



Alliance for AI, IoT and Edge
Continuum Innovation



euos

EU Observatory for
ICT Standardisation

Report of TWG IoT & Edge: **Landscape of Internet of Things | V.2**

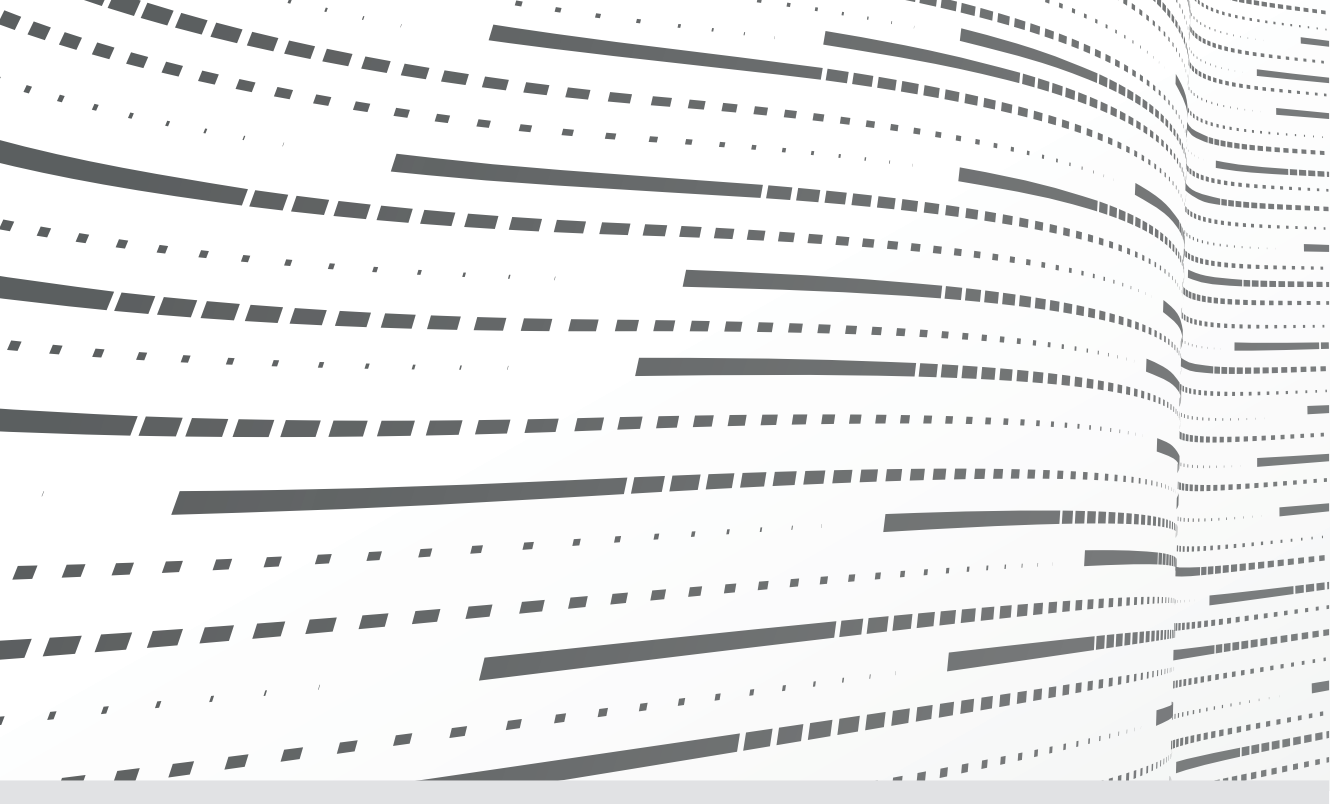
Editor: Georgios Karagiannis

Series Editors: Maria Giuffrida and XiaoRui Zhang

Powered by

standICT.eu2026

ICT Standardisation Observatory and Support Facility in Europe



Disclaimer

The TWG IoT and Edge operates in full autonomy and transparency. The views and recommendations in this report are those of the Expert Group, the StandICT.eu Fellows acting in their personal capacities and do not necessarily represent the opinions of the European Commission or any other body; nor do they commit the Commission to implement them. Reuse is authorized provided the source and authors are acknowledged. For any use or reproduction of photos or other material that is not under EU copyright, permission must be sought directly from the copyright holders.

Legal notice

The document has been prepared for the European Commission and SDOs however it reflects the views only of the authors, and neither the European Commission nor the Standards Developing Organisations can be held responsible for any use which may be made of the information contained therein. More information 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.

About AIOTI

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



**Alliance for AI, IoT and Edge
Continuum Innovation**

■ Table of Contents

1. Introduction.....	5
2. Contributors of EUOS StandICT.eu IoT and Edge Computing Standardisation Landscape reports 2025	6
Buildings.....	8
Horizontals & Verticals	8
Buildings.....	8
Built Environment.....	9
Smart City	9
Case Studies and Rankings	9
Horizontals & Verticals	9
Manufacturing.....	12
Mobility.....	13
Energy.....	14
Food and Agriculture	14
Water	14
Smart City	15
Buildings.....	17
Health.....	17
Connectivity.....	18
Horizontals & Verticals	18
Manufacturing.....	54
Mobility.....	54
Water	57
Home.....	57
Buildings.....	58
Health.....	58
Data_and_Architecture.....	58
Horizontals & Verticals	58
Manufacturing.....	110
Mobility.....	118
Energy.....	129
Food and Agriculture	131
Water	133
SmartCity.....	133
Social Community and Wellbeing	139
Buildings.....	139
Health.....	140
Education Training and Learning	142
Horizontals & Verticals	142
Energy.....	144

Energy 145

 Energy.....145

 SmartCity.....145

Environment.....147

 Horizontals & Verticals.....147

 SmartCity.....147

Food and Agriculture 149

 Food and Agriculture 149

Industry and Business 150

 Horizontals & Verticals 150

 Manufacturing.....153

 Mobility.....164

 Water 166

Information Processing.....166

 Horizontals & Verticals 166

 Water 168

Infrastructure.....169

 Horizontals & Verticals 169

Infrastructure.....191

 Horizontals & Verticals 191

 Mobility.....209

 Energy.....217

 Water 219

 SmartCity.....221

 Buildings.....222

 Built Environment 222

 Health.....223

Organization.....229

 Horizontals & Verticals 229

 Health.....230

Privacy and Security.....231

 Horizontals & Verticals 231

 Manufacturing.....255

 Mobility.....257

 Energy.....259

 SmartCity.....261

 Built Environment 261

Safety and Emergencies.....262

 Horizontals & Verticals 262

 Mobility.....266

 Energy.....267

 Water 267

SmartCity 268

 Horizontals & Verticals 268

 SmartCity.....270

Social Community and Wellbeing	273
Horizontals & Verticals	273
Energy.....	274
SmartCity.....	274
Health.....	274
Strategies Policies and Planning.....	276
Horizontals & Verticals	276
Mobility.....	277
Buildings.....	277
Sustainability and Resilience.....	278
Horizontals & Verticals	278
Manufacturing.....	280
Energy.....	281
SmartCity.....	281
Social Community and Wellbeing	282
Buildings.....	283
Built Environment.....	283
Education Training and Learning	284
Terms and Definitions	284
Horizontals & Verticals	284
Manufacturing.....	287
Mobility.....	287
Food and Agriculture.....	287
Health.....	288
Annex.....	291

■ 1. Introduction

The Internet of Things (IoT) as a concept has been initiated more than two decades ago. IoT can be considered to be a system that interconnects heterogeneous technologies supporting our daily needs impacting on a large scale our lives as well as the way we do business, locally and globally.

IoT systems and IoT applications have been implemented and deployed in almost all vertical industry domains, such as Health, Industry & Manufacturing, Agriculture, Finance, Mobility, Energy, Public safety, Buildings and Cities.

Successful deployment of IoT technologies and IoT applications demands standards and protocols. The development and promotion of these standards and protocols is a cooperative undertaking between governments, academia, industry and the public interest.

This depends largely on the work and activities accomplished in SDOs (Standards Development Organizations), Alliances and OSS (Open-Source Software) initiatives. Currently, there are many SDOs, Alliances and OSS initiatives that are active and competing in the IoT technology and applications areas. In this context, the IoT landscape is considered to be complex, dynamic and challenging to grasp and visualize.

The goal of this report is to capture the landscape of IoT activities and IoT documents/specifications published and/or under publication by SDOs, Alliances and OSS Initiatives.

In order to realize this goal, this report has used the methodology and process defined by EUOS StandICT.eu in the “Landscape of AI Standards” report of TWG AI (Technical Working Group of Artificial Intelligence). In particular, representatives from several SDOs, Alliances, OSS Initiatives and academic institutions have created an open-access database of IoT related specifications and documents, such as architectures, requirements, technical reports, reviews, white papers, guidelines, etc. in a way that encourages future extensions, re-use, cross-comparisons and re-classification according to various needs. Applying the EUOS StandICT.eu aforementioned methodology and process, the EUOS StandICT.eu TWG IoT and Edge and AIOTI (Alliance for AI, IoT and Edge Continuum Innovation) WG Standardisation team members, who collated this report, made the collected disparate outcomes from across the global community, readable and accessible, and at the same time provided the possibility to make dynamic extensions of these collected outcomes in the future.

This is version 2 of the report and it updates the IoT landscape presented in version 1 of the report “Landscape of Internet of Things (IoT) Standards”, published on 13 October 2022, by including new specifications and updating information on specifications included in version 1 of this report. The updated documents, e.g., specifications are labelled in this version, using the keyword “Updated” In their titles, while the new documents, e.g., specifications are labelled in this version, using the keyword “NEW” In their titles.

StandICT.eu and the team of TWG IoT and Edge thank the European Commission for supporting this work and invite experts to join us in expanding the coverage of the IoT related database behind this report, and use it to compare standards, improve them, and make their work more effective.



By the editor, Georgios Karagiannis

2. Contributors of EUOS StandICT.eu IoT and Edge Computing Standardisation Landscape reports 2025

	Name	Affiliation
1	Georgios Karagiannis (editor)	AIOTI WG Standardisation co-Chair & Huawei
2	Noleen Campbell	NSAI Standards
3	Maria Ines Robles	Tampere University
4	Michelle Wetterwald	Netellany
5	Orfeas Voutyras	Institute of Communication and Computer Systems
6	Antonio Kung	Trialog
7	Lindsay Frost	NEC
8	George Suciu	BEIA Consult
9	Amelié Gyrard	Trialog
10	Jens Gayko	VDE Association for Electrical, Electronic & Information Technologies
11	Axel Rennoch	Fraunhofer FOKUS
12	Edward C. Zimmermann	NONMONOTONIC Networks
13	Marco Carugi	Consultant
14	Amanda Suo	UNE - Spanish Standardisation Body
15	XiaoRui Zhang	Dublin City University
16	Richard Pitwon	Resolute Photonics
17	Christine Perey	Spime Wrangler
18	Kong Lingbo	Huawei
19	Shen Bin	CAICT
20	Samir Medjiah	Laas-CNRS Toulouse
21	Damir Filipovic	AIOTI Secretary General
22	Dave Raggett	W3C/ ERCIM
23	Natalia Stathakarou	Massive Dynamic Sweden
24	Alissa Zaccaria	Intellimech
25	Ana Petrache	BEIA Consult
26	Asbjørn Hovstø	Hafenstrom
27	Artur Krukowski	RFSAT
28	Zbigniew Kopertowski	Orange Poland
29	Erwin Schoitsch	Austrian Institute of Technology

■ 3. Landscape of standards



■ Buildings

Horizontals & Verticals

(NEW) ETSI TS 103 849 V1.1.1 Smart M2M; Smart Escalators IoT System

 **URL:** https://www.etsi.org/deliver/etsi_ts/103800_103899/103849/01.01.01_60/ts_103849v010101p.pdf

ABSTRACT: The scope of this standard is the specification of the IoT system for Smart Escalators. It includes: the identification of the relevant roles; the information models in the Smart Lift system, including signals, alarms and commands; the mapping to the communication system (oneM2M); It is a twin specification of ETSI TS 103.735 “Smart Lift IoT System” and is expected to share most of the technical content with it in light of the similarities among lifts and escalators information systems. It is also expected to be linked with the ontology in TS 103410-11 “SAREF for Lifts”.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-08

Buildings

(NEW) ITU-T Y.dt-SComCam ommon requirements and capability framework of digital twin for smart complex and campus

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18750

ABSTRACT: A complex or campus is a collection of buildings and grounds that belong to a given institution, either academic or non-academic. There are many types of complex, such as complexes for corporates, industries, sport and meeting venues, commerce, etc. A campus refers to a specific area for academic purposes. Complexes and campuses play an important role in people’s work and life, and have common requirements in terms of smart management. With the development of the Internet of Things and artificial intelligence, the management of complex and campus has gradually moved towards intelligence, and many smart complex and campus systems have emerged to improve the management and operation efficiency. The digital twin technology can solve the problems like historical record or baseline, operational performance monitoring, testing or predicting future outcomes. It has been widely used in smart complex and campus system. By combining with emerging ICT technologies, such as cloud computing, the Internet of Things, big data, and artificial intelligence, it is possible to access various terminals to collect the data of physical complex and campus in real time, and to model people (without personally identifiable information), devices, things and events in the complex and campus, realize intelligent monitoring and simulation, and realize remote control of the physical complex and campus through the digital twin complex and campus. Digital twin based smart complex and campus system can address challenges of management and operation of complex and campus, such as low management efficiency, poor service experience, serious energy waste, weak comprehensive security, and high operational costs. It implements digital transformation of such complex and campus and enhances service experience.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

■ Built Environment

Smart City

(Updated) ITU-T L.1370 Sustainable and intelligent building services

 **URL:** <https://handle.itu.int/11.1002/1000/13724>

ABSTRACT: This recommendation sets out the services and data required for a sustainable and intelligent building to improve the quality of life of citizens, as well as the specification of its functional features and the technical requirements to be met by the device that provides these services and data.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-11

■ Case Studies and Rankings

Horizontals & Verticals

(NEW) 3GPP TR 22.840 V19.0.0 Study on Ambient power-enabled Internet of Things (Release 19)

 **URL:** https://www.3gpp.org/ftp/Specs/archive/22_series/22.840/

ABSTRACT: The present document describes use cases, traffic scenarios, device constraints of Ambient Internet of Things and identify new potential service requirements as well as new KPIs. An Ambient Internet of Things (Ambient IoT) device is an IoT device, being either battery-less or with limited energy storage capability (i.e., using a capacitor) and the energy is provided through the harvesting of radio waves, light, motion, heat, or any other suitable power source.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

(NEW) 3GPP TR 22.865 V19.2.0 Study on satellite access Phase 3; (Release 19)

 **URL:** https://www.3gpp.org/ftp/Specs/archive/22_series/22.865/22865-j20.zip

ABSTRACT: The present document describes use cases and aspects related to enhancements of the 5G system over satellite, including:

-  Store and Forward (S&F) Satellite operation for delay-tolerant communication service
-  UE-Satellite-UE communication
-  GNSS independent operation
-  Positioning enhancements for satellite access

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

(NEW) AIOTI IoT and Edge Computing EU funded projects landscape, Release 2.0

 **URL:** <https://aioti.eu/wp-content/uploads/2023/12/AIOTI-Report-EU-funded-research-projects-landscape-IoT-and-Edge-computing-R2-Final.pdf>

ABSTRACT: This deliverable provides landscapes of EU funded projects focusing on IoT and edge computing. The main objective of this deliverable is to briefly present the EU funded projects focusing on IoT and edge computing, which can be used to: 1) leverage on existing IoT and edge computing research and innovation activities in Europe, and 2) provide input to IoT and edge computing standardisation gap analysis activities. The Release 2.0 of this report, compared to Release 1.0, includes:

-  a list of additional ongoing projects focusing on IoT and Edge computing that are funded by the EU.
-  project descriptions of projects that were labelled as ongoing in Release 1 and were in the meantime completed, are moved to the respective sections with completed projects.
-  new figures of projects landscape in relation to Standardisation Organisations and Initiatives.

 **DOCUMENT TYPE:** Landscape

 **PUBLICATION DATE:** 2023-12

(NEW) ETSI TR 103 675 AI for IoT: A Proof of Concept

 **URL:** http://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf

ABSTRACT: The present document is addressing the development of a Proof of Concept based on three Use Cases analysed and selected in the associated ETSI TR 103 674. ETSI TR 103 674 addresses the issues related to the introduction of AI into IoT systems and, as first priority, into the oneM2M architecture. ETSI TR 103 674 has identified and described several Use Cases of which three are used for the development of the Proof of Concept described in the present document.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-12

(NEW) ETSI/oneM2M TR 103 716 V1.1.1 oneM2M Discovery and Query solution(s) simulation and performance evaluation

 **URL:** http://www.etsi.org/deliver/etsi_tr/103700_103799/103716/01.01.01_60/tr_103716v010101p.pdf

ABSTRACT: This work will develop a simulation with the goal to provide a proof of concept and a performance evaluation to support the selection and development of the discovery and query solution to be contributed to oneM2M. An extract of the simulation results will be used to support the discussion and the proposal with oneM2M.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-04

(NEW) ETSI TS 103 410-12 V1.1.1 SmartM2M; Extension to SAREF; Part 12: Smart Grid Domain

 **URL:** http://www.etsi.org/deliver/etsi_ts/103400_103499/10341012/01.01.01_60/ts_10341012v010101p.pdf

ABSTRACT: Specify an extension to SAREF to include the semantic model for the Smart Grid domain. This extension will be based on the set of use cases and data models identified in the corresponding requirements TR.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-11

ETSI TR 103 376 SmartM2M; IoT LSP use cases and standards gaps

 **URL:** http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

ABSTRACT: The scope of this document is, starting from the use case families selected for the IoT Large Scale Pilots (LSPs), to a) to provide the collection of all missing functionalities that have been identified in standards bodies (SDOs) to offer solutions addressing the use case requirements.; b) to check that there are no omissions in the standardization activity with regard to the use cases. In particular, gaps with respect to the framework as identified by oneM2M should be identified.; c) to propose some recommendations to overcome potential gaps. Particular attention will be paid on horizontal application layer standardisation and to assure an interworking framework among different vertical industrial segments.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-10

(Updated) IETF RFC 9450 RAW use-cases

 **URL:** <https://datatracker.ietf.org/doc/rfc9450/>

ABSTRACT: This document presents wireless use-cases (such as aeronautical communications, amusement parks, industrial applications, pro audio and video, gaming, UAV and V2V control, edge robotics and emergency vehicles) demanding reliable and available behavior.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-01

(NEW) ITU-T Y.LASS-fra Requirements and capability framework of IoT-based low-altitude sensing system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19601

ABSTRACT: This Recommendation will specify the requirements and capability framework of IoT-based low-altitude sensing system. It will address the following aspects: Overview of IoT-based low-altitude sensing system. Requirements of IoT-based low-altitude sensing system. Capability framework of IoT-based low-altitude sensing system. Use cases of IoT-based low-altitude sensing system. This Recommendation will specify the requirements and capability framework of IoT-based low-altitude sensing system. It will address the following aspects:

-  Overview of IoT-based low-altitude sensing system.
-  Requirements of IoT-based low-altitude sensing system.
-  Capability framework of IoT-based low-altitude sensing system.
-  Use cases of IoT-based low-altitude sensing system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

IETF RFC 8578 Deterministic Networking Use Cases

 **URL:** <https://datatracker.ietf.org/doc/rfc8578/>

ABSTRACT: This document presents use cases for diverse industries that have in common a need for “deterministic flows”.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-01

ISO/IEC TR 22417:2017 Information technology - Internet of things (IoT) - IoT use cases

🔗 URL: <https://www.iso.org/standard/73148.html?browse=tc>

ABSTRACT: ISO/IEC TR 22417:2017(E) This technical report identifies IoT scenarios and use cases based on real-world applications and requirements. The use cases provide a practical context for considerations on interoperability and standards based on user experience. They also clarify where existing standards can be applied and highlight where standardization work is needed.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-11

oneM2M TR-0001-V4.3.0 oneM2M - Use Case collection

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28153>

ABSTRACT: The present document includes a collection of use cases from a variety of M2M industry segments. Each use case may include a description, source, actors, pre-conditions, triggers, normal and alternative flow of sequence of interactions among actors and system, post-conditions, illustrations and potential requirements. The potential requirements provide an initial view of what oneM2M requirements could arise from the Use Case as seen by the contributor. These are intended to help the reader understand the use case's needs. These potential requirements may have been subsequently submitted by the contributor for consideration as candidate oneM2M requirements, which may or may not have been agreed as a oneM2M requirement (often after much editing). As such, there may not be a direct mapping from the potential requirements to agreed oneM2M requirements.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-10

Manufacturing

(NEW) one6G 6G & Robotics: Use Cases and Potential Service Requirements

🔗 URL: <https://one6g.org/download/3287/>

ABSTRACT: The scope of this white paper is to identify robotics use cases and recognize the potential role of mobile communication systems, particularly 6G systems. To understand the involvement of mobile communication systems, the robotic system requirements for each use case are identified. For each of the robotic system requirement the potential contribution of the communication system is determined. Based on this analysis, additional capabilities that 6G systems might need to fulfil for efficiently supporting robotic use cases are outlined.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2023-6

(NEW) one6G 6G & Robotics: A Methodology to identify Potential Service Requirements for 6G-empowered Robotic Use Cases

🔗 URL: <https://one6g.org/download/3962/?tmstv=1699546970>

ABSTRACT: The goal of this white paper is to present a methodology to determine the requirements of 6G robotic UCs across different dimensions namely, wireless sensing, communication, computation and support of AI/ML methods. The proposed methodology represents robotic UCs as a composition

of different phases (i.e., set up, perception and task execution), atomic functions (e.g., registration, environment model establishment, task definition and task sharing) and UC-specific atomic function handlers (e.g., event handlers for human behaviour perception, task handler for human robotic interaction and task handler for motion planning). Depending on the robotic UC, the atomic functions will interact in different ways and each of the different atomic functions will have specific requirements in the dimensions outlined above. The present methodology is further described based on examples from the UC classifications derived in the previous white paper, to demonstrate how to establish system requirements for robotic UCs. Different categories of baseline system requirements of robotic applications, wireless sensing, communication and AI/ML have been derived for a distinctive atomic function and handler per UC class example. By having detailed system requirements per atomic function, the future 6G system may be optimised to provide these network services for each of the atomic functions that compose robotic UCs in the most cost-effective and sustainable way.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2023-11

(NEW) one6G 6G & Robotics: Identifying Use Cases and Potential Service Requirements - Methodology and Examples

🔗 URL: <https://one6g.org/download/4571?tmstvt=1717576666>

ABSTRACT: In this whitepaper, a selection of robotic use cases are discussed, detailing requirements for communication services and sensing operations to support robotic operations within two important scenarios: robot-to-robot cooperation and disaster recovery operations. A variety of use cases are presented which consider the functional requirements for supporting multimodal sensing operations (e.g. 3D mapping, object detection & identification, environment modelling), aspects related to robot autonomy and AI, aspects related to robot control and actuation, and many more topics of interest for 6G robotics applications. The two scenarios explored in this white paper are intended to be the first step towards further consideration of robotics use cases and requirements. Additional use cases will be considered in future volumes of the one6G 6G and Robotics series of white papers.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2024-06

Mobility

5GAA Tele-operated Driving Use Cases, System Architecture and Business Considerations

🔗 URL: <https://5gaa.org/news/tele-operated-driving-use-cases-system-architecture-and-business-considerations/>

ABSTRACT: The evolution of driving automation technology is gradually reducing our dependence on human drivers. Tele-operated Driving (ToD) technology separates drivers or driving automation systems from the physical vehicle, effectively operating it from a remote location. ToD thus enables shared remote assistance or remote driving services from a central location, which has the benefit of reducing labour costs (fewer drivers), while improving safety and comfort for the drivers.

This 5GAA white paper describes the technical and business framework, and a visionary roadmap for ToD services. Different ToD types, which are classified according to the impact on the operation level of an automated vehicle, are studied under the different environments such as automated vehicle parking areas, or public roads or even using different mobile networks. This white paper is an abstract of the following published 5GAA ToD technical reports, where interested readers can find further technical details and business considerations on ToD services.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2021-12

Energy

(NEW) ITU-T YSTR.Ambient IoT Analysis on requirements and use cases of ambient power-enabled IoT

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18752

ABSTRACT: In IoT systems, a large number of physical terminals may not have the space to hold batteries or bear the cost of batteries, such scenarios include but are not limited to fast-moving consumer goods, logistics packages, product line packaging, warehouse goods inventory, etc. Huge scenarios may involve up to more than ten thousand IoT nodes, which conventional IoT devices are not able to implement in terms of cost, size, and power mode. An Ambient power-enabled IoT is a global infrastructure for the information society, enabling IoT services by harvesting ambient energy to power the IoT devices. Instead of using batteries to power the devices, Ambient-IoT devices are capable of harvesting ambient energy to power electronic modules. The ambient power can be provided by distributed power transfer nodes (e.g., existing network infrastructure, dedicated power transfer device) or natural power (e.g., light, vibration, thermal).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Food and Agriculture

(NEW) ITU-T Y Suppl. 76 Use cases of Internet of things-based smart agriculture

 **URL:** https://www.intertekinform.com/en-gb/standards/itu-t-y-suppl-76-09-2023--1344020_saig_itu_itu_3342182/

ABSTRACT: Supplement 76 to ITU-T Y-series Recommendations surveys use cases related to smart agriculture from the perspective of, but not limited to: 1) smart greenhouse; 2) smart open field; 3) smart hydroponics; 4) smart livestock barn; and 5) smart agriculture data service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-09

Water

(NEW) ITU-T Y.Sup.SmartAqua-usecases LTU-T Y.4000-series - Use cases of IoT-based smart aquaculture

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18753

ABSTRACT: Due to climate change and growing population, problems of food shortage are expected globally. Aquaculture, also known as fish farming, adjusts water environments using IoT, AI, and robot technologies to provide better conditions for fish growing. Examples of water environmental parameters which may affect fish growing include dissolved oxygen (DO), air- and water-temperature, pH, carbon dioxide (CO₂), electrical conductivity (EC), suspended solid (SS), turbidity, oxidation-reduction potential (ORP), total ammonia nitrogen, and water levels. A number of diverse IoT devices (including sensors, actuators, and robots) are involved in smart aquaculture in order to provide different services such as water monitoring and management, and autonomous fish farm management. Therefore, it is necessary to survey present smart agriculture technologies as well as future-promising technologies. Based on the survey results, meaningful standardization work items can be identified.

This new work item surveys use cases related to smart aquaculture in the perspective of fish farming using IoT, AI, and robot technologies.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Smart City

(NEW) ITU-T Y.Sup.EdgeloT-usecases Supplement to ITU-T Y.4208 - Use cases of edge computing based Internet of Things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19063

ABSTRACT: Edge computing based Internet of Things is crucial for navigating the evolving global digital economy and advancing digital transformation. This supplement to Y.4208 defines the types of edge computing based Internet of Things, recommended template and classification schemes of use cases. Several use cases are illustrated in details. It also identifies challenges, opportunities, observations as well as suggestions of edge computing based Internet of Things.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-datainterop-usecases Supplement to ITU-T Y.4563 - Use cases of data interoperability in Internet of things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19608

ABSTRACT: ITU-T Y.4563 outlines the requirements and functional model to support data interoperability in Internet of things environments. However, in ITU-T Y.4563 there is a scarcity of use cases related to the data interoperability in IoT and, more generally, data interoperability is not sufficiently addressed for IoT environments. This s draft Supplement to ITU-T Y.4563 provides use cases of data interoperability in IoT. Types, architectural considerations and classification of data interoperability in IoT are specified. Use cases corresponding to the types of data interoperability in IoT are described based on the recommended template. Challenges and opportunities are identified to motivate following standardization works related to this work item.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-IoT-BC Applicability cases of blockchain in the IoT

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19060

ABSTRACT: Cities are taking action and embracing cutting-edge solutions such as artificial intelligence (AI), 5G, digital twin, Internet of Things (IoT) and the metaverse to digitize and automate city operations. Digital technologies are at the forefront of creating smart sustainable cities that promote efficiency, economic development and improved quality of life for inhabitants. Blockchain is identified as one of the important cutting-edge (also referred as emerging technologies) digital technologies enabling city digital transformation. As the lead group of IoT and its applications, as well as the lead group of smart cities and communities and related digital services, ITU-T SG20 has 6 published and 5 on-going blockchain related work items. This Supplement complements the ITU-T SG20 blockchain related Recommendations and is expected to benefit further research and standardization on blockchain integration with IoT. The scope of this Supplement includes:

- 📄 Recommended template for the description of use cases
- 📄 Use cases

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-SCC-AI Supplement to ITU-T Y.4223 - Use cases of smart cities and communities supported by AI

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19604

ABSTRACT: Smart cities and communities (SC&C) share the goal of achieving urban sustainability without sacrificing the quality of life (QoL) of their citizens. Artificial intelligence (AI) offers a powerful tool to address these issues, enabling cities to harness vast amounts of data generated from SC&C. AI can analyze and process this data in real-time, providing actionable insights that help city planners and administrators make more informed decisions. This Supplement specifies the use cases of smart cities and communities supported by AI.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-NGUM Use Cases for Next Generation Urban Measurements

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17915

ABSTRACT: This draft Supplement provides practical use cases from real cities on how to measure selected city KPIs such as air quality, noise pollution, road quality, among others, by using the Next Generation Urban Measurements methodology described in ITU-T Y.SSC-NGUM. This draft Supplement complements the Recommendation ITU-T Y.4903/L.1603 which gives general guidance to cities and provides key performance indicators (KPIs) for smart sustainable cities (SSCs) to help cities achieve sustainable development goals (SDGs). Next Generation Urban Measurements methodology in ITU-T Y.SSC-NGUM uses innovative sensing techniques to collect extensive and more frequent city data from various locations in the city at different times. This draft Supplement will illustrate how real cities collect extensive amount of data from various locations in the city through fixed (e.g. buildings) and mobile units (e.g. taxis, satellites), at different times during the day (and the week), and will discuss how KPIs are measured by these cities. It will also illustrate the high-level architectures adopted by these cities to collect, store and process measurements data by using various technologies (e.g. IoT, AI).

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-Proc-SSC : Procurement guidelines for smart sustainable cities

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19089

ABSTRACT: Summary This draft Supplement will provide guidance on how to effectively procure and implement smart city solutions that are sustainable, resilient, and inclusive. It aims to provide practical procurement processes or steps to take throughout the digital data and technology buying cycle - planning, informing the market, evaluation and managing delivery. It will also delve into effective and efficient procurement during emergencies/ crises. This draft Supplement is based on the U4SSC report entitled "Procurement guidelines for smart sustainable cities".

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

Buildings

IETF RFC7733 Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control

 **URL:** <https://datatracker.ietf.org/doc/rfc7733/>

ABSTRACT: The purpose of this document is to provide guidance in the selection and use of protocols from the Routing Protocol for Low-Power and Lossy Networks (RPL) protocol suite to implement the features required for control in building and home environments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-02

Health

(NEW) one6G 6G & eHealth: Use Cases and Potential Service Requirements

 **URL:** <https://one6g.org/download/5016/?tmstv=1725618580>

ABSTRACT: The goal of this whitepaper is to overview the potential of 6G technology on the eHealth do-main to tackle the key trends in the healthcare sector. To achieve this, we identified and developed use cases together with their functional requirements and key performance indicators in terms of communication, sensing and AI/ML support necessary to realize the use cases. Through discussions with different stakeholders from the medical domain, industry and academic researchers, we have identified 4 clusters of eHealth use cases: Medical Robotic Applications, Vital Sign Wireless Sensing, Medical Data & Model Sharing, and Immersive & Ubiquitous Treatment. The developed use cases per cluster are guided by the model-based medicine vision identified and further developed by members of the medical domain in one6G, where all actors in the healthcare system are mapped with their corresponding digital twin models, and evidence is quickly generated for what-if scenarios in healthcare processes (e.g., health outcome of a patient given medical treatment) in a cost efficient manner. Altogether, the use cases provide different key functional components to enable this vision. Use cases may be realized on its own independent of the model-based vision. We elaborate on initial considerations related to risk mitigation, potential countermeasures, privacy and ethics. Additional use cases will be considered in future volumes of the one6G 6G and eHealth series of white papers.

 **DOCUMENT TYPE:** Whitepaper

 **PUBLICATION DATE:** 2024-09

■ Connectivity

Horizontals & Verticals

3GPP TR 36.763 V17.0.0 Study on Narrow-Band Internet of Things (NB-IoT) / enhanced Machine Type Communication (eMTC) support for Non-Terrestrial Networks (NTN)

🔗 **URL:** <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3747>

ABSTRACT: The objectives for this document are, based on the outcomes of the Release-17 NR NTN WI and Release-16 TR 38.821, to study a set of necessary features/adaptations enabling the operation of the IoT NTN for 3GPP Release 17 with a priority on satellite access.

The first objective of this Study is to identify scenarios applicable to NB-IoT/eMTC, including:

- 📄 Bands of interest in sub 6 GHz
- 📄 Device type with PC3 or PC5 (LEO and GEO)
- 📄 Satellite constellation orbit LEO and GEO
- 📄 Transparent payload.
- 📄 Link budget

The second objective is, for the above identified scenarios, to study and recommend necessary changes to support NB-IoT and eMTC over satellite, reusing as much as possible the conclusions of the studies performed for NR NTN in TR38.821. This objective will address the following items:

- 📄 Aspects related to random access procedure/signals
- 📄 Mechanisms for time/frequency adjustment including Timing Advance, and UL frequency compensation indication
- 📄 Timing offset related to scheduling and HARQ-ACK feedback
- 📄 Aspects related to HARQ operation
- 📄 General aspects related to timers (e.g. SR, DRX, etc.)
- 📄 RAN2 aspects related to idle mode and connected mode mobility [RAN2]
- 📄 RLF-based for NB-IoT
- 📄 Handover-based for eMTC
- 📄 System information enhancements
- 📄 Tracking area enhancements

Recommendations for NB-IoT and recommendations for eMTC will be documented in the conclusions

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-06

3GPP TR 36.763 V17.0.0 Study on Narrow-Band Internet of Things (NB-IoT) / enhanced Machine Type Communication (eMTC) support for Non-Terrestrial Networks (NTN)

🔗 **URL:** https://www.3gpp.org/news-events/1805-iot_r14

ABSTRACT: The objectives for this document are, based on the outcomes of the Release-17 NR NTN WI and Release-16 TR 38.821, to study a set of necessary features/adaptations enabling the operation of the IoT NTN for 3GPP Release 17 with a priority on satellite access.

The first objective of this Study is to identify scenarios applicable to NB-IoT/eMTC, including:

- 📄 Bands of interest in sub 6 GHz

- 🔖 Device type with PC3 or PC5 (LEO and GEO)
- 🔖 Satellite constellation orbit LEO and GEO
- 🔖 Transparent payload.
- 🔖 Link budget

The second objective is, for the above identified scenarios, to study and recommend necessary changes to support NB-IoT and eMTC over satellite, reusing as much as possible the conclusions of the studies performed for NR NTN in TR38.821. This objective will address the following items:

- 🔖 Aspects related to random access procedure/signals
- 🔖 Mechanisms for time/frequency adjustment including Timing Advance, and UL frequency compensation indication
- 🔖 Timing offset related to scheduling and HARQ-ACK feedback
- 🔖 Aspects related to HARQ operation
- 🔖 General aspects related to timers (e.g. SR, DRX, etc.)
- 🔖 RAN2 aspects related to idle mode and connected mode mobility
- 🔖 RLF-based for NB-IoT
- 🔖 Handover-based for eMTC
- 🔖 System information enhancements
- 🔖 Tracking area enhancements

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2021-06

3GPP TR 36.802 V13.0.0 Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IOT; Technical Report for BS and UE radio transmission and reception

🔗 URL: https://www.3gpp.org/ftp/Specs/archive/36_series/36.802/

ABSTRACT: The present document summarizes the studies of radio requirements for BS and UE radio transmission and reception as part of the work item on Narrowband Internet of Things (NB-IoT).

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2016-06

(Updated) 3GPP TR-0024-V4.3.0 3GPP Interworking

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31840>

ABSTRACT: The present document is a study of interworking between oneM2M Architecture and 3GPP Rel-13 architecture for Service Capability Exposure as defined in the release 13 version of ETSI TS 123 682 [i.5]. The key objective and value is analyzed and described. The document also investigates the potential solution in oneM2M by evaluating the existing technical solutions.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-03

5G PPP H2020 ICT-18-2018 5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors - Challenges and Opportunities

🔗 URL: https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf

ABSTRACT: The white paper focuses on 5G infrastructure along the main EU transport paths, to enable a series of advanced Cooperative, Connected and Automated Mobility (CCAM) use cases and services across Europe. It introduces the scope, use cases, trial sites and particularities of each of the related corridor projects. It also identifies and elaborates on the main concerns and challenges arising from deploying advanced CCAM use cases at regional borders. This analysis takes into consideration technological, administrative, security and legislative aspects.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2020-10

AIOTI Identifiers in Internet of Things (IoT)

🔗 URL: https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1.0.pdf.pdf

ABSTRACT: Identification is a major topic in Internet of Things (IoT). Besides identification of the things itself, many other entities have to be identified in IoT solutions. In this paper we discuss the various identification needs with related use cases and requirements. Furthermore we look at identifier standards, their applicability for the different identifier needs and discuss identifier allocation, registration, resolution, security, privacy and interoperability. The starting point for this deliverable was a survey that was conducted in spring 2017 within the IoT standardization and research community. This survey is a significant input to this deliverable, along with several research and standardisation documents related to IoT identities. Due to the large application area for IoT and the wide landscape of standardization activities, research work, technologies and already existing IoT platforms and solutions the paper can only provide a general overview. It does not claim to cover the whole space of IoT use cases, requirements and standards for identifiers. The document provides a high level discussion on the above topics. It provides a structured approach by classification of identifier usage and a categorization of requirements. In general no single identification scheme fits all needs. Furthermore many identification are already standardized and in use. It therefore does not define or recommend specific solutions and standards, but provides examples and summaries in order to indicate what has to be taken into account when considering identifiers in IoT. This also includes different topics related to interoperability of identifiers. Furthermore security and privacy are raised as important topics for identifiers and appropriate threat and risk analysis have to be performed and relevant regulatory and legal framework have to be taken into account.

📄 DOCUMENT TYPE: Landscape

📅 PUBLICATION DATE: 2018-02

(NEW) AIOTI Computing Continuum Scenarios, Proof of Concepts, Requirements and Optical Communication enablers, Release 2.0

🔗 URL: <https://aioti.eu/wp-content/uploads/AIOTI-Computing-Continuum-Report-R2-Final.pdf>

ABSTRACT: This report introduces Computing Continuum use cases, requirements and KPIs on communication infrastructures, IoT and edge computing platforms. Compared to many current activities, the computing continuum enables a more flexible allocation of compute and communication resources and workload placement. Many novel applications require rather stringent KPIs since the IoT becomes more and more mission-critical. The new system requirements include strong security, very high bandwidth, very low delays, and very high reliability. Depending on the use case and deployment scenario, various technology enablers are currently under standardization, including the F5G optical network architecture, as well as novel approaches for computing, networking and establishing security. Regarding computing continuum platforms, high-performance secure computing together with optical communication can be considered as an ideal combination fulfilling the high-end IoT requirements. In fact, many basic requirements for high-end IoT can be satisfied by optical communication enablers. Such enablers can also help meeting stringent communication requirements stemming from the distributed nature of the continuum including multiple, potentially different, computing locations. Furthermore, high-end IoT devices, that may be connected via optical communication technologies, can enable a whole new application area to be explored and supported. For example, some use cases might need very high resolution and high frame rate of camera sensors that send uncompressed video to AI-enabled analytics platforms with minimum delay. These analytics

platforms typically need to react fast on any given situation and steer actors appropriately. The proof of concepts validates the great potential of passive optical networks for new use cases such as fibre to the room, but also for industrial applications where low latency In combination with Wi-Fi is required. Recommendations for the evolution of the current technologies employed for high-end IoT systems running on computing continuum platforms are discussed. Finally, it is shown that passive optical networks play an important role for decarbonizing vertical sectors due to their improved footprint over conventional switch-based networking solutions, especially in scenarios with large numbers of access points.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-05

bloTope project D3.5 Prototype of Platform Integration using API Mediators

🔗 URL: <https://stl1.ning.com/topology/rest/1.0/file/get/1065014?profile=original>

ABSTRACT: This document is a part of the definition of the overall bloTope Systems of Systems (SoS) ecosystem architecture by providing state-of-the-art framework for information source publication and consumption developed around Open API standards including Open Messaging Interface (O-MI) and Open Data Format (O-DF) specifications. This SoS platform will enable users, developers, and resource providers to publish, consume, compose, and integrate services in order to explain the coordination of various platforms with the standardized APIs. For the platform to be successful, the APIs and platforms need to be robust and better managed, acting as technological foundation for an open Internet of Things (IoT) innovation ecosystem.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-06

bloTope project D3.6 V2.0 Information Source Publication and Consumption Framework

🔗 URL: <https://storage.ning.com/topology/rest/1.0/file/get/35619932?profile=original>

ABSTRACT: The main objective of this document is to present the final version of the mechanisms used to enable IoT device and IoT-related information systems to publish their presence, and be discovered by, other IoT systems, by extending the discovery functionality provided by O-MI and O-DF standards with geo-location and semantic web discovery methods (e.g., describing meta-data about different services).

📄 DOCUMENT TYPE: Framework

📅 PUBLICATION DATE: 2018-01

bloTope project D5.2 V1.0 Service Composition Framework

🔗 URL: <https://stl1.ning.com/topology/rest/1.0/file/get/1064994?profile=original>

ABSTRACT: This document discusses the problem domain of IoT service composition and outlines the bloTope approach to overcome the identified problems by introducing an exemplary setting that helps illustrating the basic principles. The document also concretizes the methods by examples based on real-world data and describes the architecture and integration method chosen to implement the data-integration platform that follows the suggested approach and drives the service composition framework. Finally, the document provides an overview on tools for graphical user interaction that may be used as a frontend for service composition, and discusses related work that has already been done in the field.

📄 DOCUMENT TYPE: Framework

📅 PUBLICATION DATE: 2017-01

bloTope project D5.5 V2.0 Service Composition Framework

 **URL:** <https://storage.ning.com/topology/rest/1.0/file/get/35619974?profile=original>

ABSTRACT: This document presents an approach for standardized workflow composition between bloTope XaaS components. It shows how this approach can be implemented on a technical level as a framework. The framework resembles a toolbox of building blocks that allow the definition of workflows between bloTope XaaS components, thus fostering integration and interoperability. It is centered around an open-source visual programming environment (Node-RED). It contains visual representations (nodes) of XaaS components provided by the bloTope consortium, to compose bloTope services, as well as predefined workflows and useful services that aim to support end-users in orchestrating and working with bloTope components.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2017-12

CEN EN 13757-3:2018 Communication systems for meters - Part 3: Application protocols

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:61820&cs=1699FDB9F0D54F7BB01D7266589ED286A

ABSTRACT: This draft European Standard specifies application protocols for communication systems for meters and remote reading of meters. This draft European Standard specifies application protocols, especially the M-Bus application protocol. This draft European Standard is intended to be used with the lower layer specifications determined in EN 13757-2, EN 13757-4, EN 13757-5, EN 13757-6 and prEN 13757-7.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-10

CEN EN 13757-4:2019 Communication systems for meters - Part 4: Wireless M-Bus communication

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60262&cs=156CDF6A723103E3251766A06586779B6

ABSTRACT: This European Standard specifies the requirements of parameters for the physical and the link layer for systems using radio to read remote meters. The primary focus is to use the Short Range Device (SRD) unlicensed telemetry bands. The standard encompasses systems for walk-by, drive-by and fixed installations. As a broad definition, this European Standard can be applied to various application layers.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-11

CEN EN 13757-6:2015 Communication systems for meters - Part 6: Local Bus

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41515&cs=14E87496D5D72D87C65ABEBFFCB3BD0AB

ABSTRACT: This European Standard specifies the physical layer parameters of a local meter readout system (Local Bus) for the communication with and the readout of a single meter or a small cluster of meters via a single battery powered readout device (master) which can be connected temporarily or stationary for the communication directly to a meter (i.e. local readout) or via a fixed wiring or a small bus (i.e. remote readout). For generic descriptions concerning communication systems for meters and remote reading of meters, refer to EN 13757-1.

CEN EN 13757-7:2018 Communication systems for meters - Part 7: Transport and security services

URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:61822&cs=107399C785EC0B2EDACF60D74955A90D5

ABSTRACT: This draft European Standard specifies Transport and Security Services for communication systems for meters and remote reading of meters. This draft European Standard specifies secure communication capabilities by design and supports the building of a secure system architecture. This draft European standard is applicable to the protection of consumer data to ensure privacy. This draft European Standard is intended to be used with the lower layer specifications determined in EN 13757-2, EN 13757-3, EN 13757-4, EN 13757-5 and EN 13757-6.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2018-10

CEN EN 1434-3:2015 Heat meters - Part 3: Data exchange and interfaces

URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41516&cs=157EF44C329D0ADE1DB97DF0406BAA443

ABSTRACT: This European Standard specifies the general requirements and applies to heat meters. Heat meters are instruments intended for measuring the energy which in a heat-exchange circuit is absorbed (cooling) or given up (heating) by a liquid called the heat-conveying liquid. The meter indicates heat in legal units. Part 3 specifies the data exchange between a meter and a readout device (POINT / POINT communication). For these applications using the optical readout head, the EN 62056-21 protocol is recommended. For direct or remote local readout of a single or a few meters via a battery driven readout device, the physical layer of EN 13757-6 (local bus) is recommended. For bigger networks with up to 250 meters, a master unit with AC mains supply according to EN 13757-2 is necessary to control the M-Bus. For these applications the physical and link layer of EN 13757-2 and the application layer of EN 13757-3 is required. For wireless meter communications, EN 13757-4 describes several alternatives of walk/drive-by readout via a mobile station or by using stationary receivers or a network. Both unidirectionally and bidirectionally transmitting meters are supported by this standard.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2016-06

CEN EN 16836-2:2016 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 2: Networking layer and stack specification

URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41099&cs=181323929D1945B365914E7CE01F502AD

ABSTRACT: This European Standard specifies the medium access control/physical layer MAC/PHY and networking layer of a communication protocol for the exchange of data from metering devices to other devices within a mesh network. The referenced documents in this European Standard contain specifications, interface descriptions, object descriptions, protocols and algorithms pertaining to this protocol standard, the device objects, device profile, the application framework, the network layer, and security services. They are referenced in their entirety for reasons of backwards compatibility and interoperability with products in the field currently using this technology.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2017-05

CEN EN 16836-3:2016 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 3: Energy profile specification dedicated application layer

URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41100&cs=1C46CE950442B0C43F9EDDAC4585ACF19

ABSTRACT: This European Standard specifies the application layer of a communication protocol for the exchange of data from metering devices to other devices within a mesh network. This European Standard makes reference to a number of documents whereby core requirements are specified. This referencing is in compliance with the Bridge Consortium and additionally the Memorandum of Understanding between the ZigBee Alliance and CEN/CENELEC. The EN 16836 series represents a feature subset of a larger standard and as such not all of the features specified in the referenced documents are specified in this standard, due to some features being outside the scope of CEN/TC 294. Where this is the case the out of scope feature has either been omitted or specified as excluded.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2017-05

CEN/TR 17167:2018 Communication system for meters - Accompanying TR to EN 13757-2,-3 and -7, Examples and supplementary information

URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:61828&cs=1338F0A4C7239D0EC0470C6E1605E2BCF

ABSTRACT: This Technical Report contains additional information to the requirements determined in EN 13757-2, EN 13757-3 and EN 13757-7, in particular examples for the implementation, Datagram examples secured by security mechanism of part 7 and additional non-normative requirements beyond meter communication itself.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2018-04

(Updated) Contiki-NG Contiki-NG, the OS for Next Generation IoT Devices

URL: <https://www.contiki-ng.org/>

ABSTRACT: 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.

DOCUMENT TYPE: Framework

PUBLICATION DATE: 2024-09

ETSI EN 300 175-1 Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview

 **URL:** http://www.etsi.org/deliver/etsi_en/300100_300199/30017501/02.09.01_60/en_30017501v020901p.pdf

ABSTRACT: This standard gives an introduction and overview of the complete Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

It contains an abstract of the other parts of the DECT standard together with a general description of: the objectives of the standard; the DECT Common Interface; the protocol architecture of DECT.

The standard also provides an extensive vocabulary; in particular it contains the common definitions of all the technical terms used in different parts of the standard.

The standard includes New Generation DECT, a further development of the DECT standard introducing wideband speech, improved data services, new slot types and other technical enhancements. The standard includes DECT Evolution.

This is the first part of a multi-part standard with Part 1: Overview; Part 2: Physical Layer (PHL); Part 3: Medium Access Control (MAC) layer; Part 4: Data Link Control (DLC) layer; Part 5: Network (NWK) layer; Part 6: Identities and addressing; Part 7: Security features; Part 8: Speech and audio coding and transmission.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-03

ETSI EN 302 065-1 Short Range Devices (SRD) using Ultra Wide Band technology (UWB); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Requirements for Generic UWB applications

 **URL:** http://www.etsi.org/deliver/etsi_en/302000_302099/30206501/02.01.01_60/en_30206501v020101p.pdf

ABSTRACT: This standard applies to transceivers, transmitters and receivers utilizing Ultra WideBand (UWB) technologies and used for short range applications.

It applies to impulse, modified impulse and RF carrier based UWB communication technologies. The standard applies to fixed (indoor only), mobile or portable applications, e.g.: stand-alone radio equipment with or without its own control provisions; plug-in radio devices intended for use with, or within, a variety of host systems, e.g. personal computers, hand-held terminals, etc.; plug-in radio devices intended for use within combined equipment, e.g. cable modems, set-top boxes, access points, etc.; combined equipment or a combination of a plug-in radio device and a specific type of host equipment.

It is the first part of a multi-part standard, with Part 1: Requirements for Generic UWB applications; Part 2: Requirements for UWB location tracking; Part 3: Requirements for UWB devices for ground based vehicular applications; Part 4: Material Sensing devices using UWB technology below 10,6 GHz; Part 5: Devices using UWB technology onboard aircraft.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-11

ETSI GR IP6 001 IPv6 Deployment in the Enterprise

 **URL:** https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_IP6001v010101p.pdf

ABSTRACT: The present document outlines the motivation for the deployment of IPv6 in enterprises, the objectives, the benefits, the risks, the challenges, the technology guidelines, the different choices that arise when designing IPv6-only or dual-stack enterprise network, step-by-step process, the addressing plan, and the milestones.

ETSI GR IP6 008 IPv6-based Internet of Things Deployment of IPv6-based Internet of Things

URL: https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_IP6008v010101p.pdf

ABSTRACT: The present document outlines the motivation for IPv6 in IoT, the technical challenges to address IoT on constrained devices and networks, the impact on the IPv6 technology and protocols, the technology guidelines, the step by step process, the benefits, the risks, as applicable to IoT domains including: M2M, Energy, Industrial, Mining, Oil and gas, Smart city, Transportation (including EVs), etc. IPv6-based IoT in this context refers to the connectivity network layers needed to support the communication between things. It is understood that a complete IoT system may use of an IoT architecture including but not necessarily an abstraction layer part of an IoT platform. The description of such IoT platform is out of the scope of the present document.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2017-06

ETSI GS LTN 002 Low Throughput Networks (LTN) - Functional Architecture

URL: https://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN002v010101p.pdf

ABSTRACT: The present document aims to:

- describe the characteristics of the architecture of a Low Throughput Network
- illustrate the applicability of LTN in industrial communication
- highlight the specificity of LTN deployment

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2014-09

ETSI GS LTN 003 Low Throughput Networks (LTN) - Protocols and Interfaces

URL: https://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN003v010101p.pdf

ABSTRACT: The document aims to define the protocols and interfaces of LTN systems. It goes along with the document GS LTN 002 [5] on LTN functional architecture.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2014-09

ETSI GS NGP 005 Next Generation Protocol Requirements

URL: https://www.etsi.org/deliver/etsi_gs/NGP/001_099/005/01.01.01_60/gs_NGP005v010101p.pdf

ABSTRACT: The scope of the Standard is to specify the minimum set of key requirements for the Next Generation Protocols (NGP), Industry Specific Group (ISG). The present document addresses requirements in the following areas:

- Business Case and Techno-Economics
- Migration
- General Technical Requirements
- Addressing

- 🔖 Security
- 🔖 Mobility
- 🔖 Multi-Access Support (including FMC)
- 🔖 Context Awareness
- 🔖 Performance (including Content Enablement)
- 🔖 Network Virtualisation
- 🔖 IoT Support
- 🔖 Energy Efficiency
- 🔖 e-Commerce
- 🔖 MEC
- 🔖 Mission Critical Services
- 🔖 Drones and Autonomous Vehicles and Connected Vehicles
- 🔖 Ultra Reliable Low Latency Communications

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-04

ETSI TR 103 249 Low Throughput Network (LTN); Use Cases and System Characteristics

🔗 URL: http://www.etsi.org/deliver/etsi_tr/103200_103299/103249/01.01.01_60/tr_103249v010101p.pdf

ABSTRACT: This report provides illustrative use cases for LTN Systems and key characteristics of such systems to support the development of the LTN Standard.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-10

ETSI TR 103 467 Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem

🔗 URL: https://www.etsi.org/deliver/etsi_tr/103400_103499/103467/01.01.01_60/tr_103467v010101p.pdf

ABSTRACT: The present document discusses Quality of Service (QoS) aspects of services related to the Internet of Things (IoT) ecosystem from an end-to-end perspective; a strict end-user, service-oriented point of view. Here, end-to-end is understood as "from a service user/terminal/provider to a service user/terminal/provider".

The discussion deals with two questions. The first question is if the existing framework for QoS parameter definitions and methodologies is sufficient to also include the IoT angle of view. The second question is if the existing portfolio of QoS parameters needs extensions or adaptations.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-06

ETSI TR 103 514 DECT; DECT-2020 New Radio (NR) interface; Study on Physical (PHY) layer

🔗 URL: https://www.standict.eu/sites/default/files/2021-01/tr_103514v010101p.pdf

ABSTRACT: The document aims on studying "DECT-2020: New Radio", a new radio interface based on state of the art paradigms able to offer the required data rates, propagation characteristics and spectrum efficiency, while maintaining compatibility with the carrier and time structure of the DECT band.

The document is focused on the Physical layer. DECT-2020, as defined by the present document, will be based on OFDM and may support space multiplexing (MIMO). The study focuses on:

- 1) Review of use cases and key application areas for DECT-2020.
- 2) Identification of methodology, initial sources, simulation tools and models.
- 3) Initial definition of “DECT-2020: New Radio” PHY layer, providing guidance for a following technical specification.
- 4) Preliminary simulation results and preliminary study on spatial multiplexing (MIMO).

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-07

ETSI TR 103 515 DECT; Study on URLLC use cases of vertical industries for DECT evolution and DECT-2020

🔗 URL: https://www.etsi.org/deliver/etsi_tr/103500_103599/103515/01.01.01_60/tr_103515v010101p.pdf

ABSTRACT: The document presents a study of use cases and vertical scenarios for Ultra-Reliable Low-Latency Communications (URLLC) intended to be used as base requirements for evolving DECT.

The proposed use cases can be classified as belonging to the following three major application areas:

- 📁 Home and Building Automation, including Smart Living;
- 📁 Industry automation - Factories of the Future, Industry 4.0;
- 📁 Media and entertainment industry - Programme Making and Special Events (PMSE).

The identified scenarios are intended to be implementable under 5G technology assumptions and timeframe. However some of them may also be implementable enhancements of current DECT technology.

By 5G technology assumptions, it is meant state of the art radio interfaces based on OFDM with optional use of MIMO.

The present document also describes the methodology and sources used for the identification of use cases, and describes the required DECT standard specifications for the implementation of the different evolution paths.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-03

ETSI TS 102 939-1 DECT; Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1)

🔗 URL: https://www.etsi.org/deliver/etsi_ts/102900_102999/10293901/01.03.01_60/ts_10293901v010301p.pdf

ABSTRACT: The present document specifies the first set of functionalities of the ETSI radio technology named DECT Ultra Low Energy (ULE).

The set of features defined in the present document is named “Home Automation Network (HAN), phase 1”, and is primarily targeted to provide a global M2M solution within domestic scenarios. However, this does not prevent the use of the present document in other scenarios.

DECT Ultra Low Energy (ULE) provides bi-directional radio communication with medium range, data protection, and Ultra Low Power consumption between different types of Portable Devices and Radio Fixed Parts.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-10

ETSI TS 103 357 Short Range Devices; Low Throughput Networks (LTN); Protocols for radio interface A

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103357/01.01.01_60/ts_103357v010101p.pdf

ABSTRACT: The present document specifies the radio protocols of three radio technologies, referred to as “families”. It contains an implementable description of physical and MAC/link protocol layers. It concludes with a section on implementation commonalities between the three LTN families.

NOTE: ETSI TR 103 249 describes LTN use cases and system characteristics. ETSI TS 103 358 specifies the architecture of LTN systems.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-06

ETSI TS 103 358 Short range devices; Low Throughput Networks (LTN) Architecture; LTN Architecture

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103358/01.01.01_60/ts_103358v010101p.pdf

ABSTRACT: The Internet of Things (IoT) presents a wide and growing range of communications requirements. Certain of these requirements are addressed by systems which are referred to as ‘Low Throughput Networks’ (LTN) in ETSI documents. The use cases addressed by LTN systems and the LTN systems characteristics are provided in ETSI TR 103 249. LTN systems may be considered to be a subset of Low Power Wide Area Networks (LPWAN), that may include other systems, already existing or developed in the future.

This standard specifies the architecture of LTN systems. It contains requirements and/or recommendations on functional blocks and interfaces that are related to the architecture (i.e. high-level description) of LTN systems. It develops the work done in LTN ISG (ETSI GS LTN 002) on architecture for LTN systems. The present document should be read in conjunction with ETSI TR 103 249 and related documents, in which details of entities and interfaces are documented.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-06

ETSI TS 103 596-1 V1.1.1 (Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 1: Conformance Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359601/01.01.01_60/ts_10359601v010101p.pdf

ABSTRACT: While the Internet of Things (IoT) is on the rise, the quality assurance of interconnected systems becomes an everincreasing challenge. Within the last years, many different IoT protocols came to the fore.

The present document provides a test specification, i.e. an overall test suite structure and catalogue of test purposes for the Constrained Application Protocol (CoAP). It will be a reference base for both client-side test campaigns and serverside test campaigns addressing the conformance issues.

In the present document the conformance testing is presented. It provides a basis for interoperability testing and performance testing. The latter is presented in ETSI TS 103 536-3.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

ETSI TS 103 596-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 2: Security Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359602/01.01.01_60/ts_10359602v010101p.pdf

ABSTRACT: The present document provides an introduction and guide for developers and users investigating in security testing of the COAP communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. It belongs to a multi-part deliverable addressing the most relevant testing aspects of COAP: conformance, security and performance testing. While the conformance testing part presents a complete set of test purposes, the content for security and performance parts is different and focus on evaluating relevant testing techniques and the provision of samples that are specific for COAP. For this reason, the structure of the present document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for COAP. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the COAP protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

ETSI TS 103 596-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 3: Performance Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359603/01.01.01_60/ts_10359603v010101p.pdf

ABSTRACT: The present document provides an introduction and possible test specification, i.e. an overall test suite structure and catalogue of performance test purposes for the Constrained Application Protocol (CoAP) protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the performance issues.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

ETSI TS 103 597-1 V1.1.2 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 1: Conformance Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359701/01.01.02_60/ts_10359701v010102p.pdf

ABSTRACT: While the Internet of Things (IoT) is on the rise, the quality assurance of interconnected systems becomes an ever-increasing challenge. Within the last years, many different IoT protocols came to the fore. The MQ Telemetry

Transport (MQTT) protocol is one of the most popular representatives as many surveys have shown.

Although many implementations for the MQTT protocol exist, it lacks in satisfying quality assurance. While many IoT components communicate over standardized protocols, communication protocols for IoT like MQTT or CoAP evolved over time without a holistic approach for quality assurance.

In the present document the conformance testing is presented. It provides a basis for interoperability testing and performance testing. The latter is presented in ETSI TS 103 597-3.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-01

ETSI TS 103 597-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 2: Security Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359702/01.01.01_60/ts_10359702v010101p.pdf

ABSTRACT: The present document provides an introduction and guide for developers and users investigating in security testing of the MQTT communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. It belongs to a multipart technical specification addressing the most relevant

testing aspects of MQTT:

-  conformance;
-  security; and
-  performance testing.

While the conformance testing part presents a complete set of test purposes, the content for security and performance parts is different and focus on evaluating relevant testing techniques and the provision of samples that are specific for MQTT. For this reason, the structure of the document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for MQTT. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the MQTT protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

ETSI TS 103 597-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 3: Performance Tests

 **URL:** https://www.etsi.org/deliver/etsi_ts/103500_103599/10359703/01.01.01_60/ts_10359703v010101p.pdf

ABSTRACT: Technology advancements are bringing ever-increasing computing power and network speed in the communication domain. The number of communicating devices is expected to increase by 2 orders of magnitude in the following decade and with that several challenges emerge. A main challenge pertains to efficiency regarding resource consumption and overall performance.

As existing communication protocols evolve and new ones are created to fit the current technological capabilities and societal needs and the standards that serve the basis for interoperability and compliance. This is most relevant in the foreseen context of the Internet of Things (IoT) which envisions a very high density of connected devices in the near future. The Message Queuing Telemetry Transport (MQTT) protocol is one such example of evolution.

While many IoT components communicate over standardized protocols, communication protocols for IoT like MQTT or CoAP evolved over time without a holistic approach for quality assurance. Although there are many published evaluations of various MQTT implementations, a lack of common language, methods and presentation of results is slowing down the adoption rate and overall evolution of the protocol.

In the present document the performance testing is presented. It provides a basis for benchmark testing and performance evaluation for the MQTT protocol.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-01

(Updated) FIT IoT-LAB Testbed The Very Large Scale Internet of Things Testbed

 **URL:** <https://www.iot-lab.info/>

ABSTRACT: IoT-LAB provides a facility suitable for testing networking with small wireless sensor devices and heterogeneous communicating objects.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2024-09

(Updated) FIWARE Internet of Things Framework

 **URL:** <https://www.fiware.org/>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Open_Source

 **PUBLICATION DATE:** 2024-09

(Updated) IEC 61406-1 ED1 Identification Link - Part 1: General requirements

 **URL:** <https://webstore.iec.ch/publication/67673>

ABSTRACT: IEC 61406-1:2022 specifies minimum requirements for a globally unique identification of physical objects which also constitutes a link to its related digital information. This identification is designated hereinafter as “Identification Link” (IL), with the encoded data designated as IL string. The IL string has the data-format of a link (URL). The IL is machine-readable and is attached to the physical object in a 2D symbol or NFC tag. The requirements in this standard apply to physical objects:

-  that are provided by the manufacturer as an individual unit,
-  and that have already been given a unique identity by the manufacturer.

This document does not specify any requirements on the content and the layout of nameplates/typeplates (e.g. spatial arrangement, content of the plain texts, approval symbols etc.).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-09-15

(NEW) IEC 61406-2:2024 Identification link - Part 2: Types/models, lots/batches, items and characteristics

 **URL:** <https://webstore.iec.ch/publication/77973>

ABSTRACT: IEC 61406-2:2024 complements IEC 61406-1 by providing additional requirements for those cases where data elements are encoded within the Structured Identification Link string with standardized syntax and semantics.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-05-08

IEEE 802.1AS-2020 Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks

 **URL:** <https://standards.ieee.org/ieee/802.1AS/7121/>

ABSTRACT: This standard defines a protocol and procedures for the transport of timing over bridged and virtual bridged local area networks. It includes the transport of synchronized time, the selection of the timing source (i.e., best master), and the indication of the occurrence and magnitude of timing impairments (i.e., phase and frequency discontinuities). The PDF of this standard is available at the IEEEGET program. The "IEEE Get Program" grants public access to view and download individual PDFs of select standards at no charge. Visit <http://standards.ieee.org/about/get/index.html> for details.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06

(NEW) IEEE 1901c-2024 IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications Amendment 3: Enhanced Flexible Channel Wavelet (FCW) Physical and Media Access Control Layers for Use on Any Media

 **URL:** <https://standards.ieee.org/ieee/1901c/10922/>

ABSTRACT: Physical (PHY) and media access control (MAC) layers of an improved flexible channel wavelet (FCW) technology to be usable for communication on any media called extended flexible channel wavelet (FCW) PHY/MAC are specified in this amendment. New communication channels are defined in low-frequency bands to extend the communication range and increase the robustness of communication, and how the IEEE Std 1588 precision time protocol (PTP) works over wavelet networks is specified to enhance network functions.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 15/05/2024

(Updated) IETF draft-ietf-raw-technologies Reliable and Available Wireless Technologies

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-raw-technologies/>

ABSTRACT: This document presents a series of recent technologies that are capable of time synchronization and scheduling of transmission, making them suitable to carry time-sensitive flows with high reliability and availability

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-07

(NEW) IETF draft-nichols-iotops-defined-trust-transport Defined-Trust Transport (DeftT) Protocol for Limited Domains

 **URL:** <https://datatracker.ietf.org/doc/draft-nichols-iotops-defined-trust-transport/>

ABSTRACT: This document describes a broadcast-oriented, many-to-many Defined- trust Transport (DeftT) framework that makes it simple to express and enforce application and deployment specific integrity, authentication, access control and behavior constraints directly in the protocol stack. DeftT enables secure and completely self-contained (e.g., no external identity servers or certificate authorities) overlay networks where credentialed members can join and leave at any time. DeftT is

part of a Defined-trust Communications approach with a specific example implementation available. Combined with IPv6 multicast and modern hardware-based methods for securing keys and code, it provides an easy to use foundation for secure and efficient communications in Limited Domains (RFC8799), in particular for Operational Technology (OT) networks

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-03

(NEW) IETF draft-walther-iotops-iot-ops IoT Operational Issues

🔗 URL: <https://datatracker.ietf.org/doc/draft-walther-iotops-iot-ops/>

ABSTRACT: This I-D is based on a presentation at IETF 119 in the IOTOPS WG.

🔗 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2024-03

ZigBee ZigBee Document 13-0402-14 - Base Device Behaviour Specification -

🔗 URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: The purpose of this specification is to clearly define the environment, initialization, commissioning and operating procedures of a base device operating on the ZigBee® PRO stack to ensure profile interoperability. Commissioning devices into networks has been made more consistent through this specification.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-02

Zigbee Document 05-3474-22 - Zigbee Specification

🔗 URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: This document contains specifications, interface descriptions, object descriptions, protocols and algorithms pertaining to the ZigBee® protocol standard. ZigBee® technology uses the globally available, license-free 2,4 GHz frequency band. It enables wireless applications using a standardized set of high-level communication protocols sitting atop low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-04

Zigbee Document 075123 - Cluster Library Specification

🔗 URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: The ZigBee® Cluster Library specification (ZCL) defines cluster functionality as a common platform for developers of ZigBee® applications as well as its data model. This is needed to create ZigBee® devices that are inter-operable at the application level.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-12

ietf RFC 7388 Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

 **URL:** <https://datatracker.ietf.org/doc/rfc7388/>

ABSTRACT: This document defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for managing IPv6 over

Low-Power Wireless Personal Area Networks (6LoWPANs).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2010-10

ietf RFC 7973 Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation

 **URL:** <https://datatracker.ietf.org/doc/rfc7973/>

ABSTRACT: When carried over Layer 2 technologies such as Ethernet, IPv6 datagrams using Low-Power Wireless Personal Area Network (LoWPAN) encapsulation as defined in RFC 4944 must be identified so the receiver can correctly interpret the encoded IPv6 datagram. The IETF officially requested the assignment of an Ethertype for that purpose and this document reports that assignment.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-11

ietf RFC 8025 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch

 **URL:** <https://datatracker.ietf.org/doc/rfc8025/>

ABSTRACT: This specification updates RFC 4944 to introduce a new context switch mechanism for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) compression, expressed in terms of Pages and signaled by a new Paging Dispatch.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-11

ietf RFC 8036 Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc8036/>

ABSTRACT: This document discusses the applicability of the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-01

IETF RFC 8065 Privacy Considerations for IPv6 Adaptation-Layer Mechanisms

 **URL:** <https://datatracker.ietf.org/doc/rfc8065/>

ABSTRACT: This document discusses how a number of privacy threats apply to technologies designed for IPv6 over various link-layer protocols, and it provides advice to protocol designers on how to address such threats in adaptation-layer specifications for IPv6 over such links.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2017-02

IETF 8066 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines

 **URL:** <https://datatracker.ietf.org/doc/rfc8066/>

ABSTRACT: RFC 4944 defines the ESC dispatch type to allow additional dispatch octets in the 6LoWPAN header. The value of the ESC dispatch type was updated by RFC 6282; however, its usage was not defined in either RFC 6282 or RFC 4944. This document updates RFC 4944 and RFC 6282 by defining the ESC extension octet code points and listing registration entries for known use cases at the time of writing of this document.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-02

IETF RFC 8075 Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8075/>

ABSTRACT: This document provides reference information for implementing a cross-protocol network proxy that performs translation from the HTTP protocol to the Constrained Application Protocol (CoAP). This will enable an HTTP client to access resources on a CoAP server through the proxy. This document describes how an HTTP request is mapped to a CoAP request and how a CoAP response is mapped back to an HTTP response. This includes guidelines for status code, URI, and media type mappings, as well as additional interworking advice.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-02

IETF RFC 8105 Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)

 **URL:** <https://datatracker.ietf.org/doc/rfc8105/>

ABSTRACT: This document describes how IPv6 is transported over DECT ULE using IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-05

IETF RFC 8132 PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8132/>

ABSTRACT: This specification defines the new CoAP methods, FETCH, PATCH, and iPATCH, which are used to access and update parts of a resource.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-04

IETF RFC 8138 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header

 **URL:** <https://datatracker.ietf.org/doc/rfc8138/>

ABSTRACT: This specification introduces a new IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) dispatch type for use in 6LoWPAN route-over topologies, which initially covers the needs of Routing Protocol for Low-Power and Lossy Networks (RPL) data packet compression (RFC 6550). Using this dispatch type, this specification defines a method to compress the RPL Option (RFC 6553) information and Routing Header type 3 (RFC 6554), an efficient IP-in-IP technique, and is extensible for more applications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-04

IETF RFC 8163 Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc8163/>

ABSTRACT: Master-Slave/Token-Passing (MS/TP) is a medium access control method for the RS-485 physical layer and is used primarily in building automation networks. This specification defines the frame format for transmission of IPv6 packets and the method of forming link-local and statelessly autoconfigured IPv6 addresses on MS/TP networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-05

IETF RFC 8180 Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration

 **URL:** <https://datatracker.ietf.org/doc/rfc8180/>

ABSTRACT: This document describes a minimal mode of operation for an IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) network. This minimal mode of operation specifies the baseline set of protocols that need to be supported and the recommended configurations and modes of operation sufficient to enable a 6TiSCH functional network. 6TiSCH provides IPv6 connectivity over a Time-Slotted Channel Hopping (TSCH) mesh composed of IEEE Std 802.15.4 TSCH links. This minimal mode uses a collection of protocols with the respective configurations, including the IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) framework, enabling interoperable IPv6 connectivity over IEEE Std 802.15.4 TSCH. This minimal configuration provides the necessary bandwidth for network and security bootstrapping and defines the proper link between the IETF protocols that interface to IEEE Std 802.15.4 TSCH. This minimal mode of operation should be implemented by all 6TiSCH-compliant devices.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2017-05

IETF RFC 8323 CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets

 **URL:** <https://datatracker.ietf.org/doc/rfc8323/>

ABSTRACT: This document outlines the changes required to use CoAP over TCP, TLS, and WebSockets transports. It also formally updates RFC 7641 for use with these transports and RFC 7959 to enable the use of larger messages over a reliable transport.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-02

IETF RFC 8368 Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)

 **URL:** <https://datatracker.ietf.org/doc/rfc8368/>

ABSTRACT: This document describes how to integrate OAM processes with an autonomic control plane in order to provide stable and secure connectivity for those OAM processes.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-05

IETF RFC 8376 Low-Power Wide Area Network (LPWAN) Overview

 **URL:** <https://datatracker.ietf.org/doc/rfc8376/>

ABSTRACT: This memo is an informational overview of the set of LPWAN technologies being considered in the IETF and of the gaps that exist between the needs of those technologies and the goal of running IP in LPWANs.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-05

IETF RFC 8392 CBOR Web Token (CWT)

 **URL:** <https://datatracker.ietf.org/doc/rfc8392/>

ABSTRACT: CBOR Web Token (CWT) is a compact means of representing claims to be transferred between two parties. The claims in a CWT are encoded in the Concise Binary Object Representation (CBOR), and CBOR Object Signing and Encryption (COSE) is used for added application-layer security protection. A claim is a piece of information asserted about a subject and is represented as a name/value pair consisting of a claim name and a claim value. CWT is derived from JSON Web Token (JWT) but uses CBOR rather than JSON.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-05

IETF 8480 6TiSCH Operation Sublayer (6top) Protocol (6P)

 **URL:** <https://datatracker.ietf.org/doc/rfc8480/>

ABSTRACT: This document defines the "IPv6 over the TSCH mode of IEEE 802.15.4e" (6TiSCH) Operation Sublayer (6top) Protocol (6P), which enables distributed scheduling in 6TiSCH networks. 6P allows neighbor nodes to add/delete Time-Slotted Channel Hopping (TSCH) cells to/on one another. 6P is part of the 6TiSCH Operation Sublayer (6top), the layer just above the IEEE Std 802.15.4 TSCH

Medium Access Control layer. 6top is composed of one or more Scheduling Functions (SFs) and the 6top Protocol defined in this document. A 6top SF decides when to add/delete cells, and it triggers 6P Transactions. The definition of SFs is out of scope for this document; however, this document provides the requirements for an SF.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-11

IETF RFC 8505 Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery

🔗 URL: <https://datatracker.ietf.org/doc/rfc8505/>

ABSTRACT: This specification updates RFC 6775 -- the Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery specification -- to clarify the role of the protocol as a registration technique and simplify the registration operation in 6LoWPAN routers, as well as to provide enhancements to the registration capabilities and mobility detection for different network topologies, including the Routing Registrars performing routing for host routes and/or proxy Neighbor Discovery in a low-power network.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-11

IETF RFC 8516 “Too Many Requests” Response Code for the Constrained Application Protocol

🔗 URL: <https://datatracker.ietf.org/doc/rfc8516/>

ABSTRACT: This document defines a new CoAP response code for a server to indicate that a client should reduce the rate of requests.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-01

IETF RFC 8557 Deterministic Networking Problem statement

🔗 URL: <https://datatracker.ietf.org/doc/rfc8557/>

ABSTRACT: This paper documents the needs in various industries to establish multi-hop paths for characterized flows with deterministic properties.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-05

IETF RFC 8710 Multipart Content-Format for the Constrained Application Protocol (CoAP)

🔗 URL: <https://datatracker.ietf.org/doc/rfc8710/>

ABSTRACT: This memo defines application/multipart-core, an application- independent media type that can be used to combine representations of zero or more different media types (each with a Constrained Application Protocol (CoAP) Content-Format identifier) into a single representation, with minimal framing overhead.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-02

IETF RFC 8724 SCHC: Generic Framework for Static Context Header Compression and Fragmentation

 **URL:** <https://datatracker.ietf.org/doc/rfc8724/>

ABSTRACT: This document defines the Static Context Header Compression and fragmentation (SCHC) framework, which provides both a header compression mechanism and an optional fragmentation mechanism.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-04

IETF RFC 8929 IPv6 Backbone Router

 **URL:** <https://datatracker.ietf.org/doc/rfc8929/>

ABSTRACT: This document updates RFCs 6775 and 8505 in order to enable proxy services for IPv6 Neighbor Discovery by Routing Registrars called “Backbone Routers”. Backbone Routers are placed along the wireless edge of a backbone and federate multiple wireless links to form a single Multi-Link Subnet (MLSN).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8992 Autonomic IPv6 Edge Prefix Management in Large-Scale Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc8992/>

ABSTRACT: This document defines two autonomic technical objectives for IPv6 prefix management at the edge of large-scale ISP networks, with an extension to support IPv4 prefixes.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-05

IETF RFC 9008 Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane

 **URL:** <https://datatracker.ietf.org/doc/rfc9008/>

ABSTRACT: This document looks at different data flows through Low-Power and Lossy Networks (LLN) where RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) is used to establish routing. The document enumerates the cases where RPL Packet Information (RPI) Option Type (RFC 6553), RPL Source Route Header (RFC 6554), and IPv6-in-IPv6 encapsulation are required in the data plane. This analysis provides the basis upon which to design efficient compression of these headers. This document updates RFC 6553 by adding a change to the RPI Option Type. Additionally, this document updates RFC 6550 by defining a flag in the DODAG Information Object (DIO) Configuration option to indicate this change and updates RFC 8138 as well to consider the new Option Type when the RPL Option is decompressed.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

IETF RFC 9011 Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN

 **URL:** <https://datatracker.ietf.org/doc/rfc9011/>

ABSTRACT: This document defines a profile of SCHC (RFC 8724) for use in LoRaWAN networks and provides elements such as efficient parameterization and modes of operation.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2021-04

IETF RFC 9016 Flow and Service Information Model for Deterministic Networking (DetNet)

 **URL:** <https://datatracker.ietf.org/doc/rfc9016/>

ABSTRACT: This document describes the flow and service information model for Deterministic Networking (DetNet). These models are defined for IP and MPLS DetNet data planes.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-03

IETF RFC 9019 A Firmware Update Architecture for Internet of Things

 **URL:** <https://datatracker.ietf.org/doc/rfc9019/>

ABSTRACT: This document provides the motivation for the standardization of a manifest format as a transport-agnostic means for describing and protecting firmware updates.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

IETF RFC 9024 Deterministic Networking (DetNet) Data Plane: IEEE 802.1 Time-Sensitive Networking over MPLS

 **URL:** <https://datatracker.ietf.org/doc/rfc9024/>

ABSTRACT: This document specifies the Deterministic Networking data plane when Time-Sensitive Networking (TSN) networks are interconnected over a DetNet MPLS network.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-06

IETF RFC 9025 Deterministic Networking (DetNet) Data Plane: MPLS over UDP/IP

 **URL:** <https://datatracker.ietf.org/doc/rfc9025/>

ABSTRACT: This document specifies the MPLS Deterministic Networking (DetNet) data plane operation and encapsulation over an IP network. The approach is based on the operation of MPLS-over-UDP technology.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

IETF RFC 9030 An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)

 **URL:** <https://datatracker.ietf.org/doc/rfc9030/>

ABSTRACT: This document describes a network architecture that provides low-latency, low-jitter, and high-reliability packet delivery. It combines a high-speed powered backbone and subnetworks using IEEE 802.15.4 time-slotted channel hopping (TSCH) to meet the requirements of low-power wireless deterministic applications.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-05

IETF RFC 9031 Constrained Join Protocol (CoJP) for 6TiSCH

 **URL:** <https://datatracker.ietf.org/doc/rfc9031/>

ABSTRACT: This document describes the minimal framework required for a new device, called a “pledge”, to securely join a 6TiSCH (IPv6 over the Time-Slotted Channel Hopping mode of IEEE 802.15.4) network. The framework requires that the pledge and the JRC (Join Registrar/Coordinator, a central entity), share a symmetric key. How this key is provisioned is out of scope of this document. Through a single CoAP (Constrained Application Protocol) request-response exchange secured by OSCORE (Object Security for Constrained RESTful Environments), the pledge requests admission into the network, and the JRC configures it with link-layer keying material and other parameters. The JRC may at any time update the parameters through another request-response exchange secured by OSCORE. This specification defines the Constrained Join Protocol and its CBOR (Concise Binary Object Representation) data structures, and it describes how to configure the rest of the 6TiSCH communication stack for this join process to occur in a secure manner. Additional security mechanisms may be added on top of this minimal framework.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IETF RFC 9032 Encapsulation of 6TiSCH Join and Enrollment Information Elements

 **URL:** <https://datatracker.ietf.org/doc/rfc9032/>

ABSTRACT: In the Time-Slotted Channel Hopping (TSCH) mode of IEEE Std 802.15.4, opportunities for broadcasts are limited to specific times and specific channels. Routers in a TSCH network transmit Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which additional information critical for new nodes (pledges) and long-sleeping nodes may be carried within the EB in order to conserve use of broadcast opportunities.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IETF RFC 9033 6TiSCH Minimal Scheduling Function (MSF)

 **URL:** <https://datatracker.ietf.org/doc/rfc9033/>

ABSTRACT: This specification defines the “IPv6 over the TSCH mode of IEEE 802.15.4” (6TiSCH) Minimal Scheduling Function (MSF). This Scheduling Function describes both the behavior of a node when joining the network and how the communication schedule is managed in a distributed fashion. MSF is built upon the 6TiSCH Operation Sublayer Protocol (6P) and the minimal security framework for 6TiSCH.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IETF RFC 9034 Packet Delivery Deadline Time in the Routing Header for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

 **URL:** <https://datatracker.ietf.org/doc/rfc9034/>

ABSTRACT: This document specifies a new type for the 6LoWPAN routing header containing the deadline time for data packets, designed for use over constrained networks. The deadline time enables forwarding and scheduling decisions for time-critical machine-to-machine (M2M) applications running on Internet-enabled devices that operate within time-synchronized networks. This document also specifies a representation for the deadline time values in such networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-06

IETF RFC 9035 A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header

 **URL:** <https://datatracker.ietf.org/doc/rfc9035/>

ABSTRACT: This document updates RFC 8138 by defining a bit in the Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration option to indicate whether compression is used within the RPL Instance and to specify the behavior of nodes compliant with RFC 8138 when the bit is set and unset.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

IETF RFC 9037 Deterministic Networking (DetNet) Data Plane: MPLS over IEEE 802.1 Time-Sensitive Networking (TSN)

 **URL:** <https://datatracker.ietf.org/doc/rfc9037/>

ABSTRACT: This document specifies the Deterministic Networking (DetNet) MPLS data plane when operating over an IEEE 802.1 Time-Sensitive Networking (TSN) sub-network.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-06

IETF RFC 9039 Uniform Resource Names for Device Identifiers

 **URL:** <https://datatracker.ietf.org/doc/rfc9039/>

ABSTRACT: This document describes a new Uniform Resource Name (URN) namespace for hardware device identifiers. A general representation of device identity can be useful in many applications, such as in sensor data streams and storage or in equipment inventories. A URN-based representation can be passed along in applications that need the information.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-06

IETF RFC 9055 Deterministic Networking (DetNet) Security Considerations

 **URL:** <https://datatracker.ietf.org/doc/rfc9055/>

ABSTRACT: This document addresses DetNet-specific security considerations from the perspectives of both the DetNet system-level designer and component designer.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-06

IETF RFC 9056 Deterministic Networking (DetNet) Data Plane: IP over MPLS

 **URL:** <https://datatracker.ietf.org/doc/rfc9056/>

ABSTRACT: This document specifies the Deterministic Networking data plane when encapsulating IP over an MPLS packet-switched network.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-10

IETF RFC 9090 Concise Binary Object Representation (CBOR) Tags for Object Identifiers

 **URL:** <https://datatracker.ietf.org/doc/rfc9090/>

ABSTRACT: This document defines CBOR tags for object identifiers (OIDs) and is the reference document for the IANA registration of the CBOR tags so defined.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-07

IETF RFC 9123 Deterministic Networking (DetNet) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking (TSN)

 **URL:** <https://datatracker.ietf.org/doc/rfc9123/>

ABSTRACT: This document specifies the Deterministic Networking IP data plane when operating over a Time-Sensitive Networking (TSN) sub-network.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-06

IETF RFC 9159 IPv6 Mesh over BLUETOOTH(R) Low Energy Using the Internet Protocol Support Profile (IPSP)

 **URL:** <https://datatracker.ietf.org/doc/rfc9159/>

ABSTRACT: RFC 7668 describes the adaptation of IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques to enable IPv6 over Bluetooth Low Energy (Bluetooth LE) networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth LE links established by using the Bluetooth Internet Protocol Support Profile (IPSP). This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-12

IETF RFC 4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals

🔗 URL: <https://datatracker.ietf.org/doc/rfc4919/>

ABSTRACT: This document describes the assumptions, problem statement, and goals for transmitting IP over IEEE 802.15.4 networks. The set of goals enumerated in this document form an initial set only.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2007-08

IETF RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc4944/>

ABSTRACT: This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. Additional specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2007-09

IETF RFC 5548 Routing Requirements for Urban Low-Power and Lossy Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc5548/>

ABSTRACT: This documents aims to specify a set of IPv6 routing requirements reflecting these and further U-LLNs' tailored characteristics.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2009-05

IETF RFC 6206 The Trickle Algorithm

🔗 URL: <https://datatracker.ietf.org/doc/rfc6206/>

ABSTRACT: This document describes the Trickle algorithm and considerations in its use.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2011-03

IETF RFC 6282 Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc6282/>

ABSTRACT: This document updates RFC 4944, "Transmission of IPv6 Packets over IEEE 802.15.4

Networks". This document specifies an IPv6 header compression format for IPv6 packet delivery in Low Power Wireless Personal Area Networks (6LoWPANs). The compression format relies on shared context to allow compression of arbitrary prefixes. How the information is maintained in that shared context is out of scope. This document specifies compression of multicast addresses and a framework for compressing next headers. UDP header compression is specified within this framework.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2011-09

IETF RFC 6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc6550/>

ABSTRACT: This document specifies the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), which provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point as well as point-to-multipoint traffic from the central control point to the devices inside the LLN are supported. Support for point-to-point traffic is also available.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2012-03

IETF RFC 6551 Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc6551/>

ABSTRACT: This document specifies a set of link and node routing metrics and constraints suitable to LLNs to be used by the Routing Protocol for Low-Power and Lossy Networks (RPL).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2012-03

IETF RFC 6552 Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)

🔗 URL: <https://datatracker.ietf.org/doc/rfc6552/>

ABSTRACT: This document specifies a basic Objective Function that relies only on the objects that are defined in the RPL and does not use any protocol extensions.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2012-03

IETF RFC 6568 Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

🔗 URL: <https://datatracker.ietf.org/doc/rfc6568/>

ABSTRACT: This document investigates potential application scenarios and use cases for low-power wireless personal area networks (LoWPANs). This document provides dimensions of design space for LoWPAN applications. A list of use cases and market domains that may benefit and motivate the work currently done in the 6LoWPAN Working Group is provided with the characteristics of each dimension. A complete list of practical use cases is not the goal of this document.

IETF RFC 6606 Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing

URL: <https://datatracker.ietf.org/doc/rfc6606/>

ABSTRACT: This document provides the problem statement and design space for 6LoWPAN routing. It defines the routing requirements for 6LoWPANs, considering the low-power and other particular characteristics of the devices and links. The purpose of this document is not to recommend specific solutions but to provide general, layer-agnostic guidelines about the design of 6LoWPAN routing that can lead to further analysis and protocol design.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2012-05

IETF RFC 6690 Constrained RESTful Environments (CoRE) Link Format

URL: <https://datatracker.ietf.org/doc/rfc6690/>

ABSTRACT: This specification defines Web Linking using a link format for use by constrained web servers to describe hosted resources, their attributes, and other relationships between links. Based on the HTTP Link Header field defined in RFC 5988, the Constrained RESTful Environments (CoRE) Link Format is carried as a payload and is assigned an Internet media type. "RESTful" refers to the Representational State Transfer (REST) architecture. A well-known URI is defined as a default entry point for requesting the links hosted by a server.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2012-08

IETF RFC 6719 The Minimum Rank with Hysteresis Objective Function

URL: <https://datatracker.ietf.org/doc/rfc6719/>

ABSTRACT: This specification describes the Minimum Rank with Hysteresis Objective Function (MRHOF), an Objective Function that selects routes that minimize a metric, while using hysteresis to reduce churn in response to small metric changes. MRHOF works with additive metrics along a route, and the metrics it uses are determined by the metrics that the RPL Destination Information Object (DIO) messages advertise.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2012-09

IETF RFC 6775 Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

URL: <https://datatracker.ietf.org/doc/rfc6775/>

ABSTRACT: The IETF work in IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) defines 6LoWPANs such as IEEE 802.15.4. This and other similar link technologies have limited or no usage of multicast signaling due to energy conservation. In addition, the wireless network may not strictly follow the traditional concept of IP subnets and IP links. IPv6 Neighbor Discovery was not designed for non-transitive wireless links, as its reliance on the traditional IPv6 link concept and

its heavy use of multicast make it inefficient and sometimes impractical in a low-power and lossy network. This document describes simple optimizations to IPv6 Neighbor Discovery, its addressing mechanisms, and duplicate address detection for Low-power Wireless Personal Area Networks and similar networks. The document thus updates RFC 4944 to specify the use of the optimizations defined here.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2012-11

IETF RFC6997 Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks

🔗 URL: <https://datatracker.ietf.org/doc/rfc6997/>

ABSTRACT: This document specifies a point-to-point route discovery mechanism, complementary to the Routing Protocol for Low-power and Lossy Networks (RPL) core functionality. This mechanism allows an IPv6 router to discover “on demand” routes to one or more IPv6 routers in a Low-power and Lossy Network (LLN) such that the discovered routes meet specified metrics constraints.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2013-08

IETF RFC 6998 A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network

🔗 URL: <https://datatracker.ietf.org/doc/rfc6998/>

ABSTRACT: This document specifies a mechanism that enables a Routing Protocol for Low-power and Lossy Networks (RPL) router to measure the aggregated values of given routing metrics along an existing route towards another RPL router, thereby allowing the router to decide if it wants to initiate the discovery of a better route.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2013-08

IETF RFC 7252 The Constrained Application Protocol (CoAP)

🔗 URL: <https://datatracker.ietf.org/doc/rfc7252/>

ABSTRACT: The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. The nodes often have 8-bit microcontrollers with small amounts of ROM and RAM, while constrained networks such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) often have high packet error rates and a typical throughput of 10s of kbit/s. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2014-06

IETF RFC 7390 Group Communication for the Constrained Application Protocol (CoAP)

🔗 URL: <https://datatracker.ietf.org/doc/rfc7390/>

ABSTRACT: This specification defines how CoAP should be used in a group communication context. An approach for using CoAP on top of IP multicast is detailed based on existing CoAP functionality as well as new features introduced in this specification. Also, various use cases and corresponding protocol

flows are provided to illustrate important concepts. Finally, guidance is provided for deployment in various network topologies.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2014-10

IETF RFC 9009 Efficient Route Invalidation

 **URL:** <https://datatracker.ietf.org/doc/rfc9009/>

ABSTRACT: This document explains the problems associated with the use of No-Path Destination Advertisement Object (NPDAO) messaging in RFC 6550 and also discusses the requirements for an optimized route invalidation messaging scheme. Further, this document specifies a new proactive route invalidation message called the “Destination Cleanup Object” (DCO), which fulfills requirements for optimized route invalidation messaging.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: 2021-04

IETF RFC 9010 Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves

 **URL:** <https://datatracker.ietf.org/doc/rfc9010/>

ABSTRACT: This specification provides a mechanism for a host that implements a routing-agnostic interface based on IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery to obtain reachability services across a network that leverages RFC 6550 for its routing operations. It updates RFCs 6550, 6775, and 8505.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: 2021-04

(Updated) IRTF draft-irtf-t2trg-rest-iot Guidance on RESTful Design for Internet of Things Systems

 **URL:** <https://datatracker.ietf.org/doc/draft-irtf-t2trg-rest-iot/>

ABSTRACT: This document gives guidance for designing Internet of Things (IoT) systems that follow the principles of the Representational State Transfer (REST) architectural style. This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2024-07

IRTF RFC 8691 Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11

 **URL:** <https://datatracker.ietf.org/doc/rfc8691/>

ABSTRACT: This document provides methods and settings for using IPv6 to communicate among nodes within range of one another over a single IEEE 802.11-OCB link.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2019-12

ISO/IEC 20005:2013 Information technology - Sensor networks - Services and interfaces supporting collaborative information processing in intelligent sensor networks

 **URL:** <https://www.iso.org/standard/50952.html?browse=tc>

ABSTRACT: ISO/IEC 20005:2013 specifies services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks which includes:

CIP functionalities and CIP functional model, common services supporting CIP, common service interfaces to CIP.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2013-07

ITU-T G.9959 Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications

 **URL:** <https://www.itu.int/rec/T-REC-G.9959-201501-I/en>

ABSTRACT: Recommendation ITU-T G.9959 specifies the physical (PHY), medium access control (MAC), segmentation and reassembly (SAR), and logical link control (LLC) layers for short range narrow-band digital radiocommunication transceivers (TRXs). This Recommendation contains the non-radio (frequency) related aspects of the radiocommunication TRX. Sub 1 GHz TRXs claiming compliance with this specification shall also comply with Annex A of this Recommendation.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T Q.4060 (10/2018) The structure of the testing of heterogeneous Internet of things gateways in a laboratory environment

 **URL:** <https://handle.itu.int/11.1002/1000/13700>

ABSTRACT: This recommendation describes the testing methodology of the heterogeneous network gateway, which is to be used for communication among IoT devices. The tests will include the following, but not limited to: a) checking the gateway to verify stress load (benchmarking); b) checking the gateway to determine the possibility for the transmission of various types and sizes of frames and (or) packages; c) verifying joint conversions from different protocols and multiple interfaces; d) checking the gateway operation settings (CPU, RAM, etc.); and e) checking the network parameters (delay, data loss, etc.).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-10

ITU-T Y.4117 (10/2017) Requirements and capabilities of Internet of Things for support of wearable devices and related services

 **URL:** <https://handle.itu.int/11.1002/1000/13386>

ABSTRACT: The scope of this recommendation includes: a) description of characteristics of WD and WDS; b) specific requirements of the IoT for support of WD and WDS; c) specific capabilities of the IoT for support of WD and WDS; d) Information concerning use cases for WD and WDS.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-10

ITU-T Y.4411/Q.3052 (02/2016) Overview of application programming interfaces and protocols for M2M service layer

 **URL:** <https://handle.itu.int/11.1002/1000/12698>

ABSTRACT: This recommendation provides an overview of APIs and protocols for the M2M service layer and the related API and protocol requirements. It describes the component based M2M reference model, including the reference points of the M2M service layer. Then, APIs and protocols for M2M are introduced, including existing APIs and protocols for M2M service layer and M2M protocol structure and stacks. Finally, API and protocol requirements with respect to the M2M service layer are analysed.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-02

ITU-T Y.4418 (06/2018) Functional architecture of gateway for Internet of things applications

 **URL:** <https://handle.itu.int/11.1002/1000/13640>

ABSTRACT: This recommendation provides the gateway functional architecture for Internet of things (IoT) applications. The scope of this recommendation also includes: a) the gateway functional entities for IoT applications; b) the gateway reference points for IoT applications; c) typical logical flows.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-06

ITU-T Y.4451 (09/2016) Framework of constrained node networking in the IoT environments

 **URL:** <https://handle.itu.int/11.1002/1000/13026>

ABSTRACT: The scope of this recommendation includes the following items: a) An overview of constrained node device networking in the IoT environments; b) Communication of constrained node devices; c) Architectures of constrained node device networking; d) Functionalities of constrained node device networking.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2016-09

LAAS-CNRS Node-Red IDE-OM2M Node-Red IDE-OM2M V1.0.2: A framework for the rapid development of IoT applications using the OM2M platform through Node-RED

 **URL:** <https://www.npmjs.com/package/node-red-contrib-ide-iot>

ABSTRACT: The Internet of Things (IoT) has emerged strongly in recent years thanks to the proliferation of wireless communication devices and networks. It has spawned an explosion of new uses and services such as supply chain management, property and person monitoring, residential or business home automation, etc. However, several challenges must be overcome in order to develop IoT applications such as interoperability and interaction with and between different connected objects. In this paper, we propose a high-level Integrated Development Environment (IDE) that provides end-to-end solution for writing and deploying IoT applications. This IDE uses the Node-RED graphical environment to interact with the OM2M standard which serves as a middle-ware between our Node-RED module and the various heterogeneous devices. It also offers semantic support for an intuitive interaction with these devices.

DOCUMENT TYPE: Open_Source

PUBLICATION DATE: 2018-08

NGI-Ontochain ADOS (AirTrace Decentralized Oracle System)

URL: <https://ontochain.ngi.eu/content/ados>

ABSTRACT: An advanced AI-based oracle system for securing off-chain IoT data integrity when injecting in the blockchain ADOS offers the chance to B-IoT (Blockchain of IoT) practitioners to track and quantify data integrity before and after injecting into the Blockchain. This new dimension greatly improves reliability in the IoT data auditing process.

DOCUMENT TYPE: EU & National funded Open Source projects

PUBLICATION DATE: Under development

OASIS Advanced Message Queuing Protocol (AMQP) TC

URL: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp

ABSTRACT: The OASIS AMQP TC advances a vendor-neutral and platform-agnostic protocol that offers organizations an easier, more secure approach to passing real-time data streams and business transactions. The goal of AMQP is to ensure information is safely and efficiently transported between applications, among organizations, across distributed cloud computing environments, and within mobile infrastructures. AMQP avoids proprietary technologies, offering the potential to lower the cost of enterprise middleware software integrations through open interoperability. By enabling a commoditized, multi-vendor ecosystem, AMQP seeks to create opportunities for transforming the way business is done in the Cloud and over the Internet.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: N/A

OASIS Message Queuing Telemetry Transport (MQTT) TC

URL: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt

ABSTRACT: The OASIS MQTT TC is producing a standard for the Message Queuing Telemetry Transport Protocol compatible with MQTT V3.1, together with requirements for enhancements, documented usage examples, best practices, and guidance for use of MQTT topics with commonly available registry and discovery mechanisms. The standard supports bi-directional messaging to uniformly handle both signals and commands, deterministic message delivery, basic QoS levels, always/sometimes-connected scenarios, loose coupling, and scalability to support large numbers of devices. Candidates for enhancements include message priority and expiry, message payload typing, request/reply, and subscription expiry.

As an M2M/Internet of Things (IoT) connectivity protocol, MQTT is designed to support messaging transport from remote locations/devices involving small code footprints (e.g., 8-bit, 256KB ram controllers), low power, low bandwidth, high-cost connections, high latency, variable availability, and negotiated delivery guarantees. For example, MQTT is being used in sensors communicating to a broker via satellite links, SCADA, over occasional dial-up connections with healthcare providers (medical devices), and in a range of home automation and small device scenarios. MQTT is also ideal for mobile applications because of its small size, minimized data packets, and efficient distribution of information to one or many receivers (subscribers).

For more information on the MQTT TC, see the TC Charter.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: N/A

Updated) OMA-TS-REST_NetAPI_DeviceCapabilities-V1_0_1-20151123-A RESTful Network API for Device Capabilities

 **URL:** https://www.openmobilealliance.org/release/DevCapREST/V1_0_1-20151123-A/OMA-TS-REST_NetAPI_DeviceCapabilities-V1_0_1-20151123-A.pdf

ABSTRACT: This specification defines a RESTful Device Capabilities API using an HTTP protocol binding, based on the similar API defined in [3GPP 29.199-18].

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2015-11

ETSI TR 118 524 V2.0.0 3GPP Release 13 Interworking

 **URL:** https://www.etsi.org/deliver/etsi_tr/118500_118599/118524/02.00.00_60/tr_118524v020000p.pdf

ABSTRACT: The present document is a study of interworking between oneM2M Architecture and 3GPP Rel-13 architecture for Service Capability Exposure as defined in the release 13 version of ETSI TS 123 682 [i.5]. The key objective and value is analyzed and described. The document also investigates the potential solution in oneM2M by evaluating the existing technical solutions.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-09

oneM2M TS-0009-V4.4.0 HTTP Protocol Binding

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34550>

ABSTRACT: This document discussed HTTP Protocol Binding procedures.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2022-02

oneM2M TS-0020-V4.0.0 WebSocket Protocol Binding

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35387>

ABSTRACT: The present document specifies the binding of Mca and Mcc primitives onto the WebSocket binding. It specifies: a) Procedures and message formats for operating and closing of WebSocket connections; b) How request and response primitives are mapped into the payload of the WebSocket protocol.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2022-12

oneM2M-TR-0064 ZigBee Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32243>

ABSTRACT: This technical report investigates oneM2M and ZigBee interworking scenarios and proposes possible solutions to support the interworking scenarios.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2020-04

RIOT OS The friendly Operating System for the Internet of Things

 **URL:** <https://www.riot-os.org/>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2014-05

Manufacturing

IETF RFC 5673 Industrial Routing Requirements in Low-Power and Lossy Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc5673/>

ABSTRACT: The wide deployment of lower-cost wireless devices will significantly improve the productivity and safety of industrial plants while increasing the efficiency of plant workers by extending the information set available about the plant operations. The aim of this document is to analyze the functional requirements for a routing protocol used in industrial Low-power and Lossy Networks (LLNs) of field devices.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2009-10

Mobility

CEN EN ISO 14814:2006 Road transport and traffic telematics - Automatic vehicle and equipment identification - Reference architecture and terminology (ISO 14814:2006)

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:21173&cs=184DD778D0F4ED9BEEC2F72C92F3FFFB1

ABSTRACT: ISO 14814:2006 establishes a common framework to achieve unambiguous identification in ITS/RTTT (Intelligent Transport Systems/Road Transport and Traffic Telematics) AVI/AEI (Automatic Vehicle Identification/Automatic Equipment Identification) applications. This scheme and Reference Architecture Model is designed to be an “enabling” structure to allow interoperability between different commercial systems, and not prescriptive in determining any one system. It is not frequency- nor air interface protocol-specific, provides maximum interoperability, has a high population capability, and provides the possibility of upwards migration to more capable systems. ISO 14814:2006 provides a reference structure which enables an unambiguous identification and also identifies the data construct as an ITS/RTTT message. The construct also identifies which ITS/RTTT data structure is contained in the message.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2006-03

(Updated) CEN prEN 13757-8 Communication systems for meters - Part 8: Adaptation layer

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:73097&cs=1FA1D115B811F4639F7CC78EB38A0B513

ABSTRACT: This document describes the functionalities and specifies the requirements of an Adaptation Layer to be applied when transporting M-Bus upper layers using a wireless communication protocol other than Wireless M-Bus. These alternative radio technologies developed outside CEN/TC 294 could be based on Internet Protocol or not and operate either in licensed or unlicensed frequency bands.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-03

IEEE 802.11p IEEE 802.11p amendment for wireless access in vehicular environments (WAVE)

 **URL:** <https://ieeexplore.ieee.org/document/5514475>

ABSTRACT: Communications/Networking - DSRC is a U.S. Department of Transportation (DOT) project based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2010-07

ITU-T H.560 (12/2017) Communications interface between external applications and a Vehicle Gateway Platform

 **URL:** <https://handle.itu.int/11.1002/1000/13435>

ABSTRACT: This recommendation defines the requirements for vehicle gateway platform (VGP) services, VGP service functionalities and VGP management. The VGP service functions support service capabilities for applications running and data/message processing. The VGP service functionalities support core capabilities used by VGP services such as session management or in-vehicle resource access management. Finally, the VGP management supports functions for VGP configuration and monitoring such as security management.

This Recommendation also defines the network requirements for communication interfaces used between the defined VGP services and external applications. These external applications could be running over nomadic devices brought into the vehicle, roadside infrastructure, or cloud-based servers. Applications downloaded to one of the in-vehicle devices after the time of manufacture are also considered external applications since they may not be fully integrated into the driver-vehicle interface (DVI) and require a communications interface.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-12

SAE 6857 Requirements for a Terrestrial Based Positioning, Navigation, and Timing (PNT) System to Improve Navigation Solutions and Ensure Critical Infrastructure Security

 **URL:** <https://www.sae.org/standards/content/sae6857/>

ABSTRACT: This Recommended Practice defines the technical requirements for a terrestrial-based PNT system to improve vehicle (e.g., unmanned, aerial, ground, maritime) positioning/navigation

solutions and ensure critical infrastructure security, complementing GNSS technologies.

🔗 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-04

SAE J2735 ASN1 V2X Communications Message Set Dictionary™ ASN file

🔗 URL: https://www.sae.org/standards/content/j2735asn_202007/

ABSTRACT: This Abstract Syntax Notation (ASN.1) File is the precise source code used for SAE International Standard J2735. As part of an international treaty, all US ITS standards are expressed in “ASN.1 syntax”. ASN.1 Syntax is used to define the messages or “ASN specifications”. Using the ASN.1 specification, a compiler tool produces the ASN library which will then be used to produce encodings (The J2735 message set uses UPER encoding). The library is a set of many separate files that collectively implement the encoding and decoding of the standard. The library is then used by any application (along with the additional logic of that application) to manage the messages. The chosen ASN tool is used to produce a new copy of the library when changes are made, and it is then linked to the final application being developed. The ASN library manages many of the details associated with ASN syntax, allowing for subtle manipulation to make the best advantage of the encoding style.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-07

SAE J2735 V2X Communications Message Set Dictionary

🔗 URL: https://www.sae.org/standards/content/j2735_202007/

ABSTRACT: This SAE standard specifies a message set, and its data frames and data elements, for use by applications that use vehicle-to-everything (V2X) communications systems. While the data dictionary was originally designed for use over DSRC, this document is intended to be independent of the underlying communications protocols used to exchange data between participants in V2X applications.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-07

SAE J2945 Guidance Dedicated Short-Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts™

🔗 URL: https://www.sae.org/standards/content/j2945_201712/

ABSTRACT: This SAE Standard serves as the guidance document for the J2945/x family of standards. It contains cross-cutting material which applies to the other J2945/x standards, including recommended practice for the use of Systems Engineering (SE) and generic DSRC interface requirements content.

The scope for the DSRC system environment is to provide for the information exchange between a host vehicle and another DSRC enabled device, a device worn by or otherwise attached to a traveller, a roadside device, or a management centre, to address safety, mobility, and environmental system needs.

The audience for this document includes the technical teams of developers of the J2945/x documents and the implementers of the applications which are based on the J2945/x documents.

🔗 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-12

SAE J2945/2 Dedicated Short-Range Communications (DSRC) Performance Requirements for V2V Safety Awareness

 **URL:** https://www.sae.org/standards/content/j2945/2_201810/

ABSTRACT: This SAE Document specifies DSRC interface requirements for V2V Safety Awareness applications, including detailed Systems Engineering documentation (needs and requirements mapped to appropriate message exchanges). These applications include: Emergency Vehicle Alert, Roadside Alert, and Safety Awareness Alerts for Objects and Adverse Road Conditions. This document extends the V2V Communications capabilities defined in J2945/1 to support these applications, and the National ITS Architecture.

The purpose of this SAE Document is to enable interoperability for V2V Safety Awareness communications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-10

Water

ISO/IEC 30177 ED1 Internet of Things (IoT) - Underwater network management system (U-NMS) interworking

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104960

ABSTRACT: This document specifies the detailed description on interworking components in underwater network management system (U-NMS). It provides the intra-working of U-NMS components, interworking between U-NMS's terrestrial domain components and U-NMS's surface domain components, interworking between U-NMS's surface domain components and U-NMS's underwater domain components, and interworking in U-NMS's underwater domain components.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Home

IETF RFC5826 Home Automation Routing Requirements in Low-Power and Lossy Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc5826/>

ABSTRACT: This document presents requirements specific to home control and automation applications for Routing Over Low power and Lossy (ROLL) networks. In the near future, many homes will contain high numbers of wireless devices for a wide set of purposes. Examples include actuators (relay, light dimmer, heating valve), sensors (wall switch, water leak, blood pressure), and advanced controllers (radio-frequency-based AV remote control, central server for light and heat control). Because such devices only cover a limited radio range, routing is often required. The aim of this document is to specify the routing requirements for networks comprising such constrained devices in a home-control and automation environment.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2010-04

Buildings

IETF RFC5867 Building Automation Routing Requirements in Low-Power and Lossy Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc5867/>

ABSTRACT: The Routing Over Low-Power and Lossy (ROLL) networks Working Group has been chartered to work on routing solutions for Low-Power and Lossy Networks (LLNs) in various markets: industrial, commercial (building), home, and urban networks. Pursuant to this effort, this document defines the IPv6 routing requirements for building automation.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2010-06

Health

HL7 V2.9 HL7 Version 2 Messaging Standard

 **URL:** http://www.hl7.org/implement/standards/product_brief.cfm?product_id=516

ABSTRACT: Communications/Networking, Data and Information Management - Electronic data exchange between systems in the clinical domain. The standard is designed to support a central patient care system as well as a more distributed environment where data resides in departmental systems.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-12

■ Data_and_Architecture

Horizontals & Verticals

(NEW) 3GPP TS 23.434 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows; (release 19)

 **URL:** https://www.3gpp.org/ftp/Specs/archive/23_series/23_434/23434-j30.zip

ABSTRACT: This document specifies a functional architecture for service enabler architecture layer (SEAL) over 3GPP networks to support vertical applications (e.g. V2X applications). This functional architecture will include common application plane and signalling plane entities. A set of common services (e.g. group management, configuration management, location management) specified in this document can be shared across vertical applications.

The SEAL functional architecture takes into consideration the common capabilities to support mission critical and other vertical applications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-09

(NEW) 3GPP TS 23.433 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications (Release 19)

 **URL:** https://www.3gpp.org/ftp/Specs/archive/23_series/23.433/23433-j30.zip

ABSTRACT: With increasing demand of applications consumption over mobile networks, more and more application content is transmitted over the mobile networks. Vertical applications have diverse requirements for the application content distribution and delivery. To ease the various data delivery demands for vertical applications, a data delivery enabler is specified in this document.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-09

(NEW) AIOTI High Priority IoT Standardisation Gaps and Relevant SDOs Release 3.0

 **URL:** <https://aioti.eu/wp-content/uploads/2024/01/AIOTI-High-Priority-IoT-Gaps-R3-Final.pdf>

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

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

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-01

(NEW) AIOTI Guidance for the Integration of IoT and Edge Computing in Data Spaces

 **URL:**

 <https://aioti.eu/wp-content/uploads/2022/09/AIOTI-Guidance-for-IoT-Integration-in-Data-Spaces-Final.pdf>

ABSTRACT: This document provides an analysis on the integration of IoT and edge computing in data spaces. It explains the context, providing a definition of data spaces, enumerating challenges of data spaces, as well as the positioning of data spaces in the AIOTI high-level architecture (HLA) 1. It provides an architecture analysis of data spaces, covering:

- data space systems of interest from three perspectives: computing continuum, federation of systems, and data collecting / trading;
- stakeholders of data space systems;
- concerns and properties, general to data spaces, specific to cyber physical systems, to the integration of edge computing and processing, and to trustworthiness;
- building blocks to address concerns related to data governance, cyber physical systems and digital twins, trustworthiness support, interoperability support, infrastructure reconfiguration support, and data business marketplaces. It describes the relation to existing solutions:
- a construction approach relying on reference architecture standards and patterns:
- the use of reference architectures proposal from IDSA, oneM2M, ETSI MEC;
- the work carried out by a number of large-scale projects: PLATOON, INTERCONNECT, SmartBear, ASSIST-IoT. It provides recommendations for data space standards.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-09

(NEW) AIOTI Ontology Landscape Online

 **URL:** <https://aiotieu.github.io/ontologylandscape/>

ABSTRACT: Choosing the right ontologies is an important basis for successfully implementing semantic systems and achieving semantic interoperability between the systems. To make the choice of ontologies easier, the Semantic Interoperability Expert Group of the Alliance for Internet of Things Innovation (AIOTI) Working Group on Standardization has created an Ontology Landscape that currently includes 30 ontologies from different application areas of IoT. Browse catalogue here: <https://aiotieu.github.io/ontologylandscape/catalogue.html>

 **DOCUMENT TYPE:** Landscape

 **PUBLICATION DATE:** N/A

AIOTI Computing Continuum Scenarios, Requirements and Optical Communication enablers

 **URL:** <https://aioti.eu/wp-content/uploads/2022/04/AIOTI-Computing-Continuum-Final.pdf>

ABSTRACT: This report introduces Computing Continuum use cases, requirements and KPIs on communication infrastructures, IoT and edge computing platforms. Compared to many current activities the computing continuum enables a more flexible allocation of compute and communication resources and workload placement. Many novel applications require rather stringent KPIs since IoT is more and more mission critical. The new system requirements include strong security, very high bandwidth, very low delay, and very high reliability. Depending on the use case and deployment scenario, various technology enablers are currently under standardization, including the F5G optical network architecture, novel approaches to compute, and securing networking and compute.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-04

AIOTI High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0

 **URL:** <https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf>

ABSTRACT: This report introduces an approach for the definition and identification of key gaps in several initiatives. Based on the prioritisation of these gaps, the deliverable starts to address the work done within the relevant SDOs that need to cooperate in order to solve these gaps. The purpose of this document is to reflect a structured discussion within the AIOTI WG03 community and to provide consolidated technical elements as well as guidance and recommendations. The revision of this report has been started in October 2018. The objective of the present Version 2.0 is to continue the study of resolution of High Priority IoT Standardisation Gaps by relevant SDOs (main focus) and insert new gaps in the table when relevant contributions are approved by the AIOTI WG03 group.

 **DOCUMENT TYPE:** Gap analysis

 **PUBLICATION DATE:** 2020-01

(Updated) AIOTI IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges, Release 3.0

 **URL:** <https://aioti.eu/wp-content/uploads/2023/11/AIOTI-Report-IoT-and-Edge-impact-on-Beyond-5G-R3-Final.pdf>

ABSTRACT: This report highlights several IoT and Edge Computing vertical domain use cases collected by the Alliance for IoT and Edge Computing Innovation (AIOTI) and determines the specific requirements they impose on the underlying (Beyond) 5G network infrastructure. These use cases and

requirements can be used by Standards Developing Organizations (SDOs), such as 3GPP, ITU-T, ISO, and IEEE as requirements for automation in vertical domains focusing on critical communications. In addition to these use cases, emerging topics in the area of (Beyond) 5G technology are also introduced.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2023-11

AIOTI IoT High-Level Architecture (HLA) Release 5.0

📄 URL: https://aioti.eu/wp-content/uploads/2020/12/AIOTI_HLA_R5_201221_Published.pdf

ABSTRACT: In the context of the AIOTI WG Standardisation (AIOTI WG03) and by following the evolution on IoT Architectural aspects and available specifications, AIOTI WG Standardisation has developed a High Level Architecture (HLA) for IoT that should be applicable to AIOTI Large Scale Pilots. The HLA takes into account existing SDOs and alliances architecture specifications. This document is an integral part of a set of deliverables from AIOTI WG03 that also cover other aspects such as IoT landscape and Semantic Interoperability. AIOTIWG03 recommends that the HLA be the basis for further discussion with the Large Scale Pilot(LSP) and AIOTI WGs in order to promote architectural convergence with SDOs, alliances, consortia and other relevant parties.

📄 DOCUMENT TYPE: Framework

📅 PUBLICATION DATE: 2020-12

(Updated) AIOTI IoT LSP Standard Framework Concepts Release 3.0

📄 URL: <https://aioti.eu/wp-content/uploads/2023/01/AIOTI-SDOs-Alliance-Landscape-IoT-LSP-standards-framework-R3-Final.pdf>

ABSTRACT: The report introduces IoT Standards Developing Organisation (SDO), Alliance and Open Source Software (OSS) landscapes to be used as input for the recommendations for Large Scale Pilots (LSPs) standard framework and gap analysis. The LSPs can play an important role in investigating and solving specific challenges for the IoT industry and promoting innovation that is related to specific activities such as:

- 1) the applied standards framework,
- 2) deployments,
- 3) technological and business model validation and
- 4) acceptability.

The main objective of this deliverable is to briefly present the global dynamics and landscapes of IoT SDO, Alliance and OSS initiatives, which can be used:

- 1) to leverage on existing IoT standardization, industry promotion and implementation of standards and protocols,
- 2) as input for LSP standards framework and gap analysis and
- 3) to provide a guideline for the proponents of future project proposals associated with future IoT related calls financed by the EC on the positioning of these initiatives within these landscapes.

📄 DOCUMENT TYPE: Landscape

📅 PUBLICATION DATE: 2023-02

AIOTI Ontology Landscape

📄 URL: <https://aioti.eu/wp-content/uploads/2022/02/AIOTI-Ontology-Landscape-Report-R1-Published-1.0.1.pdf>

ABSTRACT: Choosing the right ontologies is an important basis for successfully implementing semantic systems and achieving semantic interoperability between the systems. To make the choice

of ontologies easier, the Semantic Interoperability Expert Group of the Alliance for Internet of Things Innovation (AIOTI) Working Group on Standardization has created an Ontology Landscape that currently includes 30 ontologies from different application areas of IoT. Apart from the application domain, the landscape visualizes how the ontology is maintained (by the colour used: single maintainer, organization, group of organizations/industry association or standardization organization).

📄 DOCUMENT TYPE: Landscape

📅 PUBLICATION DATE: 2021-12

AIOTI Semantic IoT Solutions - A Developer Perspective

🔗 URL: https://www.researchgate.net/publication/336679022_Semantic_IoT_Solutions_-_A_Developer_Perspective

ABSTRACT: This paper is co-authored by an informal group of experts from a broad range of backgrounds, all of whom are active in standards groups, consortia, alliances and/or research projects in the Internet of Things (IoT) space. The idea is to show how IoT systems can be built using semantic technologies, enabling semantic interoperability and thus allowing applications to reuse information originally provided for a specific application or IoT domain. The primary target audience is IoT developers that do not have a previous background in semantic technologies. The paper describes the different tasks and activities required when building semantic systems. The goal is to enable developers to build systems utilizing semantic technologies. It can be seen as one building block to achieve semantic interoperability in IoT and thus create the basis for a true Internet of Things.

📄 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2019-10

AIOTI Towards semantic interoperability standards based on ontologies

🔗 URL: https://www.researchgate.net/publication/336677616_Towards_Semantic_Interoperability_Standards_based_on_Ontologies

ABSTRACT: This paper is co-authored by an informal group of experts from a broad range of backgrounds, all of whom are active in standards groups, consortia, alliances and/or research projects in the Internet of Things (IoT) space. This paper has two objectives: 1) explain the need for semantic interoperability, 2) provide recommendations for semantic interoperability standards using ontologies. The target audience for this paper is a) IoT system product owners who need to understand how they can effectively ensure interoperability of their products; b) IoT system and standardization engineers without background in semantic technologies.

📄 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2019-10

bloTope project D2.7 V2.0 bloTope SoS Reference Platform Specification

🔗 URL: <https://storage.ning.com/topology/rest/1.0/file/get/35619929?profile=original>

ABSTRACT: This document provides the technical specifications of the bloTope SoS platform for IoT. A standard modelling language (UML) will be used to create and formalize the technical specifications, while considering key IoT reference architectures such as IoT-A (e.g., the IM and DM models).

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-03

CEN Wireless mesh networking - Communication systems for meter data exchange

 **URL:** <https://standards.iteh.ai/catalog/tc/cen/a0640f96-2f0c-4456-af8e-20887cd8b203/cen-tc-294-wg-6>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Database

 **PUBLICATION DATE:** N/A

(NEW) ETSI/oneM2M TR 118 518 V2.5.1 Industrial Domain Enablement

 **URL:** www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.05.01_60/tr_118518v020501p.pdf

ABSTRACT: Industrial domain is expected to be able to improve efficiency and flexibility by utilizing ICT technology: collecting data from devices in multiple factories, analyzing them, and applying the analysis results to decisions. So, it is desirable to utilize oneM2M standardized technology in the industrial domain. To better understand the special requirements to support the operations of the industrial environment, it is desirable to conduct studies on various functionalities that are keen to support this purpose so as to identify necessary technical works to enhance the future oneM2M specifications. This work item is intended to study such functionalities and the results of that study will be presented in a Technical Report.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-07

(Updated) ETSI TR 103 946 Methods for Testing and Specification (MTS); Security validation of IoT architecture application and conformity Case Study Experiences

 **URL:** https://www.etsi.org/deliver/etsi_tr/103900_103999/103946/01.01.01_60/tr_103946v010101p.pdf

ABSTRACT: The goal of the present document is to compile case study experiences related to the security validation and assurance for the integration and conformity of IoT applications with an existing IoT architecture in order to have a common understanding in MTS and related committees and to support trustworthiness. Industrial experiences may cover but are not restricted to the following domains: smart home, smart grid, unmanned air systems, automated driving.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-10

ETSI GR CIM 011 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)

 **URL:** https://www.etsi.org/deliver/etsi_gr/CIM/001_099/011/01.01.01_60/gr_CIM011v010101p.pdf

ABSTRACT: The present document is a choice of Test Purposes Description Language (TPDL), with the intention to capture all of the information required by the Test Template and should be parsable using software.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-04

ETSI GS CIM 016 Context Information Management (CIM); NGSI-LD Testing Framework: Test Template

 **URL:** https://www.etsi.org/deliver/etsi_gs/CIM/001_099/016/01.01.01_60/gs_CIM016v010101p.pdf

ABSTRACT: The Testing Framework (document format) specifies a testing framework defining a methodology for the development of the test strategies, test systems and resulting test specifications. The present document identifies the implementation under test (scope of the testing), the format for the test specification, the test architecture, the points of control and observation, the naming conventions (e.g. for test case ID and test case grouping ID), etc. It also provides the Implementation Conformance Statement which is basically a checklist for a client-owner so they know what parts of the specification will be tested and if any is optional. The ICS will be published as a separate GS.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

(Updated) ETSI TS 103 264 V3.2.1 SAREF: the Smart Applications REference ontology and oneM2M Mapping

 **URL:** https://www.etsi.org/deliver/etsi_ts/103200_103299/103264/03.02.01_60/ts_103264v030201p.pdf

ABSTRACT: The Smart Applications REference ontology (SAREF) is intended to enable interoperability between solutions from different providers and among various activity sectors in the Internet of Things (IoT), thus contributing to the development of the global digital market.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-01

ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions

 **URL:** http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

ABSTRACT: The scope of this document is a) to provide an overview of the IoT standards landscape: requirements, architecture, protocols, tests and related open source projects; b) to provide the roadmaps of the IoT standards, when they are available and to analyse the interactions of standards and open source in the context of IoT.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-10

ETSI TR 103 527 SmartM2M; Virtualized IoT Architectures with Cloud Back-ends

 **URL:** http://www.etsi.org/deliver/etsi_tr/103500_103599/103527/01.01.01_60/tr_103527v010101p.pdf

ABSTRACT: Scope: identification of new architectural elements (components, required mappings, etc.) that are required to address IoT on a cloud back-end. Description of use cases that benefit from virtualization.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-07

ETSI TR 103 528 SmartM2M; Landscape for open source and standards for cloud native software applicable for a Virtualized IoT service layer

 **URL:** http://www.etsi.org/deliver/etsi_tr/103500_103599/103528/01.01.01_60/tr_103528v010101p.pdf

ABSTRACT: provides a detailed description of open source projects, their key features and their level of maturity for the purpose of building a virtualized IoT service layer.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-08

ETSI TR 103 537 PlugtestsTM preparation on Semantic Interoperability

 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf

ABSTRACT: As part of its activities towards platforms interoperability, the document aims at preparing a PlugtestsTM event on Semantic Interoperability. For this PlugtestsTM event, the interoperability will be based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing, with the objective to demonstrate a more practical/industrial use. The document intends to identify the testing requirements from the semantic interoperability standards, especially those collected in ETSI TR 103 535 and ETSI TR 103 536.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-09

ETSI TR 103 778 SmartM2M; Use cases for cross-domain data usability of IoT devices

 **URL:** http://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf

ABSTRACT: The scope of this document is to a) identify, select and describe use cases where the IoT data and services require usability specifications; b) analyse the impact of these use cases for both machines and humans.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-12

ETSI TR 103 783 SmartM2M; SAREF: SDT interoperability and oneM2M base ontology alignment

 **URL:** https://www.etsi.org/deliver/etsi_tr/103700_103799/103783/01.01.01_60/tr_103783v010101p.pdf

ABSTRACT: The objective of this technical report is to assure full alignment of SAREF and the oneM2M base ontology and provide guidelines about how devices adopting the oneM2M SDT (Smart Device Template) informational model can interoperate seamlessly with oneM2M devices and systems adopting SAREF and vice versa.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-05

ETSI TR 118 503 V1.0.0 Architecture Part 2: Study for the merging of architectures proposed for consideration

 **URL:** https://2020.standict.eu/sites/default/files/tr_118503v010000p.pdf

ABSTRACT: The present document provides an evaluation of existing M2M-related Architecture work undertaken by the founding partners of oneM2M, including: the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) of Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) of the USA; the China Communications Standards Association (CCSA); the European Telecommunications Standards Institute (ETSI); and the Telecommunications Technology Association (TTA) of Korea. Common Functional Entities and Reference Points are identified, as well as critical differences. New functionality will not be considered as part of this study. The present document is intended to ensure a common understanding of existing M2M Architectural approaches, in order to facilitate future normative work resulting in oneM2M Technical Specifications. The present document has been prepared under the auspices of the oneM2M Technical Plenary, by the oneM2M Architecture Working Group.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2015-04

ETSI TS 103 267 SmartM2M; Smart Applications; Communication Framework

 **URL:** http://www.etsi.org/deliver/etsi_ts/103200_103299/103267/02.01.01_60/ts_103267v020101p.pdf

ABSTRACT: Alignment of the SAREF communication framework to oneM2M latest developments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-02

(Updated) ETSI TS 103 780 V1.1.1 SmartM2M; SAREF: oneM2M usage guidelines

 **URL:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103780/01.01.01_60/ts_103780v010101p.pdf

ABSTRACT: The objective of this standard is to provide guidelines for the usage of SAREF over oneM2M (also including the SDT interoperability) for vertical industry sectors.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-08

(Updated) ETSI TS 103 780 V1.1.1 SmartM2M; SAREF: oneM2M usage guidelines

 **URL:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103780/01.01.01_60/ts_103780v010101p.pdf

ABSTRACT: The objective of this standard is to provide guidelines for the usage of SAREF over oneM2M (also including the SDT interoperability) for vertical industry sectors.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-08

(NEW) ETSI TS 103 846 V1.1.1 SmartM2M; Digital Twins: Functionalities and communication Reference Architecture

 **URL:** http://www.etsi.org/deliver/etsi_ts/103800_103899/103846/01.01.01_60/ts_103846v010101p.pdf

ABSTRACT: With reference to the findings and analysis in DTR/SmartM2M-103844 (D1) and the standardized functionalities and requirements in DTS/SmartM2M-103845 (D2)

-  Definition of Digital Twins communication functionalities and properties,
-  Guidelines for the adoption of Digital Twins
-  Standardization of Digital Twins communication.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-08

(NEW) ETSI EN 303 760 V1.0

 **URL:** http://www.etsi.org/deliver/etsi_en/303700_303799/303760/01.01.00_20/en_303760v010100a.pdf

ABSTRACT: The relevance of the semantic work to assure semantic interoperability has driven the development of ontology specifications according to the SAREF methodology. IoT is currently experiencing a period of evolution and adoption in the different sectors, as a consequence the SAREF specifications are deemed to evolve quickly with the evolution of IoT solutions.

Therefore the SAREF Technical Specification suite is expected to evolve dynamically to timely accommodate new needs and contributions coming from all the interested stakeholders (from the same or from different domains). This requires the adoption of an effective SAREF methodology with the ability to point to the latest technical specifications.

This EN will specify the guidelines for the application of SAREF methodology in order to:

-  apply SAREF
-  extend SAREF
-  evolve SAREF

The document will make extensive use of references to the SAREF Technical Specification suite and to the SAREF Portal.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-06

(NEW) ETSI GS CIM 029 V1.1.1 Context Information Management (CIM); NGSI-LD Implementation Conformance Statement

 **URL:** http://www.etsi.org/deliver/etsi_gs/CIM/001_099/029/01.01.01_60/gs_CIM029v010101p.pdf

ABSTRACT: The relevance of the semantic work to assure semantic interoperability has driven the development of ontology specifications according to the SAREF methodology. IoT is currently experiencing a period of evolution and adoption in the different sectors, as a consequence the SAREF specifications are deemed to evolve quickly with the evolution of IoT solutions.

Therefore the SAREF Technical Specification suite is expected to evolve dynamically to timely accommodate new needs and contributions coming from all the interested stakeholders (from the same or from different domains). This requires the adoption of an effective SAREF methodology with the ability to point to the latest technical specifications.

This EN will specify the guidelines for the application of SAREF methodology in order to:

-  apply SAREF
-  extend SAREF
-  evolve SAREF

The document will make extensive use of references to the SAREF Technical Specification suite and to the SAREF Portal.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-04

(NEW) ETSI GS CIM 027 V1.1.1 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)

URL: http://www.etsi.org/deliver/etsi_gs/CIM/001_099/027/01.01.01_60/gs_CIM027v010101p.pdf

ABSTRACT: includes test purpose description language extracted from ETSI GS CIM 016.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-04

(NEW) ETSI TS 103 828 V1.1.1 SmartM2M; SAREF: Ontology Support for Urban Digital Twins and usage guidelines

URL: http://www.etsi.org/deliver/etsi_ts/103800_103899/103828/01.01.01_60/ts_103828v010101p.pdf

ABSTRACT: This deliverable will fill the priority gaps identified related to SAREF in DTR/ SmartM2M-103827 and will include guidelines about how to use SAREF in the context of Urban Digital Twins and with Digital Twins.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-03

(NEW) ETSI TS 103 845 V1.1.1 SmartM2M; Digital Twins Communication Requirements

URL: http://www.etsi.org/deliver/etsi_ts/103800_103899/103845/01.01.01_60/ts_103845v010101p.pdf

ABSTRACT: This deliverable will fill the priority gaps identified related to SAREF in DTR/ SmartM2M-103827 and will include guidelines about how to use SAREF in the context of Urban Digital Twins and with Digital Twins

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-02

(NEW) ETSI TR 103 827 V1.1.1 SmartM2M; SAREF: Digital Twins opportunities for the Ontology Context

URL: http://www.etsi.org/deliver/etsi_tr/103800_103899/103827/01.01.01_60/tr_103827v010101p.pdf

ABSTRACT: The present document defines security provisions for Smart Voice-Controlled Devices extending from the provisions for consumer IoT devices defined in ETSI EN 303 645 [1].

In terms of security concerns, Smart Voice-Controlled Device has a different focus than other generic IoT devices (e.g., distributed sensors, smart appliances, etc.). For example, Smart Voice-Controlled Devices mainly interact with users through voice assistants that can understand users' voice commands and assist users to control other devices in the IoT network. This feature actually expands the attack surface of Smart Voice-Controlled Devices. In addition, Smart Voice-Controlled Devices usually collect the user's voice and train a model uniquely suitable for the current user to provide personalized service. Therefore, Smart Voice-Controlled Devices-related privacy protection issues are particularly prominent. This vertical will focus on addressing the unique security issues of Smart Voice-Controlled Devices.

NOTE 1: Smart Voice-Controlled Devices in the context of this standard refers specifically to Smart Voice-Controlled Devices used in consumer environments, not those used in industrial environments. Smart Voice-Controlled Devices for industrial purpose is not in the scope of this document.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-09

(NEW) ETSI TR 103 781 V1.1.1 SmartM2M; Study for SAREF ontology patterns and usage guidelines

📄 URL: http://www.etsi.org/deliver/etsi_tr/103700_103799/103781/01.01.01_60/tr_103781v010101p.pdf

ABSTRACT: to report on the modularization and factorization potential of the TC SmartM2M suite using reference ontology patterns. The present document lists identified modelling discrepancies in SAREF extensions, along with proposals to homogenise the modelling. As a result, the present document describes a set of core ontology patterns and how they can be used as a basis for future normative work in TC SmartM2M

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-09

ETSI TR 118 502 V1.0.0 Architecture Part 1: Analysis of the architectures proposed for consideration

📄 URL: https://www.etsi.org/deliver/etsi_tr/118500_118599/118502/01.00.00_60/tr_118502v010000p.pdf

ABSTRACT: The present document provides an analysis and comparison of existing M2M-related Architecture work undertaken by the founding partners of oneM2M, including: the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) of Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) of the USA; the China Communications Standards Association (CCSA); the European Telecommunications Standards Institute (ETSI); and the Telecommunications Technology Association (TTA) of Korea. In addition, architectural work by other non-oneM2M Partner Type 1 organizations is provided for consideration. The present document is intended to ensure a common understanding of existing M2M Architectural approaches, in order to facilitate future normative work resulting in oneM2M Technical Specifications (TS). The present document has been prepared under the auspices of the oneM2M Technical Plenary, by the oneM2M Architecture Working Group.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2015-04

(NEW) IEEE 2668-2022 IEEE Standard for Maturity Index of the Internet of Things--Evaluation, Grading, and Ranking

📄 URL: <https://standards.ieee.org/ieee/2668/7254/>

ABSTRACT: The maturity index of Internet-of-things (IoT), referred to as IDex, is defined in this standard. The formats for 1) the IDex and 2) the IDex database and the IDex evaluation model database are specified. The general mechanism of the IDex evaluation is defined as pertinent to the applications and technical fields of the IoT objects to be evaluated. The IDex can be applied to IoT devices, networks, applications, algorithms, hardware, software, systems, and infrastructure. With slight modifications, the IDex can be extended to evaluate objects and infrastructure in various services, such as smart city services.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-12

(NEW) IEEE 1451.0-2024 IEEE Standard for a Smart Transducer Interface for Sensors and Actuators--Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats

 **URL:** <https://standards.ieee.org/ieee/1451.0/11001/>

ABSTRACT: The common functions, network services, transducer services, and Transducer Electronic Data Sheet (TEDS) formats for members of the IEEE 1451 family of standards to be interoperable in both network interface and transducer interface are provided. The common functions and characteristics that are to be performed by a network capable application processor (NCAP), which is a 1451 server, and all devices that implement the NCAP are defined. A set of network services that includes a set of commands and replies to access transducer data and TEDS data from the NCAP (1451 server) by the Internet of Things (IoT) applications (APPs) that are 1451 clients are also defined. Application programming interfaces (APIs) of network services are outlined to facilitate communications between the APPs (1451 clients) and NCAPs. Furthermore, the common functions and characteristics that are to be performed by a transducer interface module (TIM) and all devices that implement the TIM are discussed. A set of transducer services that includes a set of commands and replies to facilitate the setup and control of the TIM, as well as reading and writing the data used by the NCAP, are outlined. APIs of transducer services are also discussed to facilitate communications between the NCAPs and TIMs. Finally, the formats for a TEDS and methods to access the TEDS are specified, along with the common functions and characteristics that are to be performed by an APP and all devices that implement the APP. Additional Open Source content available here: <https://opensource.ieee.org/1451/1451.0-schema/>

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-06

(Updated) IEEE 1872.2-2021 IEEE Approved Draft Standard for Autonomous Robotics (AuR) Ontology

 **URL:** <https://standards.ieee.org/ieee/1872.2/7094/>

ABSTRACT: This standard extends IEEE 1872-2015 Standard for Ontologies for Robotics and Automation to represent additional domain-specific concepts, definitions, and axioms commonly used in Autonomous Robotics (AuR). This standard is general and can be used in many ways - for example, to specify the domain knowledge needed to unambiguously describe the design patterns of AuR systems, to represent AuR system architectures in a unified way, or as a guideline to build autonomous systems consisting of robots operating in various environments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-05

IEEE 754-2008 IEEE Standard for Floating-Point Arithmetic

 **URL:** <https://ieeexplore.ieee.org/document/4610935>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2008-08

(NEW) IEEE/ISO/IEC 42010-2022 IEEE/ISO/IEC International Standard for Software, systems and enterprise--Architecture description

 **URL:** <https://standards.ieee.org/ieee/42010/6846/>

ABSTRACT: This document specifies requirements for the structure and expression of an architecture description (AD) for various entities, including software, systems, enterprises, systems of systems, families of systems, products (goods or services), product lines, service lines, technologies and business domains. This document distinguishes the architecture of an entity of interest from an AD expressing that architecture. Architectures are not the subject of this document. This document specifies requirements for use of the architectural concepts and their relationships as captured in an AD. It does not specify requirements for any entity of interest or its environment. This document specifies requirements for an architecture description framework (ADF), an architecture description language (ADL), architecture viewpoints and model kinds in order to usefully support the development and use of an AD. This document specifies conformance to the requirements for an AD, ADF, ADL, architecture viewpoint and model kind. This document does not specify the processes, architecting methods, models, notations, techniques or tools by which an AD is created, utilized or managed. This document does not specify any format or media for recording an AD.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-11

IEC 60869-1:2018 Fibre optic interconnecting devices and passive components - Fibre optic passive power control devices - Part 1: Generic specification

 **URL:** <https://webstore.iec.ch/publication/60884>

ABSTRACT: IEC 60869-1:2018 is available as (<https://webstore.iec.ch/publication/64221>) IEC 60869-1:2018 RLV, which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 60869-1:2018 applies to fibre optic passive power control devices. These have all of the following general features:

-  they are passive in that they contain no optoelectronic or other transducing elements;
-  they have two ports for the transmission of optical power and control of the transmitted power in a fixed or variable fashion;
-  the ports are non-connectorized optical fibre pigtails, connectorized optical fibres or receptacles.
-  This document establishes generic requirements for the following passive optical devices:
 -  optical attenuator;
 -  optical fuse;
 -  optical power limiter.

This document also provides generic information including terminology for the IEC 61753-05x series. Published IEC 61753-05x series documents are listed in Bibliography

This fifth edition cancels and replaces the fourth edition published in 2012 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- a) the terms and definitions have been reviewed;
- b) the requirement concerning the IEC Quality Assessment System has been reviewed;
- c) the clause concerning quality assessment procedures has been deleted;
- d) Annex G, relating to technical information on variable optical attenuators, has been added.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-11

IEC 60875-1:2015 Fibre optic interconnecting devices and passive components - Non-wavelength-selective fibre optic branching devices - Part 1: Generic specification

 **URL:** <https://webstore.iec.ch/publication/22396>

ABSTRACT: IEC 60875-1:2015 applies to non-wavelength-selective fibre optic branching devices, all exhibiting the following features:

-  they are passive, in that they contain no optoelectronic or other transducing elements;
-  they have three or more ports for the entry and/or exit of optical power, and share optical power among these ports in a predetermined fashion;
-  the ports are optical fibres, or optical fibre connectors.
-  This standard establishes uniform requirements for the optical, mechanical and environmental properties. This sixth edition cancels and replaces the fifth edition published in 2010 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:
 -  removal of terms and definitions for splitter, coupler, symmetric non-wavelength-selective branching device, asymmetric non-wavelength-selective branching device;
 -  addition of terms and definitions for bidirectional non-wavelength-selective branching device and non-bidirectional non-wavelength-selective branching device, removal of assessment level.

Keywords: non-wavelength-selective fibre optic branching devices, uniform requirements for the optical, mechanical and environmental properties.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-05

IEC 61300-1:2022 Fibre optic interconnecting devices and passive components - Basic test and measurement procedures - Part 1: General and guidance

 **URL:** <https://webstore.iec.ch/publication/67663>

ABSTRACT: IEC 61300-1:2022 provides general information and guidance for the basic test and measurement procedures defined in IEC 61300-2 (all parts) and IEC 61300-3 (all parts) for interconnecting devices, passive components, mechanical splices, fusion splice protectors, fibre management systems and protective housings. This document is used in combination with the relevant specification which defines the tests to be used, the required degree of severity for each of them, their sequence, if relevant, and the permissible performance limits. In the event of conflict between this document and the relevant specification, the latter takes precedence. This fifth edition cancels and replaces the fourth edition published in 2016. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

-  addition of the information of measurement uncertainties in 4.2.1;
-  change of the requirements for attenuation variation in 4.2.2;
-  addition of the multimode launch conditions of other fibres than A1-OM2, A1-OM3, A1-OM4, A1-OM5 and A3e in 10.4;
-  addition of the multimode launch conditions of the planer waveguide in 10.6;
-  splitting Annex A for EF and Annex B for EAF;
-  correction of errors in the definitions of encircled flux and encircled angular flux.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-04

IEC 61753-1:2018 Fibre optic interconnecting devices and passive components - Performance standard - Part 1: General and guidance

 **URL:** <https://webstore.iec.ch/publication/67249>

ABSTRACT: IEC 61753-1:2018 provides guidance for the drafting of performance standards for all passive fibre optic products. This document defines the tests and severities which form the performance categories or general operating service environments and identifies those tests which are considered to be product specific. Test and severity details are given in Annex A. This second edition cancels and replaces the first edition published in 2007. It constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- a) definitions updated with new products: wall outlets, wall or pole mounted boxes, splices, ODF modules, street cabinets, hardened connectors and field mountable connectors;
- b) categories U and O are replaced by categories OP and OP+. No mandatory sequence in category OP+. Category OP+ contains the tests from category OP with the addition of only 4 other tests;
- c) addition of Category I (Industrial);
- d) temperature ranges added (with the HD suffix to the categories C, OP, OP+ and I) in case passive optical components are placed in a housing together with active electronics (HD stands for “heat dissipation”);
- e) the height of category A changed from 3 m to ground level (0 m);
- f) the lower level height of category G environment changed from ground level (0 m) to –1 m below ground level. Upper level remains at 3 m above ground level;
- g) addition of performance tests, test severities and performance criteria for new products: Wall outlet, wall or pole mounted boxes, mechanical splices, fusion splice protectors, ODF modules, street cabinets, field mountable connectors and hardened optical connectors;
- h) test severity of “Mating durability” test for connectors in categories C, OP, OP+ and I is reduced to 200 cycles for connectors with cylindrical ferrules and 50 cycles for connectors with rectangular ferrules;
- i) test severity of “Change of temperature” test for connectors and passive optical components in category I is reduced from 20 cycles to 12 cycles (harmonized with connectors and components from other categories);
- j) test severity of “Flexing of strain relief” test for connectors in categories C, OP and OP+ is reduced to 50 cycles;
- k) test severities of “Assembly and disassembly of fibre optic mechanical splices, fibre management systems and closures” test for all enclosures is reduced to 5 cycles;
- l) test severities of “Change of temperature” test for all protective housings in categories C, A, G and S is reduced from 20 cycles to 12 cycles (harmonized with connectors and components);
- m) test severities of “Resistance to solvents and contaminating fluids” test for closures in categories G and S changed – kerosene is removed, diesel oil exposure reduced to 1 h immersion and 24 h drying at room temperature;
- n) sealing performance criteria of sealed closures for categories G and A are reduced to 20 kPa overpressure.
- o) the change in attenuation criterion for connectors has changed from peak-to-peak into a +/- deviation from the original value of the transmitted power at the start of the test (harmonized with the change in attenuation criterion for components, splices and protective housings).

Keywords: performance standards for all passive fibre optic products.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-08-15

IEC 61754-4:2022 Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 4: Type SC connector family

 **URL:** <https://webstore.iec.ch/publication/29284>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-02

IEC 61754-7-3:2019 Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 7-3: Type MPO connector family - Two fibre rows 16 fibre wide

 **URL:** <https://webstore.iec.ch/publication/26692>

ABSTRACT: IEC 61754-7-3: 2019 defines the standard interface dimensions for type MPO family of connectors with two rows of 16 fibres.

Keywords: interface dimensions for type MPO connectors

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-04-05

IEC 61756-1:2019 Fibre optic interconnecting devices and passive components - Interface standard for fibre management systems - Part 1: General and guidance

 **URL:** <https://webstore.iec.ch/publication/59508>

ABSTRACT: IEC 61756-1:2019 covers general information on fibre management system interfaces. It includes the definitions and rules under which a fibre management system interface is created and it provides also criteria to identify the minimum bending radius for stored fibres. This document allows both single-mode and multimode fibre to be used. Liquid, gas or dust sealing requirements at the cable entry area or cable element ending are not covered in this document. This second edition cancels and replaces the first edition published in 2006. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

-  addition of figures to show the interface between protective housing and fibre management system;
-  addition of definitions for protective housing, closure, wall box, street cabinets and optical distribution frame modules;
-  addition of table with dimensions of fusion splice protectors and mechanical splices;
-  addition of method to identify the minimum bending radius for stored fibres;
-  addition of clause for other factors relevant to fibre management systems;
-  addition of annex A for example of calculating the minimum bending radius of stored fibres in a fibre management system.

Keywords: fibre management system interfaces, minimum bending radius for stored fibres

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-11

IEC 62005-1:2001 Reliability of fibre optic interconnecting devices and passive components - Part 1: Introductory guide and definitions

🔗 URL: <https://webstore.iec.ch/publication/6280>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2001-03

IEC 62099:2001 Fibre optic wavelength switches - Generic specification

🔗 URL: <https://webstore.iec.ch/publication/6459>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2001-03-30

IETF RFC 8610 Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures

🔗 URL: <https://datatracker.ietf.org/doc/rfc8610/>

ABSTRACT: This document proposes a notational convention to express Concise Binary Object Representation (CBOR) data structures (RFC 7049). Its main goal is to provide an easy and unambiguous way to express structures for protocol messages and data formats that use CBOR or JSON.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-06

IETF RFC 8655 Deterministic Networking Architecture

🔗 URL: <https://datatracker.ietf.org/doc/rfc8655/>

ABSTRACT: This document provides the overall architecture for Deterministic Networking (DetNet), which provides a capability to carry specified unicast or multicast data flows for real-time applications with extremely low data loss rates and bounded latency within a network domain

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-10

IETF RFC 8742 Concise Binary Object Representation (CBOR) Sequences

 **URL:** <https://datatracker.ietf.org/doc/rfc8742/>

ABSTRACT: his document describes the Concise Binary Object Representation (CBOR) Sequence format and associated media type “application/cbor-seq”. A CBOR Sequence consists of any number of encoded CBOR data items, simply concatenated in sequence.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-02

IETF RFC 8746 Concise Binary Object Representation (CBOR) Tags for Typed Arrays

 **URL:** <https://datatracker.ietf.org/doc/rfc8746/>

ABSTRACT: This document makes use of this extensibility to define a number of CBOR tags for typed arrays of numeric data, as well as additional tags for multi-dimensional and homogeneous arrays. It is intended as the reference document for the IANA registration of the CBOR tags defined.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-02

IETF RFC 8943 Concise Binary Object Representation (CBOR) Tags for Date

 **URL:** <https://datatracker.ietf.org/doc/rfc8943/>

ABSTRACT: This specification defines a CBOR tag for a date text string (as per RFC 3339) for applications needing a textual date representation within the Gregorian calendar without a time. It also defines a CBOR tag for days since the date 1970-01-01 in the Gregorian calendar for applications needing a numeric date representation without a time. This specification is the reference document for IANA registration of the CBOR tags defined.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8949 Concise Binary Object Representation (CBOR)

 **URL:** <https://datatracker.ietf.org/doc/rfc8949/>

ABSTRACT: This document obsoletes RFC 7049, providing editorial improvements, new details, and errata fixes while keeping full compatibility with the interchange format of RFC 7049. It does not create a new version of the format

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8964 Deterministic Networking (DetNet) Data Plane: MPLS

 **URL:** <https://datatracker.ietf.org/doc/rfc8964/>

ABSTRACT: This document specifies the Deterministic Networking (DetNet) data plane when operating over an MPLS Packet Switched Network.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-01

ISO/PAS 19450:2015 Automation systems and integration - Object-Process Methodology

🔗 URL: <https://www.iso.org/standard/84612.html?browse=tc>

ABSTRACT: ISO/PAS 19450:2015 specifies Object-Process Methodology (OPM) with detail sufficient for enabling practitioners to utilise the concepts, semantics, and syntax of Object-Process Methodology as a modelling paradigm and language for producing conceptual models at various extents of detail, and for enabling tool vendors to provide application modelling products to aid those practitioners.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-12

(Updated) IPSO IPSO Smart Object Guidelines

🔗 URL: <https://omaspecworks.org/develop-with-oma-specworks/ipsa-smart-objects/guidelines/>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2024-09

(Updated) IPSO Repo Public IPSO Repository

🔗 URL: <https://technical.openmobilealliance.org/OMNA/LwM2M/LwM2MRegistry.html>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2024-09

(NEW) ISO/IEC 30161-2:2023 Internet of Things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points

🔗 URL: <https://webstore.iec.ch/en/publication/68295>

ABSTRACT: ISO/IEC 30161-2:2023 specifies the following items for the transport interoperability between nodal points in the IoT data exchange platform (IoT DEP):

- 🔗 requirements;
- 🔗 functional blocks;
- 🔗 operation mechanism.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-03

ISO/IEC 21823-1:2019 Interoperability for internet of things systems -- Part 1: Framework

 **URL:** <https://webstore.iec.ch/publication/60604>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-02

ISO/IEC 21823-2:2020 Internet of Things (IoT) - Interoperability for IoT systems - Part 2 : Transport interoperability

 **URL:** <https://webstore.iec.ch/publication/61085>

ABSTRACT: ISO/IEC 21823-2:2020 (E) specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies: transport interoperability interfaces and requirements between IoT systems; transport interoperability interfaces and requirements within an IoT system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-04

ISO/IEC 21823-3:2021 Internet of Things (IoT) - Interoperability for IoT systems - Part 3: Semantic interoperability

 **URL:** <https://webstore.iec.ch/publication/61088>

ABSTRACT: ISO/IEC 21823-3:2021 provides the basic concepts for IoT systems semantic interoperability, as described in the facet model of ISO/IEC 21823-1, including: a) requirements of the core ontologies for semantic interoperability; b) best practices and guidance on how to use ontologies and to develop domain-specific applications, including the need to allow for extensibility and connection to external ontologies; c) cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies; d) relevant IoT ontologies along with comparative study of the characteristics and approaches in terms of modularity, extensibility, reusability, scalability, interoperability with upper ontologies, and so on, and e) use cases and service scenarios that exhibit necessities and requirements of semantic interoperability.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-02

ISO/IEC 21823-4:2022 Internet of Things (IoT) - Interoperability for IoT systems - Part 4: Syntactic interoperability

 **URL:** <https://webstore.iec.ch/publication/65649>

ABSTRACT: ISO/IEC 21823-4:2022 specifies the IoT interoperability from a syntactic point of view. In ISO/IEC 21823-1: Framework [2], five facets are described for IoT interoperability, i.e. transport, semantic, syntactic, behavioural and policy. In this document, the following specifications for IoT interoperability from syntactic viewpoint are included: a) a principle of how to achieve syntactic interoperability among IoT systems which include IoT devices; b) requirements on information related to IoT devices

for syntactic interoperability; and c) a framework for processes on developing information exchange rules related to IoT devices from the syntactic viewpoint.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-03

ISO/IEC 29182-1:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 1: General overview and requirements

🔗 URL: <https://webstore.iec.ch/publication/11411>

ABSTRACT: ISO/IEC 29182-1:2013 provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2013-06

ISO/IEC 29182-2:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 2: Vocabulary and terminology

🔗 URL: <https://webstore.iec.ch/publication/11412>

ABSTRACT: ISO/IEC 29182-2:2013 is intended to facilitate the development of International Standards in sensor networks. It presents terms and definitions for selected concepts relevant to the field of sensor networks. It establishes a general description of concepts in this field and identifies the relationships among those concepts. It may also be used as guidance for development of other parts of ISO/IEC 29182 and any other sensor network related standard.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2013-06

ISO/IEC 29182-3:2014 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 3: Reference architecture views

🔗 URL: <https://webstore.iec.ch/publication/11413>

ABSTRACT: ISO/IEC 29182-3:2014 provides Sensor Network Reference Architecture (SNRA) views. The architecture views include business, operational, systems, and technical perspectives, and these views are presented in functional, logical, and/or physical views where applicable. ISO/IEC 29182-3:2014 focuses on high-level architecture views which can be further developed by system developers and implementers for specific applications and services.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2014-02

ISO/IEC 29182-4:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 4: Entity models

 **URL:** <https://webstore.iec.ch/publication/11414>

ABSTRACT: The purpose of the ISO/IEC 29182 series is to a) - provide guidance to facilitate the design and development of sensor networks, b) improve interoperability of sensor networks, and c) make sensor network components plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/from an existing sensor network. ISO/IEC 29182-4 presents models for the entities that enable sensor network applications and services according to the Sensor Network Reference Architecture (SNRA).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2013-07

ISO/IEC 29182-5:2013 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 5: Interface definitions

 **URL:** <https://webstore.iec.ch/publication/11415>

ABSTRACT: ISO/IEC 29182-5:2013 provides the definitions and requirements of sensor network (SN) interfaces of the entities in the Sensor Network Reference Architecture and covers the following aspects: - interfaces between functional layers to provide service access for the modules in the upper layer to exchange messages with modules in the lower layer; - interfaces between entities introduced in the Sensor Network Reference Architecture enabling sensor network services and applications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2013-07

ISO/IEC 29182-5:2013 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 6: Applications

 **URL:** <https://webstore.iec.ch/publication/11416>

ABSTRACT: ISO/IEC 29182-6:2014, describes and provides - a compilation of sensor network applications for which International Standardized Profiles (ISPs) are needed, - guidelines for the structured description of sensor network applications, and - examples for structured sensor network applications. It does not cover ISPs for which drafting rules are described in ISO/IEC TR 10000. Due to the generic character of ISO/IEC 29182, fully developed ISPs will not be included in this International Standard.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-07

ISO/IEC 29182-7:2015 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 7: Interoperability guidelines

 **URL:** <https://webstore.iec.ch/publication/21827>

ABSTRACT: ISO/IEC 29182-7:2015 provides a general overview and guidelines for achieving interoperability between sensor network services and related entities in a heterogeneous sensor network.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-02

ISO/IEC 30101:2014 Information technology -- Sensor networks: Sensor network and its interfaces for smart grid system

 **URL:** <https://webstore.iec.ch/publication/11540>

ABSTRACT: ISO/IEC 30101:2014 is for sensor networks in order to support smart grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications, and associated environmental challenges. This International Standard characterizes the requirements for sensor networks to support the aforementioned applications and challenges. Data from sensors in smart grid systems is collected, transmitted, published, and acted upon to ensure efficient coordination of the various systems and subsystems. The intelligence derived through the sensor networks supports synchronization, monitoring and responding, command and control, data/information processing, security, information routing, and human-grid display/graphical interfaces. This International standard specifies: - interfaces between the sensor networks and other networks for smart grid system applications, - sensor network architecture to support smart grid systems, - interface between sensor networks with smart grid systems, and - sensor network based emerging applications and services to support smart grid systems.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-11

ISO/IEC 30128:2014 Information technology -- Sensor networks -- Generic Sensor Network Application Interface

 **URL:** <https://webstore.iec.ch/publication/11545>

ABSTRACT: ISO/IEC 30128:2014 specifies the interfaces between the application layers of service providers and sensor network gateways, which is Protocol A in interface 3, defined in ISO/IEC 29182-5. This International Standard covers: - description of generic sensor network applications' operational requirements, - description of sensor network capabilities, and - mandatory and optional interfaces between the application layers of service providers and sensor network gateways.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-11

(Updated) ISO/IEC 30141:2018 Internet of Things (IoT) - Reference Architecture

 **URL:** <https://webstore.iec.ch/publication/60606>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-08

ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

 **URL:** <https://webstore.iec.ch/publication/62644>

ABSTRACT: ISO/IEC 30147:2021(E) provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015.

The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-05

ISO/IEC 30161-1:2020 Internet of things (IoT) - Data exchange platform for IoT services - Part 1: General requirements and architecture

🔗 URL: <https://webstore.iec.ch/publication/63404>

ABSTRACT: ISO/IEC 30161-1:2020(E) specifies requirements for an Internet of Things (IoT) data exchange platform for various services in the technology areas of:

- 📄 the middleware components of communication networks allowing the co-existence of IoT services with legacy services;
- 📄 the end-points performance across the communication networks among the IoT and legacy services;
- 📄 the IoT specific functions and functionalities allowing the efficient deployment of IoT services;
- 📄 the IoT service communication networks' framework and infrastructure; and
- 📄 the IoT service implementation guideline for the IoT data exchange platform

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-11

(Updated) ISO/IEC 30161-2 Information technology — Internet of Things (IoT) — Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points

🔗 URL: <https://webstore.iec.ch/publication/67281>

ABSTRACT: This document specifies the following items for the transport interoperability between nodal points in the IoT data exchange platform (IoT DEP).

- 📄 Requirements
- 📄 Functional blocks
- 📄 Operation mechanism

When the number of connected IoT devices and IoT-users increase or the IoT system is deployed widely as a horizontal deployment, IoT devices and IoT-users are connected to each other through multiple nodal points. In ISO/IEC 30161-1, a nodal point is defined as a point for relaying IoT data according to the routing information decided by a communication protocol, and a communication entity in the IoT DEP network, which is any of an access network, a service network, or a user network. To provide data exchange among nodal points in an IoT system with small overheads or acquiring data with low latency, this document focuses on the transport interoperability for efficient transfer of IoT data among nodal points in an IoT system.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-06

ISO/IEC 30165:2021 Internet of things (IoT) - Real-time IoT framework

🔗 URL: <https://webstore.iec.ch/publication/63972>

ABSTRACT: ISO/IEC 30165:2021 specifies the framework of a real-time IoT (RT-IoT) system, including: a) RT-IoT system conceptual model based on domain-based IoT reference model defined in ISO/IEC 30141; b)

impacts of time-parameter in terms of four viewpoints (time, communication, control and computation).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-07

ISO/IEC 30178 ED1 Internet of Things (IoT) - Data format, value and coding

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104965

ABSTRACT: This document defines common formats, value, and coding for Internet of things (IoT).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

ISO/IEC 30181 ED1 Internet of Things (IoT) – Functional architecture for resource ID interoperability

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108552

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

ITU-T Study Group 20 ITU-T - SG20 - Internet of things (IoT) and smart cities and communities (SC&C)

🔗 URL: <https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx>

📄 ABSTRACT: SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end architectures for IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: N/A

ITU-T Y.4208 Internet of things requirements for support of edge computing

🔗 URL: <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14162>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-01

ITU-T Q.3952 (01/2018) The architecture and facilities of Model network for IoT testing

🔗 URL: <https://handle.itu.int/11.1002/1000/13489>

ABSTRACT: The testing of IoT technologies requires the specific model network which can simulate different scenarios of IoT implementations. This recommendation describes the architecture and facilities of Model Network for IoT testing.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-01

ITU-T Q.4062 (09/2020) Framework for IoT Testing

🔗 URL: <https://handle.itu.int/11.1002/1000/14387>

ABSTRACT: The main goal of this recommendation is the testing framework for Internet of Things definition. Conformity, interoperability and benchmarking testing frameworks for IoT are the recommendation scope.

📄 DOCUMENT TYPE: Framework

📅 PUBLICATION DATE: 2020-09

ITU-T Q.4063 (09/2020) Framework for testing identification systems used in Internet of things

🔗 URL: <https://handle.itu.int/11.1002/1000/14391>

ABSTRACT: The recommendation provides a description and test suites of identification procedures used in Internet of Things (IoT). There are a lot of applications of Internet of Things, the testing of their identity might be considered as a very important issue as it allows customer to ensure the authenticity of the IoT. The classification of IoT, in terms of testing of their identification procedures and the relevant testing approaches are subjects of this Recommendation.

📄 DOCUMENT TYPE: Framework

📅 PUBLICATION DATE: 2020-09

ITU-T Y.4001/F.748.2 (11/2015) Overview and reference model of machine socialization

🔗 URL: <https://handle.itu.int/11.1002/1000/12621>

ABSTRACT: This recommendation covers the following: a) overview of machine socialization; b) requirements for machine socialization; and c) reference models of machine socialization including service model, functional model and architectural model.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-11

ITU-T Y.4002/F.748.3 (11/2015) Relation management and descriptions for machine socialisations

 **URL:** <https://handle.itu.int/11.1002/1000/12622>

ABSTRACT: This recommendation covers the following: a) relation management models for machine socialization; b) relation descriptions for machine socialization; and c) use cases for relation management models.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-11

ITU-T Y.4100/Y.2066 (06/2014) Common requirements of Internet of Things

 **URL:** <https://handle.itu.int/11.1002/1000/12169>

ABSTRACT: This recommendation provides the common requirements of the Internet of things (IoT). These requirements are based on general use cases of the IoT and IoT actors, which are built from the definition of IoT contained in Recommendation ITU-T Y.2060. The common requirements of the IoT are independent of any specific application domain, which refer to the areas of knowledge or activity applied for one specific economic, commercial, social or administrative scope, such as transport application domain and health application domain. This recommendation builds on the overview of IoT (Recommendation ITU-T Y.2060), developing the common requirements based on general use cases of the IoT and the IoT actors and taking into account important areas of consideration from a requirement perspective. Some representative use cases of the IoT, which are abstracted from application domains, are also provided. The common requirements of the IoT specified in this Recommendation are classified into the categories of non-functional requirements, application support requirements, service requirements, communication requirements, device requirements, data management requirements and security and privacy protection requirements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2014-06

ITU-T Y.4101/Y.2067 Common requirements and capabilities of gateways for IoT applications

 **URL:** <https://handle.itu.int/11.1002/1000/13384>

ABSTRACT: This Recommendation provides the common requirements and capabilities of a gateway for Internet of things (IoT) applications. The common requirements and capabilities provided are intended to be generally applicable in gateway application scenarios.

The scope of this Recommendation includes:

-  general characteristics of a gateway for IoT applications;
-  common requirements of a gateway for IoT applications;
-  common capabilities of a gateway for IoT applications.
-  Use cases of a gateway for IoT applications are provided in appendices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-10

ITU-T Y.4102/Y.2074 (01/2015) Requirements for Internet of Things devices and operation of Internet of Things applications during disaster

 **URL:** <https://handle.itu.int/11.1002/1000/12421>

ABSTRACT: This recommendation provides requirements for IoT devices that can be used for operation of IoT applications in the context of disaster in addition to the common requirements of IoT [ITU-T Y.2066]. It also provides special requirements for operation of IoT applications during disaster. The scope of this Recommendation includes: a) requirements for IoT devices in the context of disaster; b) requirements for operation of IoT applications during disaster (for each of the three identified operating strategies). This Recommendation is relevant for IoT application developers and IoT service providers as well as for emergency service providers.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T Y.4111/Y.2076 (02/2016) Semantic related requirements and framework of the Internet of Things

URL: <https://handle.itu.int/11.1002/1000/12705>

ABSTRACT: This recommendation specifies semantic related requirements and framework of the Internet of Things (IoT). Taking into consideration the IoT reference model [ITU-T Y.2060], semantic requirements including those related to the four layers (i.e. Application layer, SSAS layer, Network layer and Device layer) and the management and security capabilities [ITU-T Y.2060], as well as semantic requirements across layers are specified. Based on the identified IoT semantic requirements and existing semantic related technologies, the IoT semantic framework is specified. The scope of this recommendation includes: a) Introduction to semantic related technologies; b) IoT semantic requirements; c) IoT semantic framework.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2016-02

ITU-T Y.4115 (04/2017) Reference architecture for IoT device capabilities exposure

 **URL:** <https://handle.itu.int/11.1002/1000/13266>

ABSTRACT: This recommendation specifies the reference architecture for IoT device capabilities exposure. The scope of this recommendation includes: a) the concept, general characteristics and requirements of IoT device capability exposure; b) the reference architecture for IoT device capability exposure including common procedures.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-04

ITU-T Y.4118 (06/2018) Internet of Things requirements and technical capabilities for support of accounting and charging

 **URL:** <https://handle.itu.int/11.1002/1000/13496>

ABSTRACT: This recommendation provides accounting and charging requirements for Internet of things (IoT). Building on the requirements and framework for accounting and charging capabilities in the next generation network (NGN) [ITU-T Y.2233], this Recommendation provides specific requirements derived from the analysis of business use cases specific to the IoT. Based on the identified requirements, an IoT accounting and charging technical capability framework is then specified. The

scope of this Recommendation includes: a) business use cases applied to the IoT; b) IoT accounting and charging requirements; c) IoT accounting and charging technical capability framework.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-06

ITU-T Y.4121 (06/2018) Requirements for an Internet of Things enabled network for support of applications for global processes of the Earth

🔗 URL: <https://handle.itu.int/11.1002/1000/13636>

ABSTRACT: This recommendation describes requirements of an Internet of things (IoT) enabled network for support of applications monitoring and studying global processes of the Earth. This concept of “Internet of things for monitoring and studying global processes (IoT GP)” combines geographically distributed IoT devices, and one or more control and management centres (CMCs) for the monitoring of global natural and man-made processes. This Recommendation describes key IoT GP features, deployment schemes of IoT GP devices, and requirements of the IoT GP network.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-06

ITU-T Y.4203 (02/2019) Requirements of things description in the Internet of things

🔗 URL: <https://handle.itu.int/11.1002/1000/13857>

ABSTRACT: The goal of this recommendation is to specify requirements for an effective way of representing things as far as possible in a homogeneous way. The focus of the document is on the following two concerns of things description: a) Representing physical things as virtual things to map the physical things into information world; b) Representing the relationship of virtual things to reflect the relationship of the represented physical things.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-02

ITU-T Y.4206 (06/2019) Requirements and capabilities of user-centric work space service

🔗 URL: <https://handle.itu.int/11.1002/1000/13919>

ABSTRACT: The objective of this recommendation is to identify requirements and capabilities of user-centric work space (UCS) service. In particular, the scope of this recommendation includes: a) Requirements of UCS service; b) Capability framework of UCS service; and c) Workflow of UCS service.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-06

ITU-T Y.4401/Y.2068 (03/2015) Functional framework and capabilities of the internet of things

🔗 URL: <https://handle.itu.int/11.1002/1000/12419>

ABSTRACT: This recommendation provides the functional framework and associated capabilities of Internet of Things (IoT), in particular components of the functional framework, their capabilities, and the relationships among these components. The recommendation also describes the relationships

between the IoT requirements specified in [ITU-T Y.l0T-common-reqts] and the capabilities specified in this Recommendation. Finally, the recommendation provides security considerations for the IoT functional framework.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-03

ITU-T Y.4412/F.747.8 (11/2015) Requirements and reference architecture for audience-selectable media service framework in the IoT environment

🔗 URL: <https://handle.itu.int/11.1002/1000/12620>

ABSTRACT: This recommendation defines requirements and reference architecture for audience-selectable media (ASM) service in the IoT environment. The scope of this recommendation includes: a) Concept of ASM service framework; b) - Requirements of ASM service framework; c) Reference architecture of ASM service framework; and, d) Functional entities of ASM service framework.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-11

ITU-T Y.4413/F.748.5 (11/2015) Requirements and reference architecture of M2M service layer

🔗 URL: <https://handle.itu.int/11.1002/1000/12623>

ABSTRACT: The objective of this recommendation is to identify requirements of the M2M service layer, which are common to all M2M verticals or specific to e-health application support, and to provide an architectural framework of the M2M service layer. In particular, the scope of this recommendation includes: a) Definition of the M2M service layer; b) Requirements of the M2M service layer; c) Architectural framework of the M2M service layer; d) Reference points of the M2M service layer.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-11

ITU-T Y.4415 (06/2018) Architecture of web of objects based virtual home network

🔗 URL: <https://handle.itu.int/11.1002/1000/13637>

ABSTRACT: This recommendation describes an architecture of a Web of Objects (WoO) based virtual home network (WVHN) by identifying the following: a) overview of WVHN; b) WVHN objects processing functions; c) WVHN service functions; d) security and trust support of WVHN.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-06

ITU-T Y.4416 Architecture of the Internet of Things based on next generation network evolution

🔗 URL: <https://handle.itu.int/11.1002/1000/13638>

ABSTRACT: This Recommendation describes an architecture of the Internet of things (IoT) based on extensions and enhancement to next generation network evolution (NGNe) functional entities, reference points and components as described in [ITU-T Y.2012], and other related Recommendations. The Recommendation takes into account the IoT reference model specified in [ITU-T Y.4000], the IoT

common requirements specified in [ITU-T Y.4100], and the IoT functional framework and capabilities specified in [ITU-T Y.4401].

The scope of this Recommendation includes:

- the extension to NGNe functional entities to support the IoT;
- the extension of NGNe reference points to support the IoT;
- the extension of NGNe components to support the IoT;
- the enhancement to NGNe capabilities to support the IoT.

Security of the extensions and enhancement specified in this Recommendation is also considered.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-06

ITU-T Y.4417 (06/2018) Framework of self-organization network in the IoT environments

🔗 URL: <https://handle.itu.int/11.1002/1000/13639>

ABSTRACT: The scope of this recommendation includes: a) concept of self-organization network in the Internet of Things (IoT) environments; b) characteristics of self-organization network in the IoT environments; c) requirements for self-organization networking in IoT; d) functional architecture for self-organization networking in IoT.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-06

ITU-T Y.4452 (09/2016) IoT application support models of the Internet of Things

🔗 URL: <https://handle.itu.int/11.1002/1000/13027>

ABSTRACT: This recommendation provides application support models of the Internet of Things (IoT). It includes the basis of IoT application support models; the configurable application support model, the adaptable application support model and the reliable application support model. The three application support models are described in functional view, implementation view and deployment view, in order to identify, respectively, the configurable capabilities, the adaptable capabilities and the reliable capabilities for support of IoT applications having some characteristic requirements.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-09

ITU-T Y.4453 Adaptive software framework for IoT devices

🔗 URL: <https://handle.itu.int/11.1002/1000/13028>

ABSTRACT: This Recommendation describes the high-level requirements and functional architecture of the adaptive software framework (ASF) for Internet of things (IoT) devices..

In particular, the scope of this Recommendation includes:

- an overview of the ASF,
- features and high-level requirements of the ASF: monitoring capability, policy decision capability and management capability;
- functional architecture of the ASF: application monitoring manager function, system information manager function and policy manager function.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-09

ITU-T Y.4553 Requirements of smartphone as sink node for IoT applications and services

 **URL:** <https://handle.itu.int/11.1002/1000/12779>

ABSTRACT: This Recommendation specifies the common requirements of using the smartphone as sink node for IoT applications and services, while the smartphone could provide the functions of both end-user terminal as well as the mobile gateway to connect the mobile network and the sensor network. More specifically, this recommendation covers the followings:

-  Concept of IoT sink node of the IoT
-  Sensing mode of the smartphone work as sink node for IoT applications and services
-  Requirements of using smartphone as sink node for IoT applications and services

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-03

ITU-T Y.4702 (03/2016) Common requirements and capabilities of device management in IoT

 **URL:** <https://handle.itu.int/11.1002/1000/12780>

ABSTRACT: This recommendation studies the requirements and capabilities of device management in IoT. The scope of this recommendation includes: a) the requirements of device management in IoT; b) the reference technical framework of device management in IoT; c) the capabilities of device management in IoT.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-03

ITU-T Y.4801/F.748.1 (10/2014) Requirements and common characteristics of IoT identifier for IoT service

 **URL:** <https://handle.itu.int/11.1002/1000/12229>

ABSTRACT: The objective of this Recommendation is to analyse identifiers in existing technologies and networks for IoT service, and describe the requirements of IoT identifier, common characteristics of IoT identifier, and the general architecture of IoT identifier.

This Recommendation describes the requirements and common characteristics of IoT identifier for IoT service. The scope of this Recommendation includes:

-  Analysis of identifiers in existing technologies and networks
-  Describe requirements of IoT identifier
-  Describe common characteristics of IoT identifier
-  Describe the general architecture of IoT identifier

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-10

(NEW) ITU-T Y.dtmv-if Interface model and its requirements of integrating virtual and physical worlds through digital twins for the metaverse

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19592

ABSTRACT: Noting the popularization of digital twin applications and metaverse services, the convergence of virtual and physical worlds through the use of digital twins within the metaverse is

emerging as a technical challenge. This challenge will be addressed by identifying service scenarios, defining relevant requirements, and specifying a reference model along with its functional entities that perform a set of functional roles involving data and information exchanges. Some data exchanges may involve digital twin-related actions, while others may occur with external systems or devices such as IoT devices, IoT gateways, application systems, management systems, and metaverse systems. This proposed interface model focuses specifically on data exchange associations among communication participants. It aims to ensure robust data and information flow between the metaverse's digital twin objects and external entities, enhancing system interoperability and service operability across various platforms, systems, and devices. The interface model will be developed to be protocol-agnostic from a functional perspective and independent of any particular interface technology.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU_T Y.dtmv-ref Reference model of integrating virtual and physical worlds through digital twins for the metaverse

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19591

ABSTRACT: The metaverse is a vast virtual space comprising numerous distinct virtual worlds, each with its unique purpose and characteristics. Within this diversity of virtual worlds, there exists a specific type of virtual world that incorporates digital twins. In such a virtual world, each digital twin serves as an interface bridging the gap between virtual and physical worlds, enabling bidirectional interaction between virtual objects and the corresponding counterparts. Through this bidirectional interaction facilitated by digital twins, information from physical objects can be transmitted to the corresponding virtual objects in the virtual world, resulting in synchronization between them. Manipulating virtual objects can lead to the control of physical objects. By analyzing service scenarios, requirements can be derived. Based on these derived requirements, it can develop a reference model for integration. This draft Recommendation defines a reference model of integrating virtual and physical worlds through digital twins for the metaverse.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU_T Y.dtmv-reqts Requirements of integrating virtual and physical worlds through digital twins for the metaverse

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19590

ABSTRACT: The metaverse is a vast virtual space comprising numerous distinct virtual worlds, each with its unique purpose and characteristics. Within this diversity of virtual worlds, there exists a specific type of virtual world that incorporates digital twins. In such a virtual world, each digital twin serves as an interface bridging the gap between virtual and physical worlds, enabling bidirectional interaction between virtual objects and the corresponding counterparts. Through this bidirectional interaction facilitated by digital twins, information from physical objects can be transmitted to the corresponding virtual objects in the virtual world, resulting in synchronization between them. Manipulating virtual objects can lead to the control of physical objects. This draft Recommendation explores the service scenarios and defines the requirements of integrating virtual and physical worlds through digital twins for the metaverse.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-APS-Reqts Requirements and capability framework of Internet of Things for support of application-aware service

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19605

ABSTRACT: The integration of new-generation information technologies such as the fifth-generation mobile communication network (IMT-2020) technologies, AI, big data, and cloud computing has greatly facilitated the development of IoT applications. The applications involved in the IoT verticals place differentiated and dynamic requirements for IoT capabilities. Application-aware service is a service to adapt IoT capabilities as appropriate based on the specific requirements of IoT applications applied in various scenarios. Application-aware service assists IoT in identifying the types, priorities and dynamic needs of applications, and dynamically adapting IoT capabilities in coordination with the network capabilities. At the same time, IoT applications can adjust their status according to the status of IoT resources. The service experience of IoT applications can be optimized through application-aware service. This Recommendation specifies the requirements and capability framework of Internet of Things for support of application-aware service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4496 (ex Y.RA-PHE) Requirements and reference architecture of smart service for public health emergency

 **URL:** http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17921

ABSTRACT: Recommendation ITU-T Y.4496 is intended to provide the requirements and architecture for a smart service for public health emergency system that can be implemented to address current and future potential public health risks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4501 (ex Y.RA-SDL) Functional architecture for smart door lock service framework

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17926

ABSTRACT: This Recommendation describes the functional architecture for the smart door lock (SDL) service framework. With the development of mobile communication technology and smart hardware, various technologies are introduced into the door lock to form the smart door lock. Multiple unlocking methods can be realized, and abnormal alarm reporting and flexible door lock management can be performed. In order to promote the deployment of the smart door lock (SDL) service around the world, a unified standard is needed to specify, and functions should be realized for the SDL service framework. The scope of this Recommendation includes the introduction of the SDL service framework, requirements of the SDL service framework and functional architecture of the SDL service framework.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) Y.4502 (ex Y.IoT-SQMS) Requirements and functional architecture of IoT sensing quality management service

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17937

ABSTRACT: Emerging technologies, such as artificial intelligence, crowdsourcing, etc, are enhancing

the sensing capabilities of IoT systems in recent years. IoT sensing quality management has become more complex. Consequently, sensing quality management service needs to be compatible with these emerging technologies in order to help in improving service quality of IoT systems. This Recommendation specifies the functions architecture of IoT sensing quality management service.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.4507 (ex Y.arc-psfws) A functional architecture of power supply facilities warning systems

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18746

ABSTRACT: The early warning system of power supply facilities based on the Internet of Things technology can obtain the real-time status parameters of power equipment and realize the equipment status prediction and fault early warning through the status assessment and early warning model. It can improve the operation economy of assets and ensure the reliability of power supply. It is necessary to put forward the warning system for power supply facilities. This Recommendation provides the functional architecture of power supply facilities warning system, use cases and data flows also are provided in this recommendation.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.DT-CS Requirements and functional architecture for blockchain-based sustainable and cooperative digital-twin creation system

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19611

ABSTRACT: Smart cities support human life by services that reference and analyse digital twins of surrounding environment, and that control actuators and systems including vehicles, traffic systems, lightings, air conditioners, etc. Digital twins provide the basis of control and, therefore, they need to reflect the up-to-date state of the object of interest. Numerous object exist in the real world, and taking their digital twins and maintaining the digital twins up to date requires massive effort due to the amount of the digital twin data. The creation and update of the digital twin data is likely to be performed by cooperation of many entities including municipalities, companies, other organizations, and even individuals by exploiting the concept of “sharing economy”. The contribution on digital twins made by those entities should be properly recorded to make the responsibility in contributed digital twins explicit and the digital twins correct. Also, incentive mechanism involving both givers and takers of the incentive is required to promote contribution. This Recommendation specifies the requirements and functional architecture for the infrastructure to create up-to-date digital twins by cooperation of many entities on the basis of blockchain technology.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-BoT-pee Capability and functional architecture of blockchain of things peers

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17936

ABSTRACT: Recommendation ITU-T Y.4464 “Framework of blockchain of things as decentralized service platform” introduces a decentralized Internet of things (IoT) service platform, blockchain of things (BoT), and provides its common capabilities and functionalities. A BoT entity is a functional entity or physical entity (e.g., IoT server, IoT device, IoT gateway and end user device) that participates in the activities performed in a BoT. A BoT peer is a logic function of a BoT entity to perform BoT-related

functionalities in processes of communications, consensus-making, transactions and management. BoT peers are participants of BoTs which create and maintain BoTs. This Recommendation presents common capabilities, functional architecture and general interactions of blockchain of things peers.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-CONV-fr Convergence framework for enhancement of service intelligence based on Internet of Things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17958

ABSTRACT: Internet of Things (IoT) has become a fundamental technology in service infrastructure, integrating with the other emerging ICTs to produce intelligent and autonomous solutions. This draft Recommendation describes "Convergence framework for enhancement of service intelligence based on Internet of Things". This document outlines a framework detailing how IoT can be integrated with technologies of AI (Artificial Intelligence), Cloud, Edge computing, Distributed Ledger Technology (DLT) and, Big data to enhance service intelligence.

📄 DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-MVarch Functional architecture of the IoT-based machine vision system

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19620

ABSTRACT: With the popularization and development of smart cities, intelligent agriculture and smart manufacturing, the connotation of the internet of things (IoT) is also expanding and is no longer limited to simple sensor data collection and discrimination. The IoT based machine vision will become one of the main development directions of the IoT which use cameras and cloud-network systems to capture the objects (including human being, vehicle, animal etc.) in real time and transmit them in the way of fusion networks and make analysis. The applications built based on the existing IoT architecture cannot perceive the cloud-network capabilities and resource distribution. Some applications are built in private network, the services unable to scale deployment, interconnectivity, and flexible expansion. The data unable to be fully utilized due to the capabilities of network and computing resource are not well managed in the IoT platform. This draft Technical Report analysis the functional architecture as well as functional entities and reference points for IoT based machine vision system.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-NCM-arch Functional architecture of network connectivity management in the Internet of things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18462

ABSTRACT: This Recommendation provides the functional architecture of network connectivity management in the Internet of things, including the functional entities, relevant reference points and logical flows.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup.IoT-CONV (ex YSTR.IoT-CONV) Overview of IoT Convergence

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17959

ABSTRACT: Internet of Things has become fundamental technology of service infrastructure with convergence with the other emerging ICT to produce intelligent and autonomous solution. At the beginning, IoT technology focuses on “something connected”. After connecting devices or sensors, ICT services obtain the useful information and have utilized it for accomplishing life convenience and increasing productivity. These days, Human being does not think of ‘connectivity’ is not a new technology anymore. Human being expects more convenient life style and accomplishes much more products and better services. Such expectations make it that IoT does not just remain technology of ‘connectivity’ itself but also developing and evolving into ‘intelligence’ and ‘autonomy’. In fact, there are a lot of things to be developed for future IoT. In IoT, intelligence and connectivity enable an entirely new set of product functions and capabilities, which can be grouped into four areas: monitoring, control, optimization, and autonomy. IoT can be categorized into three stages: 1st Stage: connectivity, 2nd Stage: intelligence, 3rd Stage: autonomy. The state of IoT technology remains at the beginning of 2nd stage for intelligence. Connectivity can be achieved with two or more devices only. However, the intelligence and autonomy of IoT require the other emerging technologies, such as AI, Cloud, Edge computing, DLT, Big Data and so on for convergence services. This new technical report is to provide a overview how IoT is merged with technologies of AI, Cloud, Edge computing, DLT and, (Big) data for enhancement of service intelligence.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4503 (ex Y.IoT-CRE-fr) Framework of common rule enablement for intelligent IoT services in heterogeneous IoT platform environments

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18466

ABSTRACT: The Internet of Things (IoT) brings a diverse range of devices to the network, which are managed by rule-enabled IoT platforms that react to events dynamically and automatically. However, the heterogeneity of the IoT networks makes it challenging to deploy consistent rule scenarios across multiple platforms due to differences in protocols and data formats. The IoT rule agent is a platform that implements the framework of common rule enablement. The agent is deployed in the proxy layer to bridge clients and devices in heterogeneous IoT networks. Between different IoT networks, the heterogeneity of the platforms is handled by the agent to deliver the corresponding format of rule profile to the destination platform through the platform-specific protocol. The agent includes the device proxies to enable the heterogeneous rule profiles to be a common format and registered through the rule registry for the further deployment process. For deploying the rules to the heterogeneous IoT platforms, the device proxies translate the common format to platform-specific style and deliver to the corresponding platforms. In the agent, each device proxy only considers the corresponding IoT network to perform translation and deployment. Based on the agent, the heterogeneous IoT platforms operate the common rule scenario although heterogeneous rules are delivered to the environment. This Recommendation specifies a framework of common rule enablement for intelligent IoT services in heterogeneous IoT platform environments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 29/08/2024

(NEW) ITU-T Y.4504 (ex Y.SF-prediction) Service framework of prediction for intelligent IoT

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18465

ABSTRACT: As the artificial intelligence (AI) technology develops and begins to be applied to various fields, enhanced internet of things (IoT) services using the AI technology are being developed. Machine

learning, the core of the AI technology, has been mostly researched in the direction of increasing the accuracy of inference. To apply the AI technology into real fields and to provide intelligent IoT services, the AI services must be operated at a level that can be provided to customers effectively. It is needed to study the technologies to efficiently provide the AI services by focusing on inference(prediction) rather than training(learning). This draft Recommendation describes the service framework in terms of prediction for intelligent IoT services by reflecting the development of the AI technology and the requirements from the market. To do this, this draft Recommendation introduces the concept of service framework of prediction for intelligent IoT and the requirements. And this draft Recommendations describes a functional architecture of service framework of prediction for intelligent IoT.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-08-29

(NEW) ITU-T Y.4508 (ex Y.DPM-alm-fra) Functional requirements and architecture of blockchain-based activity logs management for IoT data processing and management

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18467

ABSTRACT: There are many Internet of things (IoT) platforms to process and manage same IoT data in different stages and in different areas. In traditional solutions, each of the IoT platforms usually stores its activity logs for processing and managing IoT data (IoT DPM) into its storage separately. Those activity logs are separated and managed by the IoT platforms respectively. Therefore, the accessibility and trustworthiness of those activity logs are not guaranteed. In this case, it is uneasy to trace activities about IoT DPM in full lifecycle for the activity logs are stored and managed by different IoT platforms. In order to trace activities about IoT DPM, different IoT platforms may use same activity log storage and related functionalities. Activity logs management (ALM) enabled by blockchain technologies provides functionalities to manage activity logs for IoT DPM in full lifecycle across IoT platforms. Different IoT platforms can save activity logs of IoT DPM into the trustworthy shared storages via the ALM for IoT DPM individually. And then when they read activity logs of IoT DPM via the ALM, they can get all the relevant activity logs of IoT DPM in full lifecycle from the trustworthy shared storages via the ALM for IoT DPM, if authorized. The ALM and the trustworthy shared storages are based on blockchain technologies and can keep the activity logs un-tampered. The ALM can facilitate the IoT platforms to store and trace activity logs of IoT DPM in full lifecycle transparently and trustworthily. This Recommendation presents a blockchain-based activity logs management for IoT data processing and management, and specifies its characteristics, functional requirements and architecture.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 12/07/2024

(NEW) ITU-T Y.AIoT-dfs-arc Reference architecture of data fusion service in artificial intelligence of things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19626

ABSTRACT: Data fusion service (DFS) is a converged data service in artificial intelligence of things (AIoT), which merges, combines and integrates metadata (not raw data) from different data resources (such as IoT devices, IoT systems, databases, cloud data platforms) into a coherent form, and provides data processing and management (DPM) capabilities to data consumers (such as for machine learning model training). The DFS can be enhanced by knowledge database (such as relational, graph), artificial intelligence (AI) and machine learning (ML). The DFS dynamically collects metadata (not raw data) from different data resources and make intelligent data catalogs in real-time by using AI/ML and knowledge database, and provides smart data provision capability to allow data consumers in AIoT to access data with QoE/QoS and security assurance. The DFS supports smart data integration capability. By using the DFS, the data organizations and consumers don't need to integrate and bring raw data together from different data resources. The DFS can enable organizations in AIoT to unify their disparate data systems, improve data governance capability, provide intelligent data

accessibility and integration across multiple data platforms, and to enhance data collaboration within organizations. This draft new Recommendation specifies the data fusion service in artificial intelligence of things (AIoT), and provides relevant technical characteristics, functional requirements, reference architecture and capabilities of the data fusion service in AIoT.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.AIoT-fr Framework of Artificial Intelligence of Things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19624

ABSTRACT: The Artificial Intelligence of Things (AIoT) is the combination of artificial intelligence (AI) technologies with the Internet of Things (IoT) infrastructure to achieve more efficient IoT operations, improve human-machine interactions and enhance data management and analytics, but not limited to. From a comprehensive review of existing standardization efforts on AI and IoT, this draft Recommendation describes concepts, characteristics, technical features and approaches of AIoT. Then, it presents a conceptual model for AIoT.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.AIoT-FRA Functional requirements and architecture for Artificial Intelligence of Things

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19625

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.cii (ex Y.rrm-data) Requirements and reference model of data collected from city infrastructure

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17900

ABSTRACT: This Recommendation specifies requirements and reference model of IoT related data from city infrastructure. The scope of this recommendation includes: –Overview of IoT related data from city infrastructure –Requirements of IoT related data from city infrastructure –Reference model of IoT related data from city infrastructure All content related to data collection, storage, retrieval and delete covered in this document is recommended to be conducted in accordance with the laws and regulations of the country or region where the standard is used.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: under development

(NEW) ITU-T Y.DSE-LISF Reference architecture of data sharing and exchange based on lightweight intelligent software framework for Internet of things devices

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19630

ABSTRACT: Artificial intelligence has been growing rapidly through deep learning technology, and large amounts of training data are needed to create accurate learning models. To overcome this problem, it has become necessary to share and exchange not only training data but also the learning models (e.g., federated learning model). Additionally, federated learning may be used to collect data from multiple IoT devices and to share and collaborate a learning model with the assistance of a server via exchanging model parameters rather than directly sharing decentralized datasets, which can break data islands and meanwhile bring the advantage of data privacy protection and legal compliance. Nevertheless, the problem of cultural and social bias in the training data itself still needs to be resolved. This draft Recommendation specifies the data (i.e, sensing data, management data and learning model) sharing and exchange principles between a server/edge system and IoT devices equipped with the lightweight intelligent software framework (LISF) that supports Internet of things (IoT) applications requiring intelligent processing and enables such processing to work on resource-limited IoT devices. This draft also identifies general requirements and provides a functional architecture for the data sharing and exchange based on the LISF.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.Interop-DPM Integrated Interoperability framework for Data Processing and Management

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19633

ABSTRACT: SG20 has carried out a considerable amount of work on data interoperability from a technical point of view with many recommendations on different aspects of this topic. However, without a clear understanding of how to achieve semantic and operational interoperability the impact of the work may be limited. ITU has developed a foundational piece of work on this topic in FG-DPM. Other work has been done elsewhere, including the European Interoperability Framework for Smart Cities and Communities. This work would build on these to provide a framework for interoperability that sets technical interoperability alongside, for instance, semantic and operational interoperability. The U4SSC report “Redefining smart city platforms: Setting the stage for Minimal Interoperability Mechanisms” points out that: “Interoperability is one of the main challenges – and opportunities – in the development of smart sustainable cities and communities, using digital technologies to become more resilient, liveable and attractive for inhabitants and businesses. “The goal is to develop platforms that can allow key stakeholders, including governments, businesses, knowledge institutions and inhabitants, to communicate and work together across domains. The key to achieving this goal is in defining modular and scalable, multi-layered ICT solutions to enable cross-domain interoperability, moving beyond existing siloed solutions that address specific challenges such as improvement of traffic flows, surveillance, smart lighting, among others. The report goes on to say that: “It is also important to recognize that interoperability is not just related to digital technology. The GridWise Architecture Council’s eight-layer stack can help in understanding the context for determining interoperability requirements and defining exchanges of information. The Gridwise eight layer stack highlights that interoperability is needed, not simply to cover technical issues, but also semantic, operational and regulatory. This Recommendation would explore those aspects of interoperability that are not usually the focus of SG20 deliverables and would provide guidance as to how smart cities and communities could address the organisational and other barriers to interoperability of data.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.MIMbased-arch MIM-based Architectural framework for interoperability in support of data sharing ecosystems

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19634

ABSTRACT: Recommendation Y.MIM will be proposed for consent in the July 2024 SG20 plenary meeting. Once this is done, the next step would be to develop a minimal architectural framework that would strike a balance of precision in the technical specifications, neither over- nor under-specifying the requirements. The goals of a Y.MIM-based architecture framework for a digital ecosystem for cities and communities would be to ensure that the capabilities of interoperable data platforms take into account both the functional and the non-functional requirements needed to implement the minimal interoperability that cities and communities need to deliver a prosperous, sustainable, and inclusive future for their citizens. The fundamental perspective is that of the technical capabilities required for minimal data interoperability. This focus would background many implementation aspects, e.g., related to specific software and hardware stacks, and would allow great flexibility when it comes to adapting concrete deployment and integration to a local context. It would also be based on a realisation from current experiences that establishing data spaces on a minimal but sufficient common ground can be a catalyst to deliver mainstream trusted services for cities and communities in a connected world. The requirements for interoperable city data platforms would lead to specifications that ensure that the platforms are reliable, durable, future proof and efficient so that the city can build on the platforms and foster further innovations and evolution. These specifications would also ensure that the platforms can: extend to a 'system of systems' with all relevant digital means of a community, scale to the needs of the cities and communities; and guarantee privacy and security by design, making the platforms trustworthy. Open-source development and the involvement of communities are powerful methods in order to guarantee transparency and consequently trust in the platforms for public operators. This particular aspect will be particularly relevant when injecting algorithms based on AI mechanisms into the platforms. The implementation of minimal interoperability provides the common technical ground that cities and communities need to enable choice, flexibility, value for money and independence, through avoiding vendor lock-in. The architectural framework would support formal, de-facto and emerging standards, in order to ensure they are future-proof and stable. The trustworthiness and the interoperability of the platforms addresses the triple baseline of social, environmental, and economic benefits, and supports strategic aims such as the United Nations Sustainable Development Goals.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T YSTR.dscm Analysis of data sharing control models

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18468

ABSTRACT: With the continuous transformation and upgrading of digital economy, data sharing becomes the driving force and also bottleneck to further generate data value. It is crucial to ensure that data sharing among various stakeholders is secure and trustworthy in smart cities and communities. Representations of security and trustworthy factors and their enforcement are two main challenges in trusted data sharing. To address the aforementioned challenges, this technical report presents the life-cycle of data sharing. This technical report analyses data sharing control models regarding data transmission, data storage, data usage and data destruction, and illustrates use cases.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T YSTR.GenAI-Sem-Interop Implications of Generative Artificial Intelligence on Semantic Interoperability for Data Use

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19635

ABSTRACT: GenAI can be utilised for a broad range of technical and non-technical challenges smart cities and communities face. One aspect of particular importance in advancing their digital ecosystems is semantic interoperability. Making systems interoperable is key to reap the benefits of having digital

ecosystems in the first place, and the use of proprietary systems, outdated/non-conformant standards, and/or lack of technical expertise creates unnecessary challenges for smart cities and communities. Although large language model (LLM) output quality needs to be closely monitored, in particular for complex operations, GenAI offers an increasingly robust approach for improving semantic interoperability, helping to connect systems that are otherwise (partially) incompatible. When using LLMs in live cloud environments, i.e. to continuously transform/harmonise data, additional security implications need to be considered. This technical report aims at exploring how GenAI is already used to solve semantic interoperability challenges within smart cities and communities – and how reliable and secure existing solutions are; finding commonalities among existing solutions; and recommending normative work items to standardise GenAI usage for increasing interoperability across decentralised smart city and community data infrastructure, helping to process, manage, and share data across digital services such as digital twins and metaverse applications.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-acs-fra Functional requirements and architecture of access control service of IoT platform enabled by zero trust technology in decentralized environments

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18740

ABSTRACT: There are many big challenges for Internet of things (IoT) platforms in decentralized environments to make trust among the IoT entities (such as IoT devices, IoT services, IoT gateways, and other IoT resources) when they interact with each other. The traditional access control solutions of IoT platforms (such as perimeter control, password authentication, virtual private network) could not fully cope with those challenges, especially when IoT entities are deployed in decentralized environments. Zero trust (ZT) is one type of cybersecurity principles, which provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised [b-NIST SP 800-207]. In ZT-based access control solutions, it is no longer to determine access rights, by location and security domain for IoT entities to discover and access other IoT entities in same or different IoT platforms. It is required to be determined for any requests to discover and access to any IoT entities in IoT platforms. Therefore, ZT-based access control solutions are apt to IoT platforms in decentralized environments. This draft new Recommendation introduces an access control service of IoT platform in decentralized environments as enabled by zero trust technologies, and specifies its characteristics, functional requirements and architecture.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(Updated) NGI-Fed4Fire COMPUTATION OFFLOADING FOR IOT-ENABLED APPLICATIONS

🔗 URL: <https://www.fed4fire.eu/index.html>

ABSTRACT: COMFORT-APP aims to provide an offloading mechanism for IoT-enabled applications. IoT devices have limited resources in terms of energy, computation and networking, thus the execution of computation intensive applications is still restrictive for them. MEC offers the processing power of cloud computing at the proximity of mobile users.

📄 DOCUMENT TYPE: EU & National funded Open Source projects

📅 PUBLICATION DATE: Under development

(Updated) NGI-Trust B-Smart

 **URL:** <https://things.is/>

ABSTRACT: A human-centric interface, providing the best User Experience for managing privacy settings. One of the main issues related to the upcoming vision of the IoT is related to privacy: in particular, setting privacy controls. b-smart addresses this from the user perspective.

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

NGI-Trust D-SBOM (Distributed Software Bill of Materials)

 **URL:** <https://www.trublo.eu/d-sbom/>

ABSTRACT: -SBOM (Distributed Software Bills of Material) will provide a solution in complex IoT software supply chains to document all the software used in IoT devices and distribute this information in a secure and trusted way towards all users and actors.

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

NGI-Trust PY 2.0

 **URL:** <https://www.pyguard.fr/>

ABSTRACT: Aims to address issues by combining two emerging technologies known as edge AI and fog computing. Our solution will aggregate the data collected by the IoT devices into fog nodes and apply edge AI for data analysis at the edge of the infrastructure

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

OGC 12-006 Sensor Observation Service

 **URL:** <https://www.ogc.org/standards/sos#overview>

ABSTRACT: The SOS standard is applicable to use cases in which sensor data needs to be managed in an interoperable way. This standard defines a Web service interface which allows querying observations, sensor metadata, as well as representations of observed features. Further, this standard defines means to register new sensors and to remove existing ones. Also, it defines operations to insert new sensor observations. This standard defines this functionality in a binding independent way; two bindings are specified in this document: a KVP binding and a SOAP binding.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2012-04

OGC® document: 17-079r1 OGC SensorThings API Part 2 – Tasking Core

 **URL:** <http://docs.opengeospatial.org/is/17-079r1/17-079r1.html>

ABSTRACT: The OGC SensorThings API [OGC 15-078r6] provides an open, geospatial-enabled and unified way to interconnect the Internet of Things (IoT) devices, data, and applications over the Web. At a high level, the OGC SensorThings API provides two main functions and each function is handled by the Sensing part or the Tasking part. The Sensing part provides a standard way to manage and retrieve observations and metadata from heterogeneous IoT sensor systems. The Tasking part provides a standard way for parameterizing - also called tasking - of taskable IoT devices, such as

individual sensors and actuators, composite consumer / commercial / industrial / smart cities in-situ platforms, mobile and wearable devices, or even unmanned systems platforms such as drones, satellites, connected and autonomous vehicles, etc. This document specifies core of the SensorThings Tasking part.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-01

OGC® document: 18-088 OGC SensorThings API Part 1: Sensing Version 1.1

🔗 URL: <https://docs.ogc.org/is/18-088/18-088.html>

ABSTRACT: The OGC SensorThings API provides an open, geospatial-enabled and unified way to interconnect the Internet of Things (IoT) devices, data, and applications over the web. At a high level the OGC SensorThings API provides two main functionalities and each function is handled by a part. The two parts are the Sensing part and the Tasking part. The Sensing part provides a standard way to manage and retrieve observations and metadata from heterogeneous IoT sensor systems. This document is version 1.1 and it is extending the first version of Sensing part.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-08

Open Group Reference Architectures and Open Group Standards for the Internet of Things

🔗 URL: <https://publications.opengroup.org/w16d>

ABSTRACT: The Internet of Things (IoT) is one of the new technological phenomena driving the current digital revolution, and addressed by the Open Platform 3.0™ Forum, a Forum of The Open Group. Networked sensors and controls will enable enterprises to provide new products and services, and improve their existing operations. This White Paper discusses how architects can use standards to define IoT systems and solutions, compares four leading and emerging standard IoT reference architectures, and explains the role of The Open Group IoT Standards

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2016-12

Open Group O-DF Open Data Format (O-DF), The Open Group Standard for the Internet of Things (IoT), Version 2.0

🔗 URL: <https://publications.opengroup.org/c19d>

ABSTRACT: The Open Data Format (O-DF) standard is intended to represent information about things in a standardized way that can be understood and exchanged in a universal way by all information systems that need to manage IoT-related data. The O-DF standard can be used for publishing the available data using ordinary URL (Uniform Resource Locator) addresses. O-DF structures can also be used for requesting and sending published data between systems, notably when used together with The Open Group Open Messaging Interface (O-MI) standard.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-12

oneM2M TR-0017-V2.0.0 Home Domain Abstract Information Model

 **URL:** https://onem2m.org/images/files/deliverables/Release2/TR-0017-Home_Domain_Abstract_Information_Model-V2_0_0.pdf

ABSTRACT: The present document allows application developers to describe the status of devices as resources on oneM2M-based platform in various ways. Thus different application developers can create different resource trees even when they build the same kinds of applications. Moreover when handling the same kinds of devices from different vendors on M2M platforms, application developers may create disunited resource trees without common information model.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-8

oneM2M TR-0066-V-0.3.0 System Enhancement to Support Data License Management (DLM)

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33583>

ABSTRACT: The document is analysing existing data license schemes and how these licenses are being used in existing data management platforms to understand essential functions to utilize data license in the oneM2M system. Based on the result of the technical report, it will identify potential requirements and key features to support data license management in the oneM2M system.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2021-04

oneM2M TS-0001-V4.14.0 Functional Architecture

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34648>

ABSTRACT: This document specifies the functional architecture for the oneM2M Services Platform.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2022-03

oneM2M TS-0012-V3.7.3 OneM2M Base Ontology

 **URL:** https://www.onem2m.org/images/pdf/TS-0012-Base_Ontology-V3_7_3.pdf

ABSTRACT: oneM2M's Base Ontology constitutes a basis framework for specifying the

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: 2019-02

oneM2M TS-0034-V4.2.0 Semantics Support

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31425>

ABSTRACT: This specification provides normative text for semantic enablement in oneM2M.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2020-08

OMA ObjLwM2M_ACL LIGHTWEIGHTM2M ACCESS CONTROL

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_ACL/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Access Control v1.1

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_APN_Conn LIGHTWEIGHTM2M APN CONNECTION PROFILE

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_APN_Conn/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M APN Connection Profile v1.1.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Bearer_Conn LIGHTWEIGHTM2M BEARER SELECTION

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Bearer_Conn/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Bearer Selection v1.1.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Cell_Conn LIGHTWEIGHTM2M CELLULAR CONNECTIVITY

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Cell_Conn/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Cellular Connectivity v1.1.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Conn_Mon LightweightM2M Connectivity Monitoring

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Mon/V1_3-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Connectivity Monitoring v1.3.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Conn_Stat LightweightM2M Connectivity Statistics

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Stat/V1_0_5-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Connectivity Statistics v1.0.5.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_COSE LightweightM2M COSE

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_COSE/V1_0-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M COSE v1.0.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Device LightweightM2M Device

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Device/V1_2-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Device v1.2.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Firmware LightweightM2M Firmware Update

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Firmware/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Firmware Update v1.1.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

(Updated) ObjLwM2M_Gateway LightweightM2M Gateway

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Gateway/V1_0-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Gateway v1.0.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Location LightweightM2M Location

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Location/V1_0_3-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Location v1.0.3.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_MQTT_Server LightweightM2M MQTT Server

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_MQTT_Server/V1_0-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M MQTT Server v1.0.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_OSCORE LightweightM2M OSCORE

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_OSCORE/V2_0-20211123-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M OSCORE v2.0.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Routing LightweightM2M Routing

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Routing/V1_0-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Routing v1.0.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Security LightweightM2M Security

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Security/V1_2-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Security v1.2.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_Server LightweightM2M Server

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_Server/V1_2-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M Server v1.2.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_WLAN_Conn LightweightM2M WLAN Connectivity

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_WLAN_Conn/V1_1-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M WLAN Connectivity v1.1.

 DOCUMENT TYPE: Guideline

 PUBLICATION DATE: 2020-11

OMA ObjLwM2M_5GNR_Conn LIGHTWEIGHTM2M 5GNR CONNECTIVITY

 **URL:** https://www.openmobilealliance.org/release/ObjLwM2M_5GNR_Conn/V1_0-20201110-A/

ABSTRACT: DOCUMENT LISTING FOR SUP LightweightM2M 5GNR Connectivity v1.0.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** 2020-11

(Updated) W3C Thing Description (TD) Ontology

 **URL:** <https://www.w3.org/2019/wot/td>

ABSTRACT: The Thing Description (TD) ontology is an RDF axiomatization of the TD information model, one of the building blocks of the Web of Things (WoT). Besides providing an alternative to the standard JSON representation format for TD documents, the TD ontology can also be used to process contextual information on Things and for alignments with other WoT-related ontologies.

 **DOCUMENT TYPE:** Standard_Specification

PUBLICATION DATE: 2023-12

(Updated) W3C DIDs Decentralized Identifiers (DIDs) v1.0 (2021)

 **URL:** www.w3.org/TR/did-core/

ABSTRACT: Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject.

Each DID document can express cryptographic material, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject. A DID might provide the means to return the DID subject itself, if the DID subject is an information resource such as a data model.

This document specifies the DID syntax, a common data model, core properties, serialized representations, DID operations, and an explanation of the process of resolving DIDs to the resources that they represent.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-07

W3C JSON-LD 1.1 A JSON-based Serialization for Linked Data

 **URL:** www.w3.org/TR/json-ld11/

ABSTRACT: Data and Information Management - JSON is a data serialization and messaging format. This specification defines JSON-LD, a JSON-based format to serialize Linked Data. The syntax is designed to easily integrate into deployed systems that already use JSON, and provides a smooth upgrade path from JSON to JSON-LD. It is primarily intended to be a way to use Linked Data in Web-based programming environments, to build interoperable Web services, and to store Linked Data in JSON-based storage engines.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07

W3C ODRL Information Model 2.2 Open Digital Rights Language (ODRL) Information Model 2.2

 **URL:** www.w3.org/TR/odrl-model/

ABSTRACT: Data and Information Management, Security and Trustworthiness - A policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. The ODRL Information Model describes the underlying concepts, entities, and relationships that form the foundational basis for the semantics of the ODRL policies.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-02

W3C OGC 16-079 W3C Semantic Sensor Network Ontology

 **URL:** <https://www.w3.org/TR/vocab-ssn/>

ABSTRACT: The Semantic Sensor Network (SSN) ontology is an ontology for describing sensors and their observations, the involved procedures, the studied features of interest, the samples used to do so, and the observed properties, as well as actuators. SSN follows a horizontal and vertical modularization architecture by including a lightweight but self-contained core ontology called SOSA (Sensor, Observation, Sample, and Actuator) for its elementary classes and properties. With their different scope and different degrees of axiomatization, SSN and SOSA are able to support a wide range of applications and use cases, including satellite imagery, large-scale scientific monitoring, industrial and household infrastructures, social sensing, citizen science, observation-driven ontology engineering, and the Web of Things. Both ontologies are described below, and examples of their usage are given.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-10

W3C RDF Resource Description Framework (RDF) v1.1 (2014)

 **URL:** www.w3.org/RDF/

ABSTRACT: Enterprise/Systems Integration, Data and Information Management, Analytics and AI - RDF is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-02

W3C Verifiable Credentials Data Model v1.1 Verifiable Credentials Data Model v1.1 (2021)

 **URL:** www.w3.org/TR/vc-data-model/

ABSTRACT: Data and Information Management, Security and Trustworthiness - Create cryptographically secure, privacy respecting, and machine-verifiable credentials for establishing trust among different entities in a decentralized setting

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-03

(NEW) W3C Web of Things (WoT) Architecture 1.1

 **URL:** <https://www.w3.org/TR/wot-architecture11/>

ABSTRACT: The W3C Web of Things (WoT) enables interoperability across IoT platforms and application domains. The goal of the WoT is to preserve and complement existing IoT standards and solutions. The W3C WoT architecture is designed to describe what exists, and only prescribes new mechanisms when necessary.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

(NEW) W3C Web of Things (WoT) Thing Description 1.1

 **URL:** <https://www.w3.org/TR/wot-thing-description11/>

ABSTRACT: This document describes a formal information model and a common representation for a Web of Things (WoT) Thing Description 1.1. A Thing Description describes the metadata and interfaces of Things, where a Thing is an abstraction of a physical or virtual entity that provides interactions to and participates in the Web of Things. Thing Descriptions provide a set of interactions based on a small vocabulary that makes it possible both to integrate diverse devices and to allow diverse applications to interoperate. Thing Descriptions, by default, are encoded in a JSON format that also allows JSON-LD processing. The latter provides a powerful foundation to represent knowledge about Things in a machine-understandable way. A Thing Description instance can be hosted by the Thing itself or hosted externally when a Thing has resource restrictions (e.g., limited memory space) or when a Web of Things-compatible legacy device is retrofitted with a Thing Description. Furthermore, this document introduces the Thing Model, which allows authors to describe only the model or class of an Internet of Things (IoT) entity. Thing Models can be seen as a template for Thing Description instances, but with reduced constraints such as no or few requirements for specific communication metadata.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

(NEW) W3C Web of Things (WoT) Discovery

 **URL:** <https://www.w3.org/TR/wot-discovery/>

ABSTRACT: The WoT Discovery process is divided into two phases, Introduction, and Exploration. The Introduction phase leverages existing discovery mechanisms but does not directly expose metadata; they are simply used to discover Exploration services, which provide metadata but only after secure authentication and authorization.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

DIN SPEC 16593-1 Reference Model for Industry 4.0 Service Architectures - Part 1: Basic Concepts of an Interaction-based Architecture

 **URL:** www.beuth.de/de/technische-regel/din-spec-16593-1/287632675

ABSTRACT: System Architecture - Concepts of component interaction in Plattform Industry 4.0

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-04

IEC 62541-10:2020 OPC Unified Architecture - Part 10: Programs

 **URL:** <https://webstore.iec.ch/publication/61119>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07-07

IEC 62541-100:2015 OPC Unified Architecture - Part 100: Device Interface

 **URL:** <https://webstore.iec.ch/publication/21987>

ABSTRACT: IEC 62541-100:2015 is an extension of the overall OPC Unified Architecture standard series and defines the information model associated with Devices. This part of IEC 62541 describes three models which build upon each other: - the (base) Device Model intended to provide a unified view of devices; - the Device Communication Model which adds Network and Connection information elements so that communication topologies can be created; - the Device Integration Host Model finally which adds additional elements and rules required for host systems to manage integration for a complete system. It allows reflecting the topology of the automation system with the devices as well as the connecting communication networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-03-25

IEC 62541-11:2020 OPC Unified Architecture - Part 11: Historical Access

 **URL:** <https://webstore.iec.ch/publication/61129>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06-23

IEC 62541-13:2020 OPC Unified Architecture - Part 13: Aggregates

 **URL:** <https://webstore.iec.ch/publication/61131>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06-11

IEC 62541-14:2020 OPC Unified Architecture - Part 14: PubSub

 **URL:** <https://webstore.iec.ch/publication/61108>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07-08

IEC 62541-3:2020 OPC Unified Architecture - Part 3: Address Space Model

 **URL:** <https://webstore.iec.ch/publication/61112>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07-08

IEC 62541-4:2020 OPC Unified Architecture - Part 4: Services

 **URL:** <https://webstore.iec.ch/publication/61113>

ABSTRACT: IEC 62541-4:2020 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-4:2020 defines the OPC Unified Architecture (OPC UA) Services. The Services defined are the collection of abstract Remote Procedure Calls (RPC) that are implemented by OPC UA Servers and called by OPC UA Clients. All interactions between OPC UA Clients and Servers occur via these Services. The defined Services are considered abstract because no particular RPC mechanism for implementation is defined in this document. IEC 62541-6 specifies one or more concrete mappings supported for implementation. For example, one mapping in IEC 62541-6 is to XML Web Services. In that case the Services described in this document appear as the Web service methods in the WSDL contract. Not all OPC UA Servers will need to implement all of the defined Services. IEC 62541-7 defines the Profiles that dictate which Services need to be implemented in order to be compliant with a particular Profile. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07-13

IEC 62541-5:2020 OPC Unified Architecture - Part 5: Information Model

 **URL:** <https://webstore.iec.ch/publication/61114>

ABSTRACT: IEC 62541-5:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-5:2020 defines the Information Model of the OPC Unified Architecture. The Information Model describes standardized Nodes of a Server's AddressSpace. These Nodes are standardized types as well as standardized instances used for diagnostics or as entry points to server-specific Nodes. Thus, the Information Model defines the AddressSpace of an empty OPC UA Server. However, it is not expected that all Servers will provide all of these Nodes. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- a) Added Annex F on User Authentication. Describes the Role Information Model that also allows configuration of Roles.
- b) Added new data types: "Union", "Decimal", "OptionSet", "DateString", "TimeString", "DurationString", "NormalizedString", "DecimalString", and "AudioDataType".
- c) Added Method to request a state change in a Server.
- d) Added Method to set Subscription to persistent mode.
- e) Added Method to request resending of data from a Subscription.
- f) Added concept allowing to temporarily create a file to write to or read from a server in C.4. g) Added new Variable type to support Selection Lists.
- g) Added optional properties to FiniteStateMachineType to expose currently available states and transitions.
- h) Added UrisVersion Property to ServerType. This version information can be used for session-less service invocation.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-07-10

IEC 62541-6:2020 OPC Unified Architecture - Part 6: Mappings

 **URL:** <https://webstore.iec.ch/publication/61115>

ABSTRACT: IEC 62541-6:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-6:2020 specifies the OPC Unified Architecture (OPC UA) mapping between the security model described in IEC TR 62541-2, the abstract service definitions specified in IEC 62541-4, the data structures defined in IEC 62541-5 and the physical network protocols that can be used to implement the OPC UA specification. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- a) Encodings:
 -  added JSON encoding for PubSub (non-reversible);
 -  added JSON encoding for Client/Server (reversible);
 -  added support for optional fields in structures;
 -  added support for Unions.
- b) Transport mappings:
 -  added WebSocket secure connection – WSS;
 -  added support for reverse connectivity;
 -  added support for session-less service invocation in HTTPS.
- c) Deprecated Transport (missing support on most platforms):
 -  SOAP/HTTP with WS-SecureConversation (all encodings).
- d) Added mapping for JSON Web Token.

- e) Added support for Unions to NodeSet Schema.
- f) Added batch operations to add/delete nodes to/from NodeSet Schema.
- g) Added support for multi-dimensional arrays outside of Variants.
- h) Added binary representation for Decimal data types.
- i) Added mapping for an OAuth2 Authorization Framework.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-07-13

IEC 62541-7:2020 OPC Unified Architecture - Part 7: Profiles

🔗 URL: <https://webstore.iec.ch/publication/61116>

ABSTRACT: IEC 62541-7:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-7:2020 defines the OPC Unified Architecture (OPC UA) Profiles. The Profiles in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs. This could equally as well refer to test tools provided by another organization or a test lab provided by another organization. What is important is the concept of automated tool-based testing versus lab-based testing. The scope of this standard includes defining functionality that can only be tested in a lab and defining the grouping of functionality that is to be used when testing OPC UA products either in a lab or using automated tools. The definition of actual TestCases is not within the scope of this document, but the general categories of TestCases are within the scope of this document. Most OPC UA applications will conform to several, but not all, of the Profiles. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

a) new functional Profiles:

- 🔗 profiles for global discovery and global certificate management;
- 🔗 profiles for global KeyCredential management and global access token management;
- 🔗 facet for durable subscriptions;
- 🔗 standard UA Client Profile;
- 🔗 profiles for administration of user roles and permissions.

b) new transport Profiles:

- 🔗 HTTPS with JSON encoding;
- 🔗 secure WebSockets (WSS) with binary or JSON encoding;
- 🔗 reverse connectivity.

c) new security Profiles:

- 🔗 transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy);
- 🔗 securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15);
- 🔗 securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP);
- 🔗 user Token JWT (Jason Web Token).

d) deprecated Security Profiles (due to broken algorithms):

- 🔗 securityPolicy – Basic128Rsa15 (broken algorithm Sha1);
- 🔗 securityPolicy – Basic256 (broken algorithm Sha1);
- 🔗 transportSecurity – TLS 1.0 (broken algorithm RC4);
- 🔗 transportSecurity – TLS 1.1 (broken algorithm RC4).

e) deprecated Transport (missing support on most platforms):

- 🔗 SOAP/HTTP with WS-SecureConversation (all encodings).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06-22

IEC 62541-8:2020 OPC Unified Architecture - Part 8: Data Access

 **URL:** <https://webstore.iec.ch/publication/61117>

ABSTRACT: IEC 62541-8:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-8:2020 is part of the overall OPC Unified Architecture (OPC UA) standard series and defines the information model associated with Data Access (DA). It particularly includes additional VariableTypes and complementary descriptions of the NodeClasses and Attributes needed for Data Access, additional Properties, and other information and behaviour. The complete address space model, including all NodeClasses and Attributes is specified in IEC 62541-3. The services to detect and access data are specified in IEC 62541-4. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) added new VariableTypes for AnalogItems; b) added an Annex that specifies a recommended mapping of OPC UA DataAccess to OPC COM DataAccess; c) changed the ambiguous description of “Bad_NotConnected”; d) updated description for EUInformation to refer to latest revision of UNCEFACT units.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06-22

IEC 62541-9:2020 OPC Unified Architecture - Part 9: Alarms and Conditions

 **URL:** <https://webstore.iec.ch/publication/61118>

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

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06-18

IEC 62714-1:2018 Engineering data exchange format for use in industrial automation systems engineering - Automation Markup Language - Part 1: Architecture and general requirements

 **URL:** <https://webstore.iec.ch/publication/32339>

ABSTRACT: IEC 62714-1:2018 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62714-1:2018 is a solution for data exchange focusing on the domain of automation engineering. The data exchange format defined in the IEC 62714 series (Automation Markup Language, AML) is an XML schema based

data format and has been developed in order to support the data exchange in a heterogeneous engineering tools landscape. The goal of AML is to interconnect engineering tools in their different disciplines, e.g. mechanical plant engineering, electrical design, process engineering, process control engineering, HMI development, PLC programming, robot programming, etc. This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) use of CAEX 3.0 according to IEC 62424:2016 b) improved modelling of references to documents outside of the scope of the present standard, c) modelling of references between CAEX attributes and items in external documents, d) revised role libraries, e) modified Port concept, f) modelling of multilingual expressions, g) modelling of structured attribute lists or array, h) a new AML container format, i) a new standard AML attribute library

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-04-30

IEC 62714-2:2015 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 2: Role class libraries

🔗 URL: <https://webstore.iec.ch/publication/22030>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-03-30

IEC 62714-3:2017 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 3: Geometry and kinematics

🔗 URL: <https://webstore.iec.ch/publication/34158>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-01-25

IEC 62714-4:2020 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 4: Logic

🔗 URL: <https://webstore.iec.ch/publication/28979>

ABSTRACT: IEC 62714-4:2020 specifies the integration of logic information as part of an AML model for the data exchange in a heterogeneous 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06-16

IEC 62714-5:2022 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 5: Communication

🔗 URL: <https://webstore.iec.ch/publication/65493>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-03-11

(Updated) IEC 63365:2022 ED1Industrial process measurement, control and automation - Digital nameplate

🔗 URL: <https://webstore.iec.ch/publication/67436>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-10-18

IEC TR 62541-1:2020 OPC Unified Architecture - Part 1: Overview and concepts

🔗 URL: <https://webstore.iec.ch/publication/61109>

ABSTRACT: 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.

ISO/IEC 30161:2020 Internet of things (IoT) - Data exchange platform for IoT services - Part 1: General requirements and architecture

URL: <https://webstore.iec.ch/publication/63404>

ABSTRACT: ISO/IEC 30161-1:2020(E) specifies requirements for an Internet of Things (IoT) data exchange platform for various services in the technology areas of: a) the middleware components of communication networks allowing the co-existence of IoT services with legacy services; b) the end-points performance across the communication networks among the IoT and legacy services; c) the IoT specific functions and functionalities allowing the efficient deployment of IoT services; d) the IoT service communication networks' framework and infrastructure; and e) the IoT service implementation guideline for the IoT data exchange platform.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2020-11

(NEW) ITU-T Y.AIoT-dpsm Requirements and framework of data processing for smart manufacturing with Artificial Intelligence of Things

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19627

ABSTRACT: Smart manufacturing with Artificial Intelligence of Things(AIoT) integrates advanced technologies like AI to transform manufacturing and production processes. AIoT enables smart manufacturing in high level intelligence and autonomous. Data processing for smart manufacturing with AIoT improves production efficiency, reduces operational costs and enhances quality control by enabling real-time data processing based on the data collected from smart manufacturing environments. This Recommendation describes the requirements and framework of data processing for smart manufacturing with AIoT.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

Mobility

C2CC C2CCC_RS_2035 Objectives

URL: https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2035_Objectives.pdf

ABSTRACT: The wide scope of the Cooperative Intelligent Transport Systems (C-ITS) definition affects all parts of traffic and thus involves many different stakeholders. This set of stakeholders may also comprise international entities or Standards Developing Organizations (SDO) of different nations. The primary objective of the C2C-CC is to ensure interoperability in field of C-ITS between different vehicle manufacturers. This document provides objectives regarding C-ITS from C2C-CC point of view. They focus on vehicles but can be applied to other traffic participants too. In terms of C2C-CC, an objective is defined as an abstract requirement without any further specification about its details.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2021-12

C2CC C2CCC_RS_2036 Features

 **URL:** https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2036_Features.pdf

ABSTRACT: Within the open system architecture of Cooperative Intelligent Transport System (C-ITS) four types of participants, called sub-systems, are identified in ETSI EN 302 665: vehicle, roadside, personal, and central. Each of these sub-systems includes a C-ITS station, but based on their sub-system specific equipment they enable different features. As a result of their feature list and their role in traffic, for each sub-system a set of use cases becomes possible to improve road safety and traffic efficiency. This document provides all features in scope of a vehicle sub-system from C2C-CC point of view. This set of features is the consolidated and communicated understanding of the core vehicle system features in a vehicle C-ITS station. The list in this document focuses on specifying the vehicle C-ITS station transmitting side. Moreover, this set is oriented towards enabling the vehicle use cases as included in the current C2C-CC release. Features themselves are detailed by one or more requirements. A feature can be assumed as tested if all requirements which detail this feature are tested.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-12

CEN EN 16157-1:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 1: Context and framework

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:62523&cs=15997C7BB19A97A296D8A7719196409AD

ABSTRACT: This document specifies and defines components required to support the exchange and shared use of data and information in the field of traffic and travel. The components include the framework and context for the modelling approach, data content, data structure and relationships. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator-initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. This part of EN 16157 specifies the DATEX II framework of all parts of this European Standard, the context of use and the modelling approach taken and used throughout this European Standard. This approach is described using formal methods and provides the mandatory reference framework for all other parts

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-12

CEN EN 16157-2:2019 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 2: Location referencing

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60747&cs=1C3A140087AD1FDE865115EA876607C93

ABSTRACT: This European Standard series (EN 16157) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The

component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard series is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This European Standard series establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this European Standard series may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - operator initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. This part of the EN 16157 series specifies the informational structures, relationships, roles, attributes and associated data types, for the implementation of the location referencing systems used in association with the different publications defined in the Dutex II framework. It also defines a Dutex II publication for exchanging predefined locations. This is part of the Dutex II platform independent data model

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-03

CEN EN 16157-3:2018 Intelligent transport systems - Dutex II data exchange specifications for traffic management and information - Part 3: Situation Publication

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60748&cs=13B159A7784936BDC97A42AFA8C21211A

ABSTRACT: This document specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - operator-initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. This document specifies the informational structures, relationships, roles, attributes and associated data types required for publishing situation traffic and travel information within the Dutex II framework. This is specified as a Dutex II Situation Publication sub-model which is part of the Dutex II platform independent model, but this part excludes those elements that relate to: - location information which are specified in FprEN 16157 2; - common information elements, which are specified in EN 16157 7.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-12

CEN EN 16157-4:2021 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 4: VMS publication

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68227&cs=19CD8A5DF8D8A747A2648590BAC670053

ABSTRACT: This European Standard (EN16157 series) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard is applicable to: - Traffic and travel information which is of relevance to road networks (non-urban and urban), - Public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - Traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This European Standard establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this European Standard may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content: - Road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment, - Operator initiated actions, - Road traffic measurement data, status data, and travel time data, - Travel information relevant to road users, including weather and environmental information, - Road traffic management information and instructions relating to use of the road network. This part of the CEN/TS 16157 series specifies the informational structures, relationships, roles, attributes and associated data types required for publishing variable message sign information within the DateX II framework. This is specified in two publications, a DATEX II VMS Table Publication sub-model and a VMS Publication sub-model, which are part of the DATEX II platform independent model, but this part excludes those elements that relate to: - location information which are specified in EN 16157-2, - common information elements, which are specified in EN 16157-7, - situation information which are specified in EN 16157-3. The VMS Table Publication supports the occasional exchange of tables containing generally static reference information about deployed VMS which enable subsequent efficient references to be made to pre-defined static information relating to those VMS. The VMS Publication supports the exchange of the graphic and textual content of one or several VMS plus any status information on device configuration that aid the comprehension of the informational content. This content is potentially subject to rapid change. These publications are not intended to support the control or configuration of VMS equipment. Each is part of the DATEX II platform independent model.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-03

CEN EN 16157-5:2020 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 5: Measured and elaborated data publications

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68225&cs=15C7361EFFF209FF289AF2AAE0FBC17A1

ABSTRACT: This document is the fifth part of the DATEX II European Standard which deals with the publication sub-models within the DATEX II model that support the exchange of measured and elaborated information. These publications are intended to support the exchange of informational content from the organization having the measured data and creating elaborated data to other organisations providing ITS services or onward information exchange. It also includes the exchange of static information about measurement sites. This is specified in three sub-models, a DATEX II Measurement Site Table Publication sub-model, a DATEX II Measured Data Publication sub-model and a DATEX II Elaborated Data Publication sub-model.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-08

CEN EN 16157-7:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 7: Common data elements

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:62524&cs=14AD3FDA01670AAB7137D7857613CB12B

ABSTRACT: This document specifies and defines component facets required to support the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for data content, data structure and relationships, communications specification. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. This part of EN 16157 specifies common informational structures, relationships, roles, attributes and associated data types required for publishing information within the DATEX II framework. This is specified as a DATEX II sub-model which is part of the DATEX II platform independent model, but this part only covers common elements that are used by more than one publication. It excludes those elements that relate to location information which are specified in FprEN 16157 2.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-12

(Updated) CEN/TS 16157-6 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 6: Parking publications

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:FSP_LANG_ID:69724,25&cs=1451A03D2D2D1D87355F1559FEB7FA425

ABSTRACT: This new work item will revise and extend the sixth part of the DATEX II Technical Specifications which defines three DATEX II parking-related publications and a truck parking profile and that supports the exchange of static as well as dynamic information about parking facilities and areas, including intelligent truck parking as defined by the Directive 2010/40/EU priority action e as well as urban parking as specified in action a. The formerly used Level B extension will be replaced by a new namespace in the context of version 3.0 of DATEX II. The publications are intended to support the exchange of informational content from the organisation performing measurements and collecting/eliciting basic data to other organisations providing ITS services or onward information exchange. It is the ambition to harmonise existing information models from different sources such as EasyWay deployment guidelines and truck parking initiatives, and to liaise with the stakeholders involved, especially with the Alliance for Parking Data Standards and CEN/TC 278 working group 3.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-07

CEN ISO/TS 19468:2022 Intelligent transport systems - Data interfaces between centres for transport information and control systems - Platform-independent model specifications for data exchange protocols for transport information and control systems

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71962&cs=18889333092FF2E127C49B472E09BA2FB

ABSTRACT: This document defines and specifies component facets supporting the exchange and shared usage of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the data content, structure and relationships necessary and the communications specifications, in such a way that they are independent from any defined technical platform. This document establishes specifications for data exchange between any two instances of the following actors: — Traffic information centres (TICs); — Traffic control centres/Traffic management centres (TCCs/TMCs); — Service providers (SPs). This document can also be applied for use by other actors, e.g. car park operators. This document includes the following types of information: — use cases and associated requirements, and features relative to different exchange situations; — different functional exchange profiles; — abstract elements for protocols; — data model for exchange (informational structures, relationships, roles, attributes and associated data types required). In order to set up a new technical exchange framework, it is necessary to associate one functional exchange profile with a technical platform providing an interoperability domain where plug-and-play interoperability at a technical level can be expected. The definition of such interoperability domains is out of scope of this document but can be found in other International Standards or Technical Specifications (e.g. the ISO 14827 series). This document is restricted to data exchange. Definition of payload content models is out of the scope of this document.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-02

CEN/TS 16157-10:2022 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 10: Energy infrastructure publications

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71189&cs=17CE8E7FC7390CF7CC48C34700D0A825D

ABSTRACT: The EN 16157 series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. The EN 16157 series is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban); - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service); - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This series establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs); - Traffic Control Centres (TCCs); - Service Providers (SPs). Use of this series can be applicable for use by other actors. This series covers, at least, the following types of informational content: - road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment; - operator initiated actions; - road traffic measurement data, status data, and travel time data; - travel information relevant to road users, including weather and environmental information; - road traffic management information and instructions relating to use of the road network. This part of the CEN/TS 16157 series specifies details of infrastructure for vehicle energy supply. The provided data model is separated into two publications for static and dynamic information. The static information regarding the infrastructure is not subject to frequent changes, whereas the dynamic part offers the ability to provide highly up-to-date information. The static part covers all relevant information on vehicle energy infrastructure, e.g. sites, stations and refill points for electric vehicles as well as petrol, gasoline or gas-based refuelling for vehicles. In terms of

dynamic information, the availability of the infrastructure, possible faults and a price indication are covered.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-03

CEN/TS 16157-11 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 11: Publication of machine interpretable traffic regulations

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71777&cs=10465408B33310F1C137C3B2AABC7EE51

ABSTRACT: This document specifies a publication sub-model within the DATEX II model that supports the publication of electronic traffic regulations. This publication is intended to support the exchange of informational content from road traffic authorities issuing traffic regulation orders and organisations implementing these orders to other organisations providing ITS services or onward information exchange.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-03

CEN/TS 16157-12 Intelligent transport systems — DATEX II management and information — Part 12: Facilities publications

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:FSP_LANG_ID:73025,25&cs=191FBA7A8FAE57738466F76A27106F67D

ABSTRACT: This document specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel.

The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-05

CEN/TS 16157-6:2015 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 6: Parking Publications

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:40220&cs=1084702C54C56E3547969771C8305250B

ABSTRACT: This new work item will produce the sixth part of the DATEX II Technical Specifications which deals with a DATEX II Level B extension (two publications and a Truck Parking profile) that supports the exchange of static as well as dynamic information about parking facilities and areas, including intelligent truck parking as defined by the directive 2010/40/EU priority actions e and f. The publications are intended to support the exchange of informational content from the organisation performing measurements and collecting/eliciting basic data to other organisations providing ITS services or onward information exchange. It is the ambition to harmonise existing information models from different sources such as EasyWay deployment guidelines, In-Time CAI and Truck Parking initiatives, and to liaise with the stakeholders involved

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2015-10

CEN/TS 16157-8 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 8: Traffic management publications and extensions dedicated to the urban environment

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68653&cs=18BC2B0B4960475D11D2ABEA1D8C23A2D

ABSTRACT: This document constitutes a Part of the CEN 16157 DATEX II series of standards and technical specifications. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 8, this document, specifies additional data model structures that are applicable for traffic management applications in the urban environment. This Part addresses data concepts to support the exchange of Traffic Management Plans, rerouting, extensions of the existing DATEX II core model to better support application to the urban environment. It establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document may be applicable for use by other actors.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-04

CEN/TS 16157-9 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 9: Traffic signal management publications dedicated to the urban environment

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68652&cs=18B5180A209437120996363BB8237DDAC

ABSTRACT: This document constitutes a part of the CEN 16157 DATEX II series of standards and technical specifications. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 9, this document, specifies additional data model structures that are applicable for traffic signal management applications in the urban environment. This part specifies data concepts to support the exchange of traffic signal status messaging, intersection geometry definition and attribution in a consistent way with existing C-ITS standards and technical specifications. It establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document may be applicable for use by other actors

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-04

CEN/TS 16614-1:2020 Public transport - Network and Timetable Exchange (NeTEx) - Part 1: Public transport network topology exchange format

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:66892&cs=1CAED5ABB1179CBAE5D7E61C865704C55

ABSTRACT: 1.1 General NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information). It is based on Transmodel V6 (EN 12896 series) and SIRI (CEN/TS 15531-4/-5 and EN 15531-1/-2/-3) and supports the exchange of information of relevance for passenger information about public transport services and also for running Automated Vehicle Monitoring Systems (AVMS). NOTE

Many NeTeX concepts are taken directly from Transmodel; the definitions and explanation of these concepts are extracted directly from the respective standard and reused in NeTeX, sometimes with adaptations in order to fit the NeTeX context. Although the data exchanges targeted by NeTeX are predominantly oriented towards provisioning passenger information systems and AVMS with data from transit scheduling systems, it is not restricted to this purpose and NeTeX can also provide an effective solution to many other use cases for transport data exchange.

1.2 Transport modes All mass public transport modes are taken into account by NeTeX, including train, bus, coach, metro, tramway, ferry, and their submodes. It is possible to describe airports and air journeys, but there has not been any specific consideration of any additional requirements that apply specifically to air transport.

1.3 Compatibility with existing standards and recommendations Concepts covered in NeTeX that relate in particular to long-distance train travel include; rail operators and related organizations; stations and related equipment; journey coupling and journey parts; train composition and facilities; planned passing times; timetable versions and validity conditions. In the case of long distance train the NeTeX takes into account the requirements formulated by the ERA (European Rail Agency) - TAP/TSI (Telematics Applications for Passenger/ Technical Specification for Interoperability, entered into force on 13 May 2011 as the Commission Regulation (EU) No 454/2011), based on UIC directives. As regards the other exchange protocols, a formal compatibility is ensured with TransXChange (UK), VDV 452 (Germany), NEPTUNE (France), UIC Leaflet, BISON (The Netherlands) and NOPTIS (Nordic Public Transport Interface Standard). The data exchange is possible either through dedicated web services, through data file exchanges, or using the SIRI exchange protocol as described in part 2 of the SIRI documentation.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-04

ETSI EG 202 798 ITS; Testing; Framework for conformance and interoperability testing

🔗 URL: http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/01.01.01_60/eg_202798v010101p.pdf

ABSTRACT: This document specifies the global framework for conformance and interoperability testing in ITS.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2011-01

ETSI EN 302 665 ITS; Communications Architecture

🔗 URL: http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf

ABSTRACT: Definition of ITS Communications Architecture for Europe including the following views:

- 📄 Scenario description;
- 📄 Functional View and Information View;
- 📄 OSI reference model view including Application View, Security View, Network&Transport View, Interface View, Management view;
- 📄 Engineering view to support Implementation Guidelines for Interoperability;
- 📄 Enterprise/Organizational/Operational view.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2010-09

(Updated) ETSI TS 102 894-2 V2.2.1 ITS; Users and applications requirements; Part 2: Applications and facilities layer common data dictionary

 **URL:** https://www.etsi.org/deliver/etsi_ts/102800_102899/10289402/02_02_01_60/ts_10289402v020201p.pdf

ABSTRACT: Definition and specifications on the common data container at the applications and facilities layer.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-10

(Updated) ETSI TS 103 301 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01_03_01_60/ts_103301v010301p.pdf

ABSTRACT: The present document provides specifications of infrastructure related ITS services to support communication between infrastructure ITS equipment and traffic participants using ITS equipment (e.g. vehicles, pedestrians). It defines services in the Facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity.

It has been published for both Release 1 (V1.3.1) and Release 2 (V2.1.1) of the ETSI C-ITS standards.

 **DOCUMENT TYPE:** Standard_Specification

PUBLICATION DATE: 2021-03

(NEW) ITU-T Y.IoT-CMP-VR Functional framework and capabilities of coordination management platform for IoT based vehicle-roads

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19615

ABSTRACT: This Recommendation provides coordination management platform for IoT based vehicle-road, including reference framework and associated capabilities. This Recommendation defines a unified framework that incorporates vehicles and other traffic participants, roadside infrastructure, cloud management platforms, and management applications for intelligent connected vehicle management and intelligent traffic management.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.Sup.VFS Functional architecture of connected vehicle formation supporting based on edge computing

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19070

ABSTRACT: This Supplement provides the functional architecture of connected vehicle formation supporting based on edge computing, including functional architecture, functional entity, and reference point, which is a supplementary to ITU-T Y.4471 Recommendation.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.IoT-IWAT Framework of interworking with agent-based transportation for intelligent IoT services

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19629

ABSTRACT: Vehicles in the transportation are equipped with a various IoT devices, which can be defined as things based on agent like software in terms of IoT. These IoT devices collect and generate various types of IoT data related to IoT-based smart city services in real time. In addition, the things in the transportation can be interworked with external IoT services to provide new intelligent IoT services by fusing them with the collected or generated IoT data. Therefore, the interworking of IoT data between things in the transportation and intelligent IoT services in the smart city can facilitate the development of various intelligent IoT convergence services. In particular, the smart city is equipped with an infrastructure that enables things to send and receive IoT data to and from various things in the smart city through V2X (Vehicle to Everything) communication. Therefore, it is possible to deliver and exchange data between things in the transportation, and to configure new intelligent IoT convergence services through data fusion between them. To this end, this draft Recommendation introduces the concept of interworking with agent-based transportation for intelligent IoT services and the requirements needed to configure intelligent IoT convergence services through it. And this draft Recommendation also describes the functional architecture, functional components, and interactions between them.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

SAE AIR6988 Artificial Intelligence in Aeronautical Systems: Statement of Concerns

 **URL:** <https://www.sae.org/standards/content/air6988/>

ABSTRACT: This document reviews current aerospace software, hardware, and system development standards used in the certification/approval process of safety-critical airborne and ground-based systems, and assesses whether these standards are compatible with a typical Artificial Intelligence (AI) and Machine Learning (ML) development approach. The document then outlines what is required to produce a standard that provides the necessary accommodation to support integration of ML-enabled sub-systems into safety-critical airborne and ground-based systems, and details next steps in the production of such a standard.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-04

SAE J2945/1 On-Board System Requirements for V2V Safety Communications

 **URL:** https://www.sae.org/standards/content/j2945/1_202004/

ABSTRACT: This standard specifies the system requirements for an on-board vehicle-to-vehicle (V2V) safety communications system for light vehicles, including standards profiles, functional requirements, and performance requirements. The system is capable of transmitting and receiving the SAE J2735-defined basic safety message (BSM) over a dedicated short-range communications (DSRC) wireless communications link as defined in the IEEE 1609 suite and IEEE 802.11 standards. DSRC is a U.S. Department of Transportation (DOT) project based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-04

CENELEC EN 50090 (ISO 14543) Home and Building Electronic Systems (HBES)

 **URL:** https://standards.cenelec.eu/dyn/www/f?p=CENELEC:110:::FSP_PROJECT,FSP_ORG_ID:55668,1258281&cs=14BD408738BD97FB5CF4581F27FF76877

ABSTRACT: System Architecture, Communications/Networking, Data and Information Management - KNX is an open standard (see EN 50090, ISO/IEC 14543) for commercial and domestic building automation. KNX evolved from three earlier standards: the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB or Instabus). On this network, the devices form distributed applications and tight interaction is possible. This is implemented via interworking models with standardized datapoint types and objects, modelling logical device channels.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2012-02

EEBUS SHIP (Smart Home IP) and SPINE (Smart Premises Interoperable Neutral Message Exchange)

 **URL:** www.eebus.org/media-downloads/#specifications

ABSTRACT: System Architecture, Communications/Networking, Data and Information Management - EEBUS specifies the language of energy using the SHIP, SPINE and Use Case specifications. Bosch Software Innovations and KEO Connectivity provide a simple implementation of the EEBUS interface via their software products for EEBUS integration.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** N/A

Energetics ETP v1.2 Energistics Transfer Protocol (ETP) v1.2 (2021)

 **URL:** <https://www.energistics.org/energistics-releases-v1-2-of-energistics-transfer-protocol/>

ABSTRACT: Data and Information Management - The ETP data exchange specification enables efficient transfer of data between applications. The initial use case is for real-time data; however, it is anticipated that ETP will be expanded to include functionality for historical data queries. ETP has been specifically envisioned and designed to meet the unique needs of the upstream oil and gas industry and especially to facilitate the exchange of data across the Energistics family of data standards, which includes WITSML, PRODML and RESQML.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-09

(Updated) ETSI TS 103 410-1 V1.2.1 SmartM2M; Extension to SAREF; Part 1: Energy Domain

 **URL:** https://www.etsi.org/deliver/etsi_ts/103400_103499/10341001/01_02_01_60/ts_10341001v010201p.pdf

ABSTRACT: This work extends the Smart Appliances reference ontology as defined in TS 103 264. The objective is to include input from the energy domain actors. This specification is defined as an extension of TS 103 264.

Note: The TS 103 410 set of standards covers the following domains:

- 🔖 TS 103 410-1 - Extension to SAREF; Part 1: Energy Domain
- 🔖 TS 103 410-2 - Extension to SAREF; Part 2: Environment Domain
- 🔖 TS 103 410-3 - Extension to SAREF; Part 3: Building Domain
- 🔖 TS 103 410-4 - Extension to SAREF; Part 4: Smart Cities Domain
- 🔖 TS 103 410-5 - Extension to SAREF; Part 5: Industry and Manufacturing Domains
- 🔖 TS 103 410-6 - Extension to SAREF; Part 6: Smart Agriculture and Food Chain Domain
- 🔖 TS 103 410-7 - Extension to SAREF; Part 7: Automotive Domain
- 🔖 TS 103 410-8 - Extension to SAREF; Part 8: eHealth/Ageing-well Domain
- 🔖 TS 103 410-9 - Extension to SAREF; Part 9: Wearables Domain
- 🔖 TS 103 410-10 - Extension to SAREF; Part 10: Water Domain
- 🔖 TS 103 410-11 - Extension to SAREF; Part 11: Lift Domain

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-11

ISO/IEC TR 30148:2019 Internet of things (IoT) - Application of sensor network for wireless gas meters

🔗 URL: <https://webstore.iec.ch/publication/63562>

ABSTRACT: ISO/IEC TR 30148:2019 (E) describes: a) the structure of wireless gas meter networks, and b) the application protocol of wireless gas meter networks.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-10

(NEW) ITU-T Y.smart-PBRS Functional Architecture of Smart Power Bank Rental Service Framework

🔗 URL: <https://www.itu.int/rec/T-REC-L.1333-202209-I>

ABSTRACT: With the adoption of Internet of Things (IoT) technology, Smart Power Bank Rental (SPBR) service can satisfy the on-the-go charging needs for people, improve the service efficiency and provide real-time service monitoring and management for the service providers. Relevant products of SPBR service have emerged and developed in a certain scale in several countries and regions. Lack of standards might cause deviating capabilities and uneven performance of the service, which can lead to inconsistent service experience and limit vendors' ability to meet rising demand across the global, thus affecting the market acceptance of this service. This Recommendation introduces SPBR Service, and specifies functional requirements of SPBR Service and functional architecture of SPBR Service framework to provide guidance for device manufacturers and service providers when developing the SPBR equipment and services.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under developmemt

(NEW) ITU-T Y.DTS-arch Architecture of the digital twin system in power grid

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19612

ABSTRACT: The digital twin concept turns a new view of technology into the power grid. Digital Twin system in power grid can perform online analysis of the grid in real-time and integrates all the information and express the current grid status to the producers and consumers and predicts the future grid status. Thus, the power grid transmission loss and location of the overheated line and power connection missing can be detected in addition decision-making and self-healing can possible. The future prediction saves the power grid from small to large accidents such as power outages

and even blackout problems. This draft recommendation provides the architecture of the digital twin power grid, describes the functional entities in the digital twin system, as well as the use cases.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.EDSS Framework and requirements of electricity data sharing system

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19632

ABSTRACT: The rapid development of smart grids and the increasing deployment of IoT devices have resulted in a significant increase in electricity data generation (including consumption data, generation data, grid status data, etc.), which is collected and transmitted by IoT devices such as smart meters, sensors, and smart appliances. Efficient utilization of electricity data can lead to substantial benefits such as optimizing grid operations, enhancing energy efficiency, regulatory compliance and reporting, infrastructure planning and investment and improving customer services. However, the collection, storage, and sharing of electricity data pose significant challenges, particularly in terms of privacy and security. This draft new Recommendation introduces the framework, requirements and use cases of electricity data sharing system, and aims to establish a robust system for the secure and privacy-preserving sharing of electricity data. This framework leverages advanced techniques to ensure that data privacy is maintained throughout the data lifecycle, from collection to processing and sharing.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.metadata-EPI (ex Y.Sup.metadata-EPI) Metadata for IoT-based electric power infrastructure monitoring system

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19074

ABSTRACT: TThe extensive deployment of IoT-based electric power infrastructure monitoring systems has improved the intelligence and digitization of power systems. However, due to the uneven nature of systems, the suitability and performance vary greatly when monitoring a specific event, which increases the difficulty of efficient application of monitoring system. Constructing metadata of IoT-based electric power infrastructure monitoring system, can effectively enhance the data management and application capabilities of electric power infrastructure monitoring system, and improve more transparent, intelligent, and advanced energy services in smart cities.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under developmemt

Food and Agriculture

(NEW) ISO 5231:2022 Extended farm management information systems data interface (EFDI) — Concept and guidelines

🔗 URL: https://www.intertekinform.com/en-gb/standards/itu-t-y-suppl-76-09-2023--1344020_saig_itu_itu_3342182/

ABSTRACT: This document specifies an extensible communication system concept and defines rules for adding new functionalities to cover specific use cases.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-10

ITU-T Y.4466 (01/2020) Framework of smart greenhouse service

 **URL:** <https://handle.itu.int/11.1002/1000/14169>

ABSTRACT: This recommendation describes the reference architecture for the smart greenhouse service which provides and maintains optimal conditions for growing crops in greenhouse environment. The scope covered by the framework of smart greenhouse service includes the following issues: a) Overview of the smart greenhouse service; b) Reference architecture for smart greenhouse service; c) Interfaces for smart greenhouse service; d) Use Cases of smart greenhouse service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-01

(NEW) ITU-T Y.SFPP Reference framework for the smart farmland production platform

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19066

ABSTRACT: The development of smart farmland is an important issue of global concern. Smart farmland production has evolved from the primary stage to the advanced stage. A large number of manufacturers provide various types of sensors and subsystems. But these vertical subsystems are independent of each other, and the data and information are not effectively shared. In order to integrate these vertical subsystems and fully utilize the data and information, it is necessary to define a unified farmland production platform, which can effectively utilize resources, and support multiple applications. This platform can effectively integrate multiple subsystems, improve data usage efficiency, and support farmland production decision-making ability. It can provide comprehensive and clear guidance for the production of smart farmland, and can guide the development of the entire industry chain towards more advanced level. This draft new Recommendation introduces the farmland production platform, and specifies its requirements and reference framework.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.DM-SLF Conceptual data model of smart livestock farming service

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18470

ABSTRACT: Smart livestock farming (SLF) is a convergence service where Information and Communication Technologies (ICT) are applied into the livestock value chains. Apart from ICT technology, for a more productive and sustainable production smart livestock it is highly required to integrate various domain-specific information; examples of such information include precision livestock farming, management information systems, stockbreeding, and transportation. In order to integrate various domain-specific information, a well-defined data model is required. The well-defined data model can accelerate a number of new smart livestock related services as well as AI, data acquisition. Because it can facilitate automatization, interoperability and composability for the IoT applications and AI. For this purpose, this draft Recommendation defines data entities required for smart livestock service, their relationship, and then it addresses conceptual data model of smart livestock farming service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Water

ISO/IEC 30183 ED1 Internet of Things (IoT) – Addressing interoperability guidelines between heterogeneous underwater sensor networks (UWASNs) based on underwater delay and disruption tolerant network (U-DTN)

 **URL:** https://www.iec.ch/dyn/www/?p=103:38:204774363295796::FSP_ORG_ID_FSP_APEX_PAGE_FSP_PROJECT_ID:20486.23,108553

ABSTRACT: This document provides addressing interoperability guidelines between heterogeneous underwater acoustic sensor networks (UWASNs) based on underwater delay and disruption tolerant network (UDTN): - Architecture for heterogeneous UWASNs interworking; - U-DTN functions on heterogeneous UWASNs interworking; - Addressing interoperability guidelines between heterogeneous UWASNs.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.dt-IWCS Requirements and capability framework of digital twin for intelligent water conservancy system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18459

ABSTRACT: Water conservancy is always a hot topic and it is an important factor in urban and rural governance. Smart water conservancy system driven by digital twin is suggested to be implemented since it can support the intelligent monitor, control and regulate the usage and safety of water conservancy via the digital twin interaction between digital object and physical object of water conservancy. This draft Recommendation addresses requirements and capability framework of digital twin for intelligent water conservancy system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

SmartCity

(Updated) IEEE - P1451.99 Standard for Harmonization of Internet of Things (IoT) Devices and Systems

 **URL:** <https://standards.ieee.org/ieee/1451.99/11634/>

ABSTRACT: This standard defines an Internet of Things (IoT) TRusted Area Networking (TRAN) architecture, designated as IoT-TRAN, for harmonizing IEEE Std 1451 sensor networks, IoT and Industrial IoT (IIoT) systems. IoT-TRAN provides an interoperability framework, including communication and semantics, allowing data sharing and interoperability in a trusted environment in which security of messages, agreements between devices, life-cycle management, and ownership of devices are granted over a cloud-oriented, federated, and decentralized network of things. The standard is built on top of the eXtensible Messaging and Presence Protocol (XMPP). A set of technologies is identified, allowing different devices to interoperate regardless of underlying communication technology. Each such technology is built as a standardized extension to this open protocol. A gateway to IoT-TRAN is an infrastructural component identified as a binding providing technology-specific devices reachability and real-time transparent conversion with other devices using their respective IoT protocols. As part of the IEEE Std 1451 standard family, features like Transducer Electronic Data Sheet (TEDS) and IEEE Std 1451.0 Universally Unique

Identification (UUID) are leveraged in this standard to enhance the support of interfacing with IoT and IIoT systems.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-05

ITU-T Y.4201 (02/2018) High-level requirements and reference framework of smart city platforms

🔗 URL: <https://handle.itu.int/11.1002/1000/13388>

ABSTRACT: This recommendation presents the high-level requirements and reference framework of Smart City Platform (SCP). The SCP is a fundamental platform supporting all the services and applications of a smart city, with the objective to improve quality of life, provide urban operation and services for the benefit of the citizens while ensuring city sustainability. These high-level requirements include comprehensive and updated repositories of city information, infrastructure life-cycle management, inter-system communication, security support, maintenance support, controls of processor, decision making support, real-time dissemination of public information, resiliency, and interoperability.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-02

ITU-T Y.4461 (01/2020) Framework of Open Data in Smart Cities

🔗 URL: <https://handle.itu.int/11.1002/1000/14164>

ABSTRACT: This recommendation defines a conceptual model of Open Data in Smart Cities, in order to establish and foster a common understanding of Open Data in Smart Cities. The scope of this Recommendation includes: a) definition of Open Data in Smart Cities; b) benefits of Open Data in Smart Cities; c) fundamental requirements of Open Data in Smart Cities; d) conceptual model of Open Data in Smart Cities.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-01

(NEW) ITU-T Y.AI-DECCS Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17929

ABSTRACT: The maturity of Internet of things technology and the widespread deployment of network provide good infrastructure conditions to the application of AI at the device, edge and cloud for IoT and smart city. The requirements of AI models in IoT and smart city are dynamic, thus how to make AI system continuously and dynamically update, as well as infer and predict in real-time is essential to the application of AI in IoT and smart city. The device-edge-cloud collaborative service enables collaborative inference, and dynamic learning and updating of AI models on the device-edge-cloud architecture, so as to meet the needs of various current and future application scenarios. This recommendation specifies the Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-SAS Functional architecture of IoT-enabled smart accessibility service in smart communities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19617

ABSTRACT: Accessibility services are typically designed for public facilities or personal devices and depend on the ability of persons with disabilities to learn and adapt. These individuals must familiarize themselves with the functions of these services to select the ones that best meet their needs. With the continuous advancement of technologies such as the Internet of Things (IoT) and artificial intelligence, more intelligent applications, services, and devices are becoming integrated into smart community life. Unlike existing accessibility services, the use of these emerging technologies can significantly reduce the reliance on the learning abilities of persons with disabilities, enhancing their quality of life and ensuring their equal integration into the digital society. The Recommendation focuses on how to realize IoT-based smart accessibility services in the context of smart communities from the functional architecture perspective, mainly concentrating on the service support and application support layer and device layers. The users of the IoT-enabled smart accessibility service standardized in this standard include persons with disabilities, persons with age-related disabilities, and those with specific needs. It is beneficial for communities worldwide to initiate a new Recommendation - Functional architecture of IoT-enabled smart accessibility services in smart communities.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.IoT-SPA Functional architecture of smart park based on Internet of Things

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19067

ABSTRACT: This Recommendation provides the functional architecture of smart park based on Internet of Things, including the concept, goals and key components, the requirements and the functional architecture of the smart park based on Internet of Things.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.NCE.arch.EIoT Functional architecture enhancement with network capability exposure to support flexible QoS/QoE requirements from enterprise IoT services and applications

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17934

ABSTRACT: Compared to communication between humans, communication between machines in enterprise IoT services is much more challenging. Different customers may have different needs, for example, some manufacturing customers mainly use lots of sensors which needs high network capacity and delay insensitive, some manufacturing customers mainly use robots which needs high network reliability and delay sensitive, and some customers have multiple types of terminals in the same factory, such as sensors, cameras, robots and PLC controllers. In general, different services and applications requires different network capability exposure. Flexible QoS requirements and QoE requirements need to be considered as important elements for building functional architectures to support enterprise services. This draft new Recommendation specifies functional architecture enhancement with network capability exposure to support flexible QoS and QoE requirements, and functional entities and reference points of the proposed functional architecture.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.RA-FML Requirements and reference architecture of IoT and smart city & community service based on federated machine learning

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17924

ABSTRACT: The widespread popularity of data-driven services and applications transforms the IoT and Smart City & Community (SC&C) system from a traditional data collecting and transportation network into a more holistic architecture with AI-native data processing and service delivery capability. One of the key challenges in designing an AI-based architecture for large IoT and SC&C networking systems is to implement distributed data processing and learning across a large number of decentralized datasets that can be owned or managed by different entities such as cities, communities, buildings, devices, government and business entities. Federated machine learning (FML) is an emerging distributed AI framework that enables collaborative machine learning (ML) and model construction across decentralized datasets. It offers a viable solution for data-driven data learning and synthesis across a wide variety of entities across large SC&C networking systems. The main purpose of this recommendation is to provide a feasible and standardized solution for the IoT and SC&C relevant services and applications to use and deploy FML-enabled collaborative data learning across distributed and decentralized data sources.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.SA-DSC-SSC System architecture of digital supply chain for smart sustainable cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19618

ABSTRACT: Digital supply chain for SSC is a complex system engineering covering strategic transformation, organizational restructuring, function upgrading, data mining and technology introduction. For managers and stakeholders of SSC, the research, design, construction and management of digital supply chain are not systematic. Therefore, there is an urgent need to standardize a set of conceptual model and general reference framework covering the whole elements and the whole process of the digital supply chain. This recommendation presents system architecture of digital supply chain for SSC, expounds the constituent elements and interrelationship of digital supply chain from the aspects of device, network, service and application support, service function, security and management, and explain the construction method of digital supply chain for SSC.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.SC-DESMS Functional architecture of IoT-based distributed energy storage management system in smart cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19609

ABSTRACT: This proposal introduces the functional architecture of an IoT-based distributed energy storage(DES) management system for smart cities. It comprises the application layer, the service and application support layer, the network layer, and the device layer, covering specific needs in areas such as data collection, intelligent analysis, services, networking, equipment inspection, and security. Additionally, it defines the specific functional units of the IoT-based DES management system for smart cities. The draft recommendation provides guidance for the design, development, and application of IoT-based DES management systems for smart cities, promoting the global development of distributed energy storage and supporting the construction of smart cities.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.Sup_SUPS TU-T Y.4456 - Functional architecture of IoT based smart underground parking services

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19619

ABSTRACT: This proposal proposes to initiate a new work item on functional architecture of Internet of Things (IoT) based underground smart parking services (SUPS). This contribution discusses the important role of SUPS in urban traffic management. SUPS is based on IoT technology and its functional architecture is divided into four layers: device, network, support, and application, aiming to provide information services for both people and vehicles in underground parking lots to enhance user experience and management efficiency.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T YSTR.SemComm.IoT architectural Framework for Semantic Communication Services for IoT and Smart City & Community

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17960

ABSTRACT: This Technical Report specifies the requirements and architectural framework for semantic communication services in IoT and Smart City & Community.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.CL-EDM Energy data model for city-level energy management platform

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18463

ABSTRACT: This draft Recommendation specifies an energy data model of the city-level energy management platform (CL-EMP) to support building energy services and to share energy data with other city platforms for integrated city energy services in a smart sustainable city. It describes requirements, energy data model and energy data sharing. The energy data model defines what data is shared to support the integration of the CL-EMP and other city platforms. As a result, the model enables a variety of integrated city energy services in which multiple city sectors are linked.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.IoT-IIEC Framework of the integrated intelligent IoT service based on multi edge computing

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19628

ABSTRACT: Framework of the integrated intelligent IoT service based on multi edge computing

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.SmartBuilding-Integration: Framework for Smart Building Integration into Smart Cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19071

ABSTRACT: This Recommendation will set the framework for interoperability to ensure that different building systems can communicate with smart city functionalities. It will enable the seamless integration of smart buildings with broader smart city infrastructure. This Recommendation will provide guidelines for data exchange, communication protocols and system interfaces, allowing smart buildings to connect with transportation systems, utilities, emergency services, and other city-level services. By developing this Recommendation, cities can benefit from a harmonized approach to smart building implementation and advance the adoption of smart technology in the urban environment.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.Evaluation-dfp Quality evaluation framework of data as a factor of production for smart sustainable cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19644

ABSTRACT: At present, while many countries and cities worldwide recognize the importance of data as a factor of production and smart city initiatives, there exist disparities in the level of data quality evaluation and smart city maturity across different regions and municipalities. Thus, it is essential to develop standards and guidelines for evaluating the quality of data as a factor of production that underpin various smart city applications and services. Data plays a crucial role in smart cities, enabling data-driven decision-making, optimized urban planning, efficient resource allocation, and improved public services. However, the quality of data, such as completeness, accuracy, timeliness, consistency, and interoperability, can significantly impact the effectiveness and reliability of smart city solutions. This draft Recommendation focuses on the requirements for quality evaluation of data as a factor of production for smart sustainable cities. It will benefit city administrators, stakeholders, and citizens by ensuring the high quality of data across domains. By establishing comprehensive standards and best practices for evaluating data quality, this work item will facilitate the integration and harmonization of data from multiple sources, enhance the reliability of data-driven decision-making processes, and foster innovation and collaboration among smart city stakeholders. Evaluating and improving the quality of data is crucial for maximizing the potential of data, increasing operational efficiency, and creating a more livable, inclusive, and sustainable urban environment for citizens. This work item will ultimately contribute to the effective and efficient development of smart sustainable cities worldwide.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Social Community and Wellbeing

(NEW) ITU-T Y.cnce-IoT-arch unctional architecture of network capability exposure for smart hospital based on Internet of things

 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17894

ABSTRACT: In traditional hospitals, there might be some issues to be improved, such as low efficiency of medical care, poor service experience of patients and lack of management efficiency. Smart hospital is a new concept to provide digital medical treatment by automatic and remote services based on information and communication technologies, e.g. prevention and diagnosis of illness, treatment and nursing for patients. Smart hospitals have demands for high-precision positioning, and the service quality guarantee of all kinds of local services, which may require network capability exposure to support the mentioned requirements. With the support of network capability exposure, some new services such as high-precision positioning can be provided and better service experience can be achieved. This recommendation provides the functional architecture and functional entities of network capability exposure for smart hospital based on Internet of things. Related use cases are provided in the appendix.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

Buildings

(NEW) ITU-T Y.KCI-IM Requirements of knowledge construction and implementation for IoT management

 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19631

ABSTRACT: The Internet of Things (IoT) is characterized by a massive number of devices, complex and variable network structures, and highly specified and diverse service scenarios, which present significant challenges for IoT management. According to ITU-T Y.4000, the IoT management capabilities can be categorized into generic management capabilities and specific management capabilities. Essential generic management capabilities in the IoT include device management, local network topology management, traffic and congestion management, service management, etc. Specific management capabilities are closely coupled with application-specific requirements of different industries. Knowledge construction and implementation techniques can enhance the management efficiency and effectiveness of devices, networks and services within Internet of Things (IoT). Utilizing knowledge technologies can more comprehensively mine and extract hidden information from multimodal data collected from IoT devices, networks, and vertical industries. Through the process of knowledge construction and implementation, the massive data can be transformed into multidimensional and multi-layered associated knowledge, which can effectively support the various needs of IoT management along with other AI technologies.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

IHE Patient Care Device (PCD) Profiles

 **URL:** https://wiki.ihe.net/index.php?title=PCD_Profiles

ABSTRACT: System Architecture, Communications/Networking, Data and Information Management - The IHE PCD develops standards-based interoperability profiles that address specific integration problems within the domain charter.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** N/A

ISO/IEEE 11073 (2014) Health informatics – Point-of-care medical device communication.

 **URL:** <https://www.iso.org/standard/77338.html>

ABSTRACT: System Architecture - Personal Health Device (PHD) standards are a group of standards addressing the interoperability of personal health devices (PHDs) such as weighing scales, blood pressure monitors, blood glucose monitors and the like.

ISO/IEEE 11073 is a multi-part standard whose core, non-device-specific elements include, among others:

-  ISO/IEEE 11073-00103:2012 (Overview)
-  ISO/IEEE 11073-10101:2004 (Nomenclature)
-  ISO/IEEE 11073-10201:2018 (Domain information model)
-  ISO/IEEE 11073-10206 (Abstract information content model)
-  ISO/IEEE 11073-20101:2004 (Application Profile – Base Standard)
-  ISO/IEEE 11073-20601:2010 (Application profile – Optimized exchange protocol)
-  ISO/IEEE 11073-20702:2016 (Medical Devices Communication Profile for Web Services)

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-08

ISO/IEC 30180 ED1 Internet of Things (IoT) - Functional requirements to determine the status of self-quarantine through Internet of Things data interfaces

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,106630

ABSTRACT: This document specifies the functional requirements about the following items to figure out the status of self-quarantine through IoT data interfaces working over a set of hand-held devices, wristbands, and a management system: - Functional requirements for self-quarantine app and optional wristband at a self-quarantine place; - Functional requirements for self-quarantine management app and system at the management side; and - Functional requirements for the protection of the self-quarantine status and the privacy information.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

ITU-T Y.4908 (12/2020) Performance evaluation frameworks of e-health systems in the Internet of things

 **URL:** <https://handle.itu.int/11.1002/1000/14425>

ABSTRACT: This recommendation specifies performance evaluation frameworks of e-health systems in the IoT for e-health services. From information and communication technologies point of view, e-health services are classified. Performance evaluation factors applicable for e-health systems in the IoT are specified. Then performance evaluation frameworks are normalized for the classified e-health services. The scope of this recommendation includes: a) Classification of e-health services; b) Performance evaluation factors applicable for e-health systems in the IoT; c) Key performance frameworks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-12

(NEW) ITU-T Y.SPDM-reqts Requirements and a reference model of data for Smart Pest and Disease Management (SPDM) service

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19636

ABSTRACT: Smart Pest and Disease Management (SPDM) is an approach to managing pests and diseases in agriculture or other settings that emphasizes the use of multiple techniques in a coordinated manner. The goal of SPDM is to minimize the damage caused by pests and diseases while minimizing risks to human health, the environment, and non-target organisms. Existing pesticide control systems based on Internet of Things can minimize the impact of chemicals on human health as well as reduce labour but have difficulties in achieving optimal pest and disease control. In order to efficiently provide SPDM service by enabling sophisticated data analytics and the widespread adoption of AI-powered surveillance systems, a large amount of data is needed to be involved. However, this data is difficult to collect because of lack of meaningful existing data and lack of common data formats. In order to efficiently manage and analyze vast amounts of data and to create various services based on the analyzed data, a standardized data model including data collection and management system is required. In particular, compatibility of data generated and consumed by heterogeneous devices must be guaranteed to ensure interoperability between devices of heterogeneous vendors. However, the SPDM data model currently used in the market is vendor-specific, and thus interoperability between devices is not guaranteed. In other words, data sharing and real-time data communication between heterogeneous devices is not supported. For data interoperability, this draft Recommendation defines requirements and reference model of data for SPDM service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

■ Education Training and Learning

Horizontals & Verticals

Cloudwatch D3.6 Cloudwatch D3.6 Security and Interoperability Standards Status Report

📄 **URL:** https://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Security-and-Interoperability-Standards-Status-Report.pdf

ABSTRACT: This document provides a monitoring of the standards landscape, identifying necessary extensions and profiles, and identifying relevant standards groups for future engagement of the EU projects.

Through this deliverable Cloud WATCH2 is able to:

- 📄 Leverage input provided by finalized and on-going FP7 and H2020 projects to prepare and maintain a list of standards used by the different consortia. The list describes the level of adoption of each standard and the most common implementations.
- 📄 Identify contributions to existing and developing standards from the FP7 and H2020 projects.
- 📄 Provide evidence to the standardization community of identified gaps by analysing input from the above mentioned FP7 and H2020 projects.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2017-09

ETSI TR 103 534-1 Teaching Material: Part 1 (Security)

📄 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf

ABSTRACT: The document is based on the Security Report ETSI TR 103 533. It presents teaching material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2019-08

ETSI TR 103 534-2 Teaching Material: Part 2 (Privacy)

📄 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf

ABSTRACT: The document is based on the Privacy Report ETSI TR 103 591. It focuses on producing teaching material on privacy and to direct the reader to other materials that are available in order to gain a basic understanding on what is involved in the privacy concept that is especially relevant, also, for the IoT environment.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2019-10

ETSI TR 103 535 Guidelines for semantic interoperability in the industry

📄 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf

ABSTRACT: The document addresses the topic of semantic interoperability in the context of its potential usage by the industry in the development of IoT systems. The main objective of the document is to concretely foster the use of semantic interoperability in IoT by identify why it is important in industry

IoT projects, to analyse the advantages and drawback of the available solutions.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-10

(NEW) ITU-T Y.IoT-smartschool Requirements of IoT-based smart school management system

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19059

ABSTRACT: This Recommendation focuses on the utilization of IoT technologies in school management to improve intelligent level in school security, teaching assessment, academic affairs, and school life, ultimately increasing the effectiveness and efficiency of school management. By sensing, collecting, and identifying school related management information, combined with the appropriate usage of cloud computing and AI technologies, school administrations can achieve real-time monitoring, early warning, and actionable intelligence from a management issues, thereby ensuring the quality of education while safeguarding students' smart school life and life safety. The Recommendation provides overview, device requirements, network requirements, service and application support requirements, and application requirements of IoT-based smart school management system (SSMS).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup.IoT-SEDR Functional framework and capability for digital resources in smart education based on IoTs

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19069

ABSTRACT: This supplement specifies the functional framework and capabilities for digital resources in smart education that is defined in ITU-T Y.4485. This supplement provides the overview of digital resources in smart education, service and application of digital resources, sensing and acquisition capabilities of digital resources, services and application support capabilities, services integrate and data exchange capabilities of digital educational resources.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.CSDL Requirements and framework for crowdsourced system based on distributed learning

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18744

ABSTRACT: Building up distributed learning mode for crowdsourced system and enhance the crowdsourced service data security is important. The distributed learning mode can effectively solve the data security problem in the crowdsourcing process. The crowdsourced raw data will be computed on the distributed worker node and only encrypted intermediate computation result will be transferred to the crowdsourced platform. Besides, compared with the traditional crowdsourced systems utilizing the centralized computation mode, which was defined in ITU-T Y.4217, the realization of crowdsourced system based on distributed learning can also provide intelligent cooperation capabilities between crowdsourced resources and reduce bandwidth consumption and transmission time consumption. This recommendation specifies the requirements and framework for crowdsourced system based on distributed learning in order to solve the distributed model parallelism and data parallelism issues for complex crowdsourced task, crowdsourced nodes communication strategy under distributed learning, coordination mode of heterogeneous models and data.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Evaluation-SE Evaluation of capabilities for IoT-enabled frameworks of smart education

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19086

ABSTRACT: IoT-enabled smart education systems leverage extensive digitalization, interactive and smart services to substantially enhance learning experiences, teaching efficiency, and adaptability of content. The capabilities for these systems have direct impacts on the improvement of educational quality. The evaluation of these capabilities plays a significant role in effectively advancing the application of smart education and guiding the evolution of smart education system platforms. The establishment of comprehensive and unified key performance indicators for the assessment of the capabilities in IoT-enabled smart education can promote the widespread adoption of smart education and guide the evolution of smart education system platforms. This recommendation specifies the evaluation of capabilities for IoT-enabled frameworks of smart education. It provides the key performance indicators of capabilities evaluation based on the dimensions of user experience and engagement, digital information management, intelligent processing, rationality and reliability of information and algorithms, digital information sensing and acquisition for the smart education.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Energy

ISO/IEC TR 30148:2019 Internet of things (IoT) - Application of sensor network for wireless gas meters

 **URL:** <https://webstore.iec.ch/publication/63562>

ABSTRACT: ISO/IEC TR 30148:2019 describes:

-  the structure of wireless gas meter networks, and
-  the application protocol of wireless gas meter networks.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-10

■ Energy

Energy

(NEW) ITU-T Y.Fram-ssdp Requirements and framework of metaverse simulation service for disaster prevention in electric power facilities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19614

ABSTRACT: Electric power facilities are increasingly vulnerable to natural disasters exacerbated by global climate change, necessitating urgent action. However, conducting real emergency drills poses challenges due to the complexity of reproducing disaster scenarios, coordinating multi-party personnel collaboration across various agencies, enterprises, and sectors, and the associated high economic costs. The metaverse, an immersive digital environment integrating digital twins, augmented reality, virtual reality, and other digital technologies and information and communication technologies, offers a promising solution. It provides a robust simulation framework for disaster prevention in electric power facilities. This Recommendation specifies the requirements and reference framework of metaverse simulation service for disaster prevention in electric power facilities, which will help to optimize the emergency response strategies and improve the disaster prevention and mitigation capability for electric power facilities.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

SmartCity

(NEW) ITU-T Y.DEMC-fra Requirements and framework of IoT-based distributed energy resources management and control services

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19607

ABSTRACT: This Recommendation aims to achieve the goal of effective management and proactive interaction for distributed energy resources with complex and heterogeneous data in the IoT environment. The core content includes the main aggregation and interaction requirements and overall framework of distributed energy resources management and control services. This Recommendation fits the application scenarios of massive resources access and interaction in the IoT environment, and meets the business needs of distributed energy clusters to participate in power grid interaction, distributed local control, and resource security access, building a distributed, low-cost, and highly reliable power system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.IoT-PD Requirements of electric power data perception based on the Internet of Things

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19061

ABSTRACT: Driven by the global efforts to achieve carbon neutrality goals, the cities are accelerating their transformation towards intelligence, greenery, and low-carbon development. Electric power is the main form of energy consumption in cities, achieving electric power data's comprehensive perception and intelligent monitoring will become an important foundation to support smart cities sustainable development. The goal of this draft Recommendation differs from the existing relevant

standards of SDOs involved in IoT perception and IoT application in the electric power field. This draft Recommendation aims to address the challenges faced by new energy rapid development. It can fully leverage IoT technical characteristics and propose a framework and requirements for electric power data perception services. It also effectively fills the standard gap, provides technical means and basis for electric power supply departments to comprehensively grasp distributed energy data, and further promotes smart cities sustainable development.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.PGComNet-Reqts Requirements of IoT-based power grid communication network

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18748

ABSTRACT: The IoT-based power grid communication network provides bidirectional data interaction in all phases of power grid operations, including electric power generation, transmission, distribution and consumption. It is an effective means to achieve comprehensive awareness of power grid status, to enable human-computer interaction and ubiquitous access of the IoT devices of the power grid. This Recommendation specifies the requirements of IoT-based power grid communication network.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

■ Environment

Horizontals & Verticals

(Updated) ISO/IEC 30179 ED1 Internet of Things (IoT) - Overview and general requirements of IoT system for ecological environment monitoring

🔗 **URL:** https://www.iec.ch/dyn/www/?p=103:38:204774363295796:::FSP_ORG_ID FSP_APEX_PAGE_FSP_PROJECT_ID:20486,23,105254

ABSTRACT: This document specifies the Internet of Things system for ecological environment monitoring in the following: — System infrastructure and system entities of the IoT system for ecological environment monitoring for natural entities such as air, water, soil, living creatures; and — The general requirements of the IoT system for ecological environment monitoring.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2023-01

(NEW) ITU-T Y.IoT-soil Requirements of IoT-based soil environmental protection and remediation

🔗 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19058

ABSTRACT: Soil is vitally important for both human well-being and the health of our planet. It serves as the foundation for maintaining ecological balance, ensuring food safety, promoting sustainable development, and protecting against health risks. By utilizing technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), it is possible to achieve integrated space-air-ground soil environmental monitoring and data-driven intelligent decision-making for soil protection and remediation strategies. This Recommendation provides overview, device requirements, network requirements, service support and application support requirements, and application requirements of IoT-based Soil Environmental Protection and Remediation (SEPR).

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** Under development

SmartCity

ITU-T Y Suppl. 27 (01/2016) ITU-T Y.4400 series – Smart Sustainable Cities – Setting the framework for an ICT architecture

🔗 **URL:** <https://handle.itu.int/11.1002/1000/12753>

ABSTRACT: The scope of this standardization work is to describe the ICT architecture development framework of SSC and provide corresponding architecture views and guides with the key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but is not limited to: a) ICT Architecture development methodology; b) SSC ICT Architecture development methodology; c) SSC ICT architecture framework; d) Guidelines for the SSC ICT architecture; e) SSC ICT Architecture interfaces.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2016-01

ITU-T Y Suppl. 28 (01/2016) ITU-T Y.4550 series – Smart Sustainable Cities – Integrated management for smart sustainable cities

 **URL:** <https://handle.itu.int/11.1002/1000/12754>

ABSTRACT: The scope of this standardization work is to provide a technical proposal for integrated management, which can be followed by any municipality interested in improving the management of its infrastructure, operations and citizen interactions, and in addressing critical urban challenges – such as security, criminality, pollution, traffic congestion, inadequate infrastructure, and response to natural hazards. Specifically, the proposed new Supplement covers, but is not limited to: a) Resources, challenges and technologies of integrated management for smart sustainable cities; b) Integrated management for smart sustainable cities; c) Service framework.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-01

ITU-T Y Suppl. 29 (01/2016) ITU-T Y.4250 series – Smart Sustainable Cities – Multi-service infrastructure in new-development areas

 **URL:** <https://handle.itu.int/11.1002/1000/12755>

ABSTRACT: The scope of this standardization work is to describe the various infrastructures for a smart sustainable city in a new-development area with a key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but is not limited to: a) Smart Sustainable Building Utility Services; b) SSC (Smart Sustainable Cities) Utility Service Requirements; c) Opportunities for sharing infrastructure at street level.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-01

ITU-T Y Suppl. 30 (01/2016) ITU-T Y.4250 series – Smart Sustainable Cities – Overview of smart sustainable cities infrastructure

 **URL:** <https://handle.itu.int/11.1002/1000/12756>

ABSTRACT: The scope of this standardization work is to provide a technical overview on infrastructure related to information and communications technology (ICT), specific to developing smart sustainable cities (SSC) with the key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but not limited to: a) SSC stakeholders; b) ICT infrastructure for SSC; c) Physical infrastructure and its intelligent upgrading; d) Planning deployment of ICT infrastructure for SSC; e) Example of open access network for smart cities; f) Strategies for the deployment of digital/ICT infrastructure.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-01

■ Food and Agriculture

Food and Agriculture

(NEW) ITU-T Y.SCGMS Requirements and capabilities of IoT-based smart crop growth monitoring system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19602

ABSTRACT: Building up the IoT-based smart crop growth monitoring system is essential to modern agricultural development. Traditional monitoring of crop growth often relies on manual inspection and sampling, which is both inefficient and susceptible to human subjective factors, potentially leading to bias in the monitoring results. Besides, the research and application of crop growth monitoring technology is relatively lagging behind, and the effective linkage with agricultural environment monitoring technology also appears to be insufficient. Therefore, it is necessary to define the IoT-based smart crop growth monitoring system including device layer, network layer, service and application support layer and application layer, from an ICT perspective. The IoT-based smart crop growth status monitoring system can provide real-time monitoring, intelligent analysis of crop growth status, yield prediction and guidance for the growth process. This system can enhance the efficiency of agricultural production, optimize the allocation of resources, reduce production costs, minimize risky losses, and ultimately increase grain yield and quality. It provides solid technical support for the precise management and efficient production of modern agriculture and promotes the sustainable development of agriculture.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

■ Industry and Business

Horizontals & Verticals

3GPP TR 38.825 V16.0.0 Study on NR industrial Internet of Things (IoT)

🔗 **URL:** <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3492>

ABSTRACT: The present document is related to Study on NR Industrial Internet of Things (IoT). The document describes NR enhancements to Ultra Reliable Low Latency Communications (URLLC) and Industrial Internet of Things, which were analysed as part of the study such as data duplication and multi-connectivity enhancements, solutions for UL/DL intra-UE prioritization/multiplexing and Time Sensitive Networking support (TSN) via accurate reference timing delivery, QoS/scheduling enhancements for TSN traffic types, Ethernet header compression. The Technical Report captures also performance analysis of TSN requirements.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2019-03

(Updated) All Industrial Internet Architecture

🔗 **URL:** <https://en.aii-alliance.org/uploads/2/20220302/dda5a36a9ff8ffa8a8415914f223ec66.pdf>

ABSTRACT: The industrial internet involves all segments and all entities of industry and ICT fields such as internet and is evolving into an entirely new and complicated eco-system. Discrepancies in understanding industrial internet may lead to divergences in choosing technologies and standard roadmaps, which will affect the interoperability and raise deployment costs. For this reason, Alliance of Industrial Internet (All) launched the study on the industrial internet architecture, and developed this "Industrial Internet Architecture" report (version 1.0) based on summarizing development practices at both home and abroad, which introduces the connotations, targets, architecture, key elements and trends of the industrial internet. It aims to drive industry community to reach a wide consensus on industrial internet, to provide references and guidance to All's works, such as the technical innovation, standard development, test and verification, application practices, etc. of industrial internet by taking the architecture as a traction, and to boost the healthy and fast development of industrial internet.

📄 **DOCUMENT TYPE:** Whitepaper

📅 **PUBLICATION DATE:** 2016-12

GSI EPCIS EPC Information Services (EPCIS) Standard, v1.2 (2016)

🔗 **URL:** <https://ref.gsi.org/standards/epcis/>

ABSTRACT: Data and Information Management - Enable trading partners to share information about the physical movement and status of products as they travel throughout the supply chain

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2022-06

(NEW) IEC 63278-2 ED1 Asset Administration Shell for Industrial Applications – Part 2: Information meta model

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:502560904033881:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109017

ABSTRACT: This document provides a specification of the Asset Administration Shell for Industrial Applications, focusing in Part 2 on the Information meta model.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

(NEW) IEC 63278-4 ED1 Asset administration shell for industrial applications - Part 4: Use cases and modelling examples

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:508054836884348:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,116472

ABSTRACT: This document provides a specification of the Asset administration shell for industrial applications, focusing in Part 4 on Use cases and modelling examples.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

(NEW) IEC 63278-5 ED1 Asset Administration Shell for industrial applications – Part 5: Interfaces

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:508054836884348:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,121674

ABSTRACT: This document provides a specification of the Asset administration shell for industrial applications, focusing in Part 5, on Interfaces.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

ISO/IEC 30162:2022 Internet of things (IoT) - Compatibility requirements and model for devices within Industrial IoT systems

 **URL:** <https://webstore.iec.ch/publication/63489>

ABSTRACT: ISO/IEC 30162:2022 specifies network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of:

- a) data transmission protocols interaction;
- b) distributed data interoperability & management;
- c) connectivity framework;
- d) connectivity transport;
- e) connectivity network;
- f) best practices and guidance to use in IIoT area

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: 2022-02

ISO/IEC 30163:2021 System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services

 **URL:** <https://www.iso.org/standard/53283.html>

ABSTRACT: ISO/IEC 30163:2021 specifies the system requirements of an Internet of Things (IoT)/ Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including: - System infrastructure that describes functional components; - System and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.; - Performance requirements and performance specifications of each functional component; - Interface definition of the integrated platform system. This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-03

(NEW) ITU-T Y.CIP Requirements of metaverse-based emergency response in chemical industrial parks

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19637

ABSTRACT: Chemical Industrial Parks (CIPs) are specialized zones which contains a diverse range of chemical factories. Leveraging exceptional infrastructure and shared services within the parks, CIPs aim to streamline operations and facilitate efficient business operations within the chemical sector. This management style means to enhance energy and resource efficiency, environmental performance, and economic competitiveness. However, as a high concentration of those hazards in a limited space, CIPs may cause a chain reaction in the event of an accident. Once an accident happens, it may result in large scale loss of life and property. Thus, emergency response in CIPs requires more proactive measures to prevent accidents. This document focuses on establishing a set of comprehensive application requirements designed to mitigate risks and strengthen emergency response capabilities within CIPs. It details overview of emergency response in CIPs, requirements of metaverse-based emergency response in CIPs, and framework of metaverse-based emergency response in CIPs. It provides guidance to improve situational awareness, response times, and overall safety through more dynamic and interactive emergency response.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

oneM2M TR-0018-V-4.0.0 Industrial Domain Enablement

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=29334>

ABSTRACT: This oneM2M Technical Report collects the use cases of the industrial domain and the requirements needed to support them collectively. Furthermore, the Technical Report also identifies necessary technical work needing to be addressed while enhancing future oneM2M specifications.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-09

UN P1095 E Negotiation

 **URL:** <https://uncefact.unece.org/display/uncefactpublic/E+Negotiation>

ABSTRACT: Data and Information Management - Semantics of the negotiation process and exchanged information prior to the exchange of purchase order information

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** 2022-01

Manufacturing

IEC 61987-1:2006 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 1: Measuring equipment with analogue and digital output

 **URL:** <https://webstore.iec.ch/publication/6225>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2006-12-14

IEC 61987-10:2009 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 10: List of Properties (LOPs) for Industrial-Process Measurement and Control for Electronic Data Exchange - Fundamentals

 **URL:** <https://webstore.iec.ch/publication/6227>

ABSTRACT: IEC 61987-10:2009 provides a method of standardizing the descriptions of process control devices, instrumentation and auxiliary equipment as well as their operating environments and operating requirements (for example, measuring point specification data). The aims of this standard are:

-  to define a common language for customers and suppliers through the publication of Lists of Properties (LOPs),
-  to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations,
-  to reduce transaction costs.

The standard describes industrial-process device types and devices using structured lists of properties and makes the associated properties available in a component data dictionary. This bilingual version, published in 2010-11, corresponds to the English version.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2009-07-23

IEC 61987-11:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 11: List of properties (LOPs) of measuring equipment for electronic data exchange - Generic structures

 **URL:** <https://webstore.iec.ch/publication/32275>

ABSTRACT: 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”.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-12-15

IEC 61987-12:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 12: Lists of properties (LOPs) for flow measuring equipment for electronic data exchange

 **URL:** <https://webstore.iec.ch/publication/24401>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-03-23

IEC 61987-13:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 13: Lists of properties (LOP) for pressure measuring equipment for electronic data exchange

 **URL:** <https://webstore.iec.ch/publication/24400>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-03-23

IEC 61987-14:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 14: Lists of properties (LOP) for temperature measuring equipment for electronic data exchange

 **URL:** <https://webstore.iec.ch/publication/24637>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-04-26

IEC 61987-15:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 15: Lists of properties (LOPs) for level measuring equipment for electronic data exchange

 **URL:** <https://webstore.iec.ch/publication/26177>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-11-08

IEC 61987-16:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 16: List of properties (LOPs) for density measuring equipment for electronic data exchange

 **URL:** <https://webstore.iec.ch/publication/34265>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-12-15

(Updated) IEC 61987-32:2024 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

 **URL:** <https://webstore.iec.ch/publication/63344>

ABSTRACT: This part of IEC 61987 provides an operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for I/O modules and a device list of properties (DLOP) for the description of a range of I/O module types.

The structures of the OLOP and the DLOPs 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.

Aspects other than the OLOP, needed in different electronic data exchange processes and described in IEC 61987-10 and IEC 61987-11, are published in IEC 61987-92.

The locations of the libraries of properties and of blocks used in the LOPs concerned are listed in Annex C and Annex D.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-06

IEC 61987-41 ED1 Generic structures of List of Properties (LOP) of Process Analyzer Technology (PAT) measuring devices for electronic data exchange

 **URL:** https://www.iec.ch/ords/f?p=103:38:401030832849310:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,107355

ABSTRACT: This document specifies the Generic structures of List of Properties (LOP) of the Process Analyzer Technology (PAT) measuring devices used for electronic data exchange.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

IEC 61987-92:2018 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 92: Lists of properties (LOP) of measuring equipment for electronic data exchange - Aspect LOPs

 **URL:** <https://webstore.iec.ch/publication/33096>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-06-05

IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

 **URL:** <https://webstore.iec.ch/publication/7030>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2010-11

IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

 **URL:** <https://webstore.iec.ch/publication/34421>

ABSTRACT: IEC 62443-4-2:2019 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C (component). As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs): a) identification and authentication control (IAC), b) use control (UC), c) system integrity (SI), d) data confidentiality (DC), e) restricted data flow (RDF), f) timely response to events (TRE), and g) resource availability (RA). These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-02

IEC 62832-1:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 1: General principles

 **URL:** <https://webstore.iec.ch/publication/65858>

ABSTRACT: 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).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

IEC 62832-2:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 2: Model elements

 **URL:** <https://webstore.iec.ch/publication/60214>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

IEC 62832-3:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 3: Application of Digital Factory for life cycle management of production systems

 **URL:** <https://webstore.iec.ch/publication/60277>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

IEC 62872-2:2022 Industrial-process measurement, control and automation - Part 2: Internet of Things (IoT) - Application framework for industrial facility demand response energy management

 **URL:** <https://webstore.iec.ch/publication/63419>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-02

(Updated) IEC 63278-1 ED1 Asset Administration Shell for industrial applications – Part 1: Asset Administration Shell structure

 **URL:** <https://webstore.iec.ch/publication/65628>

ABSTRACT: IEC 63278-1:2023 defines the structure of a standardized digital representation of an asset, called Asset Administration Shell (AAS). The Asset Administration Shell gives uniform access to

information and services.

The purpose of the Asset Administration Shell is to enable two or more software applications to exchange information and to mutually use the information that has been exchanged in a trusted and secure way.

This document focuses on Asset Administration Shells representing assets of manufacturing enterprises including products produced by those enterprises and the full hierarchy of industrial equipment. It defines the related structures, information, and services.

The Asset Administration Shell applies to:

- any type of industrial process (discrete manufacturing, continuous process, batch process, hybrid production);
- any industrial sector applying industrial-process measurement, control and automation;
- the entire life cycle of assets from idea to end of life treatment;
- assets which are physical, digital, or intangible entities.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2023-12-14

IEC 63278-3 ED1 Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells

URL: https://www.iec.ch/dyn/www/f?p=103:38:731054763917753::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23109075

ABSTRACT: This specification describes the Asset Administration Shell for Industrial Applications, focusing on Part 3: Security provisions for Asset Administration Shells.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(Updated) IEC 63339:2024 ED1 Unified reference model for smart manufacturing

URL: <https://webstore.iec.ch/publication/67119>

ABSTRACT: IEC 63339:2024 specifies the unified reference model for smart manufacturing (URMSM) using a terminology and structure, and establishes criteria for creating reference models, as specializations, that support smart manufacturing. The terminology and structure comprise a set of common modelling elements, their associations, and conformance criteria. These common modelling elements address aspects and perspectives of products and production and their lifecycle considerations.

The URMSM enables an approach for creating multiple models based upon a reference model that is sufficient for understanding significant relationships among entities involved in smart manufacturing (SM) and for the development of standards and other specifications.

The URMSM specifications in this document accommodate consistent, coherent, compatible specializations for relevant aspects of manufacturing systems consisting of equipment, products, and services within the domain of manufacturing. Provisions of this document are applicable for a new smart manufacturing reference model (SMRM) or elaboration of existing SMRM capabilities, for example, improving capabilities for analysis of opportunities and synthesis of technological advances, and improving interoperability of new and existing systems.

This document is not intended to prescribe interoperability considerations or data schemas of models. Standardization of content relative to models will be the subject of other standards and texts specific to those model domains.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-10-10

(Updated) IEC 63376 ED1 INDUSTRIAL FACILITY ENERGY MANAGEMENT SYSTEM (FEMS) – Functions and Information Flows

 **URL:** <https://webstore.iec.ch/publication/67721>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-02-19

IEC TR 63283-1:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 1: Terms and definitions

 **URL:** <https://webstore.iec.ch/publication/66314>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-03

(NEW) IEC TR 63283-2:2022 ED1 Industrial-process measurement, control and automation - Smart manufacturing - Part 2: Use cases

 **URL:** <https://webstore.iec.ch/publication/66315>

ABSTRACT: IEC TR 63283-2:2022(EN) has the goal of analyzing the impact of “Smart Manufacturing” on the daily operation of an industrial facility. It focusses on the perspective of automation and control of the production system, but also on the supporting processes of ordering, supply chain management, design, engineering and commissioning, operational technology, life cycle management, and resource management.

These recommendations are accomplished on the basis of several carefully selected use cases that are familiar to manufacturing industry. Therefore, each use case is described, followed by an analysis of the possible influence of “Smart Manufacturing” and the assessment of the impact on existing and future standardization.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-03-09

(NEW) IEC TR 63283-3:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 3: Challenges for cybersecurity

 **URL:** <https://webstore.iec.ch/publication/66316>

ABSTRACT: IEC TR 63283-3:2022(E) identifies challenges which apply to the engineering of a smart manufacturing facility related to cybersecurity.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-03-09

(NEW) IEC TR 63283-5:2024 Industrial-process measurement, control and automation – Smart manufacturing – Part 5: Market and innovation trends analysis

 **URL:** <https://webstore.iec.ch/en/publication/71399>

ABSTRACT: IEC TR 63283-5:2024 describes the market and innovation trend analysis affecting smart manufacturing (SM). The market and innovation trends will influence the evolution of smart manufacturing and it will be important to have good insights on these trends. Specific aspects of the market trends are the evolution of the business cases that is assumed to highlight new supplier chain models, new revenue streams, new customer services, and/or new customer segments.

The document will address the following topics:

-  **Market watch:** Identify the important, likely, and/or disruptive market trends (e.g. mass customization) from an end-to-end perspective, which impact smart manufacturing topics/aspects. This includes the end-user, producers, supply chain, regulators, etc.
-  **Business model watch:** Identify the new business model trends from an end-to-end perspective, which impact smart manufacturing.
-  **Technological watch:** Identify the important, likely, and/or disruptive innovations (AI chipsets, 6G, quantum computing, etc.) describing the impacted smart manufacturing topics/aspects; this topic will focus on those technologies that are still under development but is assumed to influence (or is assumed to be influenced by) smart manufacturing.

There are many more new trends which are used in SM. In this document, only some frequently discussed trends are presented. Some technologies are considered to have priority according to their maturity.

This work will focus on how they can be used in SM.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-11-20

IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

 **URL:** <https://webstore.iec.ch/publication/7029>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2009-07

IEC TS 62872-1:2019 Industrial-process measurement, control and automation - Part 1: System interface between industrial facilities and the smart grid

 **URL:** <https://webstore.iec.ch/publication/62884>

ABSTRACT: 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).

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2019-06

ISO/IEC 30162:2022 Internet of Things (IoT) - Compatibility requirements and model for devices within Industrial IoT systems

 **URL:** <https://webstore.iec.ch/publication/63489>

ABSTRACT: ISO/IEC 30162:2022 specifies network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of: a) data transmission protocols interaction; b) distributed data interoperability & management; c) connectivity framework; d) connectivity transport; e) connectivity network; f) best practices and guidance to use in IIoT area.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: February 2022

ISO/IEC 30163:2021 Internet of Things (IoT) - System requirements of IoT and sensor network technology-based integrated platform for chattel asset monitoring

 **URL:** <https://webstore.iec.ch/publication/63491>

ABSTRACT: ISO/IEC 30163:2021 specifies the system requirements of an Internet of Things (IoT)/ Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including: a) System infrastructure that describes functional components; b) System and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.; c) Performance requirements and performance specifications of each functional component; d) Interface definition of the integrated platform system. This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: March 2021

ISO 20140-5:2017 Automation systems and integration - Evaluating energy efficiency and other factors of manufacturing systems that influence the environment - Part 5: Environmental performance evaluation data

 **URL:** <https://webstore.iec.ch/publication/34147>

ABSTRACT: ISO 20140-5:2017 specifies the types of environmental performance evaluation (EPE) data, including their attributes, which can be used for evaluating the environmental performance

of manufacturing systems based on the general principles described in ISO 20140-1. It also provides recommendations for mapping the EPE data on to information models specified by IEC 62264. ISO 20140-5:2017 applies to discrete, batch and continuous manufacturing. ISO 20140-5:2017 is applicable to entire manufacturing facilities and to parts of a manufacturing facility. ISO 20140-5:2017 specifically excludes from its scope the syntax of the data and information models, the protocols to exchange data models, the functions that can be enabled by data models, and the activities in Level 1 and Level 2. The scope of ISO 20140-5:2017 also includes indicating the differences among various data and information models and the differences among various representations of environmental performance by actual data. ISO 20140-5:2017 refers to the semantics of the structured data and information models used by communication protocols. The semantics explain the meaning of the attributes and of the context information. The following are outside the scope of ISO 20140-5:2017: a) product life cycle assessment; b) EPE data that are specific to a particular industry sector, manufacturer or machinery; c) acquisition of data; d) the activity of data communication.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-04

ISO/IEC TR 30166:2020 Internet of Things (IoT) - Industrial IoT

🔗 URL: <https://webstore.iec.ch/publication/64321>

ABSTRACT: ISO/IEC TR 30166:2020 (E) describes the following: a) general Industrial IoT (IIoT) systems and landscapes which outline characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure and a listing of standardizing organisations, consortia and open-source communities with work on all aspects on IIoT; b) considerations for the future standardization perspective of IIoT including risk analysis, new technologies and identified collaboration.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-04

oneM2M TR-0049-V-0.3.0 Industrial Domain Information Model Mapping & Semantics Support

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30216>

ABSTRACT: Industrial Domain Information Model Mapping & Semantics Support.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-05

(NEW) ITU-T Y.4228 (ex Y.IIoT-infra-SM-fr) Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17949

ABSTRACT: Industrial Internet of things (IIoT) infrastructure for smart manufacturing refers to common facilities based on IoT that support smart manufacturing in industries or sectors. It is independent from the products and production process in specific enterprises. This Recommendation provides requirements and reference framework of the IIoT infrastructure capabilities for smart manufacturing to help service providers implementing their system according to the needs of smart manufacturing, and merge existing and newly developed IIoT infrastructure, in order to give the stakeholders of smart manufacturing guidance for their applications.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development: Approved on 2024-08-29

ISO/IEC TR 22560:2017 Information technology - Sensor network - Guidelines for design in the aeronautics industry: Active air-flow control

 **URL:** <https://webstore.iec.ch/publication/60608>

ABSTRACT: This Technical Report describes the concepts, issues, objectives, and requirements for the design of an active air-flow control (AFC) system for commercial aircraft based on a dense deployment of wired and wireless sensor and actuator networks. It focuses on the architecture design, module definition, statement of objectives, scalability analysis, system-level simulation, as well as networking and implementation issues using standardized interfaces and service-oriented middleware architectures.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-10

(Updated) IETF RFC 9365 IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases

 **URL:** <https://datatracker.ietf.org/doc/rfc9365/>

ABSTRACT: This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation systems (ITS).

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-12

(NEW) ITU-T Y.4232 (ex Y.IoT-RTPS) Requirements, capabilities and use cases of Internet of Things infrastructures in roadside traffic perception system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18461

ABSTRACT: RTPS, which refers to roadside traffic perception system, is a system composed of Internet of Things (IoT) infrastructures, including sensing devices, cloud facilities, intelligent traffic lights and smart traffic signs. By utilizing IoT technologies, roadside traffic perception system (RTPS) can enhance traffic safety and efficiency with capabilities of its components. To enhance traffic safety and efficiency, IoT infrastructures in RTPS need to collaborate with each other using IoT technologies. Therefore, common and specific requirements and capabilities for IoT infrastructures are described in this recommendation. Use cases of RTPS are also given in the appendix.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Determined on 2024-07-12

(NEW) ITU-T Y.4506 (ex Y.DRI-arch) Reference architecture for the interworking of autonomous urban delivery robots

 **URL:** <https://www.itu.int/rec/T-REC-L.1480-202212-1>

ABSTRACT: This Recommendation is to define the reference architecture for autonomous delivery robots based on the ITU-T Y.4607 that interwork with delivery robot service provider, user devices, and urban infrastructure to facilitate the delivery of goods without human intervention.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development: Determined on 2024-07

oneM2M TR-0055-3GPP_V2X_Interworking-V0_5_0 3GPP V2X Interworking

URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30468>

ABSTRACT: The document is a study of interworking between oneM2M Architecture and 3GPP V2X architecture so that oneM2M can support V2X service for the benefit of IoT applications.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2019-07

oneM2M-TR-0058-V-0.0.1: Railway Domain Enablement

URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28240>

ABSTRACT: This Technical Report investigates how to enable oneM2M system working in the railway vertical domain. This TR includes use cases, studies on essential features and summaries of other standards organizations on the railway vertical domain for the next oneM2M release(s) which considers and supports railway domain devices and services.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2018-12

oneM2M-TS-0036-V-0.0.1 Advanced Vehicular Domain Enablement

URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=24640>

ABSTRACT: Advanced Vehicular Domain Enablement.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2017-11

oneM2M-TR-0026-V-4.8.0 Vehicular Domain Enablement

URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31410>

ABSTRACT: This oneM2M Technical Report examines how the current oneM2M System can be used in the Vehicular Domain and includes a study of advanced features which the future oneM2M release(s) could support for this vertical domain.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2019-12

ISO/IEC 30140-1:2018 Information technology - Underwater acoustic sensor network (UWASN) - Part 1: Overview and requirements

 **URL:** <https://webstore.iec.ch/publication/60609>

ABSTRACT: ISO/IEC 30140-1:2018(E) This part of ISO/IEC 30140 provides a general overview of underwater acoustic sensor networks (UWASN). It describes their main characteristics in terms of the effects of propagation variability and analyses the main differences with respect to terrestrial networks. It further identifies the specificities of UWASN and derives some specific and general requirements for these networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-02

■ Information Processing

Horizontals & Verticals

ETSI TS 103 779 SmartM2M; Requirements and Guidelines for cross-domain data usability of IoT devices

 **URL:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103779/01.01.01_60/ts_103779v010101p.pdf

ABSTRACT: This specification defines minimum requirements for data and services usability on professional and general public IoT devices and platforms, whether they are critical or not. It constitutes a horizontal cross-domain specification encompassing these requirements.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-05

ISO/IEC 19637:2016 Information technology - Sensor network testing framework

 **URL:** <https://webstore.iec.ch/publication/59623>

ABSTRACT: ISO/IEC 19637:2016 specifies: a) testing framework for conformance test for heterogeneous sensor networks; b) generic services between test manager (TMR) and test agent (TA) in the testing framework; and c) guidance for creating testing platform and enabling the test of different sensor network protocols.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-12

ISO/IEC TR 22417:2017 Information technology - Internet of things (IoT) - IoT use cases

 **URL:** <https://webstore.iec.ch/publication/60605>

ABSTRACT: This technical report identifies IoT scenarios and use cases based on real-world applications

and requirements. The use cases provide a practical context for considerations on interoperability and standards based on user experience. They also clarify where existing standards can be applied and highlight where standardization work is needed.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-11

(NEW) ITU-T YSTR.DIC Reference framework for distributed intelligent computing based on IoT

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19638/en

ABSTRACT: With the advancement of artificial intelligence application based on IoT, it introduces new features like ubiquitous intelligence perception, cloud-edge collaborative computing, distributed machine learning, and more. Physical computing resources are required to match the new intelligent IoT characteristics of terminal intelligence, especially for the IoT ubiquitous intelligence and distributed intelligence. It is necessary to have a computing architecture that is consistent with the development of the intelligent computing for Internet of Things. This technical report describes the status of the distributed intelligent computing (DIC) based on IoT. It also specifies gaps and challenges in existing work, as well as the reference framework and typical functional entities which would support the DIC.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.DT-SSC-CVP Classification of visualization precision levels for digital twin systems in smart sustainable cities

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19645

ABSTRACT: Digital twin technology has become a crucial component of smart city systems, and enabling urban planners and managers to simulate, analyze, and predict various scenarios of urban development by creating virtual replicas of the physical urban environment, offering intuitive tools for management and decision-making. Its foundation lies in providing a 3D model representation of objects in the physical world in digital space. However, the precision of 3D model representation varies in different digital twin systems, which equates to different precision levels of visualization for digital twin systems. This Recommendation established a unified digital twin visualization precision levels classification framework, which can assist decision makers identify the general requirements that different precision levels should meet, choose appropriate precision levels for the construction of digital twin systems, avoid unnecessary consumption of resource and cost. This can also promote the interoperability and comparability between different systems and projects.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

oneM2M TR-0006-Study_of_Management_Capability_Enablement-V0_5_1 Study of Management Capability Enablement Technologies for Consideration

🔗 URL: https://onem2m.org/images/files/deliverables/TR-0006-Study_of_Management_Capability_Enablement-V0_5_1.doc

ABSTRACT: The present document describes and collects the state-of-art of the existing technologies on management capability, evaluates if the technologies can match the requirements defined in oneM2M, analyzes how the technologies can leverage the design of the architecture of oneM2M.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2015-04

ISO/IEC 30140-2:2017 Information technology - Underwater acoustic sensor network (UWASN) - Part 2: Reference architecture

 **URL:** <https://webstore.iec.ch/publication/60610>

ABSTRACT: This part of ISO/IEC 30140 provides an underwater acoustic sensor network (UWASN) conceptual model by identifying and defining three domains (application domain, network domain and UWASN domain). It also provides multiple reference architecture views consistent with the requirements defined in ISO/IEC 30140-1 (systems reference architecture, communication reference architecture and information reference architecture). For each view, related physical and functional entities are described.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-10

ISO/IEC 30140-3:2018 Information technology - Underwater Acoustic Sensor Network (UWASN) - Part 3: Entities and interfaces

 **URL:** <https://webstore.iec.ch/publication/60611>

ABSTRACT: The 30140 series provides general requirements, reference architecture and high-level interface guidelines supporting interoperability among underwater acoustic sensor networks (UWASNs). Part 3 provides descriptions for the entities and interfaces of the UWASN reference architecture.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-07

ISO/IEC 30140-4:2018 Information technology - Underwater Acoustic Sensor Network (UWASN) - Part 4: Interoperability

 **URL:** <https://webstore.iec.ch/publication/60612>

ABSTRACT: The ISO/IEC 30140 series provides general requirements, reference architecture and high-level interface guidelines supporting interoperability among underwater acoustic sensor networks (UWASNs). Part 4 provides information on interoperability requirements among entities within a UWASN and among various UWASNs.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-07

■ Infrastructure

Horizontals & Verticals

(NEW) 3GPP TR 28.841 V18.0.1 Study on management aspects of Internet of Things (IoT) Non-Terrestrial Networks (NTN) enhancements (Release 18)

📎 URL: https://www.3gpp.org/ftp/Specs/archive/28_series/28.841/28841-i01.zip

ABSTRACT: The present document studies on management aspects of IoT NTN enhancements. It investigates specific IoT NTN related parameters which should be considered by O&M, investigates NRM enhancement, performance measurement and related new KPIs of IoT NTN. It studies the key issues associated with service and network management of IoT NTN enhancements (whether as NG-RAN or E-UTRAN) and potential solutions, and provides recommendations for the further normative work.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2023-06

(NEW) 3GPP TS 23.542 V18.4.0 Application layer support for Personal IoT Network;

📎 URL: <https://www.3gpp.org/DynaReport/23542.htm>

ABSTRACT: The present document specifies the application enabler layer architecture, procedures and information flows necessary for enabling PIN applications over 3GPP networks. The specification includes the capabilities (e.g. PIN management, discovery of elements, capabilities and services related to PIN) at the application enablement layer that fulfil the deployment and operational requirements of PIN applications over 3GPP networks. The PIN enabler capabilities applies to 5GS.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-06

bloTope project D6.6 V1.0 Proof-of-Concept “Helsinki Pilot” Implementation

📎 URL: <https://storage.ning.com/topology/rest/1.0/file/get/35619980?profile=original>

ABSTRACT: This report describes in detail the goals and the use case of an Helsinki pilot, architecture of the solution, the relation to the other use cases, the current state of implementation, demonstrated scenarios, and the plan to accomplish the implementation from the demo stage to the final solution. The proof of concept and demonstration of the current stage of implementation has been shown by a demonstrator that consists of three components: Client Android app, O-MI Reference implemented Agent, and the charging hardware box. The basic scenario of searching and selection of a suitable charging station in the area has been implemented and shown.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-02

CEN EN 13757-1 Communication systems for meters - Part 1: Data exchange

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT,FSP_ORG_ID:65216,6275&cs=1520E24EB7BA8E7321D0D175C7F1CF004

ABSTRACT: This document specifies data exchange and communications for meters in a generic way. This document establishes a protocol specification for the Application Layer for meters and establishes several protocols for meter communications which can be applied depending on the application being fulfilled. This document also specifies the overall structure of the Object Identification System (OBIS) and the mapping of all commonly used data items in metering equipment to their identification codes. NOTE Electricity meters are not covered by this document, as the standardization of remote readout of electricity meters is a task for CENELEC/IEC.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-12

CEN EN 13757-2 Communication systems for meters - Part 2: Wired M-Bus communication

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT,FSP_ORG_ID:61821,6275&cs=148E2A53815B1043A00AB94D1340B84A1

ABSTRACT: This draft European standard is applicable to the physical and link layer parameters of baseband communication over twisted pair (M Bus) for meter communication systems. It is especially applicable to thermal energy meters, heat cost allocators, water meters and gas meters. NOTE It is usable also for other meters (like electricity meters) and for sensors and actuators. For generic descriptions concerning communication systems for meters and remote reading of meters see EN 13757-1.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-10

CEN EN 13757-5 Communication systems for meters - Part 5: Wireless M-Bus relaying

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT,FSP_ORG_ID:36150,6275&cs=1B9B9291A8674B58CF7FF96F8B88F5B85

ABSTRACT: This European Standard specifies the protocols to use when performing relaying in wireless meter readout networks. This European Standard is an extension to wireless meter readout specified in EN 13757-4. It supports the routing of modes P and Q, and simple single-hop repeating of modes S, T, C, F and N. The main use of this standard is to support simple retransmission as well as routed wireless networks for the readout of meters. NOTE Electricity meters are not covered by this standard, as the standardisation of remote readout of electricity meters is a task for IEC/CENELEC.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-05

CEN EN 16836-1 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 1: Introduction and standardization framework

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT,FSP_ORG_ID:41098,6275&cs=11019FC07793F83E7C3B39E9E3A6DBF78

ABSTRACT: This European Standard gives the standardization framework of communication systems applicable to the exchange of data from metering devices to other devices within a mesh network.

This European Standard specifies how to interpret prEN 16836-2:2015 and prEN 16836-3:2015 which give a list of references to the ZigBee documents. This series is applicable to communications systems that involve messages and networking between a meter or multiple meters and other devices in a mesh network, such as in home displays (IHDs) and communications hubs. This European Standard allows routing between devices and also allows channel agility to avoid contention with other networks of the same type, or indeed networks of other types operating in the same frequency bands. This European Standard is designed to support low power communications for devices such as gas and water meters which can make data from such devices available on the mesh network at any time through a proxy capability within a permanently powered device.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-05

(Updated) CEN prEN 14154-4 Water meters — Part 4: Additional functionalities

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT,FSP_LANG_ID:73396,25&cs=1DA0D2906520CD899CB94F5BB61C72E7F

ABSTRACT: This document specifies definitions, requirements and testing of additional functionalities for water meters, without metrological impact, in combination with Additional Functionality Devices (AFD) and in response to EU/EFTA Mandate M/441 EN. These AFDs are considered as “ancillary devices” as defined in EN ISO 4064 1:2017 and EN ISO 4064 4:2014.

This document does not cover the changing of metrological software within the meter or the upload/download of metrological software.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-03

Eclipse IoT-Testware

🔗 URL: <https://projects.eclipse.org/projects/technology.iottestware>

ABSTRACT: It is the aim of the project to supply a rich set of TTCN-3 test suites and test cases for IoT technologies to enable developers in setting up a comprehensive test environment of their own, if needed from the beginning of a project. TTCN-3 has been defined and standardized by the European Telecommunication Standards Institute in ETSI ES 201873 and related extension packages. It is implemented and supported in Eclipse IoT by the Eclipse Titan project.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: N/A

Eclipse OM2M Eclipse OM2M v1.4.1 - Open-Source platform for M2M communication

🔗 URL: <https://www.eclipse.org/om2m/>

ABSTRACT: The Eclipse OM2M project, initiated by LAAS-CNRS, is an open-source implementation of oneM2M and SmartM2M standard. It provides a horizontal M2M service platform for developing services independently of the underlying network, with the aim to facilitate the deployment of vertical applications and heterogeneous devices.

📄 DOCUMENT TYPE: Open_Source

📅 PUBLICATION DATE: 2012-02

ETSI TR 103 674 SmartM2M; Artificial Intelligence and the oneM2M architecture

 **URL:** http://www.etsi.org/deliver/etsi_tr/103600_103699/103674/01.01.01_60/tr_103674v010101p.pdf

ABSTRACT: Detailed description of selected use cases and identification of architectural evolutions (components, required mappings, etc.) to the oneM2M framework.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-02

ETSI TR 103 714 SmartM2M; Study for oneM2M; Discovery and Query use cases and requirements

 **URL:** http://www.etsi.org/deliver/etsi_tr/103700_103799/103714/01.01.01_60/tr_103714v010101p.pdf

ABSTRACT: this work will identify additional requirements to be potentially submitted to oneM2M in the areas of discovery and query languages (syntax and semantic), by means of the development of relevant use cases. As a minimum, this work should include discovery of specific information and of aggregated information, and interaction with external sources of data and queries. The oneM2M architecture, the oneM2M semantic approach, the current oneM2M capabilities and SAREF will be at the basis of these use cases and requirements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-07

ETSI TR 103 717 SmartM2M; Study for oneM2M; Discovery and Query specification development

 **URL:** http://www.etsi.org/deliver/etsi_tr/103700_103799/103717/01.01.01_60/tr_103717v010101p.pdf

ABSTRACT: This work will develop the specification for the discovery solution selected in DTR/SmartM2M-123151. This deliverable will document the specification while the real standardisation proposal will be contributed to oneM2M TS-0001 (Architecture), oneM2M TS-0034 (Semantic support), oneM2M TS-0033 (Interworking Framework), oneM2M TS-0004 (Protocols) (other oneM2M TS may be also impacted) with the help of the supporting companies active in oneM2M.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-07

ETSI TS 103 246-1 Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 1: Functional requirements

 **URL:** http://www.etsi.org/deliver/etsi_ts/103200_103299/10324601/01.03.01_60/ts_10324601v010301p.pdf

ABSTRACT: This standard addresses integrated location systems that combine Global Navigation Satellite Systems (GNSS), with other navigation technologies, as well as with telecommunication networks in order to deliver location-based services to users. The requirements are intended to address the growing use of complex location systems needed for the provision of location-based applications particularly for the mass-market (refer to ETSI TR 103 183).

The standard defines the functional requirements applicable to location systems, based on a synthesis of types of applications relying on location-related data provided by location system. It can be considered as the Stage 1 characterization of location systems according to the ITU/3GPP approach (Recommendation ITU-T I.130).

It is the first part of a multi-part standard, with Part 1: Functional requirements; Part 2: Reference Architecture; Part 3: Performance requirements; Part 4: Requirements for location data exchange

protocols; Part 5: Performance Test Specification.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-10

(NEW) ETSI GS MEC 033 V3.1.1 Multi-access Edge Computing (MEC); IoT API

📄 URL: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/033/03.01.01_60/gs_MEC033v030101p.pdf

ABSTRACT: The present document defines the IoT API to assist the deployment and usage of devices that require additional support in a MEC environment, e.g. due to security constraints, limited power, compute and communication capabilities, such as IoT and MTC devices. The API enables the device provisioning and configuration of the associated components and applications requiring connection to these devices. The present document describes the information flows and the required information. It also specifies the RESTful binding with the data model.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-12

(NEW) ETSI/oneM2M TR 118 567 V4.0.0 oneM2M: Study on Management Object migration to SDT

📄 URL: http://www.etsi.org/deliver/etsi_tr/118500_118599/118567/04.00.00_60/tr_118567v040000p.pdf

ABSTRACT: The present document studies the completion of SDT (Smart Device Template) using <flexContainer> resource specializations and the possible migration of the existing device management model using Management Object (<mgmtObj>). The present document is initiated in the context of the Management Object Migration.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2021-11

(NEW) ETSI TS 118 122 V4.5.1 oneM2M; Field Device Configuration

📄 URL: https://www.etsi.org/deliver/etsi_ts/118100_118199/118122/04.05.01_60/ts_118122v040501p.pdf

ABSTRACT: The present document specifies the architectural options, resources and procedures needed to pre-provision and maintain devices in the Field Domain (e.g. ADN, ASN/MN) in order to establish M2M Service Layer operation between the device's AE and/or CSE and a Registrar and/or Hosting CSE. The resources and procedures includes information about the Registrar CSE and/or Hosting CSE needed by the AE or CSE to begin M2M Service Layer operation.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-07

(NEW) ETSI GS NIN 006 V1.1.1 Non-IP Networking (NIN); Scenario Definitions of Next Generation Protocols (NGP)

📄 URL: http://www.etsi.org/deliver/etsi_gs/NIN/001_099/006/01.01.01_60/gs_NIN006v010101p.pdf

ABSTRACT: The present work item intends to provide updates to the GS NGP 001 V1.3.1.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-07

(NEW) ETSI TR 103 844 V1.1.1 SmartM2M; Digital Twins and Standardization Opportunities in ETSI

 **URL:** http://www.etsi.org/deliver/etsi_tr/103800_103899/103844/01.01.01_60/tr_103844v010101p.pdf

ABSTRACT: With reference to Digital Twins:

-  Analysis the major characteristics and architectures
-  Identification major functionalities,
-  selection of the candidate communication functionalities for standardization
-  Collection, identification and Definition of uses cases for IoT and in particular industrial IoT
-  Identification of potential requirements

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-11

(NEW) ETSI TR 103 839 V1.1.1 SmartM2M; Scenarios for evaluation of oneM2M deployments

 **URL:** http://www.etsi.org/deliver/etsi_tr/103800_103899/103839/01.01.01_60/tr_103839v010101p.pdf

ABSTRACT: Identification of relevant deployment scenarios. The description of these scenarios include detailed information of the IoT solution topology, characteristics of both IoT devices and applications in terms of number of entities, traffic profiles, targeted performances, etc.

The deliverable will also include the procedures to define additional evaluation scenarios.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-09

(NEW) IEEE SA - IEEE 2735-2022 EEE Standard for Interoperability of Complex Virtual Instruments for Internet of Things

 **URL:** <https://standards.ieee.org/ieee/2735/7392/>

ABSTRACT: A framework for IoT application systems, a definition of a complex virtual instrumentation model, and agreement on a framework and interfaces to achieve interoperability of IoT applications, while specifying the communication methods, invocation parameters and return value formats of the interfaces, is given in this standard.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-02

(NEW) IEEE 2735.1-2022 IEEE Standard Design Criteria of Complex Virtual Instruments for Household Appliance Test

 **URL:** <https://standards.ieee.org/ieee/2735.1/7393/>

ABSTRACT: This standard designs and standardizes data input interfaces, computing service interfaces, interconnection service interfaces, Laboratory Information Management System (LIMS) service interfaces, functional design requirements, and constraints for Complex Virtual Instruments (CVI) in the field of household appliance testing based on IEEE Std 2735. The purpose is to process the data or metadata from different types of household appliance complex virtual instruments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-02

(NEW) IEEE 1935-2023 IEEE Standard for Edge/Fog Manageability and Orchestration

 **URL:** <https://standards.ieee.org/ieee/1935/7181/>

ABSTRACT: With the innovation of mobile applications and the arrival of the fifth generation of telecommunication, edge computing has become a popular scheme due to its geographical proximity to end users. The overall architecture has the advantage of lower latency and improved user experience. However, because of physical limitations, management and orchestration in the edge system is necessary to maintain operations, common functions, and application lifecycle. Accordingly, a standardized, orchestration-wise design to simplify the process and offer better system performance and user experience was introduced by the IEEE P1935 working group. The framework, architecture, and procedures of the edge-fog system as well as its application lifecycle management are involved in this standard.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-07

(NEW) IEEE 1918.1-2024 IEEE Approved Draft Standard for Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture, Functions, and Technical Assumptions

 **URL:** <https://standards.ieee.org/ieee/1918.1/6721/>

ABSTRACT: This standard defines a framework for the Tactile Internet, including descriptions of various application scenarios, definitions and terminology, functions, and technical assumptions. This framework prominently also includes a reference model and architecture, which defines common architectural entities, interfaces between those entities, and the mapping of functions to those entities. The Tactile Internet encompasses mission critical applications (e.g., manufacturing, transportation, healthcare and mobility), as well as non-critical applications (e.g., edutainment and events).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-09

(NEW) IEEE P2992 Recommended Practice for Data Expression, Exchange, and Processing in Smart Agriculture

 **URL:** <https://standards.ieee.org/ieee/2992/10614/>

ABSTRACT: This standard defines recommended practices for designing smart agriculture data focusing on the data format, data tags, their naming rules, and data transfers to show the unified practices of data expression, exchange, and processing. This is indispensable for smart agriculture systems, such as data acquisition, data management, data service provisioning, and data processing for data security, as well as privacy from the perspective of agricultural machinery control, greenhouse management, and farming management. This recommended practice provides the co-existence and interoperability using common data structure and transfer between heterogeneous systems; namely, various systems of different manufacturers work together to achieve the farmers' requirement efficiently and effectively as for a smart agriculture system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IEC Internet of Things: Wireless Sensor Networks

 **URL:** <https://www.iec.ch/basecamp/internet-things-wireless-sensor-networks>

ABSTRACT: Wireless sensor networks (WSN) are generating increasing interest from industry and research. This is driven by the availability of inexpensive, low-powered miniature components such as processors, radios and sensors which are sometimes integrated on a single chip. The idea of the Internet of Things (IoT) developed in parallel to WSNs. While IoT doesn't assume a specific communication technology, wireless communication technologies will play a major role in the roll-out of IoT. WSNs will drive many applications and many industries. This white paper discusses the use and evolution of WSNs in the wider context of IoT. It provides a review of WSN applications, infrastructures technologies, applications as well as standards that apply to WSN designs.

The white paper was prepared by the IEC Market Strategy Board (MSB) wireless sensor networks project team in cooperation with the US National Institute of Standards and Technology (NIST).

 **DOCUMENT TYPE:** Whitepaper

 **PUBLICATION DATE:** 2014-11

(Updated) 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

 **URL:** <https://webstore.iec.ch/publication/63343>

ABSTRACT: Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 31: List of Properties (LOPs) of infrastructure devices for electronic data exchange – Generic structures

IEC 61987-31:2022 provides a characterization for the integration of infrastructure devices in the Common Data Dictionary (CDD);

generic structures in conformance with IEC 61987-10 for Operating Lists of Properties (OLOPs) and Device Lists of Properties (DLOPs) of infrastructure devices.

The generic structures for the OLOP and DLOP contain the most important blocks for infrastructure devices. Blocks pertaining to a specific equipment type will be described in the corresponding part of the IEC 61987 series. Similarly, equipment properties are not part of this part of IEC 61987. For instance, the OLOP and DLOP for I/O-modules are to be found in IEC 61987-32.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-12

IEEE Transdisciplinary Framework for 5G-Enabled Applications and Services

 **URL:** <https://standards.ieee.org/industry-connections/transdisciplinary-framework-5g/>

ABSTRACT: The goal of this activity is to develop a structured, sustainable communication framework that is flexible, adaptable, and scalable for newer ecosystems. This framework is intended to be formulaic and can be extended for different ecosystems and may be used by governments, industry, and academia.

 **DOCUMENT TYPE:** Framework

 **PUBLICATION DATE:** Under development

(Updated) IETF draft-ietf-asdf-sdf Semantic Definition Format (SDF) for Data and Interactions of Things

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-asdf-sdf/>

ABSTRACT: In this document, an SDF specification describes definitions of SDF Objects and their associated interactions (Events, Actions, Properties), as well as the Data types for the information exchanged in those interactions.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-02

(Updated) IETF draft-ietf-rats-tpm-based-network-device-attest TPM-based Network Device Remote Integrity Verification

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/>

ABSTRACT: This document describes a workflow for remote attestation of the integrity of firmware and software installed on network devices that contain Trusted Platform Modules [TPM1.2], [TPM2.0], as defined by the Trusted Computing Group (TCG)), or equivalent hardware implementations that include the protected capabilities, as provided by TPMs.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-03

(Updated) IETF draft-ietf-rats-yang-tpm-charra A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs.

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/>

ABSTRACT: This document defines YANG RPCs and a few configuration nodes required to retrieve attestation evidence about integrity measurements from a device, following the operational context defined in TPM-based Network Device Remote Integrity Verification.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-07

(Updated) IETF draft-ietf-raw-architecture Reliable and Available Wireless Architecture

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-raw-architecture/>

ABSTRACT: This document defines the RAW Architecture following an OODA loop that involves OAM, PCE, PSE and PAREO functions. It builds on the DetNet Architecture and discusses specific challenges and technology considerations needed to deliver DetNet service utilizing scheduled wireless segments and other media, e.g., frequency/time-sharing physical media resources with stochastic traffic.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-07

(Updated) IETF draft-ietf-raw-framework Reliable and Available Wireless Framework

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-raw-framework/>

ABSTRACT: Reliable and Available Wireless Framework following an OODA loop that involves OAM, PCE, PSE and PAREO functions.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-03

(Updated) IETF draft-ietf-raw-industrial-requirements Requirements for Reliable Wireless Industrial Services

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-raw-industrial-requirements/>

ABSTRACT: This document provides an overview on communication requirements for handling reliable wireless services within the context of industrial environments.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-10

(Updated) IETF draft-ietf-raw-oam-support Operations, Administration and Maintenance (OAM) features for RAW

 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-raw-oam-support/>

ABSTRACT: This document lists the requirements of the Operation, Administration, and Maintenance (OAM) features are recommended to construct a predictable communication infrastructure on top of a collection of wireless segments.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-03

(Updated) IETF draft-morais-iotops-inxu Intra-Network eXposure analyzer Utility Specification

 **URL:** <https://datatracker.ietf.org/doc/draft-morais-iotops-inxu/>

ABSTRACT: This document proposes the Intra-Network eXposure analyzer Utility (INXU) as a vulnerability management solution for IoT networks.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-05

(Updated) IETF draft-choi-icnrg-aiot Requirements and Challenges for User-level Service Managements of IoT Network by utilizing Artificial Intelligence

 **URL:** <https://datatracker.ietf.org/doc/draft-choi-icnrg-aiot/>

ABSTRACT: This document describes the requirements and challenges to employ artificial intelligence (AI) into the constraint Internet of Things (IoT) service environment for embedding intelligence and increasing efficiency.

 **DOCUMENT TYPE:** Technical_Report

(Updated) IETF draft-km-iotops-iiot-frwk Virtualization of PLC in Industrial Networks - Problem Statement

🔗 **URL:** <https://datatracker.ietf.org/doc/draft-km-iotops-iiot-frwk/>

ABSTRACT: This document introduces virtual PLC concept, describes the details and benefits of virtualized PLCs, then focuses on the problem statement and requirements.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2022-05

(Updated) IETF RFC 9372 L-band Digital Aeronautical Communications System (LDACS)

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc9372/>

ABSTRACT: This document gives an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2023-12

ietf RFC 8352 Energy-Efficient Features of Internet of Things Protocols

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc8352/>

ABSTRACT: This document describes the challenges for energy-efficient protocol operation on constrained devices and the current practices used to overcome those challenges.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2018-02

ietf RFC 8366 A Voucher Artifact for Bootstrapping Protocols

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc8366/>

ABSTRACT: This document defines a strategy to securely assign a pledge to an owner using an artifact signed, directly or indirectly, by the pledge's manufacturer. This artifact is known as a "voucher".

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2018-05

ietf RFC 8428 Sensor Measurement Lists (SenML)

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc8428/>

ABSTRACT: This specification defines a format for representing simple sensor measurements and device parameters in Sensor Measurement Lists (SenML). Representations are defined in JavaScript Object Notation (JSON), Concise Binary Object Representation (CBOR), Extensible Markup Language (XML), and Efficient XML Interchange (EXI), which share the common SenML data model. A simple sensor, such as a temperature sensor, could use one of these media types in protocols such as HTTP or the Constrained Application Protocol (CoAP) to transport the

measurements of the sensor or to be configured.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-08

IETF RFC 8747 Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)

🔗 URL: <https://datatracker.ietf.org/doc/rfc8747/>

ABSTRACT: This specification describes how to declare in a CBOR Web Token (CWT) (which is defined by RFC 8392) that the presenter of the CWT possesses a particular proof-of-possession key. Being able to prove possession of a key is also sometimes described as being the holder-of-key. This specification provides equivalent functionality to “Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)” (RFC 7800) but using Concise Binary Object Representation (CBOR) and CWTs rather than JavaScript Object Notation (JSON) and JSON Web Tokens (JWTs).

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-03

IETF RFC 8768 Constrained Application Protocol (CoAP) Hop-Limit Option

🔗 URL: <https://datatracker.ietf.org/doc/rfc8768/>

ABSTRACT: This document specifies the Hop-Limit CoAP option.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-03

IETF RFC 8778 Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)

🔗 URL: <https://datatracker.ietf.org/doc/rfc8778/>

ABSTRACT: This document specifies the conventions for using the Hierarchical Signature System (HSS) / Leighton-Micali Signature (LMS) hash-based signature algorithm with the CBOR Object Signing and Encryption (COSE) syntax. The HSS/LMS algorithm is one form of hash-based digital signature; it is described in RFC 8554.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-04

IETF RFC 8790 FETCH and PATCH with Sensor Measurement Lists (SenML)

🔗 URL: <https://datatracker.ietf.org/doc/rfc8790/>

ABSTRACT: This document defines new media types for the CoAP FETCH, PATCH, and iPATCH methods for resources represented using the SenML data model.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06

IETF RFC 8798 Additional Units for Sensor Measurement Lists (SenML)

 **URL:** <https://datatracker.ietf.org/doc/rfc8798/>

ABSTRACT: This document registers a number of additional unit names in the IANA registry for units in SenML. It also defines a registry for secondary units that cannot be in SenML's main registry, as they are derived by linear transformation from units already in that registry.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06

IETF RFC 8824 Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8824/>

ABSTRACT: This document defines how to compress Constrained Application Protocol (CoAP) headers using the Static Context Header Compression and fragmentation (SCHC) framework

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-06

IETF RFC 8928 Address-Protected Neighbor Discovery for Low-Power and Lossy Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc8928/>

ABSTRACT: This document updates the IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery (ND) protocol defined in RFCs 6775 and 8505. The new extension is called Address-Protected Neighbor Discovery (AP-ND), and it protects the owner of an address against address theft and impersonation attacks in a Low-Power and Lossy Network (LLN). Nodes supporting this extension compute a cryptographic identifier (Crypto-ID), and use it with one or more of their Registered Addresses. The Crypto-ID identifies the owner of the Registered Address and can be used to provide proof of ownership of the Registered Addresses. Once an address is registered with the Crypto-ID and a proof of ownership is provided, only the owner of that address can modify the registration information, thereby enforcing Source Address Validation

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8930 On Forwarding 6LoWPAN Fragments over a Multi-Hop IPv6 Network

 **URL:** <https://datatracker.ietf.org/doc/rfc8930/>

ABSTRACT: This document provides generic rules to enable the forwarding of an IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) fragment over a route-over network. Forwarding fragments can improve both end-to-end latency and reliability as well as reduce the buffer requirements in intermediate nodes; it may be implemented using RFC 4944 and Virtual Reassembly Buffers (VRBs).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8931 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Selective Fragment Recovery

 **URL:** <https://datatracker.ietf.org/doc/rfc8931/>

ABSTRACT: This document updates RFC 4944 with a protocol that forwards individual fragments across a route-over mesh and recovers them end to end, with congestion control capabilities to protect the network.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8938 Deterministic Networking (DetNet) Data Plane Framework

 **URL:** <https://datatracker.ietf.org/doc/rfc8938/>

ABSTRACT: This document provides an overall framework for the Deterministic Networking (DetNet) data plane. It covers concepts and considerations that are generally common to any DetNet data plane specification. It describes related Controller Plane considerations as well.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-11

IETF RFC 8939 Deterministic Networking (DetNet) Data Plane: IP

 **URL:** <https://datatracker.ietf.org/doc/rfc8939/>

ABSTRACT: This document specifies the Deterministic Networking (DetNet) data plane operation for IP hosts and routers that provide DetNet service to IP-encapsulated data.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

IETF RFC 8974 Extended Tokens and Stateless Clients in the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8974/>

ABSTRACT: This document provides considerations for alleviating Constrained Application Protocol (CoAP) clients and intermediaries of keeping per-request state. To facilitate this, this document additionally introduces a new, optional CoAP protocol extension for extended token lengths.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-01

IETF RFC 8990 GeneRic Autonomic Signaling Protocol (GRASP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8990/>

ABSTRACT: This document specifies the GeneRic Autonomic Signaling Protocol (GRASP), which enables autonomic nodes and Autonomic Service Agents to dynamically discover peers, to synchronize state with each other, and to negotiate parameter settings with each other.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IETF RFC 8991 GeneRic Autonomic Signaling Protocol Application Program Interface (GRASP API)

 **URL:** <https://datatracker.ietf.org/doc/rfc8991/>

ABSTRACT: This document is a conceptual outline of an application Programming Interface (API) for the GeneRic Autonomic Signaling Protocol (GRASP).

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-05

IETF RFC 8993 A Reference Model for Autonomic Networking

 **URL:** <https://datatracker.ietf.org/doc/rfc8993/>

ABSTRACT: This document describes a reference model for Autonomic Networking for managed networks.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-05

IETF RFC 8994 An Autonomic Control Plane (ACP)

 **URL:** <https://datatracker.ietf.org/doc/rfc8994/>

ABSTRACT: This document defines such a plane and calls it the “Autonomic Control Plane”, with the primary use as a control plane for autonomic functions.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2021-05

IETF RFC 9006 TCP Usage Guidance in the Internet of Things (IoT)

 **URL:** <https://datatracker.ietf.org/doc/rfc9006/>

ABSTRACT: This document provides guidance on how to implement and use the Transmission Control Protocol (TCP) in Constrained-Node Networks (CNNs), which are a characteristic of the Internet of Things (IoT).

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-03

IETF RFC 9100 Sensor Measurement Lists (SenML) Features and Versions

 **URL:** <https://datatracker.ietf.org/doc/rfc9100/>

ABSTRACT: This short document updates RFC 8428, “Sensor Measurement Lists (SenML)”, by specifying the use of independently selectable “SenML Features” and mapping them to SenML version numbers.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-08

IETF RFC 9124 A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices

 **URL:** <https://datatracker.ietf.org/doc/rfc9124/>

ABSTRACT: This document describes the information that must be present in the manifest.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-01

IETF RFC 9164 Concise Binary Object Representation (CBOR) Tags for IPv4 and IPv6 Addresses and Prefixes

 **URL:** <https://datatracker.ietf.org/doc/rfc9164/>

ABSTRACT: This specification defines two Concise Binary Object Representation (CBOR) tags for use with IPv6 and IPv4 addresses and prefixes.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-12

IETF RFC 9165 Additional Control Operators for the Concise Data Definition Language (CDDL)

 **URL:** <https://datatracker.ietf.org/doc/rfc9165/>

ABSTRACT: The present document defines a number of control operators that were not yet ready at the time RFC 8610 was completed: .plus, .cat, and .det for the construction of constants; .abnf/abnfb for including ABNF (RFC 5234 and RFC 7405) in CDDL Specifications; and .feature for indicating the use of a non-basic feature in an instance.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-12

IETF RFC 9175 Constrained Application Protocol (CoAP): Echo, Request-Tag, and Token Processing

 **URL:** <https://datatracker.ietf.org/doc/rfc9175/>

ABSTRACT: This document specifies enhancements to the Constrained Application Protocol (CoAP) that mitigate security issues in particular use cases.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-03

IETF RFC 9222 Guidelines for Autonomic Service Agents

 **URL:** <https://datatracker.ietf.org/doc/rfc9222/>

ABSTRACT: This document proposes guidelines for the design of Autonomic Service Agents for autonomic networks.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-03

IETF RFC7400 6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

 **URL:** <https://datatracker.ietf.org/doc/rfc7400/>

ABSTRACT: RFC 6282 defines header compression in 6LoWPAN packets (where “6LoWPAN” refers to “IPv6 over Low-Power Wireless Personal Area Network”). The present document specifies a simple addition that enables the compression of generic headers and header-like payloads, without a need to define a new header compression scheme for each such new header or header-like payload.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2014-11

IETF RFC7416 A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)

 **URL:** <https://datatracker.ietf.org/doc/rfc7416/>

ABSTRACT: This document presents a security threat analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). The development builds upon previous work on routing security and adapts the assessments to the issues and constraints specific to low-power and lossy networks. A systematic approach is used in defining and evaluating the security threats. Applicable countermeasures are application specific and are addressed in relevant applicability statements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2015-01

IETF RFC7428 Transmission of IPv6 Packets over ITU-T G.9959 Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc7428/>

ABSTRACT: This document describes the frame format for transmission of IPv6 packets as well as a method of forming IPv6 link-local addresses and statelessly autoconfigured IPv6 addresses on ITU-T G.9959 networks.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-02

IETF RFC7554 Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement

 **URL:** <https://datatracker.ietf.org/doc/rfc7554/>

ABSTRACT: This document describes the environment, problem statement, and goals for using the Time-Slotted Channel Hopping (TSCH) Medium Access Control (MAC) protocol of IEEE 802.15.4e in the context of Low-Power and Lossy Networks (LLNs). The set of goals enumerated in this document form an initial set only.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2015-05

IETF RFC7641 Observing Resources in the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc7641/>

ABSTRACT: This document specifies a simple protocol extension for CoAP that enables CoAP clients to “observe” resources, i.e., to retrieve a representation of a resource and keep this representation updated by the server over a period of time. The protocol follows a best-effort approach for sending new representations to clients and provides eventual consistency between the state observed by each client and the actual resource state at the server.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-09

IETF RFC7668 IPv6 over BLUETOOTH(R) Low Energy

 **URL:** <https://datatracker.ietf.org/doc/rfc7668/>

ABSTRACT: Bluetooth Smart is the brand name for the Bluetooth low energy feature in the Bluetooth specification defined by the Bluetooth Special Interest Group. The standard Bluetooth radio has been widely implemented and available in mobile phones, notebook computers, audio headsets, and many other devices. The low-power version of Bluetooth is a specification that enables the use of this air interface with devices such as sensors, smart meters, appliances, etc. The low-power variant of Bluetooth has been standardized since revision 4.0 of the Bluetooth specifications, although version 4.1 or newer is required for IPv6. This document describes how IPv6 is transported over Bluetooth low energy using IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) techniques.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

IETF RFC7731 Multicast Protocol for Low-Power and Lossy Networks (MPL)

 **URL:** <https://datatracker.ietf.org/doc/rfc7731/>

ABSTRACT: This document specifies the Multicast Protocol for Low-Power and lossy Networks (MPL), which provides IPv6 multicast forwarding in constrained networks. MPL avoids the need to construct or maintain any multicast forwarding topology, disseminating messages to all MPL Forwarders in an MPL Domain.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-02

IETF RFC7732 Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)

 **URL:** <https://datatracker.ietf.org/doc/rfc7732/>

ABSTRACT: The purpose of this document is to specify an automated policy for the routing of Multicast Protocol for Low-Power and Lossy Networks (MPL) multicast messages with Admin-Local scope in a border router.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-02

IETF RFC7744 Use Cases for Authentication and Authorization in Constrained Environments

 **URL:** <https://datatracker.ietf.org/doc/rfc7744/>

ABSTRACT: This document includes a collection of representative use cases for authentication and authorization in constrained environments. These use cases aim at identifying authorization problems that arise during the life cycle of a constrained device and are intended to provide a guideline for developing a comprehensive authentication and authorization solution for this class of scenarios.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-02

IETF RFC7774 Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6

 **URL:** <https://datatracker.ietf.org/doc/rfc7774/>

ABSTRACT: This document defines a way to configure a parameter set for MPL (Multicast Protocol for Low-Power and Lossy Networks) via a DHCPv6 option. MPL has a set of parameters to control its behavior, and the parameter set is often configured as a network-wide parameter because the parameter set should be identical for each MPL Forwarder in an MPL Domain. Using the MPL Parameter Configuration Option defined in this document, a network can easily be configured with a single set of MPL parameters.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-03

IETF RFC7959 Block-Wise Transfers in the Constrained Application Protocol (CoAP)

 **URL:** <https://datatracker.ietf.org/doc/rfc7959/>

ABSTRACT: this specification extends basic CoAP with a pair of “Block” options for transferring multiple blocks of information from a resource representation in multiple request-response pairs. In many important cases, the Block options enable a server to be truly stateless: the server can handle each block transfer separately, with no need for a connection setup or other server-side memory of previous block transfers. Essentially, the Block options provide a minimal way to transfer larger representations in a block-wise fashion.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-08

IRTF RFC 9139 Information-Centric Networking (ICN) Adaptation to Low-Power Wireless Personal Area Networks (LoWPANs)

 **URL:** <https://datatracker.ietf.org/doc/rfc9139/>

ABSTRACT: This document defines a convergence layer for Content-Centric Networking (CCNx) and Named Data Networking (NDN) over IEEE 802.15.4 Low-Power Wireless Personal Area Networks (LoWPANs)

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-11

ISO/IEC 30169 Information technology — Internet of Things (IoT) — IoT applications for electronic label system (ELS)

 **URL:** <https://webstore.iec.ch/publication/66659>

ABSTRACT: This document applies to the design and development of the IoT applications for ELS. The IoT applications for ELS specified in this document are mainly applicable to the retail industry, and can also provide reference for the design and development of the IoT applications for ELS in other industries.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-05

(Updated) ISO/IEC 30172 Information technology — Internet of Things (IoT) — Digital twin – Use Cases

 **URL:** https://www.iec.ch/ords/f?p=103:38:411250985150323::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104881

ABSTRACT: This document provides a collection of representative use cases of Digital Twin applications in a variety of domains, e.g., smart manufacturing, smart cities, etc. This document is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-01

ISO/IEC TR 30176:2021 Internet of Things (IoT) - Integration of IoT and DLT/blockchain: Use cases

 **URL:** <https://webstore.iec.ch/publication/66420>

ABSTRACT: This report identifies and collects use cases for the integration of the DLT/blockchain within IoT systems, applications, and/or services. The use cases presented in this document use the IoT use case template.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-11

(Updated) ISO/IEC TS 30168 Information technology — Internet of Things (IoT) — Generic Trust Anchor Application Programming Interface for Industrial IoT Devices

 **URL:** <https://webstore.iec.ch/en/publication/66553>

ABSTRACT: This document specifies a generic application programming interface (API) for the integration of secure elements within Industrial IoT (IIoT) devices. It considers needs from industrial usage scenarios and applications. This document also provides guidance for implementation, testing, and conformity validation.

This specification provides a versatile Application Programming Interface (API) for security to allow a generic integration of secure elements (SE) into Industrial IoT devices. The API is vendor independent and independent regarding the secure element technology being deployed. This allows easy redesign for different secure elements and supports software-hardware co-design for security. The API aims at achieving high level abstraction profiles for security services and mechanisms to avoid typical low-level interoperability complexity and implementation failures. Requirements and architectural constraints from Industrial IoT applications will dominate the final design of the API and its usability.

(NEW) ITU-T Y.4417-Rev Framework of self-organization networking in Internet of things environments

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19610

ABSTRACT: The evolution of IoT can be divided into three stages: the first stage being connectivity, the second stage being intelligence, and the third stage being autonomy. Currently, IoT technology is positioned at the early phase of the second stage, which focuses on intelligence. In addition, most of the standards development in the field of IoT technology has been focused on connectivity-based IoT standards. However, there is a gradual emergence of standards for intelligent IoT as well. Nevertheless, in the context of autonomous IoT, standard development has been primarily concentrated on service technologies. Through analyses such as those presented in Table 2, it is evident how the evolution of standard technologies has progressed alongside the evolution of IoT technology. It highlights that the standardization phase of IoT is still in its early stages when it comes to developing intelligent standards. Recommendation ITU-T Y.4417 (06/2018) specifies a framework of self-organization networking in IoT environments with characteristics, requirements, functional architectures, and functionalities. The framework manages the functionalities to enable intelligent and autonomous services for IoT network technology. However, the functionalities within the framework – including the Coordinator election, Initialization and configuration, Identification, Data forwarding and delivery, Network recovery, and Routing and path discovery – are defined without considering the technical concepts and characteristics of intelligent IoT and autonomous IoT. As a result, Recommendation ITU-T Y.4417 needs to be revised to achieve a certain level of standard quality maturity to better configure networks for the coming intelligent and autonomous IoT environments.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.4477-Rev Framework for service interworking with device discovery and management in heterogeneous Internet of things environments

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19064

ABSTRACT: 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.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.4480Rev0 Low power protocol for wide area wireless networks

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18747

ABSTRACT: This Recommendation defines a protocol for wide area wireless networks, which is optimized for battery-powered end-devices that may be either mobile or mounted at a fixed location.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4463 Framework of delegation service for Internet of things devices

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19073

ABSTRACT: Recommendation ITU-T Y.4463 is a framework of the delegation service for transferring ownership (i.e., access rights to the Internet of things (IoT) devices) among authorized IoT devices. This Recommendation gives an overview and types of delegation service in IoT environment. It also describes the requirements and architectural models of delegation service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-08

(NEW) ITU-T Y.4499 (ex Y.UIM-cs-framework) Framework of urban infrastructure monitoring based on crowdsourcing

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17944

ABSTRACT: Recommendation ITU-T Y.4499 specifies a framework for urban infrastructure monitoring based on crowdsourcing, including requirements, functional architecture, common procedures, as well as security and privacy considerations. Urban infrastructure includes the physical facilities and systems that a city must have for its operation and development. It has the characteristics of large quantity, wide distribution and high management difficulty. Crowdsourcing is the practice of engaging a group of people for a common goal. It can provide a scalable and financially viable way to monitor urban infrastructure.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-07

(NEW) ITU-T Y.IoT-3DMS Requirements and functional capabilities for three-dimensional model based monitoring service

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19072

ABSTRACT: This draft Recommendation defines the requirements for providing 3D model-based monitoring services and describes functional capabilities for a 3-dimensional model monitoring system by utilizing IoT sensing metadata. Three dimensional modelling is essential technology for IoT monitoring service, especially facilities to access difficulties by humans. For example, monitoring high-risk building structures, bridges, dams, monitoring natural environments, etc. This 3D modelling is important to predict potential risks (falling, peeling, cracking, etc.) in such environment. And, 3D model-based capabilities are to provide IoT monitoring services in smart city environments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

ITU-T Y.4112/Y.2077 (02/2016) Requirements of the Plug and Play Capability of the IoT

 **URL:** <https://handle.itu.int/11.1002/1000/12706>

ABSTRACT: The document specifies the common requirements for the plug and play capability of the IoT. More specifically, this recommendation covers the followings: a) Concept and scope of plug and play capability of the IoT; b) Plug and play use cases of the IoT; c) Functional requirements for the plug and play capability of the IoT; d) System requirements for the plug and play capability of the IoT.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-02

ITU-T Y.4113 (09/2016) Requirements of the network for the Internet of Things

 **URL:** <https://handle.itu.int/11.1002/1000/13025>

ABSTRACT: This recommendation describes the requirements of the network for the Internet of things (IoT). The common requirements of the IoT described in [ITU-T Y.4100] are high-level; thus this Recommendation is complementary to [ITU-T Y.4100] in term of specific requirements of the network for the IoT.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-09

■ Infrastructure

Horizontals & Verticals

NGI-Trust EDGE-TINC

 **URL:** <https://edge-tinc.gitlab.io/fluentic/>

ABSTRACT: Edge-TINC is developing the networking stack and all the required protocols to enable in-network nodes that possess CPU capacity to accommodate requests for computation.

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

(Updated) NGI-Trust IZI

 **URL:** <https://github.com/mizolotu/izi>

ABSTRACT: Implement a prototype of a defense framework relying on advanced technologies that have recently emerged in the area of software-defined networking (SDN) and network function virtualization (NFV) for IoT devices

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

NGI-Trust PY

 **URL:** <https://www.panga.fr/>

ABSTRACT: The network architecture of connected buildings and cities Local networks to transform buildings and cities into a service platform for their users and managers.

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

NGI-Trust Totem

 **URL:** <https://insigh.io/>

ABSTRACT: set of innovations along with open hardware devices and software applications/tools that will enable the holistic monitoring of the connected home network activities, identify and prevent potential security/trust breaches.

 **DOCUMENT TYPE:** EU & National funded Open Source projects

 **PUBLICATION DATE:** Under development

oneM2M TR-0033-Study_on_Enhanced_Semantic_Enablement-V4_5_0 Study on Enhanced Semantic Enablement

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31093>

ABSTRACT: In this study requirements on enhanced semantic enablement and approaches for addressing these requirements will be developed and discussed. The intention is to achieve agreement between the interested participants on the approaches to be pursued in oneM2M. On this basis normative contributions to Technical Specifications can then be made.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-10

oneM2M TR-0046-V-4.0.1 Study on Public Warning Service Enabler

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/?docId=21832>

ABSTRACT: The present document studies public warning service enabler for oneM2M system including case studies of similar/existing solutions, oneM2M use cases and requirements, possible architecture enhancement, and security analysis. Also, this TR suggests abstract data models for public warning service over IoT technologies.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-06

oneM2M TR-0060-V-0.2.0 Study of action triggering enhancements

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31865>

ABSTRACT: This work item defines how to autonomously send a series of commands to trigger actions based on the configuration of conditions by M2M application. As the extension to the previous work TR-0021, this TR focuses on Complex Event Processing support in oneM2M.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-02

oneM2M TR-0065 V0.1.0 oneM2M-SensorThings API interworking

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34408>

ABSTRACT: This document investigates in oneM2M-to-SensorThings API interworking.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-01

oneM2M TR-0067-V-0.2.0 Study on Management Object migration to SDT

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33846>

ABSTRACT: The document is a study of how SDT <flexContainer> type resources could replace <mgmtObj> resources in the future.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-06

oneM2M TR-0068-V-0.2.0 AI enablement to oneM2M

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34206>

ABSTRACT: The document is analysing existing AI/ML technologies that can be resourced into oneM2M architecture. The document is also investigating potential AI/ML service use cases that use data collected in the oneM2M system. The study on existing AI/ML technologies and use cases are further analysed in this document to understand what features are supported and unsupported by the oneM2M system. Based on the result of this technical report, it will identify potential requirements and key features to enable AI/ML in the oneM2M system.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2021-11

(New) oneM2M TS-0004-V4.19.0 Service Layer Core Protocol

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36773>

ABSTRACT: The present document specifies the communication protocol(s) for oneM2M compliant Systems, M2M Applications, and/or other M2M Systems. The present document also specifies common data formats, interfaces and message sequences to support reference points(s) defined by oneM2M.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-04

oneM2M TS-0005-V4.0.0 Management Enablement (OMA)

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30113>

ABSTRACT: Specifies the usage of OMA DM and OMA LwM2M resources and the corresponding message flows including normal cases as well as error cases to fulfill the oneM2M management requirements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-06

oneM2M TS-0006-V4.0.0 Management enablement (BBF)

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30114>

ABSTRACT: Specifies the usage of the BBF TR-069 protocol and the corresponding message flows including normal cases as well as error cases to fulfil the oneM2M management requirements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-06

oneM2M TS-0008- V-4.5.0 CoAP Protocol Binding

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36186>

ABSTRACT: The specification will cover the protocol specific part of communication protocol used by oneM2M compliant systems as 'CoAP binding'.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2023-08

oneM2M TS-0013-V.3.3.1 Interoperability Testing

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34003>

ABSTRACT: The specification address the testing of the primitives on the oneM2M interfaces as specified in TS-0001 and TS-0004. The purpose of the interoperability testing is to prove end-to-end functionality between Application Entities and Common Service Entities over the Mca and Mcc reference points.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-09

oneM2M TS-0021-V2.0.1 oneM2M and AllJoyn Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26333>

ABSTRACT: This document specifies the oneM2M and AllJoyn interworking technologies.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-03

oneM2M TS-0022-V4_5_0 Field Device Configuration

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35590>

ABSTRACT: Field Device Configuration TS.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2023-02

oneM2M TS-0023-V4.8.0 SDT based Information Model and Mapping for Vertical Industries

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33779>

ABSTRACT: This technical specification includes oneM2M defined information model for home appliances and the mapping with other information models from external organization.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2021-04

oneM2M TS-0024-V4.0.0 OCF Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35756>

ABSTRACT: The present document specifies the interworking between oneM2M-specified entities and OCF-specified clients and/or servers.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2023-03

oneM2M TS-0026-V4.7.0 3GPP Interworking between oneM2M service layer and 3GPP features

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35587>

ABSTRACT: This document specifies interworking between oneM2M service layer and 3GPP features, so that some 3GPP features can be exposed to oneM2M service layer for the benefit of IoT applications, and viceversa.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2023-02

oneM2M TS-0040-V4.0.0 Modbus Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35378>

ABSTRACT: The present document specifies the oneM2M and Modbus interworking technologies that enable Modbus devices and oneM2M entities produce/consume services. This includes the interworking architecture model that describes where the Modbus Interworking Proxy Entity (IPE) is hosted and how the IPE is composed with. This document describes Modbus services to oneM2M resource mapping structure and rules, followed by describing detailed interworking procedures.

 DOCUMENT TYPE: Technical_Report

oneM2M WI-0096 Effective IoT Communication to Protect 3GPP Networks

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33091>

ABSTRACT: This Work Item is intended to produce a specification that describes how a oneM2M service layer hosted on a 3GPP Cellular IoT device ensures that the device operates in an efficient manner that applies the requirements described by GSMA TS.34.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-01

oneM2M WI-0102 System enhancements to support Data License Management

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32157>

ABSTRACT: Proposes a work item to study oneM2M system enhancement to support data license management.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2020-05

oneM2M WI-0104 V0_0_1 SDT based Information Model and Mapping for Vertical Industries – SIMVI

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33391>

ABSTRACT: The purpose of this Work Item is to enable the continuation of contributions of Information Models including ModuleClasses and Device models from various domains for TS-0023.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-03

oneM2M WI-0105 V0_1_0 System enhancements to support AI capabilities

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35882>

ABSTRACT: This work item aims to enable oneM2M to utilize Artificial Intelligence models and data management for AI services.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2023-04

oneM2M WI-0109 IPE-based Device Management with FlexContainers

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34558>

ABSTRACT: Propose a work item for Device Management (DMG) with IPE-based approach with FlexContainers.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2022-02

oneM2M-TR-0042-V-0.4.0 WoT Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26945>

ABSTRACT: This technical report identifies the interworking scenarios and its requirements between oneM2M and W3C Web of Things systems and analyze possible architectural solutions to address the requirements.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2018-05

oneM2M-TR-0043-V-0.3.0 Modbus Interworking

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35844>

ABSTRACT: This technical report investigates oneM2M and modbus interworking scenarios and proposes possible solutions to support the interworking scenarios.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2023-04

oneM2M-TR-0044-V-0.6.0 Physical object heterogeneous identification and tracking in oneM2M

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31631>

ABSTRACT: This technical report investigates the various IoT ID standards and application requirements, discussion on how to be compatible with the IoT ID standards, and providing the heterogeneous identification and tracking services.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2020-02

oneM2M-TR-0053-V-0.6.0 Lightweight oneM2M Services

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31776>

ABSTRACT: The document is a study of lightweight oneM2M services. Based on the result of the study, it identifies proposed optimizations and enhancements to the oneM2M system to streamline and optimize its features and services.

 DOCUMENT TYPE: Technical_Report

oneM2M-TR-0054-V-0.8.0 oneM2M Service Subscribers and Users

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32207>

ABSTRACT: This document is a study on the definition of oneM2M service subscribers and their authorized users. This study explores use cases which require oneM2M service subscribers and users. The study also analyses different solutions to support oneM2M service subscribers and users.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2020-06

oneM2M-TR-0057-V-0.6.0 Getting Started with oneM2M

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33407>

ABSTRACT: Getting Started with oneM2M.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-02

oneM2M-TR-0059-V-0.2.0 oneM2M Services and Platforms Discovery

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30111>

ABSTRACT: The document is describing what services and platforms discovery scenarios are considered beneficial from a oneM2M standpoint and how these can be supported by oneM2M system. Based on the result of the technical report, it will identify possible advanced features and enhancements which the next oneM2M release(s) could support.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2019-06

oneM2M-TS-0018-V-4.6.0 Test Suite Structure and Test Purposes

🔗 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34702>

ABSTRACT: The Test Suite Structure and Test Purposes document for conformance testing consists of: Defining the test suite structure by grouping the test purposes according to different criteria; Specifying test purposes for conformance test. A test purpose is an informal description of the expected test behaviour.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2022-04

OMA OMA-AD-CPNS-V1_1-20160209-A Converged Personal Network Service Architecture

📄 **URL:** https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-AD-CPNS-V1_1-20160209-A.pdf

ABSTRACT: The scope of the CPNS (Converged Personal Network Service) architecture document is to define the architecture for the CPNS v1.1 Enabler. This document provides the functional capabilities needed to support the Enabler as described in CPNS requirements document [CPNS-RD].

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2016-02

OMA OMA-AD-DM-V2_0-20160209-A Device Management Architecture

📄 **URL:** https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-AD-DM-V2_0-20160209-A.pdf

ABSTRACT: The scope of the Device Management architecture document is to define the architecture for the Device Management v2.0 enabler. This document fulfils the functional capabilities and information flows needed to support this enabler as described in the Device Management requirements document.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2016-02

OMA OMA-AD-FUMO-V1_0-20070209-A Firmware Update Management Object Architecture

📄 **URL:** https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-AD-FUMO-V1_0-20070209-A.pdf

ABSTRACT: The scope of this document is the architecture for the Firmware Update Management Object (FUMO) specifications. In general, the scope includes the DM server environment, download mechanisms and devices.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2007-02

OMA OMA-AD-GwMO-V1_1-20170725-A Gateway Management Object Architecture

📄 **URL:** https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-AD-GwMO-V1_1-20170725-A.pdf

ABSTRACT: 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.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2017-07

OMA OMA-AD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Architecture

 **URL:** https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-AD-OpenCMAPI-V1_0-20160126-A.pdf

ABSTRACT: This document provides the architecture for the OpenCMAPI Enabler. This architecture is based on the requirements as listed in the OpenCMAPI Requirement Document.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-01

OMA-ERELED-CPNS-V1_1-20160209-A Enabler Release Definition for Converged Personal Network Service

 **URL:** https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-ERELED-CPNS-V1_1-20160209-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of Converged Personal Network Service (CPNS) enabler according to OMA Release process and the Enabler Release specification baseline listed in section 5. The CPNS Enabler enables CPNS entities in a personal network (PN) to consume services within that PN, services from and to other PNs, and services provided by service providers outside the PN.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-02

OMA-ERELED-DM-V2_0-20160209-A Enabler Release Definition for OMA Device Management

 **URL:** https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-ERELED-DM-V2_0-20160209-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of OMA Device Management v2.0 according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-02

OMA-ERELED-FUMO-V1_0_4-20090828-A Enabler Release Definition for Firmware Update Management Object

 **URL:** https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-ERELED-FUMO-V1_0_4-20090828-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of Firmware Update Management Object specifications according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2009-08

OMA OMA-ERELD-GwMO-V1_1-20170725-A Enabler Release Definition for Gateway Management Object (GwMO)

 **URL:** https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-ERELD-GwMO-V1_1-20170725-A.pdf

ABSTRACT: 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.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2017-07

OMA-ERELD-LightweightM2M-V1_2-20201110-A Enabler Release Definition for LightweightM2M

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-ERELD-LightweightM2M-V1_2-20201110-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of LightweightM2M v1.2 according to OMA Release process and the Enabler Release specification baseline listed below.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2020-11

OMA OMA-ERELD-LWM2M_BinaryAppDataCont-V1_0_1-20190221-A Enabler Release Definition for LwM2M BinaryAppDataCont

 **URL:** https://www.openmobilealliance.org/release/LwM2M_APPDATA/V1_0_1-20190221-A/OMA-ERELD-LWM2M_BinaryAppDataCont-V1_0_1-20190221-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of LwM2M BinaryAppDataCont according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2019-02

OMA OMA-ERELD-LWM2M_Gateway-V1_1-20210518-A Enabler Release Definition for LWM2M Gateway

 **URL:** https://www.openmobilealliance.org/release/LwM2M_Gateway/V1_1-20210518-A/OMA-ERELD-LWM2M_Gateway-V1_1-20210518-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of LWM2M_Gateway according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2021-05

OMA OMA-ERELD-OpenCMAPI-V1_0-20160126-A Enabler Release Definition for Open Connection Manager API

 **URL:** https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-ERELD-OpenCMAPI-V1_0-20160126-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of the Open Connection Manager API (OpenCMAPI) Enabler according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-01

OMA-ER-GotAPI-V1_1-20180724-A Generic Open Terminal API Framework (GotAPI)

 **URL:** https://www.openmobilealliance.org/release/GOTAPI/V1_1-20180724-A/OMA-ER-GotAPI-V1_1-20180724-A.pdf

ABSTRACT: This Enabler Release (ER) document is a combined document that includes requirements, architecture and technical specification of the Generic Open Terminal API Framework (GotAPI) Enabler.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-07

OMA OMA-ETS-LightweightM2M_INT-V1_1-20190912-D Enabler Test Specification (Interoperability) for Lightweight M2M

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/ETS/OMA-ETS-LightweightM2M-V1_1-20190912-D.pdf

ABSTRACT: This document describes in detail available test cases for LightweightM2M as specified in OMA-TS-LightweightM2MV1_1-20180710-A and OMA-TS-LightweightM2M_Transport-V1_1-20180710-A.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-08

OMA OMA-EVP-LightweightM2M-V1_0-20140819-C Enabler Validation Plan for Lightweight M2M

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/EVP/OMA-EVP-LightweightM2M-V1_0-20140819-C.pdf

ABSTRACT: This document details the Validation plan for the Lightweight M2M V1.0 Enabler Release. The successful accomplishment of the validation activities will be required for the Enabler to be considered for Approved status.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2014-08

OMA OMA-RD-CPNS-V1_1-20160209-A Converged Personal Network Service Requirements

 **URL:** https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-RD-CPNS-V1_1-20160209-A.pdf

ABSTRACT: This Requirement Document (RD) defines the requirements for the Converged Personal Network Service-CPNS 1.1 and deferred requirements that can be used as a base for future version of CPNS. The CPNS Enabler enables CPNS entities in a personal network (PN) to consume services within that PN, services from and to other PNs, and services provided by service providers outside the PN.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-02

OMA OMA-RD-DM-V1_2-20070209-A Device Management Requirements

 **URL:** https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-RD-DM-V1_2-20070209-A.pdf

ABSTRACT: The scope of this document is a requirements description for Device Management (for the definition of Device see section 3.2). This document describes a set of functional requirements (partly on an abstract level) for the management of a Device's changeable parameters, as seen from the Management Authority's points of view.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2007-02

OMA OMA-RD-DM-V2_0-20160209-A Device Management Requirements

 **URL:** https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-RD-DM-V2_0-20160209-A.pdf

ABSTRACT: This document contains use cases and requirements for Device Management 2.0. It describes a set of functional requirements for the management of a Device. These functional requirements MAY be overlapped with the requirements for DM 1.x Enabler.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-02

OMA-RD-ENCap-M-V1_0-20180621-A Exposing Network Capabilities to M2M Requirements

 **URL:** https://www.openmobilealliance.org/release/ENCap/V1_0-20180621-A/OMA-RD-ENCap_M-V1_0-20180621-A.pdf

ABSTRACT: This document defines the requirements for Exposing Network Capabilities to M2M Applications and/or M2M Service Platforms through APIs. In addition, it contains: Use cases where M2M Applications and/or M2M Service Platforms can leverage network capabilities to enrich the services or to streamline the operations.; Gap analysis to identify any missing Network APIs to address the above use cases.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2018-06

OMA-RD-GwMO-V1_1-20170725-A GwMO Requirements

 **URL:** https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-RD-GwMO-V1_1-20170725-A.pdf

ABSTRACT: 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).

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2017-07

OMA-RD-LightweightM2M-V1_2-20201110-A OMA Lightweight Machine to Machine Requirements

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-RD-LightweightM2M-V1_2-20201110-A.pdf

ABSTRACT: This document represents Lightweight M2M version 1.2 consolidated requirements.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-11

OMA-RD-M2MInterface-V1_0-20150324-A Management Interface for M2M Requirements

 **URL:** https://www.openmobilealliance.org/release/M2MInterface/V1_0-20150324-A/OMA-RD-M2MInterface-V1_0-20150324-A.pdf

ABSTRACT: This technical report defines requirements for an interface from Device Management (DM) server to the Machine to Machine (M2M) systems on top. This Northbound Interface (NBI) allows M2M service layer to access the DM server functionality. These requirements are derived from device and service management use cases.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2015-03

OMA-RD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Requirements

 **URL:** https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-RD-OpenCMAPI-V1_0-20160126-A.pdf

ABSTRACT: This document defines the requirements for the OMA Open Connection Manager API (OpenCMAPI) V1.0.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-01

OMA OMA-RRELD-ENCap-M2M-V1_0-20180621-A Reference Release Definition for for Exposing Network Capabilities to M2M

 **URL:** https://www.openmobilealliance.org/release/ENCap/V1_0-20180621-A/OMA-RRELD-ENCap-M2M-V1_0-20180621-A.pdf

ABSTRACT: The scope of this document is limited to the Referencer Release Definition of ENCap-M2M according to OMA Release process and the Reference Release specification baseline listed in section 5.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2018-06

OMA OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A Reference Release Definition for M2M Device Classification

 **URL:** https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A.pdf

ABSTRACT: The scope of this document is limited to the Reference Release Definition of the M2M Device Classification White Paper Reference Release according to OMA Release process and the Reference Release document baseline listed in section 5.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2012-10

OMA OMA-RRELD-M2Minterface-V1_0-20150324-A Reference Release Definition for M2Minterface

 **URL:** https://www.openmobilealliance.org/release/M2Minterface/V1_0-20150324-A/OMA-RRELD-M2Minterface-V1_0-20150324-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of M2M interface according to OMA Release process and the Enabler Release specification baseline listed in section 5.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2015-03

OMA OMA-TS-CPNS_Core-V1_1-20160209-A Converged Personal Network Service Core Technical Specification

 **URL:** https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-TS-CPNS_Core-V1_1-20160209-A.pdf

ABSTRACT: This document specifies the functions, interfaces and behaviour of CPNS entities, then protocols and CPNS System concept together with syntax and semantics of CPNS messages.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-02

OMA OMA-TS-DM_Protocol-V2_0-20160209-A OMA Device Management Protocol

 **URL:** https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-TS-DM_Protocol-V2_0-20160209-A.pdf

ABSTRACT: This protocol is called the OMA Device Management Protocol version 2.0, and it defines the

protocol for various management procedures. The scope for this protocol is to define the interfaces that are used between the DM Server and the DM Client. Interfaces residing within the device or within the server are outside of the scope of this specification.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2016-02

OMA OMA-TS-DM-FUMO-V1_0_2-20090828-A Firmware Update Management Object

📄 URL: https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-TS-DM_FUMO-V1_0_2-20090828-A.pdf

ABSTRACT: This document specifies management object(s) and their necessary behaviour to support the updating of firmware in mobile devices. It leverages the OMA DM enabler [OMADM] and supports alternate download mechanisms (such as OMA Download [DLOTA]). This represents the interface between the client and server required to manage the update of a mobile device's firmware.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2009-08

OMA OMA-TS-DM-GwMO_ZigBeeMO-V1_0-20170725-A Management Objects for ZigBee Devices

📄 URL: https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO_ZigBeeMO-V1_0-20170725-A.pdf

ABSTRACT: 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. This ZigBee MO is optional for any OMA DM Gateway implementation.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-07

OMA OMA-TS-GwMO-V1_1-20170725-A Gateway Management Object Technical Specification

📄 URL: https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO-V1_1-20170725-A.pdf

ABSTRACT: This technical specification describes Management Objects and Generic Alerts that are needed to provide the DM Gateway functionality.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-07

(New) OMA OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A Lightweight Machine to Machine Technical Specification: Core

📄 URL: https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A.pdf

ABSTRACT: This document, the LwM2M CORE technical specification, describes the LwM2M messaging layer. The LwM2M TRANSPORT specification, a companion specification, details the mapping of the messaging layer to selected transports. The separation between transport and messaging layer

improves readability and simplifies extending LwM2M to further transports. The LwM2M messaging layer uses a RESTful design with several interfaces and a simple data model.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2024-06

(New) OMA-TS-LightweightM2M_Transport-V1_2_2-20240613-A Lightweight Machine to Machine Technical Specification: Transport Bindings

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-TS-LightweightM2M_Transport-V1_2_2-20240613-A.pdf

ABSTRACT: This document specifies the transport bindings of the Lightweight Machine-to-Machine (LwM2M) protocol version 1.2. The split between the LwM2M core and the transport binding specification improves readability, allows a cleaner separation between the LwM2M messaging layer and the underlying protocols for conveying these messages, and ultimately better extensibility.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2024-06

OMA-TS-LWM2M_BinaryAppDataContainer-V1_0_1-20190221-A Lightweight M2M – Binary App Data Container

 **URL:** https://www.openmobilealliance.org/release/LwM2M_APPDATA/V1_0_1-20190221-A/OMA-TS-LWM2M_BinaryAppDataContainer-V1_0_1-20190221-A.pdf

ABSTRACT: This document defines an Object to be used to transfer Application Data with the Lightweight M2M enabler in order to manage application service data on the device.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2019-02

OMA-TS-LWM2M_Gateway-V1_1-20210518-A Lightweight Machine to Machine Gateway Technical Specification

 **URL:** https://www.openmobilealliance.org/release/LwM2M_Gateway/V1_1-20210518-A/OMA-TS-LWM2M_Gateway-V1_1-20210518-A.pdf

ABSTRACT: This specification extends the LwM2M architecture to support the LwM2M Gateway functionality.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2021-05

OMA-TS-OpenCMAPI-V1_0-20160126-A Open Connection Manager API

 **URL:** https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-TS-OpenCMAPI-V1_0-20160126-A.pdf

ABSTRACT: This specification of the OpenCMAPI defines an interface, through which connection management services are made available to different applications.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2016-01

OMA OMA-WP-M2M_Device_Classification-20121030-A White Paper on M2M Device Classification

 **URL:** https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-WP-M2M_Device_Classification-20121030-A.pdf

ABSTRACT: This document is to provide a Machine-to-Machine (M2M) device classification framework based on the horizontal attributes (e.g., wide area communication interface, local area communication interface, IP stack, human I/O capabilities, persistent configuration storage) of interest to communication service providers (CSPs) and M2M service providers (MSPs), independent of vertical markets, such as smart grid, connected cars, e-health, smart home, etc.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2012-10

(NEW) OMA OMA-ERELD-LightweightM2M-V1_2_2-20240613 Enabler Release Definition for LightweightM2M

 **URL:** https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-ERELD-LightweightM2M-V1_2_2-20240613-A.pdf

ABSTRACT: The scope of this document is limited to the Enabler Release Definition of LightweightM2M v1.2.2 according to OMA Release process and the Enabler Release specification baseline.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-06

Open Group IT4IT Open Messaging Interface (O-MI), The Open Group Standard for the Internet of Things (IoT), Version 2.0

 **URL:** <https://publications.opengroup.org/c19e>

ABSTRACT: The Open Messaging Interface (O-MI) standard connectivity model is similar to that of the World-Wide Web (WWW). Where the WWW uses the HTTP protocol for transmitting HTML-coded information mainly intended for human users, O-MI requests are used for transmitting lifecycle-related information mainly intended for automated processing by information systems. A defining characteristic of the O-MI standard is that O-MI nodes do not have predefined roles, as it follows a “peer-to-peer” communications model

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-12

Open Group MSA-IoT Microservices Architecture for the Internet of Things (MSA-IoT)

 **URL:** <https://publications.opengroup.org/g187>

ABSTRACT: In this Guide, we will explore the synergies between these two evolving solutions, and identify where MSA can be an optimal fit, and an enabler to, IoT solutions. Patterns and critical decision factors relating to security and architecture will be considered, and the benefits of the MSA approach will be further highlighted in a series of case studies.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** 2018-04

(NEW) 5GAA 5G-V2X Direct Communication Evaluation Approach: An Automotive Analysis

 URL: <https://5gaa.org/content/uploads/2024/07/5gaa-wi-nr-v2x-eval.pdf>

ABSTRACT: Fifth-generation Vehicle-to-Everything (5G-V2X) technology, including the new direct communications radio technology (also called NR V2X), is moving toward deployment – starting in Europe with consensus among automotive OEMs, suppliers, and vendors. To prepare for a massive deployment, an evaluation of NR V2X technology is needed. Such an evaluation needs to be realistic enough to cope with automotive requirements, use cases, and system limitations (considering, at least, the first environment for implementation). This White Paper is considering realistic evaluation assumptions based on a common understanding between both the automotive industry and 5G-V2X technology vendors.

 DOCUMENT TYPE: Whitepaper

 PUBLICATION DATE: 2024-07

(NEW) 5GAA Vehicle-to-Network-to-Everything (V2N2X) Communications: Architecture, Solution Blueprint, and Use Case Implementation Examples

 URL: <https://5gaa.org/content/uploads/2024/06/v2n2x-communications-architecture-solution-blueprint-and-use-case-implementation.pdf>

ABSTRACT: This Technical Report (TR) complements the 5GAA whitepaper “Road traffic operation in a digital age” and describes for different stakeholders how to realise various V2X applications and use cases (UCs), using cellular network communications in combination with information sharing structures between backend systems.

The TR provides an application-level reference blueprint architecture and introduces an “information sharing domain” to facilitate a federated, scalable digital data exchange between ecosystem stakeholders, e.g., Vehicle OEMs, Service Providers and Infrastructure Owners and Operators (IOOs). The TR provides descriptions on how to realise V2X applications of different types utilising cellular network communications and information sharing, with different protocols and deployment options across stakeholder domains, and exemplified with safety and mobility-enhancing UCs, such as Traffic event information sharing, Traffic signal information sharing, Traffic signal priority request, Emergency Vehicle Approaching, HD MAP handling, Automated valet parking, Object Detection and Sharing, and Vulnerable Road User protection. The TR also clarifies the different implementation options of the application in a vehicle and related implications, namely OEM-controlled App (OEM App), OEM-supported SP App, and OEMindependent SP App. This TR furthermore describes verified solutions and includes references to initial operational deployments that realise the suggested application level reference architecture, e.g., C-Roads, Talking Traffic, Mobilidata, etc.

 DOCUMENT TYPE: Technical_Report

 PUBLICATION DATE: 2024-05

(NEW) 5GAA Creating Trust in Connected and Automated Vehicles

 URL: <https://5gaa.org/content/uploads/2024/05/5gaa-trust4auto-white-paper-2024.pdf>

ABSTRACT: Connected and Automated Vehicles (CAVs) create a complex, dynamic network, where the safety and behaviour of each ‘node’ or vehicle directly affects the efficiency and safety of the entire system. These systems are vulnerable to untrustworthy actors for various reasons. Therefore, a method to assess and quantify the trustworthiness of shared data is necessary. This will establish trust between cooperating nodes, enabling them to work in collaboration.

This 5GAA white paper proposes a framework for trust assessment within CAVs. By first defining key terms related to trust and trustworthiness, it establishes a foundation for building trust between these vehicles. It then creates a taxonomy for classifying different trust relationships.

Furthermore, the paper details a list of trustworthiness properties crucial for Cooperative Intelligent Transport Systems (C-ITS) and CAVs. These properties serve as the foundation for real-time trust assessments. The paper emphasises the importance of verifiable evidence supporting these assessments, even when dealing with inherent uncertainties within the evidence itself.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2024-05

(NEW) 5GAA Trustable Position Metrics for V2X Applications

🔗 URL: <https://5gaa.org/content/uploads/2023/10/5gaa-a-220044-tpm4v2x-tr-1.pdf>

ABSTRACT: The present document focuses on the issue of trustworthiness in relation to position information exchanged in the context of vehicle-to-everything (V2X) communication. In order to start the analysis, this work has been focusing on Day-1 applications to understand the problem in the context of the current standard.

The document provides an overview of the current standards related to positioning, including the integrity of the position and confidence levels, and reviews the definitions and metrics used so far. It then provides an analysis of the gaps in the current/available V2X standard related to the confident use of such positioning information.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2023-10

(NEW) 5GAA Accelerating 5G Adoption for Connected and Autonomous Mobility Services

🔗 URL: <https://5gaa.org/content/uploads/2023/04/5gaa-wp-market-pull-mapu.pdf>

ABSTRACT: The purpose of this white paper is to highlight the wide array of new business opportunities that 5G will enable for the connected mobility ecosystem.

Our intention is to move the discussion beyond safety and automated driving to other innovative solutions and customer experiences.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2023-04

(NEW) 5GAA C-V2X Use Cases and Service Level Requirements — Volume III

🔗 URL: <https://5gaa.org/content/uploads/2023/01/5gaa-tr-c-v2x-use-cases-and-service-level-requirements-vol-iii.pdf>

ABSTRACT: The present report contains the third volume (Volume III) of 5GAA WG1 agreed use case (UC) descriptions for Use Cases developed within the 5GAA and consolidated in WG1. The results and conclusions of this report, and of the future use case descriptions and related communication requirements, are intended to serve as input for the work of other WGs in 5GAA, as well as sources for input and feedback to standardization activities, e.g., in 3GPP.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2023-01

C2CC C2CCC_RS_2037 Vehicle C-ITS station profile

 **URL:** https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2037_Profile.pdf

ABSTRACT: For interoperability, each sub-system of Cooperative Intelligent Transport System (C-ITS) (vehicle, roadside, personal and central) requires a specific set of standards, called system profile, defining in which way possible options of the related standards are implemented. Thus, the system profile describes external interfaces matching those of other sub-systems where communication is intended. This document provides all requirements related to the features of a vehicle C-ITS station to enable Inter-sub-system interoperability. In terms of C2C-CC each requirement details a feature (which again details an objective) and provides its implementation details. In some cases, requirements are written in a way which let the implementation open, for example if they refer to very specific parts of a vehicle. Those requirements have to be further detailed by anybody implementing that requirement. Beside these special requirements, all other requirements can be further detailed, too.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-12

C2CC C2CCC_TR_2000 C2CCC_TR_2000_ReleaseOverview - Basic System Profile Release Overview, Release 1.6.1

 **URL:** https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_TR_2000_ReleaseOverview.pdf

ABSTRACT: This Release Overview provides information on the specification which are part of this release, like: a) which deliverables are part of the release or; b) what are the changes since the last release. Furthermore, C2C-CC has published a large set of white papers, studies and technical reports which can be found at <https://www.car-2-car.org/documents/general-documents/>. Publications from external sources, but yet related to the work of C2C-CC, are also available at <https://www.car-2-car.org/documents/publications/>.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-12

(Updated) CEN ISO/TS 17425:2016 Intelligent transport systems - Cooperative systems - Data exchange specification for in-vehicle presentation of external road and traffic related data

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:35914&cs=10C18F278124980B9F4075E355AB45BC3

ABSTRACT: This document defines the In-Vehicle Signage service and application that delivers In-Vehicle Signage information to ITS stations (vehicle ITS stations or personal ITS stations devices) concerning road and traffic conditions, qualified by road authorities/operators, in a consistent way with road authority's/operator's requirements, in the manner that is coherent with the information that would be displayed on a road sign or variable message sign (VMS).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-06

(Updated) CEN ISO/TS 17429:2017 Intelligent transport systems - Cooperative ITS - ITS station facilities for the transfer of information between ITS stations

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:35915&cs=1DF674B52BAF01613FICDAABBB1D408E6

ABSTRACT: ISO/TS 17429:2017 specifies generic mechanisms enabling the exchange of information between ITS stations for applications related to Intelligent Transport Systems. It complies with the ITS station reference architecture (ISO 21217) and defines the following ITS station facilities layer functionalities: - Communication Profile Handler (CPH); - Content Subscription Handler (CSH); - Facilities Services Handler (FSH). These functionalities are used by ITS-S application processes (ITS-S-AP) to communicate with other ITS-S application processes and share information. These functionalities describe - how lower-layer communication services assigned to a given data flow are applied to the service data units at the various layers in the communication protocol stack (CPH, see 6.2.3), - how content from data dictionaries can be published and subscribed to by ITS-S application processes (CSH, see 6.2.5), - how well-known ITS station facilities layer and management services can be applied to application process data units (FSH, see 6.2.4), relieving (ITS-S) application processes from having to implement these services on their own, - how service access points (SAP) primitives specified in ISO 24102-3 are used, - service primitives for the exchange of information between ITS-S application processes and the ITS station facilities layer (FA-SAP), and - a set of communication requirements and objectives (profiles) using the methods defined in ISO/TS 17423 to select the level of performance (best effort or real-time, etc.), confidence and security (authentication, encryption, etc.) for information exchange between ITS stations, such as data provision, event notification, roadside configuration, map update.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-04

(Updated) CEN ISO/TS 19091:2019 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:64994&cs=155A0F218787309EC4D33F96797394306

ABSTRACT: This document defines the message, data structures, and data elements to support exchanges between the roadside equipment and vehicles to address applications to improve safety, mobility and environmental efficiency. In order to verify that the defined messages will satisfy these applications, a systems engineering process has been employed that traces use cases to requirements and requirements to messages and data concepts. This document consists of a single document that contains the base specification and a series of annexes. The base specification lists the derived information requirements (labelled informative) and references to other standards for message definitions where available. Annex A contains descriptions of the use cases addressed by this document. Annexes B and C contain traceability matrices that relate use cases to requirements and requirements to the message definitions (i.e. data frames and data elements). The next annexes list the base message requirements and application-oriented specific requirements (requirements traceability matrix) that map to the message and data concepts to be implemented. As such, an implementation consists of the base plus an additional group of extensions within this document. Details on information requirements, for other than SPaT, MAP, SSM, and SRM messages are provided in other International Standards. The focus of this document is to specify the details of the SPaT, MAP, SSM, and SRM supporting the use cases defined in this document. Adoption of these messages varies by region and their adoption can occur over a significant time period. This document covers the interface between roadside equipment and vehicles. Applications, their internal algorithms, and the logical distribution of application functionality over any specific system architecture are outside the scope of this document.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-07

CEN ISO/TS 19321:2020 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68350&cs=1FE9288D0BD55B9A6A45F662E5E523F64

ABSTRACT: This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

(Updated) CEN ISO/TS 19321:2020 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68350&cs=1FE9288D0BD55B9A6A45F662E5E523F65

ABSTRACT: This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

(Updated) CEN prCEN ISO/TS 19321 rev Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:FSP_LANG_ID:73937,25&cs=108B9C05FB54333B566ACFD5122C7E1F9

ABSTRACT: This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-07

ETSI EN 302 636-1 ITS; Vehicular Communications; GeoNetworking; Part 1: Requirements

URL: http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf

ABSTRACT: This document is the first part of a multi-part standard. It specifies the general, functional and performance requirements that apply to the GeoNetworking protocols. It is applicable to ITS stations implementing ETSI ITS for both single hop and multi-hop communications.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2014-04

ETSI EN 302 637-2 ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

URL: http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf

ABSTRACT: Cooperative awareness within road traffic means that road users and roadside infrastructure are informed about each other's position, dynamics and attributes. Road users are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians and roadside infrastructure equipment including road signs, traffic lights or barriers and gates. The awareness of each other is the basis for several road safety and traffic efficiency applications with many use cases as described in ETSI TR 102 638. It is achieved by regular exchange of information among vehicles (V2V, in general all kind of road users) and between vehicles and road side infrastructure (V2I and I2V) based on wireless networks, called V2X network and as such is part of Intelligent Transport Systems (ITS). The information to be exchanged for cooperative awareness is packed up in the periodically transmitted Cooperative Awareness Message (CAM). The construction, management and processing of CAMs is done by the Cooperative Awareness basic service (CA basic service), which is part of the facilities layer within the ITS communication architecture.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2019-04

ETSI EN 302 637-3 ITS; Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

URL: http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.03.01_60/en_30263703v010301p.pdf

ABSTRACT: The DEN basic service is an application support facility provided by the ITS facilities layer. It constructs, manages and processes the Decentralized Environmental Notification Message (DENM). The construction of a DENM is triggered by an ITS-S application. A DENM contains information related to a road hazard or an abnormal traffic conditions, such as its type and its position. Typically for an ITS application, a DENM is disseminated to ITS-S that are located in a geographic area through communications among ITS stations. At the receiving side, the DEN basic service of an receiving ITS-S processes the received DENM and provides the DENM content to an ITS-S application.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2019-04

ETSI EN 302 663 ITS; ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

 **URL:** http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf

ABSTRACT: The present document specifies the European profile of the physical and medium access control sub-layer of 5 GHz intelligent transport systems (ITS) using IEEE 802.11 as the base standard. One of the additionally selected functionalities being an essential part of the present document is "communication outside the context of a BSS" as developed by IEEE 802.11.

Communication outside the context of a BSS enables exchange of data frames between stations that are not members of a BSS. This type of communication allows for immediate exchange of data frames, avoiding the latency associated with the establishment of a BSS.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-01

ETSI EN 303 613 ITS; LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

 **URL:** http://www.etsi.org/deliver/etsi_en/303600_303699/303613/01.01.01_60/en_303613v010101p.pdf

ABSTRACT: This document specifies the access layer for the LTE-V2X technology.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-01

ETSI TR 101 607 ITS; Cooperative ITS (C-ITS); Release 1

 **URL:** http://www.etsi.org/deliver/etsi_tr/101600_101699/101607/01.02.01_60/tr_101607v010201p.pdf

ABSTRACT: For the development of standards which address Cooperative Intelligent Transport Systems (C-ITS) a release oriented process has been adopted. The present document lists standards, specifications and other deliverables which have been developed to form a consistent set of standards as the basis for Release 1 including standards for interoperability developed in accordance with the work plan of the European Commission Standardisation Mandate M/453.

The deliverables forming Release 1 are synchronized and harmonized with similar documents prepared by other SDOs such as ISO/CEN, IEEE and SAE. The present document also serves as basis for defining further standardization activities which will lead to forming the Release 2 of standards related to Cooperative ITS.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-02

(Updated) ETSI TR 102 638 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Release 2

 **URL:** https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/02.01.01_60/tr_102638v020101p.pdf

ABSTRACT: This document is currently under revision to document the Release 2 set of standards.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-04

ETSI TS 103 544-1 Publicly Available Specification (PAS); ITS; MirrorLink; Part 1: Connectivity

 **URL:** http://www.etsi.org/deliver/etsi_ts/103500_103599/10354401/01.03.01_60/ts_10354401v010301p.pdf

ABSTRACT: Definition of the lower layer wired and wireless connectivity protocols for MirrorLink. Integration of change requests based on feedback from plugfests and initial implementations undergoing CCC's MirrorLink device certification program.

This document is the first part of a multi-part standard made of 29 specifications (TS 103 544-n).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-10

ITU-T F.749.1 (11/2015) Functional requirements for vehicle gateway

 **URL:** <https://handle.itu.int/11.1002/1000/12631>

ABSTRACT: This recommendation specifies functional requirements for vehicle gateway (VG), including transport functional requirements, networking functional requirements, network access functional requirements, communication-with-in-vehicle devices functional requirements, and network access management & security functional requirements. It also describes communications interfaces to support the seamless wired and wireless connectivity in the heterogeneous access network environments.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-11

ITU-T F.749.2 (03/2017) Service requirements for vehicle gateway platforms

 **URL:** <https://handle.itu.int/11.1002/1000/13183>

ABSTRACT: This recommendation provides the service description, application scenarios and requirements for Vehicle Gateway Platforms. A series of Recommendations for Vehicle Gateway Platforms is currently opened in ITU- T SG 16. This recommendation is part of that series and gives the service description, application scenarios and requirements.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-03

ISO/IEC 30144:2020 Internet of things (IoT) - Wireless sensor network system supporting electrical power substation

 **URL:** <https://webstore.iec.ch/publication/62503>

ABSTRACT: ISO/IEC 30144:2020 (E) specifies intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure and communications internal and external to the infrastructure, and technical requirements for iWSN to realize smart electrical power substations.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-10

ITU-T L.1221 (11/2018) Innovative energy storage technology for stationary use - Part 2: Battery

 **URL:** <https://handle.itu.int/11.1002/1000/13721>

ABSTRACT: This recommendation contains the main requirements for evaluating appropriate innovative batteries for stationary use for powering ICT equipment in telecom sites, active network units and data centres or customer premises with standardized power interfaces in –48V, up to 400 VDC or 12V.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-11

ITU-T L.1222 (05/2018) Innovative energy storage technology for stationary use - Part 3: Supercapacitor technology

 **URL:** <https://handle.itu.int/11.1002/1000/13579>

ABSTRACT: This recommendation provides an overview of available supercapacitor (SC) technology, with details of SC characteristics (electrical, mechanical, thermal) and applicability in the telecommunication/information and communication technology (TLC/ICT) domain.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-05

(NEW) ITU-T Y. EPWS-fc: Functional capabilities to support IoT-based electric power work site operation services

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19613

ABSTRACT: The power industry is one of the cornerstones of modern human society, providing a stable and reliable energy supply for everyone. As the process of urbanization accelerates, the demand for electricity also grows. The United Nations' "Tracking SDG7: The Energy Progress Report" sets a goal to focus on ensuring that people have access to affordable, reliable, and sustainable modern energy. From environmental protection to sustainable development, an adequate and reliable power supply is an important support for economic transformation and an important guarantee for harmonious social development. The electric power work site (EPWS) is the core place for the operation and maintenance of the power system, characterized complexity in operations. This proposal is going to standardize functional capabilities of electric power work site operation services to improve operational efficiency, providing an important technical means for establishing a safe, scientific, and efficient electric power work site.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-DPE Management framework for IoT-based distributed power equipment

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18745

ABSTRACT: In recent years, the trend towards the intelligence and IoT integration of power equipment has become increasingly evident. Utilizing various distributed sensors and their IoT systems enables functions such as power equipment status monitoring, diagnostic evaluation, and maintenance decision-making. Meanwhile, the safe, stable, and reliable operation of power equipment also depends on the effective collaboration of numerous IoT sensing and controlling devices. Consequently, the need for unified management and coordination of power equipment and their sensing/controlling devices using distributed IoT technology has become increasingly urgent. This Recommendation provides the management framework for IoT-based distributed power equipment, including the framework, functional systems, and reference interfaces.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.4706 (ex Y.dem-IoT) Data exchange model for IoT devices in power transmission and transformation equipment

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18743

ABSTRACT: The Internet of things (IoT) devices in the power transmission and transformation equipment can meet the demand for comprehensive and accurate data acquisition of power transmission and transformation equipment. It is necessary to develop a data exchange model for enable applications, sharing, coordination when constructing the system for power transmission and transformation equipment based on IoT. This Recommendation provides the requirements and model of IoT data exchange in power transmission and transformation equipment.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2024-07

Zigbee Document 07-5356-21 Zigbee Smart Energy Standard

URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: This document is a standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy and water. A wireless network is implemented at the consumer's premises using the ZigBee® PRO protocol with the Smart Energy application profile. It enables the development of smart energy applications.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2017-06

Zigbee Document 14-0563-18 Zigbee PRO Green Power feature specification Basic functionality set V1.1.1

URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: This document specifies a wireless feature of Zigbee® that allows for energy-harvesting technology to be used directly with the Zigbee stack. Zigbee® Green Power (ZGP) enables battery-less

(energy-harvesting) or ultra-long battery devices to securely join Zigbee® PRO networks. Common ZGP devices include switches, sensors, detectors, and buttons. ZGP uses a compact packet format that minimizes the amount of energy used to transmit data. This allows energy-harvesting devices to operate successfully and battery-powered devices to operate for periods in excess of what would be possible on a standard Zigbee network before requiring a replacement battery.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-11

WITSML WITSML (Well-site Information Transfer Standard Markup Language) 2.0 (2016)

🔗 URL: http://docs.energistics.org/WITSML/WITSML_TOPICS/WITSML-000-000-titlepage.html

ABSTRACT: Data and Information - WITSML is the upstream oil and gas data-transfer standard for specifying and exchanging data for wells and well-related operations and objects, such as drilling, logging, and mud logging.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-11

Water

CEN EN 13757-2:2018/prA1 Communication systems for meters - Part 2: Wired M-Bus communication

🔗 URL: https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT,FSP_LANG_ID:74544,25&cs=1761F4D6E55C0F87848EB2822BAF9FAAF

ABSTRACT: This draft European standard is applicable to the physical and link layer parameters of baseband communication over twisted pair (M Bus) for meter communication systems. It is especially applicable to thermal energy meters, heat cost allocators, water meters and gas meters. NOTE It is usable also for other meters (like electricity meters) and for sensors and actuators. For generic descriptions concerning communication systems for meters and remote reading of meters see EN 13757-1.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

ISO/IEC 30142:2020 Internet of Things (IoT) - Underwater acoustic sensor network (UWASN) - Network management system overview and requirements

🔗 URL: <https://webstore.iec.ch/publication/62443>

ABSTRACT: ISO/IEC 30142:2020 provides the overview and requirements of a network management system in underwater acoustic sensor network (UWASN) environment. It specifies the following: a) functions which support underwater network management system; b) entities required for underwater network management system; c) data about the communication between elements in underwater network management system; d) guidelines to model the underwater network management system; e) general and functional requirements of underwater network management system

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06

ISO/IEC 30143:2020 Internet of Things (IoT) - Underwater acoustic sensor network (UWASN) - Application profiles

 **URL:** <https://webstore.iec.ch/publication/62405>

ABSTRACT: ISO/IEC 30143:2020 provides the guidelines for designing and developing new applications in the underwater environment such as fish farming, environment monitoring, harbour security, etc. This document also: a) provides the components required for developing the application; b) provides instructions for modelling the application with examples; c) helps the user to understand the communication between the elements in the application for modelling the communication between elements; d) guides the user with the design process of underwater applications.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06

ISO/IEC 30171-1 Information technology — Internet of Things (IoT) — Base-station based Underwater Wireless Acoustic Network (B-UWAN) – Part 1: Overview and requirements

 **URL:** <https://webstore.iec.ch/publication/66927>

ABSTRACT: ISO/IEC 30171-1:2022 provides the general overview of base-station based underwater wireless acoustic networks (B-UWANs). It gives detailed description for main components of B-UWAN and also provides functions of B-UWAN components. It further specifies the requirements of B-UWAN.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-05

ISO/IEC TR 30167:2021 Internet of Things (IoT) - Underwater communication technologies for IoT

 **URL:** <https://webstore.iec.ch/publication/65619>

ABSTRACT: ISO/IEC TR 30167:2021 describes the enabling and driving technologies of underwater communication such as acoustic communication, optical communication, Very Low Frequency (VLF)/Extremely, Low Frequency (ELF) communication, and Magnetic Fusion Communication (MFC). This document also highlights: a) technical overview of different communication technologies; b) characteristics of different communication technologies; c) trends of different communication technologies; d) applications of each communication technology; e) benefits and challenges of each communication technology.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-06

ETSI TR 103 290 Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment

 **URL:** http://www.etsi.org/deliver/etsi_tr/103200_103299/103290/01.01.01_60/tr_103290v010101p.pdf

ABSTRACT: Smart City study would undertake compilation and review of activities taking place in the area of SMART City in Europe, Asia, and US. It will analyse the relevance of Smart City applications, and possible underlying network architecture. The report will describe use case descriptions for Smart City applications in context of but not limited to IoT communications.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2015-04

ETSI TS 103 424 Publicly Available Specification (PAS); Smart Machine-to-Machine communications (SmartM2M)

 **URL:** http://www.etsi.org/deliver/etsi_tr/103500_103599/103527/01.01.01_60/tr_103527v010101p.pdf

ABSTRACT: The Home Gateway Initiative (HGI) worked on Specifications for home connectivity and Services enablement, in particular to encompass a delivery framework for Smart Home services. The defined architecture includes support for a standard, general purpose software execution environment in the HG (for third party applications), API definitions, device abstraction and interfacing with Cloud based platforms. This specification defines a smart home system architecture and derives requirements for the Home Gateway.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2016-11

ITU-T Y.4805 (08/2017) Identifier service requirements for the interoperability of Smart City applications

 **URL:** <https://handle.itu.int/11.1002/1000/13267>

ABSTRACT: This recommendation specifies a set of requirements for identifier services in smart city applications with a view to ensure that such systems are interoperable and secure. This set of requirements may additionally serve as guidelines for developing new identifier services for smart city. It includes security features for service integrity, data confidentiality. The recommendation defines a full list of identifier service requirement, including security requirements, for the identifier service.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-08

(NEW) ITU-T Y.SCCNS-Reqts Requirements of smart city communication network system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19603

ABSTRACT: Smart sustainable city is a new concept and model of global urban development. The smart city communication network provides support for different smart city systems (such as energy management, emergency management, etc.) and smart city platforms. There is currently no identified standards specification specifying requirements of smart city communication network. It is needed to study smart city communication network based on the comprehensive requirements of the smart cities. Based on the study of different application scenarios of smart city communication

network system, this Recommendation introduces the concept of smart city communication network system (SCCNS), which provides a reliable and secure data transmission service between the SCP and Sensing and Data Collection Systems (SDCS). It then analyses the requirements of the SCCNS and specifies the functions of SCCNS. The study aims to enable enhanced support of the operation of diverse services and applications in smart cities and provide guidance for the design and deployment of smart city communication network by clarifying the requirements and functions of SCCNS.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Buildings

ZigBee Document 15-0014-05 ZigBee Lighting & Occupancy Device Specification

🔗 URL: <https://csa-iot.org/developer-resource/specifications-download-request/>

ABSTRACT: The Zigbee® Lighting & Occupancy Device (ZLO) Specification is a subset of the Zigbee Home Automation Profile specification that focuses specifically on Lighting & Occupancy-type Zigbee® devices. This document includes device-type definitions, required clusters for each device type, and required attributes for each cluster.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-02

Built Environment

(Updated) CENELEC prEN 50090-6-3 Home and Building Electronic Systems (HBES)- Part 6-3 -3rd Party HBES IoT API

🔗 URL: https://standards.cenelec.eu/dyn/www/f?p=305:110:0::FSP_PROJECT,FSP_LANG_ID:74475,25&cs=1046EE8EC4361FACC3F6370EBB7B68089

ABSTRACT: The 3rd Party HBES IoT API consists of:

- 📄 Required restful access methods to read or write Endpoints, to set or retrieve Installation state data.
- 📄 Required Endpoints hosting concepts such as Functions and Datapoints comprising the Runtime communication of an (HBES) Installation.
- 📄 Required methods to authorize from an IoT 3rd Party Client, additionally, such as the security methods to be used to access the API.
- 📄 Required access permission control types: for security reasons the actual access to Functions or Datapoints is gated by the IoT 3rd Party Server, this access will be granted as part of the authorization.
- 📄 Endpoints allowing to setup notifications on changes of Installation state data, provided to subscribers that are clients to the Installation.
- 📄 For all Endpoints, their expected request/ response document formats, and their content. Moreover, their mandatory and optional parts

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-07

ETSI TR 103 394 Smart Body Area Networks (SmartBAN); System Description

 **URL:** http://www.etsi.org/deliver/etsi_tr/103300_103399/103394/01.01.01_60/tr_103394v010101p.pdf

ABSTRACT: This report provides the system description for Smart Body Area Networks (Smart BANs). It defines the system overview and use cases of Smart BAN.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-01

ETSI TR 103 751 Smart Body Area Networks (SmartBAN); Implant communications

 **URL:** http://www.etsi.org/deliver/etsi_tr/103700_103799/103751/01.01.01_60/tr_103751v010101p.pdf

ABSTRACT: This report evaluates ultra-low power, ultra-wide band technology (UWB) for a swallowable, pill-camera, wireless medical device operating in the 3,1 GHz to 10,6 GHz frequency band. This evaluation is within the context of Smart Body Area Networks (SmartBAN). It considers the SmartBAN requirements, UWB physical layer (PHY) regulation and Medium Access Control (MAC) layer parameters, such as: data rates, modulation, forward error correction, signal-to-noise ratio, quality-of-service and channel sharing, which does not cover article 3.1(b) and 3.2 requirements. The output is a report containing the results of the studies and simulations and concluding with recommendations.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-04

(Updated) ETSI TS 103 325 V1.2.1 Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN

 **URL:** https://www.etsi.org/deliver/etsi_ts/103300_103399/103325/01.02.01_60/ts_103325v010201p.pdf

ABSTRACT: This standard specifies the medium access control and routing for Smart Body Area Networks (Smart BANs). It defines an ultra low power medium access control protocol for on-body communications between a hub and sensor nodes. It also contains provision made for relaying of data through a relay node to the hub.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-07

ETSI TS 103 326 Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103326/01.02.01_60/ts_103326v010201p.pdf

ABSTRACT: This standard specifies the Physical Layer for Smart Body Area Networks (Smart BANs). It defines the lowest layer of the Open Systems Interconnection (OSI) model, the Physical Layer, for on-body communications between a hub and sensor nodes. It has also been enhanced by introducing a more robust synchronization for generic IoT.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-07

ETSI TS 103 327 Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327v010101p.pdf

ABSTRACT: This standard gives the high level description of infrastructure and mechanisms providing solutions for heterogeneity management in Smart BANs. The scope mainly covers the networking level up to the service and application level. The expected solutions mainly concerns the description and the specification of a standardized infrastructure for Smart BAN entities (e.g. sensors, actuators) interactions, data access and monitoring, irrespective of whatever lower layers and radio technologies are used underneath. Finally, on the service and application side, standardized APIs for secure interaction and access to SmartBAN data/entities (data transfer and sharing mechanisms included) are addressed (e.g. PN inspired, web based, XaaS).

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-04

ETSI TS 103 378 Smart Body Area Networks (SmartBAN) Unified data representation formats, semantic and open data model

 **URL:** http://www.etsi.org/deliver/etsi_ts/103300_103399/103378/01.01.01_60/ts_103378v010101p.pdf

ABSTRACT: This standard specifies and formalizes SmartBAN unified data representation formats, semantic open data model and corresponding ontology.

It is applicable to a BAN and/or a Smart BAN comprising wearable sensors/actuators devices, a relay/coordinator device and a Hub. The relay/Coordinator and the Hub functionalities may be handled by a single device or by two distinct devices.

In particular, it defines a unified description model with an extensible semantic metadata for Smart BAN entities and related data (including in particular sensor/actuator/relay/coordinator/Hub descriptions and sensed/measured data), as well as for key monitoring and control information.

The document does not address the specification and the formalization of the SmartBAN service ontology and associated enablers. This will be addressed in later dedicated documents of TC SmartBAN.

DOCUMENT TYPE: Standard_Specification

 **PUBLICATION DATE:** 2015-12

ETSI TS 103 757 SmartM2M; Asynchronous Contact Tracing System; Fighting pandemic disease with Internet of Things (IoT)

 **URL:** http://www.etsi.org/deliver/etsi_ts/103700_103799/103757/02.01.01_60/ts_103757v020101p.pdf

ABSTRACT: Asynchronous Contact Tracing (ACT) traces the IoT connected object that may have been infected by the Covid-19 virus (or future pandemic viruses).

This shifts the paradigm, from searching for a person in the process of infecting another to the tracing of both potential contamination and infections, and leveraging on the combination of the two information.

The scope of this WI is to standardize the full support of Asynchronous Contact Tracing (ACT) by means of

- a) providing some examples of use and deployment of ACT by means of a few explanatory use cases.
- b) specifying the ACT method and its interaction with deployed contact tracing applications for human and systems. This includes the interaction with the different technologies used by non ACT contact tracing solutions.
- c) specifying the ACT system including application protocols and API.

The new ACT method will require the use of existing ready-to-market IoT-based technology and well-established wireless network techniques, in particular the ones specified in the ETSI standards ecosystem.

Moreover, it will preserve the user's privacy in accordance with GDPR and/or other regional requirements not requiring the transmission of any personal information by the user.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-08

HL7 FHIR Fast Healthcare Interoperability Resources (FHIR) v4.0.1 (2019)

🔗 URL: <http://hl7.org/fhir/directory.html>

ABSTRACT: Data and Information Management, Interoperability - FHIR is a standard describing data formats and elements and an application programming interface for exchanging electronic health records.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-05

(Updated) IEC 63203-801-1 Wearable electronic devices and technologies - Part 801-1: Smart Body Area Network (SmartBAN) - Enhanced Ultra-Low Power Physical Layer

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:38:615499235431339::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20537,23,103719

ABSTRACT: This part of IEC 63203-801 specifies the ultra-low power physical layer (PHY) Smart BAN. As the use of wearables and connected body sensor devices grows rapidly in the Internet of Things (IoT), Wireless Body Area Networks (BAN) facilitate the sharing of data in smart environments such as smart homes, smart life etc. In specific areas of digital healthcare, wireless connectivity between the edge computing device or hub coordinator and the sensing nodes requires a standardized communication interface and protocols. The present document describes the Physical Layer (PHY) specifications: - packet formats; - modulation; - forward error correction

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-11

(Updated) IEC 63203-801-2 Wearable electronic devices and technologies - Part 801-2: Smart Body Area Network (SmartBAN) - Low Complexity Medium Access Control (MAC) for SmartBAN

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:38:615499235431339::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20537,23,103720

ABSTRACT: 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.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-11

ISO/CD 24227 ISO/CD 24227 Accuracy evaluation protocol for daily living walking speed extracted from sensor systems that measure human body motion

 **URL:** www.iso.org/standard/78134.html

ABSTRACT: System Architecture - Accuracy evaluation protocol for daily living walking speed extracted from sensor systems that measure human body motion.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

ITU-T H.831 (01/2015) Conformance testing: WAN Interface Part 1: Web services interoperability: Sender

 **URL:** <https://handle.itu.int/11.1002/1000/12249>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.832 (01/2015) Conformance testing: WAN Interface Part 2: Web services interoperability: Receiver

 **URL:** <https://handle.itu.int/11.1002/1000/12250>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.833 (01/2015) Conformance testing: WAN Interface Part 3: SOAP/ATNA: Sender

 **URL:** <https://handle.itu.int/11.1002/1000/12251>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.834 (01/2015) Conformance testing: WAN Interface Part 4: SOAP/ATNA: Receiver

 **URL:** <https://handle.itu.int/11.1002/1000/12252>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.835 (01/2015) Conformance testing: WAN Interface Part 5: PCD-01 HL7 Messages: Sender

 **URL:** <https://handle.itu.int/11.1002/1000/12253>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.836 (01/2015) Conformance testing: WAN Interface Part 6: PCD-01 HL7 Messages: Receiver

 **URL:** <https://handle.itu.int/11.1002/1000/12254>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

ITU-T H.837 (01/2015) Conformance testing: WAN Interface Part 7: Consent Management: Sender

 **URL:** <https://handle.itu.int/11.1002/1000/12255>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-01

oneM2M TR-0022-V2.0.0 Continuation & integration of HGI Smart Home activities

 **URL:** https://onem2m.org/images/files/deliverables/Release2/TR-0022-Continuation_and_Integration_of_HGI_Smart_Home_activities-V2_0_0.pdf

ABSTRACT: The present document is a study of the continuation and integration of some HGI Smart Home activities into oneM2M, following the (PT2) HGI announcement of its closure by June 2016. It includes the description of HGI SH deliverables versus the appropriate oneM2M deliverables for the integration of these HGI achievements.

It intends to be used as a liaison working document with HGI about the status progress of this continuation and integration and is expected to be useful for both HGI and oneM2M to check that all technical items from HGI SH Task Force expected to be integrated are appropriately handled by oneM2M.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-08

■ Organization

Horizontals & Verticals

ENISA Good practices for IoT and Smart Infrastructures Tool

🔗 **URL:** <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool>

ABSTRACT: This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.

📄 **DOCUMENT TYPE:** Database

📅 **PUBLICATION DATE:** N/A

IEC role in the IoT

🔗 **URL:** <https://www.iec.ch/basecamp/iec-role-iot>

ABSTRACT: 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 will increase 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.

📄 **DOCUMENT TYPE:** Presentation

📅 **PUBLICATION DATE:** 2018-10

(Updated) ISO/IEC 30186 Digital Twin – Maturity model and guidance for a maturity assessment

🔗 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108352

ABSTRACT: 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.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** Under development

ISO/IEC TR 30164:2020 Internet of Things (IoT) - Edge computing

🔗 **URL:** <https://webstore.iec.ch/publication/62522>

ABSTRACT: 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.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2020-04

ITU-T H.821 (04/2017) Conformance of ITU-T H.810 personal health system: Healthcare information system interface

 **URL:** <https://handle.itu.int/11.1002/1000/13200>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for HRN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices by HRN Interface to transfer patient information from a Continua WAN device (HRN Sender) to an Electronic Health Record device (HRN Receiver). This document only focuses on the TSS&TP for HRN Sender because, at this moment, HRN Receiver is out of the scope of Continua Certification Program.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2017-04

ITU-T H.841 (08/2020) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 1: Optimized Exchange Protocol: Personal Health Device

 **URL:** <https://handle.itu.int/11.1002/1000/14344>

ABSTRACT: This recommendation provides a test suite structure (TSS) and the test purposes (TP) for personal health devices using the IEEE 11073-20601 optimized exchange protocol in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITU-T H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-08

ITU-T H.843 (08/2018) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 3: Continua Design Guidelines: Personal Health Device

 **URL:** <https://handle.itu.int/11.1002/1000/13680>

ABSTRACT: The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for PAN/LAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2018-08

■ Privacy and Security

Horizontals & Verticals

(NEW) ETSI TS 103 701 V1.1.1 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

 **URL:** http://www.etsi.org/deliver/etsi_tr/103400_103499/103438/01.01.01_60/tr_103438v010101p.pdf

ABSTRACT: The goal of this TR is to consider Digital Ecosystem through user's point of view under the following two directions:

- identification of user's needs such as QoS, security, usability, flexibility, Service Level Objectives (SLO)
- study impact of technical implementations related to user's requirements/concerns

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2019-02

(NEW) ETSI TR 103 621 V1.2.1 Guide to Cyber Security for Consumer Internet of Things

 **URL:** http://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf

ABSTRACT: The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-09

(NEW) ETSI TS 103 927 V1.1.1 CYBER; Cyber Security for Consumer Internet of Things; Requirements for Smart Voice-Controlled Devices

 **URL:** http://www.etsi.org/deliver/etsi_ts/103900_103999/103927/01.01.01_60/ts_103927v010101p.pdf

ABSTRACT: The present document defines security provisions for Smart Voice-Controlled Devices extending from the provisions for consumer IoT devices defined in ETSI EN 303 645.

In terms of security concerns, Smart Voice-Controlled Device has a different focus than other generic IoT devices (e.g., distributed sensors, smart appliances, etc.). For example, Smart Voice-Controlled Devices mainly interact with users through voice assistants that can understand users' voice commands and assist users to control other devices in the IoT network. This feature actually expands the attack surface of Smart Voice-Controlled Devices. In addition, Smart Voice-Controlled Devices usually collect the user's voice and train a model uniquely suitable for the current user to provide personalized service. Therefore, Smart Voice-Controlled Devices-related privacy protection issues are particularly prominent. This vertical will focus on addressing the unique security issues of Smart Voice-Controlled Devices.

NOTE 1: Smart Voice-Controlled Devices in the context of this standard refers specifically to Smart Voice-Controlled Devices used in consumer environments, not those used in industrial environments. Smart Voice-Controlled Devices for industrial purpose is not in the scope of this document.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-01

(NEW) ETSI TR 103 936 V1.1.1 Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control

 **URL:** http://www.etsi.org/deliver/etsi_tr/103900_103999/103936/01.01.01_60/tr_103936v010101p.pdf

ABSTRACT: The use of IoT devices by users to abuse and coerce vulnerable users is a matter that ETSI cannot ignore. The number, and format, of devices, their penetration, and their core functionality, all make them attractive to both the vulnerable user and their abuser. The intent of this work item is to identify design practices that guide the development of measures that allow some degree of mitigation in both the devices themselves and in the services that the devices support.

Thread #1: Coercive control resistant design

The role of coercive control resistant design is addressed in device and service design. It is expected that this will examine and guide the designer on the roles of user identification, location and access control, in order to limit, where possible, the ability of the abusive or coercive party to use the device whilst not limiting the access to the device functionality by the intended user.

Thread #2: Trauma informed design

Trauma informed design requires acceptance that devices are actively targeted as threat-agents of coercion. This element of the work is expected to address feature extensions in IoT devices and services to allow the at risk user to seek help without interference from the coercive party. The work should also identify where future standards are required to further strengthen the protection of the vulnerable user.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-01

(NEW) ETSI TS 103 815 V1.1.1 CYBER; Cyber Security for Consumer Internet of Things; Requirements for Residential Smart Door Locking Devices

 **URL:** http://www.etsi.org/deliver/etsi_ts/103800_103899/103815/01.01.01_60/ts_103815v010101p.pdf

ABSTRACT: This document specifies requirements and guidelines for cyber security, credential related security, electromechanical security and mechanical security (e.g. referring to existing CEN standards) of consumer residential connected smart door locking devices. This document builds on EN 303 645 for cyber security requirements, adding additional provisions specific to smart door locking devices. This document builds on other standards for credential related security, electromechanical security and mechanical security. The document includes both product security performance requirements and test methodology. The intent is to provide an appropriate level of assurance.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-01

(NEW) ITU-T Y.IoT-IADS Intelligent anomaly detection system for Internet of things

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19643

ABSTRACT: This draft new Recommendation proposes an Intelligent Anomaly Detection System for IoT (IADS), which leverages advanced technologies to identify and mitigate anomalous behaviors in IoT-based systems. This system utilizes a hybrid approach, combining rule-based security mechanisms for known attacks with machine learning techniques to detect and adapt to new anomalies. This dual-method approach enhances the security of IoT applications and systems by bringing protection closer to the IoT devices. The IADS framework includes comprehensive guidelines and best practices designed for policymakers, developers, and researchers involved in IoT deployment and management. It addresses various aspects crucial for implementing robust anomaly detection systems. This draft new Recommendation aims to establish a standardized framework that promotes the deployment and management of intelligent anomaly detection systems in IoT environments. By offering detailed

guidelines and best practices, it seeks to bolster the security, reliability, and efficiency of IoT applications and systems, thereby fostering greater trust and adoption of IoT technologies across various sectors.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup.SRS-SR : Supplement to ITU-T Y.4120 - Security threats and requirements of IoT applications for smart retail stores

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19642

ABSTRACT: Retail stores are one of the important application fields of the IoT. The usage of IoT enables “smart retail stores”. More and more smart retail stores rely on various IoT devices and are closely integrated with electronic shelf labels, product management system, etc., resulting in complex network structures and diverse application in smart retail store. This Supplement focuses on the security threats and requirements of IoT based smart retail stores. The purpose is to improve the security protection capability of the smart retail store systems during operation and maintenance.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sup-Imp-CSIADE Supplement to ITU-T Y.4811 - Implementation of converged service for identification and authentication for IoT devices in decentralized environment

🔗 URL: <https://www.itu.int/rec/T-REC-I.1410-201412-I/en>

ABSTRACT: Recommendation ITU-T Y.4811 specifies a converged service for identification and authentication for IoT devices in decentralized environment (CSIADE), and provides its common characteristics, general requirements, functional architecture, main capabilities and procedures. CSIADE can facilitate IoT devices and IoT services to identify and authenticate each other in IoT decentralized environments when they use same or different types of decentralized IoT identification and authentication solutions. This draft Supplement provides a set of implementation guidelines to perform the CSIADE defined in Recommendation ITU-T Y.4811, including that of CSIADE as an independent system and as subsystem embedded in IoT devices and services, to improve compatibility when using self-resolving identities for IoT devices and services, to use self-controllable storage to manage identities of IoT devices and services, to support online and offline endorsement for the identity of IoT devices and services, and to support multiple solutions of identification and authentication in CSIADE. This draft Supplement is to promote the implementation and deployment of CSIADE.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

AIOTI Application-Centric Security, Privacy & Trust in IoT

🔗 URL: https://aioti.eu/wp-content/uploads/2019/06/Webinar_Nr1_ApplicationCentric_SecurityPrivacyTrustInIoT_ArthursLegal_v2019.1_vPresented.pdf

ABSTRACT: This presentation focuses on “Security, Privacy & Trust in IoT Application-Centric Series” in: a) Personal Wearables (H2x); b) Moving Sensors (M2x); c) Long Term Fixed IoT Applications (M2x).

📄 DOCUMENT TYPE: Presentation

📅 PUBLICATION DATE: 2019-06

bloTope project D3.3 V1.0 Context-Sensitive Security, Privacy Management, Adaptation Framework

 **URL:** <https://st11.ning.com/topology/rest/1.0/file/get/1065330?profile=original>

ABSTRACT: This document is part of the scope of building a Secure, Open & Standardised Systems of Systems Platform for IoT. It provides the technological foundation of the bloTope Systems of Systems (SoS) Platform for information source publication and consumption in the IoT, based on the O-MI and O-DF standards. It includes new mechanisms to better manage 'Identities' and 'Context-sensitive Security and Privacy' (SaaS) of Connected Smart Objects and People to cope with the dynamic nature of the IoT.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2017-03

CENELEC EN 17529:2022 Cybersecurity and Data Protection

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::FSP_PROJECT,FSP_ORG_ID:63633,2307986&cs=11F702120AA40D5CC2DD42848140B1806

ABSTRACT: This document provides requirements for manufacturers and/or service providers to implement Data protection and Privacy by Design and by Default (DPbDD) early in their development of their products and services, i.e. before (or independently of) any specific application integration, to make sure that they are as privacy ready as possible. The document will be applicable to all business sectors, including the security industry.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-05

(Updated) CENELEC EN 17640:2022 Fixed-time cybersecurity evaluation methodology for ICT products

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::FSP_PROJECT,FSP_ORG_ID:70971,2307986&cs=1DA2D43E88931425C57B373E6C1A14866

ABSTRACT: This document describes a cybersecurity evaluation methodology that can be implemented using pre-defined time and workload resources, for ICT products. It is intended to be applicable for all three assurance levels defined in the CSA (i.e. basic, substantial and high). The methodology comprises different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the mentioned three assurance levels. Where appropriate, it can be applied both to third-party evaluation and self-assessment.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-10

(Updated) CEN EN 17927:2023 Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::FSP_PROJECT,FSP_LANG_ID:74909,25&cs=157BB6AD851BD6F80A208E00FBBD6B8DD

ABSTRACT: This document describes a cybersecurity evaluation methodology, named SESIP, for components of connected ICT products. Security claims in SESIP are made based on the security services offered by those components. Components can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of components which apply to the

foundational components of devices that are not application specific. The methodology describes the re-use of evaluation results.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-11

ECSSO System security and certification considerations

📄 URL: <https://www.youtube.com/watch?v=mXiytFIOXeI>

ABSTRACT: Explore system's cyber security challenges, particularities and considerations inside the EU regulatory context, learn about the importance of defining a cyber security risk perimeter and gain insights on important security notions related to governance, maturity and diversity of processes, as well as people's competencies for design, build and commission. Last but not least, find out how to secure and operate a mission- specific system, and gain prospects on the existing relevant certification possibilities.

📄 DOCUMENT TYPE: Presentation

📅 PUBLICATION DATE: 2022-01

ENISA Baseline Security Recommendations for IoT

📄 URL: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

ABSTRACT: The study which is titled 'Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures', aims to set the scene for IoT security in Europe. It serves as a reference point in this field and as a foundation for relevant forthcoming initiatives and developments.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2017-11

ENISA IoT Security Standards Gap Analysis

📄 URL: <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>

ABSTRACT: This study analyses the gaps and provides guidelines for, in particular, the development or repositioning of standards, facilitating the adoption of standards and governance of EU standardisation in the area of NIS.

ENISA brings in this relationship its technical and organisational know-how in NIS which can be further leveraged into standards in terms of extending or assessing them to render them more appropriate to stakeholders and more compliant with the prevailing regulatory framework.

Special attention is given to the EU needs related to emerging cybersecurity certification schemes which will operate under the European cybersecurity certification framework. The framework is currently not adopted but is expected to be finished at the end of this year. Standards or other widely adopted technical specifications containing requirements form the basis for any certification activity. European standards for security evaluation models, methods, techniques and tools adopted to the IoT world are urgently needed to complement existing initiatives, good practices and industry guidelines on IoT security.

📄 DOCUMENT TYPE: Gap analysis

📅 PUBLICATION DATE: 2019-01

(Updated) ETSI TS 103 942 Methods for Testing and Specification (MTS); Security Testing; IoT Security Functional Modules

 **URL:** https://www.etsi.org/deliver/etsi_ts/103900_103999/103942/01.01.01_60/ts_103942v010101p.pdf

ABSTRACT: Assemble security related functional modules within an IoT architecture, that support Security by Design and trustworthiness in order to retrieve relevant security testing methods and specific detailed test purposes using TDL-TO for generic IoT architectures applicable in multiple industrial domains.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-11

(Updated) ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

 **URL:** http://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

ABSTRACT: The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. Moreover, the present document addresses security considerations specific to constrained devices. The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table B.1 provides a schema for the reader to give information about the implementation of the provisions. Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document. The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-09

ETSI TR 103 533 Security; Standards Landscape and best practices

 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr_103533v010101p.pdf

ABSTRACT: The document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT.

The document complements the overview of the Standards Landscape and best practice for privacy to be found in ETSI TR 103 591.

 **DOCUMENT TYPE:** Landscape

 **PUBLICATION DATE:** 2019-08

ETSI TR 103 591 Privacy study report; Standards Landscape and best practices

 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf

ABSTRACT: The purpose of the document is to demonstrate that in view of the increasingly growing number of connected objects anticipated in the near future, effective protection of privacy and data protection would require that the relevant decisions are made upfront, at the design stage of the IoT systems.

 **DOCUMENT TYPE:** Landscape

 **PUBLICATION DATE:** 2019-10

ETSI TS 103 646 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for foundational Security IoT-Profile

 **URL:** https://www.etsi.org/deliver/etsi_ts/103600_103699/103646/01.01.01_60/ts_103646v010101p.pdf

ABSTRACT: The present document provides a test specification based on selected security requirements as known from IEC 6244-4-2. The chosen requirements have been collected by defining a dedicated IoT profile. The resulting IoT profile represents a generic minimum security level for IoT devices. Advanced requirements for higher security demands have been excluded.

The present document serves as reference for a test campaign addressing the foundational security requirements of the IoT-Profile. The standardized notation TDL-TO has been applied for the definition of test purposes as it supports a unified presentation and semantics.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-01

ETSI TS 103 701 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

 **URL:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

ABSTRACT: The present document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 / ETSI EN 303 645, addressing the mandatory and recommended provisions as well as conditions and complements ETSI TS 103 645 / ETSI EN 303 645 by defining test cases and assessment criteria for each provision.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-08

(NEW) IEEE 3219-2023 IEEE Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT)

 **URL:** <https://standards.ieee.org/ieee/3219/11163/>

ABSTRACT: The surging needs for the Internet of Things (IoT) are dramatically shifting the network structure and challenging the traditional perimeter security paradigm. To establish secure and trustworthy interoperability among billions of heterogeneous interconnected devices, there is a need for standards defining a common framework. In this standard, a blockchain-based Zero-Trust access control framework is defined. The framework provides a typical implementation model and deployment variations, addressing general security and trust in IoT applications with the inspiration of the emerging Zero-Trust paradigm and blockchain technology. The leverage of blockchain and Zero-Trust discussed could provide reliable interactions among people, things, and applications in the presence of failures and attacks, and improve an IoT system's overall information technology security posture.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 26/04/2024

(NEW) IEEE/UL 2933-2024 IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security

 **URL:** <https://standards.ieee.org/ieee/2933/7592/>

ABSTRACT: A framework with TIPPSS principles (trust, identity, privacy, protection, safety, and security) for Clinical Internet of Things (IoT) data and device interoperability is established in this standard. This

includes wearable clinical IoT and interoperability with healthcare systems including electronic health records (EHR), electronic medical records (EMR), other Clinical IoT devices, in-hospital devices, and future devices and connected healthcare systems.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 30/09/2024

(NEW) IEEE P2418.3 Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture

🔗 URL: <https://standards.ieee.org/ieee/2418.3/7714/>

ABSTRACT: This standard provides a common framework for distributed ledger technology (DLT) usage, implementation, and interaction in agriculture. The framework maps DLT terms including transactions, smart contracts, tokens, assets and networks to terms in agriculture, and addresses technical aspects including scalability, security and privacy challenges with regard to DLT in agriculture. Concerns from different stakeholders and requirements in horizontal and vertical categories of agriculture are included in the framework.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-07

IEC IoT 2020: Smart and secure IoT platform

🔗 URL: <https://www.iec.ch/basecamp/iot-2020-smart-and-secure-iot-platform>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Whitepaper

📅 PUBLICATION DATE: 2016-10

IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

🔗 URL: <https://webstore.iec.ch/publication/30727>

ABSTRACT: IEC 62443-3-2:2020 establishes requirements for:

- 📄 defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- 📄 partitioning the SUC into zones and conduits;
- 📄 assessing risk for each zone and conduit;
- 📄 establishing the target security level (SL-T) for each zone and conduit; and

📄 documenting the security requirements.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06

(Updated) IETF draft-ietf-rats-ar4si Attestation Results for Secure Interactions

📄 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/>

ABSTRACT: This document defines reusable Attestation Result information elements. When these elements are offered to Relying Parties as Evidence, different aspects of Attester trustworthiness can be evaluated.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-03

(Updated) IETF draft-ietf-rats-daa Direct Anonymous Attestation for the Remote Attestation Procedures Architecture

📄 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-daa/>

ABSTRACT: This document maps the concept of Direct Anonymous Attestation (DAA) to the Remote Attestation Procedures (RATS) Architecture. The role DAA Issuer is introduced and its interactions with existing RATS roles is specified.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-03

(Updated) IETF draft-ietf-rats-eat The Entity Attestation Token (EAT)

📄 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-eat/>

ABSTRACT: This document extends CBOR Web Token (CWT) and JSON Web Token (JWT).

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-08

(Updated) IETF draft-ietf-rats-network-device-subscription Attestation Event Stream Subscription

📄 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/>

ABSTRACT: This memo provides the methods and means to define additional Event Streams for other Conceptual Message as illustrated in the RATS Architecture, e.g. Attestation Results, Endorsements, or Event Logs.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-07

(Updated) IETF draft-ietf-rats-reference-interaction-models Reference Interaction Models for Remote Attestation Procedures

📄 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/>

ABSTRACT: This document describes interaction models for remote attestation procedures (RATS). Three conveying mechanisms -- Challenge/Response, Uni-Directional, and Streaming Remote Attestation -- are illustrated and defined.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-07

(Updated) IETF draft-ietf-teep-otrp-over-http HTTP Transport for Trusted Execution Environment Provisioning: Agent Initiated Communication

🔗 URL: <https://datatracker.ietf.org/doc/draft-ietf-teep-otrp-over-http/>

ABSTRACT: This document specifies the HTTP transport for TEEP communication where a Trusted Application Manager (TAM) service is used to manage code and data in TEEs on devices that can initiate communication to the TAM.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2023-03

(Updated) IETF draft-ietf-teep-protocol Trusted Execution Environment Provisioning (TEEP) Protocol

🔗 URL: <https://datatracker.ietf.org/doc/draft-ietf-teep-protocol/>

ABSTRACT: This document specifies a protocol that installs, updates, and deletes Trusted Components in a device with a Trusted Execution Environment (TEE). This specification defines an interoperable protocol for managing the lifecycle of Trusted Components.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-05

(Updated) IETF draft-ietf-rats-uccs A CBOR Tag for Unprotected CWT Claims Sets

🔗 URL: <https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/>

ABSTRACT: This specification defines a CBOR tag for such unprotected CWT Claims Sets (UCCS) and discusses conditions for its proper use.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-07

(NEW) IETF draft-li-iotops-intelligent-security Intelligent Protection Optimization System for IOT

🔗 URL: <https://datatracker.ietf.org/doc/draft-li-iotops-intelligent-security/>

ABSTRACT: Communication technology is becoming more and more developed, the Internet of Things coverage is becoming more and more comprehensive, and a large number of data and devices are joining, which also makes more data security and privacy issues appear. Therefore, this draft proposes a scheme to build an information-centered network. By analyzing common network attack methods, an intelligent protection optimization system is established from three aspects: naming and parsing, data exchange, and data caching, so as to achieve better content privacy protection without adding additional costs.

DOCUMENT TYPE: Guideline

PUBLICATION DATE: 2024-02

(NEW) IETF draft-ietf-iotops-security-summary A summary of security-enabling technologies for IoT devices

URL: <https://datatracker.ietf.org/doc/draft-ietf-iotops-security-summary/>

ABSTRACT: The IETF has developed security technologies that help to secure the Internet of Things even over constrained networks and when targetting constrained nodes. These technologies can be used independently or can be composed into larger systems to mitigate a variety of threats. This documents illustrates an overview over these technologies and highlights their relationships. Ultimately, a threat model is presented as a basis to derive requirements that interconnect existing and emerging solution technologies.

DOCUMENT TYPE: Guideline

PUBLICATION DATE: 2023-10

(NEW) IETF draft-irtf-t2trg-taxonomy-manufacturer-anchors A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

URL: <https://datatracker.ietf.org/doc/draft-irtf-t2trg-taxonomy-manufacturer-anchors/>

ABSTRACT: This document provides a taxonomy of methods used by manufacturers of silicon and devices to secure private keys and public trust anchors. This deals with two related activities: how trust anchors and private keys are installed into devices during manufacturing, and how the related manufacturer held private keys are secured against disclosure.

DOCUMENT TYPE: Guideline

PUBLICATION DATE: 2024-01

(NEW) IETF draft-irtf-t2trg-security-setup-iot-devices Terminology and processes for initial security setup of IoT devices

URL: <https://datatracker.ietf.org/doc/draft-irtf-t2trg-security-setup-iot-devices/>

ABSTRACT: This document provides an overview of terms that are commonly used when discussing the initial security setup of Internet of Things (IoT) devices. This document also presents a brief but illustrative survey of protocols and standards available for initial security setup of IoT devices. For each protocol, we identify the terminology used, the entities involved, the initial assumptions, the processes necessary for completion, and the knowledge imparted to the IoT devices after the setup is complete.

DOCUMENT TYPE: Guideline

PUBLICATION DATE: 2024-03

(NEW) IETF draft-ietf-scitt-software-use-cases Detailed Software Supply Chain Uses Cases for SCITT

URL: <https://datatracker.ietf.org/doc/draft-ietf-scitt-software-use-cases/>

ABSTRACT: This document includes a collection of representative Software Supply Chain Use Cases. These use cases aim to identify software supply chain problems that the industry faces today and act as a guideline for developing a comprehensive security architecture and solutions for these scenarios.

DOCUMENT TYPE: Guideline

(NEW) IETF draft-ietf-scitt-architecture An Architecture for Trustworthy and Transparent Digital Supply Chains

🔗 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/>

ABSTRACT: This document defines a generic, interoperable and scalable architecture to enable transparency across any supply chain with minimum adoption barriers. It provides flexibility, enabling interoperability across different implementations of Transparency Services with various auditing and compliance requirements. Issuers can register their Signed Statements on any Transparency Service, with the guarantee that all Auditors and Verifiers will be able to verify them.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2024-03

(NEW) IETF draft-ietf-scitt-scrapi SCITT Reference APIs

🔗 **URL:** <https://datatracker.ietf.org/doc/draft-ietf-scitt-scrapi/>

ABSTRACT: This document describes a REST API that supports the normative requirements of the SCITT Architecture. Optional key discovery and query interfaces are provided to support interoperability issues with Decentralized Identifiers, X509 Certificates and Artifact Repositories.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2024-03

(Updated) IETF RFC 9528 Ephemeral Diffie-Hellman Over COSE (EDHOC)

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc9528/>

ABSTRACT: This document specifies Ephemeral Diffie-Hellman Over COSE (EDHOC), a very compact and lightweight authenticated Diffie-Hellman key exchange with ephemeral keys.

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2024-03

(Updated) IETF RFC 9529 Traces of EDHOC

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc9529/>

ABSTRACT: This document contains some example traces of Ephemeral Diffie-Hellman Over COSE (EDHOC).

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2024-03

(Updated) IETF RFC 9334 Remote Attestation Procedures Architecture

🔗 **URL:** <https://datatracker.ietf.org/doc/rfc9334/>

ABSTRACT: This document provides an architectural overview of the entities involved that make such tests possible through the process of generating, conveying, and evaluating evidentiary claims.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2023-12

(Updated) IETF RFC 9397 Trusted Execution Environment Provisioning (TEEP) Architecture

URL: <https://datatracker.ietf.org/doc/rfc9397/>

ABSTRACT: This architecture document motivates the design and standardization of a protocol for managing the lifecycle of trusted applications running inside such a TEE.

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2023-07

ietf RFC 8152 CBOR Object Signing and Encryption (COSE)

URL: <https://datatracker.ietf.org/doc/rfc8152/>

ABSTRACT: This specification describes how to create and process signatures, message authentication codes, and encryption using CBOR for serialization. This specification additionally describes how to represent cryptographic keys using CBOR.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2017-01

ietf RFC 8387 Practical Considerations and Implementation Experiences in Securing Smart Object Networks

URL: <https://datatracker.ietf.org/doc/rfc8387/>

ABSTRACT: This memo describes challenges associated with securing resource -constrained smart object devices

DOCUMENT TYPE: Technical_Report

PUBLICATION DATE: 2018-05

ietf RFC 8613 Object Security for Constrained RESTful Environments (OSCORE)

URL: <https://datatracker.ietf.org/doc/rfc8613/>

ABSTRACT: This document defines Object Security for Constrained RESTful Environments (OSCORE), a method for application-layer protection of the Constrained Application Protocol (CoAP), using CBOR Object Signing and Encryption (COSE). OSCORE provides end-to-end protection between endpoints communicating using CoAP or CoAP-mappable HTTP. OSCORE is designed for constrained nodes and networks supporting a range of proxy operations, including translation between different transport protocols.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2019-07

ietf RFC 8812 CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web

Authentication (WebAuthn) Algorithms

 **URL:** <https://datatracker.ietf.org/doc/rfc8812/>

ABSTRACT: This specification registers the following algorithms (which are used by WebAuthn and CTAP implementations) in the IANA “COSE Algorithms” registry: RSASSA-PKCS1-v1_5 using SHA-256, SHA-384, SHA-512, and SHA-1; and Elliptic Curve Digital Signature Algorithm (ECDSA) using the secp256k1 curve and SHA-256. It registers the secp256k1 elliptic curve in the IANA “COSE Elliptic Curves” registry. Also, for use with JSON Object Signing and Encryption (JOSE), it registers the algorithm ECDSA using the secp256k1 curve and SHA-256 in the IANA “JSON Web Signature and Encryption Algorithms” registry and the Secp256k1 elliptic curve in the IANA “JSON Web Key Elliptic Curve” registry.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-08

IETF RFC 8995 Bootstrapping Remote Secure Key Infrastructure (BRSKI)

 **URL:** <https://datatracker.ietf.org/doc/rfc8995/>

ABSTRACT: This document specifies automated bootstrapping of an Autonomic Control Plane.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-05

IETF RFC7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation

 **URL:** <https://datatracker.ietf.org/doc/rfc7815/>

ABSTRACT: This document describes a minimal initiator version of the Internet Key Exchange version 2 (IKEv2) protocol for constrained nodes.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2016-03

IRTF RFC 8576 Internet of Things (IoT) Security: State of the Art and Challenges

 **URL:** <https://datatracker.ietf.org/doc/rfc8576/>

ABSTRACT: This document first discusses the various stages in the lifecycle of a thing. Next, the security threats to a thing and the challenges that one might face to protect against these threats are discussed. Lastly, the next steps needed to facilitate the deployment of secure IoT systems are presented.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2019-04

(Updated) ISO 31700-1:2023 Consumer protection — Privacy by design for consumer goods and services - Part 1: High-level requirements

 **URL:** <https://www.iso.org/standard/84977.html>

ABSTRACT: This document establishes high-level requirements for privacy by design to protect privacy throughout the lifecycle of a consumer product, including domestic data processing by the consumer.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-01

(NEW) ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

🔗 URL: <https://www.iso.org/standard/64140.html>

ABSTRACT: The target audience for this document is primarily evaluators applying the ISO/IEC 15408 series and certifiers confirming evaluator actions. Evaluation sponsors, developers, protection profile (PP), PP-Module, PP-Configuration, and security target (ST) authors, and other parties interested in IT security, can be a secondary audience. This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-08

(NEW) ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model

🔗 URL: <https://www.iso.org/standard/72891.html>

ABSTRACT: The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software. This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the ISO/IEC 15408 series; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

This document introduces:

- 📄 the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;
- 📄 a description of the organization of security components throughout the model;
- 📄 the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;
- 📄 general information about the evaluation methods given in ISO/IEC 18045;
- 📄 guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;
- 📄 general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;
- 📄 information in regard to the scope of evaluation schemes.

📄 DOCUMENT TYPE: Standard_Specification

(NEW) ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

🔗 **URL:** <https://www.iso.org/standard/72892.html>

ABSTRACT: Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP, PP-Module, functional package or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies. This document defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2022-08

(NEW) ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

🔗 **URL:** <https://www.iso.org/standard/72906.html>

ABSTRACT: Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PP-Configuration, or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs. This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2022-08

(NEW) ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities

🔗 **URL:** <https://www.iso.org/standard/72913.html>

ABSTRACT: This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.

This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and

evaluation activities in their particular area of interest.

In particular, this document describes a framework that can be used for deriving evaluation activities from work units of ISO/IEC 18045 and grouping them into evaluation methods (EMs). Evaluation activities or evaluation methods can be included in protection profiles (PPs) and any documents supporting them. Where a PP, PP-Configuration, PP-Module, package, or Security Target (ST) identifies that specific evaluation methods/evaluation activities are to be used, then the evaluators are required by ISO/IEC 18045 to follow and report the relevant evaluation methods/evaluation activities when assigning evaluator verdicts. As noted in ISO/IEC 15408-1, in some cases an evaluation authority can decide not to approve the use of particular evaluation methods/evaluation activities: in such a case, the evaluation authority can decide not to carry out evaluations following an ST that requires those evaluation methods/evaluation activities.

This document also allows for evaluation activities to be defined for extended SARs, in which case derivation of the evaluation activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/IEC 15408-3 for SARs (such as when defining rationales for evaluation activities), then, in the case of an extended SAR, the reference applies instead to the equivalent action elements and work units defined for that extended SAR.

For clarity, this document specifies how to define evaluation methods and evaluation activities but does not itself specify instances of evaluation methods or evaluation activities.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-08

(NEW) ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

🔗 URL: <https://www.iso.org/standard/72917.html>

ABSTRACT: This document provides pre-defined packages of security requirements. Such security requirements can be useful for stakeholders as they strive for conformity between evaluations. Packages of security requirements can also help reduce the effort in developing Protection Profiles (PPs) and Security Targets (STs).

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-08

(NEW) ISO/IEC TR 40141 Internet of Things (IoT) – Reference architecture guidance

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:38:16526658145347:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,126453

ABSTRACT: This document provides:

- 📄 Guidance on using the ISO/IEC 30141 - IoT Reference Architecture Edition 2;
- 📄 Background on the changing context IoT systems are being developed in, an overview of the different sections of the IoT Reference Architecture;
- 📄 Some rationales on why to use the IoT Reference Architecture and information about how to use it to architect an IoT system; and
- 📄 An explanation of construction patterns.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(Updated) ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 1: Introduction and general model

 **URL:** <https://www.iso.org/standard/72891.html>

ABSTRACT: This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the ISO/IEC 15408 series; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

This document introduces:

-  the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;
-  a description of the organization of security components throughout the model;
-  the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;
-  general information about the evaluation methods given in ISO/IEC 18045;
-  guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;
-  general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;
-  information in regard to the scope of evaluation schemes.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-08

(Updated) ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

 **URL:** <https://www.iso.org/standard/72889.html>

ABSTRACT: This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2022-08

(Updated) ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships - Part 3: Guidelines for hardware, software, and services supply chain security

 **URL:** <https://www.iso.org/standard/82890.html>

ABSTRACT: This document provides guidance for product and service acquirers, as well as suppliers of hardware, software and services, regarding:

- a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered hardware, software, and services supply chains;
- b) responding to risks stemming from this physically dispersed and multi-layered hardware, software,

and services supply chain that can have an information security impact on the organizations using these products and services;

- c) integrating information security processes and practices into the system and software life cycle processes, as described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, while supporting information security controls, as described in ISO/IEC 27002.

This document does not include business continuity management/resiliency issues involved with the hardware, software, and services supply chain. ISO/IEC 27031 addresses information and communication technology readiness for business continuity.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2023-06

(NEW) ISO/IEC 27400 – AWI TS 5689 Cybersecurity - Security frameworks based on the conceptual model of cyber-physical systems

🔗 URL: <https://www.iso.org/standard/87375.html>

ABSTRACT: This document provides the followings:

CPS conceptual model and its specific characteristics

- 📄 a conceptual model of cyber-physical systems (CPS) and its general features;
- 📄 specific characteristics of CPS compared to other related concepts;
- 📄 Concerns and security frameworks
- 📄 security concerns as the basis for the discussion of security risks and security controls for the CPS based on the conceptual model;
- 📄 several security frameworks to address those security concerns;
- 📄 Practical use cases for CPS
- 📄 use cases based on the respective security frameworks for CPS;
- 📄 provision of visibility of use cases into the specific use of the security frameworks, etc.

This document does not provide specific security controls needed in cyber-physical systems.

This document applies to all sectors where CPS are or will be present, which encapsulate a diverse set of sectors ranging from industrial (e.g., manufacturing) to public (e.g., smart cities). CPS stakeholders such as users, developers, and operators can have a common understanding of CPS (e.g., concepts, risks, security framework) through this document.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: Under development

ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines

🔗 URL: <https://www.iso.org/standard/44373.html>

ABSTRACT: This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-06

(Updated) ISO/IEC 27404 Information technology — Security techniques — Universal cybersecurity labelling framework for consumer IoT

 **URL:** <https://www.iso27001security.com/html/27404.html>

ABSTRACT: This document defines a Universal Cybersecurity Labelling Framework for the development and implementation of cybersecurity labelling programmes for consumer IoT products and includes guidance on the following topics:

-  Risks and threats associated with consumer IoT products;
-  Stakeholders, roles and responsibilities; • Relevant standards and guidance documents;
-  Conformity assessment options;
-  Labelling issuance and maintenance requirements; and
-  Mutual recognition considerations.

The scope of this document is limited to consumer IoT products, such as

-  IoT gateways, base stations and hubs to which multiple devices connect;
-  smart cameras, televisions, and speakers;wearable health trackers;
-  connected smoke detectors, door locks and window sensors;
-  connected home automation and alarm systems, especially their gateways and hubs;
-  connected appliances, such as washing machines and fridges; smart home assistants; and
-  connected children's toys and baby monitors.

The Universal Cybersecurity Labelling Framework addresses the expected and intended use of IoT devices and systems by consumers, that is, the general public and non-technical users. These devices and systems are used with the understanding that the label and criteria are designed for consumer use and consumer security concerns.

Safety is not addressed in this Universal Cybersecurity Labelling Framework even though it is an important aspect to consider.

Consumer IoT devices used in an enterprise context may not be classified as consumer IoT devices due to potentially more serious implications if compromised, which then entails more stringent cybersecurity provisions. Furthermore, in threat models of consumer IoT, there is no IT/system administrator as a pre-condition.

Products that are not intended for consumer use are excluded from this standard. Examples of excluded devices are those that are primarily intended for manufacturing, healthcare and other industrial purposes.

The Universal Cybersecurity Labelling Framework is based on requirements from international standards, with objectives to facilitate mutual recognition of labelling schemes for consumer IoT (regardless if they are binary or multi-level), avoid fragmentation of standards, eradicate duplicated testing (across countries), reduce the cost of compliance and facilitate market access for developers.

This document is applicable to consumers, developers, issuing bodies of cybersecurity labels and independent test laboratories.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(Updated) ISO/IEC 30149 ED1 Internet of Things (IoT) - Trustworthiness Principles

 **URL:** <https://webstore.iec.ch/publication/67281>

ABSTRACT: ISO/IEC TS 30149:2024 provides principles for IoT trustworthiness based on ISO/IEC 30141 - IoT Reference Architecture.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-05

(Updated) ISO/IEC 27402 Cybersecurity — IoT security and privacy — Device baseline requirements

 **URL:** <https://www.iso.org/standard/80136.html>

ABSTRACT: his document provides baseline ICT requirements for IoT devices to support security and privacy controls.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-11

(Updated) ISO/IEC 27403 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

 **URL:** <https://www.iso.org/standard/78702.html>

ABSTRACT: This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT)-domotics systems.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-06

(Updated) ISO/IEC 24392 Cybersecurity — Security reference model for industrial Internet platform (SRM- IIP)

 **URL:** <https://www.iso.org/standard/78703.html>

ABSTRACT: This document presents specific characteristics of industrial internet platforms (IIPs), including related security threats, context-specific security control objectives and security controls.

This document covers specific security concerns in the industrial context and thus complements generic security standards and reference models. In particular, this document includes secure data collection and transmission among industrial devices, data security of industrial cloud platforms, and secure collaborations with various industry stakeholders.

The users of this document are organizations who develop, operate, or use any components of IIPs, including third parties who provide services to the abovementioned stakeholders.

This document provides recommendations for users on how to protect IIPs against IIP-specific threats.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-07

(Updated) ISO/IEC 27071 Cybersecurity — Security recommendations for establishing trusted connections between devices and services

 **URL:** <https://www.iso.org/standard/56572.html>

ABSTRACT: This document provides a framework and recommendations for establishing trusted connections between devices and services based on hardware security modules. It includes recommendations for components such as: hardware security module, roots of trust, identity, authentication and key establishment, remote attestation, data integrity and authenticity.

This document is applicable to scenarios that establish trusted connections between devices and services based on hardware security modules.

This document does not address privacy concerns.

 **DOCUMENT TYPE:** Standard_Specification

ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications

🔗 **URL:** <https://www.iso.org/standard/64140.html>

ABSTRACT: ISO/IEC TS 19249:2017 provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively. ISO/IEC TS 19249:2017 gives guidelines for the development of secure products, systems and applications including a more effective assessment with respect to the security properties they are supposed to implement. ISO/IEC TS 19249:2017 does not establish any requirements for the evaluation or the assessment process or implementation.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2017-10

(NEW) ITU-T YSTR.IoT-IMS Identification management service of IoT device

🔗 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18473

ABSTRACT: To support complex IoT scenarios, identification management service of the IoT device is needed. The proposed identification management service of the IoT device can help IoT platform service providers to manage the access control of the IoT device for platform services. The main purpose of this proposed draft technical report is to help IoT platform service providers write identification data to IoT devices of different vendors, and to help IoT platforms identify identification data from a variety of IoT devices. The requirements related to the modification and deletion of identification data in IoT devices are also included in the proposed draft technical report. The significance of this proposed draft technical report is to improve the operation efficiency of the IoT platform on the identification data of IoT devices, so as to reduce the time and money spent on the integration of IoT devices and platforms.

📄 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** Under development

(Updated) NGI-0 Discovery NEUROPIL

🔗 **URL:** <https://gitlab.com/pi-lar/neuropil>

ABSTRACT: Neuropil is an open-source de-centralized messaging layer that focuses on security and privacy by design. Persons, machines, and applications first have to identify their respective partners and/or content before real information can be sent. The discovery is handled internally and is based on so called “intent messages” that are secured by cryptographic primitives. This project aims to create distributed search engine capabilities based on neuropil, that enable the discovery and sharing of information with significantly higher levels of trust and privacy and with more control over the search content for data owners than today's standard.

📄 **DOCUMENT TYPE:** EU & National funded Open Source projects

📅 **PUBLICATION DATE:** Under development

onM2M TR-0012-V2.0.0 End-to-End Security and Group Authentication

🔗 **URL:** https://onem2m.org/images/files/deliverables/Release2/TR-0012-End-to-End-Security_and

ABSTRACT: The present document provides options and analyses for the security features and mechanisms providing end-to-end security and group authentication for oneM2M. The scope of this technical report includes use cases, threat analyses, high level architecture, generic requirements, available options, evaluation of options, and detailed procedures for executing end-to-end security and group authentication.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2016-8

oneM2M TR-0016-V-2.0.0 Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies

📄 URL: https://onem2m.org/images/files/deliverables/Release2/TR-0016-Authorization_Architecture_and_Access_Control_Policy-V2_0_0.pdf

ABSTRACT: The present document provides technical solutions for oneM2M authorization architecture, authorization procedures and access control policies. The present document also gives evaluations of these proposed technical solutions.

ETSI TS 118 103 [i.2] only defines a high level authorization architecture that describes its major components and general authorization procedure. The objective of the present document is to provide candidate security solutions related to authorization architecture, authorization procedures and access control policies. The present document provides security solutions in the following three aspects: a) Detailed design of authorization architecture: This part investigates the interfaces among authorization components (e.g. procedures and parameters), how these components could be distributed in different oneM2M entities (i.e. different CSEs), and how to implement Role Based Access Control (RBAC) and token based access control; b) Supporting user specified access control policies: This part investigates how the oneM2M authorization system could be an extensible system that can support user-defined access control mechanisms and/or access control policy languages; c) Investigating existing access control policy languages: This part investigates if some standardized access control policy languages could become oneM2M recommended access control policy description languages.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2016-08

oneM2M TR-0062-V-0.3.0 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)

📄 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33146>

ABSTRACT: The document is describing state of the art privacy related regulations and their features followed by gap analysis to find out what features are supported and not supported by the current oneM2M system. Based on the result of the technical report, it will identify possible enhancement features to support data protection regulations which the next oneM2M release(s) could support.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-11

oneM2M TR-0063-V-0.0.1 Effective IoT Communication to Protect 3GPP Networks

📄 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31370>

ABSTRACT: This work item describes how a oneM2M service layer hosted on a 3GPP Cellular IoT device can implement the requirements defined in GSMA TS.34 to ensure that a device does not operate in a manner that can impair the 3GPP Cellular network.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-11

(New) oneM2M TS-0003-V4.8.1 Security Solutions

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36602>

ABSTRACT: The TS defines security solutions for M2M systems.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2024-02

oneM2M WI-0095 System enhancements to support Data Protection Regulations

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30968>

ABSTRACT: Proposes a work item to study oneM2M system enhancement to support data protection regulations such as General Data Protection Regulation from EU.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-10

oneM2M-TR-0041-V-0.4.0 oneM2M Decentralized Authentication

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26293>

ABSTRACT: Technical Report of oneM2M Decentralized Authentication.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-03

oneM2M-TR-0050-V-0.13.0 Attribute Based Access Control Policy

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32114>

ABSTRACT: This work item develops attribute based access control policy scheme and the corresponding access control policy management mechanism in oneM2M System.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-05

Manufacturing

IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

 **URL:** <https://webstore.iec.ch/publication/22810>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2015-06

IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

 **URL:** <https://webstore.iec.ch/publication/30727>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-06

IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

 **URL:** <https://webstore.iec.ch/publication/7033>

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2013-08-07

IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

 **URL:** <https://webstore.iec.ch/publication/34421>

Abstract: EC 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2018-01-15

IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment

🔗 URL: <https://webstore.iec.ch/publication/22811>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2015-06-30

IEC TR 62443-3-1:2009 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems

🔗 URL: <https://webstore.iec.ch/publication/7031>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2009-07-30

IEC TR 62541-2:2020 OPC Unified Architecture - Part 2: Security Model

🔗 URL: <https://webstore.iec.ch/publication/61110>

ABSTRACT: IEC TR 62541-2:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-2:2020

describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and Profiles that are specified normatively in other parts of the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2020-11-17

Mobility

(Updated) ETSI TS 102 731 V2.0.0 ITS; Security; Security Services and Architecture

📄 URL: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/02.00.00_60/ts_102731v020000p.pdf

ABSTRACT: The document will specify mechanisms and protocols for secure and privacy-preserving communication in vehicular environments, including vehicle-to-vehicle and vehicle-to-infrastructure communication. It will provide credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. It will incorporate mechanisms such as addressing schemes building on pseudonymization concepts, the protocols for address update, and for exchanging, updating, and invalidating credentials to counterfeit attacks on security and reliability of communication. Further methods to prevent malicious tracking of identity and location will be provided.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-11

(Updated) ETSI TS 102 940 V2.1.1 ITS; Security; ITS communications security architecture and security management

📄 URL: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

ABSTRACT: The present document specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731, it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in EN 302 665. The present document also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.

It has been published for both Release 1 (V1.3.1) and Release 2 (V2.1.1) of the ETSI C-ITS standards

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-07

IEEE 1609.2 IEEE 1609.2 standard for Security, Network Services and Multi-Channel Operation

📄 URL: <https://ieeexplore.ieee.org/document/7426684>

ABSTRACT: Communications/Networking - DSRC is a U.S. Department of Transportation (DOT) project

based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-03

IEEE 1609.3 IEEE 1609.3 standard for Security, Network Services and Multi-Channel Operation

🔗 URL: <https://ieeexplore.ieee.org/document/7458115>

ABSTRACT: Communications/Networking - DSRC is a U.S. Department of Transportation (DOT) project based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-04

IEEE 1609.4 IEEE 1609.4 standard for Security, Network Services and Multi-Channel Operation

🔗 URL: <https://ieeexplore.ieee.org/document/7435228>

ABSTRACT: Communications/Networking - DSRC is a U.S. Department of Transportation (DOT) project based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-03

SAE ARINC687 Onboard secure Wi-Fi Network Profile Standard

🔗 URL: <https://www.sae.org/standards/content/arinc687/>

ABSTRACT: This document defines a standard implementation for strong client authentication and encryption of Wi-Fi-based client connections to onboard Wireless LAN (WLAN) networks. WLAN networks may consist of multi-purpose inflight entertainment system networks operating in the Passenger Information and Entertainment System (PIES) domain, dedicated aircraft cabin wireless networks or localized Aircraft Integrated Data (AID) devices operating in the Aircraft Information Services (AIS) domain. The purpose of this document is to focus on the client devices requiring connections to these networks such as electronic flight bags, flight attendant mobile devices, onboard Internet of Things (IoT) devices, AID devices (acting as clients) and mobile maintenance devices. Passenger devices are not within the focus of this document.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-06

SAE J2931/7 Security for Plug-In Electric Vehicle Communications

🔗 URL: https://www.sae.org/standards/content/j2931/7_201802/

ABSTRACT: This SAE Information Report J2931/7 establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).

Energy

(NEW) ITU-T Y.bsis-sec Security requirements and capabilities of base station inspection services using unmanned aerial vehicles

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19640

ABSTRACT: Base stations refer to outdoor stations in smart cities that provide public services, such as power transmission stations, communication base stations, weather monitoring stations, and water quality monitoring stations. These stations are typically located outdoors and are susceptible to damage due to weather changes and material aging. Therefore, they require timely and periodic inspections. Unlike traditional IoT security, inspection services for these base stations face significant and unique security threats. The large number and widespread deployment of UAVs, especially with remote docker, resulting in a wide exposure surface for information security and making the service process vulnerable to attacks. Such vulnerabilities could lead to data leakage, including the unauthorized access to sensitive images of restricted areas, which poses significant security risks overall. This draft new Recommendation focuses on security requirements and capabilities for base station inspection (BSI) services using unmanned aerial vehicles (UAVs). It aims to enhance the information security protection when conducting BSI services using UAVs. By doing so, it aims to prevent information security incidents such as errors, malicious intrusions, and data tampering, thereby ensuring the overall security of base stations and maintaining the quality of public services in smart cities.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.iepi-dm-sa framework of security assessment for data management for IoT-based electric power infrastructure

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19081

ABSTRACT: Security assessment for data management encompasses various aspects of the IoT-EPI data lifecycle, including data collection, transmission, storage, processing, and services. By evaluating the security capabilities at each stage, it aims to demonstrate the overall security level, thereby mitigating security risks associated with IoT-based electric power infrastructure and ensuring the provision of efficient and secure data services in smart cities. This draft new Recommendation specifies security assessment framework and security assessment factors for data management for IoT-based electric power infrastructure.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.Sec-outdoor Security requirements and capability of IoT Management platform for outdoor electric power infrastructure

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19075

ABSTRACT: As part of the outdoor electric power infrastructure monitoring system, the IoT management platform has various capability requirements, with security requirements being a critical aspect. Classifying the security requirements and capabilities of IoT management platform can enhance the information security protection capabilities of the IoT management platform during its operation and maintenance, preventing information security incidents such as errors, tampering,

or malicious intrusions from affecting the overall safety of smart city outdoor electric power infrastructure. This draft new Recommendation specifies security requirements and capability of IoT Management platform for outdoor electric power infrastructure.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.sup.access-sec Supplement to ITU-T Y.4221 - Use cases and security requirements for sensing devices to access IoT-based electric power infrastructure monitoring system

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19641

ABSTRACT: IoT-based electric power infrastructure monitoring system (IoT-EPIMS) relies on a large number of sensing devices for data acquisition and operational control. With the digitalization of the electric power industry, the number and diversity of sensing devices have been increasing, especially different security requirements stemming from the different electric power services. To enhance the security of IoT-EPIMS, the security risks and security framework for sensing devices to access IoT-EPIMS, security requirements for three types of sensing devices to access IoT-EPIMS and use cases are supplemented to ITU-T Y.4221.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.uas-dc-fr Framework of unified authentication service for data collaboration in IoT-based electric power infrastructure

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19083

ABSTRACT: The power system utilizes IoT-based electric power infrastructure to collect, aggregate, and distribute IoT data, which is used to enhance the digitization and intelligence of energy and electricity, has become a development trend. In terms of data collaboration, an entity is required to get data from multiple power information systems. However, the authentication methods of the power information systems varies, as a result, entities are required to develop multiple functions to cope with corresponding authentication methods, which results in a high cost for development and maintenance. Therefore, a unified authentication service for data collaboration is required. The unified authentication service is deployed between entities and power information systems, and can be deployed in a centralized way for better efficiency or distributed way for security issues. It receives authentication requests from different entities with unified format, convert data format to adapt for target systems, distribute them to destinations and return information to entities, which reduces the development and maintenance cost. This draft new Recommendation specifies a framework of unified authentication service for data collaboration.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(NEW) ITU-T Y.IoT-Smartcity-Risk Reference framework of cybersecurity risk management of IoT ecosystems on smart cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17916

ABSTRACT: This recommendation contains a reference framework for the process of cybersecurity risk management of IoT ecosystems in smart cities, which provides a series of key risk indicators (KRI). So, city officials can assess the level of risk in IoT ecosystems that are used in the development of a smart city, in order to support their sustainability and resilience goals. The Guidelines include: To describe the elements of an IoT system and analyzing the contribution of each one to the total value of cyber risk in a smart city environment. To analyze the risk factors that should be considered when applying a cyber risk management methodology in IoT systems in smart city environments. To assist governments at all levels to do self-evaluations and encourage them to share the results with others.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Built Environment

CENELEC CLC/prTS 50491-7 Home and Building Electronic Systems - IT security and data protection - User Guide

 **URL:** https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:75291,25&cs=1AC4B90B75A5026B198062B2BBB1F96BE

ABSTRACT: This Technical Specification provides guidance to set-up and manage/update a cybersecure HBES / BACS system. This document provides: 1) Categories of HBES / BACS networks related to cybersecurity updates (managed and unmanaged networks) 2) Risk assessment guide for the above-mentioned categories (at device level for both managed and unmanaged networks, at system level for managed ones only). For manufacturers the document provides a classification scheme based on the security levels from existing standards (ETSI EN 303 645, IEC 62443). For installers, system integrators and other administrators of HBES/BACS this document provides - a generic method for assessment of the security risk for each product in the perspective of the overall system. The result of the evaluation gives the minimum required security level on product level corresponding to the manufacturer classification above. - A guide to select products to comply with the required security level. - Best practice measures on the system security level. - A guide to enhance the maturity level of the cyber security management process.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** Under development

■ Safety and Emergencies

Horizontals & Verticals

ASTM F3463-21 Standard Guide for Ensuring the Safety of Connected Consumer Products

 **URL:** <https://www.astm.org/f3463-21.html>

ABSTRACT: This guide provides guidance for connected consumer products, as it relates to physical product safety hazards created by virtue of their connectivity. It applies to connected products that need testing and evaluation to prevent cybersecurity vulnerabilities and weaknesses that could compromise the safety-related performance of the product, create a physical safety hazard in the product or its operation, or result in a noncompliance to the underlying end product safety standard.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** 2021-10

bloTope project D6.5 V1.0 Proof-of-Concept «Brussels-Capital Region Pilot» Implementation

 **URL:** <https://storage.ning.com/topology/rest/1.0/file/get/35619888?profile=original>

ABSTRACT: This report presents 3 pilots: Safety Around Schools, Waterbus, and Smart Parking for Disabled People. A focus is made on the integration of the bloTope building blocks, mainly in the 'Safety Around School' use case. In particular, it includes the implementation of the IoT gateway based on the O-MI and O-DF standards that enables to publish data coming from heterogeneous systems and its registration on the bloTope marketplace (referred to as IoTbNB) for discovery purposes.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-02

ETSI TR 103 582 EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations

 **URL:** https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf

ABSTRACT: The present document considers communications involving IoT devices in all types of emergency situations. This includes the use of IoT devices to enhance:

-  Emergency calling, e.g. between individuals and emergency authorities/organizations, between emergency authorities/organizations, and between individuals.
-  Mission critical communications within emergency services/public safety organizations, e.g. between public safety officers and control centres, between the control centres of different public safety organizations, and between individual public safety officers.
-  Public Warning System type communications from authorities to the general public.
-  Automated emergency response (new IoT domain) between two IoT devices.

The current state of the art for IoT device communications, especially when relevant to emergency situations, is described and use cases illustrate how such communications can be used to provide additional/enhanced information for communicating parties involved in emergency situations. The impact of the use cases on the existing emergency, public warning, and mission critical communications is then considered, and recommendations for requirements to existing specifications for each domain are provided.

 **DOCUMENT TYPE:** Technical_Report

ITU X.1303 bis Secure applications and services – Emergency communications: Common Alerting Protocol Version 1.2

📎 **URL:** <https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/T-REC-X.1303bis-201403-.pdf>

ABSTRACT: The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

📁 **DOCUMENT TYPE:** Recommended Practice

📅 **PUBLICATION DATE:** 2014-03

ITU-T Y.4116 Requirements of transportation safety services including use cases and service scenarios

📎 **URL:** <https://handle.itu.int/11.1002/1000/13385>

ABSTRACT: This Recommendation addresses requirements for providing transportation safety services based on Internet of things (IoT) technologies. These requirements are applicable to various means of transportation, e.g., road, railway, maritime and air.

In this Recommendation, the concepts of transportation safety management according to the processing phases of IoT sensing data and the IoT sensing data necessary for safety management are introduced. An example of a decision-making hierarchy for transportation safety is also described.

The requirements for transportation safety services are described and classified according to the ITU T IoT reference model [ITU-T Y.4000].

Use cases and related service scenarios used to extract requirements for the various transportation safety services are described in Appendix I.

Appendix II shows the relationship between the requirements provided in clause 7 and the use cases described in Appendix I.

📁 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** 2017-10

(NEW) ITU-T Y.4705 (ex Y.nmm-isms) Metadata model of sensing capability for disaster monitoring system

📎 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17883

ABSTRACT: This Recommendation provides a Sensing Capability Metadata Model (SCMM) for Disaster Monitoring System (DMS). It clarifies the basic metadata categories of sensing capability for DMS, and describes the structure and contents of sensing capability metadata elements of SCMM for DMS.

📁 **DOCUMENT TYPE:** Standard_Specification

📅 **PUBLICATION DATE:** Under development: Consented 2024-07

(NEW) ITU-T Y.4222 (ex Y.smart-evacuation) Framework of smart evacuation in a disaster or emergency in smart cities and communities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17886

ABSTRACT: Smart evacuation facilitates effective and efficient solutions for people inside a disaster or emergency zone and for people that need to enter such a zone as part of the response. Internet of things (IoT) and smart cities and communities could be used to provide smart evacuation during a disaster or an emergency. This Recommendation describes concepts and features of smart evacuation control in disaster and emergency situations. It identifies high-level requirements and ICT infrastructure for smart evacuation along with use cases in disaster and emergency situations. The introduction of a smart evacuation service will allow the maintenance of the level of comfort for the population achieved in a smart city even in the event of an emergency. This is fundamental to justify the enormous material costs for the rapid development of smart cities around the world against the background of emergencies that have become more frequent throughout the world.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development:Determined on 2024-07

(NEW) ITU-T Y.4229 (ex Y.IoT-SFFS) Requirements and reference functional model of IoT-based smart forest firefighting system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17955

ABSTRACT: The frequent occurrence of forest fires has become a world-class problem. Although many countries have invested a lot of money in numerous counter-measures there are still several remaining challenges to be overcome. These challenges include the vastness of forest areas that cannot be fully monitored, and the incomplete network coverage of forests preventing efficient information transmission. Additionally, the performance of typical Internet of things (IoT) devices often fails to meet the actual requirements of forest applications. There are also a lack of early warning systems for impending forest fires, which delays the fire-extinguishing and rescue operations when fires occur, as well as a lack of adequate assessment and inspection of post-fire capabilities. With the development of IoT and artificial intelligence (AI), forest firefighting systems have become smarter. Smart forest firefighting systems are deployed in forest areas to enable real-time monitoring and early warning before forest fires occur. They can predict, locate, evaluate and extinguish fire when a fire occurs and provide inspection and damage assessment after a fire. This Recommendation introduces the smart forest firefighting system based on IoT and specifies the reference functional model and requirements. This Recommendation is intended to guide the design, development and implementation of the IoT-based smart forest firefighting system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development: Determined on 2024-07

(NEW) ITU-T Y.4230 (ex Y.EV-charging) Requirements and capability framework of public smart charging service for electric vehicles

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17954

ABSTRACT: With the rapid increase in the public usage of electric vehicles (EVs) in the city, more and more EV users put forward high requests for public charging service. Therefore, public smart charging service for EVs is the future development direction, and is an important part of the smart city. Compared with the traditional charging service, public smart charging service has the advantages of highly networked and digitized system, flexible and convenient use and intelligent management of electric power. Public smart charging service will be implemented on smart city infrastructure and it is indispensable for smart city in the future. This Recommendation specifies requirements and

capability framework of public smart charging service for EVs, to optimize the EV charging service process and improve the EV charging service experience of EV users.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Determined on 2024-07

OASIS CAP-v1.2 Common Alerting Protocol Version 1.2

🔗 URL: <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html>

ABSTRACT: The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2010-07

oneM2M TS-0037-V-4.0.2 IoT Public Warning Service Enablement

🔗 URL: <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35597>

ABSTRACT: This technical specification specifies the information model of the public warning service, and defines the resource mapping rule for the information model of the public warning.

🔗 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2023-02

Manufacturing

IEC 63237-1 ED1 Household and similar electrical appliances - Product information properties - Part 1: Fundamentals

🔗 URL: https://www.iec.ch/dyn/www/f?p=103:7:602873313141987::FSP_ORG_ID,FSP_LANG_ID:1275,25

ABSTRACT: This part of IEC 63237 provides a method of standardizing the descriptions of household electrical appliances. The aims of this standard are: a) to define a common language for customers and suppliers through the publication of classes, represented by properties and their attributes; b) enable electronic data exchange by machines (including information technology systems, see M2M communication); c) to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations; d) to offer also a dictionary to legislators and; e) to reduce transaction costs.

The standard describes household electrical appliances using properties and makes the associated properties available in the IEC Common Data Dictionary (IEC CDD). Furthermore, this document provides rules, methods and the generic data structure for product specific classification standards and on how to produce a reference dictionary based on IEC 61360 Series. This in turn creates a descriptive basis of company internal and external descriptions of household electrical appliances based on structured classes and lists of properties.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

(Updated) ETSI TS 103 300-3 V2.2.1 ITS; Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2

 **URL:** https://www.etsi.org/deliver/etsi_ts/103300_103399/10330003/02.02.01_60/ts_10330003v020201p.pdf

ABSTRACT: Cooperative awareness within road traffic means that road users and roadside infrastructure are informed about each other's position, dynamics and attributes. Road users are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians and roadside infrastructure equipment including road signs, traffic lights or barriers and gates. The awareness of each other is achieved by regular exchange of information among vehicles, pedestrians and roadside infrastructure based on wireless networks. An integral part of road ITS are the class of vulnerable road users (VRU) including pedestrians, bicyclists, motorcyclists and animals. In order to efficiently participate in the road safety related ITS communication a continuous repeated awareness message is transmitted by these VRUs using the VRU Awareness Message (VAM).

The construction, management and processing of VAMs is done by the VRU basic service, which is part of the facilities layer within the ITS communication architecture defined in ETSI EN 302 665.

This document is the third and last part of the ETSI TS 103 300 standard for VRU awareness.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2023-02

(NEW) ITU-T Y.Highway-KPI Key performance indicators of ICT based highway traffic safety assessment

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18476

ABSTRACT: This Recommendation gives a general guidance to cities and provides a set of key performance indicators (KPIs) related to the use of information and communication technology (ICT) in the context of highway traffic safety assessment (HTSA). This Recommendation can help assess highway traffic safety by offering a set of KPIs when identifying, analyzing and evaluating the highway traffic risk.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: Under development

ITU-T Y.4457 (06/2018) Architectural framework for transportation safety service

 **URL:** <https://handle.itu.int/11.1002/1000/13641>

ABSTRACT: This recommendation addresses a transportation safety management model that describes disaster management steps based on Internet of things (IoT) technologies in order to reduce damage from disasters. An architectural model for transportation safety services is described based on [ITU T Y.4116] and on requirements according to the IoT reference model [ITU T Y.4000]. The scope and characteristics of transportation disasters from various transportations (e.g., road, railway, maritime and air transportation) are based on [ITU-T Y.4116]. Transportation safety management parameters (e.g., safety index and driver tiredness) are presented respectively in Annex A and Annex B and sensing data pre-processing procedure and characteristics of transportation application services are described in the appendices of this Recommendation.

 DOCUMENT TYPE: Standard_Specification

 PUBLICATION DATE: 2018-06

Energy

(NEW) ITU-T Y.SNPG-ref Reliability evaluation frameworks of sensing network in power grid

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19646

ABSTRACT: Traditional power grid is undergoing profound transformations, with large-scale renewable energy generation and distributed clean energy increasingly becoming dominant. As high proportions of clean energy and a massive number of intelligent power distribution terminals equipped with power sensing technologies are integrated, the types, frequency, and quality of data collected by power grid sensing information are enhanced. The volume and dimensions of data are experiencing exponential growth, forming a vast sensing network in power grid. The Internet of things (IoT) as a relatively new technology is transforming sensing network in power grid to further enhance sensing data transformation services. However, this transformation concomitantly creates a need for effective reliability evaluation frameworks of sensing network in power grid. This recommendation specifies the reliability evaluation frameworks of sensing network in power grid. Based on existing network evaluation standards, the main factors of the reliability evaluation are stability, fault-tolerance, maintainability and security. This framework provides a comprehensive reference for reliability evaluation of sensing network in power grid.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Water

(NEW) ITU-T Y.KPI-Flood Key Performance Indicators of ICT based Urban Flood Disaster Prevention and Mitigation Capability

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17963

ABSTRACT: Flood disaster is a critical issue influencing the safety of a city. There are many kinds of flood prevention and mitigation measures, however, no comprehensive assessment of these measures is provided yet. This recommendation presents methodology of evaluating ICT based urban disaster prevention and mitigation capability for floods. It provides a set of key performance indicators to quantitatively assess the flood disaster prevention and mitigation capability of cities.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Horizontals & Verticals

(NEW) ITU- T Y.4226 (ex Y.isms) Functional framework and requirements for disaster monitoring system

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17882

ABSTRACT: This Recommendation provides an overview of a disaster monitoring system (DMS) for Smart Sustainable Cities (SSC) and identifies requirements and functional framework of the DMS.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4505 (ex Y.MIM) Minimal Interoperability Mechanisms for smart and sustainable cities and communities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18458

ABSTRACT: This Recommendation defines the concept, purpose, and structure of Minimal Interoperability Mechanisms (MIMs) that provide the requirements for implementing minimal but sufficient capabilities needed to achieve interoperability based on a minimal common ground. The value of this approach is becoming widely recognised and several organisations and national and regional agencies are showing interest in the development of MIMs covering a range of different topics.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T YSTR.ACC-SCC Guidelines on developing ICT services for accessible smart cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18454

ABSTRACT: Smart city services can have a ripple effect beyond improving physical accessibility for persons with disabilities, those with age-related disabilities and those with specific needs. Persons with disabilities can benefit from more efficient and sophisticated city services through smart city services. Thus, it is an important opportunity to improve the quality of life using city functions equivalent to those without disabilities. However, as seen in many other use cases of ICTs, without consideration for persons with disabilities from the design stage, it is bound to be another barrier for persons with disabilities. Using a two-layer structure of accessibility consideration principles, this Technical Report provides development guidelines to be considered at each layer to implement accessible smart city services. Also, exemplar accessible smart city services are illustrated in the appendix.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.4227 (ex Y.IoT-BC-reqts-cap) IoT requirements and capabilities for support of blockchain

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17932

ABSTRACT: Blockchain can help IoT and smart city and community related services and applications

to establish trust, accountability and transparency while streamlining business processes. In order to promote the integration of blockchain with the IoT infrastructure, as well as enable richer flexible service scenarios for different IoT and smart cities and community verticals, this Recommendation, from the IoT point of view, identifies the functionalities of the blockchain, specifies the requirements of blockchain enabled IoT, and describes the specific IoT capabilities that are necessary to support blockchain.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

ISO/IEC 30146:2019 Information technology - Smart city ICT indicators

🔗 URL: <https://www.iso.org/standard/70302.html>

ABSTRACT: This document defines a comprehensive set of evaluation indicators specially related to information and communication technologies (ICT) adoption and usage in smart cities. Firstly, this document establishes an overall framework for all the indicators. Then, this document specifies the name, description, classification and measure method for each indicator.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-10

ISO/IEC 30182:2017 Smart city concept model — Guidance for establishing a model for data interoperability

🔗 URL: <https://www.iso.org/standard/53302.html>

ABSTRACT: ISO/IEC 30182:2017 describes, and gives guidance on, a smart city concept model (SCCM) that can provide the basis of interoperability between component systems of a smart city, by aligning the ontologies in use across different sectors. It includes:

- concepts (e.g. ORGANIZATION, PLACE, COMMUNITY, ITEM, METRIC, SERVICE, RESOURCE); and
- relationships between concepts (e.g. ORGANIZATION has RESOURCES, EVENT at a PLACE).

The SCCM does not replace existing models where they exist, but, by mapping from a local model to a parent model, questions can be asked about data in a new and joined-up way.

ISO/IEC 30182:2017 is aimed at organizations that provide services to communities in cities, and manage the resulting data, as well as decision-makers and policy developers in cities.1)

The SCCM is relevant wherever many organizations provide services to many communities within a place.

It does not cover the data standards that are relevant to each concept in the SCCM and does not attempt to list or recommend the sources of identifiers and categorizations that cities map to the SCCM.

The SCCM has been devised to communicate the meaning of data. It does not attempt to provide concepts to describe the metadata of a dataset, for example, validity and provenance of data.

It covers semantic interoperability, that is, defining the meaning of data, particularly from many sources. It does not cover other barriers to interoperability, some of which are described at 3.2.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2017-05

oneM2M-TR-0061 -V-0.5.0 Study on ontologies for Smart City Services

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35482>

ABSTRACT: Study on ontologies for Smart City Services.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2022-12

SmartCity

(NEW) ITU_T Y.4231 (ex Y.IoT-Vreqs) Requirements and capability framework of the internet of things for vision

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17953

ABSTRACT: With the popularization and development of smart cities and numerous IoT based verticals, the connotation of the internet of things (IoT) is expanding and is no longer limited to simple sensor data collection and discrimination. The IoT for vision is one of the main development directions of the IoT which use digital cameras and other types of sensors in order to perceive objects of interest (including human beings, vehicles, animals etc.) for diverse applications based on appropriate analysis. This Recommendation provides requirements and capability framework of the IoT for vision, a typical IoT for vision application workflow as well as some relevant IoT for vision use cases.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Determined on 2024-07-12

(NEW) ITU-T Y.4233 (ex Y.FSPH Framework for smart public health emergency management in smart and sustainable cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18460

ABSTRACT: This Recommendation specifies the framework of smart public health management in Smart and Sustainable Cities (SSC). SSCs are capable of fostering data driven smart applications to manage limited resources and implement them to thwart the advent of future pandemics of the same magnitude. Linking SSC with public health frameworks to manage future pandemics/epidemics to the attainment of the SDGs (3: Global Health, 1: Poverty Eradication and 11: Make cities inclusive, safe, resilient, and sustainable, and the Sendai Framework for Disaster Risk Reduction) is a challenge and serves a dual purpose. With the utilization of appropriate emergency communication and public health frameworks, it will become easier to develop models to predict the spread of diseases, ascertain the source of illnesses, coordinate lockdowns, detect and report symptoms, identify viral strains and provide remote assistance as required with limited human interaction, through an IoT-based infrastructure. This Recommendation is based on the U4SSC report entitled "Smart public health emergency management and ICT implementations" [b-U4SSC] and its structure is as follows: it starts with an analysis of the public health context and of corresponding frameworks, and returns a generic public health framework, which specifies the pandemic's lifecycle. Then, this generic framework is interconnected with the SSC and with city resilience. Then, it depicts with UML diagrams how this framework can be executed within the SSC environment and highlights the SSC components that play role in this execution.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Determined on 2024-07-12

(NEW) ITU-T Y.4234 (ex Y.RemoteEd) Requirements, capabilities and deployment models for e-learning in remote classrooms

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18751

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

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Determined on 2024-07-12

(NEW) Y.4420-rev framework of Internet of things based monitoring and management for Lift

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19606

ABSTRACT: Recommendation ITU-T Y.4420 describes a framework of Internet of things (IoT) based monitoring and management for lifts, including a protocol and a data model. Lifts need to interact with applications through communication networks to provide different kinds of services to end users. In many cases, lifts cannot connect to communication networks directly. Therefore, gateways support the interconnection of such lifts with communication networks. Y.4420 can be applied to various services that utilise lifts in smart buildings. However, indoor delivery services and lift remote control require remote connectivity to the lift. The revised Y.4420 enhances Y.4420 including the requirements, data models and enhanced use cases that apply to services requiring remote connectivity to the lift.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.EMM-Reqts: Requirements for Real-Time Event Monitoring and Integrated Management in Smart City Platforms

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17952

ABSTRACT: This draft Recommendation presents the overview and specifies the requirements of a Real-time Event Monitoring and Integrated Management (EMM) platform. The real-time event monitoring and integrated management platform is one of Smart City Platforms [ITU-T Y.4201]. It connects various intelligent facilities equipped with IoT sensors, providing stakeholders with the necessary data (integrated information) to make informed decisions and respond promptly to an event that may rise in a city. The platform is particularly designed for integration of data and allowing the users to utilize data and to monitor city events in real time.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.energy-storage Requirements and capability framework of energy storage service for residential community in smart city

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18749

ABSTRACT: With the promotion of renewable energy generation in residential communities, a large number of community users are transformed into prosumers with a dual role of producer and consumer. To maximize the interests of community users, it is necessary to introduce energy storage service for residential community (ESSRC) to centrally manage energy. Furthermore, ESSRC operators can earn the price difference through the difference of spot prices in the electricity market, so as to achieve a win-win situation. ESSRC is an important part of smart residential communities in smart cities, and a large number of ESSRC operators have entered this market. But the lack of standards could limit the operators' ability to meet rising demand across the globe. ESSRC is based on an ICT-based information management system, so this Recommendation focuses on requirements and capability framework of ESSRC in smart city. This Recommendation will help to promote the achievement of circular and sustainable smart cities and communities. The use case of ESSRC is provided in Appendix

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.EV-PUD Requirements of electric vehicle power usage data acquisition and management for smart city

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19062

ABSTRACT: Electric vehicle (EV) market is growing, and the power consumption cannot be ignored. For better tracking and management of carbon emission in smart cities, fine-granularity power usage (PU) data is required. This Recommendation provides the requirements for the electric vehicle power usage data acquisition and management. The data collected pertains to the electric vehicle's power usage process, and the smart city infrastructure, including roadside units, cellular base stations, hotspots etc., should be used for EV PU data delivery and utilization in smart city platform. Following the specified requirements, uniform electric vehicle power usage data can be acquired and managed, which can enable smart city to trace vehicle level carbon footprint as well as to provide information support to other applications e.g., power charging station planning, insurance pricing, etc. This Recommendation specifies the requirements and reference system framework for electric vehicle power usage data acquisition and management for smart city, as well as it describes some relevant reference use cases for EV PU data acquisition and management.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

■ Social Community and Wellbeing

Horizontals & Verticals

ISO/IEC TR 30174:2021 Internet of Things (IoT) - Socialized IoT system resembling human social interaction dynamics

 **URL:** <https://webstore.iec.ch/publication/66419>

ABSTRACT: ISO/IEC TR 30174:2021(E) describes: a) key features of the socialized IoT systems, e.g. sensing the external physical world, resolving the uncertainties of targets, satisfying users' demand and providing quality service, etc.; b) socialized attributes, i.e. socialized network, socialized collaboration, and socialized services, which are derived from the key features; and c) guidelines on how to use or apply the socialized attributes in the design and development of IoT systems.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2021-11

(NEW) ITU-T Y.ACC-ASM Requirements and capabilities of accessible service management using user accessibility preference profile for IoT services

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19057

ABSTRACT: 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.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.dt-PAF Requirements and capabilities of a digital twin for pedestrian accessibility facilities for persons with disabilities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19600

ABSTRACT: Various walking assistance facilities are installed on pedestrian paths throughout the city to help persons with disabilities walk. For example, wheelchair ramps are installed on stairs where wheelchairs are difficult to move for those with physical disabilities who use wheelchairs. Moreover, braille blocks for those with visual disabilities are installed on pedestrian roads, and sound signals that inform the change of traffic lights through audio signals are installed at crossings. These diverse facilities support the independent mobility of persons with disabilities. However, their usage and management are often hindered by the harsh conditions in which they are installed. The challenges range from incorrect installations that render the facilities unusable to accidents that lead to breakages and even instances where the facilities, though present, are underutilised due to a lack of promotion. For persons with disabilities, even a single problem on their walking path can make the entire journey impossible. This underscores the critical importance of the control and management of these facilities. Ensuring independent mobility is not just a matter of convenience, but a fundamental right that we

must strive to protect. This Recommendation provides the requirements and capabilities of a digital twin for pedestrian accessibility facilities for persons with disabilities, which supports controlling and managing pedestrian assistance facilities for persons with disabilities installed on pedestrian roads, providing appropriate information to users, and assisting in maintenance and management.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Energy

ITU-T L.1383 (10/2021) Smart energy for cities and home applications

🔗 URL: <https://handle.itu.int/11.1002/1000/14719>

ABSTRACT: This recommendation will focus on smart energy solutions in different applications for saving energy and reducing carbon emissions. With the development of ICT technology, smart energy solutions are not only used for ICT systems, but also in homes, remote islands, businesses, industries, and countries. The following aspects will be taken into consideration in this Recommendation: - Different energy input solutions - Electric characteristic - Safety performances - Environmental impacts - Reliability - Any other items

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2021-10

SmartCity

bloTope project D6.4 V1.0 Proof-of-Concept “Greater Lyon Pilot” Implementation

🔗 URL: <https://storage.ning.com/topology/rest/1.0/file/get/35619978?profile=original>

ABSTRACT: This document presents two pilot use cases deployed in Lyon: bottle banks management and heat wave mitigation. It presents how the use cases meet the smart metropolis strategy, the expectations of the different stakeholders, and which services are provided. Hardware and software solutions contributing to the services are then described. A focus is made on the integration of the heat wave mitigation use case in the bloTope ecosystem including the description of the gateways built between heterogeneous systems and the O-DF/O-MI standard, the semantic annotations added to data and the publication on the bloTope marketplace. Concerning the bottle banks use case, the document shows how the interoperability enabled by the bloTope ecosystem makes it possible to develop new collaborative services with several partners and the metropolis.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2018-01

Health

ETSI SR 003 809 eHEALTH; The role of ICT to enable Health crisis management and recovery; Responding to the 2019 SARS-CoV-2 Pandemic

🔗 URL: https://www.etsi.org/deliver/etsi_sr/003800_003899/003809/01.01.02_60/sr_003809v010102p.pdf

ABSTRACT: This report contains a detailed review of actions to be taken by ETSI, in partnership with

other SDOs and industrial development groups, in driving ICT standards to support societal responses to health crisis. It considers the role played by ICT in response to the SARS-CoV-19 pandemic and identifies where there were successes, where there were failures, and where ICT and particularly standards in ICT, may play a role in future mitigations.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2021-12

ITU-T H.842 (11/2019) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 2: Optimized Exchange Protocol: Personal Health Gateway

URL: <https://handle.itu.int/11.1002/1000/14116>

ABSTRACT: This recommendation provides a test suite structure (TSS) and the test purposes (TPs) for personal health gateways (PHGs) using the IEEE 11073-20601 optimized exchange protocol in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITU-T H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-11

ITU-T H.844 (11/2019) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 4: Continua Design Guidelines: Personal Health Gateway

🔗 URL: <https://handle.itu.int/11.1002/1000/14117>

ABSTRACT: This recommendation provides a test suite structure (TSS) and the test purposes (TP) for Personal Health Gateways (PHGs) in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITU-T H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2019-11

■ Strategies Policies and Planning

Horizontals & Verticals

CEN/CENELEC CWA 17431 Principles and guidance for licensing Standard Essential Patents in 5G and the Internet of Things (IoT), including the Industrial Internet

🔗 URL: <https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa17431.pdf>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Guideline

📅 PUBLICATION DATE: 2019-06

ETSI TR 103 536 Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms

🔗 URL: https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf

ABSTRACT: The document outlines the nature, the role of IoT platforms and proposes elements for the identification of the most relevant ones. It also addresses detailed examples such as Industrial IoT to outline the challenges posed to generic IoT platforms. It addresses the issues related to the interoperability and interworking of IoT platforms, in particular standardized IoT platforms, and how the way they are handled can foster their adoption by the IoT community.

📄 DOCUMENT TYPE: Technical_Report

📅 PUBLICATION DATE: 2019-12

(Updated) ISO/IEC AWI 21823-5 Internet of Things (IoT) - Behavioral and policy interoperability

🔗 URL: <https://www.iso.org/standard/90177.html>

ABSTRACT: This part of ISO/IEC 21823 specifies interoperability from a behavioural and policy viewpoint. In this document, the following specifications for interoperability from a policy and behavioural point of view are included:

- a principle of how to achieve behavioural and policy interoperability;
- requirements on information related to behavioural and policy interoperability, and
- a framework for processes on developing information exchange rules from a behavioural and policy viewpoint

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Mobility

oneM2M TS-0002-V5.1.0 Requirements

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36546>

ABSTRACT: The present document contains an informative functional role model and normative technical requirements for oneM2M.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2024-01

SAE ARINC686 Roadmap for IPv6 Transition in Aviation

 **URL:** <https://www.sae.org/standards/content/arinc686/>

ABSTRACT: This report represents the consensus of industry to prepare a roadmap migration from IPv4 to IPv6. This document describes airline objectives (air and ground side when possible) towards the development and introduction of IPv6. There are three distinct elements considered: 1) the applications for addressing aspects 2) the communication network(s) over which the applications are running for the IP protocol level itself and associated features, and 3) the physical link(s) the network(s) interface.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** 2020-06

Buildings

ETSI TS 103 735 SmartM2M; Smart Lifts IoT System

 **URL:** http://www.etsi.org/deliver/etsi_ts/103700_103799/103735/01.01.02_60/ts_103735v010102p.pdf

ABSTRACT: Standardize the IoT system for Smart Lifts. It includes : a) the identification of the relevant roles; b) the Information models in the Smart Lift system, including signals, alarms and commands; c) the mapping to Semantic model of oneM2M (SDT) and ETSI SAREF; d) the communication system.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-07

■ Sustainability and Resilience

Horizontals & Verticals

(NEW) 3GPP TR 22.867 V18.2.0 Study on 5G Smart Energy and Infrastructure (Release 18)

🔗 **URL:** https://www.3gpp.org/ftp/Specs/archive/22_series/22.867/22867-i20.zip

ABSTRACT: The present document is to address study use cases, potential new service requirements for 5G system to support Smart Grid including the following topics:

- Smart Grid services, e.g. IEC standards, and their communications requirements including capacity, latency, availability, end-to-end QoS, resilience/redundancy and security.
- Deployment requirements when considering constraints e.g. service lifetime, coverage (ubiquity), electromagnetic applicability (e.g. penetration, ability to operate in high EM environments,) etc.
- Additional requirements due to operational manageability – e.g. the ability to configure and monitor the real (achieved & up to date) availability of virtual network topologies
- New Smart Grid use cases and potential service function requirements: e.g. on-demand power supply, distributed power supply system, distribution automation, higher accuracy power load measurement and control, meter automation, etc.
- Communication KPI and service requirements for enabling microgrids, DER and specifically distributed generation (DG) that require 5G wireless communication (e.g. wind and solar energy generation, including scenarios at or near residential / consumer premises, etc.)

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-12

(NEW) 3GPP TR 23.776 V17.0.0 Study on architecture enhancements for 3GPP support of advanced Vehicle-to-Everything (V2X) services; Phase 2; (Release 17)

🔗 **URL:** https://www.3gpp.org/ftp/Specs/archive/23_series/23.776/23776-h00.zip

ABSTRACT: The objective of this Technical Report is to investigate 5G System enhancements based on what has been specified in Rel-16, for enhanced support of V2X operation for pedestrian UEs (i.e. UEs for Vulnerable Road Users), e.g. V2X communication with power efficiency, according to vehicular services requirements defined in TS 22.185 and TS 22.186

📄 **DOCUMENT TYPE:** Technical_Report

📅 **PUBLICATION DATE:** 2021-03

(NEW) ISO/IEC 20924:2024 Internet of Things (IoT) and digital twin - Vocabulary

🔗 **URL:** <https://webstore.iec.ch/en/publication/70408>

ABSTRACT: ISO/IEC 20924:2024 is available as ISO/IEC 20924:2024 RLV which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. ISO/IEC 20924:2024 provides a definition of Internet of Things and digital twin along with a set of terms and definitions. This document is a terminology foundation for the Internet of Things and digital twin. This third edition cancels and replaces the second edition published in 2021. This edition constitutes a technical revision. This edition includes the following technical changes with respect to the previous edition:

- a) addition of new terms which are used in other ISO/IEC IoT related standards;
- b) update of some definitions to align with current usage in IoT standards;
- c) extension of digital twin related vocabularies with title and scope changes

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2024-02

(NEW) ITU_T L.1333 Carbon data intensity for network energy performance monitoring

🔗 URL: <https://www.itu.int/rec/T-REC-L.1333-202209-I>

ABSTRACT: 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.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2022-09

(NEW) ITU_T L.1410 Methodology for environmental life cycle assessments of information and communication technology goods, networks and services

🔗 URL: <https://www.itu.int/rec/T-REC-L.1410-201412-I/en>

ABSTRACT: 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

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2014-12

(NEW) ITU_T L.1480 Enabling the Net Zero transition: Assessing how the use of information and communication technology solutions impact greenhouse gas emissions of other sectors

🔗 URL: <https://www.itu.int/rec/T-REC-L.1480-202212-I>

ABSTRACT: 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:

- ICT solution(s) implemented in a specific context by the user of the ICT solution(s).
- ICT solution(s) implemented at different scales, including at an organizational level (whether private or public organizations), at a city level, at a country level or at worldwide level.
- ICT solution(s) seen from the perspective of an ICT organization contributing to the ICT solution(s). This includes:

- 1) Assessment of the aggregated effect of all ICT solutions provided by an ICT organization across all its customers;
- 2) Assessment of the aggregated effect of one or several ICT solutions provided by an ICT organization across some of its customers;
- 3) Assessment of the effect of one or more specific ICT solutions implemented in an actual context for a specific customer.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2022-12

(NEW) ITU-T Y.IoT-ISP Reference framework for the smart industry service platform based blockchain and IoT

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19065

ABSTRACT: Data security and dependable exchange are critical to the industry's digital revolution. IoT and blockchain technologies will provide new technological solutions for industrial transformation. It aim to connect devices securely and share data reliably among different industrial platforms by leveraging IoT and blockchain technology, which could improve collaboration between supply chain and production processes. The object of this Recommendation is to define the the smart industry service platform based blockchian and IoT, and provide requirements and functional framework for the the smart industry service platform based blockchian and IoT. IoT and blockchain technologies will provide new technological solutions for industrial transformation. Smart industry service platform based blockchian and IoT aims to connect devices securely and share data reliably among different industrial platforms by leveraging IoT and blockchain technology, which could improve collaboration between supply chain and production processes. The object of this Recommendation is to define the smart industry service platform based IoT and blockchian, and provide requirements and functional framework for the smart industry service platform.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Manufacturing

(NEW) ITU-T Y.KPEM-SM Key performance evaluation models of smart manufacturing

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18474

ABSTRACT: This criteria specifies technically oriented key performance indicators used in the life cycle of smart manufacturing. It provides the key performance evaluation framework, indicators and methods for digital transformation of manufacturing, quantitatively evaluate the value and benefits of digital transformation from the aspects of business innovation, operation optimization and sustainable development, provides a basis for city managers to make decisions and accelerates the process of digital transformation of manufacturing. It is designed as a practical tool for city managers, and all relevant stakeholders to study the performance and benefits of digital transformation of manufacturing from a technical perspective. Thus, it gives general guidance for accurately assessing the benefits of digital transformation and helping cities achieve sustainable development goals.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

Energy

(Updated) CENELEC prEN IEC 63345 Energy Efficiency Systems - Simple External Consumer Display

URL: https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:74332,25&cs=10C4D76ADB0C4C7D5B9DA81FF8E547C2D

ABSTRACT: This Standard specifies a data model to abstract the metering world towards a simple external consumer display. The data model, as described by means of functional blocks contained in this IEC Standard, lays down the format of metering data accessible by a simple external consumer display. This data interface would be typically part of the meter communication functions and be accessed by a simple external consumer display via the H1 interface of the CEN/CLC/ETSI TR 50572 between the display and the meter communication functions.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: 2023-10

CENELEC prEN IEC 63402 Energy Efficiency Systems - Smart Grid - Customer Energy Management Systems - General Requirements and Architecture

URL: https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:74575,25&cs=167DD57F4AA099C41201ADC1979E157B2

ABSTRACT: This Standard specifies General Requirements and Architecture of an application layer interface between the Customer Energy Manager (CEM) and Smart Devices (SD) operating within the smart grid premises-side system (i.e. home or building but not industrial premises).

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

SmartCity

(NEW) ITU-T Y.IoT-BEMS-af Assessment framework of IoT infrastructure in building energy management system

URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19088

ABSTRACT: IoT is already having a significant impact on the smart building sector. With the integration of the Internet of Things (IoT) into the field of building energy management system (BEMS), opportunities have emerged to enhance energy efficiency and reduce capital expenditures in buildings. Consequently, implementation and assessment of IoT infrastructure in BEMS has become crucial. Therefore, this contribution proposes a new work item, "Assessment framework of IoT infrastructure in building energy management system". This document provides an assessment framework and assessment factors for the IoT infrastructure of BEMS, taking into consideration an IoT reference model, with the aim of enhancing implementation efficiency for stakeholders.

DOCUMENT TYPE: Standard_Specification

PUBLICATION DATE: Under development

(NEW) ITU-T Y.SSC-NGUM A Methodology for Next Generation Urban Measurements

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17914

ABSTRACT: Smart and sustainable cities and communities measure their performance through well-defined Key Performance Indicators (KPIs). Measurement of these KPIs rely on collected data and their accuracy. Next Generation Urban Measurements methodology described in this Recommendation uses innovative sensing techniques to collect extensive and more frequent city data from various locations in the city at different times. Hence data for city KPIs such as air quality, noise pollution, road quality and traffic congestion, among others, may potentially be collected by using the Next Generation Urban Measurements methodology described in this Recommendation. This Recommendation provides a structured step-wise methodology to help cities apply the Next Generation Urban Measurements techniques. It also indicates big data implications and related high-level building blocks required for implementing Next Generation Urban Measurements.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ITU-T Y.Sup.MM-EDMC-SSC Maturity model of digital management capability of industrial equipment used in smart sustainable cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18741

ABSTRACT: As the basic carrier of manufacturing activities, the digital management capability of equipment is of great significance to the value creation activities of industry in SSC. With the rapid development of advanced information technologies such as the Internet of Things, big data and artificial intelligence, the intelligent level of equipment has been continuously improved. Enhancing the digital management capacity of equipment contributes to improve production efficiency, reduce operation cost and increase economic benefits. Therefore, digital management of equipment provides a feasible way for urban innovation and sustainable development. This draft Supplement provides a maturity model of digital management capability of industrial equipment for SSC. The maturity model helps to identify the maturity levels, dimensions and guidelines of digital management capability of industrial equipment for SSC. It is designed as a practical tool for city managers and related stakeholders to study the effectiveness of digital management of equipment from resource, environment, operation and other dimensions. Thus, it provides overall guidance for assessing the maturity of digital management capability of industrial equipment and helping cities achieve sustainable development goals.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

Social Community and Wellbeing

(NEW) ITU-T Y.QE-DMI-SSC Quality evaluation of digital models in industry for smart sustainable cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18475

ABSTRACT: As the foundation of smart sustainable cities (SSC), industry has become a critical element in SSCs. With the advancements in information technology, industrial digital twins are driving industrial innovation. The industrial digital twin is the real-time connection and interaction between industrial digital models and industrial assets, such as products, production facilities, transport vehicles, etc. Thus, the industrial digital model is an abstract representation of real industrial assets, which is the foundation of the industrial digital twin. At present, the digital model in industry is widely used for the simulation, analysis and optimization of industrial products. As the digital representation of industrial

knowledge mechanisms, they reflect the structure, knowledge and spatio-temporal characteristics of industrial products. Therefore, the quality of digital models of industrial products is essential for the promotion of industrial development, and helps in the construction and management of SSC. This draft new Recommendation comprehensively evaluates the quality of industrial digital models from three aspects: the digital model construction quality, the digital model application quality and the digital models cost-effectiveness. It aims to provide all relevant stakeholders with a practical assessment tool that gives general guidance for accurately assessing the quality of digital models in industry to help improve industrial product quality.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Buildings

ITU-T L.1371 (06/2020) A methodology for improving, assessing and scoring the sustainability performance of office buildings

🔗 URL: <https://handle.itu.int/11.1002/1000/14304>

ABSTRACT: This recommendation provides a consistent framework for owners, managers and building operators to critically assess ten (10) key areas of environmental performance and management of office buildings; Energy, Water, Air, Comfort, Health & Wellness, Purchasing, Custodial, Waste, Site, and Stakeholders.

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2020-06

Built Environment

(NEW) ITU-T Y.IoT-ESSB Functional architecture of IoT-based energy-saving service for smart buildings

🔗 URL: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19616

ABSTRACT: Smart buildings suffer from issues such as uncoordinated equipment operation and low energy utilization rates, resulting in a series of industry pain points, including high energy consumption, low data utilization, high operation and maintenance costs. Through IoT technology, smart buildings can achieve real-time monitoring and remote control of energy consumption data, allowing for refined management and intelligent optimization of energy use. This Recommendation specifies the functional architecture of IoT-based energy-saving service for smart buildings. This Recommendation is intended to guide the design, development, implementation, and application of IoT-based energy-saving service for smart buildings

📄 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: Under development

Education Training and Learning

(NEW) ITU-T Y.KHI-PE Key health indicators and evaluation model for power equipment in Smart Sustainable Cities

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18742

ABSTRACT: This Recommendation specifies the evaluation model of key health indicators and implementation methods for smart power equipment. Based on smart power equipment maintenance, operation and environmental information, and characteristic information of the same type of device, a health indicator quantitative evaluation model is established, which includes three steps of parameter type collection, performance / component collection, and comprehensive evaluation. The establishment of the health indicator evaluation model combines the accumulation of experience in equipment maintenance, and the health evaluation driven by intelligent equipment data. For the urban power equipment group, it provides the overall decision-making basis of equipment operation and maintenance and power grid risk management for the power supply management.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

■ Terms and Definitions

Horizontals & Verticals

(NEW) ETSI TR 118 551 V2.0.0 oneM2M API guide

URL: http://www.etsi.org/deliver/etsi_tr/118500_118599/118551/02.00.00_60/tr_118551v020000p.pdf

ABSTRACT: The guide will list the CRUDN messages for managing some of the main resources defined in TS-0001. It aims at providing the description and associated flow in basic examples. It is foreseen to use HTTP binding and JSON serialization as example. Other binding and serialization could be considered later, or in a companion document. It also aims to use this list as a common sets of APIs and extend them to include other APIs (such as 3GPP interworking) so developers will have an option to write applications that can run across different platforms and specific implementations.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2020-11

ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach

 **URL:** http://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr_003680v010101p.pdf

ABSTRACT: Providing guidelines for Security, Privacy and Interoperability in IoT System Definition based on the analysis of representative use cases.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2020-03

(Updated) IETF draft-irtf-t2trg-secure-bootstrapping Terminology and processes for initial security setup of IoT devices

 **URL:** <https://datatracker.ietf.org/doc/draft-irtf-t2trg-secure-bootstrapping/>

ABSTRACT: This document provides an overview of terms that are commonly used when discussing the initial security setup of Internet of Things (IoT) devices. This document also presents a brief but illustrative survey of protocols and standards available for initial security setup of IoT devices.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2024-03

ietf RFC 7228 Terminology for Constrained-Node Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc7228/>

ABSTRACT: This document provides a number of basic terms that have been useful in the standardization work for constrained-node networks.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2014-05

ietf RFC7102 Terms Used in Routing for Low-Power and Lossy Networks

 **URL:** <https://datatracker.ietf.org/doc/rfc7102/>

ABSTRACT: This document provides a glossary of terminology used in routing requirements and solutions for networks referred to as Low-Power and Lossy Networks (LLNs). An LLN is typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links. There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (e.g., heating, ventilation, air conditioning, lighting, access control, fire), connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2014-01

(Updated) ISO/IEC TR 30194 Internet of Things (IoT) and digital twin – Best practices for use case projects - ISO/IEC PWI JTC1-SC41-6 Guidance for IoT and Digital Twin use cases

 **URL:** https://www.iec.ch/dyn/www/f?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104897

ABSTRACT: This document describes best practices for use case projects in terms of characterization, template, plan and 63 maintenance. It is intended to developers of use case projects, including in the context of standardisation. In the latter case, the document can be used to complement existing methodology standards such as IEC 62559

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** Under development

ITU-T Y.4000/Y.2060 (06/2012) Overview of Internet of Things

 **URL:** <https://handle.itu.int/11.1002/1000/11559>

ABSTRACT: This recommendation provides an overview of the Internet of things (IoT). It clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model. The ecosystem and business models are also provided in an informative appendix.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2012-06

(NEW) ITU-T Y.ACC-IoTMV Accessibility requirements for metaverse services supporting IoT

 **URL:** https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19599

ABSTRACT: The virtual world based on real-world data collected through IoT technology and using XR technology as UX is collectively referred to as a metaverse supporting IoT. The metaverse interface should be designed to alleviate difficulties experienced by persons with disabilities and those with specific needs who struggle with certain senses in the real world. This draft Recommendation defines the accessibility requirements that metaverse services supporting IoT should have. Digital twin technology, implemented through data accumulated through the Internet of Things (IoT) based technology, builds an identical virtual world to the real world. The digital twin can be used to digitally implement the geographical and temporal environment of the real world to monitor various information, conduct complex experiments or predict future events. Immersive extended reality (XR) technologies, such as augmented reality (AR), virtual reality (VR), and mixed reality (MR), can be used as a user experience (UX) in this virtual world. The virtual world based on real-world data collected through IoT technology and using XR technology as UX is collectively referred to as a metaverse supporting IoT. The metaverse supporting IoT can provide services in various fields, such as remote medical services, smart factories, smart agriculture, and simulation education.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

oneM2M TS-0011-V4.1.1 Common Terminology

 **URL:** <https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36347>

ABSTRACT: This TS contains a collection of specific technical terms (definitions and abbreviations) used within oneM2M .

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2023-10

Manufacturing

ISO/IEC 20924:2021 RLV Redline version Internet of Things (IoT) - Vocabulary

 **URL:** <https://webstore.iec.ch/publication/68737>

ABSTRACT: ISO/IEC 20924:2021 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. ISO/IEC 20924:2021 (E) provides a definition of Internet of Things along with a set of terms and definitions. This document is a terminology foundation for the Internet of Things.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-03 (Withdrawn)

Mobility

SAE ARINC688 Intersystem Network Integration

 **URL:** <https://www.sae.org/standards/content/arinc688/>

ABSTRACT: The purpose of this document is to provide guidelines for integrating previously standalone cabin systems such as cabin management systems, In-Flight Entertainment (IFE) systems, In-Flight Connectivity (IFC) systems, galley systems, surveillance systems, etc.

Resource sharing between systems can reduce airline costs and/or increase functionality. But, as systems expose their internal resources to external systems, the risk of an intrusion that could degrade function and/or negatively expose the supplier's or airline's brand increases. This document provides a recommended IP networking design framework between aircraft systems to reduce the operational security threats while still supporting the necessary intersystem routing.

 **DOCUMENT TYPE:** Guideline

 **PUBLICATION DATE:** 2021-06

Food and Agriculture

ETSI TR 103 545 SmartM2M; Pilot test definition and guidelines for testing cooperation between oneM2M and Ag equipment standards

 **URL:** http://www.etsi.org/deliver/etsi_tr/103500_103599/103545/01.01.01_60/tr_103545v010101p.pdf

ABSTRACT: The objective of this TR is to provide the necessary input for a Plugtest® event to validate the possible cooperation between the oneM2M platform and AEF ISOBUS standards implemented between a tractor and its implement (an implement is a machine usually trailed behind the tractor and performing a specific agricultural task). The use case would include a tractor entering a road from the fields. The collaboration of Agri IoT and the oneM2M platform would enable to trigger the transmission of an alarm to the cars on the road. ETSI TC ITS standards, such as EN 302 637-3 (Decentralized Environmental Notification Basic Service) are also expected to be part of this cooperation in the use case to be demonstrated.

 **DOCUMENT TYPE:** Technical_Report

 **PUBLICATION DATE:** 2018-08

(NEW) ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security Part 1: Principles and concepts

 **URL:** <https://www.iso.org/standard/71538.html>

ABSTRACT: This document provides the principles, concepts, terms and definitions for health software and health IT systems, key properties of safety, effectiveness and security, across the full life cycle, from concept to decommissioning, as represented in Figure 1. It also identifies the transition points in the life cycle where transfers of responsibility occur, and the types of multi-lateral communication that are necessary at these transition points. This document also establishes a coherent concepts and terminology for other standards that address specific aspects of the safety, effectiveness, and security (including privacy) of health software and health IT systems.

This document is applicable to all parties involved in the health software and health IT systems life cycle including the following:

- a) Organizations, health informatics professionals and clinical leaders designing, developing, integrating, implementing and operating health software and health IT systems – for example health software developers and medical device manufacturers, system integrators, system administrators (including cloud and other IT service providers);
- b) Healthcare service delivery organizations, healthcare providers and others who use health software and health IT systems in providing health services;
- c) Governments, health system funders, monitoring agencies, professional organizations and customers seeking confidence in an organization's ability to consistently provide safe, effective and secure health software, health IT systems and services;
- d) Organizations and interested parties seeking to improve communication in managing safety, effectiveness and security risks through a common understanding of the concepts and terminology used in safety, effectiveness and security management;
- e) Providers of training, assessment or advice in safety, effectiveness and security risk management for health software and health IT systems;
- f) Developers of related safety, effectiveness and security standards.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-03

(NEW) IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

 **URL:** <https://www.iso.org/standard/72026.html>

ABSTRACT: This document specifies general requirements for ORGANIZATIONS in the application of RISK MANAGEMENT before, during and after the connection of a HEALTH IT SYSTEM within a HEALTH IT INFRASTRUCTURE, by addressing the KEY PROPERTIES of SAFETY, EFFECTIVENESS and SECURITY whilst engaging appropriate stakeholders. IEC 80001-1:2021 cancels and replaces the first edition published in 2010. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) structure changed to better align with ISO 31000; b) establishment of requirements for an ORGANIZATION in the application of RISK MANAGEMENT; c) communication of the value, intention and purpose of RISK MANAGEMENT through principles that support preservation of the KEY PROPERTIES during the implementation and use of connected HEALTH SOFTWARE and/or HEALTH IT SYSTEMS.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-09

(NEW) ISO 27269:2021 Health informatics — International patient summary

 **URL:** <https://www.iso.org/standard/79491.html>

ABSTRACT: This document defines the core data set for a patient summary document that supports continuity of care for a person and coordination of their healthcare. It is specifically aimed at supporting the use case' scenario for 'unplanned, cross border care' and is intended to be an international patient summary (IPS). Whilst the data set is minimal and non-exhaustive, it provides a robust, well-defined core set of data items. The tight focus on this use case also enables the IPS to be used in planned care. This means that both unplanned and planned care can be supported by this data set within local and national contexts, thereby increasing its utility and value.

It uses the European Guideline from the eHN as the initial source for the patient summary requirements, then takes into consideration other international patient summary projects to provide an interoperable data set specification that has global application.

This document provides an abstract definition of a Patient Summary from which derived models are implementable. Due to its nature therefore, readers should be aware that the compliance with this document does not imply automatic technical interoperability; this result, enabled by this document, can be reached with the conformity to standards indicated in the associated technical specification and implementation guides.

This document does not cover the workflow processes of data entry, data collection, data summarization, subsequent data presentation, assimilation, or aggregation. Furthermore, this document does not cover the summarization act itself, i.e. the intelligence/skill/competence that results in the data summarization workflow.

It is not an implementation guide that is concerned with the various technical layers beneath the application layer. Implementation guidance for specifically jurisdictional concerns, e.g. Directives, terminologies, formats, etc., an example is specified in the associated Technical Specification.

In particular, representation by various coding schemes, additional structures and terminologies are not part of this document. Terminology and its binding are addressed in Reference. The Identification of Medicinal Products standards (abbreviated to IDMP) are the recommended target for the Medication Summary related to this document but, prior to IDMP's full implementation in practice, this IPS standard cannot insist in its use at this point in time and recognizes that interim schemes might be necessary until IDMP becomes established as a norm.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** 2021-04

(NEW) ISO/DPAS 24305 Health informatics — Guidelines for implementation of HL7 FHIR based on ISO 13940:2015, ISO 13606-1:2019 and ISO 13606-3:2019

 **URL:** <https://www.iso.org/committee/54960.html>

ABSTRACT: This specification provides guidelines for implementation of HL7 FHIR based on ISO 13940:2015, ISO 13606-1:2019 and ISO 13606-3:2019.

 **DOCUMENT TYPE:** Standard_Specification

 **PUBLICATION DATE:** Under development

(NEW) ISO 27799:2016(en) Health informatics — Information security management in health using ISO/IEC 27002

 **URL:** <https://www.iso.org/obp/ui/es/#iso:std:iso:27799:ed-2:v1:en>

ABSTRACT: ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health

information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, but some controls require additional explanation in regard to how they can best be used to protect the confidentiality, integrity and availability of health information. There are also additional health sector specific requirements. This International Standard provides additional guidance in a format that persons responsible for health information security can readily understand and adopt.

In the health domain, it is possible for an organization (a hospital, say) to be certified using ISO/IEC 27001 without requiring certification against or even acknowledgement of ISO 27799. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with ISO 27799 as a stricter standard for healthcare will also become widespread.

🔗 DOCUMENT TYPE: Standard_Specification

📅 PUBLICATION DATE: 2016-08

■ Annex

Title	Date	Weblink
3GPP TR 36.763 V17.0.0 Study on Narrow-Band Internet of Things (NB-IoT) / enhanced Machine Type Communication (eMTC) support for Non-Terrestrial Networks (NTN)	2021-06	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3747
3GPP TR 36.763 V17.0.0 Study on Narrow-Band Internet of Things (NB-IoT) / enhanced Machine Type Communication (eMTC) support for Non-Terrestrial Networks (NTN)	2021-06	https://www.3gpp.org/news-events/1805-iot_r14
3GPP TR 36.802 V13.0.0 Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IOT; Technical Report for BS and UE radio transmission and reception	2016-06	https://www.3gpp.org/ftp/Specs/archive/36_series/36.802/
3GPP TR 38.825 V16.0.0 Study on NR industrial Internet of Things (IoT)	2019-03	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3492
(NEW) 3GPP TR 22.840 V19.0.0 Study on Ambient power-enabled Internet of Things (Release 19)	2023-12	https://www.3gpp.org/ftp/Specs/archive/22_series/22.840/
(NEW) 3GPP TR 22.865 V19.2.0 Study on satellite access Phase 3; (Release 19)	2023-12	https://www.3gpp.org/ftp/Specs/archive/22_series/22.865/22865-j20.zip
(NEW) 3GPP TR 22.867 V18.2.0 Study on 5G Smart Energy and Infrastructure (Release 18)	2021-12	https://www.3gpp.org/ftp/Specs/archive/22_series/22.867/22867-i20.zip
(NEW) 3GPP TR 23.776 V17.0.0 Study on architecture enhancements for 3GPP support of advanced Vehicle-to-Everything (V2X) services; Phase 2; (Release 17)	2021-03	https://www.3gpp.org/ftp/Specs/archive/23_series/23.776/23776-h00.zip
(NEW) 3GPP TR 28.841 V18.0.1 Study on management aspects of Internet of Things (IoT) Non-Terrestrial Networks (NTN) enhancements (Release 18)	2023-06	https://www.3gpp.org/ftp/Specs/archive/28_series/28.841/28841-i01.zip
(NEW) 3GPP TS 23.542 V18.4.0 Application layer support for Personal IoT Network;	2024-06	https://www.3gpp.org/DynaReport/23542.htm
(NEW) 3GPP TS 23.433 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications (Release 19)	2024-09	https://www.3gpp.org/ftp/Specs/archive/23_series/23.433/23433-j30.zip
(NEW) 3GPP TS 23.434 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL);	2024-09	https://www.3gpp.org/ftp/Specs/archive/23_series/23.434/23434-j30.zip
Functional architecture and information flows; (release 19)	2024-09	https://www.3gpp.org/ftp/Specs/archive/23_series/23.434/23434-j30.zip

Title	Date	Weblink
5G PPP 5G PPP H2020 ICT-18-2018 5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors - Challenges and Opportunities	2020-10	https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf
5GAA Tele-operated Driving Use Cases, System Architecture and Business Considerations	2021-12	https://5gaa.org/news/tele-operated-driving-use-cases-system-architecture-and-business-considerations/
(NEW) 5GAA 5G-V2X Direct Communication Evaluation Approach: An Automotive Analysis	2024--07	https://5gaa.org/content/uploads/2024/07/5gaa-wi-nr-v2x-eval.pdf
(NEW) 5GAA Vehicle-to-Network-to-Everything (V2N2X) Communications: Architecture, Solution Blueprint, and Use Case Implementation Examples	2024-05	https://5gaa.org/content/uploads/2024/06/v2n2x-communications-architecture-solution-blueprint-and-use-case-implementation.pdf
(NEW) 5GAA Creating Trust in Connected and Automated Vehicles	2024-05	https://5gaa.org/content/uploads/2024/05/5gaa-trust4auto-white-paper-2024.pdf
(NEW) 5GAA Trustable Position Metrics for V2X Applications	2023-10	https://5gaa.org/content/uploads/2023/10/5gaa-a-220044-tpm-4v2x-tr-1.pdf
(NEW) 5GAA Accelerating 5G Adoption for Connected and Autonomous Mobility Services	2023-04	https://5gaa.org/content/uploads/2023/04/5gaa-wp-market-pull-mapu.pdf
(NEW) 5GAA C-V2X Use Cases and Service Level Requirements — Volume III	2023-01	https://5gaa.org/content/uploads/2023/01/5gaa-tr-c-v2x-use-cases-and-service-level-requirements-vol-iii.pdf
(Updated) AII Industrial Internet Architecture	2016-12	https://www.aii-alliance.org/en/c289/n3074.html
AIOTI Application-Centric Security, Privacy & Trust in IoT	2019-06	https://aioti.eu/wp-content/uploads/2019/06/Webinar_Nr1_ApplicationCentric_SecurityPrivacyTrustInIoT_ArthursLegal_v2019.1_vPresented.pdf
AIOTI Computing Continuum Scenarios, Requirements and Optical Communication enablers	2022-04	https://aioti.eu/wp-content/uploads/2022/04/AIOTI-Computing-Continuum-Final.pdf
AIOTI High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0	2020-01	https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf
AIOTI Identifiers in Internet of Things (IoT)	2018-02	https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1.0.pdf.pdf
(Updated) AIOTI IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges, Release 3.0	2023-11	https://aioti.eu/wp-content/uploads/2023/11/AIOTI-Report-IoT-and-Edge-impact-on-Beyond-5G-R3-Final.pdf

Title	Date	Weblink
AIOTI IoT High-Level Architecture (HLA) Release 5.0	2020-12	https://aioti.eu/wp-content/uploads/2020/12/AIOTI_HLA_R5_201221_Published.pdf
(Updated) AIOTI IoT LSP Standard Framework Concepts Release 3.0	2023-02	https://aioti.eu/wp-content/uploads/2023/01/AIOTI-SDOs-Alliance-Landscape-IoT-LSP-standards-framework-R3-Final.pdf
AIOTI Ontology Landscape	2021-12	https://aioti.eu/wp-content/uploads/2022/02/AIOTI-Ontology-Landscape-Report-R1-Published-1.0.1.pdf
AIOTI Semantic IoT Solutions - A Developer Perspective	2019-10	https://www.researchgate.net/publication/336679022_Semantic_IoT_Solutions_-_A_Developer_Perspective
AIOTI Towards semantic interoperability standards based on ontologies	2019-10	https://www.researchgate.net/publication/336677616_Towards_Semantic_Interoperability_Standards_based_on_Ontologies
(New) AIOTI IoT and Edge Computing EU funded projects landscape, Release 2.0	2023-12	https://aioti.eu/wp-content/uploads/2023/12/AIOTI-Report-EU-funded-research-projects-landscape-IoT-and-Edge-computing-R2-Final.pdf
(NEW) AIOTI Computing Continuum Scenarios, Proof of Concepts, Requirements and Optical Communication enablers, Release 2.0	2024-05	https://aioti.eu/wp-content/uploads/AIOTI-Computing-Continuum-Report-R2-Final.pdf
(NEW) AIOTI High Priority IoT Standardisation Gaps and Relevant SDOs Release 3.0	2024-01	https://aioti.eu/wp-content/uploads/2024/01/AIOTI-High-Priority-IoT-Gaps-R3-Final.pdf
(NEW) AIOTI Guidance for the Integration of IoT and Edge Computing in Data Spaces	2022-09	https://aioti.eu/wp-content/uploads/2022/09/AIOTI-Guidance-for-IoT-Integration-in-Data-Spaces-Final.pdf
(NEW) AIOTI Ontology Landscape Portfolio - Catalogue of Ontologies for Semantic Interoperability	N/A	https://aiotieugithub.io/ontology-landscape/
ASTM ASTM F3463-21 Standard Guide for Ensuring the Safety of Connected Consumer Products	2021-10	https://www.astm.org/f3463-21.html
bioTope D2.7 V2.0 bioTope SoS Reference Platform Specification	2018-03	https://storage.ning.com/topology/rest/1.0/file/get/35619929?profile=original
bioTope D3.3 V1.0 Context-Sensitive Security, Privacy Management, Adaptation Framework	2017-03	https://st11.ning.com/topology/rest/1.0/file/get/1065330?profile=original
bioTope D3.5 Prototype of Platform Integration using API Mediators	2017-06	https://st11.ning.com/topology/rest/1.0/file/get/1065014?profile=original
bioTope D3.6 V2.0 Information Source Publication and Consumption Framework	2018-01	https://storage.ning.com/topology/rest/1.0/file/get/35619932?profile=original

Title	Date	Weblink
bioTope D5.2 V1.0 Service Composition Framework	2017-01	https://storage.ning.com/topology/rest/1.0/file/get/1064994?profile=original
bioTope D5.5 V2.0 Service Composition Framework	2017-12	https://storage.ning.com/topology/rest/1.0/file/get/35619974?profile=original
bioTope D6.4 V1.0 Proof-of-Concept "Greater Lyon Pilot" Implementation	2018-01	https://storage.ning.com/topology/rest/1.0/file/get/35619978?profile=original
bioTope D6.5 V1.0 Proof-of-Concept "Brussels-Capital Region Pilot" Implementation	2018-02	https://storage.ning.com/topology/rest/1.0/file/get/35619888?profile=original
bioTope D6.6 V1.0 Proof-of-Concept "Helsinki Pilot" Implementation	2018-02	https://storage.ning.com/topology/rest/1.0/file/get/35619980?profile=original
C2C-CC C2CCC_RS_2035 Objectives	2021-12	https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2035_Objectives.pdf
C2C-CC C2CCC_RS_2036 Features	2021-12	https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2036_Features.pdf
C2C-CC C2CCC_RS_2037 Vehicle C-ITS station profile	2021-12	https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_RS_2037_Profile.pdf
C2C-CC C2CCC_TR_2000 C2CCC_TR_2000_ReleaseOverview - Basic System Profile Release Overview, Release 1.6.1	2021-12	https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.1/C2CCC_TR_2000_ReleaseOverview.pdf
CEN Wireless mesh networking - Communication systems for meter data exchange	N/A	https://standards.iteh.ai/catalog/tc/cen/a0640f96-2f0c-4456-af8e-20887cd8b203/cen-tc-294-wg-6
CEN EN 13757-1 Communication systems for meters - Part 1: Data exchange	2021-12	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::F-SP_PROJECT,FSP_ORG_ID:65216,6275&cs=1520E24EB7BA8E-7321D0D175C7F1CF004
CEN EN 13757-2 Communication systems for meters - Part 2: Wired M-Bus communication	2018-10	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::F-SP_PROJECT,FSP_ORG_ID:61821,6275&cs=148E2A-53815B1043A00AB94D1340B84A1
CEN EN 13757-2:2018/prA1 Communication systems for meters - Part 2: Wired M-Bus communication	Under development - Last accessed month: 2025-02	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::FSP_PROJECT,F-SP_LANG_ID:74544,25&cs=1761F-4D6E55C0F87848EB2822BAF9FAAF
CEN EN 13757-3:2018 Communication systems for meters - Part 3: Application protocols	2018-10	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::FSP_PROJECT:61820&cs=1699FDB9F0D-54F7BB01D7266589ED286A

Title	Date	Weblink
CEN EN 13757-4:2019 Communication systems for meters - Part 4: Wireless M-Bus communication	2019-11	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60262&cs=156CDF6A723103E-3251766A06586779B6
CEN EN 13757-5 Communication systems for meters - Part 5: Wireless M-Bus relaying	2016-05	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT:FSP_ORG_ID:36150.6275&cs=1B-9B9291A8674B58CF7FF96F8B-88F5B85
CEN EN 13757-6:2015 Communication systems for meters - Part 6: Local Bus	2016-06	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:41515&cs=14E87496D-5D72D87C65ABEBFFCB3BD0AB
CEN EN 13757-7:2018 Communication systems for meters - Part 7: Transport and security services	2018-10	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:61822&cs=107399C785EC0B2E-DACF60D74955A90D5
CEN EN 1434-3:2015 Heat meters - Part 3: Data exchange and interfaces	2016-06	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41516&cs=157EF44C329D0AD-E1DB97DF0406BAA443
CEN EN 16157-1:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 1: Context and framework	2018-12	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:62523&cs=15997C7B-B19A97A296D8A7719196409AD
CEN EN 16157-2:2019 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 2: Location referencing	2019-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60747&cs=1C3A140087AD1F-DE865115EA876607C93
CEN EN 16157-3:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 3: Situation Publication	2018-12	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:60748&cs=13B159A7784936BD-C97A42AFA8C2121A
CEN EN 16157-4:2021 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 4: VMS publication	2021-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:68227&cs=19CD8A5DF-8D8A747A2648590BAC670053
CEN EN 16157-5:2020 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 5: Measured and elaborated data publications	2020-08	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68225&cs=15C7361EFFD209F-F289AF2AAE0FBC17A1
CEN EN 16157-7:2018 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 7: Common data elements	2018-12	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:62524&cs=14AD3F-DA01670AAB7137D7857613CB12B

Title	Date	Weblink
CEN EN 16836-1 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 1: Introduction and standardization framework	2017-05	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::F-SP_PROJECT,FSP_ORG_ID:41098,6275&cs=11019F-C07793E83E7C3B39E9E3A6DBF78
CEN EN 16836-2:2016 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 2: Networking layer and stack specification	2017-05	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:41099&cs=181323929D-1945B365914E7CE01F502AD
CEN EN 16836-3:2016 Communication systems for meters - Wireless mesh networking for meter data exchange - Part 3: Energy profile specification dedicated application layer	2017-05	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:41100&cs=1C46CE950442B-0C43F9EDDAC4585ACF19
CEN EN ISO 14814:2006 Road transport and traffic telematics - Automatic vehicle and equipment identification - Reference architecture and terminology (ISO 14814:2006)	2006-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:21173&cs=184DD778D0F4ED-9BEEC2F72C92F3FFFB1
(Updated) CEN CEN/TS 16157-6 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 6: Parking publications	2022-10	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT,FSP_LANG_ID:69724,25&cs=1451A03D-2D2D1D87355F1559FEB7FA425
(Updated) CEN ISO/TS 17425:2016 Intelligent transport systems - Cooperative systems - Data exchange specification for in-vehicle presentation of external road and traffic related data	2016-06	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:35914&cs=10C18F278124980B-9F4075E355AB45BC3
(Updated) CEN ISO/TS 17429:2017 Intelligent transport systems - Cooperative ITS - ITS station facilities for the transfer of information between ITS stations	2017-04	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:35915&cs=1DF674B-52BAF01613F1CDAABBB1D408E6
(Updated) CEN ISO/TS 19091:2019 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections	2019-07	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT:64994&cs=155A0F-218787309EC4D33F96797394306
CEN ISO/TS 19321:2020 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures	2020-10	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68350&cs=1FE9288D0BD-55B9A6A45F662E5E523F64
(Updated) CEN ISO/TS 19321:2020 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures	2020-10	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68350&cs=1FE9288D0BD-55B9A6A45F662E5E523F65

Title	Date	Weblink
CEN ISO/TS 19468:2022 Intelligent transport systems - Data interfaces between centres for transport information and control systems - Platform-independent model specifications for data exchange protocols for transport information and control systems	2022-02	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71962&cs=18889333092F-F2E127C49B472E09BA2FB
(Updated) CEN prCEN ISO/TS 19321 rev Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures	2024-07	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT.FSP_LANG_ID:73937,25&cs=108B9C05FB-54333B566ACFD5122C7E1F9
CEN prEN 13757-8 Communication systems for meters - Part 8: Adaptation layer	Under development - Last accessed month: 2025-02	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT.FSP_LANG_ID:73097,25&cs=19B-94878D7D6F98142DFDE0433C-C7D3C1
(Updated) CEN prEN 14154-4:2023 Water meters — Part 4: Additional functionalities	2023-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT.FSP_LANG_ID:73396,25&cs=-1DA0D2906520CD899CB94F5BB-61C72E7F
CEN/CENELEC CWA 17431 Principles and guidance for licensing Standard Essential Patents in 5G and the Internet of Things (IoT), including the Industrial Internet	2019-06	https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa17431.pdf
CEN/TR 17167:2018 Communication system for meters - Accompanying TR to EN 13757-2,-3 and -7, Examples and supplementary information	2018-04	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:61828&cs=1338F0A4C-7239D0EC0470C6E1605E2BCF
CEN/TS 16157-10:2022 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 10: Energy infrastructure publications	2022-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71189&cs=17CE8E7FC-7390CF7CC48C34700D0A825D
CEN/TS 16157-11 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 11: Publication of machine interpretable traffic regulations	2022-03	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:71777&cs=10465408B33310E1C-137C3B2AABC7EE51
CEN/TS 16157-12 Intelligent transport systems — DATEX II management and information — Part 12: Facilities publications	2022-05	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT.FSP_LANG_ID:73025,25&cs=191FBA7A-8FAE57738466F76A27106F67D
CEN/TS 16157-8 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 8: Traffic management publications and extensions dedicated to the urban environment	2020-04	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68653&cs=18BC2B0B-4960475D11D2ABEA1D8C23A2D

Title	Date	Weblink
CEN/TS 16157-9 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information - Part 9: Traffic signal management publications dedicated to the urban environment	2020-04	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:68652&cs=18B5180A209437720996363BB8237DDAC
CEN/TS 16614-1:2020 Public transport - Network and Timetable Exchange (NeTex) - Part 1: Public transport network topology exchange format	2020-04	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:66892&cs=1CAED5ABB-1179CBAE5D7E61C865704C55
CENELEC CLC/prTS 50491-7 Home and Building Electronic Systems - IT security and data protection - User Guide	Under development - Last accessed month: 2025-02	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT:F-SP_LANG_ID:75291,25&cs=1AC4B-90B75A5026B198062B2BBB1F96BE
CENELEC EN 17529:2022 Cybersecurity and Data Protection	2022-05	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::F-SP_PROJECT,FSP_ORG_ID:63633,2307986&cs=-11F702120AA40D5C-C2DD42848140B1806
CENELEC EN 50090 (ISO 14543) Home and Building Electronic Systems (HBES)	2012-02	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::F-SP_PROJECT,FSP_ORG
CENELEC prEN 17640 Fixed time cybersecurity evaluation methodology for ICT products	Under development - Last accessed month: 2025-02	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT,FSP_LANG_ID:70971,25&cs=16CB6A9987F-11452CBD61C83CAD57215B
(Updated) CENELEC EN 50090-6-3:2023 Home and Building Electronic Systems (HBES)- Part 6-3 -3rd Party HBES IoT API	2023-07	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::F-SP_PROJECT,FSP_LANG_ID:74475,25&cs=1046EE8EC4361FAC-C3F6370EBB7B68089
(Updated) CENELEC prEN IEC 63345 Energy Efficiency Systems - Simple External Consumer Display	2023-10	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:74332,25&cs=10C-4D76ADB0C4C7D5B9DA81FF-8E547C2D
CENELEC prEN IEC 63402 Energy Efficiency Systems - Smart Grid - Customer Energy Management Systems - General Requirements and Architecture	Under development - Last accessed month: 2025-02	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::F-SP_PROJECT,FSP_LANG_ID:74575,25&cs=167DD57F4AA-099C41201ADC1979F157B2
(Updated) CEN EN 17927:2023 Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.	2023-11	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::F-SP_PROJECT,FSP_LANG_ID:74909,25&cs=157BB6AD851BD-6F80A208FE00FBBDB6B8DD
(Updated) Contiki-NG, the OS for Next Generation IoT Devices	2024-09	https://www.contiki-ng.org/
CSA ZigBee Document 13-0402-14 Base Device Behaviour Specification - ZigBee Document 13-0402-14	2016-02	https://csa-iot.org/developer-resource/specifications-download-request/

Title	Date	Weblink
CSA-IOT Zigbee Document 05-3474-22 Zigbee Specification	2017-04	https://csa-iot.org/developer-resource/specifications-download-request/
CSA-IOT Zigbee Document 075123 Cluster Library Specification	2019-12	https://csa-iot.org/developer-resource/specifications-download-request/
CSA-IOT Zigbee Document 07-5356-21 Zigbee Smart Energy Standard	2017-06	https://csa-iot.org/developer-resource/specifications-download-request/
CSA-IOT Zigbee Document 14-0563-18 Zigbee PRO Green Power feature specification Basic functionality set V1.1.1	2019-11	https://csa-iot.org/developer-resource/specifications-download-request/
CSA-IOT ZigBee Document 15-0014-05 ZigBee Lighting & Occupancy Device Specification	2016-02	https://csa-iot.org/developer-resource/specifications-download-request/
DIN/DKE DIN SPEC 16593-1 Reference Model for Industry 4.0 Service Architectures - Part 1: Basic Concepts of an Interaction-based Architecture	2018-04	www.beuth.de/de/technische-regel/din-spec-16593-1/287632675
Eclipse Foundation Eclipse IoT-Testware	N/A	https://projects.eclipse.org/projects/technology.iottestware
ECSO System security and certification considerations	2022-01	https://www.youtube.com/watch?v=mXiytFIOXeI
EEBUS SHIP (Smart Home IP) and SPINE (Smart Premises Interoperable Neutral Message Exchange)	N/A	https://www.eebus.org/media-downloads/
Energetics ETP v1.2 Energetics Transfer Protocol (ETP) v1.2 (2021)	2021-09	https://www.energistcs.org/energistcs-releases-v1-2-of-energistcs-transfer-protocol/
ENISA Baseline Security Recommendations for IoT	2017-11	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
ENISA Good practices for IoT and Smart Infrastructures Tool	N/A	https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool
ENISA IoT Security Standards Gap Analysis	2019-01	https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis
(Updated) ETSI TR 103 946 V1.1.1 (2023-10) Methods for Testing and Specification (MTS); Security validation of IoT architecture application and conformity Case Study Experiences	2023-10	https://www.etsi.org/deliver/etsi_tr/103900_103999/103946/01.01.01_60/tr_103946v010101p.pdf
ETSI EG 202 798 ITS; Testing; Framework for conformance and interoperability testing	2011-01	http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/01.01.01_60/eg_202798v010101p.pdf
ETSI EN 300 175-1 Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview	2022-03	http://www.etsi.org/deliver/etsi_en/300100_300199/30017501/02.09.01_60/en_30017501v020901p.pdf

Title	Date	Weblink
ETSI EN 302 065-1 Short Range Devices (SRD) using Ultra Wide Band technology (UWB); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Requirements for Generic UWB applications	2016-11	http://www.etsi.org/deliver/etsi_en/302000_302099/30206501/02.01.01_60/en_30206501v020101p.pdf
ETSI EN 302 636-1 ITS; Vehicular Communications; GeoNetworking; Part 1: Requirements	2014-04	http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf
ETSI EN 302 637-2 ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	2019-04	http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf
ETSI EN 302 637-3 ITS; Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	2019-04	http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.03.01_60/en_30263703v010301p.pdf
ETSI EN 302 663 ITS; ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	2020-01	http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf
ETSI EN 302 665 ITS; Communications Architecture	2010-09	http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf
ETSI EN 303 613 ITS; LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	2020-01	http://www.etsi.org/deliver/etsi_en/303600_303699/303613/01.01.01_60/en_303613v010101p.pdf
(Updated) ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	2024-09	http://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
ETSI GR CIM 011 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)	2021-04	https://www.etsi.org/deliver/etsi_gr/CIM/001_099/011/01.01.01_60/gr_CIM-011v010101p.pdf
ETSI GR IP6 001 IPv6 Deployment in the Enterprise	2017-06	https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_IP-6001v010101p.pdf
ETSI GR IP6 008 IPv6-based Internet of Things Deployment of IPv6-based Internet of Things	2017-06	https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_IP-6008v010101p.pdf
ETSI GS CIM 016 Context Information Management (CIM); NGSI-LD Testing Framework: Test Template	2021-04	https://www.etsi.org/deliver/etsi_gs/CIM/001_099/016/01.01.01_60/gs_CIM-016v010101p.pdf
ETSI GS LTN 002 Low Throughput Networks (LTN) - Functional Architecture	2014-09	https://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN-002v010101p.pdf
ETSI GS LTN 003 Low Throughput Networks (LTN) - Protocols and Interfaces	2014-09	https://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN-003v010101p.pdf

Title	Date	Weblink
ETSI GS NGP 005 Next Generation Protocol Requirements	2017-04	https://www.etsi.org/deliver/etsi_gs/NGP/001_099/005/01.01.01_60/gs_NG-P005v010101p.pdf
ETSI SAREF ontology SAREF: the Smart Applications REference ontology	2020-02	https://saref.etsi.org/core/
ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach	2020-03	http://www.etsi.org/deliver/etsi_sr/03600_003699/003680/01.01.01_60/sr_003680v010101p.pdf
ETSI SR 003 809 eHEALTH; The role of ICT to enable Health crisis management and recovery; Responding to the 2019 SARS-CoV-2 Pandemic	2021-12	https://www.etsi.org/deliver/etsi_sr/03800_003899/003809/01.01.02_60/sr_003809v010102p.pdf
ETSI TR 101 607 ITS; Cooperative ITS (C-ITS); Release 1	2020-02	http://www.etsi.org/deliver/etsi_tr/101600_101699/101607/01.02.01_60/tr_101607v010201p.pdf
(Updated) ETSI TR 102 638 ITS; Vehicular Communications; Basic Set of Applications; Release 2	2024-04	https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/02.01.01_60/tr_102638v020101p.pdf
ETSI TR 103 249 Low Throughput Network (LTN); Use Cases and System Characteristics	2017-10	http://www.etsi.org/deliver/etsi_tr/103200_103299/103249/01.01.01_60/tr_103249v010101p.pdf
ETSI TR 103 290 Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment	2015-04	http://www.etsi.org/deliver/etsi_tr/103200_103299/103290/01.01.01_60/tr_103290v010101p.pdf
ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions	2016-10	http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf
ETSI TR 103 376 SmartM2M; IoT LSP use cases and standards gaps	2016-10	http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf
ETSI TR 103 394 Smart Body Area Networks (SmartBAN); System Description	2018-01	http://www.etsi.org/deliver/etsi_tr/103300_103399/103394/01.01.01_60/tr_103394v010101p.pdf
ETSI TR 103 467 Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem	2018-06	https://www.etsi.org/deliver/etsi_tr/103400_103499/103467/01.01.01_60/tr_103467v010101p.pdf
ETSI TR 103 514 DECT; DECT-2020 New Radio (NR) interface; Study on Physical (PHY) layer	2018-07	https://www.standict.eu/sites/default/files/2021-01/tr_103514v010101p.pdf
ETSI TR 103 515 DECT; Study on URLLC use cases of vertical industries for DECT evolution and DECT-2020	2018-03	https://www.etsi.org/deliver/etsi_tr/103500_103599/103515/01.01.01_60/tr_103515v010101p.pdf
ETSI TR 103 527 SmartM2M; Virtualized IoT Architectures with Cloud Back-ends	2018-07	http://www.etsi.org/deliver/etsi_tr/103500_103599/103527/01.01.01_60/tr_103527v010101p.pdf

Title	Date	Weblink
ETSI TR 103 528 SmartM2M; Landscape for open source and standards for cloud native software applicable for a Virtualized IoT service layer	2018-08	http://www.etsi.org/deliver/etsi_tr/103500_103599/103528/01.01.01_60/tr_103528v010101p.pdf
ETSI TR 103 533 Security; Standards Landscape and best practices	2019-08	https://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr_103533v010101p.pdf
ETSI TR 103 534-1 Teaching Material: Part 1 (Security)	2019-08	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf
ETSI TR 103 534-2 Teaching Material: Part 2 (Privacy)	2019-10	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf
ETSI TR 103 535 Guidelines for semantic interoperability in the industry	2019-10	https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf
ETSI TR 103 536 Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms	2019-12	https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf
ETSI TR 103 537 Plugtests™ preparation on Semantic Interoperability	2019-09	https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf
ETSI TR 103 545 SmartM2M; Pilot test definition and guidelines for testing cooperation between oneM2M and Ag equipment standards	2018-08	http://www.etsi.org/deliver/etsi_tr/103500_103599/103545/01.01.01_60/tr_103545v010101p.pdf
ETSI TR 103 582 EMTel; Study of use cases and communications involving IoT devices in provision of emergency situations	2019-07	https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf
ETSI TR 103 591 Privacy study report; Standards Landscape and best practices	2019-10	https://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf
ETSI TR 103 674 SmartM2M; Artificial Intelligence and the oneM2M architecture	2021-02	http://www.etsi.org/deliver/etsi_tr/103600_103699/103674/01.01.01_60/tr_103674v010101p.pdf
ETSI TR 103 714 SmartM2M; Study for oneM2M; Discovery and Query use cases and requirements	2020-07	http://www.etsi.org/deliver/etsi_tr/103700_103799/103714/01.01.01_60/tr_103714v010101p.pdf
ETSI TR 103 717 SmartM2M; Study for oneM2M; Discovery and Query specification development	2021-07	http://www.etsi.org/deliver/etsi_tr/103700_103799/103717/01.01.01_60/tr_103717v010101p.pdf
ETSI TR 103 751 Smart Body Area Networks (SmartBAN); Implant communications	2021-04	http://www.etsi.org/deliver/etsi_tr/103700_103799/103751/01.01.01_60/tr_103751v010101p.pdf
ETSI TR 103 778 SmartM2M; Use cases for cross-domain data usability of IoT devices	2021-12	http://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf

Title	Date	Weblink
ETSI TR 103 783 SmartM2M; SAREF: SDT interoperability and oneM2M base ontology alignment	2022-05	https://www.etsi.org/deliver/etsi_tr/103700_103799/103783/01.01.01_60/tr_103783v010101p.pdf
ETSI TR 118 503 V1.0.0 Architecture Part 2: Study for the merging of architectures proposed for consideration	2015-04	https://2020.standict.eu/sites/default/files/tr_118503v010000p.pdf
(Updated) ETSI TS 102 731 ITS; Security; Security Services and Architecture	2022-11	https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/02.00.00_60/ts_102731v020000p.pdf
(Updated) ETSI TS 102 894-2 ITS; Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	2023-10	https://www.etsi.org/deliver/etsi_ts/102800_102899/102894/02/02.02.01_60/ts_10289402v020201p.pdf
ETSI TS 102 939-1 DECT; Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1)	2017-10	https://www.etsi.org/deliver/etsi_ts/102900_102999/102939/01/01.03.01_60/ts_10293901v010301p.pdf
(Updated) ETSI TS 102 940 ITS; Security; ITS communications security architecture and security management	2021-07	https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf
ETSI TS 103 246-1 Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 1: Functional requirements	2020-10	http://www.etsi.org/deliver/etsi_ts/103200_103299/103246/01/01.03.01_60/ts_10324601v010301p.pdf
(Updated) ETSI TS 103 264 V3.2.1 SAREF ontology SAREF: the Smart Applications REference ontology and oneM2M Mapping	2024-01	https://www.etsi.org/deliver/etsi_ts/103200_103299/103264/03.02.01_60/ts_103264v030201p.pdf
ETSI TS 103 267 SmartM2M; Smart Applications; Communication Framework	2020-02	http://www.etsi.org/deliver/etsi_ts/103200_103299/103267/02.01.01_60/ts_103267v020101p.pdf
(Updated) ETSI TS 103 300-3 ITS; Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2	2023-02	https://www.etsi.org/deliver/etsi_ts/103300_103399/103300/03/02.02.01_60/ts_10330003v020201p.pdf
(Updated) ETSI TS 103 301 ITS; Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	2021-03	http://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01.03.01_60/ts_103301v010301p.pdf
(Updated) ETSI TS 103 325 Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN	2022-07	https://www.etsi.org/deliver/etsi_ts/103300_103399/103325/01.02.01_60/ts_103325v010201p.pdf
ETSI TS 103 326 Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer	2021-07	http://www.etsi.org/deliver/etsi_ts/103300_103399/103326/01.02.01_60/ts_103326v010201p.pdf
ETSI TS 103 327 Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management	2019-04	http://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327v010101p.pdf

Title	Date	Weblink
ETSI TS 103 357 Short Range Devices; Low Throughput Networks (LTN); Protocols for radio interface A	2018-06	http://www.etsi.org/deliver/etsi_ts/103300_103399/103357/01.01.01_60/ts_103357v010101p.pdf
ETSI TS 103 358 Short range devices; Low Throughput Networks (LTN) Architecture; LTN Architecture	2018-06	http://www.etsi.org/deliver/etsi_ts/103300_103399/103358/01.01.01_60/ts_103358v010101p.pdf
ETSI TS 103 378 Smart Body Area Networks (SmartBAN) Unified data representation formats, semantic and open data model	2015-12	http://www.etsi.org/deliver/etsi_ts/103300_103399/103378/01.01.01_60/ts_103378v010101p.pdf
(Updated) ETSI TS 103 410-1 V1.2.1 SmartM2M; Extension to SAREF; Part 1: Energy Domain	2023-11	https://www.etsi.org/deliver/etsi_ts/103400_103499/10341001/01.02.01_60/ts_10341001v010201p.pdf
ETSI TS 103 424 Publicly Available Specification (PAS); Smart Machine-to-Machine communications (SmartM2M)	2016-11	http://www.etsi.org/deliver/etsi_tr/103500_103599/103527/01.01.01_60/tr_103527v010101p.pdf
ETSI TS 103 544-1 Publicly Available Specification (PAS); ITS; MirrorLink; Part 1: Connectivity	2019-10	http://www.etsi.org/deliver/etsi_ts/103500_103599/10354401/01.03.01_60/ts_10354401v010301p.pdf
ETSI TS 103 596-1 V1.1.1 (Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 1: Conformance Tests	2021-05	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359601/01.01.01_60/ts_10359601v010101p.pdf
ETSI TS 103 596-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 2: Security Tests	2021-05	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359602/01.01.01_60/ts_10359602v010101p.pdf
ETSI TS 103 596-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 3: Performance Tests	2021-05	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359603/01.01.01_60/ts_10359603v010101p.pdf
ETSI TS 103 597-1 V1.1.2 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 1: Conformance Tests	2021-01	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359701/01.01.02_60/ts_10359701v010102p.pdf
ETSI TS 103 597-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 2: Security Tests	2021-04	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359702/01.01.01_60/ts_10359702v010101p.pdf
ETSI TS 103 597-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 3: Performance Tests	2021-01	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359703/01.01.01_60/ts_10359703v010101p.pdf
ETSI TS 103 646 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for foundational Security IoT-Profile	2021-01	https://www.etsi.org/deliver/etsi_ts/103600_103699/103646/01.01.01_60/ts_103646v010101p.pdf
ETSI TS 103 673 SmartM2M; SAREF Development Framework and Workflow, Streamlining the Development of SAREF and its Extensions	2020-08	http://www.etsi.org/deliver/etsi_ts/103600_103699/103673/01.01.01_60/ts_103673v010101p.pdf

Title	Date	Weblink
ETSI TS 103 701 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	2021-08	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
ETSI TS 103 735 SmartM2M; Smart Lifts IoT System	2021-07	http://www.etsi.org/deliver/etsi_ts/103700_103799/103735/01.01.02_60/ts_103735v010102p.pdf
ETSI TS 103 757 SmartM2M; Asynchronous Contact Tracing System; Fighting pandemic disease with Internet of Things (IoT)	2021-08	http://www.etsi.org/deliver/etsi_ts/103700_103799/103757/02.01.01_60/ts_103757v020101p.pdf
ETSI TS 103 779 SmartM2M; Requirements and Guidelines for cross-domain data usability of IoT devices	2022-05	https://www.etsi.org/deliver/etsi_ts/103700_103799/103779/01.01.01_60/ts_103779v010101p.pdf
(Updated) ETSI TS 103 780 SmartM2M; SAREF: oneM2M usage guidelines	2022-08	https://www.etsi.org/deliver/etsi_ts/103700_103799/103780/01.01.01_60/ts_103780v010101p.pdf
ETSI TS 103 849 Smart M2M; Smart Escalators IoT System	2022-08	https://www.etsi.org/deliver/etsi_ts/103700_103799/103735/01.01.01_60/ts_103735v010101p.pdf
(NEW) ETSI TS 103 849 Smart M2M; Smart Escalators IoT System	2022-08	https://www.etsi.org/deliver/etsi_ts/103800_103899/103849/01.01.01_60/ts_103849v010101p.pdf
(NEW) ETSI GS MEC 033 V3.1.1 Multi-access Edge Computing (MEC); IoT API	2022-12	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/033/03.01.01_60/gs_MEC033v030101p.pdf
(NEW) ETSI/oneM2M TR 118 551 V2.0.0 oneM2M API guide	2020-11	http://www.etsi.org/deliver/etsi_tr/118500_118599/118551/02.00.00_60/tr_118551v020000p.pdf
(NEW) ETSI TR 103 675 AI for IoT: A Proof of Concept	2020-12	http://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf
(NEW) ETSI/oneM2M TR 118 518 V2.5.1 Industrial Domain Enablement	2020-07	www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.05.01_60/tr_118518v020501p.pdf
(NEW) ETSI TS 103 701 V1.1.1 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	2019-02	http://www.etsi.org/deliver/etsi_tr/103400_103499/103438/01.01.01_60/tr_103438v010101p.pdf
(NEW) ETSI/oneM2M TR 103 716 V1.1.1 oneM2M Discovery and Query solution(s) simulation and performance evaluation	2021-04	http://www.etsi.org/deliver/etsi_tr/103700_103799/103716/01.01.01_60/tr_103716v010101p.pdf
(NEW) ETSI TR 103 621 V1.2.1 Guide to Cyber Security for Consumer Internet of Things	2022-09	http://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf
(NEW) ETSI/oneM2M TR 118 567 V4.0.0 oneM2M: Study on Management Object migration to SDT	2021-11	http://www.etsi.org/deliver/etsi_tr/118500_118599/118567/04.00.00_60/tr_118567v040000p.pdf

Title	Date	Weblink
(NEW) ETSI/oneM2M TS 118 122 V4.5.1 oneM2M; Field Device Configuration	2023-07	https://www.etsi.org/deliver/etsi_ts/118100_118199/118122/04.05.01_60/ts_118122v040501p.pdf
(NEW) ETSI TS 103 846 V1.1.1 SmartM2M; Digital Twins: Functionalities and communication Reference Architecture	2024-08	http://www.etsi.org/deliver/etsi_ts/103800_103899/103846/01.01.01_60/ts_103846v010101p.pdf
(NEW) ETSI GS NIN 006 V1.1.1 Non-IP Networking (NIN); Scenario Definitions of Next Generation Protocols (NGP)	2024-07	http://www.etsi.org/deliver/etsi_gs/NIN/001_099/006/01.01.01_60/gs_NIN-006v010101p.pdf
(NEW) ETSI EN 303 760 V1.1.0	2024-06	http://www.etsi.org/deliver/etsi_en/303700_303799/303760/01.01.00_20/en_303760v010100a.pdf
(NEW) ETSI GS CIM 029 V1.1.1 Context Information Management (CIM); NGSI-LD Implementation Conformance Statement	2024-04	http://www.etsi.org/deliver/etsi_gs/CIM/001_099/029/01.01.01_60/gs_CIM-029v010101p.pdf
(NEW) ETSI GS CIM 027 V1.1.1 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)	2024-04	http://www.etsi.org/deliver/etsi_gs/CIM/001_099/027/01.01.01_60/gs_CIM-027v010101p.pdf
(NEW) ETSI TS 103 828 V1.1.1 SmartM2M; SAREF: Ontology Support for Urban Digital Twins and usage guidelines	2024-03	http://www.etsi.org/deliver/etsi_ts/103800_103899/103828/01.01.01_60/ts_103828v010101p.pdf
(NEW) ETSI TS 103 845 V1.1.1 SmartM2M; Digital Twins Communication Requirements	2024-02	http://www.etsi.org/deliver/etsi_ts/103800_103899/103845/01.01.01_60/ts_103845v010101p.pdf
(NEW) ETSI TS 103 927 V1.1.1 CYBER; Cyber Security for Consumer Internet of Things; Requirements for Smart Voice-Controlled Devices	2024-01	http://www.etsi.org/deliver/etsi_ts/103900_103999/103927/01.01.01_60/ts_103927v010101p.pdf
(NEW) ETSI TR 103 936 V1.1.1 Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control	2024-01	http://www.etsi.org/deliver/etsi_tr/103900_103999/103936/01.01.01_60/tr_103936v010101p.pdf
(NEW) ETSI TS 103 815 V1.1.1 CYBER; Cyber Security for Consumer Internet of Things; Requirements for Residential Smart Door Locking Devices	2024-01	http://www.etsi.org/deliver/etsi_ts/103800_103899/103815/01.01.01_60/ts_103815v010101p.pdf
(NEW) ETSI TR 103 844 V1.1.1 SmartM2M; Digital Twins and Standardization Opportunities in ETSI	2023-11	http://www.etsi.org/deliver/etsi_tr/103800_103899/103844/01.01.01_60/tr_103844v010101p.pdf
(NEW) ETSI TS 103 410-12 V1.1.1 SmartM2M; Extension to SAREF; Part 12: Smart Grid Domain	2023-11	http://www.etsi.org/deliver/etsi_ts/103400_103499/103410/12/01.01.01_60/ts_103410/12v010101p.pdf
(NEW) ETSI TR 103 827 V1.1.1 SmartM2M; SAREF: Digital Twins opportunities for the Ontology Context	2023-09	http://www.etsi.org/deliver/etsi_tr/103800_103899/103827/01.01.01_60/tr_103827v010101p.pdf
(NEW) ETSI TR 103 781 V1.1.1 SmartM2M; Study for SAREF ontology patterns and usage guidelines	2023-09	http://www.etsi.org/deliver/etsi_tr/103700_103799/103781/01.01.01_60/tr_103781v010101p.pdf

Title	Date	Weblink
(NEW) ETSI TR 103 839 V1.1.1 SmartM2M; Scenarios for evaluation of oneM2M deployments	2023-09	http://www.etsi.org/deliver/etsi_tr/103800_103899/103839/01.01.01_60/tr_103839v010101p.pdf
FIT IoT Lab FIT IoT-LAB Testbed The Very Large Scale Internet of Things Testbed	2024-09	https://www.iot-lab.info/
FIWARE Foundation FIWARE Internet of Things Framework	2024-09	https://www.fiware.org/
GS1 EPCIS EPC Information Services (EPCIS) Standard, v1.2 (2016)	2022-06	https://ref.gs1.org/standards/epcis/
HL7 International FHIR Fast Healthcare Interoperability Resources (FHIR) v4.0.1 (2019)	2022-05	http://hl7.org/fhir/directory.html
HL7 International HL7 V2.9 HL7 Version 2 Messaging Standard	2019-12	http://www.hl7.org/implement/standards/product_brief.cfm?product_id=516
IEC IEC role in the IoT	2018-10	https://www.iec.ch/basecamp/iec-role-iot
IEC Internet of Things: Wireless Sensor Networks	2014-11	https://www.iec.ch/basecamp/inter-net-things-wireless-sensor-networks
IEC IoT 2020: Smart and secure IoT platform	2016-10	https://www.iec.ch/basecamp/iot-2020-smart-and-secure-iot-platform
IEC 60869-1:2018 Fibre optic interconnecting devices and passive components - Fibre optic passive power control devices - Part 1: Generic specification	2018-11	https://webstore.iec.ch/publication/60884
IEC 60875-1:2015 Fibre optic interconnecting devices and passive components - Non-wavelength-selective fibre optic branching devices - Part 1: Generic specification	2015-05	https://webstore.iec.ch/publication/22396
IEC 61300-1:2022 Fibre optic interconnecting devices and passive components - Basic test and measurement procedures - Part 1: General and guidance	2022-04	https://webstore.iec.ch/publication/67663
(Updated) IEC 61406-1:2022 Identification Link - Part 1: General requirements	2022-09	https://webstore.iec.ch/en/publication/67673
IEC 61753-1:2018 Fibre optic interconnecting devices and passive components - Performance standard - Part 1: General and guidance	2018-08	https://webstore.iec.ch/publication/67249
IEC 61754-4:2022 Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 4: Type SC connector family	2022-02	https://webstore.iec.ch/publication/29284

Title	Date	Weblink
IEC 61754-7-3:2019 Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 7-3: Type MPO connector family - Two fibre rows 16 fibre wide	2019-04	https://webstore.iec.ch/publication/26692
IEC 61756-1:2019 Fibre optic interconnecting devices and passive components - Interface standard for fibre management systems - Part 1: General and guidance	2019-11	https://webstore.iec.ch/publication/59508
IEC 61987-1:2006 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 1: Measuring equipment with analogue and digital output	2006-12	https://webstore.iec.ch/publication/6225
IEC 61987-10:2009 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 10: List of Properties (LOPs) for Industrial-Process Measurement and Control for Electronic Data Exchange - Fundamentals	2009-07	https://webstore.iec.ch/publication/6227
IEC 61987-11:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 11: List of properties (LOPs) of measuring equipment for electronic data exchange - Generic structures	2016-12	https://webstore.iec.ch/publication/32275
IEC 61987-12:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 12: Lists of properties (LOPs) for flow measuring equipment for electronic data exchange	2016-03	https://webstore.iec.ch/publication/24401
IEC 61987-13:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 13: Lists of properties (LOP) for pressure measuring equipment for electronic data exchange	2016-03	https://webstore.iec.ch/publication/24400
IEC 61987-14:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 14: Lists of properties (LOP) for temperature measuring equipment for electronic data exchange	2016-04	https://webstore.iec.ch/publication/24637

Title	Date	Weblink
IEC 61987-15:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 15: Lists of properties (LOPs) for level measuring equipment for electronic data exchange	2016-11	https://webstore.iec.ch/publication/26177
IEC 61987-16:2016 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 16: List of properties (LOPs) for density measuring equipment for electronic data exchange	2016-12	https://webstore.iec.ch/publication/34265
(Updated) 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	2022-12	https://webstore.iec.ch/publication/63343
(Updated) IEC 61987-32:2024 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	2024-06	https://webstore.iec.ch/publication/63344
IEC 61987-41 ED1 Generic structures of List of Properties (LOP) of Process Analyzer Technology (PAT) measuring devices for electronic data exchange	Under development - Last accessed month: 2025-02	https://www.iec.ch/ords/f?p=103:38:401030832849310:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,107355
IEC 61987-92:2018 Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 92: Lists of properties (LOP) of measuring equipment for electronic data exchange - Aspect LOPs	2018-06	https://webstore.iec.ch/publication/33096
IEC 62005-1:2001 Reliability of fibre optic interconnecting devices and passive components - Part 1: Introductory guide and definitions	2001-03	https://webstore.iec.ch/publication/6280
IEC 62099:2001 Fibre optic wavelength switches - Generic specification	2001-03	https://webstore.iec.ch/publication/6459
IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	2010-11	https://webstore.iec.ch/publication/7030
IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers	2015-06	https://webstore.iec.ch/publication/22810

Title	Date	Weblink
IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	2020-06	https://webstore.iec.ch/publication/30727
IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	2020-06	https://webstore.iec.ch/publication/30727
IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	2013-08	https://webstore.iec.ch/publication/7033
IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	2018-01	https://webstore.iec.ch/publication/34421
IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	2019-02	https://webstore.iec.ch/publication/34421
IEC 62541-10:2020 OPC Unified Architecture - Part 10: Programs	2020-07	https://webstore.iec.ch/publication/61119
IEC 62541-100:2015 OPC Unified Architecture - Part 100: Device Interface	2015-03	https://webstore.iec.ch/publication/21987
IEC 62541-11:2020 OPC Unified Architecture - Part 11: Historical Access	2020-06	https://webstore.iec.ch/publication/61129
IEC 62541-13:2020 OPC Unified Architecture - Part 13: Aggregates	2020-06	https://webstore.iec.ch/publication/61131
IEC 62541-14:2020 OPC Unified Architecture - Part 14: PubSub	2020-07	https://webstore.iec.ch/publication/61108
IEC 62541-3:2020 OPC Unified Architecture - Part 3: Address Space Model	2020-07	https://webstore.iec.ch/publication/61112
IEC 62541-4:2020 OPC Unified Architecture - Part 4: Services	2020-07	https://webstore.iec.ch/publication/61113
IEC 62541-5:2020 OPC Unified Architecture - Part 5: Information Model	2020-07	https://webstore.iec.ch/publication/61114
IEC 62541-6:2020 OPC Unified Architecture - Part 6: Mappings	2020-07	https://webstore.iec.ch/publication/61115
IEC 62541-7:2020 OPC Unified Architecture - Part 7: Profiles	2020-06	https://webstore.iec.ch/publication/61116
IEC 62541-8:2020 OPC Unified Architecture - Part 8: Data Access	2020-06	https://webstore.iec.ch/publication/61117
IEC 62541-9:2020 OPC Unified Architecture - Part 9: Alarms and Conditions	2020-06	https://webstore.iec.ch/publication/61118

Title	Date	Weblink
IEC 62714-1:2018 Engineering data exchange format for use in industrial automation systems engineering - Automation Markup Language - Part 1: Architecture and general requirements	2018-04	https://webstore.iec.ch/publication/32339
IEC 62714-2:2015 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 2: Role class libraries	2015-03	https://webstore.iec.ch/publication/22030
IEC 62714-3:2017 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 3: Geometry and kinematics	2017-01	https://webstore.iec.ch/publication/34158
IEC 62714-4:2020 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 4: Logic	2020-06	https://webstore.iec.ch/publication/28979
IEC 62714-5:2022 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 5: Communication	2022-03	https://webstore.iec.ch/publication/65493
IEC 62832-1:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 1: General principles	2020-10	https://webstore.iec.ch/publication/65858
IEC 62832-2:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 2: Model elements	2020-10	https://webstore.iec.ch/publication/60214
IEC 62832-3:2020 Industrial-process measurement, control and automation - Digital factory framework - Part 3: Application of Digital Factory for life cycle management of production systems	2020-10	https://webstore.iec.ch/publication/60277
IEC 62872-2:2022 Industrial-process measurement, control and automation - Part 2: Internet of Things (IoT) - Application framework for industrial facility demand response energy management	2022-02	https://webstore.iec.ch/publication/63419
(Updated) IEC 63203-801-1 Wearable electronic devices and technologies - Part 801-1: Smart Body Area Network (SmartBAN) - Enhanced Ultra-Low Power Physical Layer	2021-11	https://www.iec.ch/dyn/www-w/f?p=103:38:615499235431339::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:2053723103719

Title	Date	Weblink
(Updated) IEC 63203-801-2 Wearable electronic devices and technologies - Part 801-2: Smart Body Area Network (SmartBAN) - Low Complexity Medium Access Control (MAC) for SmartBAN	2021-11	https://www.iec.ch/dyn/www-w/f?p=103:38:615499235431339:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20537,23,103720
(Updated) EC 63278-1 ED1 Asset Administration Shell for industrial applications – Part 1: Asset Administration Shell structure	2023-12	https://webstore.iec.ch/en/publication/65628
IEC 63278-3 ED1 Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:731054763917753:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109075
(Updated) IEC 63339:2024 ED1 Unified reference model for smart manufacturing	2024-10	https://webstore.iec.ch/publication/67119
(Updated) IEC 63365:2022 ED1 Industrial process measurement, control and automation - Digital nameplate	2022-10	https://webstore.iec.ch/en/publication/67436
(Updated) IEC 63376 ED1 INDUSTRIAL FACILITY ENERGY MANAGEMENT SYSTEM (FEMS) – Functions and Information Flows	2024-02	https://webstore.iec.ch/en/publication/67721
IEC Cloudwatch D3.6 Cloudwatch D3.6 Security and Interoperability Standards Status Report	2017-09	https://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Security-and-Interoperability-Standards-Status-Report.pdf
IEC EC 63237-1 ED1 Household and similar electrical appliances - Product information properties - Part 1: Fundamentals	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:1645358955729:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1275,23,102429
IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment	2015-06	https://webstore.iec.ch/publication/22811
IEC TR 62443-3-1:2009 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems	2009-07	https://webstore.iec.ch/publication/7031
IEC TR 62541-1:2020 OPC Unified Architecture - Part 1: Overview and concepts	2020-11	https://webstore.iec.ch/publication/61109
IEC TR 62541-2:2020 OPC Unified Architecture - Part 2: Security Model	2020-11	https://webstore.iec.ch/publication/61110
IEC TR 63283-1:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 1: Terms and definitions	2022-03	https://webstore.iec.ch/publication/66314

Title	Date	Weblink
IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models	2009-07	https://webstore.iec.ch/publication/7029
IEC TS 62872-1:2019 Industrial-process measurement, control and automation - Part 1: System interface between industrial facilities and the smart grid	2019-06	https://webstore.iec.ch/publication/62884
(NEW) IEC 61406-2:2024 Identification link - Part 2: Types/models, lots/batches, items and characteristics	2024-05	https://webstore.iec.ch/publication/77973
(NEW) IEC 63278-2 ED1 Asset Administration Shell for Industrial Applications – Part 2: Information meta model	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:502560904033881:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109017
(NEW) IEC 63278-4 ED1 Asset administration shell for industrial applications - Part 4: Use cases and modelling examples	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:508054836884348:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,116472
(NEW) IEC 63278-5 ED1 Asset Administration Shell for industrial applications – Part 5: Interfaces	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:508054836884348:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,121674
(NEW) IEC TR 63283-2:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 2: Use cases	2022-03	https://webstore.iec.ch/publication/66315
(NEW) IEC TR 63283-3:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 3: Challenges for cybersecurity	2022-03	https://webstore.iec.ch/publication/66316
(NEW) IEC TR 63283-5:2024 Industrial-process measurement, control and automation – Smart manufacturing – Part 5: Market and innovation trends analysis.	2024-11	https://webstore.iec.ch/en/publication/71399
(Updated) IEEE - P1451.99 Standard for Harmonization of Internet of Things (IoT) Devices and Systems	2024-05	https://standards.ieee.org/ieee/1451.99/11634/
(Updated) IEEE Transdisciplinary Framework for 5G-Enabled Applications and Services	Under development - Last accessed month: 2025-02	https://standards.ieee.org/industry-connections/activities/transdisciplinary-framework-5g/
IEEE 1609.2 IEEE 1609.2 standard for Security, Network Services and Multi-Channel Operation	2016-03	https://ieeexplore.ieee.org/document/7426684
IEEE 1609.3 IEEE 1609.3 standard for Security, Network Services and Multi-Channel Operation	2016-04	https://ieeexplore.ieee.org/document/7458115
IEEE 1609.4 IEEE 1609.4 standard for Security, Network Services and Multi-Channel Operation	2016-03	https://ieeexplore.ieee.org/document/7435228

Title	Date	Weblink
IEEE 1872.2-2021 IEEE Approved Draft Standard for Autonomous Robotics (AuR) Ontology	2021-09	https://standards.ieee.org/ieee/1872.2/7094/
IEEE 754-2008 IEEE Standard for Floating-Point Arithmetic	2008-08	https://ieeexplore.ieee.org/document/4610935
IEEE 802.11p IEEE 802.11p amendment for wireless access in vehicular environments (WAVE)	2010-07	https://ieeexplore.ieee.org/document/5514475
IEEE 802.1AS-2020 Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks	2020-06	https://standards.ieee.org/ieee/802.1AS/7121/
(NEW) IEEE 2668-2022 IEEE Standard for Maturity Index of the Internet of Things-- Evaluation, Grading, and Ranking	2023-12	https://standards.ieee.org/ieee/2668/7254/
(NEW) IEEE SA - IEEE 2735-2022 IEEE Standard for Interoperability of Complex Virtual Instruments for Internet of Things	2023-02	https://standards.ieee.org/ieee/2735/7392/
(NEW) IEEE 2735.1-2022 IEEE Standard Design Criteria of Complex Virtual Instruments for Household Appliance Test	2023-02	https://standards.ieee.org/ieee/2735.1/7393/
(NEW) IEEE/ISO/IEC 42010-2022 IEEE/ISO/IEC International Standard for Software, systems and enterprise-- Architecture description	2022-11	https://standards.ieee.org/ieee/42010/6846/
(NEW) IEEE 1935-2023 IEEE Standard for Edge/Fog Manageability and Orchestration	2023-07	https://standards.ieee.org/ieee/1935/7181/
(NEW) IEEE 3219-2023 IEEE Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT)	2024-04	https://standards.ieee.org/ieee/3219/71163/
(NEW) IEEE 1451.0-2024 IEEE Standard for a Smart Transducer Interface for Sensors and Actuators--Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats	2024-06	https://standards.ieee.org/ieee/1451.0/71001/
(NEW) IEEE 1901c-2024 IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications Amendment 3: Enhanced Flexible Channel Wavelet (FCW) Physical and Media Access Control Layers for Use on Any Media	2024-05	https://standards.ieee.org/ieee/1901c/70922/
(NEW) IEEE 1918.1-2024 IEEE Approved Draft Standard for Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture, Functions, and Technical Assumptions	2024-09	https://standards.ieee.org/ieee/1918.1/6721/

Title	Date	Weblink
(NEW) IEEE/UL 2933-2024 IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security	2024-09	https://standards.ieee.org/ieee/2933/7592/
(NEW) IEEE P2418.3 Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture	2019-07	https://standards.ieee.org/ieee/2418.3/7714/
(NEW) IEEE P2992 Recommended Practice for Data Expression, Exchange, and Processing in Smart Agriculture	2021-05	https://standards.ieee.org/ieee/2992/10614/
(Updated) IETF draft-ietf-asdf-sdf Semantic Definition Format (SDF) for Data and Interactions of Things	2024-02	https://datatracker.ietf.org/doc/draft-ietf-asdf-sdf/
(Updated) IETF RFC 9365 IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases	2023-12	https://datatracker.ietf.org/doc/rfc9365/
(Updated) IETF RFC9528 Ephemeral Diffie-Hellman Over COSE (EDHOC)	2024-03	https://datatracker.ietf.org/doc/rfc9528/
(Updated) IETF RFC 9529 Traces of EDHOC	2024-03	https://datatracker.ietf.org/doc/rfc9529/
(Updated) IETF draft-ietf-rats-ar4si Attestation Results for Secure Interactions	2024-03	https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/
(Updated) IETF RFC 9334 Remote Attestation Procedures Architecture	2023-12	https://datatracker.ietf.org/doc/rfc9334/
(Updated) IETF draft-ietf-rats-daa Direct Anonymous Attestation for the Remote Attestation Procedures Architecture	2024-03	https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
(Updated) IETF draft-ietf-rats-eat The Entity Attestation Token (EAT)	2024-08	https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
(Updated) IETF draft-ietf-rats-network-device-subscription Attestation Event Stream Subscription	2024-07	https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
(Updated) IETF draft-ietf-rats-reference-interaction-models Reference Interaction Models for Remote Attestation Procedures	2024-07	https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
(Updated) IETF draft-ietf-rats-tpm-based-network-device-attest TPM-based Network Device Remote Integrity Verification	2024-03	https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/
(Updated) IETF draft-ietf-rats-uccs A CBOR Tag for Unprotected CWT Claims Sets	2024-07	https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
(Updated) IETF draft-ietf-rats-yang-tpm-charra A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs.	2024-07	https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/

Title	Date	Weblink
(Updated) IETF draft-ietf-raw-architecture Reliable and Available Wireless Architecture	2024-07	https://datatracker.ietf.org/doc/draft-ietf-raw-architecture/
(Updated) IETF draft-ietf-raw-framework Reliable and Available Wireless Framework	2024-03	https://datatracker.ietf.org/doc/draft-ietf-raw-framework/
(Updated) IETF draft-ietf-raw-industrial-requirements Requirements for Reliable Wireless Industrial Services	2023-10	https://datatracker.ietf.org/doc/draft-ietf-raw-industrial-requirements/
(Updated) IETF RFC 9372 L-band Digital Aeronautical Communications System (LDACS)	2023-12	https://datatracker.ietf.org/doc/rfc9372/
(Updated) IETF draft-ietf-raw-oam-support Operations, Administration and Maintenance (OAM) features for RAW	2023-03	https://datatracker.ietf.org/doc/draft-ietf-raw-oam-support/
(Updated) IETF draft-ietf-raw-technologies Reliable and Available Wireless Technologies	2024-07	https://datatracker.ietf.org/doc/draft-ietf-raw-technologies/
(Updated) IETF RFC 9450 RAW use-cases	2024-01	https://datatracker.ietf.org/doc/rfc9450/
(Updated) IETF RFC 9397 Trusted Execution Environment Provisioning (TEEP) Architecture	2023-07	https://datatracker.ietf.org/doc/rfc9397/
(Updated) IETF draft-ietf-teep-otrp-over-http HTTP Transport for Trusted Execution Environment Provisioning: Agent Initiated Communication	2023-03	https://datatracker.ietf.org/doc/draft-ietf-teep-otrp-over-http/
(Updated) IETF draft-ietf-teep-protocol Trusted Execution Environment Provisioning (TEEP) Protocol	2024-05	https://datatracker.ietf.org/doc/draft-ietf-teep-protocol/
(Updated) IETF draft-km-iiotops-iiot-frwk Virtualization of PLC in Industrial Networks - Problem Statement	2022-05	https://datatracker.ietf.org/doc/draft-km-iiotops-iiot-frwk/
(Updated) IETF draft-morais-iiotops-inxu Intra-Network eXposure analyzer Utility Specification	2022-05	https://datatracker.ietf.org/doc/draft-morais-iiotops-inxu/
ietf RFC 7228 Terminology for Constrained-Node Networks	2014-05	https://datatracker.ietf.org/doc/rfc7228/
ietf RFC 7388 Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2010-10	https://datatracker.ietf.org/doc/rfc7388/
ietf RFC 7973 Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation	2016-11	https://datatracker.ietf.org/doc/rfc7973/
ietf RFC 8025 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch	2016-11	https://datatracker.ietf.org/doc/rfc8025/

Title	Date	Weblink
IETF RFC 8036 Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks	2017-01	https://datatracker.ietf.org/doc/rfc8036/
IETF RFC 8065 Privacy Considerations for IPv6 Adaptation-Layer Mechanisms	2017-02	https://datatracker.ietf.org/doc/rfc8065/
IETF RFC 8066 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines	2017-02	https://datatracker.ietf.org/doc/rfc8066/
IETF RFC 8075 Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)	2017-02	https://datatracker.ietf.org/doc/rfc8075/
IETF RFC 8105 Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)	2017-05	https://datatracker.ietf.org/doc/rfc8105/
IETF RFC 8132 PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)	2017-04	https://datatracker.ietf.org/doc/rfc8132/
IETF RFC 8138 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header	2017-04	https://datatracker.ietf.org/doc/rfc8138/
IETF RFC 8152 CBOR Object Signing and Encryption (COSE)	2017-01	https://datatracker.ietf.org/doc/rfc8152/
IETF RFC 8163 Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks	2017-05	https://datatracker.ietf.org/doc/rfc8163/
IETF RFC 8180 Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration	2017-05	https://datatracker.ietf.org/doc/rfc8180/
IETF RFC 8323 CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets	2018-02	https://datatracker.ietf.org/doc/rfc8323/
IETF RFC 8352 Energy-Efficient Features of Internet of Things Protocols	2018-02	https://datatracker.ietf.org/doc/rfc8352/
IETF RFC 8366 A Voucher Artifact for Bootstrapping Protocols	2018-05	https://datatracker.ietf.org/doc/rfc8366/
IETF RFC 8368 Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)	2018-05	https://datatracker.ietf.org/doc/rfc8368/
IETF RFC 8376 Low-Power Wide Area Network (LPWAN) Overview	2018-05	https://datatracker.ietf.org/doc/rfc8376/
IETF RFC 8387 Practical Considerations and Implementation Experiences in Securing Smart Object Networks	2018-05	https://datatracker.ietf.org/doc/rfc8387/
IETF RFC 8392 CBOR Web Token (CWT)	2018-05	https://datatracker.ietf.org/doc/rfc8392/

Title	Date	Weblink
IETF RFC 8428 Sensor Measurement Lists (SenML)	2018-08	https://datatracker.ietf.org/doc/rfc8428/
IETF RFC 8480 6TiSCH Operation Sublayer (6top) Protocol (6P)	2018-11	https://datatracker.ietf.org/doc/rfc8480/
IETF RFC 8505 Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery	2018-11	https://datatracker.ietf.org/doc/rfc8505/
IETF RFC 8516 “Too Many Requests” Response Code for the Constrained Application Protocol	2019-01	https://datatracker.ietf.org/doc/rfc8516/
IETF RFC 8557 Deterministic Networking Problem statement	2019-05	https://datatracker.ietf.org/doc/rfc8557/
IETF RFC 8578 Deterministic Networking Use Cases	2019-01	https://datatracker.ietf.org/doc/rfc8578/
IETF RFC 8610 Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures	2019-06	https://datatracker.ietf.org/doc/rfc8610/
IETF RFC 8613 Object Security for Constrained RESTful Environments (OSCORE)	2019-07	https://datatracker.ietf.org/doc/rfc8613/
IETF RFC 8655 Deterministic Networking Architecture	2019-10	https://datatracker.ietf.org/doc/rfc8655/
IETF RFC 8710 Multipart Content-Format for the Constrained Application Protocol (CoAP)	2020-02	https://datatracker.ietf.org/doc/rfc8710/
IETF RFC 8724 SCHC: Generic Framework for Static Context Header Compression and Fragmentation	2020-04	https://datatracker.ietf.org/doc/rfc8724/
IETF RFC 8742 Concise Binary Object Representation (CBOR) Sequences	2020-02	https://datatracker.ietf.org/doc/rfc8742/
IETF RFC 8746 Concise Binary Object Representation (CBOR) Tags for Typed Arrays	2020-02	https://datatracker.ietf.org/doc/rfc8746/
IETF RFC 8747 Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)	2020-03	https://datatracker.ietf.org/doc/rfc8747/
IETF RFC 8768 Constrained Application Protocol (CoAP) Hop-Limit Option	2020-03	https://datatracker.ietf.org/doc/rfc8768/
IETF RFC 8778 Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)	2020-04	https://datatracker.ietf.org/doc/rfc8778/
IETF RFC 8790 FETCH and PATCH with Sensor Measurement Lists (SenML)	2020-06	https://datatracker.ietf.org/doc/rfc8790/
IETF RFC 8798 Additional Units for Sensor Measurement Lists (SenML)	2020-06	https://datatracker.ietf.org/doc/rfc8798/

Title	Date	Weblink
IETF RFC 8812 CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms	2020-08	https://datatracker.ietf.org/doc/rfc8812/
IETF RFC 8824 Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)	2021-06	https://datatracker.ietf.org/doc/rfc8824/
IETF RFC 8928 Address-Protected Neighbor Discovery for Low-Power and Lossy Networks	2020-11	https://datatracker.ietf.org/doc/rfc8928/
IETF RFC 8929 IPv6 Backbone Router	2020-11	https://datatracker.ietf.org/doc/rfc8929/
IETF RFC 8930 On Forwarding 6LoWPAN Fragments over a Multi-Hop IPv6 Network	2020-11	https://datatracker.ietf.org/doc/rfc8930/
IETF RFC 8931 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Selective Fragment Recovery	2020-11	https://datatracker.ietf.org/doc/rfc8931/
IETF RFC 8938 Deterministic Networking (DetNet) Data Plane Framework	2020-11	https://datatracker.ietf.org/doc/rfc8938/
IETF RFC 8939 Deterministic Networking (DetNet) Data Plane: IP	2020-11	https://datatracker.ietf.org/doc/rfc8939/
IETF RFC 8943 Concise Binary Object Representation (CBOR) Tags for Date	2020-11	https://datatracker.ietf.org/doc/rfc8943/
IETF RFC 8949 Concise Binary Object Representation (CBOR)	2020-11	https://datatracker.ietf.org/doc/rfc8949/
IETF RFC 8964 Deterministic Networking (DetNet) Data Plane: MPLS	2020-01	https://datatracker.ietf.org/doc/rfc8964/
IETF RFC 8974 Extended Tokens and Stateless Clients in the Constrained Application Protocol (CoAP)	2020-01	https://datatracker.ietf.org/doc/rfc8974/
IETF RFC 8990 GeneRIC Autonomic Signaling Protocol (GRASP)	2021-05	https://datatracker.ietf.org/doc/rfc8990/
IETF RFC 8991 GeneRIC Autonomic Signaling Protocol Application Program Interface (GRASP API)	2021-05	https://datatracker.ietf.org/doc/rfc8991/
IETF RFC 8992 Autonomic IPv6 Edge Prefix Management in Large-Scale Networks	2021-05	https://datatracker.ietf.org/doc/rfc8992/
IETF RFC 8993 A Reference Model for Autonomic Networking	2021-05	https://datatracker.ietf.org/doc/rfc8993/
IETF RFC 8994 An Autonomic Control Plane (ACP)	2021-05	https://datatracker.ietf.org/doc/rfc8994/
IETF RFC 8995 Bootstrapping Remote Secure Key Infrastructure (BRSKI)	2021-05	https://datatracker.ietf.org/doc/rfc8995/
IETF RFC 9006 TCP Usage Guidance in the Internet of Things (IoT)	2021-03	https://datatracker.ietf.org/doc/rfc9006/

Title	Date	Weblink
IETF RFC 9008 Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane	2021-04	https://datatracker.ietf.org/doc/rfc9008/
IETF RFC 9011 Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN	2021-04	https://datatracker.ietf.org/doc/rfc9011/
IETF RFC 9016 Flow and Service Information Model for Deterministic Networking (DetNet)	2021-03	https://datatracker.ietf.org/doc/rfc9016/
IETF RFC 9019 A Firmware Update Architecture for Internet of Things	2021-04	https://datatracker.ietf.org/doc/rfc9019/
IETF RFC 9024 Deterministic Networking (DetNet) Data Plane: IEEE 802.1 Time-Sensitive Networking over MPLS	2021-06	https://datatracker.ietf.org/doc/rfc9024/
IETF RFC 9025 Deterministic Networking (DetNet) Data Plane: MPLS over UDP/IP	2021-04	https://datatracker.ietf.org/doc/rfc9025/
IETF RFC 9030 An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)	2021-05	https://datatracker.ietf.org/doc/rfc9030/
IETF RFC 9031 Constrained Join Protocol (CoJP) for 6TiSCH	2021-05	https://datatracker.ietf.org/doc/rfc9031/
IETF RFC 9032 Encapsulation of 6TiSCH Join and Enrollment Information Elements	2021-05	https://datatracker.ietf.org/doc/rfc9032/
IETF RFC 9033 6TiSCH Minimal Scheduling Function (MSF)	2021-05	https://datatracker.ietf.org/doc/rfc9033/
IETF RFC 9034 Packet Delivery Deadline Time in the Routing Header for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2021-06	https://datatracker.ietf.org/doc/rfc9034/
IETF RFC 9035 A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header	2021-04	https://datatracker.ietf.org/doc/rfc9035/
IETF RFC 9037 Deterministic Networking (DetNet) Data Plane: MPLS over IEEE 802.1 Time-Sensitive Networking (TSN)	2021-06	https://datatracker.ietf.org/doc/rfc9037/
IETF RFC 9039 Uniform Resource Names for Device Identifiers	2021-06	https://datatracker.ietf.org/doc/rfc9039/
IETF RFC 9055 Deterministic Networking (DetNet) Security Considerations	2021-06	https://datatracker.ietf.org/doc/rfc9055/
IETF RFC 9056 Deterministic Networking (DetNet) Data Plane: IP over MPLS	2021-10	https://datatracker.ietf.org/doc/rfc9056/
IETF RFC 9090 Concise Binary Object Representation (CBOR) Tags for Object Identifiers	2021-07	https://datatracker.ietf.org/doc/rfc9090/

Title	Date	Weblink
IETF RFC 9100 Sensor Measurement Lists (SenML) Features and Versions	2021-08	https://datatracker.ietf.org/doc/rfc9100/
IETF RFC 9023 Deterministic Networking (DetNet) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking (TSN)	2021-06	https://datatracker.ietf.org/doc/rfc9023/
IETF RFC 9124 A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices	2022-01	https://datatracker.ietf.org/doc/rfc9124/
IETF RFC 9159 IPv6 Mesh over BLUETOOTH(R) Low Energy Using the Internet Protocol Support Profile (IPSP)	2021-12	https://datatracker.ietf.org/doc/rfc9159/
IETF RFC 9164 Concise Binary Object Representation (CBOR) Tags for IPv4 and IPv6 Addresses and Prefixes	2021-12	https://datatracker.ietf.org/doc/rfc9164/
IETF RFC 9165 Additional Control Operators for the Concise Data Definition Language (CDDL)	2021-12	https://datatracker.ietf.org/doc/rfc9165/
IETF RFC 9175 Constrained Application Protocol (CoAP): Echo, Request-Tag, and Token Processing	2022-03	https://datatracker.ietf.org/doc/rfc9175/
IETF RFC 9222 Guidelines for Autonomic Service Agents	2022-03	https://datatracker.ietf.org/doc/rfc9222/
IETF RFC4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals	2007-08	https://datatracker.ietf.org/doc/rfc4919/
IETF RFC4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks	2007-09	https://datatracker.ietf.org/doc/rfc4944/
IETF RFC5548 Routing Requirements for Urban Low-Power and Lossy Networks	2009-05	https://datatracker.ietf.org/doc/rfc5548/
IETF RFC5673 Industrial Routing Requirements in Low-Power and Lossy Networks	2009-10	https://datatracker.ietf.org/doc/rfc5673/
IETF RFC5826 Home Automation Routing Requirements in Low-Power and Lossy Networks	2010-04	https://datatracker.ietf.org/doc/rfc5826/
IETF RFC5867 Building Automation Routing Requirements in Low-Power and Lossy Networks	2010-06	https://datatracker.ietf.org/doc/rfc5867/
IETF RFC6206 The Trickle Algorithm	2011-03	https://datatracker.ietf.org/doc/rfc6206/
IETF RFC6282 Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks	2011-09	https://datatracker.ietf.org/doc/rfc6282/
IETF RFC6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks	2012-03	https://datatracker.ietf.org/doc/rfc6550/
IETF RFC6551 Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks	2012-03	https://datatracker.ietf.org/doc/rfc6551/

Title	Date	Weblink
IETF RFC6552 Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)	2012-03	https://datatracker.ietf.org/doc/rfc6552/
IETF RFC6568 Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2012-04	https://datatracker.ietf.org/doc/rfc6568/
IETF RFC6606 Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing	2012-05	https://datatracker.ietf.org/doc/rfc6606/
IETF RFC6690 Constrained RESTful Environments (CoRE) Link Format	2012-08	https://datatracker.ietf.org/doc/rfc6690/
IETF RFC6719 The Minimum Rank with Hysteresis Objective Function	2012-09	https://datatracker.ietf.org/doc/rfc6719/
IETF RFC6775 Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2012-11	https://datatracker.ietf.org/doc/rfc6775/
IETF RFC6997 Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks	2013-08	https://datatracker.ietf.org/doc/rfc6997/
IETF RFC6998 A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network	2013-08	https://datatracker.ietf.org/doc/rfc6998/
IETF RFC7102 Terms Used in Routing for Low-Power and Lossy Networks	2014-01	https://datatracker.ietf.org/doc/rfc7102/
IETF RFC7252 The Constrained Application Protocol (CoAP)	2014-06	https://datatracker.ietf.org/doc/rfc7252/
IETF RFC7390 Group Communication for the Constrained Application Protocol (CoAP)	2014-10	https://datatracker.ietf.org/doc/rfc7390/
IETF RFC7400 6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2014-11	https://datatracker.ietf.org/doc/rfc7400/
IETF RFC7416 A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)	2015-01	https://datatracker.ietf.org/doc/rfc7416/
IETF RFC7428 Transmission of IPv6 Packets over ITU-T G.9959 Networks	2015-02	https://datatracker.ietf.org/doc/rfc7428/
IETF RFC7554 Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement	2015-05	https://datatracker.ietf.org/doc/rfc7554/
IETF RFC7641 Observing Resources in the Constrained Application Protocol (CoAP)	2015-09	https://datatracker.ietf.org/doc/rfc7641/
IETF RFC7668 IPv6 over BLUETOOTH(R) Low Energy	2015-01	https://datatracker.ietf.org/doc/rfc7668/

Title	Date	Weblink
IETF RFC7731 Multicast Protocol for Low-Power and Lossy Networks (MPL)	2016-02	https://datatracker.ietf.org/doc/rfc7731/
IETF RFC7732 Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)	2016-02	https://datatracker.ietf.org/doc/rfc7732/
IETF RFC7733 Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control	2016-02	https://datatracker.ietf.org/doc/rfc7733/
IETF RFC7744 Use Cases for Authentication and Authorization in Constrained Environments	2016-02	https://datatracker.ietf.org/doc/rfc7744/
IETF RFC7774 Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6	2016-03	https://datatracker.ietf.org/doc/rfc7774/
IETF RFC7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation	2016-03	https://datatracker.ietf.org/doc/rfc7815/
IETF RFC7959 Block-Wise Transfers in the Constrained Application Protocol (CoAP)	2016-08	https://datatracker.ietf.org/doc/rfc7959/
IETF RFC9009 Efficient Route Invalidation	2021-04	https://datatracker.ietf.org/doc/rfc9009/
IETF RFC9010 Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves	2021-04	https://datatracker.ietf.org/doc/rfc9010/
(NEW) IETF draft-nichols-iotops-defined-trust-transport Defined-Trust Transport (DeftT) Protocol for Limited Domains	2024-03	https://datatracker.ietf.org/doc/draft-nichols-iotops-defined-trust-transport/
(NEW) IETF draft-walther-iotops-iot-ops IoT Operational Issues	2024-03	https://datatracker.ietf.org/doc/draft-walther-iotops-iot-ops/
(NEW) IETF draft-li-iotops-intelligent-security Intelligent Protection Optimization System for IOT	2024-02	https://datatracker.ietf.org/doc/draft-li-iotops-intelligent-security/
(NEW) IETF draft-ietf-iotops-security-summary A summary of security-enabling technologies for IoT devices	2023-10	https://datatracker.ietf.org/doc/draft-ietf-iotops-security-summary/
(NEW) IETF draft-irtf-t2trg-taxonomy-manufacturer-anchors A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors	2024-01	https://datatracker.ietf.org/doc/draft-irtf-t2trg-taxonomy-manufacturer-anchors/
(NEW) IETF draft-irtf-t2trg-security-setup-iot-devices Terminology and processes for initial security setup of IoT devices	2024-03	https://datatracker.ietf.org/doc/draft-irtf-t2trg-security-setup-iot-devices/

Title	Date	Weblink
(NEW) IETF draft-ietf-scitt-software-use-cases Detailed Software Supply Chain Uses Cases for SCITT	2024-04	https://datatracker.ietf.org/doc/draft-ietf-scitt-software-use-cases/
(NEW) IETF draft-ietf-scitt-architecture An Architecture for Trustworthy and Transparent Digital Supply Chains	2024-03	https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/
(NEW) IETF draft-ietf-scitt-scrapi SCITT Reference APIs	2024-03	https://datatracker.ietf.org/doc/draft-ietf-scitt-scrapi/
IHE (Integrating the Healthcare Enterprise) Patient Care Device (PCD) Profiles	N/A	https://wiki.ihe.net/index.php?title=PCD_Profiles
(Updated) IRTF draft-choi-icnrg-aiot Requirements and Challenges for User-level Service Managements of IoT Network by utilizing Artificial Intelligence	2023-06	https://datatracker.ietf.org/doc/draft-choi-icnrg-aiot/
(Updated) IRTF draft-irtf-t2trg-rest-iot Guidance on RESTful Design for Internet of Things Systems	2024-07	https://datatracker.ietf.org/doc/draft-irtf-t2trg-rest-iot/
(Updated) IRTF draft-irtf-t2trg-secure-bootstrapping Terminology and processes for initial security setup of IoT devices	2024-03	https://datatracker.ietf.org/doc/draft-irtf-t2trg-secure-bootstrapping/
IRTF RFC 8576 Internet of Things (IoT) Security: State of the Art and Challenges	2019-04	https://datatracker.ietf.org/doc/rfc8576/
IRTF RFC 8691 Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11	2019-12	https://datatracker.ietf.org/doc/rfc8691/
IRTF RFC 9139 Information-Centric Networking (ICN) Adaptation to Low-Power Wireless Personal Area Networks (LoWPANs)	2021-11	https://datatracker.ietf.org/doc/rfc9139/
ISO ISO/CD 24227 ISO/CD 24227 Accuracy evaluation protocol for daily living walking speed extracted from sensor systems that measure human body motion	Under development - Last accessed month: 2025-02	www.iso.org/standard/78134.html
(Updated) ISO ISO 31700-1:2023 Consumer protection — Privacy by design for consumer goods and services - Part 1: High-level requirements	2023-01	https://www.iso.org/standard/84977.html
ISO ISO/IEEE 11073 (2014) Health informatics – Point-of-care medical device communication.	2020-08	https://www.iso.org/standard/77338.html
ISO ISO/PAS 19450:2015 Automation systems and integration - Object-Process Methodology	2015-12	https://www.iso.org/standard/84612.html?browse=tc

Title	Date	Weblink
(NEW) ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security Part 1: Principles and concepts	2021-03	https://www.iso.org/standard/71538.html
(NEW) IEC 80001-1:2021 Application of risk management for IT- networks incorporating medical devices Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software	2021-09	https://www.iso.org/standard/72026.html
(NEW) ISO 27269:2021 Health informatics — International patient summary	2021-04	https://www.iso.org/standard/79491.html
(NEW) ISO/DPAS 24305 Health informatics — Guidelines for implementation of HL7 FHIR based on ISO 13940:2015, ISO 13606-1:2019 and ISO 13606-3:2019	Under development - Last accessed month: 2025-02	https://www.iso.org/standard/78390.html
(NEW) ISO 27799:2016(en) Health informatics — Information security management in health using ISO/IEC 27002	2016-08	https://www.iso.org/obp/ui/es/#iso:std:iso:27799:ed-2:vi:en
ISO/IEC 15408:2009 Information technology — Security techniques — Evaluation criteria for IT security	2009-12	https://www.iso.org/standard/50341.html
ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation	2008-08	https://www.iso.org/standard/46412.html
ISO/IEC 19637:2016 Information technology - Sensor network testing framework	2016-12	https://webstore.iec.ch/publication/59623
ISO/IEC 20005:2013 Information technology - Sensor networks - Services and interfaces supporting collaborative information processing in intelligent sensor networks	2013-07	https://www.iso.org/standard/50952.html?browse=tc
(Updated) ISO/IEC 20924:2021 RLV Redline version Internet of Things (IoT) - Vocabulary	2021-03 (Withdrawn)	https://webstore.iec.ch/publication/66217
ISO/IEC 21823-1:2019 Interoperability for internet of things systems -- Part 1: Framework	2019-02	https://webstore.iec.ch/publication/60604
ISO/IEC 21823-2:2020 Internet of Things (IoT) - Interoperability for IoT systems - Part2 : Transport interoperability	2020-04	https://webstore.iec.ch/publication/61085
ISO/IEC 21823-3:2021 Internet of Things (IoT) - Interoperability for IoT systems - Part 3: Semantic interoperability	2021-02	https://webstore.iec.ch/publication/61088

Title	Date	Weblink
ISO/IEC 21823-4:2022 Internet of Things (IoT) - Interoperability for IoT systems - Part 4: Syntactic interoperability	2022-03	https://webstore.iec.ch/publication/65649
(Updated) ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships - Part 3: Guidelines for hardware, software, and services supply chain security	2023-06	https://www.iso.org/standard/82890.html
ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines	2022-06	https://www.iso.org/standard/44373.html
(Updated) ISO/IEC 27404 Information technology — Security techniques — Universal cybersecurity labelling framework for consumer IoT	Under development - Last accessed month: 2025-02	https://www.iso27001security.com/html/27404.html
ISO/IEC 29182-1:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 1: General overview and requirements	2013-06	https://webstore.iec.ch/publication/11411
ISO/IEC 29182-2:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 2: Vocabulary and terminology	2013-06	https://webstore.iec.ch/publication/11412
ISO/IEC 29182-3:2014 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 3: Reference architecture views	2014-02	https://webstore.iec.ch/publication/11413
ISO/IEC 29182-4:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 4: Entity models	2013-07	https://webstore.iec.ch/publication/11414
ISO/IEC 29182-5:2013 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 5: Interface definitions	2013-07	https://webstore.iec.ch/publication/11415
ISO/IEC 29182-5:2013 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 6: Applications	2014-07	https://webstore.iec.ch/publication/11416
ISO/IEC 29182-7:2015 Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 7: Interoperability guidelines	2015-02	https://webstore.iec.ch/publication/21827
ISO/IEC 30101:2014 Information technology -- Sensor networks: Sensor network and its interfaces for smart grid system	2014-11	https://webstore.iec.ch/publication/11540
ISO/IEC 30128:201 Information technology -- Sensor networks -- Generic Sensor Network Application Interface	2014-11	https://webstore.iec.ch/publication/11545

Title	Date	Weblink
ISO/IEC 30140-1:2018 Information technology - Underwater acoustic sensor network (UWASN) - Part 1: Overview and requirements	2018-02	https://webstore.iec.ch/publication/60609
ISO/IEC 30140-2:2017 Information technology - Underwater acoustic sensor network (UWASN) - Part 2: Reference architecture	2017-10	https://webstore.iec.ch/publication/60610
ISO/IEC 30140-3:2018 Information technology - Underwater Acoustic Sensor Network (UWASN) - Part 3: Entities and interfaces	2018-07	https://webstore.iec.ch/publication/60611
ISO/IEC 30140-4:2018 Information technology - Underwater Acoustic Sensor Network (UWASN) - Part 4: Interoperability	2018-07	https://webstore.iec.ch/publication/60612
(Updated) ISO/IEC 30141:2018 Internet of things and related technologies	2020-08	https://webstore.iec.ch/publication/60606
ISO/IEC 30142:2020 Internet of Things (IoT) - Underwater acoustic sensor network (UWASN) - Network management system overview and requirements	2020-06	https://webstore.iec.ch/publication/62443
ISO/IEC 30143:2020 Internet of Things (IoT) - Underwater acoustic sensor network (UWASN) - Application profiles	2020-06	https://webstore.iec.ch/publication/62405
ISO/IEC 30144:2020 Internet of things (IoT) - Wireless sensor network system supporting electrical power substation	2020-10	https://webstore.iec.ch/publication/62503
ISO/IEC 30146:2019 Information technology - Smart city ICT indicators	2019-10	https://www.iso.org/standard/70302.html
ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes	2021-05	https://webstore.iec.ch/publication/62644
ISO/IEC 30149 ED1 Internet of Things (IoT) - Trustworthiness Principles	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www/f?p=103:38:6519395980104::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23104432
ISO/IEC 30161:2020 Internet of things (IoT) - Data exchange platform for IoT services - Part 1: General requirements and architecture	2020-11	https://webstore.iec.ch/publication/63404
ISO/IEC 30161-1:2020 Internet of things (IoT) - Data exchange platform for IoT services - Part 1: General requirements and architecture	2020-11	https://webstore.iec.ch/publication/63404
(Updated) ISO/IEC 30161-2 Information technology — Internet of Things (IoT) — Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points	2024-05	https://webstore.iec.ch/publication/67281

Title	Date	Weblink
ISO/IEC 30162:2022 Internet of things (IoT) - Compatibility requirements and model for devices within Industrial IoT systems	2022-02	https://webstore.iec.ch/publication/63489
ISO/IEC 30162:2022 Internet of Things (IoT) - Compatibility requirements and model for devices within Industrial IoT systems	February 2022	https://webstore.iec.ch/publication/63489
ISO/IEC 30163:2021 Internet of Things (IoT) - System requirements of IoT and sensor network technology-based integrated platform for chattel asset monitoring	March 2021	https://webstore.iec.ch/publication/63491
ISO/IEC 30163:2021 System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services	2021-03	https://www.iso.org/standard/53283.html
ISO/IEC 30165:2021 Internet of things (IoT) - Real-time IoT framework	2021-07	https://webstore.iec.ch/publication/63972
ISO/IEC 30169 Information technology — Internet of Things (IoT) — IoT applications for electronic label system (ELS)	2022-05	https://webstore.iec.ch/publication/66659
ISO/IEC 30171-1 Information technology — Internet of Things (IoT) — Base-station based Underwater Wireless Acoustic Network (B-UWAN) – Part 1: Overview and requirements	2022-05	https://webstore.iec.ch/publication/66927
(Updated) ISO/IEC TR 30172 Information technology — Internet of Things (IoT) — Digital twin – Use Cases	2023-01	https://www.iec.ch/ords/f?p=103:38:411250985150323:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104881
ISO/IEC 30177 ED1 Internet of Things (IoT) - Underwater network management system (U-NMS) interworking	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-wf?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104960
ISO/IEC 30178 ED1 Internet of Things (IoT) - Data format, value and coding	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-wf?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104965
(Updated) ISO/IEC 30179 ED1 Internet of Things (IoT) - Overview and general requirements of IoT system for ecological environment monitoring	2023-01	https://www.iec.ch/dyn/www-wf?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,105254
ISO/IEC 30180 ED1 Internet of Things (IoT) - Functional requirements to determine the status of self-quarantine through Internet of Things data interfaces	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-wf?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,106630

Title	Date	Weblink
ISO/IEC 30181 ED1 Internet of Things (IoT) – Functional architecture for resource ID interoperability	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:204774363295796:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108552
ISO/IEC 30182:2017 Smart city concept model — Guidance for establishing a model for data interoperability	2017-05	https://www.iso.org/standard/53302.html
ISO/IEC 30183 ED1 Internet of Things (IoT) – Addressing interoperability guidelines between heterogeneous underwater sensor networks (UWASNs) based on underwater delay and disruption tolerant network (U-DTN)	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:204774363295796:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108553
(Updated) ISO/IEC CD 27402.2 Cybersecurity — IoT security and privacy — Device baseline requirements	2023-11	https://www.iso.org/standard/80136.html
(Updated) ISO/IEC CD 27403.2 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	2024-06	https://www.iso.org/standard/78702.html
(Updated) ISO/IEC DIS 24392 Cybersecurity — Security reference model for industrial Internet platform (SRM- IIP)	2023-07	https://www.iso.org/standard/78703.html
(Updated) ISO/IEC DIS 27071 Cybersecurity — Security recommendations for establishing trusted connections between devices and services	2023-07	https://www.iso.org/standard/56572.html
ISO/IEC ISO 20140-5:2017 Automation systems and integration - Evaluating energy efficiency and other factors of manufacturing systems that influence the environment - Part 5: Environmental performance evaluation data	2017-04	https://webstore.iec.ch/publication/34147
(Updated) ISO/IEC TR 30194 Internet of Things (IoT) and digital twin – Best practices for use case projects - ISO/IEC PWI JTC1-SC41-6 Guidance for IoT and Digital Twin use cases	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:204774363295796:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104897
ISO/IEC PWI JTC1-SC41-7 Digital Twin – Maturity model	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:204774363295796:::F-SP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108352
ISO/IEC PWI JTC1-SC41-8 Internet of Things (IoT) - Behavioral and policy interoperability	Under development - Last accessed month: 2025-02	https://www.iec.ch/ords/f?p=103:38:204774363295796:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108353
ISO/IEC TR 22417:2017 Information technology - Internet of things (IoT) - IoT use cases	2017-11	https://www.iso.org/standard/73148.html?browse=tc

Title	Date	Weblink
ISO/IEC TR 22417:2017 Information technology - Internet of things (IoT) - IoT use cases	2017-11	https://webstore.iec.ch/publication/60605
ISO/IEC TR 22560:2017 Information technology - Sensor network - Guidelines for design in the aeronautics industry: Active air-flow control	2017-10	https://webstore.iec.ch/publication/60608
ISO/IEC TR 30148:2019 Internet of things (IoT) - Application of sensor network for wireless gas meters	2019-10	https://webstore.iec.ch/publication/63562
ISO/IEC TR 30148:2019 Internet of things (IoT) - Application of sensor network for wireless gas meters	2019-10	https://webstore.iec.ch/publication/63562
ISO/IEC TR 30164:2020 Internet of Things (IoT) - Edge computing	2020-04	https://webstore.iec.ch/publication/62522
ISO/IEC TR 30166:2020 Internet of Things (IoT) - Industrial IoT	2020-04	https://webstore.iec.ch/publication/64321
ISO/IEC TR 30167:2021 Internet of Things (IoT) - Underwater communication technologies for IoT	2021-06	https://webstore.iec.ch/publication/65619
ISO/IEC TR 30174:2021 Internet of Things (IoT) - Socialized IoT system resembling human social interaction dynamics	2021-11	https://webstore.iec.ch/publication/66419
ISO/IEC TR 30176:2021 Internet of Things (IoT) - Integration of IoT and DLT/ blockchain: Use cases	2021-11	https://webstore.iec.ch/publication/66420
ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications	2017-10	https://www.iso.org/standard/64140.html
(Updated) ISO/IEC TS 30168 Information technology — Internet of Things (IoT) — Generic Trust Anchor Application Programming Interface for Industrial IoT Devices	2024-05	https://webstore.iec.ch/en/publication/66553
(NEW) ISO/IEC 18045:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation	2022-08	https://www.iso.org/standard/64140.html
(NEW) ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model	2022-08	https://www.iso.org/standard/72891.html
(NEW) ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components	2022-08	https://www.iso.org/standard/72892.html

Title	Date	Weblink
(NEW) ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components	2022-08	https://www.iso.org/standard/72906.html
(NEW) ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities	2022-08	https://www.iso.org/standard/72913.html
(NEW) ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	2022-08	https://www.iso.org/standard/72917.html
(NEW) ISO/IEC TR 40141- Internet of Things (IoT) – Reference architecture guidance	Under development - Last accessed month: 2025-02	https://www.iec.ch/dyn/www-w/f?p=103:38:16526658145347:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,126453
(NEW) ISO/IEC ISO/IEC 20924:2024 Internet of Things (IoT) and digital twin - Vocabulary	2024-02	https://webstore.iec.ch/en/publication/70408
(NEW) ISO/IEC ISO/IEC 30161-2:2023 Internet of Things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points	2023-03	https://webstore.iec.ch/en/publication/68295
(NEW) ISO 5231:2022 Extended farm management information systems data interface (EFDI) — Concept and guidelines	2022-10	https://www.intertekinform.com/en-gb/standards/itu-t-y-sup-pl-76-09-2023--1344020_saig_itu_itu_3342182/
(NEW) ISO/IEC 27400 – AWI TS 5689 Cybersecurity - Security frameworks based on the conceptual model of cyber-physical systems	Under development - Last accessed month: 2025-02	https://www.iso.org/standard/87375.html
(Updated) ISO/IEC AWI 21823-5 Internet of Things (IoT) - Behavioral and policy interoperability	Under development - Last accessed month: 2025-02	https://www.iso.org/standard/90177.html
(NEW) ITU Standards Landscape - IoT & Smart Sustainable Cities	N/A	https://www.itu.int/het4/itu-t/landscape/#?topic=0.78&workgroup=1&searchValue=&page=1&sort=Relevance
ITU ITU-T Study Group 20 ITU-T - SG20 - Internet of things (IoT) and smart cities and communities (SC&C)	N/A	https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx
ITU-T Y.4208 Internet of things requirements for support of edge computing	2020-01	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14162

Title	Date	Weblink
ITU X.1303 bis Secure applications and services – Emergency communications: Common Alerting Protocol Version 1.2	2014-03	https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/T-REC-X1303bis-201403-.pdf
ITU-T F.749.1 (11/2015) Functional requirements for vehicle gateway	2015-11	https://handle.itu.int/11.1002/1000/12631
ITU-T F.749.2 (03/2017) Service requirements for vehicle gateway platforms	2017-03	https://handle.itu.int/11.1002/1000/13183
ITU-T G.9959 Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications	2015-01	https://www.itu.int/rec/T-REC-G.9959-201501-I/en
ITU-T H.560 (12/2017) Communications interface between external applications and a Vehicle Gateway Platform	2017-12	https://handle.itu.int/11.1002/1000/13435
ITU-T H.821 (04/2017) Conformance of ITU-T H.810 personal health system: Healthcare information system interface	2017-04	https://handle.itu.int/11.1002/1000/13200
ITU-T H.831 (01/2015) Conformance testing: WAN Interface Part 1: Web services interoperability: Sender	2015-01	https://handle.itu.int/11.1002/1000/12249
ITU-T H.832 (01/2015) Conformance testing: WAN Interface Part 2: Web services interoperability: Receiver	2015-01	https://handle.itu.int/11.1002/1000/12250
ITU-T H.833 (01/2015) Conformance testing: WAN Interface Part 3: SOAP/ATNA: Sender	2015-01	https://handle.itu.int/11.1002/1000/12251
ITU-T H.834 (01/2015) Conformance testing: WAN Interface Part 4: SOAP/ATNA: Receiver	2015-01	https://handle.itu.int/11.1002/1000/12252
ITU-T H.835 (01/2015) Conformance testing: WAN Interface Part 5: PCD-01 HL7 Messages: Sender	2015-01	https://handle.itu.int/11.1002/1000/12253
ITU-T H.836 (01/2015) Conformance testing: WAN Interface Part 6: PCD-01 HL7 Messages: Receiver	2015-01	https://handle.itu.int/11.1002/1000/12254
ITU-T H.837 (01/2015) Conformance testing: WAN Interface Part 7: Consent Management: Sender	2015-01	https://handle.itu.int/11.1002/1000/12255
ITU-T H.841 (08/2020) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 1: Optimized Exchange Protocol: Personal Health Device	2020-08	https://handle.itu.int/11.1002/1000/14344
ITU-T H.842 (11/2019) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 2: Optimized Exchange Protocol: Personal Health Gateway	2019-11	https://handle.itu.int/11.1002/1000/14116

Title	Date	Weblink
ITU-T H.843 (08/2018) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 3: Continua Design Guidelines: Personal Health Device	2018-08	https://handle.itu.int/11.1002/1000/13680
ITU-T H.844 (11/2019) Conformance of ITU-T H.810 personal health system: Personal Health Devices interface Part 4: Continua Design Guidelines: Personal Health Gateway	2019-11	https://handle.itu.int/11.1002/1000/14117
ITU-T L.1221 (11/2018) Innovative energy storage technology for stationary use - Part 2: Battery	2018-11	https://handle.itu.int/11.1002/1000/13721
ITU-T L.1222 (05/2018) Innovative energy storage technology for stationary use - Part 3: Supercapacitor technology	2018-05	https://handle.itu.int/11.1002/1000/13579
(Updated) ITU-T L.1370 (11/2018) Sustainable and intelligent building services	2018-11	https://handle.itu.int/11.1002/1000/13724
ITU-T L.1371 (06/2020) A methodology for improving, assessing and scoring the sustainability performance of office buildings	2020-06	https://handle.itu.int/11.1002/1000/14304
ITU-T L.1383 (10/2021) Smart energy for cities and home applications	2021-10	https://handle.itu.int/11.1002/1000/14719
ITU-T Q.3952 (01/2018) The architecture and facilities of Model network for IoT testing	2018-01	https://handle.itu.int/11.1002/1000/13489
ITU-T Q.4060 (10/2018) The structure of the testing of heterogeneous Internet of things gateways in a laboratory environment	2018-10	https://handle.itu.int/11.1002/1000/13700
ITU-T Q.4062 (09/2020) Framework for IoT Testing	2020-09	https://handle.itu.int/11.1002/1000/14387
ITU-T Q.4063 (09/2020) Framework for testing identification systems used in Internet of things	2020-09	https://handle.itu.int/11.1002/1000/14391
ITU-T Y Suppl. 27 (01/2016) ITU-T Y.4400 series – Smart Sustainable Cities – Setting the framework for an ICT architecture	2016-01	https://handle.itu.int/11.1002/1000/12753
ITU-T Y Suppl. 28 (01/2016) ITU-T Y.4550 series – Smart Sustainable Cities – Integrated management for smart sustainable cities	2016-01	https://handle.itu.int/11.1002/1000/12754
ITU-T Y Suppl. 29 (01/2016) ITU-T Y.4250 series – Smart Sustainable Cities – Multi-service infrastructure in new-development areas	2016-01	https://handle.itu.int/11.1002/1000/12755

Title	Date	Weblink
ITU-T Y Suppl. 30 (01/2016) ITU-T Y.4250 series – Smart Sustainable Cities – Overview of smart sustainable cities infrastructure	2016-01	https://handle.itu.int/11.1002/1000/12756
ITU-T Y.4000/Y.2060 (06/2012) Overview of Internet of Things	2012-06	https://handle.itu.int/11.1002/1000/11559
ITU-T Y.4001/F.748.2 (11/2015) Overview and reference model of machine socialization	2015-11	https://handle.itu.int/11.1002/1000/12621
ITU-T Y.4002/F.748.3 (11/2015) Relation management and descriptions for machine socialisations	2015-11	https://handle.itu.int/11.1002/1000/12622
ITU-T Y.4100/Y.2066 (06/2014) Common requirements of Internet of Things	2014-06	https://handle.itu.int/11.1002/1000/1269
ITU-T Y.4101/Y.2067 Common requirements and capabilities of gateways for IoT applications	2017-10	https://handle.itu.int/11.1002/1000/13384
ITU-T Y.4102/Y.2074 (01/2015) Requirements for Internet of Things devices and operation of Internet of Things applications during disaster	2015-01	https://handle.itu.int/11.1002/1000/12421
ITU-T Y.4111/Y.2076 (02/2016) Semantic related requirements and framework of the Internet of Things	2016-02	https://handle.itu.int/11.1002/1000/12705
ITU-T Y.4112/Y.2077 (02/2016) Requirements of the Plug and Play Capability of the IoT	2016-02	https://handle.itu.int/11.1002/1000/12706
ITU-T Y.4113 (09/2016) Requirements of the network for the Internet of Things	2016-09	https://handle.itu.int/11.1002/1000/13025
ITU-T Y.4115 (04/2017) Reference architecture for IoT device capabilities exposure	2017-04	https://handle.itu.int/11.1002/1000/13266
ITU-T Y.4116 Requirements of transportation safety services including use cases and service scenarios	2017-10	https://handle.itu.int/11.1002/1000/13385
ITU-T Y.4117 (10/2017) Requirements and capabilities of Internet of Things for support of wearable devices and related services	2017-10	https://handle.itu.int/11.1002/1000/13386
ITU-T Y.4118 (06/2018) Internet of Things requirements and technical capabilities for support of accounting and charging	2018-06	https://handle.itu.int/11.1002/1000/13496
ITU-T Y.4121 (06/2018) Requirements for an Internet of Things enabled network for support of applications for global processes of the Earth	2018-06	https://handle.itu.int/11.1002/1000/13636
ITU-T Y.4201 (02/2018) High-level requirements and reference framework of smart city platforms	2018-02	https://handle.itu.int/11.1002/1000/13388

Title	Date	Weblink
ITU-T Y.4203 (02/2019) Requirements of things description in the Internet of things	2019-02	https://handle.itu.int/11.1002/1000/13857
ITU-T Y.4206 (06/2019) Requirements and capabilities of user-centric work space service	2019-06	https://handle.itu.int/11.1002/1000/13919
ITU-T Y.4401/Y.2068 (03/2015) Functional framework and capabilities of the internet of things	2015-03	https://handle.itu.int/11.1002/1000/12419
ITU-T Y.4411/Q.3052 (02/2016) Overview of application programming interfaces and protocols for M2M service layer	2016-02	https://handle.itu.int/11.1002/1000/12698
ITU-T Y.4412/F.747.8 (11/2015) Requirements and reference architecture for audience-selectable media service framework in the IoT environment	2015-11	https://handle.itu.int/11.1002/1000/12620
ITU-T Y.4413/F.748.5 (11/2015) Requirements and reference architecture of M2M service layer	2015-11	https://handle.itu.int/11.1002/1000/12623
ITU-T Y.4415 (06/2018) Architecture of web of objects based virtual home network	2018-06	https://handle.itu.int/11.1002/1000/13637
ITU-T Y.4416 Architecture of the Internet of Things based on next generation network evolution	2018-06	https://handle.itu.int/11.1002/1000/13638
ITU-T Y.4417 (06/2018) Framework of self-organization network in the IoT environments	2018-06	https://handle.itu.int/11.1002/1000/13639
ITU-T Y.4418 (06/2018) Functional architecture of gateway for Internet of things applications	2018-06	https://handle.itu.int/11.1002/1000/13640
ITU-T Y.4451 (09/2016) Framework of constrained node networking in the IoT environments	2016-09	https://handle.itu.int/11.1002/1000/13026
ITU-T Y.4452 (09/2016) IoT application support models of the Internet of Things	2016-09	https://handle.itu.int/11.1002/1000/13027
ITU-T Y.4453 Adaptive software framework for IoT devices	2016-09	https://handle.itu.int/11.1002/1000/13028
ITU-T Y.4457 (06/2018) Architectural framework for transportation safety service	2018-06	https://handle.itu.int/11.1002/1000/13641
ITU-T Y.4461 (01/2020) Framework of Open Data in Smart Cities	2020-01	https://handle.itu.int/11.1002/1000/14164
ITU-T Y.4466 (01/2020) Framework of smart greenhouse service	2020-01	https://handle.itu.int/11.1002/1000/14169
ITU-T Y.4553 Requirements of smartphone as sink node for IoT applications and services	2016-03	https://handle.itu.int/11.1002/1000/12779

Title	Date	Weblink
ITU-T Y.4702 (03/2016) Common requirements and capabilities of device management in IoT	2016-03	https://handle.itu.int/11.1002/1000/12780
ITU-T Y.4801/F.748.1 (10/2014) Requirements and common characteristics of IoT identifier for IoT service	2014-10	https://handle.itu.int/11.1002/1000/12229
ITU-T Y.4805 (08/2017) Identifier service requirements for the interoperability of Smart City applications	2017-08	https://handle.itu.int/11.1002/1000/13267
ITU-T Y.4908 (12/2020) Performance evaluation frameworks of e-health systems in the Internet of things	2020-12	https://handle.itu.int/11.1002/1000/14425
(NEW) ITU-T L.1333 : Carbon data intensity for network energy performance monitoring	2022-09	https://www.itu.int/rec/T-REC-L.1333-202209-I
(NEW) ITU-T L.1410 : Methodology for environmental life cycle assessments of information and communication technology goods, networks and services	2014-12	https://www.itu.int/rec/T-REC-L.1410-201412-I/en
(NEW) ITU-T L.1480 : Enabling the Net Zero transition: Assessing how the use of information and communication technology solutions impact greenhouse gas emissions of other sectors	2022-12	https://www.itu.int/rec/T-REC-L.1480-202212-I
(NEW) ITU-T Y.4226 (ex Y.isms): Functional framework and requirements for disaster monitoring system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17882
(NEW) ITU-T Y.4505 (ex Y.MIM): Minimal Interoperability Mechanisms for smart and sustainable cities and communities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18458
(NEW) ITU-T Y.4506 (ex Y.DRI-arch): Reference architecture for the interworking of autonomous urban delivery robots	Under development - Last accessed month: 2025-02	https://www.itu.int/rec/T-REC-L.1480-202212-I
(NEW) ITU-T Y.4705 (ex Y.nmm-isms) : Metadata model of sensing capability for disaster monitoring system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17883
(NEW) ITU-T Y.dtmv-if : Interface model and its requirements of integrating virtual and physical worlds through digital twins for the metaverse	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19592
(NEW) ITU-T Y.dtmv-ref :Reference model of integrating virtual and physical worlds through digital twins for the metaverse	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19591

Title	Date	Weblink
(NEW) ITU-T Y.dtmv-reqts: Requirements of integrating virtual and physical worlds through digital twins for the metaverse	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19590
(NEW) ITU-T YSTR.ACC-SCC : Guidelines on developing ICT services for accessible smart cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18454
(NEW) ITU-T Y.4222 (ex Y.smart-evacuation) : Framework of smart evacuation in a disaster or emergency in smart cities and communities	Under development - Last accessed month: 2025-02: Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17886
(NEW) ITU-T Y.4227 (ex Y.IoT-BC-reqts-cap): oT requirements and capabilities for support of blockchain	Under development - Last accessed month: 2025-02: Approved on 2024-08-29	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17932
(NEW) ITU-T Y.4228 (ex Y.IIoT-infra-SM-fr) : Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing	Under development - Last accessed month: 2025-02: Approved on 2024-08-29	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17949
(NEW) ITU-T Y.4229 (ex Y.IoT-SFFS) : Requirements and reference functional model of IoT-based smart forest firefighting system	Under development - Last accessed month: 2025-02: Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17955
(NEW) ITU-T Y.4230 (ex Y.EV-charging) : Requirements and capability framework of public smart charging service for electric vehicles	Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17954
(NEW) ITU-T Y.4231 (ex Y.IoT-Vreqs) : Requirements and capability framework of the internet of things for vision	Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17953
(NEW) ITU-T Y.4232 (ex Y.IoT-RTPS) : Requirements, capabilities and use cases of Internet of Things infrastructures in roadside traffic perception system	Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18461
(NEW) ITU-T Y.4233 (ex Y.FSPH): Framework for smart public health emergency management in smart and sustainable cities	Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18460
(NEW) ITU-T Y.4234 (ex Y.RemoteEd) : Requirements, capabilities and deployment models for e-learning in remote classrooms	Determined on 2024-07-12	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18751

Title	Date	Weblink
(NEW) ITU-T Y.4420-rev : ramework of Internet of things based monitoring and management for Lift	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19606
(NEW) ITU-T Y.ACC-ASM : Requirements and capabilities of accessible service management using user accessibility preference profile for IoT services	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19057
(NEW) ITU-T Y.ACC-IoTMV : Accessibility requirements for metaverse services supporting IoT	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19599
(NEW) ITU-T Y.DEMC-fra : Requirements and framework of IoT-based distributed energy resources management and control services	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19607
(NEW) ITU-T Y.dt-IWCS : Requirements and capability framework of digital twin for intelligent water conservancy system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18459
(NEW) ITU-T Y.dt-PAF : Requirements and capabilities of a digital twin for pedestrian accessibility facilities for persons with disabilities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19600
(NEW) ITU-T Y.dt-SComCam: ommon requirements and capability framework of digital twin for smart complex and campus	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18750
(NEW) ITU-T Y.EMM-Reqts: CRequirements for Real-Time Event Monitoring and Integrated Management in Smart City Platforms	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17952
(NEW) ITU-T Y.energy-storage : Requirements and capability framework of energy storage service for residential community in smart city	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18749
(NEW) ITU-T Y.EV-PUD : Requirements of electric vehicle power usage data acquisition and management for smart city	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19062
(NEW) ITU-T Y.IoT-APS-Reqts : Requirements and capability framework of Internet of Things for support of application-aware service	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19605
(NEW) ITU-T Y.IoT-PDP: Requirements of electric power data perception based on the Internet of Things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19061
(NEW) ITU-T Y.IoT-smartschool: Requirements of IoT-based smart school management system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19059

Title	Date	Weblink
(NEW) ITU-T Y.IoT-soil : Requirements of IoT-based soil environmental protection and remediation	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19058
(NEW) ITU-T Y.LASS-fra : Requirements and capability framework of IoT-based low-altitude sensing system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19601
(NEW) ITU-T Y.PGComNet-Reqts : Requirements of IoT-based power grid communication network	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18748
(NEW) ITU-T Y.SCCNS-Reqts: Requirements of smart city communication network system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19603
(NEW) ITU-T Y.SCGMS : Requirements and capabilities of IoT-based smart crop growth monitoring system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19602
(NEW) ITU-T Y.Sup.EdgeIoT-usecases : Supplement to ITU-T Y.4208 - Use cases of edge computing based Internet of Things	Under development	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19063
(NEW) ITU-T Y.Sup.SmartAqua-usecases :ITU-T Y.4000-series - Use cases of IoT-based smart aquaculture	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18753
(NEW) ITU-T Y.Sup-datainterop-usecases : Supplement to ITU-T Y.4563 - Use cases of data interoperability in Internet of things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19608
(NEW) ITU-T Y.Sup-IoT-BC : Applicability cases of blockchain in the IoT	Under developemnet	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19060
(NEW) ITU-T Y.Sup-SCC-AI : Supplement to ITU-T Y.4223 - Use cases of smart cities and communities supported by AI	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19604
(NEW) ITU-T IYSTR.Ambient IoT :Analysis on requirements and use cases of ambient power-enabled IoT	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18752
(NEW) ITU-T Y.4417-Rev : Framework of self-organization networking in Internet of things environments	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19610
(NEW) ITU-T Y.4477-Rev : Framework for service interworking with device discovery and management in heterogeneous Internet of things environments	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19064

Title	Date	Weblink
(NEW) ITU-T Y.4480Rev0 : Low power protocol for wide area wireless networkss	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18747
(NEW) ITU-T Y.4496 (ex Y.RA-PHE) : Requirements and reference architecture of smart service for public health emergency	Under development - Last accessed month: 2025-02	http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17921
(NEW) ITU-T Y.4501 (ex Y.RA-SDL) :Functional architecture for smart door lock service framework	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17926
(NEW) ITU-T Y.4502 (ex Y.IoT-SQMS): Requirements and functional architecture of IoT sensing quality management service	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17937
(NEW) ITU-T Y.4507 (ex Y.arc-psfws) : A functional architecture of power supply facilities warning system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18746
(NEW) ITU-T Y. EPWS-fc: Functional capabilities to support IoT-based electric power work site operation services	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19613
(NEW) ITU-T Y.AI-DECCS : Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17929
(NEW) ITU-T Y.cnce-IoT-arch :unctional architecture of network capability exposure for smart hospital based on Internet of things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17894
(NEW) ITU-T Y.DT-CS : Requirements and functional architecture for blockchain-based sustainable and cooperative digital-twin creation system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19611
(NEW) ITU-T Y.DTS-arch : Architecture of the digital twin system in power grid	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19612
(NEW) ITU-T Y.Fram-ssdp : Requirements and framework of metaverse simulation service for disaster prevention in electric power facilities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19614
(NEW) ITU-T Y.IoT-BoT-peer: Capability and functional architecture of blockchain of things peers	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17936
(NEW) ITU-T Y.IoT-CMP-VR : Functional framework and capabilities of coordination management platform for IoT based vehicle-road	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19615

Title	Date	Weblink
(NEW) ITU-T Y.IoT-CONV-fr : Convergence framework for enhancement of service intelligence based on Internet of Things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17958
(NEW) ITU-T Y.IoT-DPE : Management framework for IoT-based distributed power equipment	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18745
(NEW) ITU-T Y.IoT-ESSB : Functional architecture of IoT-based energy-saving service for smart buildings	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19616
(NEW) ITU-T Y.IoT-ISP : Reference framework for the smart industry service platform based blockchain and IoT	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19065
(NEW) ITU-T Y.IoT-MVarch : Functional architecture of the IoT-based machine vision system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19620
(NEW) ITU-T Y.IoT-NCM-arch : Functional architecture of network connectivity management in the Internet of things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18462
(NEW) ITU-T Y.IoT-SAS : Functional architecture of IoT-enabled smart accessibility service in smart communities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19617
(NEW) ITU-T Y.IoT-SPA : Functional architecture of smart park based on Internet of Thingsg	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19067
(NEW) ITU-T Y.NCE.arch.EIoT : Functional architecture enhancement with network capability exposure to support flexible QoS/QoE requirements from enterprise IoT services and applications	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17934
(NEW) ITU-T Y.RA-FML: Requirements and reference architecture of IoT and smart city & community service based on federated machine learning	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17924
(NEW) ITU-T Y.SA-DSC-SSC : System architecture of digital supply chain for smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19618
(NEW) ITU-T Y.SC-DESMS : Functional architecture of IoT-based distributed energy storage management system in smart cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19609

Title	Date	Weblink
(NEW) ITU-T Y.SFPP : Reference framework for the smart farmland production platform	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19066
(NEW) ITU-T Y.smart-PBRS : Functional Architecture of Smart Power Bank Rental Service Framework	Under development - Last accessed month: 2025-02	https://www.itu.int/rec/T-REC-L.1333-202209-I
(NEW) ITU-T Y.Sup.IoT-CONV (ex YSTR. IoT-CONV) : Overview of IoT Convergence	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17959
(NEW) ITU-T Y.Sup.IoT-SEDR : Functional framework and capability for digital resources in smart education based on IoT	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19069
(NEW) ITU-T Y.Sup.VFS : Functional architecture of connected vehicle formation supporting based on edge computing	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19070
(NEW) ITU-T Y.Sup_SUPS : TU-T Y.4456 - Functional architecture of IoT based smart underground parking services	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19619
(NEW) ITU-T YSTR.SemComm. IoT : rchitectural Framework for Semantic Communication Services for IoT and Smart City & Community	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17960
(NEW) ITU-T Y.4463 : Framework of delegation service for Internet of things devices	2024-08	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19073
(NEW) ITU-T Y.4499 (ex Y.UIM-cs-framework) : Framework of urban infrastructure monitoring based on crowdsourcing	2024-07	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17944
(NEW) ITU-T Y.4503 (ex Y.IoT-CRE-fr) : Framework of common rule enablement for intelligent IoT services in heterogeneous IoT platform environments	2024-08	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18466
(NEW) ITU-T Y.4504 (ex Y.SF-prediction) : Service framework of prediction for intelligent IoT	2024-08	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18465
(NEW) ITU-T Y.4508 (ex Y.DPM-alm-fra) : Functional requirements and architecture of blockchain-based activity logs management for IoT data processing and management	2024-07	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18467
(NEW) ITU-T Y.4706 (ex Y.dem-IoT) :Data exchange model for IoT devices in power transmission and transformation equipment	2024-07	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18743

Title	Date	Weblink
(NEW) ITU-T Y.AIoT-dfs-arc : Reference architecture of data fusion service in artificial intelligence of things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19626
(NEW) ITU-T Y.AIoT-dpsm:Requirements and framework of data processing for smart manufacturing with Artificial Intelligence of Things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19627
(NEW) ITU-T Y.AIoT-fr :Framework of Artificial Intelligence of Things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19624
(NEW) ITU-T Y.AIoT-FRA : Functional requirements and architecture for Artificial Intelligence of Things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19625
(NEW) ITU-T Y.cii (ex Y.rrm-data) : Requirements and reference model of data collected from city infrastructure	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17900
(NEW) ITU-T Y.CL-EDM : Energy data model for city-level energy management platform	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18463
(NEW) ITU-T Y.CSDL : Requirements and framework for crowdsourced system based on distributed learning	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18744
(NEW) ITU-T Y.DM-SLF : Conceptual data model of smart livestock farming service	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18470
(NEW) ITU-T Y.DSE-LISF :Reference architecture of data sharing and exchange based on lightweight intelligent software framework for Internet of things devices	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19630
(NEW) ITU-T Y.EDSS : Framework and requirements of electricity data sharing system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19632
(NEW) ITU-T Y.Interop-DPM : Integrated Interoperability framework for Data Processing and Management	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19633
(NEW) ITU-T Y.IoT-3DMS : Requirements and functional capabilities for three-dimensional model based monitoring service	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19072

Title	Date	Weblink
(NEW) ITU-T Y.IoT-IIEC : Framework of the integrated intelligent IoT service based on multi edge computing	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19628
(NEW) ITU-T Y.IoT-IWAT : Framework of interworking with agent-based transportation for intelligent IoT services	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19629
(NEW) ITU-T Y.KCI-IM : Requirements of knowledge construction and implementation for IoT management	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19631
(NEW) ITU-T Y.metadata-EPI (ex Y.Sup. metadata-EPI) : Metadata for IoT-based electric power infrastructure monitoring system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19074
(NEW) ITU-T Y.MIMbased-arch : MIM-based Architectural framework for interoperability in support of data sharing ecosystems	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19634
(NEW) ITU-T Y.SmartBuilding-Integration : Framework for Smart Building Integration into Smart Cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19071
(NEW) ITU-T Y.SPDM-reqts : Requirements and a reference model of data for Smart Pest and Disease Management (SPDM) service	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19636
(NEW) ITU-T YSTR.dscm : Analysis of data sharing control models	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18468
(NEW) ITU-T YSTR.GenAI-Sem-Interop : Implications of Generative Artificial Intelligence on Semantic Interoperability for Data Use	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19635
(NEW) ITU-T Y.CIP : Requirements of metaverse-based emergency response in chemical industrial parks	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19637
(NEW) ITU-T YSTR.DIC : Reference framework for distributed intelligent computing based on IoT	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19638/en
(NEW) ITU-T Y.bsis-sec : Security requirements and capabilities of base station inspection services using unmanned aerial vehicles	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19640
(NEW) ITU-T Y.iepi-dm-sa : ramework of security assessment for data management for IoT-based electric power infrastructure	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19081

Title	Date	Weblink
(NEW) ITU-T Y.IoT-acs-fra : Functional requirements and architecture of access control service of IoT platform enabled by zero trust technology in decentralized environments	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18740
(NEW) ITU-T Y.IoT-IADS :Intelligent anomaly detection system for Internet of things	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19643
(NEW) ITU-T Y.IoT-Smartcity-Risk : Reference framework of cybersecurity risk management of IoT ecosystems on smart cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17916
(NEW) ITU-T Y.Sec-outdoor-EPI : Security requirements and capability of IoT Management platform for outdoor electric power infrastructure	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19075
(NEW) ITU-T Y.Sup.access-sec : Supplement to ITU-T Y.4221 - Use cases and security requirements for sensing devices to access IoT-based electric power infrastructure monitoring system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19641
(NEW) ITU-T Y.Sup.SRS-SR : Supplement to ITU-T Y.4120 - Security threats and requirements of IoT applications for smart retail stores	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19642
(NEW) ITU-T Y.Supp-Imp-CSIAD : Supplement to ITU-T Y.4811 - Implementation of converged service for identification and authentication for IoT devices in decentralized environment	Under development - Last accessed month: 2025-02	https://www.itu.int/rec/T-REC-L.1410-201412-I/en
(NEW) ITU-T Y.uas-dc-fr : Framework of unified authentication service for data collaboration in IoT-based electric power infrastructure	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19083
(NEW) ITU-T YSTR.IoT-IMS : Identification management service of IoT device	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18473
(NEW) ITU-T Y.DT-SSC-CVP : Classification of visualization precision levels for digital twin systems in smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19645
(NEW) ITU-T Y.Evaluation-dfp : Quality evaluation framework of data as a factor of production for smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19644
(NEW) ITU-T Y.Evaluation-SE : Evaluation of capabilities for IoT-enabled frameworks of smart education	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19086

Title	Date	Weblink
(NEW) ITU-T Y.Highway-KPI : Key performance indicators of ICT based highway traffic safety assessment	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18476
(NEW) ITU-T Y.IoT-BEMS-af : Assessment framework of IoT infrastructure in building energy management system	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19088
(NEW) ITU-T Y.KHI-PE :Key health indicators and evaluation model for power equipment in Smart Sustainable Cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18742
(NEW) ITU-T Y.KPEM-SM : Key performance evaluation models of smart manufacturing	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18474
(NEW) ITU-T Y.KPI-Flood : Key Performance Indicators of ICT based Urban Flood Disaster Prevention and Mitigation Capability	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17963
(NEW) ITU-T Y.QE-DMI-SSC : Quality evaluation of digital models in industry for smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18475
(NEW) ITU-T Y.SNPG-ref : Reliability evaluation frameworks of sensing network in power grid	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19646
(NEW) ITU-T Y.SSC-NGUM : A Methodology for Next Generation Urban Measurements	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17914
(NEW) ITU-T Y.Sup.MM-EDMC-SSC: Maturity model of digital management capability of industrial equipment used in smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18741
(NEW) ITU-T Y.Sup-NGUM : Use Cases for Next Generation Urban Measurements	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17915
(NEW) ITU-T Y.Sup-Proc-SSC :Procurement guidelines for smart sustainable cities	Under development - Last accessed month: 2025-02	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19089
ITU-T Y Suppl. 76 Use cases of Internet of things-based smart agriculture	2023-09	https://www.intertekinform.com/en-gb/standards/itu-t-y-sup-pl-76-09-2023--1344020_saig_itu_itu_3342182/
LAAS-CNRS Eclipse OM2M Eclipse OM2M v1.4.1 - Open-Source platform for M2M communication	2012-02	https://www.eclipse.org/om2m/

Title	Date	Weblink
LAAS-CNRS Node-Red IDE-OM2M Node-Red IDE-OM2M V1.0.2: A framework for the rapid development of IoT applications using the OM2M platform through Node-RED	2018-08	https://www.npmjs.com/package/node-red-contrib-ide-iot
(Updated) NGI-0 Discovery NEUROPIL	Under development - Last accessed month: 2025-02	https://gitlab.com/pi-lar/neuropil
(Updated) NGI-Fed4Fire COMPUTATION OFFLOADING FOR IOT-ENABLED APPLICATIONS	Under development - Last accessed month: 2025-02	https://www.fed4fire.eu/index.html
NGI-Ontochain ADOS (AirTrace Decentralized Oracle System)	Under development - Last accessed month: 2025-02	https://ontochain.ngi.eu/content/ados
(Updated) NGI-Trust B-Smart	Under development - Last accessed month: 2025-02	https://things.is/
NGI-Trust D-SBOM (Distributed Software Bill of Materials)	Under development - Last accessed month: 2025-02	https://www.trublo.eu/d-sbom/
NGI-Trust EDGE-TINC	Under development - Last accessed month: 2025-02	https://edge-tinc.gitlab.io/fluentic/
(Updated) NGI-Trust IZI	Under development - Last accessed month: 2025-02	https://github.com/mizolotu/izi
NGI-Trust PY	Under development - Last accessed month: 2025-02	https://www.panga.fr/
NGI-Trust PY 2.0	Under development - Last accessed month: 2025-02	https://www.pyguard.fr/
NGI-Trust Totem	Under development - Last accessed month: 2025-02	https://insigh.io/
OASIS Advanced Message Queuing Protocol (AMQP) TC	N/A	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp
OASIS Message Queuing Telemetry Transport (MQTT) TC	N/A	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt

Title	Date	Weblink
OASIS CAP-v1.2 Common Alerting Protocol Version 1.2	2010-07	http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html
OGC 12-006 Sensor Observation Service	2012-04	https://www.ogc.org/standards/sos#overview
OGC 17-079r1 OGC SensorThings API Part 2 – Tasking Core	2019-01	http://docs.opengeospatial.org/is/17-079r1/17-079r1.html
OGC 18-088 OGC SensorThings API Part 1: Sensing Version 1.1	2021-08	https://docs.ogc.org/is/18-088/18-088.html
(NEW) OMA IPSO IPSO Smart Object Guidelines	2024-09	https://omaspecworks.org/develop-with-oma-specworks/ipso-smart-objects/guidelines/
(NEW) OMA IPSO Repo Public IPSO Repository	2024-09	https://technical.openmobilealliance.org/OMNA/LwM2M/LwM-2MRegistry.html
OMA ObjLwM2M_5GNR_Conn LIGHTWEIGHTM2M 5GNR CONNECTIVITY	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_5GNR_Conn/V1_0-20201110-A/
OMA ObjLwM2M_ACL LIGHTWEIGHTM2M ACCESS CONTROL	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_ACL/V1_1-20201110-A/
OMA ObjLwM2M_APN_Conn LIGHTWEIGHTM2M APN CONNECTION PROFILE	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_APN_Conn/V1_1-20201110-A/
OMA ObjLwM2M_Bearer_Conn LIGHTWEIGHTM2M BEARER SELECTION	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Bearer_Conn/V1_1-20201110-A/
OMA ObjLwM2M_Cell_Conn LIGHTWEIGHTM2M CELLULAR CONNECTIVITY	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Cell_Conn/V1_1-20201110-A/
OMA ObjLwM2M_Conn_Mon LightweightM2M Connectivity Monitoring	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Mon/V1_3-20201110-A/
OMA ObjLwM2M_Conn_Stat LightweightM2M Connectivity Statistics	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Stat/V1_0_5-20201110-A/
OMA ObjLwM2M_COSE LightweightM2M COSE	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_COSE/V1_0-20201110-A/
OMA ObjLwM2M_Device LightweightM2M Device	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Device/V1_2-20201110-A/
OMA ObjLwM2M_Firmware LightweightM2M Firmware Update	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Firmware/V1_1-20201110-A/
OMA ObjLwM2M_Gateway LightweightM2M Gateway	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Gateway/V1_0-20201110-A/

Title	Date	Weblink
OMA ObjLwM2M_Location LightweightM2M Location	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Location/V1_0_3-20201110-A/
OMA ObjLwM2M_MQTT_Server LightweightM2M MQTT Server	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_MQTT_Server/V1_0-20201110-A/
OMA ObjLwM2M_OSCORE LightweightM2M OSCORE	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_OSCORE/V2_0-20211123-A/
OMA ObjLwM2M_Routing LightweightM2M Routing	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Routing/V1_0-20201110-A/
OMA ObjLwM2M_Security LightweightM2M Security	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Security/V1_2-20201110-A/
OMA ObjLwM2M_Server LightweightM2M Server	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_Server/V1_2-20201110-A/
OMA ObjLwM2M_WLAN_Conn LightweightM2M WLAN Connectivity	2020-11	https://www.openmobilealliance.org/release/ObjLwM2M_WLAN_Conn/V1_1-20201110-A/
OMA-AD-CPNS-V1_1-20160209-A Converged Personal Network Service Architecture	2016-02	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-AD-CPNS-V1_1-20160209-A.pdf
OMA-AD-DM-V2_0-20160209-A Device Management Architecture	2016-02	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-AD-DM-V2_0-20160209-A.pdf
OMA-AD-FUMO-V1_0-20070209-A Firmware Update Management Object Architecture	2007-02	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-AD-FUMO-V1_0-20070209-A.pdf
OMA-AD-GwMO-V1_1-20170725-A Gateway Management Object Architecture	2017-07	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-AD-GwMO-V1_1-20170725-A.pdf
OMA-AD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Architecture	2016-01	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-AD-OpenCMAPI-V1_0-20160126-A.pdf
OMA-ERELD-CPNS-V1_1-20160209-A Enabler Release Definition for Converged Personal Network Service	2016-02	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-ERELD-CPNS-V1_1-20160209-A.pdf
OMA-ERELD-DM-V2_0-20160209-A Enabler Release Definition for OMA Device Management	2016-02	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-ERELD-DM-V2_0-20160209-A.pdf
OMA-ERELD-FUMO-V1_0_4-20090828-A Enabler Release Definition for Firmware Update Management Object	2009-08	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-ERELD-FUMO-V1_0_4-20090828-A.pdf

Title	Date	Weblink
OMA-ERELED-GwMO-V1_1-20170725-A Enabler Release Definition for Gateway Management Object (GwMO)	2017-07	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-ERELED-GwMO-V1_1-20170725-A.pdf
(Duplicated-remove Updated) OMA-ERELED-LightweightM2M-V1_2-20201110-A Enabler Release Definition for LightweightM2M	2020-11	https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-ERELED-LightweightM2M-V1_2-20201110-A.pdf
OMA-ERELED-LWM2M_BinaryAppDataCont-V1_0_1-20190221-A Enabler Release Definition for Lwm2M BinaryAppDataCont	2019-02	https://www.openmobilealliance.org/release/Lwm2M_APPDATA/V1_0_1-20190221-A/OMA-ERELED-LWM2M_BinaryAppDataCont-V1_0_1-20190221-A.pdf
OMA-ERELED-LWM2M_Gateway-V1_1-20210518-A Enabler Release Definition for LWM2M Gateway	2021-05	https://www.openmobilealliance.org/release/Lwm2M_Gateway/V1_1-20210518-A/OMA-ERELED-LWM2M_Gateway-V1_1-20210518-A.pdf
OMA-ERELED-OpenCMAPI-V1_0-20160126-A Enabler Release Definition for Open Connection Manager API	2016-01	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-ERELED-OpenCMAPI-V1_0-20160126-A.pdf
OMA-ER-GotAPI-V1_1-20180724-A Generic Open Terminal API Framework (GotAPI)	2018-07	https://www.openmobilealliance.org/release/GOTAPI/V1_1-20180724-A/OMA-ER-GotAPI-V1_1-20180724-A.pdf
OMA-ETS-LightweightM2M_INT-V1_1-20190912-D Enabler Test Specification (Interoperability) for Lightweight M2M	2019-08	https://www.openmobilealliance.org/release/LightweightM2M/ETS/OMA-ETS-LightweightM2M-V1_1-20190912-D.pdf
OMA-EVP-LightweightM2M-V1_0-20140819-C Enabler Validation Plan for Lightweight M2M	2014-08	https://www.openmobilealliance.org/release/LightweightM2M/EVP/OMA-EVP-LightweightM2M-V1_0-20140819-C.pdf
OMA-RD-CPNS-V1_1-20160209-A Converged Personal Network Service Requirements	2016-02	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-RD-CPNS-V1_1-20160209-A.pdf
OMA-RD-DM-V1_2-20070209-A Device Management Requirements	2007-02	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-RD-DM-V1_2-20070209-A.pdf
OMA-RD-DM-V2_0-20160209-A Device Management Requirements	2016-02	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-RD-DM-V2_0-20160209-A.pdf
OMA-RD-ENCAP-M-V1_0-20180621-A Exposing Network Capabilities to M2M Requirements	2018-06	https://www.openmobilealliance.org/release/ENCAP/V1_0-20180621-A/OMA-RD-ENCAP-M-V1_0-20180621-A.pdf
OMA-RD-GwMO-V1_1-20170725-A GwMO Requirements	2017-07	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-RD-GwMO-V1_1-20170725-A.pdf

Title	Date	Weblink
OMA-RD-LightweightM2M-V1_2-20201110-A OMA Lightweight Machine to Machine Requirements	2020-11	https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-RD-LightweightM2M-V1_2-20201110-A.pdf
OMA-RD-M2MInterface-V1_0-20150324-A Management Interface for M2M Requirements	2015-03	https://www.openmobilealliance.org/release/M2Minterface/V1_0-20150324-A/OMA-RD-M2MInterface-V1_0-20150324-A.pdf
OMA-RD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Requirements	2016-01	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-RD-OpenCMAPI-V1_0-20160126-A.pdf
OMA-RRELD-ENCAp-M2M-V1_0-20180621-A Reference Release Definition for for Exposing Network Capabilities to M2M	2018-06	https://www.openmobilealliance.org/release/ENCAp/V1_0-20180621-A/OMA-RRELD-ENCAp_M2M-V1_0-20180621-A.pdf
OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A Reference Release Definition for M2M Device Classification	2012-10	https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A.pdf
OMA-RRELD-M2Minterface-V1_0-20150324-A Reference Release Definition for M2Minterface	2015-03	https://www.openmobilealliance.org/release/M2Minterface/V1_0-20150324-A/OMA-RRELD-M2Minterface-V1_0-20150324-A.pdf
OMA-TS-CPNS_Core-V1_1-20160209-A Converged Personal Network Service Core Technical Specification	2016-02	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-TS-CPNS_Core-V1_1-20160209-A.pdf
OMA-TS-DM_Protocol-V2_0-20160209-A OMA Device Management Protocol	2016-02	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-TS-DM_Protocol-V2_0-20160209-A.pdf
OMA-TS-DM-FUMO-V1_0_2-20090828-A Firmware Update Management Object	2009-08	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-TS-DM_FUMO-V1_0_2-20090828-A.pdf
OMA-TS-DM-GwMO_ZigBeeMO-V1_0-20170725-A Management Objects for ZigBee Devices	2017-07	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO_ZigBeeMO-V1_0-20170725-A.pdf
OMA-TS-GwMO-V1_1-20170725-A Gateway Management Object Technical Specification	2017-07	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO-V1_1-20170725-A.pdf
(New) OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A Lightweight Machine to Machine Technical Specification: Core	2024-06	https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A.pdf

Title	Date	Weblink
(New) OMA-TS-LightweightM2M_ Transport-V1_2_2-20240613-A Lightweight Machine to Machine Technical Specification: Transport Bindings	2024-06	https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-TS-LightweightM2M_Transport-V1_2_2-20240613-A.pdf
OMA-TS-LWM2M_ BinaryAppDataContainer-V1_0_1-20190221-A Lightweight M2M – Binary App Data Container	2019-02	https://www.openmobilealliance.org/release/LwM2M_APPDATA/V1_0_1-20190221-A/OMA-TS-LWM2M_BinaryAppDataContainer-V1_0_1-20190221-A.pdf
OMA-TS-LWM2M_Gateway-V1_1-20210518-A Lightweight Machine to Machine Gateway Technical Specification	2021-05	https://www.openmobilealliance.org/release/LwM2M_Gateway/V1_1-20210518-A/OMA-TS-LWM2M_Gateway-V1_1-20210518-A.pdf
OMA-TS-OpenCMAPI-V1_0-20160126-A Open Connection Manager API	2016-01	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-TS-OpenCMAPI-V1_0-20160126-A.pdf
OMA-WP-M2M_Device_Classification-20121030-A White Paper on M2M Device Classification	2012-10	https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-WP-M2M_Device_Classification-20121030-A.pdf
OMA-AD-CPNS-V1_1-20160209-A Converged Personal Network Service Architecture	2016-02	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-AD-CPNS-V1_1-20160209-A.pdf
(NEW) OMA-ERELD- LightweightM2M-V1_2_2-20240613 Enabler Release Definition for LightweightM2M	2024-06	https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-ERELD-LightweightM2M-V1_2_2-20240613-A.pdf
(NEW) one6G 6G & Robotics: Use Cases and Potential Service Requirements	2023-6	https://one6g.org/download/3287/
(NEW) one6G 6G & Robotics: A Methodology to identify Potential Service Requirements for 6G-empowered Robotic Use Cases	2023-11	https://one6g.org/download/3962/?tmstv=1699546970
(NEW) one6G 6G & Robotics: Identifying Use Cases and Potential Service Requirements - Methodology and Examples	2024-06	https://one6g.org/download/4571/?tmstv=1717576666
(NEW) one6G 6G & eHealth: Use Cases and Potential Service Requirements	2024-09	https://one6g.org/download/5016/?tmstv=1725618580
oneM2M ETSI TR 118 502 V1.0.0 Architecture Part 1: Analysis of the architectures proposed for consideration	2015-04	https://www.etsi.org/deliver/etsi_tr/118500_118599/118502/01.00.00_60/tr_118502v010000p.pdf
oneM2M ETSI TR 118 524 V2.0.0 3GPP Release 13 Interworking	2016-09	https://www.etsi.org/deliver/etsi_tr/118500_118599/118524/02.00.00_60/tr_118524v020000p.pdf
oneM2M TR-0001-V2.4.1 oneM2M - Use Case collection	2016-08	https://www.onem2m.org/images/files/deliverables/Release2/TR-0001-Use_Cases_Collection-V2.4.1.pdf

Title	Date	Weblink
oneM2M TR-0001-V4.3.0 oneM2M - Use Case collection	2018-10	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28153
oneM2M TR-0012-V2.0.0 End-to-End Security and Group Authentication	2016-8	https://onem2m.org/images/files/deliverables/Release2/TR-0012-End-to-End-Security-and-Group-Authentication-V2_0_0.pdf
oneM2M TR-0016-V-2.0.0 Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies	2016-08	https://onem2m.org/images/files/deliverables/Release2/TR-0016-Authorization-Architecture-and-Access-Control-Policy-V2_0_0.pdf
oneM2M TR-0017-V2.0.0 Home Domain Abstract Information Model	2016-8	https://onem2m.org/images/files/deliverables/Release2/TR-0017-Home-Domain-Abstract-Information-Model-V2_0_0.pdf
oneM2M TR-0018-V-4.0.0 Industrial Domain Enablement	2019-09	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=29334
oneM2M TR-0022-V2.0.0 Continuation & integration of HGI Smart Home activities	2016-08	https://onem2m.org/images/files/deliverables/Release2/TR-0022-Continuation-and-Integration-of-HGI-Smart-Home-activities-V2_0_0.pdf
oneM2M TR-0024-V4.3.0 – ETSI TR 118 524 V2.0.0 3GPP Release 13 Interworking	2020-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31840
oneM2M TR-0033-Study_on_Enhanced_Semantic_Enablement-V4_5_0 Study on Enhanced Semantic Enablement	2019-10	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31093
oneM2M TR-0046-V-4.0.1 Study on Public Warning Service Enabler	2021-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/?docId=21832
oneM2M TR-0049-V-0.3.0 Industrial Domain Information Model Mapping & Semantics Support	2019-05	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30216
oneM2M TR-0055-3GPP_V2X_Interworking-V0_5_0 3GPP V2X Interworking	2019-07	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30468
oneM2M TR-0060-V-0.2.0 Study of action triggering enhancements	2020-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31865
oneM2M TR-0062-V-0.3.0 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)	2020-11	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33146

Title	Date	Weblink
oneM2M TR-0063-V-0.0.1 Effective IoT Communication to Protect 3GPP Networks	2019-11	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31370
oneM2M TR-0065 V0.1.0 oneM2M-SensorThings API interworking	2020-01	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34408
oneM2M TR-0066-V-0.3.0 System Enhancement to Support Data License Management (DLM)	2021-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33583
oneM2M TR-0067-V-0.2.0 Study on Management Object migration to SDT	2020-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33846
oneM2M TR-0068-V-0.2.0 AI enablement to oneM2M	2021-11	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34206
oneM2M TS-0001-V4.14.0 Functional Architecture	2022-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34648
(New) oneM2M TS-0002-V5.1.0 Requirements	2024-01	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36546
oneM2M TS-0003-V4.6.0 Security Solutions	2021-10	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34191
oneM2M TS-0004-V4.19.0 Service Layer Core Protocol	2024-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36773
oneM2M TS-0005-V4.0.0 Management Enablement (OMA)	2019-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30113
oneM2M TS-0006-V4.0.0 Management enablement (BBF)	2019-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30114
oneM2M TS-0008- V-4.5.0 CoAP Protocol Binding	2023-08	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36186
oneM2M TS-0009-V4.4.0 HTTP Protocol Binding	2022-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34550

Title	Date	Weblink
oneM2M TS-0011-V4.1.1 Common Terminology	2023-10	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36347
oneM2M TS-0012-V3.7.3 OneM2M Base Ontology	2019-02	https://www.onem2m.org/images/pdf/TS-0012-Base_Ontology-V3_7_3.pdf
oneM2M TS-0013-V3.3.1 Interoperability Testing	2021-09	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34003
oneM2M TS-0020-V4.0.0 WebSocket Protocol Binding	2022-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35387
oneM2M TS-0021-V2.0.1 oneM2M and AllJoyn Interworking	2018-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26333
oneM2M TS-0022-V4_5_0 Field Device Configuration	2023-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35590
oneM2M- TS-0023-V4.8.0 SDT based Information Model and Mapping for Vertical Industries	2021-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33779
oneM2M TS-0024-V4.0.0 OCF Interworking	2023-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35756
oneM2M TS-0026-V4.7.0 3GPP Interworking between oneM2M service layer and 3GPP features	2023-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33896
oneM2M TS-0034-V4.2.0 Semantics Support	2020-08	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31425
oneM2M TS-0037-V-4.0.2 IoT Public Warning Service Enablement	2023-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35597
oneM2M TS-0040-V4.0.0 Modbus Interworking	2022-11	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33896
oneM2M WI-0095 System enhancements to support Data Protection Regulations	2019-10	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30968

Title	Date	Weblink
oneM2M WI-0096 Effective IoT Communication to Protect 3GPP Networks	2021-01	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33091
oneM2M WI-0102 System enhancements to support Data License Management	2020-05	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32157
oneM2M WI-0104 V0_0_1 SDT based Information Model and Mapping for Vertical Industries – SIMVI	2021-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33391
oneM2M WI-0105 System enhancements to support AI capabilities	2023-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35882
oneM2M WI-0109 IPE-based Device Management with FlexContainers	2022-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34558
oneM2M-TR-0006-Study_of_Management_Capability_Enablement-V0_5_1 Study of Management Capability Enablement Technologies for Consideration	2015-04	https://onem2m.org/images/files/deliverables/TR-0006-Study_of_Management_Capability_Enablement-V0_5_1.doc
oneM2M-TR-0026-V-4.8.0 Vehicular Domain Enablement	2019-12	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31410
oneM2M-TR-0041-V-0.4.0 oneM2M Decentralized Authentication	2018-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26293
oneM2M -TR-0042-V-0.4.0 WoT Interworking	2018-05	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26945
oneM2M -TR-0043-V-0.3.0 Modbus Interworking	2023-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35844
oneM2M -TR-0044-V-0.6.0 Physical object heterogeneous identification and tracking in oneM2M	2020-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31631
oneM2M-TR-0050-V-0.13.0 Attribute Based Access Control Policy	2020-05	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32114

Title	Date	Weblink
oneM2M -TR-0053-V-0.6.0 Lightweight oneM2M Services	2020-03	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31776
oneM2M -TR-0054-V-0.8.0 oneM2M Service Subscribers and Users	2020-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32207
oneM2M -TR-0057-V-0.6.0 Getting Started with oneM2M	2021-02	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33407
oneM2M -TR-0058-V-0.0.1: Railway Domain Enablement	2018-12	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28240
oneM2M -TR-0059-V-0.2.0 oneM2M Services and Platforms Discovery	2019-06	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30111
oneM2M -TR-0061 -V-0.5.0 Study on ontologies for Smart City Services	2022-12	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=35482
oneM2M -TR-0064 ZigBee Interworking	2020-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32243
oneM2M-TS-0018-V-4.6.0 Test Suite Structure and Test Purposes	2022-04	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34702
oneM2M -TS-0036-V-0.0.1 Advanced Vehicular Domain Enablement	2017-11	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=24640
Open Group Reference Architectures and Open Group Standards for the Internet of Things	2016-12	https://publications.opengroup.org/w16d
Open Group IT4IT Open Messaging Interface (O-MI), The Open Group Standard for the Internet of Things (IoT), Version 2.0	2019-12	https://publications.opengroup.org/c19e
Open Group MSA-IoT Microservices Architecture for the Internet of Things (MSA-IoT)	2018-04	https://publications.opengroup.org/g187
Open Group O-DF Open Data Format (O-DF), The Open Group Standard for the Internet of Things (IoT), Version 2.0	2019-12	https://publications.opengroup.org/c19d
RIOT OS The friendly Operating System for the Internet of Things	2014-05	https://www.riot-os.org/

Title	Date	Weblink
SAE 6857 Requirements for a Terrestrial Based Positioning, Navigation, and Timing (PNT) System to Improve Navigation Solutions and Ensure Critical Infrastructure Security	2018-04	https://www.sae.org/standards/content/sae6857/
SAE AIR6988 Artificial Intelligence in Aeronautical Systems: Statement of Concerns	2021-04	https://www.sae.org/standards/content/air6988/
SAE ARINC686 Roadmap for IPv6 Transition in Aviation	2020-06	https://www.sae.org/standards/content/arinc686/
SAE ARINC687 Onboard secure Wi-Fi Network Profile Standard	2021-06	https://www.sae.org/standards/content/arinc687/
SAE ARINC688 Intersystem Network Integration	2021-06	https://www.sae.org/standards/content/arinc688/
SAE J2735 ASN1 V2X Communications Message Set Dictionary™ ASN file	2020-07	https://www.sae.org/standards/content/j2735asn_202007/
SAE J2735 V2X Communications Message Set Dictionary	2020-07	https://www.sae.org/standards/content/j2735_202007/
SAE J2931/7 Security for Plug-In Electric Vehicle Communications	2018-02	https://www.sae.org/standards/content/j2931/7_201802/
SAE J2945 Guidance Dedicated Short-Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts™	2017-12	https://www.sae.org/standards/content/j2945_201712/
SAE J2945/1 On-Board System Requirements for V2V Safety Communications	2020-04	https://www.sae.org/standards/content/j2945/1_202004/
SAE J2945/2 Dedicated Short-Range Communications (DSRC) Performance Requirements for V2V Safety Awareness	2018-10	https://www.sae.org/standards/content/j2945/2_201810/
UN P1095 E Negotiation	2022-01	https://uncefact.unece.org/display/uncefactpublic/E+Negotiation..
(Updated) W3C W3C Thing Description (TD) Ontology	2023-12	https://www.w3.org/2019/wot/td
W3C DID Decentralized Identifiers (DIDs) v1.0 (2021)	2022-07	www.w3.org/TR/did-core/
W3C JSON-LD 1.1 A JSON-based Serialization for Linked Data	2020-07	www.w3.org/TR/json-ld11/
W3C ODRL Information Model 2.2 Open Digital Rights Language (ODRL) Information Model 2.2	2018-02	www.w3.org/TR/odrl-model/
W3C OGC 16-079 W3C Semantic Sensor Network Ontology	2017-10	https://www.w3.org/TR/vocab-ssn/
W3C RDF Resource Description Framework (RDF) v1.1 (2014)	2014-02	www.w3.org/RDF/
W3C Verifiable Credentials Data Model v1.1 Verifiable Credentials Data Model v1.1 (2021)	2022-03	www.w3.org/TR/vc-data-model/

Title	Date	Weblink
(NEW) W3C Web of Things (WoT) Architecture 1.1	2023-12	https://www.w3.org/TR/wot-architecture11/
(NEW) W3C Web of Things (WoT) Thing Description 1.1	2023-12	https://www.w3.org/TR/wot-thing-description11/
(NEW) W3C Web of Things (WoT) Discovery	2023-12	https://www.w3.org/TR/wot-discovery/
WITSML WITSML (Well-site Information Transfer Standard Markup Language) 2.0 (2016)	2016-11	http://docs.energistics.org/WITSML/WITSML_TOPICS/WITSML-000-000-titlepage.html





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