Horizontal IIoT Standards Landscape

An Industry IoT Consortium Reference

2024-09-20

Authors

Claude Baudoin (cébé IT & Knowledge Management),

Erin Bournival (Dell Technologies)

CONTENTS

1 OVERVIEW

In a paper entitled "Global Industry Standards for Industrial IoT[1]," published in mid-2021, the Industry IoT Consortium's (IIC) Standards Task Group (STG) proposed the elements of a standards engagement strategy for providers and customers of industrial IoT (IIoT) solutions.

IIoT is a technology environment in which integration and interoperability are critical capabilities and the complexity of this environment makes this difficult to achieve. In the paper just mentioned, we stated that standards play a critical role in IIoT for five main reasons:

1. Avoid a proliferation of one-to-one interfaces to connect systems together
2. Achieve the integration of operational technology (OT) with enterprise systems that conform to IT standards, or within a system of systems
3. Avoid vendor lock-in by increasing the substitutability of components
4. Meet the requirements of regulatory agencies, which mandate standards to increase safety and security
5. Avoid the cost of training new employees on proprietary technologies.

We can add that incorporating standards-compliant products in a system can improve time-to-market, product quality, and development and maintenance costs by eliminating the development of custom new code.

Organizations (such as IIC members) must respond to these imperatives by defining a standards strategy and taking certain actions to execute it. These actions can be limited to identifying and adopting relevant standards, but they can also extend to active participation in the definition and evolution of those standards.

IIC does not develop standards, but works closely with SDOs, including through formal liaison agreements, to provide requirements, publish best practices for standards use, and construct testbeds and technology showcases to demonstrate standards-based capabilities.

The IIC STG published in August 2023 a paper entitled "Vertical Standards Landscape,"[2] which addressed the question of which standards (we listed 35 of them) are relevant to certain vertical industries as they design and deploy IIoT capabilities.

This paper is a similar landscape of "horizontal" standards, that is, standards that apply equally to many vertical industries. For example, data communications between sensors and IT systems, or data protection through encryption, are addressed by standards that are not vertical industry-

[1] *https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf*
[2] *https://www.iiconsortium.org/industry-iot-consortium-vertical-standards-landscape-paper-form/*

specific. The list of 37 standards (or standards series) that follow was compiled from IIC member submissions, from the authors' research, and from external sources such as the European Union Observatory of Standard (EUOS)[3] landscape, in particular the one about digital twins.[4]

The paper concludes with recommendations and with a call to submit additional or revised material for future updates. The standards landscape can change quickly, and the reader is urged to seek the latest status of the standards listed here, and search for new standards that may have emerged since the publication of this document.

1.1 About the Classification of Standards in this Document

Each entry for a standard indicates which aspect of IoT it pertains to, among the following:

- System Architecture
- Information Modeling and Management
- Communications/Networking
- Security and Trustworthiness
- Interoperability
- Analytics and AI
- General

Whether a standard is directly related to Industrial IoT is sometimes ambiguous. In general, we included in this section references that explicitly mention in their description one of the terms "IoT" (or "Internet of Things"), "sensors," "actuators," or "devices," or strongly suggest that the models, protocols, data formats, etc., contained in the standard were directly related to those concepts.

In addition, the word "standard" is used with different degrees of rigor by different organizations. For some, a document listing use cases, or a set of guidelines, is a standard. For others, a standard must include normative content – with "shall" and "should" verbs that compel the targeted audience to adopt certain models, architectures, formats, or protocols. Such normative standards are sometimes accompanied by certification programs to guarantee the compliance of a product or the skills of its developers. Deciding which documents qualify as standards for the purpose of this document is a somewhat subjective exercise.

Finally, the presence of a standard in this document is not a claim that it has achieved any specific level of adoption, or that it is correct or current, let alone that it is pre-eminent or superior to alternate standards with a similar scope, or "plays well with others." We leave it to the readers to assess the maturity and suitability of a standard for their own purposes.

[3] *https://www.standict.eu/euos*

[4] *https://www.standict.eu/landscape-analysis-report/landscape-digital-twins*

1.2 INDEX OF STANDARDS LISTED

Name	Reference/Source	Section
Compatibility Requirements and Model for Devices within Industrial IoT Systems	ISO/IEC 20162	2.5
Constrained Application Protocol (CoAP)	IETF	2.3
Context Information Management – NGSI-LD/oneM2M Interworking Proxy Proposal	ETSI GR CIM 022	2.3
Context Information Management (NGSI-LD) API	ETSI GS CIM 009	2.5
Cyber Security: Critical Security Controls for Effective Cyber Defence	ETSI TR 103 305	2.4
Cybersecurity – IoT Security and Privacy -- Guidelines	ISO/IEC 27400	2.4
Data Distribution Service for Real-Time Systems (DDS)	OMG	2.3
Data Exchange Platform for IoT	ISO/IEC 30161	2.5
DDS-Security	OMG	2.4
Digital Enhanced Cordless Telecommunications (DECT™)	ETSI TS 103 636	2.3
Functional Safety and AI Systems	ISO/IEC TR 5469	2.6
Generic Sensor Network Application Interface	ISO/IEC 30128	2.5
Integration of IoT Trustworthiness Activities in ISO/IEC/IEEE 15288 System Engineering Processes	ISO 30147	2.4
Internet of Things – Base Station Based Underwater Wireless Acoustic Network (B-UWAN)	ISO/IEC TR 30171	2.3
Internet of Things – Edge Computing	ISO/IEC TR 30164	2.1
Internet of Things – Generic Trust Anchor Application Programming Interface for Industrial IoT Devices	ISO/IEC TS 30168	2.4
Internet of Things – Trustworthiness Framework	ISO 30149	2.4
Internet of Things – Underwater Communication Technologies for IoT	ISO/IEC TR 30167	2.3
Interoperability for IoT Systems	ISO/IEC 21823	2.5
IoT Reference Architecture	ISO/IEC 30141	2.1
IoT Vocabulary	ISO 20924	2.7
Message Queuing Telemetry Transport (MQTT)	OASIS	2.3
Multi-Access Edge Computing	ETSI GS MEC	2.3

OPC Unified Architecture (OPC UA)	OPC Foundation	2.3
Real-time IoT Framework	ISO/IEC 30165	2.1
Security for Industrial Automation and Control Systems	ISA-62443	2.4
Sensor network reference architecture (SNRA)	ISO/IEC 29182	2.1
Sensor Network Testing Framework	ISO/IEC 19637	2.5
Services and Interfaces Supporting Collaborative Information Processing In Intelligent Sensor Networks	ISO/IEC 20005	2.5
Simple Electronic Notation for Sensor Reporting (SENSR)	OMG	2.2
Smart Application Reference Ontology (SAREF)	ETSI	2.2
Socialized IoT System Resembling Human Social Interaction Dynamics	ISO/IEC TR 30174	2.6
Underwater Acoustic Sensor Network (UWASN)	ISO/IEC 30140	2.1
Underwater Acoustic Sensor Network (UWASN) – Network Management System	ISO/IEC 30142	2.1
Underwater Network Management System (U-NMS) Internetworking	ISO/IEC 30177	2.5
Use cases for cross-domain data usability of IoT devices	ETSI TR 103 778	2.2
Web of Things	W3C	2.1

2 LIST OF HORIZONTAL IIOT STANDARDS

2.1 SYSTEM ARCHITECTURE

Source	World Wide Web Consortium (W3C)
Name	Web of Things
Date	April 2020
URL	*www.w3.org/WoT/documentation/*
Description	Describes interaction abstraction based on the "properties, events, and actions" paradigm. A *Thing Description* defines what a *Thing* can do and how to interact with it in a generalized and machine processable manner, with the specifics of the interaction being managed by a protocol binding to the particular *Thing* implementation.
Comments	Incompletely adopted. OGC SensorThings API is a competing standard in the smart city and smart agriculture domains. OPC-UA is a competing standard in the manufacturing and energy domains.
Documents	WoT Architecture: *www.w3.org/TR/2020/REC-wot-architecture-20200409/* WoT Thing Description: *www.w3.org/TR/2020/REC-wot-thing-description-20200409/* Use cases: *www.w3.org/TR/wot-usecases/*
Submitter	Kym Watson, Fraunhofer IOSB, *kym.watson@iosb.fraunhofer.de*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30165:2021, Real-time IoT framework
Date	July 2021
URL	*www.iso.org/standard/53285.html*
Description	Framework of a real-time IoT (RT-IoT) system, including RT-IoT system conceptual model based on domain-based IoT reference model defined in ISO/IEC 30141, and impacts of real-time parameters in terms of four viewpoints (time, communication, control, and computation).
Comments	Related to ISO/IEC 30141 IoT Reference Architecture
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 29182, Sensor Network Reference Architecture (SNRA) • Part 1: General overview and requirements • Part 2: Vocabulary and terminology • Part 3: Reference architecture views • Part 4: Entity models • Part 5: Interface definitions • Part 6: Applications • Part 7: Interoperability guidelines
Dates	2013 (parts 1, 2, 4, 5), 2014 (part 3, 6), 2015 (part 7)
URL	Part 1: *https://webstore.iec.ch/publication/11411* Part 2: *https://webstore.iec.ch/publication/11412* Part 3: *https://webstore.iec.ch/publication/11413* Part 4: *https://webstore.iec.ch/publication/11414* Part 5: *https://webstore.iec.ch/publication/11415* Part 6: *https://webstore.iec.ch/publication/11416* Part 7: *https://webstore.iec.ch/publication/21827*
Description	This suite of standards describes the characteristics of a sensor network and the organization of the entities that comprise such a network.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TR 30164:2020, Internet of Things – Edge Computing
Date	April 2020
URL	*https://webstore.iec.ch/publication/62522*
Description	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.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30140, Underwater Acoustic Sensor Network (UWASN) • Part 1: Overview and requirements • Part 2: Reference architecture • Part 3: Entities and interfaces • Part 4: Interoperability
Date	2017 (part 2), 2018 (part 1, 3, 4)
URL	Part 1: *https://webstore.iec.ch/publication/60609* Part 2: *https://webstore.iec.ch/publication/60610* Part 3: *https://webstore.iec.ch/publication/60611* Part 4: *https://webstore.iec.ch/publication/60612*
Description	This series of standards describes underwater acoustic sensor networks, their characteristics due the effects of propagation variability, and the main differences with terrestrial networks.
Comments	See ISO/IEC 30142 for the UWASN management system
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30142, Underwater acoustic sensor network (UWASN) – Network management system (U-NMS) • Part 1: Overview and requirements • Part 2: Underwater management information base (u-MIB)
Date	2020 (part 1), 2022 (part 2)
URL	Part 1: *https://webstore.iec.ch/publication/62443* Part 2: *https://webstore.iec.ch/publication/67519*
Description	This standard addresses the functions that support an UWASN, the entities required, the data about the communication between the elements, and the information base of the U-NMS.
Comments	Part 1 was published without a part number in its title, as a Part 2 was not expected at that time. It is called Part 1 in this entry for clarity.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) – ISO/IEC JTC 1/SC 41
Name	ISO/IEC 30141, IoT Reference Architecture
Date	2018
URL	*www.iec.ch/dyn/www/f?p=103:38:607668603953669::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104064*
Description	IoT Reference Architecture
Comments	Relates to/competes with/complements the IIC Reference Architecture (IIRA *https://www.iiconsortium.org/iira/*
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

2.2 Information Modeling and Management

Source	Object Management Group (OMG)
Name	SENSR (Simple Electronic Notation for Sensor Reporting)
Date	July 2022
URL	*https://www.omg.org/spec/SENSR/1.0/PDF*
Description	A metamodel for describing the form of serialized data streams emitted by sensors, and how that data should be interpreted by a client to derive the intended meaning of the data. The intent is that a manufacturer's sensor products can be characterized by a model expressed in the proposed metamodel. This specification does not concern itself with the transport, networking, or wire protocol for transmitting the data from the sensor to the client.
Comments	The SENSR specification was developed by OMG in response to the experiences of the members of the Industry IoT Consortium, particularly those involved in the implementation of the IIC Testbeds initiative.
Submitter	Claude Baudoin, cébé IT & Knowledge Management, *cbaudoin@cebe-itkm.com*

Source	European Telecommunications Standards Institute (ETSI)
Name	Smart Application Reference Ontology (SAREF)
Date	2020
URL	*https://saref.etsi.org/core/*
Description	The SAREF ontology is a shared model of consensus that facilitates the matching of existing assets in the smart applications domain. SAREF provides building blocks that allow separation and recombination of different parts of the ontology depending on specific needs. SAREF explicitly specifies recurring core concepts in the smart applications domain, the main relationships between these concepts, and axioms to constrain the usage of these concepts and relationships.
Submitter	None – was identified as part of ETSI standards review

Source	European Telecommunications Standards Institute (ETSI)
Name	ETSI TR 103 778 V1.1.1: Use cases for cross-domain data usability of IoT devices
Date	December 2021
URL	*www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf*
Description	Due to the growing use of AI models in standards, ETSI Technical Bodies have decided to investigate means to assess the “quality” and usability of datasets needed to train, and also to test the AI capabilities referenced by new standards, which is one of the motivations for this work. IoT devices and platforms also provide data that are used directly by human and very often non-technical users. Trust in the IoT system can be ensured only if these data bring in a real added-value and are delivered in a non-ambiguous manner to these users.
Submitter	European Union Observatory on Standards (listed in Digital Twin Landscape)

2.3 COMMUNICATIONS / NETWORKING

The standards listed in this section have specific relevance to, or were intentionally developed for, IoT systems. Many other communication protocols can be used in industrial IoT systems, but are not specific enough to be included here. These would include 5G mobile networks, protocols developed for low-bandwidth, low-power data collection in pre-IoT SCADA systems (LoRaWan, Sigfox, Zigbee, etc.), near-field communication (NFC), or the IEEE Time-Sensitive Network (TSN) standard,

Future revisions of this landscape may include additional communication standards if their inclusions are later deemed appropriate.

Source	OPC Foundation
Name	OPC Unified Architecture (OPC UA)
Date	2008
URL	*https://opcfoundation.org/developer-tools/documents/?type=Specification*
Description	The OPC Unified Architecture (UA) is a platform-independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework. This multi-layered approach accomplishes the original design specification goals of: • Functional equivalence: all COM OPC Classic specifications are mapped to UA • Platform independence: from an embedded micro-controller to cloud-based infrastructure • Secure: encryption, authentication, and auditing • Extensible: ability to add new features without affecting existing applications • Comprehensive information modeling: for defining complex information
Comments	For OPC Classic, see *https://opcfoundation.org/about/opc-technologies/opc-classic/*
Submitter	Claude Baudoin, cébé IT & Knowledge Management, *cbaudoin@cebe-itkm.com*

Source	Object Management Group (OMG)
Name	Data Distribution Service for Real-Time Systems® (DDS®)
Date	March 2015 (v1.4 of the core specification)
URL	*www.omg.org/spec/DDS/*

Description	DDS is the first open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems.
	DDS introduces a virtual Global Data Space where applications can share information by simply reading and writing data objects addressed by means of an application-defined name (Topic) and a key. DDS features fine and extensive control of QoS parameters, including reliability, bandwidth, delivery deadlines, and resource limits. DDS also supports the construction of local object models on top of the Global Data Space.
	DDS is a family of standards, which includes:
	• Core standard:
	  ○ DDS
	  ○ DDSI-RTPS (Real-time Publish-Subscribe Protocol DDS Interoperability Wire Protocol)
	  ○ DDS-XTypes (type system and serialized representation of DDS data)
	  ○ DDS-Security
	• Type syntax, based on the Interface Definition Language (DDL), and language mappings to C++, Java, and C#
	• APIs (C++ and Java)
	• Extensions
	  ○ DDS-RPC
	  ○ DDS-XML
	  ○ DDS-JSON)
	• Gateways and transports:
	  ○ DDS-WEB
	  ○ DDS-OPCUA Gateway
	  ○ DDS-XRCE *eXtreme Resource Constrained Environments)
	  ○ DDS-TSN (Time-Sensitive Networks)

Comments	DDS-Security has a separate entry in Section 2.4 of this report
Submitters	Claude Baudoin, cébé IT & Knowledge Management, *cbaudoin@cebe-itkm.com* Rajive Joshi, Real-Time Innovations, *rajive@rti.com*

Source	Organization for the Advancement of Structured Information Standards (OASIS)
Name	Message Queuing Telemetry Transport (MQTT)
Date	March 2019 (Version 5)
URL	*https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html*
Description	"MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth."
Comments	According to OASIS, "MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc." Readers will find multiple papers on the Internet about the pros and cons of MQTT compared to other protocols. The two issues that are raised the most often are (a) latency, due to the fact that data has to go through the cloud, and (b) the lack of built-in security. IoT system architects need to weigh these arguments in the context of their specific intended use.
Submitter	Chuck Byers, IIC, *byers@omg.org*

Source	European Telecommunications Standards Institute (ETSI)
Name	ETSI GR CIM 022: Context Information Management (CIM); NGSI-LD/oneM2M interworking proxy proposal
Date	December 2022
URL	*www.etsi.org/deliver/etsi_gr/CIM/001_099/022/01.01.01_60/gr_CIM022v010101p.pdf*
Description	Provides several NGSI-LD/oneM2M interworking proxy solutions using existing oneM2M features, and analyses those to find which one is suitable for a certain condition.
Comments	This is a group report, not a formal specification.
Submitter	None – was identified as part of ETSI standards review

Source	European Telecommunications Standards Institute (ETSI)
Name	Multi-access Edge Computing (MEC)
Date	Various (2022-2023)
URL	Committee page: *https://www.etsi.org/committee/1425-mec* Full list of standards (over 40 distinct documents): *www.etsi.org/standards-search#page=1&version=1&onApproval=1&published=1&sort=3&TB=826,,835,,874*
Description	ETSI's Industry Specification Group (ISG) on Multi-access Edge Computing (MEC) creates "a standardized, open environment allowing the efficient and seamless integration of applications from vendors, service providers, and third-parties across multi-vendor MEC platforms. […] We unite the telco and IT-cloud worlds, providing IT and cloud-computing capabilities within the Radio Access Network. Our work specifies the elements that are required to enable applications to be hosted in a multi-vendor multi-access edge computing environment. MEC also enables applications and services to be hosted 'on top' of the mobile network elements, i.e. above the network layer."
Comments	This family of standards and reports has been placed in this section, largely because the focus of ETSI is telecommunications, but the family of documents generated by the MEC initiative covers a wide range of topics. In addition to network-related standards, there are documents about terminology, a framework and reference architecture, use cases, the development lifecycle, service APIs, integration, and testing.
Submitter	Chuck Byers, IIC (*byers@omg.org*)

Source	Internet Engineering Task Force (IETF)
Name	Constrained Application Protocol (CoAP)
Date	June 2014
URL	*https://datatracker.ietf.org/doc/html/rfc7252*
Description	A specialized Internet application protocol for use between resource-constrained devices (e.g., limited in power or memory), such as wireless sensor nodes, hence the applicability to IoT and machine-to-machine (M2M) communication.
Comments	Various extensions have been proposed in RFCs 7641, 7959, 8323, and 8974.
Submitter	Chuck Byers, IIC, *byers@omg.org*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TR 30167:2021, Internet of Things (IoT) – Underwater communication technologies for IoT
Date	June 2021 (Edition 1.0)
URL	*https://webstore.iec.ch/publication/65619*
Description	"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: • technical overview of different communication technologies; • characteristics of different communication technologies; • trends of different communication technologies; • applications of each communication technology; • benefits and challenges of each communication technology.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TR 30171-1:2022, Internet of Things (IoT) – Base-station based underwater wireless acoustic network (B-UWAN) – Part 1: Overview and requirements
Date	March 2022 (Edition 1.0)
URL	*www.iso.org/standard/53291.html*
Description	"This document 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."
Comments	As of November 2023, the development of subsequent parts of this standard has not started
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	European Telecommunications Standards Institute (ETSI)
Name	Digital Enhanced Cordless Telecommunications (DECT™) – DECT-2020 New Radio standard series: • TS 103 636-1: Part 1 – Overview • TS 103 636-2: Part 2 – Radio reception and transmission requirements • TS 103 636-3: Part 3 – Physical layer • TS 103 636-4: Part 4 – MAC layer • TS 103 636-5: Part 5 – DLC and convergence layers
Date	January 2023
URL	*https://www.etsi.org/technologies/dect*
Description	DECT-2020 NR is developed to address the future digitalization needs and it is optimized for local area wireless applications, which can be deployed anywhere by anyone at any time. These technologies can be adapted for many applications supporting digitalization such as industry 4.0, utility and public services, audio and media industry use. Autonomous operation and device to device direct communication enable reliable communication networks. DECT-2020 NR supports a wide range of applications which could operate below 6 GHz frequencies in unlicensed and licensed spectrum.
Comments	Updates to each of the parts are in preparation as of November 2023. This standard is included because of the specific mention of Industry 4.0 applications.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

2.4 SECURITY AND TRUSTWORTHINESS

As was the case in the previous section, there are standards that help design and implement more secure systems, but which are generic across many applications, not just IoT. This is in particular the case of ISO/IEC 27001.

Similarly, it may be appropriate to implement device and server authentication mechanisms to ensure that an attacker cannot send data from a fake device, or that a device cannot send data, let alone receive commands, from a fake server used for a “man-in-the-middle” attack, which could be particularly destructive in an IoT system that controls a critical infrastructure. Furthermore, the data and commands being sent between IoT devices or gateways and application servers may need to be encrypted, for example to avoid industrial espionage. These measures will typically rely on cryptography techniques for which standards exist, but those are not specific to IoT per se.

Source	Object Management Group (OMG)
Name	DDS-Security v1.1
Date	July 2018
URL	*www.omg.org/spec/DDS-SECURITY/1.1/About-DDS-SECURITY*
Description	This specification defines the Security Model and Service Plugin Interface (SPI) architecture for compliant DDS implementations. The DDS Security Model is enforced by the invocation of these SPIs by the DDS implementation. This specification also defines a set of built-in implementations of these SPIs.
Comments	See Section 0 for a description of the broader family of DDS specifications.
Submitter	Claude Baudoin (*baudoin@omg.org*)

Source	International Society of Automation (ISA)/IEC
Name	ISA-62443: Security for Industrial Automation and Control Systems (multiple parts)
Dates	2007 to 2020
URL	*www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards*
Description	Requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). The ISA/IEC standards set cybersecurity benchmarks in all industry sectors that use IACS, including building automation, electric power generation and distribution, medical devices, transportation, and process industries such as chemicals and oil and gas.
Documents	See the “Quick start guide: An overview of the ISA/IEC 62443 Standards” (*https://gca.isa.org/isagca-quick-start-guide-62443-standards*) published by the ISA Global Security Alliance.
Submitter	European Union Observatory on Standards (listed in Digital Twin Landscape)

Source	European Telecommunications Standards Institute (ETSI)
Name	ETSI TR 103 305: Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence • Part 3: Internet of Things Sector
Date	July 2023 (Part 3), February 2023 (Part 5)
URL	*www.etsi.org/deliver/etsi_tr/103300_103399/10330503/03.01.01_60/tr_10330503v030101p.pdf*
Description	"[Provides] guidance on individually applying the most current version of the Critical Security Controls for effective cyber defence to IoT by enterprises."
Comments	"The Critical Security Controls are a prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. Under the auspices of the Center for Internet Security (CIS), the Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices."
Submitter	None – was identified as part of ETSI standards review.

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy – Guidelines
Date	June 2022
URL	*www.iso.org/standard/44373.html*
Description	"This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions."
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO)
Name	ISO 30149: Internet of Things – Trustworthiness framework
Date	Under development in ISO/IEC JTC 1/SC 41 as of December 2023
URL	*www.iso.org/standard/53269.html*
Description	IoT trustworthiness principles
Comments	Related to ISO/IEC 30141 and 30147
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TS 30168 ED1: Internet of Things (IoT) - Generic Trust Anchor Application Programming Interface for Industrial IoT Devices
Date	Under development. At "CDTS" stage as of 1 Dec 2023.
URL	*www.iec.ch/ords/f?p=103:38:706779384458419::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104067*
Description	ISO/IEC TS 30168:2021 specifies a generic programming interface for the integration of secure elements within Industrial IoT devices. This includes requirements from industrial usage scenarios and applications. This document also provides guidance for implementation, testing, and conformity validation.
Comments	The page at the above URL includes a link to the document for people who have IEC login credentials.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO)
Name	ISO 30147:2021 – Integration of IoT Trustworthiness Activities in ISO/IEC/IEEE 15288 System Engineering Processes
Date	May 2021
URL	*www.iso.org/standard/53267.html*
Description	System life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015.
Comments	The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.
Submitter	European Union Observatory on Standards (listed in Digital Twin Landscape)

2.5 INTEROPERABILITY

Source	European Telecommunications Standards Institute (ETSI)
Name	ETSI GS CIM 009: Context Information Management (NGSI-LD) API
Date	June 2023 (Information Model), November 2021 (API)
URL	*www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.05.01_60/gs_cim009v010501p.pdf*
Description	Defines a standard API for Context Information Management (NGSI-LD API) enabling close to real-time (right-time) access to context/digital twin information coming from many different sources (not only IoT data sources). The document defines how such an API enables applications to perform updates on context, register context providers which can be queried to get updates on context, query information on current and historic context information, and subscribe to receive notifications of context changes.
Comments	"NGSI" stands for Next Generation Service Interfaces, a 2012 suite of specifications from the Open Mobile Alliance (OMA). ETSI took over this work as part of its Industry Specification Group on Context Information Management (ETSI ISG CIM). "LD" refers to linked data. For more details, see *https://en.wikipedia.org/wiki/NGSI-LD*. NGSI-LD also has an information model specification, ETSI GS CIM 006, which is a generic specification about property graphs, not specifically related to IoT.
Submitter	None – was identified as part of ETSI standards review.

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 19637:2016 – Information technology – Sensor network testing framework
Date	December 2016
URL	*www.iso.org/standard/65576.html*
Description	ISO/IEC 19637:2016 specifies a testing framework for conformance test for heterogeneous sensor networks, generic services between a test manager (TMR) and test agent (TA) in the testing framework, and guidance for creating a testing platform and enabling the test of different sensor network protocols.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 20005:2013 Information technology – Sensor networks – Services and interfaces supporting collaborative information processing in intelligent sensor networks
Date	July 2013
URL	*www.iso.org/standard/50952.html*
Description	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.
Comments	Under review for potential updating as of December 2023
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30128:2014, Information technology – Sensor networks – Generic Sensor Network Application Interface
Date	November 2014
URL	*www.iso.org/standard/53248.html*
Description	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. The standard describes: • generic sensor network applications' operational requirements, • sensor network capabilities, • mandatory and optional interfaces between the application layers of service providers and sensor network gateways.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 21823 – Internet of Things (IoT) – Interoperability for IoT systems • Part 1: Framework • Part 2: Transport interoperability • Part 3: Semantic interoperability • Part 4: Syntactic interoperability
Date	Feb. 2019 (part 1), Apr. 2020 (part 2), Sep. 2021 (part 3), Mar. 2022 (part 4)
URL	Part 1: *c* Part 2: *www.iso.org/standard/80986.html* Part 3: *www.iso.org/standard/83752.html* Part 4: *www.iso.org/standard/84773.html*
Description	The framework (Part 1) enables IoT systems to be built in such a way that the entities of the IoT system can exchange information and mutually use the information in an efficient way. Five facets of interoperability are described: transport, semantic, syntactic, behavioral, and policy. Part 2 (transport interoperability) specifies a framework and requirements to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and among entities within an IoT system. Part 3 (semantic interoperability) includes ontology requirements, best practices, and guidance on how to use ontologies, cross-domain specification and formalization of ontologies, relevant IoT ontologies, use cases and service scenarios that exhibit requirements of semantic interoperability. Part 4 (syntactic interoperability) includes a principle and requirements to achieve syntactic interoperability among IoT systems that include IoT devices, and a framework for processes to develop information exchange rules related to IoT devices from the syntactic viewpoint.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30161, Internet of things (IoT) - Data exchange platform for IoT • Part 1: General requirements and architecture • Part 2: Transport interoperability between nodal points
Date	Nov. 2020 (part 1), Mar. 2023 (part 2)
URL	Part 1: *www.iso.org/standard/53281.html* Part 2: *www.iso.org/standard/86671.html*
Description	Part 1 specifies requirements for an IoT data exchange platform: • 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; • the IoT service implementation guideline for the IoT data exchange platform. Part 2 specifies the requirements, functional blocks, and operation mechanism for transport interoperability between nodal points in the IoT data exchange platform.
Comments	The term "nodal point" is not commonly used by IoT systems architects, and is not present in the IIC Vocabulary. ISO defines a nodal point in ISO/IEC 30161-1 as "a point that investigates routing information specified in communication protocols and relays data blocks according to such information." Most practitioners would probably use the term "router" instead.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30162:2022, Internet of Things (IoT) - Compatibility requirements and model for devices within Industrial IoT systems
Date	February 2022
URL	*www.iso.org/standard/53282.html*
Description	Network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of: • data transmission protocols interaction • distributed data interoperability & management • connectivity framework • connectivity transport • connectivity network • best practices and guidance to use in IIoT area.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC 30177 – Underwater Network Management System (U-NMS) Internetworking
Date	Under development. At “PCC” stage as of 15 Dec 2023.
URL	*www.iec.ch/dyn/www/f?p=103:38:5769322594295::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104960*
Description	Unavailable
Comments	The page at the above URL includes a link to the document for people who have IEC login credentials. Related to ISO/IEC 30142.
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

Note that a related standard, ISO/IEC 30185 (“Addressing Interoperability Between IPv6-Based Network and UWASN”) is under development but is not expected to be published before 2025. The interim working documents are only available to people with IEC login credentials.

2.6 Analytics and Artificial Intelligence

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TR 5469:2024, Artificial Intelligence -- Functional Safety and AI Systems
Date	January 2024.
URL	*www.iso.org/standard/81283.html*
Description	Describes the properties, related risk factors, available methods and processes relating to: • Use of AI inside a safety-related function to realize the functionality • Use of non-AI safety-related functions to ensure safety for an AI controlled equipment • Use of AI systems to design and develop safety related functions.
Comments	While this report's applicability is broader than IIoT systems, the presence of actuators in an IIoT environment is likely to create safety risks to which this standard applies.
Submitter	European Union Observatory on Standards (listed in Digital Twin Landscape)

Source	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
Name	ISO/IEC TR 30174:2021 – Internet of Things (IoT) – Socialized IoT system resembling human social interaction dynamics
Date	November 2021
URL	*www.iso.org/standard/53294.html*
Description	This Technical Report describes: • 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.; • socialized attributes, i.e. socialized network, socialized collaboration, and socialized services, which are derived from the key features; and • guidelines on how to use or apply the socialized attributes in the design and development of IoT systems.
Submitter	European Union Observatory on Standards (listed in Digital Twin Landscape)

Also see ETSI TR 103 778 V1.1.1 (use cases for cross-domain data usability of IoT devices) in Section 2.2, as this work aimed in part to "investigate means to assess the quality and usability of datasets needed to train" AI models.

2.7 GENERAL

Source	International Organization for Standardization (ISO)
Name	ISO 20924 – IoT Vocabulary
Date	2021 (version 2). Version 3 is under development as of mid-2023.
URL	*www.iec.ch/dyn/www/f?p=103:38:103381829090100::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,106310*
Description	Provides a definition of Internet of Things along with a set of terms and definitions.
Comments	Related to ISO/IEC 30141
Submitter	Erin Bournival, Dell Technologies, *erin.bournival@dell.com*

3 RECOMMENDATIONS AND NEXT STEPS

We have enumerated several standards that are eligible for use across various domains or industries. Readers of this paper are encouraged to identify matches between the content in this document and the work they are performing, to whenever possible leverage existing standards and avoid "reinventing the wheel." We listed the various benefits of using standards at the beginning of the Overview (Section 1). We recommend that you:

- review the use of standards in your own organization,
- provide feedback on your own initiatives and experiences in the use and development of standards to the IIC Standards Task Group,
- volunteer as a Liaison Officer between the standards development organizations you engage with and the IIC,
- suggest to the Standards Task Group new liaison opportunities with the standards development organizations you participate in, and
- participate in the evolution of this document.

This landscape report is a living document. Most IoT-related standards are recent, and several more are under development. The standards mentioned in this document are highly likely to be revised over the next few years. Readers should send new or revised entries to *iic-standards@iiconsortium.org* for inclusion in subsequent versions.

Annex A TEMPLATE FOR NEW ENTRIES

This template is provided for the convenience of reviewers of this document to facilitate the submission of additional entries with all appropriate descriptors.

The Comments and Documents rows may be omitted if there is no relevant information to place in them.

Source	Name of the SDO and/or technical committee
Name	
Date	
URL	Pointer to the actual standard if available
Description	May be cut-and-pasted from the standard's description page, or a summary created by the submitter
Comments	
Documents	Reference to additional documents besides the one whose URL is given above
Submitter	Name, affiliation, and e-mail address to facilitate follow-up

AUTHORS & LEGAL NOTICE

This document is a work product of the Industry IoT Consortium Standards Task Group, chaired by Erin Bournival (Dell Technologies).

Authors: Claude Baudoin (cébé IT & Knowledge Management) and Erin Bournival (Dell Technologies).

Contributors: Kym Watson (Fraunhofer Institute) and Chuck Byers (IIC staff) contributed substantial written content to this document.

Editor: Claude Baudoin (cébé IT & Knowledge Management LLC).

Technical Editor: Chuck Byers (IIC CTO) oversaw the process of organizing the contributions of the above Authors and Contributors and securing reviews and approval of the document.