StandICT.eu 2023

ICT STANDARDISATION OBSERVATORY AND SUPPORT FACILITY IN EUROPE

“Walk & Talk” Webinar on Digital Transformation through Standardisation: IoT and Edge
NSB Standardisation System & IoT Standardisation

Xiaoying SUO (Spanish Association for Standardisation)

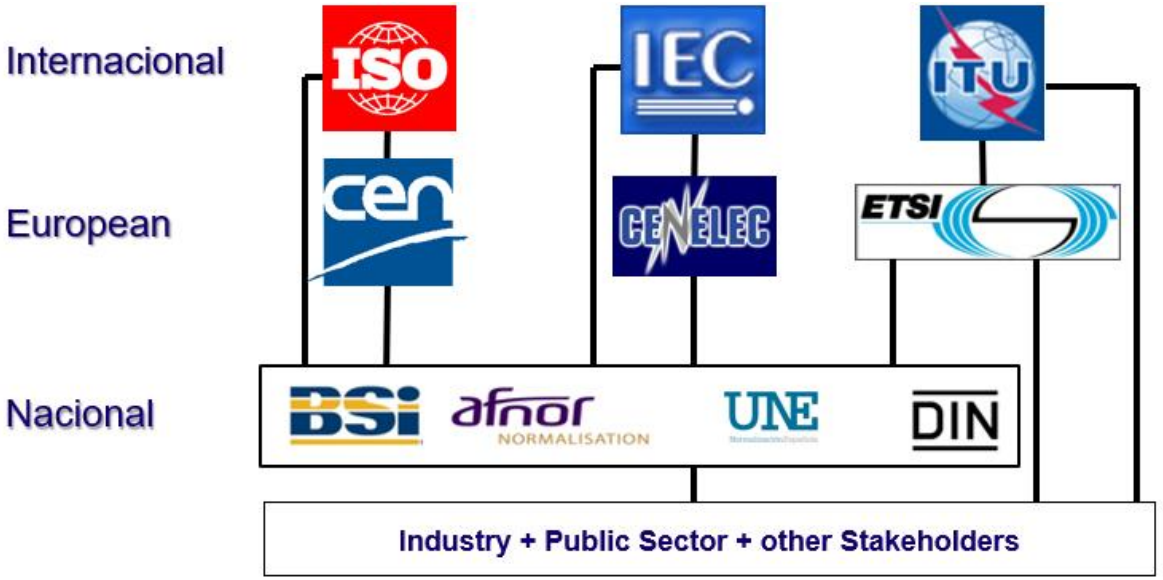
StandICT.eu has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement **No. 951972**.

NSB Standardisation System

Spanish Association for standardisation (UNE)

- Private, independent, not-for-profit
- 530 members
- Since 1986
- RD 2200/1995 (RD 1072/2015).
- Spanish member international forums

Standardisation System



UNE represents the interests of Spanish businesses and society within European and International Standardisation organizations.

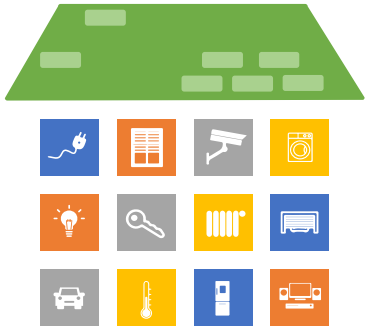
Standardisation contributes to improving productivity, competitiveness and economic growth.

Standardisation documents

Characteristics of different Standardisation documents

Type	Standard	Technical Specification	Technical Report	Workshop Agreement
International code	ISO IEC	ISO/TS IEC/TS	ISO/TR IEC/TR	IWA
European code	EN	CEN/TS CLC/TS	CEN/TR CLC/TR	CWA
National code	UNE, NF, BS, DIN, etc. UNE-EN, DIN-EN, UNE-ISO, DIN-ISO, etc.	UNE-CEN/TS, DIN-CEN/TS, UNE-ISO/TS, DIN-ISO/TS, etc.	UNE-CEN/TR, DIN-CEN/TR, UNE-ISO/TR, DIN-ISO/TR, etc.	Variable
Main characteristics	• Elaboration: 3 years • 2 steps of member approval • European: compulsory national adoption Revision: every 5 years	• Elaboration: 21 months • 1 step of member approval or internal approval in TC • European: optional national adoption Revision: at 3 years (upgrading to EN or deletion)	• Elaboration: free timeframe • Internal approval in TC • European: optional national adoption No revision required	• Elaboration: free timeframe (usually few months) • Internal approval in the Workshop • European: optional national adoption Revision: at 3 years (upgrading to EN or deletion)

IoT Standardisation



- Importance of IoT Standardisation
- IoT Standardisation developments

Importance of IoT Standardisation

IoT challenges and gaps	Standards development needs
Common language (vocab.)	There should be a common understanding about the technology and an acceptable common reference architecture to its stakeholders for the implementation. As the IoT is broad and applicable most of the sectors of the society, there is a need of common understanding about the technology as well as well-defined reference architecture acceptable from different perspective across the sectors
Interoperability (interop.)	The IoT is growing across the sectors. Seamless interoperability with different devices operating in different technology is a major challenge. In addition to this, interoperation of the network protocol stacks at higher layers involving domain specific operation, and semantic level is another challenge
Connectivity (connect.)	Connecting billions of devices is a major challenge in IoT. Apart from this, various communication technologies: Wi-Fi, Zigbee, LoRa, Low-Power Wide Aera Network (LPWAN), Long Term Evolution (LTE), LTE-advanced, 5G, etc. are ruling the current IoT paradigm and other technologies yet to come. Seamless connectivity among connecting devices across the sectors and communication technologies is a major challenge
Security and privacy (sec. & priv.)	Today, security and privacy are the prime concerns for the IoT deployment. Most of its deployments are prone to security and privacy at device, 'edge', 'cloud' platform level. It is necessary to consider appropriate deployment architecture to overcome all the related issues
Trustworthiness (trust.)	Trustworthiness reflects the degree of confidence one has that the system performs as expected with regard to characteristics including safety, security, privacy, reliability and resilience, etc. Trustworthiness of IoT systems will require active management of risks for all these characteristics
Reliability (relia.)	Reliability of the services is also another major concern in specific sectors, such as in health care, connected vehicles. These sectors require utmost reliability (99.9999% or better) to get the appropriate service
Scalability and agility (scal.)	The IoT is referred as a network of networks. The future applications or networks should be both scalable and agile to the user demands. System should be dynamically scaled up and down without sacrificing basic requirements, such as Quality of Service (QoS), security/privacy, reliability, etc. The IoT is more heterogeneous than the Internet. In the context of tremendous challenges due to unbounded, unplanned, and unregulated growth of networks in the Internet leads to significant improvements also in the IoT technology
Intelligence and analytics (intel.)	By nature, the IoT is to collect information and to react based on it. Information is collected at the devices and communicated to the cloud with or without the support of edge. The factors: delay, jitter, cost, regulatory issues, etc., play significant role to place the appropriate analytic platform; i.e. whether at edge/fog or at the cloud. Inaccurate analysis due to flaws in the data source, limited ability to analyze and manage unstructured and real-time data, missing data extraction guidelines, etc. are critical issues in the current context
Sector-specific requirements (sector.)	Deployment decision can impact the vertical, horizontal or end customer markets of the IoT. In particular, they can be consumer, industrial, and commercial IoT. In this context, specific guidelines for specific sectors of deployment are very important, which is missing in the current context for most of the sectors
Societal (socie.)	The services of IoT should satisfy consumers, developers, regulators etc. as stakeholders of the society. This societal challenge includes the mode of usage, the energy consumption, environment impact and other related societal impact, which play a vital role in the IoT deployment

IoT Standardisation developments

IoT Standardisation developments

ISO/IEC JTC 1

- **ISO/IEC JTC 1/SC 41/WG 3 'IoT Architecture'** provides standardisation in the area of Common Language - IoT Vocabulary, Architecture and Frameworks.
- **ISO/IEC JTC 1/SC 41/WG 4 'IoT Interoperability'** provides standardisation activities in the area of interoperability, connectivity, platform, middle-ware, conformance and performance correctness testing.
- **ISO/IEC JTC 1/SC 41/WG 5 'IoT applications'** deals with standardisation in the area of IoT applications, use cases, tools and implementation guidance.
- **ISO/IEC JTC 1/SC 27 'Information Security, Cybersecurity and Privacy Protection'.** ISO/IEC JTC 1/SC 41 works together with **ISO/IEC JTC 1/SC 27 'Information Security, Cybersecurity and Privacy Protection'**, for standards related to **IoT security and privacy**.

IoT Standardisation developments

ETSI

- **ETSI/TC Smart M2M** is responsible for providing specifications for applications related to IoT and Smart Cities.
- **ETSI/TC Cyber** provides standards and specifications related to IoT cybersecurity and privacy guidelines, as well as *security by design/default*.
- **ETSI/TC Earth Station and Systems (SES) is** responsible for the standardisation of all types of satellite communications systems, services and applications.

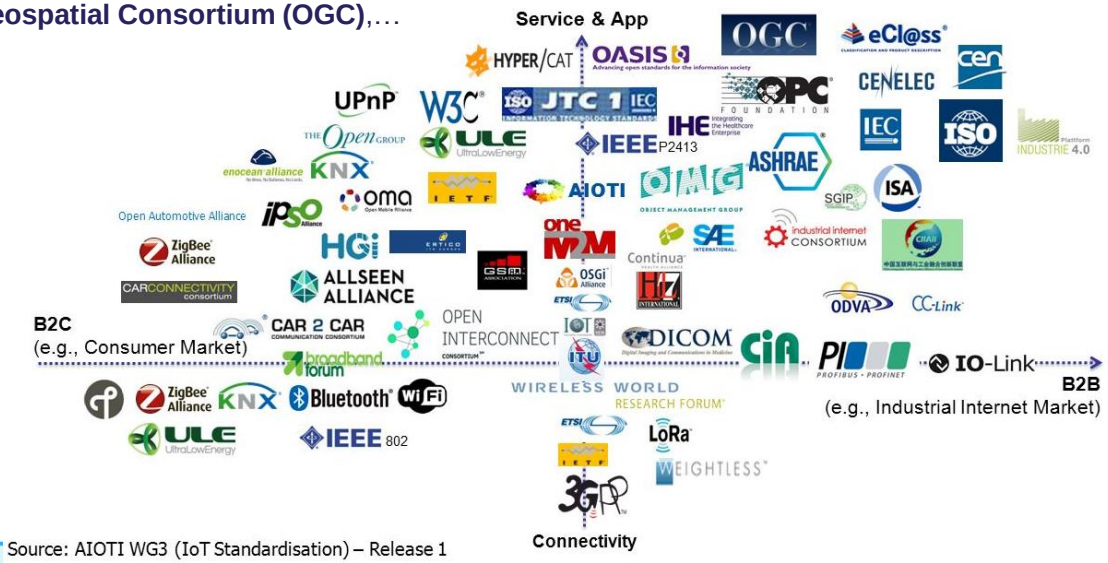
ITU

- **ITU-T SG 20 'IoT and Smart Cities and Communities' (SC&C)** addresses standardisation requirements with an initial focus on IoT applications in Smart Cities and Communities.
- **ITU-T SG 17 'Security'** coordinates security-related work in all ITU-T SGs along with a wide range of standardisation issues. In particular, for IoT, it works on the security of applications and services for the IoT and the smart grid.

IoT Standardisation developments

Other SDOs/Alliances

- **oneM2M** is a joint alliance of eight SDOs active in ICT Standardisation including ETSI. This alliance is playing an important role in developing interoperability related standards and specifications within and out of the IoT system. Basically, the specifications developed by oneM2M address the need for a common M2M Service Layer that can be readily embedded within various hardware and software and relied upon to connect the myriad of devices in the field with M2M application servers.
- **Institute of Electrical and Electronics Engineers (IEEE)** has been producing standards for local/personal area connectivity, which play a vital role in forming a physical and Medium Access Control (MAC) layer related standards.
- The **project P2413** aims to develop an architectural framework to cover the needs of different applications.
- Similarly, considering market growth of the IoT, the **third Generation Partnership Project (3GPP)** is working on and has already provided set of specifications to Long Term Evolutions (LTE), NarrowBand IoT (NB-IoT), and 5G related radio specifications and standards related for the IoT.
- **Internet Engineering Task Force (IETF)** is another leading organization in standardizing protocols for the Internet at different layers of the network stack. It is also working to optimize the IETF's protocols offerings for the lower level on LPWAN from SigFox, LoRA Alliance, 3GPP etc. as well as to define the upper layer exchanges and signaling of existing protocol offerings.
- **Message Queuing Telemetry Transport (MQTT)**, an ISO standard, submitted by Organization for the **Advancements of Structured Information Standard (OASIS)** provides a standardized mechanism to connect devices. It helps cloud based architectures to be developed with common protocol semantics for the inter-connectivity.
- **Alliances: Alliance for Internet of Things Innovation (AIOTI)**, **Association for Automatic Identification and Mobility (AIM)**, **Industrial Internet Consortium (IIC) , Global Standards One (GS1)**, **Open Connectivity Foundation (OCF), World Wide Web Consortium (W3C)**, **Open Geospatial Consortium (OGC)**,…



Source: AIOTI WG3 (IoT Standardisation) – Release 1

IoT Standardisation developments

SDOs	IoT standards	Description
JTC 1/SC 41	-TR 22417:2017 IoT -IoT use cases	-Examples and template for IoT use case analysis
	-20924:2018 IoT -Vocabulary	-Basic IoT terminologies
	-30141:2018 IoT -Reference Architecture	-Generic IoT reference architecture
	-21823-1:2019 IoT -Interoperability systems framework -Part 1– Framework	-Interoperability framework for IoT
JTC 1/SC 27	-27400 Cybersecurity - IoT Security and Privacy - Guidelines	-IoT Security and Privacy Guidelines
	-27402 Cybersecurity - IoT security and privacy - Basic device requirements	-Basic requirements for IoT device security and privacy
	-27403 Cybersecurity - IoT Security and Privacy - Guidelines for IoT and IoT-Domotics	-IoT-domotic Security and Privacy Guidelines
ITU-T	-Y.2060 (06/2012) -Overview of the Internet of things	-Clarifies the concept and scope of the IoT
	-Y.4203 -Requirements of things description in the IoT	-Introduction and requirements of things
	-Y.4459 -An architecture for IoT interoperability	-Digital Objective Architecture (DOA) features and its capabilities
	-Y.4204 -Accessibility requirements for the IoT applications and services	-Accessibility requirements for IoT applications and services
ETSI	-TR 103 375 -IoT standards landscape and future evolutions	-Requirements, protocols, tests, etc.
	-TR 103 376 -IoT LSP use cases and standards gaps	-Recommendations
	-TS 103 645 -Cyber Security for Consumer IoT	-High-level provisions for IoT security

Thanks from

StandICT.eu 2023

ICT STANDARDISATION OBSERVATORY AND SUPPORT FACILITY IN EUROPE

To find out more visit:
standict.eu

Stay in touch on Twitter
@Stand_ICT

Join us on Linkedin
linkedin.com/in/standict