ETSI TR 103 376 V1.1.1 (2016-10)

SmartM2M;
IoT LSP use cases and standards gaps

Reference
DTR/SmartM2M-103376

Keywords
IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

NOTE: 3GPP™, AllJoyn™, AllSeen™ Alliance™, ASHRAE™, AVNU Alliance™, B2MML™, BACnet™, Bluetooth™, C2C-CC™, DASH7™, DICOM™, EnOcean™, HL7™, IETF™, IIC™, KNX™, LoRa™, LR-WPAN™, LTE™, LTE-Advanced™, LTE-Advanced Pro™, MIPI™, MirrorLink™, OASIS™, OCF™, OGC™, OMA™, OMG™, OPC™, OSGi™, SAE INTERNATIONAL™, SERCOS International™, UMTS™, W3C™, Wi-Fi Alliance™, ZigBee™ and Z-Wave™ are tradenames registered by their respective owners. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of these products and/or associations.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

Starting from the use case families selected for the IoT Large Scale Pilots (LSPs) the present technical report aim is:

- To provide the collection of all missing functionalities that have been identified in standards bodies (SDOs) to offer solutions addressing the use case requirements.
- 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.
- To propose some recommendations to overcome potential gaps. Particular attention will be paid on horizontal application layer standardization and to assure an interworking framework among different vertical industrial segments.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 375: "SmartM2M; IoT Standards landscape and future evolutions".

[i.2] AIOTI WG03: "IoT Large Scale Pilots (LSP) Standard Framework Concepts", Release 2.0, October 2015.

[i.3] AIOTI WG03: "Report on High Level Architecture (HLA)", Release 2.0, October 2015.

[i.4] AIOTI WG08: "Smart City LSP Recommendations Report", October 2015.

[i.5] AIOTI WG05: "Report on Smart Living Environment for Ageing Well", October 2015.

[i.6] AIOTI WG09: "Report on Smart Mobility", October 2015.

[i.7] AIOTI WG07: "Report on Wearables", October 2015.

[i.8] AIOTI WG11: "Report on Smart Manufacturing", October 2015.

[i.9] ISO 37120: "Sustainable development of communities -- Indicators for city services and quality of life".

[i.10] Recommendation ITU-T X.1255: "Framework for discovery of identity management information".

[i.11] AIOTI WG06 Report: "Smart Farming and Food Safety Internet of Things Applications - Challenges for Large Scale Implementations", October 2015.

[i.12] Resolution ITU-R 66: "Studies related to wireless systems and applications for the development of the Internet of Things".

[i.13] IEEE 802.1X-2010™: "IEEE Standard for Local and metropolitan area networks -- Port Based Network Access Control".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

SDO: standards developing or standards setting organization

NOTE: In the present document, SDO is used equally for both types of organizations.

standardization gaps: missing or duplicate elements in the IoT standardization landscape

NOTE: Examples of standardization gaps are: missing standards or regulations, missing APIs, technical interoperability profiles that would clarify the use cases, duplications that would require harmonization. They may be technical, societal or business-related.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
ACEA	Association des Constructeurs Européens d'Automobiles
AIOTI	Alliance for IoT Innovation
API	Application Programming Interface
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
BAN	Body Area Network
BBF	Broad Band Forum
BSM	Basic Safety Message
C2C-CC	Car 2 Car Communication Consortium
CAM	Cooperative Awareness Message
CCC	Car Connectivity Consortium
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
CiA	CAN in Automation
CoAP	Constrained Application Protocol
CPPS	Cyber-Physical Production System
D2D	Device-to-Device
DDS	Data Distribution Service
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
EC	European Commission
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	European Union
FIWARE	Future Internet -ware
FMIS	Farm Management Information Systems
GNSS	Global Navigation Satellite System
HF	Human Factors
HGI	Home Gateway Initiative
HL7	Health Level Seven International
HLA	High Level Architecture
HMI	Human Machine Interface
HW	Hardware
IBM	International Business Machines (Corporation)
ICT	Information and Communication Technology

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IIC	Industrial Internet Consortium
IMT	International Mobile Telecommunications
IoT	Internet of Things
IP	Internet Protocol
IPSO	Internet Protocol for Smart Object
ISO	International Organization for Standardization
ISO/IEC JTC1	ISO/IEC joint technical committee
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Sector
KA	Knowledge Area
KNX	KoNneX
LAN	Local Area Network
LE	Low Energy
LON	Local Operator Network
LSP	Large Scale Pilot
M2M	Machine-to-Machine
MAC	Media Access Control
MAN	Metropolitan Area Network
MES	Manufacturing Execution System
MESA	Manufacturing Enterprise Solutions Association International
MQTT	MQ Telemetry Transport
NFC	Near Field Communication
NWK	NetWorK
OAA	Open Automotive Alliance
OAGi	Open Applications Group
OASIS	Advancing Open Standards for the Information Society
OCF	Open Connectivity Foundation
ODVA	Open DeviceNet Vendor Association
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
OMG	Object Management Group
OPC	Open Platform Communications
OSGi	Open Services Gateway initiative
PAN	Personal Area Network
PHD	Personal Health Device
PHY	PHYsical layer
PII	Personally Identifiable Information
PLC	Power Line Communication
PLC	Programmable Logic Controller
PSA	Protocol Standards Association
QoS	Quality of Service
ROI	Rate Of Interest
ROLL	Routing Over Low power and Lossy networks
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Developing Organization
SERCOS	SErial Real-time COmmunication System
SES	Satellite Earth Stations and Systems
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprise
SSO	Standards Setting Organization
TC	Technical Committee
TCP	Transmission Control Protocol
TIM	Transducer Interface Module
TR	Technical Report
ULE	Ultra Low Energy

US	United States
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
W3C	Worldwide Web Consortium
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
XMPP	eXtensible Messaging and Presence Protocol

4 General Considerations

4.1 Introduction

4.1.1 Defining gaps

In ETSI TR 103 375 [i.1], an inventory of the current IoT standardization has been performed. Its objective is to assess the degree of industry and vertical market fragmentation; and to point towards actions that can increase the effectiveness of IoT standardization, to improve interoperability, and to allow for the building of IoT ecosystems. ETSI TR 103 375 [i.1] identifies a number of standards that are available, i.e. that have reached a final stage in a Standards Developing Organization by the time of writing the report, and can be used for the work of the IoT Large Scale Pilots (LSP).

However, the coverage of the IoT landscape - and the possibility to develop large-scale interoperable solutions - is not fully guaranteed since some elements in this landscape may be missing. These missing elements are referred to as "gaps" in the remainder of the present document. Gaps may also be identified when harmonization or interoperability between a large number of potential solutions is missing.

These "gaps" are the main point of interest of the present document. Three categories of gaps will be addressed:

- Technology gaps. Some examples in this category are communications paradigms, data models or ontologies, software availability.
- Societal gaps. Some examples in this category are privacy, energy consumption, ease of use.
- Business gaps. Some examples in this category are siloed applications, value chain, and investment.

In the reminder of the present document, the identification of gaps will be specially made in view of ensuring that they will be further understood, handled and closed within the IoT community (and possibly beyond). This identification of gaps will rely on an approach that allows for:

- The characterization of gaps, in particular by understanding the type of gaps (see above), the scope of the gap, the difficulties it generates, and other appropriate descriptions.
- The mapping of the gaps on an architectural framework (see clause 4.1.3) that allows for the mapping of the gaps on a reference that can be understood by the IoT community and, in particular, that can be related to other frameworks e.g. those developed in other organizations, for instance in Standards Setting Organizations.

This characterization and mapping are made with the objective to ensure that - whenever possible - these gaps may be handled, and hopefully closed, by one or more organizations in the IoT community.

The present document does not have the aim to undertake the resolution of the gaps that is left to the proper organizations of the IoT community. However, its objective is also to provide recommendations for the future standard framework.

4.1.2 Identifying gaps: user survey

A critical part of the identification of gaps is the collection of those missing elements. Since they can be of very different nature (see clause 4.1.1) and may have been detected by very different actors of the IoT community, there needs to be a mechanism to collect the largest possible information. To this extent, a survey has been built in order to identify as many gaps as possible with the help of the IoT community, in particular the IoT standardization community.

The survey aims at:

- Identifying the domain of activity of the respondent.
- Understanding what his/her objectives and main area of work are.
- Defining up to three gaps of all three types as defined in clause 4.1.1.

The detailed text of the survey can be found in annex B.

The survey has been largely distributed. At the time of writing the final version of the present document, 215 answers have been collected and the survey is closed. A few statistics on the responders and answers received can be found in clause B.2.

In a second step, these answers have been analysed with the objective to identify commonalities (i.e. related missing functionalities that can be considered as one gap) and associated interoperability frameworks.

The answers received have been tentatively classified in the different clauses of the present document. Clauses 5.3, 6.3, 7.3, 8.3, 9.3, 10.3 and 11.3 provide the answers which are related to a defined vertical sector. Clause 12.1 gives the answers which apply to the horizontal domain or are more generic. However, it should be noted that the answers received are generally not applicable to one specific vertical sector. For example, readers willing to cover all answers applicable to the wearable vertical sector should refer to the clauses related to Smart Living, Smart Wearables as well as clause 12.1. The matrix provided in table 0 gives guidance in that direction.

Table 0: Cross-domain reading of the survey answers

Answers in [vertical or horizontal domain on the right] may be shared with the [vertical domain below]	Horizontal (clause 12.1)	Smart Cities (clause 5.3)	Smart Living (clause 6.3)	Smart Farming (clause 7.3)	Smart Wearables (clause 8.3)	Smart Mobility (clause 9.3)	Smart Manufacturing (clause 10.3)	Smart Environment (clause 11.3)
Smart Cities	X	X	X			X		
Smart Living	X	X	X		X			
Smart Farming	X			X			X	X
Smart Wearables	X		X		X			
Smart Mobility	X	X				X		X
Smart Manufacturing	X			X			X	
Smart Environment	X			X		X		X

4.1.3 Identifying gaps: requirements analysis

The present clause explains the methodology implemented by the editors of the present document to identify technological requirements for each of the vertical areas and tentatively map them to organizations that provide standards related to these requirements.

This study has been executed in parallel and independently from the user survey described in clause 4.1.2.

For each vertical sector, the main technological requirements are extracted from the vertical-specific AIOTI reports and other available documentation describing that vertical sector. In a second step, the listed requirements are classified according to the knowledge areas to which they belong. They are shown in the left column of the tables. For more accuracy, the Communication and connectivity knowledge area is divided according to the main usual communication layers:

- Connectivity at physical and link layer.
- Network layer.
- Service level and application enablers.
- Application level API, data models and ontologies.

The next step identifies which SDOs/Alliances address the target requirement. The standards found are not listed directly in the present document, since this list maybe complex in some cases (it may be provided however in a revised version of the present document). The reader is rather referred to the partner TR, ETSI TR 103 375 [i.1], as the reference where existing concrete standards for each SDO/Alliance that address the specific requirement in the target vertical domain and knowledge area can be found.

In the case where no standard could be identified for a specific requirement, the requirement is declared as a potential standardization gap.

4.1.4 Mapping gaps

Before mentioning gaps, and in particular standards gaps that an LSP may have to address in the achievement of its objectives, one first needs to have a target framework in mind. The AIOTI WG03 has developed a standard framework or architecture for IoT which is similar or can be mapped to other frameworks such as ITU, oneM2M, IIC. The one thing that the frameworks have in common is the fact that interoperability must be achived amongst the various elements of the IoT. Interoperability means having interworking standards with less complexity. With a target model in mind and an idea of what the current landscape looks like, which are the objectives of the ETSI TR 103 375 [i.1], it is now possible to identify which are the remaining gaps to achieve IoT. The focus of the present document is to look at such gaps in the standard that will be needed to achieve the various LSP and make recommendation on going forward.

The landscape analysed in ETSI TR 103 375 [i.1] has described the IoT standards from the view point of the elements or knowledge areas that make up the IoT framework. The present document adopts a similar structure by looking at the gaps based on the knowledge areas but it also defines the main requirements specific to each vertical sector, analyses how they are covered and what the gaps that have been identified are.

Figure 1 shows the AIOTI High Level Target Architecture for IoT (AIOTI HLA).

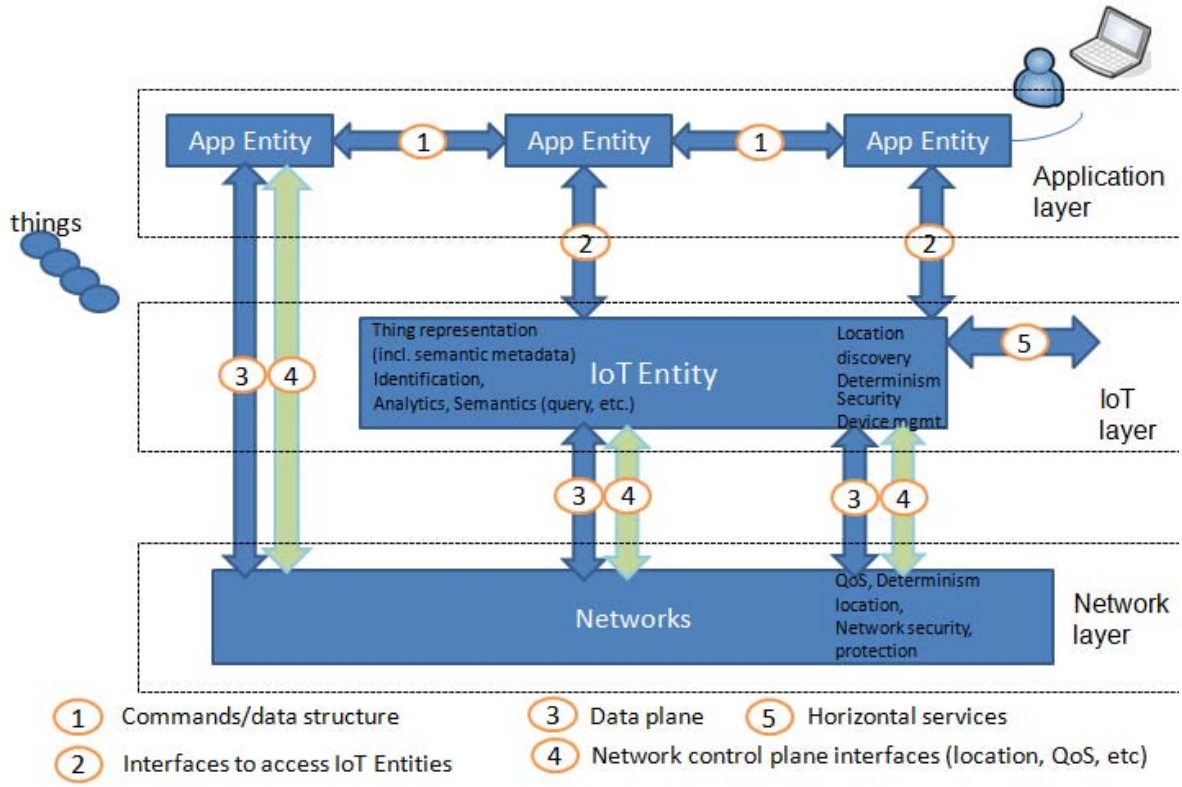


Figure 1: AIOTI high level architecture for IoT (from [i.3])

Interfaces above are:

1: Defines the structure of the data exchanged between App Entities (the connectivity for exchanged data on this interface is provided by the underlying Networks). Typical examples of the data exchanged across this interface are: authentication and authorization, commands, measurements, etc.

2: This interface enables access to services exposed by an IoT Entity to e.g. register/subscribe for notifications, expose/consume data, etc.

3: Enables the sending/receiving of data across the Networks to other entities.

4: Enables the requesting of network control plane services such as: device triggering (similar to "wake on LAN" in IEEE 802.1X [i.13]), location (including subscriptions) of a device, QoS bearers, deterministic delivery for a flow, etc.

5: Enables the exposing/requesting services to/from other IoT Entities. Examples of the usage of this interface are to allow a gateway to upload data to a cloud server, retrieve software image of a gateway or a device, etc.

4.2 Vertical domains covered

As a support for the IoT Large Scale Pilot, the vertical domains that are addressed in the present document are those where such LSP will be defined and, for some, selected and undertaken. These domains are the following:

- Smart Cities. The modern cities need to evolve and become structured, interconnected ecosystems where all components (energy, mobility, buildings, water management, lighting, waste management, environment, etc.) are working together in support of humans. By using the IoT technology, the cities are expected to achieve this transition while maintaining security and privacy, reducing negative environmental impact and doing it in a reliable, future proof and scalable manner.

- Smart Living environments for ageing well (e.g. smart house). It is expected that the IoT will support the continuously growing population of elderly people in living longer, staying active, non-dependent and out of institutional care settings, together with reducing the costs for care systems and providing a better quality of life. This should be achieved in particular with IoT for Smart Home and home automation supporting technologies.

- Smart Farming and food security. The application of IoT technologies to the overall farming value chain will improve its optimization and, as a consequence, food safety in general. Technologies such as data gathering, processing and analytics as well as orchestrated automation technologies supported by IoT are expected to achieve this.

- Smart Wearables. The integration of intelligent systems to bring new functionalities into clothes, fabrics, patches, aids, watches and other body-mounted devices will provide new opportunities and applications. Basic technologies such as nano-electronics, organic electronics, sensing, actuating, localization, communication, etc. will be offered to the end-user, with an associated range of problems such as acceptability, ease of use, privacy, security or dependability.

- Smart Mobility (smart transport/smart vehicles/connected cars). The Internet of Things applied to the mobility domain may create the potential for major innovations across a wide variety of market sectors, with mobility applications such as self-driving and connected vehicles, multi-modal transport systems and "intelligent" transportation infrastructure from roads or sea ports to parking garages.

- Smart environment (smart water management). IoT will be a key building block to solutions for vertical applications such as environmental monitoring and control that will use sensors to assist in environmental protection by monitoring air, water quality, atmospheric or soil conditions and noise pollution.

- Smart manufacturing. In support of the European manufacturing industry, all forms of competitive industries will have to massively incorporate more intelligence, which will rely in particular on IoT through advanced connected objects providing sensing, measurement, control, power management and communication, both wired and wireless.

4.3 Knowledge Areas

The Knowledge Areas (KA) used in the present document are the ones defined by the AIOTI WG03. However, considering that the definition in the AIOTI report on "IoT Landscaping" are sometimes ambiguous, they are detailed below with more precision, in particular regarding the nature of the standards that can be found in each of the KAs. These definitions are used for the classification of Standards in the subsequent clauses.

Communication and Connectivity

This KA covers mainly specification of communication protocols at all layers, e.g. PHY, MAC, NWK, Transport, Service and Application layers. It includes the management associated with the Knowledge Area.

Examples of the type of standards that can apply to this KA are:

- Connectivity at physical and link layer
- Network layer
- Service level and application enablers
- Application level API, data models and ontologies
- Management of the protocols

Integration/Interoperability

This KA covers mainly specification of common IoT features required to provide integration (assembly of sub-systems) and interoperability (interoperation of heterogeneous sub-systems).

Examples of the type of standards that can apply to this KA are:

- Profiles

- Testing Specifications

Applications

This KA covers the support of the applications lifecycle. This includes development tools, application models, deployment, monitoring and management of the applications.

NOTE 1: The application level protocols, APIs, data models, ontologies, etc., are part of the "Communication and Connectivity" and/or "Integration/Interoperability" KA.

Examples of the type of standards that can apply to this KA are:

- Flexible remote management
- Support methods for installing, starting, updating applications

Infrastructure

This KA covers the design, deployment, and management of computational platforms and infrastructures (e.g. network elements, servers, etc.) that support IoT-based usage scenarios.

Examples of the type of standards that can apply to this KA are:

- Virtualization
- Mobile-Edge Computing
- Network Management
- Network Dimensioning, Network Planning
- Functional Safety

IoT Architecture

It covers the specification of complete IoT systems, with a focus on architecture descriptions.

Examples of the type of standards that can apply to this KA are:

- Reference Architecture

Devices and sensor technology

This KA covers mainly device and sensor lifecycle management.

NOTE 2: The communication protocols between devices and other elements are covered in the "Communication/Connectivity" KA.

Examples of the type of standards that can apply to this KA are:

- Device Monitoring
- Sensor/actuators virtualization
- Configuration management

Security and Privacy

This KA covers all security and privacy topics.

Examples of the type of standards that can apply to this KA are:

- Communications security and integrity
- Access Control
- Authorization, Authentication, Identity Management

- PII (Personally Identifiable Information) Management

5 Gap analysis in the context of Smart Cities

5.1 High level description and analysis

This clause describes at high level what the specificities of the Smart Cities vertical sector are based on the AIOTI WG03 [i.2] and AIOTI WG08 [i.4] reports, and summarizes the global outcome of the standards landscape.

The concept of Smart City brings up whole new opportunities as well as very interesting challenges. A city is considered smart when part or all of its operations services are supported through an ICT infrastructure. Operation services may include transport, parking, energy, etc. The use of an ICT infrastructure is sought to enhance the efficiency and the ease of use of the city operations services. However, a Smart City is expected to be beneficial to the citizens regardless of their ICT abilities.

The realization of a Smart City is subject to many challenges in order to monitor and integrate all of the city infrastructure and services. From the technical infrastructure to be put in place to the adoption and acceptability of the offered services by the citizens as well as the business actors involved.

Regardless of the different challenges, a critical requirement for the success of a Smart City deployment remains in making the relevant data available to the relevant applications in order to achieve the idea of a Smart City. The Smart City faces the integration of different and autonomous systems that are often vendor specific (waste collection and management, parking management systems, building management, etc.). Moreover, various technologies have been employed for each application. The Smart City vertical sector is thus a domain where several technological solutions are used for solving similar problems.

The Smart City concept has the following specificities:

- Integration of a large number of heterogeneous equipment (sensors, actuators, edge devices, end user devices, enterprise and cloud systems, etc.).
- High data heterogeneity in terms of model, representation format, volume, precision, importance, etc.
- Use of various network and communications technologies (access network technologies and communication protocols).
- Interconnection of the newly deployed IoT systems with the legacy ones.

Moreover, target applications for the Smart City require access to data flows and actuation mechanisms. For example, a smart lightning application will require access to data provided by luminosity sensors, weather information, and a way to control connected city lights.

Smart Cities also rely on the principle of open data to foster local democracy/governance and thrive the local economy. Therefore, the huge amounts of data collected and processes by the different applications are to be put on open platforms and accessible through open interfaces (APIs). Based on these new data business models are to be developed in order to monetize the collected data and to support the service delivery.

Since Smart Cities put the citizen at the centre and thus deal with data provided by end-user or collected by monitoring systems, privacy and data security need to be solved. Open data principle may be seen conflictual with data security and privacy. Therefore, Smart City data need to define mechanisms for data access with the appropriate access rights and protection mechanisms in order to allow the appropriate access/processing to the appropriate entity (end-user, municipality, application, third-party operators, etc.).

Finally, Smart Cities seek enhancing the efficiency of resources use and city operations services. This is achieved through the use of ICT technologies. In this context, innovative applications should have access to high level services provided by the city and its platforms. Service platforms are thus a key for the Smart City success. Such services platforms will integrate data sources, devices, systems to a large extent.

5.2 Mapping of requirements and related standard coverage

5.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

5.2.1 Communication and Connectivity knowledge area

5.2.1.1 Connectivity at Physical and Link layer

Table 1: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Support of heterogeneous communications : wireless/wired, short/long range	3GPP, ETSI TETRA, IEEE, LoRa Alliance, ETSI ERM, ITU EnOcean Alliance, DASH7 Alliance, Zigbee, IETF, OMG
Support of Infrastructure-based communication	3GPP, ETSI TETRA, IEEE 802.15, LoRa Alliance, ETSI ERM, ITU xDSL
Support of Ad hoc communications	ETSI TETRA, IEEE, DASH7 Alliance, EnOcean Alliance

5.2.1.2 Connectivity at Network layer

Table 2: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Support of local and remote access to infrastructure services	3GPP, ETSI TETRA, IEEE 802.x, LoRa Alliance, ETSI ERM, ITU, IETF
Support of point-to-point communications	3GPP, ETSI TETRA, IEEE 802.x, ITU, EnOcean Alliance, DASH7 Alliance
Support of point-to-multipoint communications	ETSI TETRA, IEEE 802.x, ITU
Support of routing continuity across different network technologies	IETF 6lo
Support of device unique identification	This is a potential gap

5.2.1.3 Service level and application enablers

Table 3: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Query-driven communications	IETF
Event-driven communications	IETF, OASIS
Group communications	IETF, OASIS, OMG
Message format interoperability	ITU-T, W3C
Resource discovery and announcement	OASIS
General services and Interoperability between different applications	oneM2M, OCF, AllSeen Alliance

5.2.1.4 Application Layer level, APIs, Data models and ontologies

Table 4: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
Unified data model	W3C, oneM2M
Services exposition and discovery	oneM2M, ITU-T
Unified API for underlying services	oneM2M

5.2.2 Integration/Interoperability knowledge area

Table 5: Mapping of requirements integration/interoperability knowledge area

Requirements	Organizations providing related standards
Certification of devices	Wi-Fi Alliance, WiMAX, For some technologies, there is a potential gap…
Interoperability between heterogeneous devices at the communication level (message bus)	oneM2M, OCF, AllSeen Alliance
Interoperability between heterogeneous devices at the data level	ITU-T, W3C, oneM2M

5.2.3 Applications management knowledge area

Table 6: Mapping of requirements applications management

Requirements	Organizations providing related standards
Application specification	This is a potential gap
Local and remote application management (configuration, installation, start/stop, update, etc.)	OMA LWM2M,OSGi
Application performance' monitoring (computing resources)	This is a potential gap

5.2.4 Infrastructure knowledge area

Table 7: Mapping of requirements infrastructure knowledge area

Requirements	Organizations providing related standards
Integration of new and legacy systems	oneM2M, OCF, AllSeen Alliance
Deployment and management	OSGi
Functional safety	IEC

5.2.5 IoT Architecture knowledge area

Table 8: Mapping of requirements for IoT Architecture knowledge area

Requirements	Organizations providing related standards
Device discovery; capability to include new devices, sensors, actuators when they join the system. It covers integrated/complete IoT specification solutions, including architecture descriptions for Smart Cities.	oneM2M-; ITU-T; IIC; IEEE, IERC, IoT.A, ISO/IEC JTC1; AIOTI

5.2.6 Devices and sensor technology knowledge area

Table 9: Mapping of requirements for devices and sensor technology knowledge area

Requirements	Organizations providing related standards
Interoperability of sensor networks, and make sensor networks plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/from an existing sensor network.	ETSI SmartBAN, ISO/IEC, M2.COM, Zigbee
Device for home automation, home security, and climate control.	ULE ETSI DECT
Device management, Includes protocols for managing different devices not quite devices.	BBF, OMA, OCF, oneM2M
Cellular devices for accessing voice and data services.	3GPP ETSI DECT
Functions that are to be performed by a transducer interface module (TIM).	IEEE - ISO/IEC JTC1
Sensors to provide robustness, accuracy, reliability.	ISO/IEC JTC1

5.2.7 Security and privacy knowledge area

Table 10: Mapping of requirements for security and privacy knowledge area

Requirements	Organizations providing related standards
High level of trust (common good objective) bootstrap authentication and key agreement for application security.	3GPP W3C
End-to-end security.	3GPP, Hypercat, IEEE, IETF
Confidentiality and privacy, protection of personal data; encryption.	OASIS, ISO/IEC
Secure remote access to the system from third-parties; user authentication, access control.	IEEE Hypercat

5.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Cities vertical domain. The answers which spread across several domains, including the present one, are provided in clause 12. Answers related to the Smart Living and Smart Mobility vertical domains may also be applicable here.

Table 11: Survey results for the Smart Cities vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Standards fragmentation.	Integration/Interoperability	4	Consolidation and/or better interworking.
Lack of investment and application use cases.	Integration/Interoperability; Applications life-cycle support	3	
Lack of harmonisation/interop.	Integration/Interoperability	3	Consolidation, merge.
Interoperability, data governance.	Communication and Connectivity (service and application levels); Integration/Interoperability	3	Unlock the interoperability issues among models provide support to the data governance.
Today it is not possible that different companies are able to interact and interface securely and effortlessly with a wide variety of objects and sensors that are not all of them owned by the same entity and acquired to the same vendor and manufacturer. It is required a high secure and trust environment, due to mobility and seamless connectivity requirements of smart objects, that currently is not available with the exception of proprietary and isolated solutions.	Communication and Connectivity (physical up to application level); Integration/Interoperability; IoT Architecture; Devices and sensor technology; Security and Privacy	3	Establish standards that allow one Smart object to move and participate in different ecosystems like a mobile phone is able to operate through different telecom operator networks.
Too many standards to follow. Even customers don't know which standards to follow, demand or expect to be applied.	Integration/Interoperability; Applications life-cycle support; IoT Architecture; Devices and sensor technology; Security and Privacy	4	First, to set up clear standard's framework, using also existing standards, second, implement these standards. Only written is not enough. For the smart cities ISO 37120 [i.9] is a good start, but not sufficient for the industrial implementation.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Interoperability of the platforms for IoT. I can get for example FIWARE create an IoT Solution and monitoring system, but then I decide to go for IBM and I need to pay extra to get everything working together. And then, if I decide to put special sensors, an SME is providing more problems since the SME access to FIWARE and IBM data specification is "difficult" = more money. The interoperability both at data level (semantic) as well as application level (services) should be granted by IoT solution providers as well as IoT platform providers. If not, business ROI is at risk.	Communication and Connectivity (application level); Integration/Interoperability; Applications life-cycle support; Infrastructure and computational platforms; IoT Architecture	4	There should be a common data model for IoT by which all solutions providers should work with, to ensure data interoperability at data base level. And providers should be forced to use these by ensuring governments will not use those platforms/solutions unless this data model (semantic) is used. This is the only way to force the big players. If they do not do so, they will not get government contracts (in general higher than normal). At the same time all platforms should provide a service layer in which other solution providers can communicate with the platforms. If not we are once again in the same problem. ROI could be negative if we need to change provider or a provider just goes out of business.
Getting access to systems and services from first-line providers.	Devices and sensor technology	3	This is more a business and engagement problem rather than a standardization issue.
Absence of a reference business model.	<empty>	4	To help on the easy digitalization of urban services.
Missing business models and value chains in the context of smart city.	Communication and Connectivity (service level); IoT Architecture	3	<empty>
Difficult to address ROI.	Communication and Connectivity (physical and link levels); Integration/Interoperability; Applications life-cycle support; Devices and sensor technology	4	- Facilitate growth of the market to reduce costs. - Help to define ROI business models.
Interoperability.	Integration/Interoperability; Security and Privacy	3	Present a proper framework for a common ontology, but most importantly - to introduce incentives/business models that make it attractive for sensor developers and service providers to adhere to the specifications defined in the framework and ontology.
Currently it is difficult for a provider to select the most adequate standards to provide to our customers, since the problem is that there are too many and actually there is no way to actually know which the "best" in real running deployments is. So our main decision driver reason is basically the physical communication configuration of the onsite of our customers as well as the actual sensors/actuators on-site.	Communication and Connectivity (service level)		If standards would provide more technical guidance of compatibility with other standards this will help going beyond on-site infrastructure.

Table 12: Survey results for the Smart Cities vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Privacy and security aspects not sufficiently covered, developed and not real, mature models/solutions seem to be available. This could limit IoT adoption Another social gap is that many decision makers does not have a real understanding of practical potentialities IoT can provide and a dissemination campaign would be useful addressing mainly Public admins.	Communication and Connectivity (network and service levels); Integration/Interoperability; IoT Architecture; Security and Privacy	3	IoT and big data pose new challenges to an acceptable model of privacy and security management and rules (in terms of civil rights and "industrial privacy/security" guarantees: it is necessary to find out new models /approaches.
Awareness of users; preparedness of business to pre-empt citizen's concerns; need for meaningful transparency and real choice.	Communication and Connectivity (application level); IoT Architecture; Security and Privacy	5	Ethical by design (ensuring transparency).
Lack of clear definition of liability for data privacy as it relates to providers of sensor solutions.	Devices and sensor technology; Security and Privacy	4	Clear specification of data privacy requirements in given use cases.
A way to standardize consumption performance and make sure we can compare one product to another product.	Infrastructure and computational platforms	4	<empty>
Privacy.	Security and Privacy	2	Clear explanation of privacy statements.
The main gap at this moment is linked to the actual lack of methodology based support for actually aiding an organization/person to actually analyse what is the actual purpose of the sensing and what is the problem to solve. At the same time there is also the need to actually be able to analyse whether sensing something is actually beneficial, both for society as well as from a business perspective (ROI). There should be social cities in which people actually talk to each other and create communities. Then these communities should reorganize and analyse what are their real problems and based on this, apply IoT based solutions. In a second step these solutions should be shared with other communities and potentially exploited. Technology is the enabler. And the ecological footprint should also be considered and assumed as a valid cost.	Applications life-cycle support	5	There should be some kind of body that could at some point establish what is the sensing infrastructure required or suitable in order not to mass produce sensors/actuators/others... while keeping the planet resource at safe. This is a bit out of the scope of the survey, but sensing all houses, cities uselessly is not the way to go. We should focus on those who really need these, ageing, people with disabilities, health issues ... It does not make sense to make every daily activity Smart, since that could drive to a non-sociable mass of people. Or it may not. But we should also think in this direction.

Table 13: Survey results for the Smart Cities vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Resource availability on the PHY layer (spectrum resources) Awareness of the regulatory framework.	Communication and Connectivity (physical and link levels)	4	Awareness generation to make provider, developers, researchers aware of these limits.
Lack of harmonisation and consensus on the right technology.	Communication and Connectivity (network up to application level); IoT Architecture; Security and Privacy	4	Agree on very few common standards.
Development models for data centric services residing on the edge of the Internet.	Communication and Connectivity (service and application levels); Integration/Interoperability	4	Provide a set of reference models for the development and integration of new services.
Lack of a unified model/tools for deployment and management of large scale distributed network of edge devices.	Integration/Interoperability; Infrastructure and computational platforms	4	Define high level management models and API.
Lack of harmonisation and lack of interoperability.	Communication and Connectivity (application level); Integration/Interoperability	5	Focus on semantic interoperability and a drive to use new technologies to push the market forward
Too many silos are now bring together under the "Smart Cities" paradigm => transversal communication needs are hard to put in place (problems of multiple translation among various heterogeneous models).	Communication and Connectivity (application level); Integration/Interoperability; Applications life-cycle support	3	Accelerate the convergence around pragmatic proposals.
Integration of different existent data assets is expensive.	Communication and Connectivity (network and service levels)	3	Define standards to integrate different data types.
Dedicated characteristics for quality assurance and reliability as well as their approval process.	Communication and Connectivity (physical up to network level)	3	Engagement of experts and acceleration of the work.
Definition of the standard(s) to be used to increase the number of projects based on a common infrastructure or technology.	Communication and Connectivity	3	A clear scenario with standardized protocols and applications, with a focus on interoperability.
Too many Standards.	Communication and Connectivity (network and service levels)	4	Open source should be developed alongside the standards.
Interoperability between vendors/solution.	Integration/Interoperability	4	Define interoperability standards.
As the gaps are related not only to Technology but also to Societal and Business, there is a combination of various natures of gaps. Proprietary solutions, lack of harmonisation and interoperability are the main ones.	Communication and Connectivity; Integration/Interoperability; Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology; Security and Privacy	3	When developing new solutions, having a standard to refer to it provides a decision support in deciding investments and to "orient" our customer towards real value selections.
Interoperability.	Integration/Interoperability	2	Standardization.

5.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Service platform*: no clear winner among all existing IoT architectures. Each service platform is currently positioning among the other one through the proposition of underlying interworking plugins.

- *Communication infrastructure*: the use of multiple communication infrastructures is here to stay due to the characteristics of each communication technology (LoRa, GPRS/3G/4G, Satellite, etc.). IP is likely the best candidate as a convergence layer.
- *Data interoperability*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue.
- *Security and Privacy*: IoT platforms have to ensure data privacy, integrity and transmission accordingly to the information sensibility.

6 Gap analysis in the context of Smart Living environments for ageing well

6.1 High level description and analysis

This clause describes at high level what the specificities of the Smart Living and Smart Home vertical sector are, based on the AIOTI WG03 [i.2] and AIOTI WG05 [i.5] reports.

The concept of Smart Home is becoming a reality. Smarter and more efficient homes increase daily, accelerated by connected devices being deployed at home (smartphones, tablets, domestic devices: lamps, presence sensors, etc.). However, the concept of Smart Home is targeting more innovative scenarios and applications including eHealth, elder people assistance, home automation, security monitoring, energy management, habitat comfort, entertainment, etc.

The Smart Living and Smart Home vertical sector can be divided into four main clusters:

- health and wellness: monitoring of patient data from home, transfer of these data to medical personnel, ability to call emergency services when needed, fitness support, socialization, daily tasks independence;
- habit: monitoring of people daily routine to detect abnormal situations;
- safety: security surveillance, fall detection, security issues;
- home automation: managing energy consumption, air conditioning, adjusting light intensity, controlling appliances.

Smart Home is currently a field that observes a high heterogeneity in devices and networking technologies. Indeed, a Smart Home is a stage to a wide variety of standard or proprietary PAN/LAN technologies. Such heterogeneity makes interoperability among the different deployed devices unachievable. This is mainly caused by a high fragmentation of the home devices market.

Even if the Smart Home is implemented in a limited and controlled environment, its realization is still subject to multiple challenges. Concerns about the ambient environment that is a Smart Home especially for aging well are often related to issues of accessibility, acceptability and ethical concerns. Accessibility is related to the financial affordability of automation systems, the ease of use of such technical systems, and psychological trust and acceptance.

In the context of Smart Home for aging well, data privacy and security is necessary. Indeed, for various applications very sensitive data are collected (health data, habitat monitoring, etc.). Access to such data should be strictly controlled in order to allow the proper functioning of the application.

6.2 Mapping of requirements and related standard coverage

6.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

6.2.1 Communication and Connectivity knowledge area

6.2.1.1 Connectivity at physical and link layer

Table 14: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Heterogeneous types of communications: wireless/wireline, long range/short range; different communications bandwidth, latency (real time)	3GPP, Bluetooth, Enocean Alliance, ETSI DECT, ETSI ERM, IEEE 802 LAN/MAN, IEEE PLC, KNX, LoRa Alliance, Thread Group, ZigBee, Z-Wave, etc. already provide a large set of standards in this knowledge area with varied characteristics.
Fragmentation of the standardization landscape	This is a potential gap.

6.2.1.2 Connectivity at network layer

Table 15: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Local and remote access to infrastructural services	3GPP (only covers part of the requirement. See also clause 6.2.2)
Device to device communications	Thread Group, Z-Wave, IETF ROLL
Connectivity and network communication protocols	DICOM, IETF (TCP/IP protocols), LON
Interoperability of networks: devices with different communication protocols are able to share data	DICOM, IETF 6lo, KNX
Connectivity platforms	KNX
High network availability performance behaviour	This is a potential gap
Real-time handling of events	This is a potential gap

6.2.1.3 Service level and application enablers

Table 16: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	DICOM, 3GPP, IETF CoRE
Unified services support a large variety of services	KNX
Semantic interoperability between service components	ITU-T
Advanced analysis and processing of sensor data	DICOM
Interoperability and collaboration of different appliances; combine wearable devices and Smart Home devices at protocol level	KNX, IETF CoRE
Real-time + batch handling of events/data	IETF XMPP, OASIS MQTT, OMG DDS

6.2.1.4 Application layer level, APIs, data models and ontologies

Table 17: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
Applications address heterogeneous use cases: direct needs (alarms, ease of use) but also hidden issues (social isolation, loneliness, support independence); access to services through social networks and messaging functions	ZigBee, KNX, LON. Part of these requirements is covered, so this is a potential gap
Messaging, documents standards	DICOM, IETF XMPP, OASIS MQTT, OMG DDS
Applications support a wide variety of services (discovery)	KNX
Heterogeneity management (data model included)	This is a potential gap
Open APIs. One interface to access several services	oneM2M (part of the architecture), ITU-T
Organization, structure (neutral data models) and storage of the data	HL7
Possibility of correlation of the data including their context	ETSI Smart M2M, OneM2M
Standards for data handling and organization	ITU-T
Self-management of health, with decision-making processes (cognitive and robotics)	IEEE P2413 (part of the architecture)
Standards for application processes	This is a potential gap

6.2.2 Integration/interoperability knowledge area

Table 18: Mapping of requirements for integration/interoperability

Requirements	Organizations providing related standards
Certification of sensors and devices. Approval process for quality assurance and reliability	Ipv6 Forum, Wi-Fi Alliance for connectivity. Other types of certifications are a potential gap
Integration of IoT services and solutions for healthcare	ETSI SmartBAN, Continua, ITU-T, IIC, IPSO Alliance, ZigBee
Local and remote access to infrastructural services	OCF, OneM2M
Device discovery; capability to include new devices, sensors, actuators when they join the system	Allseen Alliance
Communication platforms	HGI, oneM2M, OMA
Interoperability to address the IoT fragmentation by manufacturers and communication protocols. Interoperability between devices	ETSI SmartBAN (only covers part of the requirement). This is a potential gap
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	EnOcean Alliance. Allseen Alliance, ASHRAE, Continua design guidelines, IPSO Alliance, OCF
Interoperability of networks: devices with different communication protocols are able to share data	ASHRAE (only covers part of the requirement), CEN TC 247
Interoperability and collaboration of different appliances at system level	OMA, oneM2M
Interoperability of processing rules (structure, storage, exchange)	ASHRAE (only covers part of the requirement)
Unified services support the interoperability of services	ETSI SmartBAN, HGI, OMA, W3C
Service discovery	oneM2M, W3C
Common data "terminology" across the architecture, interoperable data semantics and ontology, common semantics	oneM2M, HL7, IHE
Seamless interoperability between data systems	HGI, IIC (part of the architecture), W3C. They only cover part of the requirement
Lightweight standard for data interoperability	
HMI components (user interfaces and displays) are very easy to use. Define optional or mandatory ease-of-install, ease-of-maintenance and ease-of-operation technologies	ETSI TC HF, IHE. They only cover part of the requirement
HMI components allow easy access to system from third-parties	OMA

6.2.3 Applications management knowledge area

Table 19: Mapping of requirements for applications management

Requirements	Organizations providing related standards
Applications tailored to individual needs: evolutivity, flexibility of the components	OSGi, DICOM, BBF, OMA
Continued support to the client after purchase	This is a potential gap
Tools to enable ease of installation, configuration and personalization	This is a potential gap

6.2.4 Infrastructure knowledge area

Table 20: Mapping of requirements for infrastructure

Requirements	Organizations providing related standards
Integration of legacy systems and data sources	3GPP, oneM2M, IEEE P2413 (part of the architecture)
Functional safety	IEC
Deployment tools	BBF, HGI, OSGi Alliance

6.2.5 IoT Architecture knowledge area

Table 21: Mapping of requirements for IoT Architecture

Requirements	Organizations providing related standards
System able to cope with the availability of multi-vendor solutions	Allseen Alliance (AllJoyn framework), OCF, Thread Group, IEEE P2413, IIC, ISO/IEC JTC1, ISO/IEEE PHD
Global-level standards (international)	OneM2M, IEEE P2413, ITU-T
More uniform, mixable solutions that can be easily translated to other application domains	This is a potential gap

6.2.6 Devices and sensor technology knowledge area

Table 22: Mapping of requirements for devices and sensor technology

Requirements	Organizations providing related standards
More comfortable, less invasive devices	This is a potential gap
Devices compensating sensory impairments	This is a potential gap
Various types of devices and sensors: low power/high power (sustainability, power consumption)	ETSI SmartBAN, IETF CORE, Bluetooth LE, Enocean Alliance (harvesting feature), ETSI DECT ULE, ZigBee
Performance behaviour and quality assurance: robustness, accuracy, reliability (for imaging and diagnostics)	Thread Group, ISO-IEC JTC1
Real-time + batch handling of devices	This is a potential gap
Device discovery in the ecosystem	Allseen Alliance, BBF, ETSI SmartBAN, IETF CORE, OMA
Sensors and devices accessible locally and remotely	BBF, OMA
Externalization of sensor data and remote control	BBF, ETSI SmartBAN, ISO/IEC JTC1, OGC, OMA

6.2.7 Security and privacy knowledge area

Table 23: Mapping of requirements for security and privacy

Requirements	Organizations providing related standards
High level of trust (common good objective)	This is a potential gap
Communication activities that advertise data security and privacy featured by the framework	This is a potential gap
End-to-end security	OneM2M, 3GPP, IETF
Data security	ISO/IEC
Confidentiality and privacy, protection of personal data; encryption	ETSI DECT, IEEE, OneM2M, W3C
Secure remote access to the system from third-parties; user authentication, access control	3GPP, HyperCat, IEEE 802.1x, OASIS

6.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Living and Smart Home vertical domain. The answers which spread across several domains, including the present one, are provided in clause 12. Answers related to the Smart Cities vertical domain may also be applicable here.

Table 24: Survey results for the Smart Living vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Unclear regulatory environment in Europe resulting blurring responsibility amongst Smart Home Providers and carriers.	Communication and Connectivity (network level); Infrastructure and computational platforms	4	AIOTI to recommend EC regulations changes.
Interoperability because the whole IoTis fragmented by manufacturers and communication protocols.	Integration/Interoperability; Devices and sensor technology; Security and Privacy	3	IoTindustry standardization increase the market size, means IoT will be easily available for end users.
Proprietary solutions and no real need from consumers at this moment.	Communication and Connectivity (application level); Integration/Interoperability	4	Push organizations towards interoperability on a semantic level.
There are many competing standards to achieve similar goals. Hence, it is still difficult to know which one will prevail.	Communication and Connectivity (network up to application level)	3	<empty>
Siloed systems.	<empty>	1	I think standards and regulation is about 3 years behind the actual IoT market. The market is giving me what I need, for admittedly simple needs. Standards and regulation could help to avoid the closure of closed source systems, life-cycle termination. I have avoided this with the open-source approach.
Proprietary solution, hype and overselling phase.	Communication and Connectivity (application level); Integration/Interoperability; Devices and sensor technology	3	Frequency band harmonisation, technology standardization for interworking and solution maturity.
Proprietary solutions, interoperability, feature and quality classification model.	Communication and Connectivity (service and application levels); Integration/Interoperability; Applications life-cycle support; Infrastructure and computational platforms	3	Classifications and certifications.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
In my day-to-day experience, the business-related challenges are the hardest to tackle. As a technical innovator, all technical problems can be solved given that organizations work together - or at least in the same direction. All problems: lack of (international) standards, poor security, privacy breaches, bad or lacking interoperability etc. all boils down to the fact that the technology vendors compete rather than work together, and that they put minimal-viable-products (or rather barely-viable-products) on the market. Such problems should be approached by business (or political) experts.	<empty>	4	Perhaps higher demands on the quality of products put on the market - software (including firmware) should be kept up-to-date for 5 - 10 years, harder requirements on privacy measures (and cash compensation to users victims of privacy breaches), etc.
Business justification.	Communication and Connectivity (service level); Integration/Interoperability	5	Platforms enabling multi-vendor sensors and common APIs for service applications with service functions such as data analysis, pay management, and consent management are required in standardized manner.
Proprietary solutions, lack of providers of interoperable solutions.	Communication and Connectivity; Integration/Interoperability; Security and Privacy	3	If a standard for interoperability is depicted as the standard to follow, it will expand the market from siloed solutions that are hard to switch between too many providers with interoperable solutions.
Smart living environment needs collaboration of siloed applications and services.	Communication and Connectivity (service and application levels)	5	Starting one service application like healthcare needs collaborative links with smart home service as living environment, smart cities as outside activities, smart social service like transportation priority dispatch, and smart work environment, to better serve consumers in a meaningful way. Also it creates value-chain.

Table 25: Survey results for the Smart Living vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Exact detection of needs in order not to become a producer of ideas/Proof-of-concepts that are not welcome/asked for	Applications life-cycle support; IoT Architecture; Devices and sensor technology	3	More uniform, mixable solutions that can be easily translated to other application domains
Too many fears from people that are not well informed block numerous ideas and potential novel solutions	Security and Privacy	4	Come up with frameworks and related communication activities that advertise data security and privacy featured by the framework
Ease-of-use	Integration/Interoperability; IoT Architecture	4	Define optional or mandatory ease-of-install, ease-of-maintenance and ease-of-operation technologies as part of the standard such as use of NFC
Security concerns by consumers about who would be able to see their data and detect if they are at home or not	Security and Privacy	4	Specify minimum levels of security/encryption for applications where house occupation can be established, e.g. for Smart Meters
Safety & Privacy of IoT systems	Security and Privacy	4	Standards should show how to address Privacy & Safety across the whole of an IoT system

Table 26: Survey results for the Smart Living vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lightweight standard for data interoperability	Communication and Connectivity (application level)	4	<empty>
Interoperability	Connectivity at Physical and Link layer	3	Interoperability between devices
Lack of access and harmonization	Applications life-cycle support; Devices and sensor technology	3	<empty>
Standards for one interface for many services	Communication and Connectivity (physical up to application level); Security and Privacy	3	Interoperability for consumers
Dedicated characteristics for quality assurance and reliability as well as their approval process	Communication and Connectivity (physical up to network level)	3	Engagement of experts and acceleration of the work
Interoperability (semantic level included), heterogeneity management (data model included), low power and low energy constraints integration, cyber security	Communication and Connectivity (physical up to application level); Integration/Interoperability; Infrastructure and computational platforms; Devices and sensor technology;Security and Privacy	4	<empty>
Lack of harmonization and interoperability on lower layers	Communication and Connectivity; Integration/Interoperability	3	Framework to create economy of scale for making a global harmonized business
Optimized solutions (PHY-MAC), semantic interoperability...also solutions for enhanced privacy and trust	Communication and Connectivity (all levels); Integration/Interoperability; Devices and sensor technology; Security and Privacy	4	Evolution of ongoing activities

6.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Service platform*: no clear winner among all existing IoT architectures. Each service platform is currently positioning among the other one through the proposition of underlying interworking plugins.
- *Connectivity*: a Smart Home is a place where very different network technologies and communications protocols are used. Securing high network availability, with certified performance figures, is necessary, making sure that no alarm is delayed.
- *Data interoperability*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue. Alert/alarm message content should be standardized to enable full understanding and comprehensive information by their recipients (e.g. alert sent when a person falls should indicate the issue, as well as location and date of the fall).
- *Interoperable processing rules*: to process the sensor data in an identical manner across heterogeneous platforms.
- *Devices and sensors*: certification rules according their consumption, accuracy, reliability, probably into classes of devices.
- *Autonomicity, decision-making processes:* To design autonomous control loops, defining the decisions and actions to be taken under the reception of specific sensor data (e.g. alert the medical personnel above a certain threshold of blood pressure measurement).
- *Security and privacy*: data security, data privacy and ownership, rules to ensure trust in a common good objective.
- *Ease of use*: Devices and systems should be accessible to a large non-technician public, including older people. This applies to the usage of the device, but also to its installation and maintenance, allowing secure remote access to perform this maintenance.

7 Gap analysis in the context of Smart Farming and food security

7.1 High level description and analysis

Smart Farming is about the application of data gathering (edge intelligence), data processing, data analysis and automation technologies on the overall value chain. Smart Farming is strongly related, but not limited, to the concepts of Precision Agriculture and Precision Livestock Farming. Farming modalities may include the production of vegetables, cattle (including dairy production) and others. Food safety refers to the awareness, prevention and risk-based measures of foodborne illnesses, from food production to consumption [i.11].

Food safety refers to the awareness, prevention and risk-based measures of foodborne illnesses, from food production to consumption [i.11]. Consumers' demands are currently the main drivers encouraging food industries to produce healthier and safe food products that being at their highest possible quality specifications. The challenge is that transparency of food safety should become data-driven and near real-time so that new applications and chain cooperation can lead to a more dynamic and responsive food production network.

According to AIOTI WG6, the main topics covered by the analysed initiatives for Smart Farming include:

- Plant Farming
- Livestock Farming
- Food processing

- Logistics
- Retail
- Food safety/health/traceability
- Consumer

7.2 Mapping of requirements and related standard coverage

7.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

7.2.1 Communication and Connectivity knowledge area

7.2.1.1 Connectivity at physical and link layer

Table 27: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Communications technologies should be resilient to external factors and possible issues in the infrastructure	3GPP, Bluetooth, Enocean Alliance, ETSI DECT, ETSI ERM, IEEE 802.x, IEEE, IETF 6lo, LoRa Alliance, ZigBee, Z-Wave
Heterogeneous types of communications: wireless/wireline, long range/short range; different communications bandwidth, latency (real time)	3GPP, Bluetooth, Enocean Alliance, ETSI DECT, ETSI ERM, IEEE 802.x, IEEE, IETF 6lo, KNX, LoRa Alliance, Thread Group, ZigBee, Z-Wave

7.2.1.2 Connectivity at network layer

Table 28: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Platforms should enable a better interaction channel among service providers and stakeholders. Platforms should support scalable models so they can dynamically adapt to the needs of the farmers. Platforms should use standardized models for representing data (syntactical interoperability). Platforms used should be, if possible, open platforms. Coexistence of open and proprietary services.	OpenAG Cloud IETF FiWare There is a potential gap on these requirements, as they cover only part of them
Technologies and models that allow to easily connect new devices with legacy systems should be used.	oneM2M, OASIS, OMA
Local and remote access to infrastructural services.	3GPP, OCF, oneM2M, Bluetooth
Device to device communications.	Thread Group, Z-Wave, IETF ROLL
Connectivity and network communication protocols.	IETF
Interoperability of networks: devices with different communication protocols are able to share data.	IETF oneM2M, LoRa Alliance, OMG, Zigbee, Z-wave
Communication platforms.	oneM2M, ITU-T
High network availability performance behaviour.	This is a potential gap
Real-time handling of events.	This is a potential gap

7.2.1.3 Service level and application enablers

Table 29: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	3GPP, OCF, IETF
Unified services support a large variety of services	OMA, W3C
Semantic interoperability between service components	ITU-T
Advanced analysis and processing of sensor data	
Interoperability and collaboration of different appliances	IETF, OMA, oneM2M
Real-time + batch handling of events/data	This is a potential gap

7.2.1.4 Application layer level, APIs, data models and ontologies

Table 30: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
Messaging, documents standards	IETF OASIS OMG
Applications support a wide variety of services (discovery)	oneM2M, W3C
Open APIs	oneM2M, ITU-T, OMA
Organization, structure (neutral data models) and storage of the data	oneM2M
Possibility of correlation of the data including their context	oneM2M
Use open data models and platforms in order to create a scalable virtual and global environment of cooperation Users should have control over how their data is being used and for what purposes	ITU-T, oneM2M

7.2.2 Integration/interoperability knowledge area

Table 31: Mapping of requirements for integration/interoperability

Requirements	Organizations providing related standards
Certification of sensors and devices	IPV6 Forum, Wi-Fi, … for connectivity
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	Enocean Alliance. Allseen Alliance,
Interoperability of processing rules (structure, storage, exchange)	
Common data "terminology" across the architecture, interoperable data semantics and ontology, common semantics	oneM2M
Seamless interoperability between data systems	

7.2.3 Applications management knowledge area

Table 32: Mapping of requirements for applications management

Requirements	Organizations providing related standards
Applications tailored to individual needs: evolutivity, flexibility of the components	OSGi, BBF
Continued support to the client after purchase	This is a potential gap
Tools to enable ease of installation, configuration and personalization	This is a potential gap

7.2.4 Infrastructure knowledge area

Table 33: Mapping of requirements for infrastructure

Requirements	Organizations providing related standards
For new deployments, standardized and/or open source hardware should be used if possible to avoid vendor lock-in. For older deployments, proper methods to interact with legacy hardware may be devised In an agro environment low power technologies will be useful. Self-powered hardware will help to harness self-sufficient operations: • Hardware architecture standards should be used so components can be easily incorporated into reference designs • Robustness, reliable and secure components • Affordable cost for deployments • Low maintenance, high autonomy, environmental endurance	ITU-T, oneM2M
Integration of legacy systems and data sources	oneM2M, IEEE
Deployment tools	
Functional safety	IEC

7.2.5 IoT Architecture knowledge area

Table 34: Mapping of requirements for IoT Architecture

Requirements	Organizations providing related standards
The chosen architecture model should be flexible enough to cover requirements from territories with different needs (geology, orography, agriculture models, etc.): • Standard interfaces and APIs are needed to connect applications or services from Farm Management Information Systems (FMIS) • Platforms should allow to compose services tailored and personalized for each user	ITU- T
System able to cope with the availability of multi-vendor solutions	AllJoyn, OCF, Thread Group, IEEE P2413, IIC, ISO/IEC JTC1, oneM2M
Global-level standards (international)	oneM2M, IEEE ITU-T
Device discovery; capability to include new devices, sensors, actuators when they join the system	Allseen Alliance, oneM2M

7.2.6 Devices and sensor technology knowledge area

Table 35: Mapping of requirements for devices and sensor technology

Requirements	Organizations providing related standards
Devices and infrastructure should be intelligent enough to serve farms without stable communications with the Internet: • Software should be aware of the device they are running on in order to adapt to its resources. Cloud service deployment may be a good option when there are no connectivity problems. • Well-adopted by industry, open • Compatible with multi-actor approach • User friendly interfaces	Drones standard (DO-178C, Software Considerations in Airborne Systems and Equipment Certification) Potential gap, no available European standards
Smart devices used to gather information from the fields, animals, and farms, and processed afterwards for creating models, forecasting behaviours or applying other analytical techniques	IETF, Bluetooth LE, EnOcean Alliance, ZigBee, OMA, ETSI, oneM2M
Devices and infrastructure should be intelligent enough to serve farms without stable communications with the Internet	Drones standard (DO-178C, Software Considerations in Airborne Systems and Equipment Certification) Potential gap, no available European standards
Real-time + batch handling of events/data	IETF, OMG, oneM2M, ZigBee Alliance, OCF, 3GPP
Sensors and devices accessible locally and remotely	BBF, OMA, M2.COM
Externalization of sensor data and remote control	BBF, ISO/IEC JTC1, OMA, M2.COM

7.2.7 Security and privacy knowledge area

Table 36: Mapping of requirements for security and privacy

Requirements	Organizations providing related standards
Use open data models and platforms in order to create a scalable virtual and global environment of cooperation: • Users should have control over how their data is being used and for what purposes. • Privacy should be preserved. • Even if decision support systems are used, in the end the farmer should have the last word to apply some expert system advice.	Cybersecurity Hypercat Potential gap
High level of trust (common good objective)	This is a potential gap
End-to-end security	oneM2M, 3GPP, IETF,
Data security	This is a potential gap, oneM2M
Confidentiality and privacy, protection of personal data; encryption	oneM2M, W3C, IEEE ETSI, ISO/IEC
Secure remote access to the system from third-parties; user authentication, access control	3GPP, OASIS, IEEE, IETF, oneM2M

7.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Farming vertical domain. The answers which spread across several domains, including the present one, are provided in clause 12.

Table 37: Survey results for the Smart Farming vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Competition avoids interoperability. Many different solutions, but nothing works together. Customer is frustrated.	Integration/Interoperability	5	Neutral party (faster definition, slow acceptance), or joint group (faster acceptance, but slow definition), to define starting point.
Interoperability because the whole IoT is fragmented by manufacturers and communication protocols.	Integration/Interoperability; Devices and sensor technology; Security and Privacy	3	IoT industry standardization increase the market size, means IoT will be easily available for end users.
The technology is there but the use cases are infinite and each of these will highlight a potentially different gap.	<empty>		Need to make sure vested interests don't overly influence standardization and hamper new entrants access to IoT platforms.
Interoperability due to competitive risks.	Integration/Interoperability	4	Have all equipment, whatever brand or make, work together as if it were designed as one integrated production system.

Table 38: Survey results for the Smart Farming vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of awareness and education, lack of access to broad band (in some regions), lack of transparency of communication offerings, in some case lack of ease of use, promised functionality is absent.	Communication and Connectivity (physical up to network level); Integration/Interoperability; Security and Privacy	4	The awareness and education is important at all levels (society, users, governments, education, decision makers). Each subjectivity in IoT should put a great emphasis on meeting stakeholders and dialoguing with them.

Table 39: Survey results for the Smart Farming vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Missing standard protocols for communication between wireless sensor networks and Cloud Servers. Now it is required an intermediate server to translate data to the required format by each platform.	Communication and Connectivity (network up to application level); Integration/Interoperability; Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology	3	A standard in this area will help to design the wireless network sensors system with the ability to operate with different cloud platforms without the need of an intermediate server. This way the hole system will be cheaper and robust.
Interoperability and harmonization lack.	Integration/Interoperability; IoT Architecture	3	Better communication and interoperability among all irrigation systems and devices.
Too many technologies, protocols and development frameworks for application.	Communication and Connectivity (application level); Integration/Interoperability; Applications life-cycle support	4	To improve business environment.

7.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Service platform*: Most of the platforms for Smart Farming are proprietary solutions and there are no specific standards to address common platforms.
- *Connectivity*: tools to enable ease of installation, configuration and personalization.
- *Data interoperability*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue. Alert/alarm message content should be standardized to enable full understanding and comprehensive information by their recipients (e.g. alert sent when a person falls should indicate the issue, as well as location and date of the fall).
- *Interoperable processing rules*: to process the sensor data in an identical manner across heterogeneous platforms.
- *Devices and sensors*: certification rules according their consumption, accuracy, reliability, probably into classes of devices especially in the use of Drones which are important devices in Smart Farming, there are no European standards available.
- *Autonomicity, decision-making processes:* to design autonomous control loops, defining the decisions and actions to be taken under the reception of specific sensor data.
- *Security and privacy*: data security, data privacy and ownership, rules to ensure trust in a common good objective.

8 Gap analysis in the context of Smart Wearables

8.1 High level description and analysis

This clause describes at high level what the specificities of the Smart Wearables vertical sector are, based on the AIOTI WG03 [i.2] and AIOTI WG07 [i.7] reports.

Wearable vertical is related to all connected devices that are temporary or permanently wore by an end-user. Smart Wearables can exist as independent objects such as a smart watch, heart monitor, etc. They can also be embedded within textiles, the so-called smart clothes, such as an activity monitor baby onesie, or a micro-radar-equipped jean acting as a user interface to a smartphone.

Wearable connected devices may exist either independently or connected to a mobile gateway which is usually a smartphone or a tablet. Indeed, some devices if connected with WLAN or WAN network access technologies can operate independently and communicate directly to remote services, while other devices connect through WPAN to a smartphone or a tablet in order to reach the targeted services running on this gateway or on remote servers.

Wearable my also refer to body area networks since different wearable objects may be connected through the same network (e.g. WPAN). For example, an end user may wear different sensors connected through Bluetooth to his/her smartphone.

8.2 Mapping of requirements and related standard coverage

8.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

8.2.1 Communication and Connectivity knowledge area

8.2.1.1 Connectivity at physical and link layer

Table 40: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Heterogeneous types of communications: wireless, long range/short range; different communications bandwidth, latency (real time)	3GPP, Bluetooth, EnOcean Alliance, ETSI ERM, IEEE, LoRa Alliance, Thread Group, ZigBee, Z-Wave, etc.
Infrastructure-based communication	3GPP, ETSI, IEEE, LoRa Alliance
Ad hoc communications	ETSI, IEEE, DASH7 Alliance, EnOcean Alliance,
Real-time communications	3GPP, ETSI, IEEE
Mobility support	ETSI, IEEE, 3GPP

8.2.1.2 Connectivity at network layer

Table 41: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Local and remote access to infrastructural services	3GPP, OCF, OneM2M
Device to device communications	Thread Group, IEEE, Z-Wave, ZigBee, Bluetooth
Connectivity and network communication protocols	IETF (TCP/IP protocols)
Interoperability of networks: devices with different communication protocols are able to share data	IETF (TCP/IP protocols), IEEE
Communication platforms	HGI, oneM2M
High network availability performance behaviour	This is a potential gap
Real-time handling of events	ETSI SmartBAN
Priority handling of different data flows	ETSI SmartBAN

8.2.1.3 Service level and application enablers

Table 42: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	3GPP, OCF, IETF CORE
Unified services support a large variety of services	HGI, OMA, W3C
Semantic interoperability between service components	ETSI SmartBAN, ITU-T
Interoperability and collaboration of different appliances; interaction between wearables and IoT environments (e.g. Smart Living)	ETSI SmartBAN, IETF CORE, OMA, oneM2M, Thread Group
Real-time + batch handling of events/data	This is a potential gap

8.2.1.4 Application layer level, APIs, data models and ontologies

Table 43: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
HMI components (user interfaces and displays) are very easy to use both for enthusiast early adopters and rejecters	ETSI TC HF
Messaging, documents standards	HL7, IETF XMPP, OASIS MQTT, OMG DDS
Applications support a wide variety of services (discovery)	oneM2M, W3C
Open APIs	ETSI SmartBAN, oneM2M, ITU-T, OMA
Self-management of health, with decision-making processes (cognitive and robotics)	IEEE P2413
Standards for application processes	This is a potential gap
Organization, structure (neutral data models) and storage of the data	HL7, W3C
Possibility of correlation of the data including their context	ETSI SmartBAN, oneM2M
Standards for data handling and organization	ITU-T

8.2.2 Integration/interoperability knowledge area

Table 44: Mapping of requirements for integration/interoperability

Requirements	Organizations providing related standards
Clinical certification of wearable devices	This is a potential gap
Certification of sensors and devices	This is a potential gap
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	AllSeen Alliance, ETSI SmartBAN, EnOcean Alliance, IETF XMPP, IPSO Alliance, OCF, oneM2M
Common data "terminology" across the architecture, interoperable data semantics and ontology, common semantics	oneM2M, HL7, W3C
Seamless interoperability between data systems	IIC, W3C

8.2.3 Applications management knowledge area

Table 45: Mapping of requirements for applications management

Requirements	Organizations providing related standards
Application specification	This is a potential gap
Local and remote application management (configuration, installation, start/stop, update, etc.)	OMA LWM2M, OSGi
Application performances' monitoring	This is a potential gap
Applications tailored to individual needs: evolutivity, flexibility of the components	This is a potential gap
Continued support to the client after purchase	This is a potential gap
Tools to enable ease of installation, configuration and personalization	This is a potential gap

8.2.4 Infrastructure knowledge area

Table 46: Mapping of requirements for infrastructure

Requirements	Organizations providing related standards
Integration with legacy systems and data sources	ETSI, oneM2M, AllSeen Alliance
Deployment tools	OSGi
High speed low latency network infrastructure	ETSI, 3GPP
Functional safety	IEC

8.2.5 IoT Architecture knowledge area

Table 47: Mapping of requirements for IoT Architecture

Requirements	Organizations providing related standards
Device discovery	AllSeen Alliance, ETSI SmartBAN, oneM2M,
Support for multi-vendor solutions	AllJoyn, ETSI SmartBAN, OCF, Thread Group, IEEE P2413, IIC, ISO/IEC JTC1
Global-level standards (international)	oneM2M, IEEE P2413, ITU-T

8.2.6 Devices and sensor technology knowledge area

Table 48: Mapping of requirements for devices and sensor technology

Requirements	Organizations providing related standards
More comfortable, less invasive devices	This is a potential gap
Various types of devices and sensors: low power/high power (sustainability, power consumption)	ETSI SmartBAN, IETF COAP & CORE, Bluetooth LE, EnOcean Alliance, ZigBee, IEEE RuBee
Device discovery in the ecosystem	ETSI SmartBAN, oneM2M, AllSeen Alliance, OMA, BBF, IETF CORE
Real-time + batch handling of events/data	IETF XMPP, OASIS MQTT, OMG DDS
Sensors and devices accessible locally and remotely	oneM2M, OMA, BBF
Externalization of sensor data and remote control	ETSI SmartBAN, oneM2M, OMA, BBF
Sensor data quality	ETSI SmartBAN (covers only part of the requirement). This is a potential gap
Device modularity and support for multiple functions	MIPI Alliance (UniPro)

8.2.7 Security and privacy knowledge area

Table 49: Mapping of requirements for security and privacy

Requirements	Organizations providing related standards
High level of trust (common good objective)	This is a potential gap
End-to-end security	oneM2M, 3GPP, IETF
Data security	This is a potential gap
Confidentiality and privacy, protection of personal data; encryption	oneM2M, IEEE
Secure remote access to the system from third-parties; user authentication, access control	oneM2M, 3GPP, OASIS, IEEE 802.1x

8.3 Result of the survey

The next table gives a selection of answers received through the survey for the Smart Wearables vertical domain.

The next tables give a selection of answers received through the survey for the Smart Wearables vertical domain. The answers which spread across several domains, including the present one, are provided in clause 12. Answers related to the Smart Living vertical domain may also be applicable here.

Table 50: Survey results for the Smart Wearables vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Business stakeholders are confused because of the large number of initiatives, need to be guided how to make choices, to learn how to make business case for IoT, make roadmaps and govern this roadmap with a fast renewal cycle.	All KAs are involved	3	Interacting with the business community, educate, give visibility helping companies creating their roadmaps for profitable IoT applications using the right standardization for the right time frame.

Table 51: Survey results for the Smart Wearables vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Too many fears from people that are not well informed block numerous ideas and potential novel solutions.	Security and Privacy	4	Come up with frameworks and related communication activities that advertise data security and privacy featured by the framework.
Privacy challenge as consumers are not aware of personal data being exposed by IoT devices, and cannot babysit them permanently, plus security risks for critical infrastructures (transport, energy).	Integration/Interoperability; Applications life-cycle support; Security and Privacy	3	Promote establishment of proper regulation and their alignment across EU member states.
Technically, everything is inter-connectable. But it's still a misery for the end user to do it; plug and play is not a reality unless you stay in one vertical. It's important to make the technology invisible and come to a "it just works" environment which covers privacy, connectivity, energy, etc.	Communication and Connectivity (application level); Integration/Interoperability; Security and Privacy	4	Too many discussions on a technical level ("how" it works); not enough on what the average user needs, which is "WHAT it does". Start from that, and make sure the technology follows under the hood.

Table 52: Survey results for the Smart Wearables vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of harmonization and lack of interoperability.	Communication and Connectivity (physical, link and application levels); Integration/Interoperability; IoT Architecture; Devices and sensor technology; Security and Privacy	4	Devices with ICT capabilities should be more open to expose and consume services to/from others, creating the possibility to experience new concepts as a consequence of the creative combination of devices for solving real life problems. There are some "open" interfaces that are followed by specific devices but many on the market follow a closed approach. Definitely, interoperability problems are not technical but influenced by private business models of big corporations.
Interoperability.	Communication and Connectivity (physical up to application level); Integration/Interoperability	3	Define interoperability framework.
Lack of interoperability.	Communication and Connectivity (network and service levels); Integration/Interoperability; IoT Architecture; Security and Privacy	4	Reduce interoperability issues, allow for providing generic IoT services.

8.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Service platforms*: No service platform stands out in the field of Smart Wearables. Also, no specific service platform has been deployed specifically for Smart Wearables.
- *Connectivity*: Different networking and communications standards are used for Smart Wearables. Short range communications technologies are often used.
- *Data interoperability*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue.
- *Devices certification*: as Smart Wearables are electronics to be closer to the human body, clinical certification of devices is an issue. Moreover, the certification process of the whole wearable device does not allow rapid innovation. Standards for incremental and modular certification are needed.
- *Devices modularity*: No real standard targets the device modularity, i.e. the ability to add/remove hardware capabilities to a device.
- *Security and privacy*: Since Smart Wearables devices are dealing with very sensitive and personal data. Security and data privacy standards are necessary. The lack of these standards prevents user acceptability from both enthusiasts and rejecters.

Moreover, the following societal and business requirements are potential gaps.

- Societal:
  - User acceptance
  - Data privacy (storage, transport, processing)
  - Legal framework to support Smart Wearables deployment
- Technical:
  - Interoperability between different devices/platforms

9 Gap analysis in the context of Smart Mobility (smart transport/smart vehicles/connected cars)

9.1 High level description and analysis

This clause describes at high level what the specificities of the smart mobility vertical sector are, based on the AIOTI WG03 [i.3] and AIOTI WG09 [i.6] reports.

The concept of Smart Mobility encompasses a wide range of applications and scenarios. Human and goods transportation can use plane, train, road or simply foot; it can be public or private. Road is the most diversified of these means of transportation, with trucks carrying freight, buses carrying passengers, private or shared cars, cycles, animals and pedestrians.

For many years, the transportation domain evolution has been focused on mechanical improvements. In the last years, it has become the target of digital technologies and communications for all the use cases described above. Smart Mobility is the result of merging the transportation domain with the knowledge acquired using the digital domain, and more specifically the IoT, to enhance its efficiency.

Same as the other vertical domains, Smart Mobility observes a high heterogeneity of devices and networking technologies, ranging from radars to Internet communications. New technologies have emerged for enhanced applications: vehicular safety communications, fleet management for commercial vehicles or public transport, ticketing, connected parking, automated driving, automated freight transport, tolling systems, heavy goods vehicle rules enforcement with smart tachograph, etc. The requirements address the mobility itself, with a seamless connectivity, but also its practicality and its safety. As the large public is affected by these enhancements, the new technologies are expected to address primarily practicability, but also privacy and security besides the technical improvements, together with business attractiveness. Another important topic is the upgrade of the regulatory framework to follow this evolution. As an example, authorities are now facing the request to authorize automated vehicles on public roads.

9.2 Mapping of requirements and related standard coverage

9.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

9.2.1 Communication and Connectivity knowledge area

9.2.1.1 Connectivity at physical and link layer

Table 53: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Heterogeneous types of communications: wireless/wireline, long range/short range; different communications bandwidth	3GPP, Bluetooth, IEEE 802 LAN/MAN, IEEE P1609, ETSI TC ITS, ITU-R, ZigBee, etc. already provide a large set of standards in this knowledge area with varied characteristics
Mobility (including high speed)	ETSI TC ITS, IEEE, CEN/ISO, 3GPP
Real-time communications	3GPP, ETSI, IEEE
Congestion control	ETSI, SAE INTERNATIONAL
D2D communication without any infrastructure	ETSI, 3GPP
ITS stations to communicate with low-power sensor networks over IPV6 (6LoWPAN)	IETF 6lo

9.2.1.2 Connectivity at network layer

Table 54: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Local and remote access to infrastructural services	3GPP, ETSI TC ITS, IEEE 802 LAN/MAN, IEEE P1609
Device to device communications	IETF, IEEE 802 LAN/MAN, 3GPP V2X
Connectivity and network communication protocols	ETSI, CEN/ISO, IEEE 802 LAN/MAN, IEEE P1609
High network availability performance behaviour	This is a potential gap
Real-time handling of events and communications	3GPP, ETSI, CEN/ISO, IEEE
Mobility (including high speed)	IETF, ETSI TC ITS, IEEE, CEN/ISO, 3GPP
Congestion control	ETSI TC ITS, SAE INTERNATIONAL
V2X communication, using varied access networks: 802.11p, Wi-Fi, 3G/4G, etc.	CEN/ISO, ETSI, IETF
Addressable through internet addressing (i.e. IPV6)	IETF, IPV6 Forum

9.2.1.3 Service level and application enablers

Table 55: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	3GPP, IETF, CiA
Unified services support a large variety of services	ETSI TC ITS, SAE INTERNATIONAL
Real-time + batch handling of events/data	CEN/ISO, ETSI, IEEE
Common semantic between messages (Data Dictionary)	ETSI TC ITS, SAE INTERNATIONAL

9.2.1.4 Application layer level, APIs, data models and ontologies

Table 56: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
HMI components (user interfaces and displays) are very easy to use	ETSI TC HF, SAE INTERNATIONAL, CEN/ISO
Customization and user-specified adaptation	This is a potential gap
Messaging	IETF XMPP, OASIS MQTT, OMG DDS
Applications support a wide variety of services (discovery)	SAE INTERNATIONAL
Applications support a wide variety of services (use cases)	3GPP V2X, ETSI TC ITS, IETF ITS, SAE INTERNATIONAL
Real-time + batch handling of events/data	IETF XMPP, OASIS MQTT, OMG DDS
Decision-making processes (cognitive and robotics)	This is a potential gap (left to market competition)
Standards for data handling and organization	This is a potential gap
Traffic data handling and analysis (fusion, cleaning, processing, mining, etc.)	This is a potential gap

9.2.2 Integration/interoperability knowledge area

Table 57: Mapping of requirements for integration/interoperability

Requirements	Organizations providing related standards
Certification of sensors and devices	IPV6 Forum, Wi-Fi Alliance, … for connectivity, C2C-CC, AVNU Alliance, CCC
Integration of IoT services and solutions for ITS	3GPP V2X, CEN/ISO, ERTICO, ETSI TC ITS, IPSO Alliance, ITU-R
Unified services support a large variety of services	OMA
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	ACEA, IPSO, AVNU Alliance
Communication platforms	ERTICO
Common data "terminology" across the architecture, interoperable data semantics and ontology, common semantics	ETSI TC ITS, SAE INTERNATIONAL
Seamless interoperability between data systems, necessity to demonstrate synergies and spill over effects with other vertical areas (e.g. Smart Cities)	CEN/ISO, ETSI TC ITS
Interoperability for equivalent messages defined at regional level (e.g. CAM and BSM)	This is a potential gap
Interoperability for communications between the different regions	ITU-R
Support mixed road traffic conditions	ETSI TC ITS, 3GPP V2X, CEN/ISO, IEEE P1609
System interoperability testing and performance metrics	ETSI TC ITS, CEN/ISO, SAE INTERNATIONAL

9.2.3 Applications management knowledge area

Table 58: Mapping of requirements for applications management

Requirements	Organizations providing related standards
Applications tailored to individual needs: evolutivity, flexibility of the components	OSGi, CEN/ISO, IEEE P1609
Continued support to the client after purchase	CCC (they only cover part of the requirements)
Tools to enable ease of installation, configuration and personalization; usability and convenience	CCC (they only cover part of the requirements)
Adapt to longer vehicle life-cycle. Upgradability	OSGi, CCC

9.2.4 Infrastructure knowledge area

Table 59: Mapping of requirements for infrastructure

Requirements	Organizations providing related standards
Integration with legacy systems and data sources	ETSI, CEN/ISO
Deployment tools	BBF, OSGi Alliance
Higher scalability, pervasiveness, and integration into the core of the future internet.	IEEE, CEN/ISO, ITU-T, OAA
High speed low latency network infrastructure	3GPP, ETSI TC ITS
Edge cloud communication	CEN/ISO
Enhanced proper infrastructure to support communications in road transportation	CEN/ISO
Enhanced proper infrastructure to support automated driving	This is a potential gap
Functional safety	IEC, ISO

9.2.5 IoT Architecture knowledge area

Table 60: Mapping of requirements for IoT Architecture

Requirements	Organizations providing related standards
System able to cope with the availability of multi-vendor solutions	ETSI TC ITS, IEEE P1609, 3GPP V2X, CEN/ISO, AIOTI HLA
Global-level standards (international)	ISO, oneM2M They only cover part of the requirements. Harmonization of regional standards is a potential gap
Support vehicles, infrastructure and pedestrian transportation	ETSI TC ITS, IEEE P1609

9.2.6 Devices and sensor technology knowledge area

Table 61: Mapping of requirements for devices and sensor technology

Requirements	Organizations providing related standards
Various types of devices and sensors: low power/high power (sustainability, power consumption)	IETF CoAP & CORE, Bluetooth LE, ZigBee, IEC
Position accuracy and performance (GNSS, etc.)	ETSI TC SES
performance behaviour: robustness, accuracy, reliability and resilience over long period of time	This is a potential gap
Real-time + batch handling of events/data	CiA, AVNU Alliance
sensors and devices accessible locally and remotely	CiA, AVNU Alliance

9.2.7 Security and privacy knowledge area

Table 62: Mapping of requirements for security and privacy

Requirements	Organizations providing related standards
Trust, security and data privacy issues at all levels: preventing, detecting, and responding to unauthorized access, eavesdropping, jamming, and spoofing	CEN/ISO, ETSI TC ITS, IEEE P1609, 3GPP, W3C
Data integrity	ETSI TC ITS, Hypercat

9.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Mobility vertical domain. The answers which spread across several domains, including the present one, are provided in clause 12. Answers related to the Smart Cities vertical domain may also be applicable here.

Table 63: Survey results for the Smart Mobility vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
An integrated IoT end-to-end technical architecture is needed to include the requirements of vehicle manufacturers, vehicle repair shops, vehicle insurances, vehicle dealers, vehicle rental providers, vehicle car sharing providers and many others that require digital access to in-vehicle data for their business. Some technical solutions already exist in the domain of electric mobility to interlink charging stations operators from an EU project which demonstrated a virtual digital marketplace were "service providers" and "service requesters" of digital information create offerings and exchange data between the system ecosystem partners. It can be noted that similar gaps exist also in other vertical areas such as appliances and heavy equipment.	IoT Architecture	4	An integrated vertical IoT architecture.
Delayed decision for deployment by key stakeholders.		5	Ease deployment.
Both ITS G5 and LTE V2X target the same application of intra-vehicle connectivity, which causes duplication and potentially fragmented market with little interoperability.	Communication and Connectivity (physical up to network level); Integration/Interoperability	4	Ensure that the V2I units can cost effectively support both types of connectivity; find the right regulatory tools how the compatibility of different connectivity standards can be ensured while not picking winners beforehand.

Table 64: Survey results for the Smart Mobility vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
In the societal category, there is a missing consensus on privacy. There is a wide spectrum of opinion about what is acceptable.	Communication and Connectivity (physical up to network level); Security and Privacy	2	Regulations can be used to build consensus on privacy. Standards can provide the tools to protect privacy appropriately.
Missing features for pollution management problem.	Communication and Connectivity (application level); IoT Architecture	4	Study the problem of how ITS systems can reduce this challenge.

Table 65: Survey results for the Smart Mobility vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of naming mechanism referential.	Communication and Connectivity (physical up to application level); IoT Architecture; Devices and sensor technology; Security and Privacy	5	We need a mechanism like DNS to harmonize all the things.
A technology gap is how to effectively use multiple communication technologies, the best choice of which may vary in time and space, i.e. how to operate in a heterogeneous communication environment.	Communication and Connectivity (physical up to service level)	2	Standards can help address the heterogeneous communication environment by balancing flexibility with efficiency. I mean that we need a solution that not only is flexible enough to make use of multiple technologies, but is not so vague that it cannot be cost-effectively implemented.
Networking protocols.	Communication and Connectivity (network level)	5	Extensive use of TCP/IP family of protocols.

9.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Connectivity*: a smart vehicle is a place where very different network technologies and communications protocols are used. Securing high network availability, with certified performance figures, is necessary, making sure that no safety-related message is lost.
- *Position accuracy*: to locate with sufficient precision the position of the vehicle, based on the application requirement.
- *Data handling*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue. Vehicles will generate a huge amount of data, that need to be processed and shared with all relevant stakeholders.
- *Interoperable decision-making processing rules*: to process the sensor data and received messages in an identical manner across heterogeneous platforms.
- *Decision-making processes:* To design autonomous control loops, defining the decisions and actions to be taken under the reception of specific sensor data and messages.
- *Devices and sensors*: certification rules according their consumption, accuracy, reliability, probably into classes of devices.
- *Security and privacy*: data security, data privacy and ownership, rules to ensure trust in a common good objective and avoid vehicle spoofing.
- *Duplication of standards according to different regions of the globe*: to enable the interoperability of the regional standards and allow the usage of devices from one region in the others.
- *Fragmentation of the technology according to the target application:* to ensure consistency and if possible similarity between the technologies addressing the same needs, but in different market sub-segments.
- *Usability and customization of the solutions:* to address these different market sub-segments and simplify their usage by the large public.

Moreover, the following societal and business requirements are potential gaps:

- Societal:
  - User acceptance.
  - Laws governing the usage of autonomous cars on public roads.
  - System liability in case of accident.
  - Net neutrality.
  - Regulatory adaptations to support new technologies, legal framework.
- Business:
  - Deployment strategy.
  - Economic evaluation based on two perspectives: industry business models and societal usefulness and benefit.

10 Gap analysis in the context of Smart Environment (smart water management)

10.1 High level description and analysis

This clause specifically focuses on Smart Environment in relation to Smart Water/Energy as this is where most of the gaps are, as mentioned in ETSI TR 103 375 [i.1].

Smart environments are sets of solutions and systems that make use of new information communication technologies in order to enable water and energy grids operators to control, to diagnosis, to manage continuously and remotely maintenance operations and to use the collected data to optimize all the performance aspects of water and energy distribution.

Similarly to electricity consumption, water demand is not constant during a day (the morning and the evening are consumption peaks). However, unlike electricity, it is impossible to adapt water supply to the actual demand. Indeed, water production is at a fixed rate. To cope with an increase in the water demand, sufficient reserves are necessary, and unlike electricity, water can be stored. It is then possible to store water in prediction of a consumption peak.

To this end, smart environments solutions based on standards for IoT and M2M communications are the key to a more sustainable environment where water and energy are supplied and consumed more efficiently.

10.2 Mapping of requirements and related standard coverage

10.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

10.2.1 Communication and Connectivity knowledge area

10.2.1.1 Connectivity at physical and link layer

Table 66: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Support of heterogeneous communications: wireless/wired, short/long range,	3GPP, DASH7 Alliance, ETSI ERM, IEEE 802.x, IEEE PLC, ISO/IEC JTC1, ITU-T, LoRa Alliance, ZigBee Alliance
Support of Infrastructure-based communication	3GPP, ETSI ERM, IEEE 802.x, LoRa Alliance, ISO/IEC JTC1, ITU-T
Support of Ad hoc communications	DASH7 Alliance, IEEE 802.x, IEEE PLC, ISO/IEC JTC1, ITU-T, LoRa Alliance
Real-time communications	This is a potential gap

10.2.1.2 Connectivity at network layer

Table 67: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Local and remote access to infrastructural services	3GPP, ETSI ERM, IEEE 802.x, IEEE PLC, IETF, ITU-T, LoRa Alliance
Device to device communications	Bluetooth, DASH7 Alliance, IEEE 802.x, IEEE PLC, IETF, ISO/IEC JTC1, ITU-T, ZigBee Alliance
Connectivity and network communication protocols	IETF
Interoperability of networks: devices with different communication protocols are able to share data	IEEE 802.x, IEEE PLC, IETF
Communication platforms	oneM2M, ITU-T
High network availability performance behaviour	This a potential gap
Real-time handling of events	This a potential gap
Priority handling of different data flows	This a potential gap

10.2.1.3 Service level and application enablers

Table 68: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	3GPP, CEN, IETF, ETSI ERM, ISO/IEC JTC1, LoRa Alliance, OASIS MQTT, ZigBee Alliance
Unified services support a large variety of services	oneM2M, OMA
Semantic interoperability between service components	ISO/IEC JTC1, ITU-T
Interoperability and collaboration of different appliances	IETF, oneM2M
Real-time + batch handling of events/data	This a potential gap

10.2.1.4 Application layer level, APIs, data models and ontologies

Table 69: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
HMI components (user interfaces and displays) are very easy to use both for enthusiast early adopters and rejecters	CEN
Messaging, documents standards	IETF, OASIS
Applications support a wide variety of services (discovery)	IETF, oneM2M, OMA
Open APIs	ITU-T, oneM2M, OMA
Standards for application processes	This a potential gap
Organization, structure (neutral data models) and storage of the data	W3C
Possibility of correlation of the data including their context	oneM2M
Standards for data handling and organization	ITU-T, W3C

10.2.2 Integration/interoperability knowledge area

Table 70: Mapping of requirements for integration/interoperability

Requirements	Organizations providing related standards
Certification of sensors and devices	Ipv6 Forum, Wi-Fi Alliance, WiMax Forum, ZigBee Alliance
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	AllSeen Alliance, IETF, IPSO Alliance, Ipv6 Forum, ISO/IEC, ITU-T, OCF, oneM2M
Common data "terminology" across the architecture, interoperable data semantics and ontology, common semantics	oneM2M, W3C
Seamless interoperability between data systems	AllSeen Alliance, IETF, OCF, oneM2M

10.2.3 Applications management knowledge area

Table 71: Mapping of requirements for applications management

Requirements	Organizations providing related standards
Application specification	This a potential gap
Local and remote application management (configuration, installation, start/stop, update, etc.)	BBF, ISO/IEC, OMA, OSGi Alliance
Application performances' monitoring	This a potential gap
Applications tailored to individual needs: evolutivity, flexibility of the components	This a potential gap
Continued support to the client after purchase	This a potential gap
Tools to enable ease of installation, configuration and personalization	This a potential gap

10.2.4 Infrastructure knowledge area

Table 72: Mapping of requirements for infrastructure

Requirements	Organizations providing related standards
Integration with legacy systems and data sources	3GPP, IEEE 802.x, ITU-T, LoRa Alliance, oneM2M
Deployment tools	OSGi
High speed low latency network infrastructure	3GPP, IEEE 802.x, ITU-T
Functional safety	IEC

10.2.5 IoT Architecture knowledge area

Table 73: Mapping of requirements for IoT Architecture knowledge area

Requirements	Organizations providing related standards
Exchange of data for water pressure Standard information model for the representation of water observations data	ZigBee Alliance, oneM2M, OGC, ISO, ETSI/CEN CENELEC

10.2.6 Devices and sensor technology knowledge area

Table 74: Mapping of requirements for devices and sensor technology knowledge area

Requirements	Organizations providing related standards
Configuration of outstation and ability for interoperability	PSA
Data collection device, Sensor devices,	3GPP, ETSI, ISO/IEC.JTC, IEEE, oneM2M

10.2.7 Security and privacy knowledge area

Table 75: Mapping of requirements for security and privacy knowledge area

Requirements	Organizations providing related standards
High level of trust (common good objective) bootstrap authentication and key agreement for application security	3GPP, W3C
End-to-end security	3GPP, Hypercat, IEEE, IETF
Confidentiality and privacy, protection of personal data; encryption	OASIS, ISO/IEC
Secure remote access to the system from third-parties; user authentication, access control	IEEE, Hypercat

10.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Environment vertical domain. The answers which spread across several domains, including the present one, are provided in Clause 12.

Table 76: Survey results for the Smart Environment vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Project funding.	<empty>	5	Coordinated and coherent protocols, policies and programmes.
Business are confused because of the large number of initiatives, need to be guided how to make choices, to learn how to make business case for IoT, make roadmaps and govern this roadmap with a fast renewal cycle.	All KAs are involved	3	Interacting with the business community, educate, give visibility helping companies creating their roadmaps for profitable IoT applications using the right standardization for the right time frame.

Table 77: Survey results for the Smart Environment vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
<empty>	<empty>	<empty>	<empty>

Table 78: Survey results for the Smart Environment vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
For interoperability we need to combine the application (energy related) communication standards with horizontal IoT standards. Furthermore harmonization of data models.	Communication and Connectivity (service and application levels); Integration/Interoperability; IoT Architecture	5	Cooperation between the IoT community and energy community. The IoT community should consider the already existing vertical standards with focus on data models and Use Cases for energy management. Currently we are working with the M2M community to integrate the technologies and use M2M as a horizontal (lower) layer in communication.
No consensus around the most appropriate frameworks/protocols means duplicate effort and lack of traction of a specific solution. Reaching consensus between stakeholders on the standards for connection the Smart Metering Infrastructure with In-home Energy display/management devices for a start.	Communication and Connectivity; Integration/Interoperability; IoT Architecture; Devices and sensor technology	4	The issue is around the rate of market adoption for IoT products. Industry agreement over the adoption of a preferred solution for home energy management is key. We don't need new standards here but a multi-stakeholder agreement on the possible combinations of standards.
Lack of appropriate software; lack of interoperability among diverse vendors' solutions for sensor networks and operations.	Communication and Connectivity (service level); Integration/Interoperability; IoT Architecture; Devices and sensor technology	3	To push collaborative solutions shared by vendors, telecom operators, software developers, etc.

10.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

Currently, the main gaps are the following:

- *Service platform*: no clear winner among all existing IoT architectures. Each service platform is currently positioning among the other one through the proposition of underlying interworking plugins.
- *Connectivity*: Different networking and communications standards are used for smart environments. Lot of standards are from the sensor network and the energy/water communities.
- *Data interoperability*: A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue.
- *Security and privacy*: Smart environment data, especially those from utilities (energy/water) can be very sensitive. Security and data privacy standards are necessary. The lack of these standards prevent large scale deployments.

Moreover, the following societal and business requirements are potential gaps.

- Societal
  - Data privacy (storage, transport, processing)
  - Legal framework
- Technical
  - Interoperability between different devices/platforms: especially between energy and ICT platforms

11 Gap analysis in the context of Smart Manufacturing

11.1 High level description and analysis

This clause describes at high level what the specificities of the Smart Manufacturing vertical sector are, based on the AIOTI WG03 [i.2] and AIOTI WG11 [i.8] reports.

Conceptually, the challenge of Smart Manufacturing is to massively integrate new technologies such as IoT or Cloud Computing in order to provide much more flexibility, adaptability and security. This will require achieving a transition from:

- the current model based on the current "Manufacturing pyramid" approach, illustrated in figure 2, where the different layers of the pyramid are quite hierarchically separated and the communication between the bottom layer of IoT devices and the upper layer of the production system at-large are complex and the supporting data models often too much specialized;

to

- the "Cyber-Physical Production System" (CPPS) approach, illustrated in figure 3, where it is expected that the field level (e.g. the factory, the robots, the sensors) will be connected with a wider range of applications and services - making use of the vast quantities of data available to plan, monitor, re-tool and maintain, etc. - together with being ensured a higher level of trust and security from a redefined security architecture.

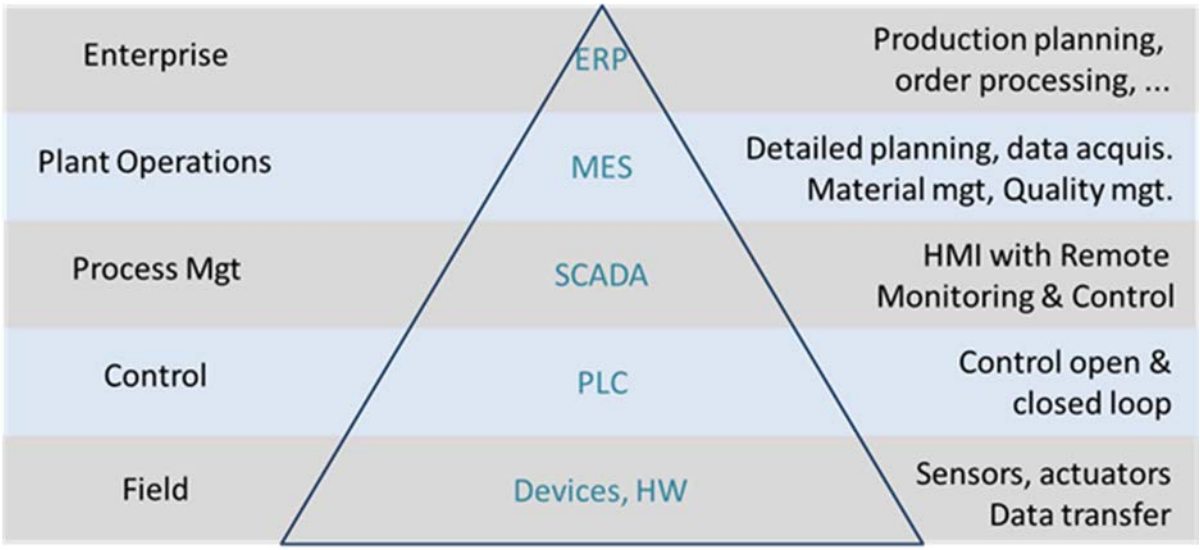


Figure 2: The "Manufacturing Pyramid"

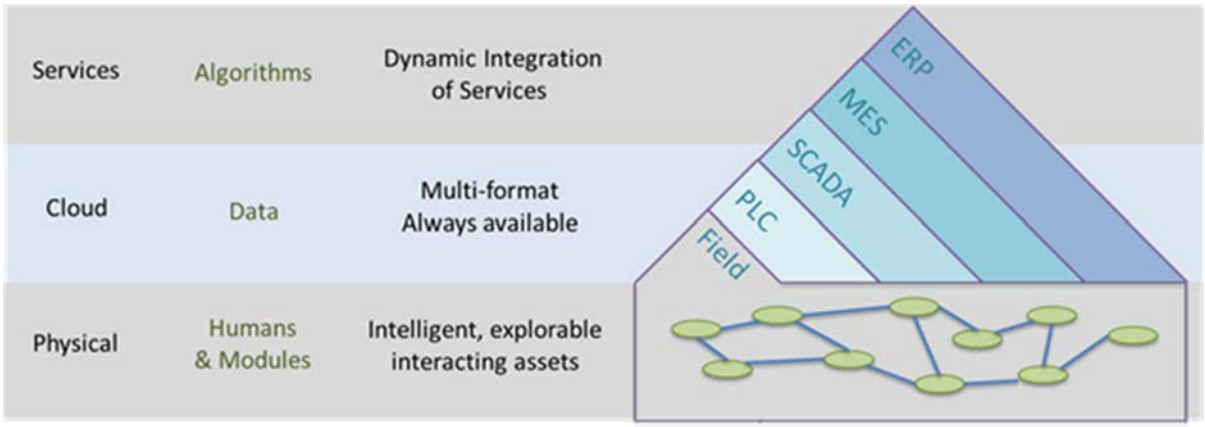


Figure 3: Cyber Physical Production Systems

The current model is well covered in standardization, as outlined in clause 11.2 (and also in the ETSI TR 103 375 [i.1] on "IoT Landscaping"). The transition towards the CPPS approach has started and will require two major efforts from a standardization standpoint:

1) adaptation of the existing set of standards to the new requirements of the "things"; and

2) definition of much more flexible data models so as to facilitate the information exchange between the field and the different systems (PLC, SCADA, etc.).

11.2 Mapping of requirements and related standard coverage

11.2.0 Methodology

The methodology implemented to identify requirements for this vertical area and organizations that provide standards related to these requirements is explained in clause 4.1.3.

11.2.1 Communication and Connectivity knowledge area

11.2.1.1 Connectivity at physical and link layer

Table 79: Mapping of requirements for connectivity at physical and link layer

Requirements	Organizations providing related standards
Support of Real-time communications	CiA, IEC, IEEE, SERCOS International
Support of Infrastructure-based communication	3GPP, ETSI, IEEE, LoRa Alliance
Support of Mobility	3GPP, ETSI, IEEE
Support of Heterogeneous types of communications: wireless, long range/short range; bandwidth; latency (real time)	3GPP, IEEE, IETF

11.2.1.2 Connectivity at network layer

Table 80: Mapping of requirements for connectivity at network layer

Requirements	Organizations providing related standards
Real-time handling of events	CiA, IEC, ISO/IEC, ODVA,
High network availability performance behaviour	This is a potential gap for large IoT networks
Local and remote access to infrastructural services	3GPP, OCF, oneM2M
Interoperability of networks: devices with different communication protocols are able to share data	IEC, IEEE, IETF
Communication platforms	oneM2M

11.2.1.3 Service level and application enablers

Table 81: Mapping of requirements for service level and application enablers

Requirements	Organizations providing related standards
Support collection of data from local/remote sensors	3GPP, OCF, IETF CORE
Semantic interoperability between service components	IEC, ITU-T

11.2.1.4 Application layer level, APIs, data models and ontologies

Table 82: Mapping of requirements for application layer level, APIs, data models and ontologies

Requirements	Organizations providing related standards
Common vocabularies	IEC, ISO
Common information models	IEC, OPC Foundation
Interoperability between business and operations levels	IEC, MESA, OAGi
Interoperability of business processes and field level	This is a potential gap
Applications support a wide variety of services (discovery)	oneM2M, W3C
Data organization, structure (neutral data models) and storage	IEC, W3C

11.2.2 Integration/interoperability knowledge area

Table 83: Mapping of requirements for integration/interoperability knowledge area

Requirements	Organizations providing related standards
Certification of sensors and devices	This is a potential gap
Interoperability of sensors and actuators, ability to read data from other sensors and activate different actuators	AllSeen Alliance, IETF, IPSO Alliance, OCF, oneM2M
Common data "terminology", interoperable data semantics and ontology, common semantics	IEC, ISO/IEC
Seamless interoperability between data systems	IIC, W3C

11.2.3 Applications management knowledge area

Table 84: Mapping of requirements for applications management knowledge area

Requirements	Organizations providing related standards
Application specification	This is a potential gap
Application performances' monitoring	This is a potential gap
Continued support to the client after purchase	This is a potential gap
Tools for easy installation, configuration and customization	This is a potential gap

11.2.4 Infrastructure knowledge area

Table 85: Mapping of requirements for infrastructure knowledge area

Requirements	Organizations providing related standards
Integration with legacy systems and data sources	Allseen Alliance, oneM2M
Deployment tools	OSGi
Functional safety	IEC

11.2.5 IoT Architecture knowledge area

Table 86: Mapping of requirements for IoT Architecture knowledge area

Requirements	Organizations providing related standards
Global-level standards (international)	IEC, Industrie 4.0, oneM2M

11.2.6 Devices and sensor technology knowledge area

Table 87: Mapping of requirements for devices and sensor technology knowledge area

Requirements	Organizations providing related standards
Support of various types of devices and sensors	IETF, IEEE, oneM2M, ZigBee
Real-time + batch handling of events/data	IEC, IETF, OASIS, OMG
Device discovery in the ecosystem	IEC, IETF, oneM2M
Sensors and devices accessible locally and remotely	oneM2M, OMA
Externalization of sensor data and remote control	oneM2M, OMA
Sensor data quality	This is a potential gap

11.2.7 Security and privacy knowledge area

Table 88: Mapping of requirements for security and privacy knowledge area

Requirements	Organizations providing related standards
Protection of data; encryption	IEC, IEEE
Confidentiality and privacy	This is a potential gap
Identity management; user authentication, access control	3GPP, OASIS, IEEE, oneM2M
Data security	This is a potential gap
End-to-end security	3GPP, IEC, IETF, ISO/IEC, oneM2M
Risk Management Framework and Methodology	Standards available from IEC, ISO This is a potential gap for Smart Manufacturing
New approaches (e.g. security by design; secure interfaces) for a high level of trust	This is a potential gap

11.3 Result of the survey

The next tables give a selection of answers received through the survey for the Smart Manufacturing vertical domain. The answers which spread across several domains, including the present one, are provided in Clause 12. Answers related to the Smart Cities vertical domain may also be applicable here.

Table 89: Survey results for the Smart Manufacturing vertical domain - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Too many standards to choose from; the market will eventually decide. Interoperability issue due to lack of universal semantic standard reference.	All KAs are involved		No specific expectation for additional standards. International standard bodies should better coordinate their IoT initiatives.
Investment.	Architectures; security	3	Nothing at this stage because standardization and regulation is for well-established market leaders (mostly big companies).
Lack of harmonisation and interoperability, e.g. for energy and industrial control.	Communication and Connectivity; Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology; Security and Privacy	4	<empty>
Companies struggle to understand the value of IoT. Implementing IoT services or an architecture is today to complex and requires an integration effort. Cloud services are silos which makes integration of the devices with the cloud very difficult and too expensive. With the amount of work needed to connect one device to a Cloud, this will not scale.	Communication and Connectivity (service level); Integration/Interoperability; IoT Architecture; Security and Privacy	5	<empty>

Table 90: Survey results for the Smart Manufacturing vertical domain - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of security in IoT	All KAs are involved	5	Only standardization can improve it

Table 91: Survey results for the Smart Manufacturing vertical domain - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of a unique standard between all the "things".	All KAs are involved	4	All the things should "speak" the same language.
Lack of network standard.	Communication and connectivity; Integration/Interoperability	4	A unique and valuable network. Like Ethernet/IP is for computers, etc.
IoT for smart manufacturing should be interoperable with other IoT industry verticals, with minor or no integration effort.	Integration/Interoperability	4	Manufacturing should be able to link with supply chain, with cities, citizens and the result should be a seamless web of applications.
Secure interoperability that is harmonized across a myriad of devices and things to a "central" repository of information.	Integration/Interoperability; IoT Architecture; Security and Privacy	5	I think it will only be achieved in specific areas solving specific use cases. I do not foresee universal standardization.
Interoperability between devices and Cloud and devices to devices. Integration of existing devices.	Communication and Connectivity (service and application levels); Integration/Interoperability; IoT Architecture; Security and Privacy	5	Enforce interoperability; the target should be an interoperability level like we have in mobile networks today.
Link different communication protocols.	Applications life-cycle support; Devices and sensor technology; Security and Privacy	4	Standards are very important to combine components or systems from different companies.

11.4 Consolidated view of the gaps

This clause gathers the results of the theoretical analysis and of the questionnaire.

To a large extent, Smart Manufacturing has a lot of existing standards to start from. As already pointed out, a significant part of the work ahead for Smart Manufacturing standardization is going to be adaptation of existing standards.

However, there are areas for new developments. The main perceived ones (and the associated gaps) are the following:

- Integration of a larger set of IoT devices. Though Manufacturing is already making a massive use of sensors and actuators, Smart Manufacturing will introduce a much larger set of devices that will have to undertake a variety of tasks from the on-line reconfiguration of the processes based on instant supply chain demands, up to predictive maintenance. The use of wireless networks to support this new range of actors is going to modify the current respective roles of wireline and wireless networks in the factory. Corresponding standards will emerge, possibly coming from the ICT sector (such as those supported by the M2M communication based platforms).

- Data Models. The need to enable a greater interoperability between systems (and a certain de-layering of the manufacturing pyramid) will foster the evolution of the existing (common) data models towards more systematically developed and managed set of ontologies.

- Cyber Security. There is still a difficulty to provide end-to-end security for complex manufacturing systems, in particular considering the large span of virtual actors (from devices and sensors up to enterprise level systems) and the overall need for human presence and decisions. Approaches such as security by design will change the current approaches (e.g. to certification). The related standards are still to come.

12 Cross IoT platform interoperability and harmonization

12.1 Result of the survey for multiple vertical domains

The tables of this clause give a selection of answers which spread across several vertical domains.

Table 92: Survey results for multiple domains - Business

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of horizontal IoT business models that valorise data. Smart X (silo) models stack up but there is no easy way to valorise data from adjacent silos.	Communication and Connectivity (service level)	4	I don't know of anything specific that would help. The current trend in standards and regulations helpfully makes data more transferable (in physical, logical and semantic senses) - it's business attitudes that need to change.
Lack of business take-up (thus private investments).	Applications life-cycle support	3	Regulation: growth/tax opportunities for private early adopters/investors.
Unbalanced costs/benefits (benefits end up with different supply/value chain partner), inability to invest in such technology in marginal markets, risk of vendor lock-in.	<empty>	5	Vendor lock-in can be prevented by universal and required standards (think of charging mobile phones, but Apple used a loophole to enforce proprietary solutions).
Business model.	Communication and Connectivity (application level); Applications life-cycle support	4	Once a solution is standardized, many companies started to develop and compete with each other, and copy the business plan. Customers won't have the possibility to choose a model.
Too many technologies that don't work together.	All KAs	4	To start making choices, or to show how things can work together.
Siloed applications and the underlying standards - Some might call this a technology issue, but I believe it is a business issue.	Communication and Connectivity (all levels); Integration/Interoperability	3	Facilitate the conversation on integration/interoperability.
Lack of interoperable standards and ecosystem that make the development of M2M/IoT solutions affordable for many more applications than just a few major verticals (ITS, smart grids).	Communication and Connectivity (service level); Integration/Interoperability; Applications life-cycle support; IoT Architecture; Security and Privacy	4	Promote the development and use of relevant standards (e.g. oneM2M) and facilitate establishment of proper ecosystems in important business areas (e-health, wearables, etc.).
Privacy challenge as consumers are not aware of personal data being exposed by IoT devices, and cannot babysit them permanently, plus security risks for critical infrastructures (transport, energy).	Integration/Interoperability; Applications life-cycle support; Security and Privacy	3	Promote establishment of proper regulation and their alignment across EU member states.
Siloed data - especially data on security and privacy breaches remains sealed and is currently often not made public due → Gaps are not found, but same attacks can be applied sequentially to many big players - no learning from mistakes of other players.	Security and Privacy	4	Rules and regulations for (a) exchanging data on security breaches, especially in sensor networks and (b) workflows for establishing trust between the players.
Today's focus is on proprietary and fast-to-market solutions. There is a gap in thinking about longer term technology, operational and business models.	Integration/Interoperability; Applications life-cycle support; IoT Architecture	3	Modify standardization process to speed up the process.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of winning standard (proprietary).	Communication and Connectivity (application level); Integration/Interoperability; IoT Architecture	3	Interoperability, mass production.
Currently there are too many fora and interoperable products already out there, making any cooperation and the take up of common business difficult. There is also too much attention on the Connectivity while the platform and device topic is not well yet positioned. Lack of "business models" and new ideas about revenue sharing.	<empty>	3	Actually from Standards point, everything necessary is already there. I hope the "gap analysis" will "separate the wheat from the chaff" and will Promote the already developed solutions like oneM2M standards, having the potential to create the ecosystem IoT needs.
Adoption of cross vertical platforms slow to progress, but can be address through proper adoption of oneM2M standards/specifications.	Communication and Connectivity (service and application levels); Integration/Interoperability	4	Support for wide use of oneM2M platform for cross vertical, cross regulatory boundaries.
Duplication.	Communication and Connectivity (service and application levels); Integration/Interoperability	4	Better coordination and global vision.
Duplication, fragmentation, lack of common standards.	Communication and Connectivity (application level); Integration /Interoperability; Applications life-cycle support; Infrastructure and computational platforms; IoT Architecture; Security and Privacy	5	Interoperability standards like oneM2M should market themselves.
Don't see that there is a gap.	<empty>	<empty>	Let vendors solve the problem.
Vendor locked ecosystems.	Communication and Connectivity (service and application levels); Integration/Interoperability; IoT Architecture	4	1. Well established technical standards that are known by most of the system integrators in the field of IoT. In that case there would be a common language in the field even if the particular installations are heterogeneous or proprietary. 2. Security & Privacy policies and architectures that are targeting the particular aspects of IoT.
Lack of standardization.	Communication and Connectivity (application level); Integration/Interoperability; IoT Architecture	4	Industry adoption.
Overlap of standards, each pertaining to one specific vertical application. Lack of conviction from each domain to break their silos and evolve towards standards enabling interoperable information exchange.	Integration/Interoperability	5	Promote a vision of the future relying on the use of global interoperable standards for cross-sector information exchange.
Too many proprietary solutions and interoperability issues leading to silos.	Integration/Interoperability; IoT Architecture; Devices and sensor technology; Security and Privacy	4	Clearly defined standards with industry wide adoption.
No standards at the application level, huge gap between legacy industry, new big companies and research.	Communication and Connectivity (service and application levels); Integration/Interoperability; IoT Architecture; Devices and sensor technology	3	Better information of the different approaches.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack harmonization interoperability.	Integration/Interoperability; IoT Architecture; Devices and sensor technology	4	To align.
In the past, the "tech push" approach was very often predominant. Today, if we want to reach the next level for a hyper connected world, "tech pull" should prevail. In this sense, industry 4.0 is interesting. A company/industry is cut in horizontal and vertical smaller pieces on a global level and technology becomes much more than a pervasive enabler. Siloed applications should be commonly integrated and investments encouraged & supported.	Communication and Connectivity (physical up to network level)	5	To evangelize and come up with simpler architectures and frameworks for industries but also in general to society, not forgetting to governments.
I believe that technological and societal gaps will soon be fulfilled. Nonetheless, the investment gap needs further attention since the IoT related products fall into the market failures categories and traditional capitalism investment paradigms (extreme competition) can no longer apply.	Communication and Connectivity (application level); Integration/Interoperability; Applications life-cycle support; Infrastructure and computational platforms	4	Lower barriers to entry/contribute in the relevant alliances, or even be subsidized to participate there.
Different physical and application layers are appropriate to different applications (vis a vis security, data rates, battery life/energy consumption, wireless range, cost, etc.).	Communication and Connectivity; Integration/Interoperability	2	It's not appropriate for regulation to pick winners, but the adoption of standards/frameworks by industry should be encouraged.
Duplication and lack of harmonization	Communication and Connectivity; Devices and sensor technology; Security and Privacy	4	Promote and support commercialization.
Many companies re-invent end2end solutions, missing trust, unable to identify reusable components across verticals, interoperability standard are still in early stage (OCF).	Communication and Connectivity (application level); Integration/Interoperability; Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology; Security and Privacy	4	Global standard, not EU or national specific. Identify and push most suitable suite of standards, We need a whole TCP/IP-like stack for IoT.
The technologies for communication are available. It is more the question how to combine the features and products without opening all "knowledge" to everyone. "If I use data from someone, do I need to pay for it?"	Integration/Interoperability; Applications life-cycle support; Devices and sensor technology	3	At the moment? Nothing. You only can regulate and standardize an already given market with structures and settled players. Wait 5 years and try again.
In field application life-cycle management.	Applications life-cycle support; Devices and sensor technology	4	Deeply embedded devices do not have any common way to manage application, in-field. This could lead to fragmentation, and loss of value of products.

Table 93: Survey results for multiple domains - Societal

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Energy consumption control	Communication and Connectivity (physical up to network level); Devices and sensor technology	3	
Interoperability	Communication and Connectivity (application level); Integration /Interoperability	3	Define important regulations and processes to close/minimize the gap.
Lack of clear map of IoT to societal benefit	Communication and Connectivity; Integration/Interoperability; IoT Architecture; Devices and sensor technology; Security and Privacy	4	Greater involvement of regulators and users to drive the societal dimension for further development of IoT.
Lack of harmonization and interoperability	Communication and Connectivity (service and application level); Integration /InteroperabilityService Applis-APIs Interop	3	To provide some standard to do the things in the same way all the actors. To write requirements to harmonize the different existent solutions and define a way to do the things if you want to have a stamp of interoperable product.
Lack of harmonization and interoperability, missing features	Communication and Connectivity (network level); Devices and sensor technology; Security and Privacy	3	Define a framework and features.
Data rights management (ownership, storage, sharing, selling, etc.) of all data generated, collected, shared, recombined and analysed coming from smart devices at home, on street, my car, in office, shopping centres, my wearables, etc.	Security and Privacy	5	To provide clear definition with legislation experts make examples and also provide samples, good practices, etc.
Privacy concerns and guidelines for data ownership	Communication and Connectivity (service and application level; Applications life-cycle support; IoT Architecture; Security and Privacy	4	Update in particular regulation to adapt technical possibilities.
Lack of awareness of security and privacy risks, lack of regulation	Communication and Connectivity (application level); Security and Privacy	5	Define minimal security requirements at device level and define end-to-end security interoperability frameworks.
<empty>	Security and Privacy	5	Set security & privacy levels (e.g. 1 being "public" to 4 being "strictly private").
Lack of data models	Communication and Connectivity (application level);	3	<empty>
Missing of privacy and security policies, and even if there are some they should be harmonized	Integration/Interoperability; Security and Privacy	3	To define privacy and security strategy and rules.
<empty>	Communication and Connectivity (service and application levels); Integration/Interoperability; Security and Privacy	3	Emphasize on privacy and security to overcome the societal gap.
Security classes	Communication and Connectivity (network up to application level); Integration/Interoperability	4	classification - certification.

Table 94: Survey results for multiple domains - Technical

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
There are gaps in the area of test suites which can be applied to connected devices and IoT systems.	Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology	3	Test specifications, test suites, test harnesses. It is important in the context of IoT that any test suites be adaptable to varying environments, both at the hardware level and at the software level.
Frequency harmonization beyond IMT. With IMT the IoT strategy cannot be reached.	PHY-DLC Network Interop Infrastr. Sensor	5	To take Radio Regulation into the IoT Strategy beyond IMT. (cf. Resolution ITU-R 66 [i.12]).
Missing feature - standardized method to distribute software components to processing nodes across a network.	Applications life-cycle support	3	Standardization would help by providing a clearly identified mechanism & protocol.
Mobile ad hoc networks need different security models, especially those not able to apply current cryptographic protocols and standard protocols, i.e. due to battery life. There exists some work on this, but research is still needed and a set of standardized protocols and technologies with respect to different capability models of sensors and embedded systems is needed.	Communication and Connectivity (network level); Security and Privacy	4	Standardized protocols for secure and privacy preserving low-energy communication protocols for several power-levels of distributed sensors/actors.
Interoperability.	Communication and Connectivity (all levels); Integration/Interoperability	3	Define interoperability framework.
Proprietary solution, lack of interoperability.	Communication and Connectivity (service and application levels); Infrastructure and computational platforms	3	High level architecture and API definitions.
Lack of harmonisation, interoperability.	Communication and Connectivity (network level); Integration/Interoperability; Security and Privacy	5	At least best practices.
Sensor standardization.	Communication and Connectivity (physical and link levels)	2	<empty>
Semantic Interoperability.	Communication and Connectivity (service and application levels); Integration/Interoperability	3	One common reference Ontology in preference in oneM2M in cooperation with W3C.
Emerging of new connectivity solution.	Communication and Connectivity (physical up to service level); Integration/Interoperability; Security and Privacy	4	Focus the technological trend so to allow proper planning of industrial activities.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
While technology is apparently "disappearing" to naive eyes, as people are focusing on services regardless of device, terminal or platform they use, awareness of data transaction is getting lower and lower. Currently there is a lack of access control technologies enabling: • data protection, based on policies, as soon as data leaves the boundary of a trusted environment; • respect of policies during the data life cycle; • portability of protection settings when data moves from one service provider to another (and, implicitly, their interoperability).	Security and Privacy	3	There is already - not yet standardized - technology enabling that. An effort toward standardization could provide many benefits to end users and increase the amount of trust in IoT.
Fragmentation of service platform and the defence of vertical business walled micro--garden. All of this is taking under hostage the overall development of IoT in Europe.	Communication and Connectivity (application level); Integration/Interoperability; Infrastructure and computational platforms; IoT Architecture; Devices and sensor technology; Security and Privacy	5	Force the vertical platform towards horizontal inter-workable solutions, especially in terms of semantic and ontology models.
Lack of offer of standard API in the devices/terminal offer for M2M/IoT application.	Communication and Connectivity (application level); Integration/Interoperability; Infrastructure and computational platforms; Devices and sensor technology; Security and Privacy	5	Require clear API in the devices to support application portability among devices/terminals.
Fragmentation of research and innovation among the different vertical sectors.	All KAs	4	Specific emphasis on the support for horizontal solutions capable to support all IoT sectors.
Proprietary solutions of focused only on specific aspects of IoT.	All KAs	1	Unique standards.
Lack of security studies on the global IoT eco-system.	Communication and Connectivity; Applications life-cycle support; Infrastructure and computational platforms; IoT Architecture; Security and Privacy	4	<empty>
Lack of "generic interoperability" across domains, organizations and M2M versus Web.	Communication and Connectivity (service and application levels); Integration/Interoperability.	5	Adopt existing standards that address the gap.
Too fragmented markets using widely different topologies.	Communication and Connectivity (network up to application level); Security and Privacy	4	Security Guidelines AND rules preventing use of the obsolete security technologies or enforcing the minimum to be used. Define security classes as we do for energy (A, B, C, D, etc.), defining a certification grade/ladder.
Proprietary solutions and multiple technologies available addressed to similar use cases: ETSI LTN, LoRa, NB-IoT, etc.	Communication and Connectivity (physical and link levels); Infrastructure and computational platforms	4	To reduce the market uncertainty.

Nature of the gap	Knowledge Area	Criticality	How can standardization or regulation improve this?
Lack of harmonization, interoperability; lack of security & privacy.	Communication and Connectivity (application level); Integration/Interoperability; Security and Privacy	4	For standardization, it is expected syntactic interoperability in most of the cases. However, the standards are difficult to manage (commonly abstract and huge schemas). Based on this, some standardization bodies are trying to elaborate more concise schemas linked with domain ontologies (semantic interoperability). Therefore, our expectations from standards are to get robust data schemas in order to uplift the interoperability into semantic and organizational.
Lack of harmonization and difficulties for interoperability.	Communication and Connectivity (service and application levels); Integration/Interoperability; IoT Architecture	4	Provide some guidelines and to decide some technology that is going to be standard.
Lack of flexibility in spectrum allocation for the IoT market.	Communication and Connectivity (physical and link levels)	2	To consider IoT as a new category of application.
Missing interoperability.	Integration/Interoperability.	3	Co-operation between major platforms.
Interoperability; still proprietary issues; lack of choice for consumers.	Communication and Connectivity (application level)	2	<empty>
PHY/network layer level harmonization. Need also to harmonize at application layer level with a new single middleware.	Communication and Connectivity (physical up to network level)	5	I expect nothing from any standardization organization because gaps are focused at the app layer.
Non common agreement on how to setup a secure IoT nodes identification model.	Integration/Interoperability; Applications life-cycle support; Infrastructure and computational platforms; IoT Architecture; Security and Privacy	3	Find an open, market friendly, well accepted solution.
There is lack of harmonization to access Cloud storage by embedded devices.	Communication and Connectivity (service and application levels); Integration/Interoperability; Infrastructure and computational platforms; IoT Architecture; Security and Privacy	3	Provide a common framework, and ideally a common standard to access cloud storage.

12.2 Consolidated view of the gaps

Currently, the main points below have been identified as cross IoT interoperability and harmonization challenges:

- Duplication of IoT architectures and models. This has been addressed by the AIOTI HLA which can be mapped to the different architectures standardized.

- A large number of communication protocols address heterogeneous types of communication requirements: wireless/wireline, long range/short range; bandwidth, latency, real time/best effort, etc. However, in this area as well, the landscape analysis shows many cases of duplication for specific needs. This triggers interoperability and deployment challenges for the end users, whether they are city authorities, manufacturers and last but not least, the public people. Moreover, despite this wide offer, connectivity performance and availability cannot be guaranteed by certification standards.

- Data models are developed on a proprietary basis and mostly specific to the vertical domains to which they apply.
- Processing rules and decision-making processes under the reception of sensor data lack harmonization. They are defined on a proprietary basis and usually not standardized.
- Security and privacy are addressed on an isolated basis for part of the applications. Data ownership is also a hot topic. Education of end users on these features has also been identified as a new requirement.
- Ease of use and of maintenance after purchase would require a more global approach, taking into account that most of the end-users are not technical people

13 Conclusion

The present document has analysed the potential gaps in IoT standardization landscape using both a survey that has been largely distributed to the different stakeholders involved in this domain and a theoretical analysis for each of the vertical sectors considered by the LSPs. This dual approach has brought two sources of information. On the one hand, the feedback of the community on the gaps they perceive - including not just the technical ones, but also the societal and business ones - has brought a large range of topics to attention. On the other hand, the view of the experts has produced a set of requirements and their mapping on the current situation of the industry, in particular with respect to standards, thus allowing for the identification of another set of gaps.

For each of the vertical sectors concerned by the analysis, a consolidated view of the gaps applying to the sector has been drawn. This list of gaps is a good indication of the level of maturity of standardization (but also business or regulatory frameworks) in a given vertical domain. In particular, it is expected that this information will be useful for the Large Scale Pilots that will start at the beginning of 2017: one of the objectives of these LSPs should be to address part of the identified gaps.

During the collection of gaps, it has appeared that there is a lot in common across most of the vertical domains (see for example security) and that this commonality should be made clear, Consequently, the report has presented the results of the survey that are common to (most of) the different vertical domains and a consolidated view of the main standardization gaps that remain overall for the IoT technology.

Moreover, the results of the study are not just concerning technology. In particular, the survey has enabled the identification of challenges that remain at business and societal levels and may prevent the European IoT ecosystem to unleash the potentials of the IoT. The business and societal gaps - though not the subject of standardization activities - are important issues for the IoT industry as well as for the identification of potential improvements regarding regulatory of legal frameworks.

The present document may be completed with further studies covering for example the list of concrete standards per SDO/Alliance that fulfil each specific requirement, as explained in clause 4.1.3.

Annex A:
Feedback from Brussels AIOTI meeting held in November 2015

Standards Gaps discussed during breakout session:

1) Identification of IoT devices: while several identification schemas exist, there remains a need to federate those identification schemas. The Digital Object Architecture as specified in Recommendation ITU-T X.1255 [i.10] could provide an initial answer to an identity federation model for IoT devices.

2) Common vocabulary.

3) How business models can impact standards.

4) IoT makes often use of constrained devices, there is a need to provide security solutions for such devices.

5) How to scale an IoT large scale deployment across multiple platform and application versions, how to manage versioning in such a complex system.

6) Metrics for quality and reliability of IoT data.

7) Standards need to address requirements pertaining to monetizing data. Data will increasingly be a market asset.

8) Standards needs to address privacy requirements and regulation pertaining to data monetization and sharing.

9) Standards to enable open market of services (at internet speeds): automated negotiation of IoT services with SLA support.

Feedback to AIOTI and WG03:

1) AIOTI and WG03 should carefully consider security as a built-in mechanism. It is not clear if and how security will be addressed in the alliance.

2) ITU-T invited WG03 to contribute its deliverables to ITU-T SG20, those are acknowledged as valuable inputs to standards processes.

3) The link between AIOTI semantic interop framework and semantic web should be clarified. AIOTI should learn from previous experiences (and failures) to ensure its semantic framework will have market impact.

4) Will AIOTI WG03 seek to harmonize existing standards? The answer was provided that AIOTI will not build standards nor harmonize standards, it will work with existing SDOs and alliances to help convergence and complementarities.

5) SMEs are having difficulties to keep up with standards developments; it was acknowledged that WG03 deliverables did a good job in providing a standards/technology overview. AIOTI can play an important role in providing a technology watch.

6) Difference between data modelling and ontologies remains unclear to stakeholders.

7) While AIOTI has EU roots, it should seek international impact. EU-US dialogues was mentioned as a positive step towards achieving this goal.

8) Open data/Closed data approaches can co-exist even within the same IoT platform. There is a need to carefully consider privacy regulations and impacts in the work of AIOTI. Privacy cannot be a parallel track.

9) There are way too many data formats, that makes building analytics applications a complex task. How can AIOTI help reduce this complexity?

Annex B:
ETSI STF 505 Gap Analysis Survey

B.1 Content of the survey

Introduction

STF505 is a group of experts, funded by the European Commission and supported by ETSI, commissioned to provide on the one hand an in-depth analysis of the IoT Standardization landscape, and on the other hand, an identification of the IoT standardization gaps. The results of this survey will help us identify what are the missing functionalities in the IoT standards landscape that could foster the development of future solutions and expand the IoT ecosystem.
The study considers "vertical" functionalities (standards and protocols) in specific application domains, i.e. a single vertical industry, such as home automation, Smart Mobility and wearable medical devices, etc. and "horizontal" functionalities that are not specific to any particular domain but aim to provide common standards, protocols and solutions applicable to as many vertical industries as possible.

Please answer the following questions to the best of your knowledge.

These questions are contained in up to five pages. The first one is to indicate your areas of interest in IoT. The next ones will help us identify IoT standardization gaps (from 1 to 3 depending on the number of gaps you want to report). At the end of the survey, you will have the option to give us your contact information.

Your areas of interest in IoT

1. From the list of service domains indicated below, please indicate your domain of interest either vertical domain i.e. for specific industry area or horizontal domain not specific to any particular industry area (several answers are possible)?

- ☐ Smart Cities
- ☐ Smart Living environments for ageing well (e.g. smart house)
- ☐ Smart Farming and food security
- ☐ Wearables
- ☐ Smart Mobility (smart transport/smart vehicles/connected cars)
- ☐ Smart manufacturing
- ☐ Smart environment (smart water management)
- ☐ Horizontal/Telecommunications
- ☐ Other (please specify):

2. From an architecture point of view, an IoT system can be thought of consisting of the knowledge areas (Kas) indicated below. From this list of Kas, please choose the ones that apply to your area of interest chosen above (several answers are possible).

- ☐ Communication and Connectivity/Connectivity at Physical and data Link layer
- ☐ Communication and Connectivity/Connectivity at Network layer
- ☐ Communication and Connectivity/Service level and application enablers
- ☐ Communication and Connectivity/Application Layer level, APIs, Data models and ontologies
- ☐ Integration/Interoperability
- ☐ Applications life-cycle support
- ☐ Infrastructure and computational platforms
- ☐ IoT integrated Architecture
- ☐ Devices and sensor technology
- ☐ Security and Privacy

The next two questions will help us analyse the answers we receive on standardization gaps by understanding what is your current status.

3. Please indicate what are your goals and expectations regarding IoT for your professional activity.

4. Please list the most important regulations, standards and frameworks that you are currently using or planning to use.

Identification of gaps

In the rest of the survey, we ask you to identify up to three of the main gaps e.g. missing elements that are needed to achieve your goals.

Please indicate what your most important gap is.

5. Category of the gap

- ○ Technology (e.g. communications paradigms, data models, software availability ….)
- ○ Societal (e.g. privacy, energy consumption, easiness of use ….)
- ○ Business (e.g. siloed applications, value chain, investment ….)

6. Nature of the gap, e.g. missing feature, duplication, proprietary solution, lack of harmonization, interoperability

7. In which knowledge area does it belong (several answers are possible)?

- ☐ Communication and Connectivity/Connectivity at Physical and data Link layer
- ☐ Communication and Connectivity/Connectivity at Network layer
- ☐ Communication and Connectivity/Service level and application enablers
- ☐ Communication and Connectivity/Application Layer level, APIs, Data models and ontologies
- ☐ Integration/Interoperability
- ☐ Applications life-cycle support
- ☐ Infrastructure and computational platforms
- ☐ IoT integrated Architecture
- ☐ Devices and sensor technology
- ☐ Security and Privacy

8. Criticality, from 1 (acceptable) to 5 (showstopper)

1 2 3 4 5

9. What would you expect from a standardization or regulation point of view to improve this situation?

10. Do you want to identify another gap?

[Conditional] Identification of gap #2

Questions 11 to 16 (same as Questions 5 to 10).

[Conditional] Identification of gap #3

Questions 17 to 21 (same as Questions 5 to 9).

Some optional information on you, if you wish:

22. Your name (optional)

23. Your company (optional)

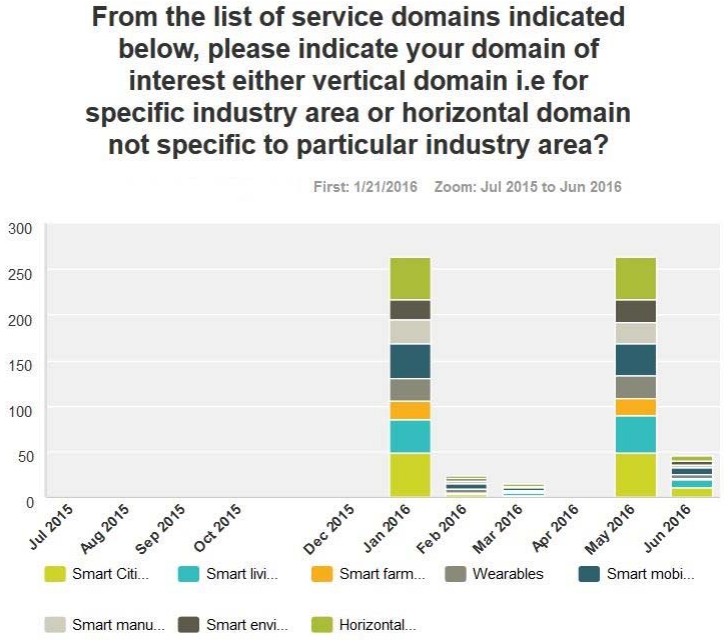
24. Your country or region (optional)

25. Your email Address (optional)

==========End of the survey==========

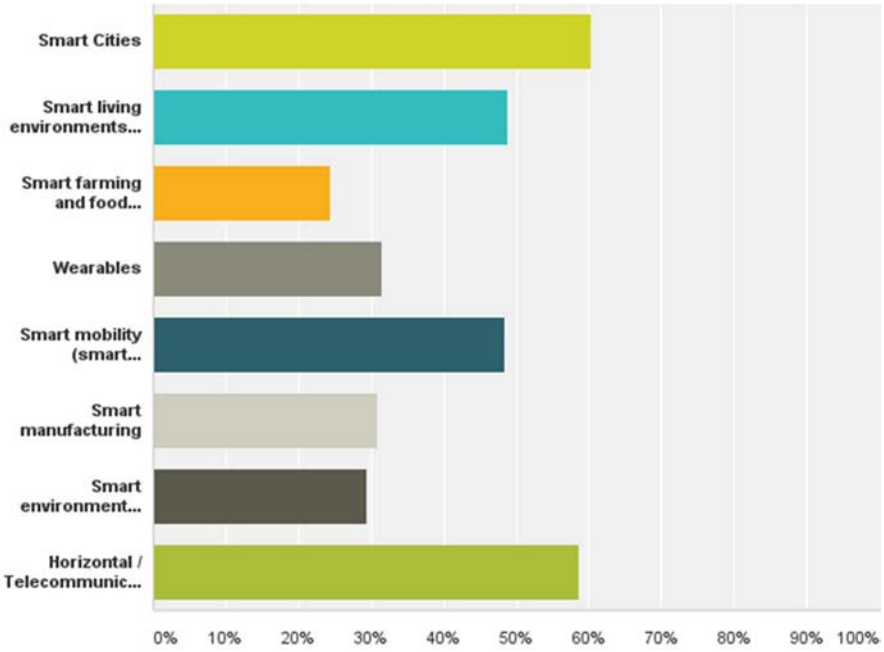
B.2 Some statistics on the answers

Distribution of answers during the opening time of the survey:

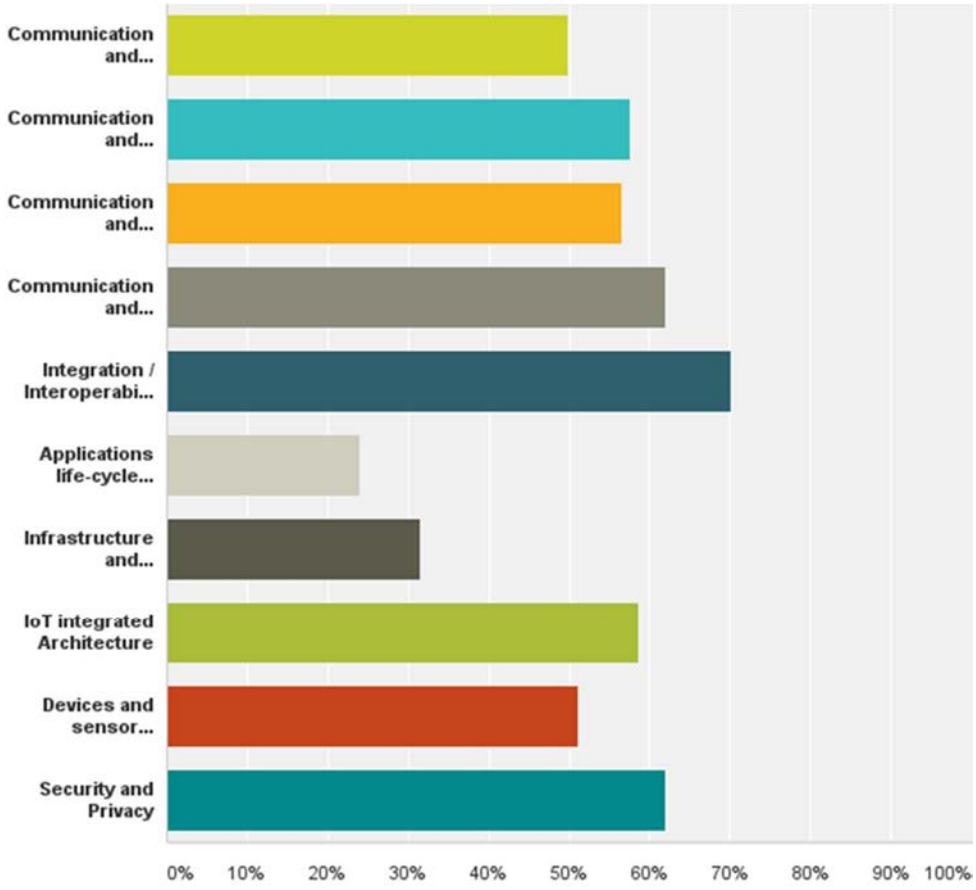


Number of responders who provided their contact details (Q25):

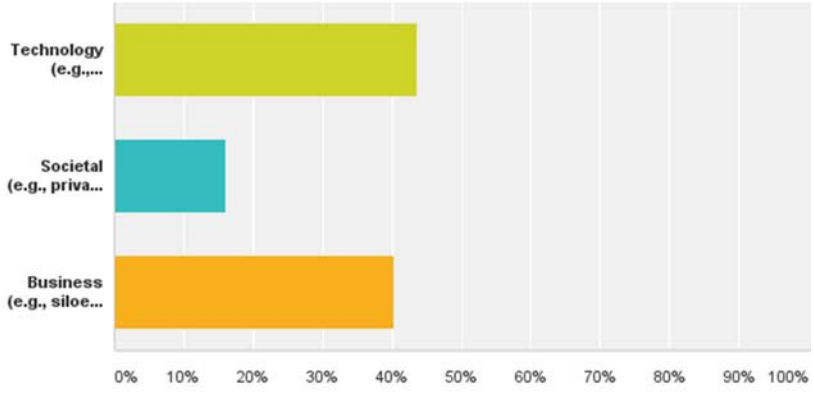
Distribution of answers per vertical sector (Q1):

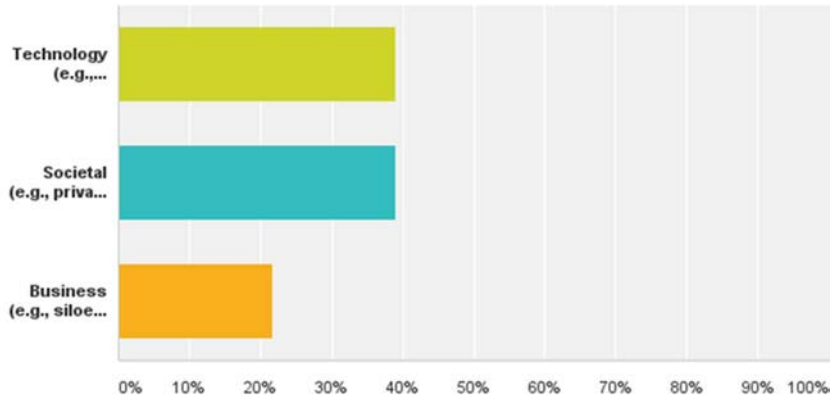


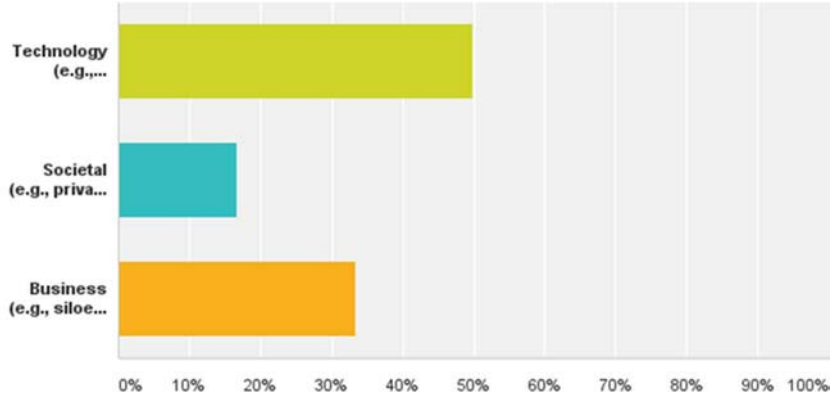
Distribution of answers per KA (Q2):



Distribution of gaps per category (Q5, Q11, Q17):




Technology (e.g.,...
Societal (e.g., priva...
Business (e.g., siloe...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


Technology (e.g.,...
Societal (e.g., priva...
Business (e.g., siloe...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

History

Document history		
V1.1.1	October 2016	Publication