Computing based on architecture, procedures and information flows for enabling Edge Applications over 3GPP network as well as capabilities for 5GS to support edge computing. The investigation includes different charging scenarios with potential business requirements, alternative solutions with potential impact on charging architecture, charging functions and charging procedures. | S2.12 (Policy descriptions, rules, and constraints); S2.22 (IoT and edge computing Platforms) |
| 3GPP | 3GPP TR 28.814 V17.0.0 (2021-09) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3744 | The document studies the potential use cases, requirements, and solutions for the management of edge computing architecture and requirement defined by TS 23.558 and TS 23.501. The document provides conclusions and recommendations on the next steps in the standardization. | S2.25 (Optimal Edge-based Lifecycle Management); S2.22 (IoT and edge computing Platforms) |
| 3GPP | 3GPP TR 26.803 V17.0.0 (2021-06) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3742 | The document is a study of use cases for multimedia processing in the edge and the potential 5G media streaming architecture extensions to enable them. | S2.22 (IoT and edge computing Platforms); S2.29 (Edge Analytics); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| 3GPP | 3GPP TR 33.839 V17.0.0 (2021-12) | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3759 | The document studies the security enhancements on the support for Edge Computing in the 5G Core network defined in TR 23.748, and application architecture for enabling Edge Applications defined in TR 23.758 and TS 23.558. Potential security requirements are provided and possible security enhancements to 5GS and edge application architecture are proposed that meet these security requirements. | S2.11 (Authentication of services and service providers); S2.22 (IoT and edge computing Platforms); |

*Table 4: EUOS indentified Edge Computing challenges covered/workd out byISO/IEC JTC1*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/ IEC JTC1 | IEEE/ ISO/IEC 8802-1Q-2020 | https://standards.ieee.org/standard/8802-1Q-2020.html | This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms. | |
| ISO/ IEC JTC1 | ISO/IEC JTC1-SC41-262 ED1 | https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108552 | This document specifies functional requirements and architecture about the following items for resource interoperability among heterogeneous IoT platforms (e.g., oneM2M, GS1 Oliot, IBM Watson IoT, OCF IoTivity, and FIWARE, etc.) through the conversion of resource identifiers (IDs) and paths (e.g., uniform resource identifier (URI)): Requirements for interoperability of resource IDs in the heterogeneous IoT platforms; Functional architecture for converting IDs and paths of resources on heterogeneous platforms; and, Functional architecture for mapping and managing resource IDs among heterogeneous platforms. | S2.10 (Service discovery support); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/IEC JTC1 | ISO/IEC PWI JTC1-SC41-5 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,20,104896 | This document provides an overview of Digital Twin, describes the capabilities, range, characteristics and requirements, and establishes a well-defined conceptual model, reference model and reference architectural views including usage view, functional view, and network view. This document is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations). | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); S2.20 (IoT Systems integration); |
| ISO/IEC JTC1 | ISO/IEC AWI 5392 | https://www.iso.org/standard/81228.html | This document defines a reference architecture of Knowledge Engineering (KE) in Artificial Intelligence (AI). The reference architecture describes KE roles, activities, constructional layers, components and their relationships among themselves and other systems from systemic user and functional views. This document also provides a common KE vocabulary by defining KE terms | S2.9 (AI/ML enabled Network and Services); |
| ISO/IEC JTC1 | ISO/IEC JTC1-SC41-257 ED1 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108033 | This document defines a structured description method, which describes the functionalities of IoT devices, including what functionalities an IoT device can provide, and how to use the functionalities of IoT device. In details, the contents: 1. Define concept of IoT Device Model: what is IoT Device Model, and how it works with underlying IoT communication protocols; 2. Specify structure of IoT Device Model: define the elements of Status, Profile, and Resource; Furthermore, specify the structure of Resource element, to describe the functionalities of IoT devices through Property, Service, and Event; 3. Specify construction method of IoT Device Model: how to build IoT device functionalities based on IoT Device Model; 4. Describe the device interoperability based on the IoT Device Model: IoT Device Model discovery, remote query, remote controlling, subscription and data uploading. | S2.10 (Service discovery support); S2.14 (Devices and open device management); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/ IEC JTC1 | ISO/ IEC TR 30164: 2020 | https://webstore.iec.ch/publication/62522 | The document describes the common concepts, terminologies, characteristics, use cases and technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware/software optimization) of edge computing for IoT systems applications. This document is also meant to assist in the identification of potential areas for standardization in edge computing for IoT. The document describes several use cases from different domains: Smart elevator, Smart video monitoring, Intelligent transport systems, Process control in smart factory, Virtual power plant, Automated crop monitoring and management system, Smart lightning system. | S2.15 (IoT and X-Continuum Paradigm); |
| 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: (1) requirements of the core ontologies for semantic interoperability; (2) best practices and guidance on how to use ontologies and to develop domain-specific applications, including the need to allow for extensibility and connection to external ontologies; (3) cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies; (4) relevant IoT ontologies along with comparative study of the characteristics and approaches in terms of modularity, extensibility, reusability, scalability, interoperability with upper ontologies, and so on; and (5) use cases and service scenarios that exhibit necessities and requirements of semantic interoperability. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge);<br>S2.6 (From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges); |
| ISO/ IEC JTC1 | ISO/IEC 38505-1:2017 | https://www.iso.org/standard/56639.html | ISO/IEC 38505-1:2017 provides guiding principles for members of governing bodies of organizations on the effective, efficient, and acceptable use of data within their organizations by  - applying the governance principles and model of ISO/IEC 38500 to the governance of data,  - assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organization's governance of data,  - informing and guiding governing bodies in the use and protection of data in their organization, and  - establishing a vocabulary for the governance of data. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/<br>IEC JTC1 | ISO/IEC PWI JTC1-SC41-8 | https://www.iec.ch/dyn/www/f?p=103:38:17567799116988::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108353 | Based on ISO/IEC 21823-1, this document provides the basic concepts for IoT systems and digital twin systems behavioral and policy interoperability. This includes - requirements - guidance on how to identify points of interoperability - guidance on how to express behavioral and policy information on capabilities - guidance on how to achieve trustworthiness interoperability, and - use cases and examples . | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); S2.6 (From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges); S2.12 (Policy descriptions, rules, and constraints); S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| ISO/<br>IEC JTC1 | ISO/IEC 30147: 2021 | https://www.iso.org/standard/53267.html | This document provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015. The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas. | S2.11 (Authentication of services and service providers); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/ IEC JTC1 | ISO/IEC 27032 :2012 | https://www.iso.org/standard/44375.html | ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides: an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues. | |
| ISO/ IEC JTC1 | ISO/ IEC TR 27550 :2019 | https://www.iso.org/standard/72024.html | This document provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes. It describes: the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design. | |
| ISO/ IEC JTC1 | ISO/ IEC TS 27110: 2021 | https://www.iso.org/standard/72435.html | This document specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations' type, size or nature. | S2.11 (Authentication of services and service providers); |
| ISO/ IEC JTC1 | ISO/ IEC CD 30149 (2022) | https://www.iec.ch/ords/f p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104432 | This document provides principles for IoT trustworthiness based on ISO/IEC 30141 – IoT Reference Architecture. The current content and scope is based on the premise that Internet of Things is an application and can use a software development lifecycle as a means to address trust in IoT. | S2.11 (Authentication of services and service providers); |
| ISO/ IEC JTC1 | ISO/ IEC TS 27570 :2021 | https://www.iso.org/standard/71678.html | The document takes a multiple agency as well as a citizen-centric viewpoint. It provides guidance on: smart city ecosystem privacy protection; how standards can be used at a global level and at an organizational level for the benefit of citizens; and processes for smart city ecosystem privacy protection. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/ IEC JTC1 | IEEE/ ISO/IEC 8802-1 AE-2020 | https://standards.ieee.org/standard/8802-1AE-2020.html | How all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. | |
| ISO/ IEC JTC1 | ISO/IEC 30173 ED1 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104883 | This document establishes terminology for Digital Twin (DT) and describes concepts in the field of Digital Twin, including the terms and definitions of Digital Twin, concepts of Digital Twin (e.g., Digital Twin ecosystem, lifecycle process for Digital Twin, and classifications of Digital Twin), Functional view of Digital Twin and Digital Twin stakeholders. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); |
| ISO/ IEC JTC1 | ISO/IEC PWI JTC1-SC41-7 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108352 | This document provides a standardized generic Digital Twin maturity model, definition of assessment indicators, guidance for a maturity assessment, and other practical classifications of Digital Twin capabilities, etc. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); |
| ISO/ IEC JTC1 | ISO/ IEC TR 30172 ED1 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104881 | This document provides a collection of representative use cases of Digital Twin applications in a variety of domains. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); |
| ISO/ IEC JTC1 | ISO/IEC PWI JTC1-SC41-6 | https://www.iec.ch/ords/f?p=103:38:523507370720228::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,20,104897 | The document defines a conceptual model for the building of use cases; specifies a use case template ontology, i.e. vocabulary as well as conventions for describing and representing use case contents; provides guidance on building use case templates and on extending a use case ontology to cover the targeted standard; provides examples of use case templates and use cases; and specifies an implementation scheme that will allow use cases to be stored and shared in a repository. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ISO/ IEC JTC1 | ISO/IEC/ IEEE DIS 24641 | https://www.iso.org/standard/79111.html | This International Standard, within the context of methods and tools for MBSSE: (1) Provides terms and definitions related to MBSSE; (2) Defines MBSSE-specific processes for model-based systems and software engineering; the processes are described in terms of purpose, inputs, tasks, and outcomes; (3) Defines methods to support the defined tasks of each process; and (4) Defines tool capabilities to automate/semi-automate tasks or methods. | |
| 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. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge); S2.8 (oT and edge computing coexistence across sectors); S2.21 (IoT sectorial and Cross-Sectorial Open Platforms); |
| 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. | S2.15 (IoT and X-Continuum Paradigm); S2.20 (IoT Systems integration); S2.22 (IoT and edge computing Platforms); |
| 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 Edge Computing challenges covered/workd out by CEN / CENELEC*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| CEN | CEN/ TC 294/ WG 6 | 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. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| CEN/ CENELEC | CWA 17431 | https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa17431.pdf | This CWA addresses a broad set of Principles and Guidance to form a solid foundation for future practice with regard to SEP licensing for ICT standards such as mobile communication standards and other wireless communication standards. The CWA also includes information about licensing to those who are new to the implementation and use of standardised technology and the licensing of patents that cover those technologies. | S2.12 (Policy descriptions, rules, and constraints) |

*Table 6: EUOS indentified Edge Computing challenges covered/workd out by IEEE*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEEE | IEEE 802.1AX-2020 | https://standards.ieee.org/standard/802_1AX-2020.html | Link Aggregation allows parallel point-to-point links to be used as if they were a single link and also supports the use of multiple links as a resilient load-sharing interconnect between multiple nodes in two separately administered networks. This standard defines a MAC-independent Link Aggregation capability and provides general information relevant to specific MAC types. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE 802.1AB-2016 | https://standards.ieee.org/standard/802_1AB-2016.html | This document defines a protocol and a set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802(R) LANs. | S2.10 (Service discovery support) |
| IEEE | IEEE 802.1CM-2018 | https://standards.ieee.org/standard/802_1CM-2018.html | This standard defines profiles that select features, options, configurations, defaults, protocols, and procedures of bridges, stations, and LANs that are necessary to build networks that are capable of transporting fronthaul streams, which are time sensitive. | S2.23 (Need for real-time or near real-time processing and decision-making) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEEE | IEEE 802-2014 | https://standards.ieee.org/standard/802-2014.html | This standard provides an overview to the family of IEEE 802® standards. It describes the reference models for the IEEE 802 standards and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of IEEE 802 MAC addresses; it provides a standard for identification of public, private, prototype, and standard protocols; it specifies an object identifier hierarchy used within IEEE 802 for uniform allocation of object identifiers used in IEEE 802 standards; and it specifies a method for higher layer protocol identification. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE 802.1Q-2014 | https://standards.ieee.org/standard/802_1Q-2014.html | This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE 802.1CB-2017 | https://standards.ieee.org/standard/802_1CB-2017.html | This standard specifies procedures, managed objects, and protocols for bridges and end systems that provide identification and replication of packets for redundant transmission, identification of duplicate packets, and elimination of duplicate packets. It is not concerned with the creation of the multiple paths over which the duplicates are transmitted. | |
| IEEE | IEEE 802.1AC-2016 | https://standards.ieee.org/standard/802_1AC-2016.html | The MAC Service and the Internal Sublayer Service (ISS) are defined in this standard. This standard specifies media-dependent convergence functions that map IEEE 802(R) MAC interfaces to the ISS. The MAC Service is derived from the ISS. | |
| IEEE | IEEE 802.1AS-2020 | https://standards.ieee.org/standard/802_1AS-2020.html | Protocols, procedures, and managed objects for the transport of timing over local area networks are defined in this standard. It includes the transport of synchronized time, the selection of the timing source (i.e., best master), and the indication of the occurrence and magnitude of timing impairments (i.e., phase and frequency discontinuities). | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.23 (Need for real-time or near real-time processing and decision-making) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEEE | IEEE 802.1BR-2012 | https://standards.ieee.org/standard/802_1BR-2012.html | This standard specifies the operation of Bridge Port Extenders, including management, protocols, and algorithms. Bridge Port Extenders operate in support of the MAC Service by Extended Bridges. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE/ISO/IEC 8802-1Q-2020 | https://standards.ieee.org/standard/8802-1Q-2020.html | This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE/ISO/IEC 8802-1BA-2016 | https://standards.ieee.org/standard/8802-1BA-2016.html | Profiles that select features, options, configurations, defaults, protocols and procedures of bridges, stations and LANs that are necessary to build networks that are capable of transporting time-sensitive audio and/or video data streams are defined in this standard. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |
| IEEE | IEEE/ISO/IEC 8802-1BR-2016 | https://standards.ieee.org/standard/8802-1BR-2016.html | This standard specifies the operation of Bridge Port Extenders, including management, protocols, and algorithms. Bridge Port Extenders operate in support of the MAC Service by Extended Bridges. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEEE | IEEE 1934-2018 | https://standards.ieee.org/standard/1934-2018.html | OpenFog Consortium--OpenFog Reference Architecture for Fog Computing is adopted by this standard. OpenFog Reference Architecture [OPFRA001.020817] is a structural and functional prescription of an open, interoperable, horizontal system architecture for distributing computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum of communicating, computing, sensing and actuating entities. It encompasses various approaches to disperse Information Technology (IT), Communication Technology (CT) and Operational Technology (OT) Services through information messaging infrastructure as well as legacy and emerging multi-access networking technologies | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.22 (IoT and edge computing Platforms) |
| IEEE | IEEE 2413-2019 | https://standards.ieee.org/standard/2413-2019.html | An architecture framework description for the Internet of Things (IoT) which conforms to the international standard ISO/IEC/IEEE 42010:2011 is defined. The architecture framework description is motivated by concerns commonly shared by IoT system stakeholders across multiple domains (transportation, healthcare, Smart Grid, etc.). A conceptual basis for the notion of things in the IoT is provided and the shared concerns as a collection of architecture viewpoints is elaborated to form the body of the framework description. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.20 (IoT Systems integration) |
| 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. | |
| IEEE | IEEE 802d-2017 | https://standards.ieee.org/standard/802d-2017.html | How Uniform Resource Name (URN) values are allocated in IEEE 802(R) standards is described in this amendment to IEEE Std 802(R)-2014. | |
| IEEE | IEEE 802.1AR-2018 | https://standards.ieee.org/standard/802_1AR-2018.html | This document presents a Secure Device Identifier (DevID), an ID cryptographically bound to a device and supports authentication of the device's identity. An Initial Device Identifier (IDevID) provided by the supplier of a device can be supplemented by Local Device Identifiers (LDevIDs) facilitating enrollment (provisioning of authentication and authorization credentials) by local network administrators. | S2.10 (Service discovery support); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IEEE | IEEE 802.1AE-2018 | https://standards.ieee.org/standard/802_1AE-2018.html | The document describes how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. | S2.11 (Authentication of services and service providers); |
| IEEE | IEEE 7005-2021 | https://standards.ieee.org/standard/7005-2021.html | Specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data are described in this standard. Specific metrics and conformance criteria regarding these types of uses from trusted global partners and how third parties and employers can meet them are provided in this standard. Certification processes, success criteria, and execution procedures are not within the scope of this standard. | |
| IEEE | IEEE/ISO/IEC 8802-1AE-2020 | https://standards.ieee.org/standard/8802-1AE-2020.html | How all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. | S2.11 (Authentication of services and service providers) |
| IEEE | ISO/IEC/IEEE DIS 24641 | https://www.iso.org/standard/79111.html | This International Standard, within the context of methods and tools for MBSSE: (1) Provides terms and definitions related to MBSSE; (2) Defines MBSSE-specific processes for model-based systems and software engineering; the processes are described in terms of purpose, inputs, tasks, and outcomes; (3) Defines methods to support the defined tasks of each process; and (4) Defines tool capabilities to automate/semi-automate tasks or methods. | S2.13 (Novel programming models and languages) |

*Table 7: EUOS indentified Edge Computing challenges covered/workd out by ITU-T*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG13 - Y.IMT 2020-CE-FEC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18094 | This draft Recommendation specifies the framework of capability exposure function (CEF) in edge computing for IMT-2020 networks and beyond. The scope of this document includes: - Requirements of capability exposure function in edge computing; - Framework of capability exposure function in edge computing; - Functionalities and reference points of capability exposure function in edge computing; - Procedures of capability exposure function in edge computing. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models)<br>S2.22 (IoT and edge computing Platforms)<br>S2.25 (Optimal Edge-based Lifecycle Management)<br>S2.27 (Multi-Tenancy at the Isolation) |
| ITU-T | ITU-T - SG13 - Y.LSMEC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18058 | The draft Recommendation describes the requirements, architecture, functional entities, reference points and information flows of local shunting for multi-access edge computing in IMT-2020 networks. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| ITU-T | ITU-T - SG13 - Y. FM-SC-MEC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18100 | This draft Recommendation aims to describe the framework of Multi-access Edge Computing for fixed? mobile and satellite convergence (FMSC) in IMT-2020 networks and beyond. This recommendation covers the following issues, but not limited to: o Requirements of Multi-access Edge Computing for supporting fixed, mobile and satellite convergence in IMT-2020 networks; o The architecture of Multi-access Edge Computing for fixed, mobile and satellite convergence; o Information flows of Multi-access Edge Computing for fixed, mobile and satellite convergence. | S2.10 (Service discovery support) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG11 - Q.IEC-PRO | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17839 | For development of the IEC architecture, there are couple of software-oriented architectural ways to build flexible protocol architecture achieved by deploying and operating the architecture, for instance, an unified software oriented architecture, which is composing logically modular functions to tightly coupled way as a monolithic architecture and microservice architecture which is loosely composing logically or physically separated own processing functions as microservices. Because IEC has developed on different hardware specifications and various functionalities that each business wants, it is standardized based on microservices and used as a reference standard for implementation. As a result of microservices based IEC architecture, it can be continuously developed and operated by updating microservices. This Recommendation specifies signalling architecture, protocol interfaces, protocol procedures and message format for microservices based intelligent edge computing. | S2.9 (AI/ML enabled Network and Services)<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.28 (Efficient OAM (Operations, Administration, and Maintenance) at the Edge) |
| ITU-T | ITU-T Y.3109 (04/2021) | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14396&lang=en | Recommendation ITU-T Y.3109 specifies quality of service (QoS) assurance-related requirements and a framework for virtual reality (VR) delivery using mobile edge computing (MEC) in International Mobile Telecommunications-2020 (IMT-2020). Recommendation ITU-T Y.3109 first provides an introduction to VR delivery using MEC supported by IMT-2020. It then specifies QoS assurance-related function and mechanism requirements and a framework. The QoS planning for VR services, typical VR user cases and guidelines for deployments of VR services are described in appendices. | S2.27 (Multi-Tenancy at the Isolation) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T Y.4122 (07/2021) | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14735&lang=en | The gateway is an important component of Internet of things (IoT) systems, enabling IoT devices to connect to communication networks. Edge computing technologies can benefit the IoT, providing computation, storage, networking and intelligence in proximity to IoT devices. Compared with the common gateway [ITU-T Y.4101], the edge-computing-enabled gateway in the IoT (EC-enabled IoT gateway) has additional capabilities supporting service layer interworking, and application layer interworking between IoT devices, IoT platforms and IoT application servers. In addition, the EC-enabled IoT gateway supports data transmission capabilities for IoT applications sensitive to time, latency, jitter and packet loss. Based on the common requirements and capabilities of a gateway for IoT applications [ITU-T Y.4101] and IoT requirements for support of edge computing [ITU-T Y.4208], additional capabilities and capability framework of the edge-computing-enabled gateway in the IoT are specified. Examples of applicability of the edge-computing-enabled gateway in the IoT are also given. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.26 (Optimal Edge Organization and Federation) |
| ITU-T | ITU-T - SG16 - F.743.13 | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14954&lang=en | This Recommendation describes the requirements for a function which enables the cooperation of multiple edge gateways (CMEG) to complete complex tasks. It also describes the required capabilities and requirements of key components. The CEMG function can support the information exchanging among multiple edge gateways and deal with gateway failure cooperatively. It can also specify the central gateway which is responsible for selecting a cooperative gateway for each gateway, which in turn monitors the status of its partner gateway, and manages the cooperative data and devices. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T F.743.12 (06/2021) | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14680&lang=en | Recommendation ITU-T F.743.12 defines the requirements for edge computing in video surveillance. Edge computing is a distributed computing paradigm aimed at providing various computing services at the edge of the network, and it brings computation and data storage closer to the data source or the location where it is needed, to improve response time and save bandwidth. By using the edge computing technology, the video surveillance system can perform intelligent video analysis and store data near the network premises units. And the edge computing platform provides the management capabilities of the edge resources and functional components to the video surveillance system. It can improve the video processing efficiency and quality of services and reduce the infrastructure cost of the video surveillance system. This Recommendation describes the application scenarios and requirements for edge computing in the video surveillance system. | S. 2.30 (Edge-to-Cloud Integration) |
| ITU-T | ITU-T F.743.10 (11/2019) | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14103&lang=en | Recommendation ITU-T F.743.10 specifies the general framework, scenarios and requirements for mobile edge computing-(MEC-)enabled content delivery networks (CDNs). Recommendation ITUT F.743.10 also specifies the requirements for MEC functions on which a CDN edge node relies. The deployment of a CDN edge node with an MEC system is described in the general framework. Several use cases are introduced in Recommendation ITU-T F.743.10 to illustrate the usage of MEC-enabled CDN. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| ITU-T | ITU-T F.749.11 (11/2019) | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14104&lang=en | Civilian unmanned aerial vehicle (CUAV) enabled mobile edge computing (MEC) utilizes CUAV as an MEC platform to realize a flexible, efficient and on-demand computing service that can be rapidly deployed and move according to the practical service needs of devices. Recommendation ITU-T F.749.11 describes the framework and specifies requirements for a CUAV-MEC system, including functional, service and security requirements. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG13 - Y.FMC-EC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18048 | A unified and cloud-based edge computing platform allows operators to flexibly deploy network functions and support infrastructure for fixed-mobile network convergence, to provide a unified multi-access edge computing capability for all network access technologies in IMT-2020 networks. This draft Recommendation aims to describe the requirements, architecture and functions of unified multi-access edge computing for supporting fixed mobile convergence (FMC) network. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.30 (Edge-to-Cloud Integration) |
| ITU-T | ITU-T - SG13 - Y.FMC-AAEC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18131 | On the basis of Y.FMC-AAEC-req, which specifies use cases and requirement of application addressing in edge computing, this draft Recommendation presents the framework and technical solutions of application addressing in edge computing in IMT-2020 network and beyond. The following aspects of application addressing in edge computing are addressed in this Recommendation: Framework of application addressing in edge computing Procedures of application addressing in edge computing Security considerations on application addressing in edge computing | S2.10 (Service discovery support) |
| ITU-T | ITU-T - SG16 - H.VSE-CArch | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17519 | Architecture for edge computing platform supporting a video surveillance system | S2.23 (Need for real-time or near real-time processing and decision-making) |
| ITU-T | ITU-H. 644.4 (06/21) | https://www.itu.int/rec/T-REC-H.644.4-202106-I/en | Recommendation ITU-T H.644.4 specifies a functional architecture for mobile/multi-access edge computing (MEC) enabled content delivery network (MEC-CDN). The functions and functional blocks within this functional architecture and the related reference points are specified in this Recommendation for matching the requirements in Recommendation ITU-T F.743.10. Particularly, this Recommendation also provides the deployment of virtualized content delivery network (CDN) service and the interworking between virtualized CDN functionalities and MEC management system, within a MEC-CDN ecosystem. In addition, a containerized solution of MEC-CDN is given in this Recommendation, followed by the basic information flows. | S2.16 Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models;<br>S2.28 (Efficient OAM (Operations, Administration, and Maintenance) at the Edge) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG13 - Y.3076 | https://www.itu.int/rec/T-REC-Y.3076-202009-I | This Recommendation specifies the requirements and architecture about ICN-enabled edge network in IMT-2020. 1) From the service and network operation point of view, it discusses detailed requirements of ICN-enabled Edge network in IMT-2020. 2) It provides architecture of ICN-enabled edge network. 3) It describes the key functions and interfaces to satisfy the requirements of ICN-enabled edge network. | S2.16<br>Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models;<br>S2.22 (IoT and edge computing Platforms) |
| ITU-T | ITU-T - SG13 - Y.ecloud-reqts | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18104 | This Recommendation provides functional requirements of edge cloud. Edge cloud is a cloud computing deployed to the edge of the network. It has small capacity resources enabling cloud service. It addresses the following subjects: - Overview of edge cloud; - Operation of edge cloud in distributed cloud; - Functional requirements of edge cloud; - Use cases of edge cloud in distributed cloud. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.30 (Edge-to-Cloud Integration) |
| ITU-T | ITU-T - SG13 - Y.3526 | https://www.itu.int/rec/T-REC-Y.3526-202111-I | This Recommendation provides requirements for edge cloud. It introduces the overview of edge cloud management including advantages of edge cloud management and relationship with global management in distributed cloud. It describes the edge cloud management local functions and mode. Additionally, this Recommendation provides edge cloud management functional requirements derived from use cases. | S2.16<br>Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models;<br>S2.30 (Edge-to-Cloud Integration);<br>S2.28 (Efficient OAM (Operations, Administration, and Maintenance) at the Edge) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG20 | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17928 | Decentralized services (e.g., enabled by distributed ledger technologies, DLT) for IoT devices can be deployed in local area networks (e.g., in IoT devices or in local IoT gateways for constrained IoT devices) or in clouds (e.g., in remote IoT gateways or in cloud systems). When deployed in local area networks, the decentralized services will be affected by the local storage capability of peers and their computation capability and communication latency among peers. When deployed in clouds, the decentralized services will be affected by speed and efficiency of data access. With the popularization of the use of edge computing, part or whole of functionalities of DLT-based decentralized services can be deployed in edge nodes. This draft Recommendation introduces decentralized service by using DLT and edge computing technologies, which is an intermediate supporting service between decentralized services in local area networks and that in clouds. Decentralized service by using DLT and edge computing technologies is deployed in edge nodes and can facilitate interaction among peers of decentralized services, no matter where the peers are deployed (e.g., in local areas or in clouds). This draft Recommendation analyses characteristics and general requirements of decentralized service by using DLT and edge computing technologies, and provides its functional framework and relevant common capabilities, functionalities and general procedures. | S2.11 (Authentication of services and service providers);<br>S2.26 (Optimal Edge Organization and Federation);<br>S2.30 (Edge-to-Cloud Integration); |
| 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. | S2.16 Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models;<br>S2.22 (IoT and edge computing Platforms); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG13 - Y.ec-reqts | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18101 | This Recommendation provides overview and requirements of edge computing. To provide requirements, this Recommendation defines terms and concept of edge computing, provides reference frameworks for edge computing based on fundamental characteristics and capabilities. Also, this Recommendation provides requirements through various use cases based on reference framework. | S2.10 (Service discovery support) |
| ITU-T | ITU-T - SG17 - X.sa-ec | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18024 | The purpose of this Recommendation is to guide operator to implement a uniformed security management for multi-vendor environment. This Recommendation analyses main security protection challenges, proposes the collaborative cloud-edge computing security architecture. In addition, this Recommendation describes key technologies and work procedures of the security architecture. | S2.11 (Authentication of services and service providers) |
| ITU-T | ITU-T - SG11 - Q.5003 | https://www.itu.int/itu-t/recommendations/rec.aspx?id=14925&lang=en | Recommendation ITU-T Q.5003 describes signalling requirements and architecture for federated multiaccess edge computing (MEC). This Recommendation specifies signalling requirements, signalling architecture with reference points and security considerations for federated MEC. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.26 (Optimal Edge Organization and Federation); |
| ITU-T | ITU-T - SG11 - Q.5001 | https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13701&lang=en | A huge volume of data has been generated from the various smart things. Lots of smart services have been working based on cloud systems. However, the network bottleneck between terminals and a cloud system has incurred various issues (e.g., data loss, network delay, etc.). An edge computing technology between user equipment and cloud server system is attracted to solve these problems. In addition, applying the intelligent data processing functions by providing AI technologies will provide enhanced networking capabilities for new emerging services and applications. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.29 (Edge Analytics) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG13 - Y.FMC -AAEC-req | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18079 | This draft Recommendation presents the use cases and technical requirements of application addressing in edge computing for future networks including IMT-2020. Application Addressing is the process to discover the IP address of the server which the application running on when UE intends to access the application This Recommendation specifies the following aspects of application addressing in edge computing in the context for future networks including IMT-2020: Use cases and requirements of application addressing in edge computing for future networks including IMT-2020. FMC architecture enhancement requirements. | 2.10 (Service discovery support);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.22 (IoT and edge computing Platforms) |
| ITU-T | Y.dec-IoT-arch | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14650 | This Recommendation describes a decentralized, IoT communication reference architecture based on ICN and blockchain. | S2.8 (IoT and edge computing coexistence across sectors);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models)<br>S2.20 (IoT Systems integration);<br>S2.22 (IoT and edge computing Platforms) |
| ITU-T | Y.IoT-DES-fr | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16855 | This draft Recommendation introduces a decentralized service by using DLT and edge computing technologies for IoT devices, and analyses its characteristics and high-level requirements, and provides its functional framework and relevant common capabilities, functionalities and general procedures. | S2.8 (IoT and edge computing coexistence across sectors);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models)<br>S2.20 (IoT Systems integration) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | Y.AI-DECCS | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16856 | This Recommendation specifies Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city. | S2.9 (AI/ML enabled Network and Services);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models)<br>S2.18 (Federated Learning and AI for IoT Edge);<br>S2.22 (IoT and edge computing Platforms) |
| ITU-T | Y.CDML-arc | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16865 | This recommendation aims to propose the reference architecture of collaborative decentralized machine learning for intelligent IoT services. | S2.9 (AI/ML enabled Network and Services);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models)<br>S2.18 (Federated Learning and AI for IoT Edge) |
| ITU-T | Y.IoT-DSE-arc | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16862 | This draft Recommendation introduces a concept of service exposure for decentralized services (DSE) for IoT applications, analyses its common characteristics and high-level requirements, and provides a reference architecture of DSE and relevant common capabilities. | S2.8 (IoT and edge computing coexistence across sectors);<br>S2.20 (IoT Systems integration) |
| ITU-T | Y.scdt-reqts | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16396 | This Recommendation provides concept of digital twin federation and defines requirements for digital twin federation in smart cities and communities. | |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | Y.RA-FML | https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16676 | This Recommendation defines the reference architectural framework and requirements of IoT and Smart City and Community services based on federated machine learning. | S2.5 (Digital Twin research challenges: From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge)<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |
| ITU-T | ITU-T - SG16 - F.DVMSF | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17612 | Recommendation ITU-T F.749.3 describes the use-cases and requirements for vehicular multimedia networks (VMN), taking into account the autonomous levels defined by [SAE J3016], and defined the Vehicular multimedia service platform (VMSP) with the following functions: multimedia services, infotainment applications, intelligent voice interaction, high precision navigation (maps), security updates, software and certificates. This recommendation suggests to use Edge computing platform as the distributed computing system with the following advantages: - computing and network resource of VMSP allocation; - increase of services performance; - decentralization; - user demand services; - reduction of delays. This recommendation considers the framework of distributed VMS for V2X networks based on the EdC possibilities. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG16 - F.CEC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17635 | With the development of industry, cloud computing and edge computing are widely used. Especially in the industrial machine vision system, with the increase of data-intensive applications and computing-intensive applications, it is necessary to use the powerful computing capabilities and communication resources of cloud computing, collaborate with the short-time response capabilities of edge computing to realize and complete corresponding application requests. Through collaborative work, the value of edge computing and cloud computing will be maximized, thereby effectively improving the performance of industrial machine vision systems.<br>Cloud-edge collaboration technology is a collaborative method of cloud computing and edge computing, including data collaboration, resource collaboration, intelligent collaboration, service collaboration and application collaboration. At the same time, cloud-edge collaboration in industrial machine vision system will meet the needs of intelligent analysis and real-time response business in different scenarios.<br>This Recommendation specifies requirements and reference framework of cloud-edge collaboration in industrial machine vision system. | S2.15 (IoT and X-Continuum Paradigm);<br>S2.30 (Edge-to-Cloud Integration) |
| ITU-T | ITU-T - SG5 - L.Spec_ Edge DC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17700 | In recent years, there a+E139:I139re more extra-large data centres worldwide. Although these kind of data centres are in strong capability of data processing, it is a little bit difficult to meet the need of data centre application from users. The Edge data centre is established to perfectly solve this problem and let users get better experience of data access. With the huge quantity application and establishment of Edge data centres, the specific requirement of data centre infrastructure, especially in Edge data centre, will be stricter in the future. This Recommendation proposes to establish clear requirements on infrastructure including ICT system, powering system, cooling system, monitoring system etc. to get green, safe, reliable, smart, energy-saving Edge data centre. | S2.30 (Edge-to-Cloud Integration);<br>S2.32 (Edge Environmental Considerations) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG16 - F.DC-CGS-TREC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17582 | Cloud gaming requires high real-time performance, so it needs special hardwares to match the needs of real-time game rendering. This recommendation will describe the detailed infrastructure requirements of cloud gaming and provide reference for infrastructure selection of mobile edge computing in different scenarios. Among the factors that restrict the development of cloud gaming, the long end-to-end delay is the most important one. Mobile Edge computing is an effective way to reduce the end-to-end delay. This recommendation will describe the architecture and interaction process of cloud gaming system optimized for edge computing. | S2.30 (Edge-to-Cloud Integration); |
| ITU-T | ITU-T - SG17 - X.gecds | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18025 | Edge computing is strongly related to 5G and UPF is the data connection point between the MEC system and 5G Network architecture. The sinking of 5G network user plane brings threats such as illegal eavesdropping, which may seriously threaten the data security in edge computing. The edge node has unique features itself and whether in the physical environment or the network, the data security will be an important problem that the edge nodes need to face. Therefore, the recommendation analyses the edge computing data security mainly from these two aspects and provides relative data security challenges and threats and data security guidelines for Edge Computing. This recommendation could help to address the data security issues in Edge Computing implementation | S2.11 (Authentication of services and service providers) |
| ITU-T | ITU-T - SG17 - X.5G sec-netec | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17985 | 5G EC would play a key role on low latency services and traffic off-load services in 5G era. Several prominent factors would enlarge and complex the security risks to the network layer that supports 5G EC and even bring new security challenges to the network security operation. These factors would be the flexible network architectures of 5G, the variable deployment positions of EC, the various application scenarios, different types of users' private networks and access networks, etc. The boundaries among the telecommunication networks and the private networks would be more ambiguous, and the exposure surface would be expanded. Therefore, the security requirements and measures of the network layer including both of the telecommunication networks and the private networks would be recommended as telecommunication operators enjoying the benefit of EC. | S2.11 (Authentication of services and service providers);<br>S2.30 (Edge-to-Cloud Integration); |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T - SG17 - X.5Gsec-ecs | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17977 | This draft Recommendation analyses the potential deployment scheme and typical application scenarios of edge computing services, specifies the security threats and requirements specific to the edge computing services and thus establishes the security framework for the operator to safeguard its applications. | S2.11 (Authentication of services and service providers);<br>S2.30 (Edge-to-Cloud Integration); |
| ITU-T | ITU-T - SG17 - X.itssec-5 | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17967 | This draft Recommendation provides security guidelines for vehicular edge computing. Vehicular edge computing (VEC) is a model that supports the core cloud's capacity for decentralizing the concentration of computing resources in data centers. VEC also provides more localized storage and application services to road users, thereby making it possible to achieve lower latency delays, faster response times providing mobility support, location awareness, high availability, and Quality of Service for streaming real-time applications since the data processing is conducted closer to the vehicle. Vehicular edge computing faces many security challenges and issues since it requires providing faster service response time to end-users. This Recommendation provides security guidelines for vehicular edge computing based on an analysis of the threats and vulnerabilities identified within VEC. Further, it also provides use cases for a security system and relevant security requirements for use in for vehicular edge computing scenarios. | S2.11 (Authentication of services and service providers);<br>S2.30 (Edge-to-Cloud Integration); |
| ITU-T | ITU-T - SG5 - L.EEMDC | https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17702 | The scope of the draft Recommendation is as follows. - considerations on micro data centre for edge computing: deployment, configuration including redundancy, components - energy efficiency in micro data centre: management functions including energy efficiency and operation perspective - energy efficiency in edge computing: management functions including energy efficiency and operation perspective Note) The scope of the Recommendation could be updated according to the main text of the Recommendation. | S2.32 (Edge Environmental Considerations) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU_T-L. 1333 | https://www.itu.int/rec/T-REC-L.1333-202209-I | To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331. | S2.1 (Digital for Green research challenges);<br>S2.2 (Digital for Green standardisation challenges) |
| ITU-T | ITU-T L. 1410 | https://www.itu.int/rec/T-REC-L.1410-201412-I/en | Recommendation ITU-T L.1410 deals with environmental life cycle assessments (LCAs) of information and communication technology (ICT) goods, networks and services. It is organized in two parts: (a) Part I: ICT life cycle assessment: framework and guidance and (b) Part II: "Comparative analysis between ICT and reference product system (Baseline scenario); framework and guidance". Part I deals with the life cycle assessment (LCA) methodology applied to ICT goods, networks and services. Part II deals with comparative analysis based on LCA results of an ICT goods, networks and services product system, and a reference product system | S2.1 (Digital for Green research challenges);<br>S2.2 (Digital for Green standardisation challenges) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| ITU-T | ITU-T L.1480 | https://www.itu.int/rec/T-REC-L.1480-202212-I | Summary Recommendation ITU-T L.1480 provides a methodology for assessing how the use of information and communication technology (ICT) solutions impacts greenhouse gas (GHG) emissions of other sectors. More specifically, the methodology provides guidance on the assessment of the use of ICT solutions covering the net second order effect (i.e., the resulting second order effect after accounting for emissions due to the first order effects of the ICT solution), and the higher order effects such as rebound. By providing a structured methodological approach, it aims to improve the consistency, transparency and comprehensiveness of assessments of how the use of ICT solutions impacts GHG emissions over time. Guidance is provided to assess the net second order effect and higher order effects of the following cases:<br>· ICT solution(s) implemented in a specific context by the user of the ICT solution(s).<br>· 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.<br>· ICT solution(s) seen from the perspective of an ICT organization contributing to the ICT solution(s). This includes:<br>o Assessment of the aggregated effect of all ICT solutions provided by an ICT organization across all its customers;<br>o Assessment of the aggregated effect of one or several ICT solutions provided by an ICT organization across some of its customers;<br>o Assessment of the effect of one or more specific ICT solutions implemented in an actual context for a specific customer. | S2.1 (Digital for Green research challenges);<br>S2.2 (Digital for Green standardisation challenges) |

*Table 8: EUOS indentified Edge Computing challenges covered/workd out by W3C*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| W3C | TR/2020/REC-wot-architecture-20200409 | https://www.w3.org/TR/2020/REC-wot-architecture-20200409/ | The document describes the abstract architecture for the W3C Web of Things. This architecture is based on a set of requirements that were derived from use cases for multiple application domains, both given in this document. A set of modular building blocks are also identified whose detailed specifications are given in other documents. This document describes how these building blocks are related and work together. The WoT abstract architecture defines a basic conceptual framework that can be mapped onto a variety of concrete deployment scenarios, several examples of which are given. However, the abstract architecture described in this specification does not itself define concrete mechanisms or prescribe any concrete implementation. | S2.22 (IoT and edge computing Platforms) |
| W3C | TR/2021/WD-wot-discovery-20210602 | https://www.w3.org/TR/wot-discovery/ | The document presents a process for WoT discovery with two phases: introduction and exploration. The Introduction phase leverages existing discovery mechanisms but does not directly expose metadata; they are simply used to discover Exploration services, which provide metadata but only after secure authentication and authorization. This document normatively defines two Exploration services, one for WoT Thing self-description with a single WoT Thing Description and a searchable WoT Thing Description Directory service for collections of Thing Descriptions. A variety of Introduction services are also described and where necessary normative definitions are given to support them. | S2.10 (Service discovery support);<br>S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models) |

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| W3C | TR/2020/REC-wot-thing-description-20200409 | https://www.w3.org/TR/2020/REC-wot-thing-description-20200409/ | The document describes a formal model and a common representation for a Web of Things (WoT) Thing Description. A Thing Description describes the metadata and interfaces of Things, where a Thing is an abstraction of a physical or virtual entity that provides interactions to and participates in the Web of Things. Thing Descriptions provide a set of interactions based on a small vocabulary that makes it possible both to integrate diverse devices and to allow diverse applications to interoperate. Thing Descriptions, by default, are encoded in a JSON format that also allows JSON-LD processing. The latter provides a powerful foundation to represent knowledge about Things in a machine-understandable way. A Thing Description instance can be hosted by the Thing itself or hosted externally when a Thing has resource restrictions (e.g., limited memory space) or when a Web of Things-compatible legacy device is retrofitted with a Thing Description. | S2.16 (Support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models);<br>S2.22 (IoT and edge computing Platforms) |

*Table 9: EUOS indentified Edge Computing challenges covered/workd out by IETF*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IETF | draft-ietf-mops-ar-use-case: Media Operations Use Case for an Augmented Reality Application on Edge Computing Infrastructure | https://datatracker.ietf.org/doc/draft-ietf-mops-ar-use-case/03/ | A use case describing transmission of an application on the Internet that has several unique characteristics of Augmented Reality (AR) applications is presented for the consideration of the Media<br>Operations (MOPS) Working Group | 2.22 IoT and edge computing Platforms |
| IETF | draft-contreras-alto-service-edge: Use of ALTO for Determining Service Edge | https://datatracker.ietf.org/doc/draft-contreras-alto-service-edge/ | This document proposes an initial approach towards the use of ALTO to provide such information and assist the selection of appropriate deployment locations for services and applications. | 2.22 IoT and edge computing Platforms |

*Table 10: EUOS indentified Edge Computing challenges covered/workd out by IRTF*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| IRTF | draft-irtf-t2trg-iot-edge:<br>IoT Edge Challenges and Functions | https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-edge/ | This document outlines the requirements of the emerging IoT Edge and its challenges. It presents a general model, and major components of the IoT Edge, to provide a common base for future discussions in T2TRG and other IRTF and IETF groups. | 2.22 IoT and edge computing Platforms |
| IRTF | draft-dwon-t2trg-multiedge-arch: Multi-cluster Edge System Architecture and Network | https://datatracker.ietf.org/doc/draft-dwon-t2trg-multiedge-arch/ | In this draft, it is presented the cluster-based edge system architecture and multi-cluster edge network topology that consists of multi-cluster edge system and core cloud. Also, the network functions and network node to configurate and operate multi-cluster edge network collaboratively. | 2.22 IoT and edge computing Platforms |
| IRTF | draft-irtf-coinrg-use-cases: Use Cases for In-Network Computing | https://datatracker.ietf.org/doc/draft-irtf-coinrg-use-cases/ | This document discusses some use cases to demonstrate how real<br>applications can benefit from COIN and to showcase essential requirements that have to be fulfilled by COIN applications. | 2.22 IoT and edge computing Platforms |
| IRTF | draft-mcbride-edge-data-discovery-overview: Edge Data Discovery for COIN | https://datatracker.ietf.org/doc/draft-irtf-coinrg-use-cases/ | This document discusses some use cases to demonstrate how real<br>applications can benefit from COIN and to showcase essential requirements that have to be fulfilled by COIN applications. | 2.22 IoT and edge computing Platforms |

*Table 11: EUOS indentified Edge Computing challenges covered/workd out by oneM2M*

| SDO | Specification | | | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
| | Title | URL | Abstract | Labels & Sections |
| oneM2M | oneM2M-TR-0052-V-0.13.1: Study on Edge and Fog Computing in oneM2M systems | [https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32633](https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32633) | The document is a study of how to leverage Edge and Fog computing in oneM2M architecture. Based on the result of the study, it will identify possible advanced features and enhancements which the next oneM2M release(s) could support. | 2.22 IoT and edge computing Platforms |

*Table 12: EUOS indentified Edge Computing challenges covered/workd out by OMA*

| SDO | Specification | | | Relevant EUOS identified Edge 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. | 2.14 Devices and open device management |
| OMA | OMA IPSO Repo Public IPSO Repository | https://technical.openmobilealliance.org/OMNA/LwM2M/LwM2MRegistry.html | The IPSO Smart Object Registry registry is intended for developers that are building products based on IPSO Objects, it is not intended to be used at runtime by applications. | 2.14 Devices and open 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]. | 2.14 Devices and open 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. | 2.14 Devices and open device management |

| SDO | Specification |  |  | Relevant EUOS identified Edge challenges |
|---|---|---|---|---|
|  | Title | URL | Abstract | Labels & Sections |
| 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). | 2.14 Devices and open device management |
| 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. | 2.14 Devices and open device management |
| OMA | OMA-TS-GwMO-V1_1-20170725-A Gateway Management Object Technical Specification | https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO-V1_1-20170725-A.pdf | This technical specification describes Management Objects and Generic Alerts that are needed to provide the DM Gateway functionality, as defined in [DMDICT]. | 2.14 Devices and open device management |

*Table 13: EUOS indentified Edge Computing challenges covered/workd out by Open Source*

| SDO | Specification | | | Relevant EUOS identified Edge 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. | 2.24 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. | 2.24 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. | 2.24 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. | 2.24 Simulation and Emulation Environments |

# Annex II 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

## 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).

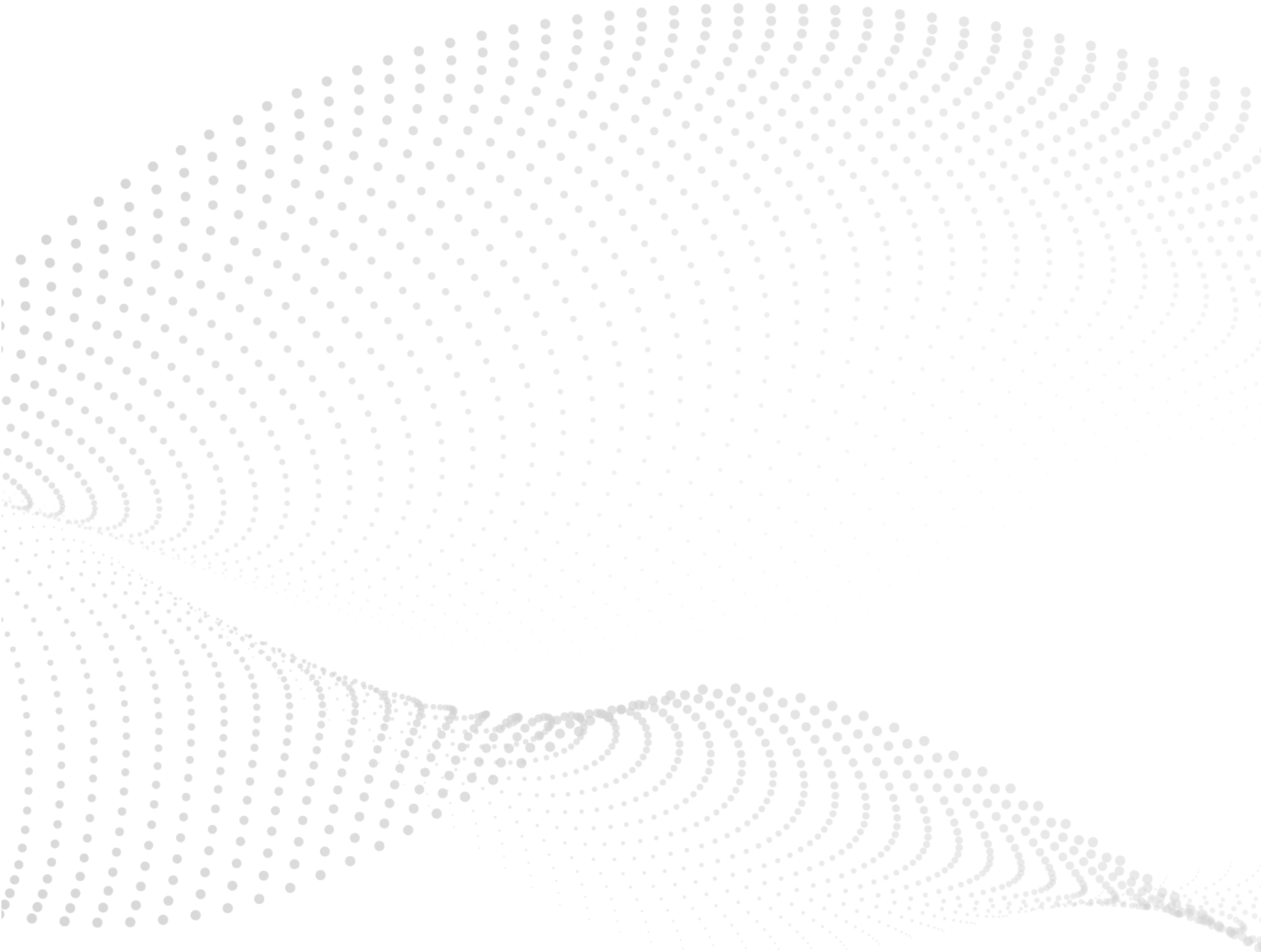
## X.4 Source

- 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.



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