Alliance for Internet of Things Innovation

High Priority IoT Standardisation Gaps and Relevant SDOs

Release 2.0

AIOTI WG03 – IoT Standardisation

January 2020

Executive Summary

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

The purpose of this document is to reflect a structured discussion within the AIOTI WG03 community and to provide consolidated technical elements as well as guidance and recommendations.

The revision of this report has been started in October 2018. The objective of the present Version 2.0 is to continue the study of resolution of High Priority IoT Standardisation Gaps by relevant SDOs (main focus) and insert new gaps in the table when relevant contributions are approved by the AIOTI WG03 group. The major part of the work consisted in adding section 6 which contains an analysis of the IoT standards gaps identified in previous actions. Sections 4 with the prioritisation od standards gaps and section 5 which contains the Gaps analysis performed for Version 1.0 of this document have also been updated. This work is performed with the support of ETSI STF547.

From a standardisation perspective, the outcome of this revision is that if some topics such as privacy, security, platform and semantic interoperability, data quality for example have been addressed, others which are more related to operational strategies, such as deployment and its scalability, software update, sustainability and green technologies, usability (Easy accessibility and usage to a large non-technical public) still need to be tackled.

Table of Contents

1 Goal and motivation 6

2 Standards Gaps: Definition 6

2.1 Definition and classification of standards gaps 6

2.2 Source for the identification of standards gaps 7

3 Standards Gaps: Identification 7

3.1 Identification of Standards Gaps: ETSI STF 505 7

3.1.1 Rationale, objectives, scope 7

3.1.2 Identification of gaps per Knowledge Areas and IoT Domains 8

3.2 Identification of Standards Gaps: AIOTI WG3 8

3.2.1 Safety 9

3.2.2 Overlapping of traditional domains and IoT 10

3.2.3 Health of Edge Computers 10

4 Standards Gaps: Prioritisation 11

4.1 STF 505: Major gaps and Key gaps 11

4.2 CREATE-IoT: Large-Scale Pilots perceived Major gaps 12

4.3 CHARIOT Project: gaps from an industrial IoT perspective 14

4.4 MONICA LSP: Identification of an IoT/SRD RF standard for the stable and highly dependable transmission of sensor data 18

4.5 SerIoT project 20

5 Gap analysis and resolution work in SDOs 22

5.1 Gap Resolution 22

5.2 Gaps identification and resolution work in ETSI 23

5.3 Maintaining an overview of standardisation activities and specifications related to IoT 24

6 Standards Gaps Analysis 29

6.1 Connectivity interoperability 31

6.2 Semantic interoperability 32

6.3 Enabling Applications to Span Multiple Ecosystems 36

6.4 Safety 38

6.5 Solution deployment and maintenance tools 39

6.6 Software deployment 41

6.7 Scalable device deployment 42

6.8 Usability 42

6.9 Harmonized identification 43
6.10 Platform interoperability 44
6.10.1 Patterns of IoT Platform Interoperability 45
6.10.2 oneM2M: AUTOPILOT IoT platform Interoperability solution 49
6.10.3 Mining and construction sector 51
6.11 Device certification 52
6.12 Data management 56
6.13 (Cyber-)Security 61
6.14 Green technologies 63
6.15 Ethics and trustworthiness 64
6.15.1 Ethics 64
6.15.2 General IoT Ethics 66
6.15.3 Challenges (based on [37]) 67
6.15.4 Trustworthiness 68
6.16 Open Markets of Digital Services 68
7 Conclusion 69
Annex I References 71
Annex II Readme worksheet of the excel sheet presented in Section 5.3 76
Annex III Security and Privacy aspects in 5G 80
Annex IV Editors and Contributors to this Deliverable 83

Table of Figures

Figure 1: STF 505 gaps per Knowledge Areas and IoT Domains 8
Figure 2: MONICA Acoustic Loop. The red routes are the time critical 20
Figure 3: Example of an end-to-end RF link where latency and jitter can be controlled to be delivered within given time constraints 20
Figure 4: Sample view of worksheet on IoT organisations 25
Figure 5: Sample view of the mind map 25
Figure 6: How the Web of Things enables applications to span multiple IoT ecosystems ... 38
Figure 7: Legacy Device Management 40
Figure 8: Patterns of IoT platform interoperability (Source [48]) 45
Figure 9: BIG IoT Architecture Overview 48
Figure 10: SEMIoTICS interoperability framework (Source: [51]) 49
Figure 11: AUTOPILOT Federated IoT Architecture, based on [53] 50

1 Goal and motivation

There are now several IoT Standards Landscape available (including the work done by the ETSI STF 505 on standards identification, see [7]) that have identified a number of standards that are available, i.e. which have reached a final stage (Technical standard (TS) or TR, etc.) in a Standards Developing Organisation or industrial consortia, and can be used for the work and developments of the IoT community (in particular for the IoT Large-Scale Pilots (LSPs) that have started their work at the beginning of 2017).

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

The purpose of this document is to start a structured discussion within the AIOTI WG03 community and to provide consolidated technical elements as well as guidance and recommendations.

2 Standards Gaps: Definition

2.1 Definition and classification of standards gaps

The definition of a Standard Gap can be taken from the STF 505 document [1]:

> **standardization gaps**: missing or duplicate elements in the IoT standardization landscape
>
> Examples of standardization gaps are: missing standards or regulations, missing APIs, technical interoperability profiles that would clarify the use cases, duplications that would require harmonization.

The gaps identified in the STF 505 document were not only related to standardisation but covering a broader number of topics. Three categories of gaps have been addressed:

- Technological gaps (e.g., communications paradigms, data models or ontologies, software availability);
- Societal gaps (e.g., privacy, energy consumption, ease of use);
- Business gaps (e.g., siloed applications, value chain, and investment).

2.2 Source for the identification of standards gaps

The identification of standards gaps is an important activity for the IoT community and has been a subject of interest and work in a number of projects, groups, etc. The current list of input for this document is the following:

- ETSI STF 505 (see [7]). The Specialist Task Force (STF) 505 has addressed the topic of standards gaps in the Technical Report "TR 103 376" [1].
- AIOTI WG03 has addressed the topics of standards gaps in a number of discussion and decided to make it a deliverable of the Working Group.
- CREATE-IoT (see [8]). As an IoT Large-Scale Pilots (LSP) Coordination and Support Action (CSA), the project has addressed the standards gaps in its Deliverable D06.01 (see [9]).

3 Standards Gaps: Identification

3.1 Identification of Standards Gaps: ETSI STF 505

The STF 505 has addressed the question of standards gaps in "TR 103 376" at the time of the definition of the IoT Large-Scale Pilots (LSPs). The results have been provided by a user's survey and by an analysis undertaken by the STF experts.

3.1.1 Rationale, objectives, scope

The rationale for the (standards) gaps analysis is that the possibility to develop large-scale interoperable solutions may not fully guaranteed if some elements in the (standards) landscape are missing. Hence, the objectives were

- To provide, starting from the use case families selected for the IoT LSPs, the collection of all missing functionalities identified in SDOs/SSOs 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).
- To propose some recommendations to overcome potential gaps. Particular attention is paid on standardization of the horizontal application layer and the need to assure an interworking framework among different vertical industrial segments.

The gap analysis has been done in the context of:

- The need to ensure cross IoT platforms interoperability and harmonisation;
- A number of "verticals" (some of them addressed by the IoT LSPs): Smart Cities; Smart Living environments for aging well; Smart Farming and food security; Smart Wearables; Smart Mobility; Smart Environment; Smart Manufacturing.

3.1.2 Identification of gaps per Knowledge Areas and IoT Domains

A total of 49 main gaps have been identified that resulted from the consolidation of findings from a survey made in the context of the 7 "verticals" identified above. The split of gaps across 1/ Knowledge Areas; and 2/ IoT Domains (sectors) can be seen in Figure 1.

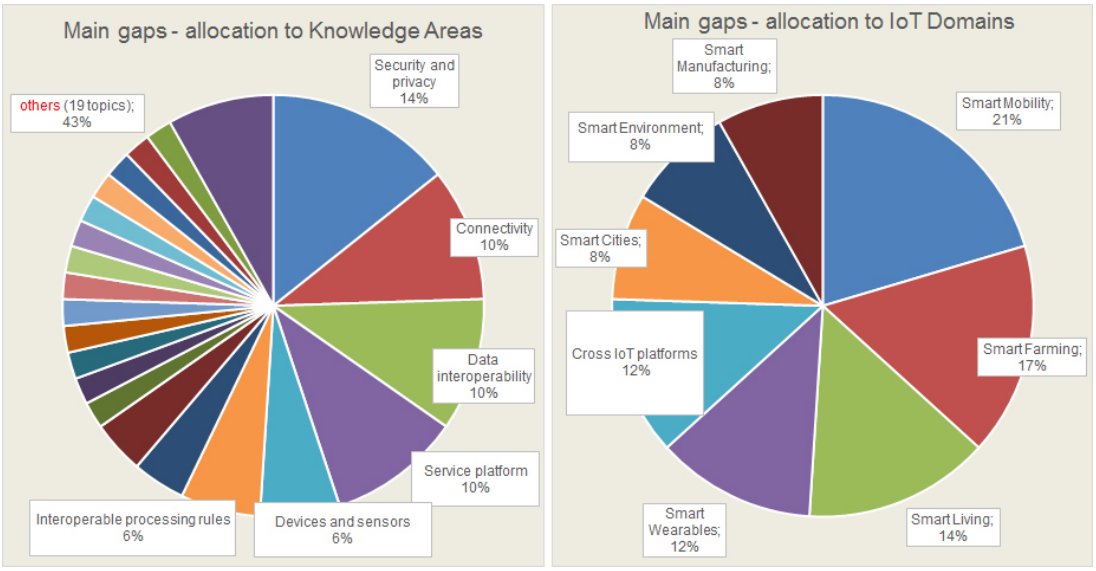

Figure 1: STF 505 gaps per Knowledge Areas and IoT Domains

The main conclusions from the STF 505 gap analysis are the following:

- Interoperability will be essential for the deployment of the IoT ecosystem and for ensuring seamless flow of data across sectors and value chains
- Solutions should be more than technical solutions
- Existing standards need to be refined to address non-technical issues
- Certification mechanisms are a very important topic, mandatory to complete technological developments
- Security and privacy are still a limiting factor
- Regulations and dissemination are needed to ensure users' acceptance
- Solutions should give advantage to transversal compatibility rather than vertical domain specifics

A more detailed description of the major gaps identified by STF 505 is provided in section 4, together with an initial attempt to prioritize the key gaps.

3.2 Identification of Standards Gaps: AIOTI WG3

The discussion in AIOTI WG03 has focused on elements that complement the approach of STF 505. At this stage, these elements have been subject to initial contributions and discussions but have not been elaborated further. They are mentioned here as a potential input for a next Release of the present document.

3.2.1 Safety

The topic of (System) Safety has been considered as important by some AIOTI participants (and also by STF 505, though the topic has not been addressed in depth in their technical report).

The main potential issue for safety (and a plausible reason to identify a gap) is that ensuring the safety of cyber-physical system may not get the same level of attention in the IoT community as their privacy or security.

Significant elements of the initial discussion in AIOTI WG03 are presented below. The rationale for considering this gap has been addressed by an initial contribution that has received a few comments.

Rationale

> While security cares about the adverse impact that the environment may have on a system (through e.g. changes of operating conditions, whether intentional e.g. attack or not e.g. accident), safety cares about the adverse impact that a system may have on its environment (e.g. explosion of a power transformer causing injuries to people).
>
> So far, while it is often stressed that security concerns are hindering IoT deployments, a lot of attention and regulatory efforts has been paid to address information privacy issues. Beyond the privacy issues, traditional cybersecurity techniques continue to apply to such systems, which remain in essence based on "cyber" process with limited direct impact on the physical world.
>
> However, it is now time to anticipate and support adoption of IoT technologies by actors outside of the ICT sector, such as automotive, manufacturing, healthcare and other industries. The need here is to create autonomous system that link sensors to actuators through a closed process control loop. In such systems, real time considerations require filtering data at the edge and relying on local processing capabilities as much as possible, resulting in many-to-many connection architectures with distributed processing.
>
> such cyber-physical systems involving actuators are meant to directly affect their physical environment. This creates a direct link between the security of such system and potential safety hazards. Ensuring the safety of such system certainly deserves at least the same level of attention as their privacy, but this is not yet emerging at the same level in the IoT community. "

Initial comments

- In systems were IoT will play an important role, particularly in mobile systems and highly automated/autonomous systems, it is important to consider all dependability and trust

properties that may apply. For example, this is addressed in the European Commission ECSEL JU projects (see [4]) under "Multi-concern Assurance".

- This is an important issue for industrial applications. However, safety is not a new issue for the industrial world. IEC 61508 (see [5]) introduces Safety Integrity Levels for hardware and system integrity. Several other standards exist for specific application areas (process industry, railway, automotive, …). So, one should start with these standards and see if gaps exist.

3.2.2 Overlapping of traditional domains and IoT

Vertical sectors have an already existing ecosystem managing safety and security. The challenge is to integrate the current rules and make them work with the IoT and future developments where not all needed standards exist currently. The mapping of standards to the various parts of the existing system where IoT devices can be inserted is vital. This will ensure that the appropriate SDO is taking care of the standards in the scope of its responsibilities. Each vertical sector has to be aware of such developments and collaboration is key for a win-win effort.

In the example of Agriculture Machinery, the integration of new features involved in the triggering of mechanical movements is currently handle in more than one SDO. The current list of Harmonised Standards* under the Machinery Directive (MD) is a first step. This identification will enable the development of the appropriate standard in parallel with future legislations. This is particularly true for functional safety of safety-related electrical, electronic and programmable electronic control systems.

*Refer to WG-2017.09-1 - CEN-CLC work programme and published standards in support of MD

3.2.3 Health of Edge Computers

A potential new IoT gap has been suggested related to the need to report/encode the Health of Edge Computers, meaning their operational stability. The questions addressed are:

- Is data from the Edge system trustworthy?
  - Is this computer uncompromised?
    - Since fabrication?
    - Since Commissioning?
  - Is the running software authentic?
    - Firmware, OS, Application code
  - Is this computer operating properly?
  - Is the data really coming from this computer?
  - Are the data properly managed and accessed only by the suitable persons?
  - What are the GDPR compliant policies with respect to personal data?
- Can device Computer vendors assess the health of the computer using Trusted Computing techniques?
- Is the above information reported to the IOT infrastructure?

4 Standards Gaps: Prioritisation

4.1 STF 505: Major gaps and Key gaps

The following table list some of the gaps that have been considered in ETSI TR 103 376. Those considered as key in a presentation made by STF 505 to AIOTI WG3 (see [3]) are in bold.

Table 1: Main STF 505 gaps and key gaps

Domain	Gaps
IoT Architecture	• **Multiplicity of IoT HLAs, platforms and discovery mechanisms**
Connectivity	• Fragmentation of the standardization landscape • Large number of heterogeneous & competing communications and networking technologies
Integration / Interoperability	• Global-level standards (international vs. regional level) • Fragmentation due to competitive platforms and standards
Device /Sensor Technology	• Quality assurance and certification • Device modularity
Service and applications	• **Data interoperability: lack of easy translation mechanisms between different specific models. Need of a global and neutral data model. Seamless inter-working between data systems** • **Interoperable processing rules: lack of definition for advanced analysis and processing of sensor events and data to interpret the sensor data in an identical manner across heterogeneous platforms** • APIs to support application portability among devices/terminals • **Specific solutions at Service Layer to enable communications between the platforms (e.g., plugins to oneM2M platform)**
Applications Management	• **Usability [Societal gap]** • Applications tailored to individual needs: evolution, flexibility of the components • Harmonized Identification • Interoperability between IoT HLAs, platforms and discovery mechanisms
Security / Privacy	• Privacy and security issues can be a blocking factor for user's acceptance and prevent large scale deployments. Security and privacy are addressed on an isolated basis for part of the applications • Lack of highly secure and trusted environments • Liability for data privacy
Deployment	• **Safety** • Deployment tools

Domain	Gaps
Regulation	• Regulations for frequency harmonization and usage
Business	• Collaboration between vertical domains, siloed applications • **Lack of a reference for business cases and value chain model to guide choices for deployment** • **Lack of knowledge about potentialities of IoT among decision makers, users**
Societal	• Green Technologies • Ethics. Transparency and choice for citizens • Not everything should be smart

4.2 CREATE-IoT: Large-Scale Pilots perceived Major gaps

In Deliverable D06.01 "Strategy and coordination plan for IoT interoperability and standard approaches" (see [9]), CREATE-IoT (Work Package 6) has summarised the initial assessment of the 5 IoT LSPs regarding the perceived criticality of the major standards gaps identified by STF 505. This assessment is listed in Table 2.

Table 2: Some standards gaps and overlaps and their perceived criticality

Nature of the gap	Type	Criticality
Competing communications and networking technologies	Technical	Medium
Easy standard translation mechanisms for data interoperability	Technical	Medium
Standards to interpret the sensor data in an identical manner across heterogeneous platforms	Technical	High
APIs to support application portability among devices/terminals	Technical	Medium
Fragmentation due to competitive platforms	Business	Medium
Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms	Technical	High
Easy accessibility and usage to a large non-technical public	Societal	High
Standardized methods to distribute software components to devices across a network	Technical	Medium
Unified model/tools for deployment and management of large-scale distributed networks of devices	Technical	Medium

Nature of the gap	Type	Criticality
Global reference for unique and secured naming mechanisms	Technical	Medium
Multiplicity of IoT HLAs, platforms and discovery mechanisms	Technical	Medium
Certification mechanisms defining "classes of devices"	Technical	Medium
Data rights management (ownership, storage, sharing, selling, etc.)	Technical	Medium
Risk Management Framework and Methodology	Societal	Medium

The criticality levels of Table 2 are resulting from the evaluation of the IoT LSPs done a few months after their launch. It may be the case that, one year after, those levels be differently evaluated, given the early feedback from the actual implementations.

CREATE-IoT WP06 has also has produced a mapping of those gasps on the three layers (Network, IoT, Application) of AIOTI WG03 HLA (see [11]) as shown in Table 3.

Table 3: IoT gaps mapped on the AIOTI HLA

Gap	Impact
Competing communications and networking technologies	Network layer
Easy standard translation mechanisms for data interoperability	IoT and application layers
Standards to interpret the sensor data in an identical manner across heterogeneous platforms	IoT layer
APIs to support application portability among devices/terminals	IoT layer
Fragmentation due to competitive platforms	Not specific to HLA
Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms	Mostly IoT layer, also Appl. and Network
Easy accessibility and usage to a large non-technical public	Not specific to HLA
Standardized methods to distribute software components to devices across a network	IoT and network layers
Unified model/tools for deployment and management of large-scale distributed networks of devices	All layers; critical in IoT layer
Global reference for unique and secured naming mechanisms	All layers
Multiplicity of IoT HLAs, platforms and discovery mechanisms	Addressed by HLA
Certification mechanisms defining "classes of devices"	Network layer
Data rights management (ownership, storage, sharing, selling, etc.)	All layers
Risk Management Framework and Methodology	All layers; interface definition

Short presentation of CREATE-IoT Deliverable D06.05

CREATE-IoT Deliverable D06.05 "Initial report on IoT standardization activities" is the initial report on standardization for the CREATE-IoT project and builds on input from the IoT European Large-Scale Pilots (LSPs). It focuses on the use of standards by the LSPs, pre-normative activities and further standardization opportunities based upon the gaps identified by the LSPs along with emerging new gaps.

The primary purpose of the deliverable is to outline the choices and possible strategies of the IoT LSPs regarding standardization and pre-normative activities. The current status of standardization in the LSPs – in particular in the LSP Use Cases under development – is examined, both in terms of standards support (which are the main standards used in support of the Use Cases implementation?) and standards gaps (what are the main missing elements that should be provided by standardization?). Based on this, a detailed analysis is made in order to identify the generic (i.e. non sector-specific) standards that can be used not only by the LSPs, but also by other IoT systems development projects.

4.3 CHARIOT Project: gaps from an industrial IoT perspective

The CHARIOT project (www.chariotproject.eu) develops technologies for the safe secure and privacy preserving IoT operation in an industrial context. CHARIOT's technical development needs to be informed therefore of all latest developments in industrial IoT and also in industrial systems that utilise IoT. Please note that the text describing CHARIOT perspective, taken with permission from CHARIOT Deliverable D1.1 [61], has been amended based on further inputs received from the AIOTI community.

There is currently significant IoT standardization activity by national and EU/international bodies such as ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS, oneM2M and OGC. Therefore, both IoT and industrial control and networking domains are characterized by a proliferation of standards. In particular, for IoT, due to its relative short existence, only some of these standards have been widely adopted. In the case of industrial IoT, there are some de facto established networking standards, but these are not always compatible with one another.

Therefore, since there are not many dominant standards, CHARIOT design and architecture is standards agnostic but *able to interoperate with any IoT* technology, by using the approach described below. Similarly, CHARIOT design and architecture is able to interoperate with any industrial system required.

The information which is transmitted in industrial networks can be classified as control, diagnostic, safety and historical information as follows:

- ***Control*** information is sent from controllers to actuators and vice versa, and feedback is either the input or output of a control loop implemented in a controller. Thus,

control data have strong real-time and deterministic requirements. Examples of control information include the actuator position, speed, tank level, fluid flow etc.

- ***Diagnostic*** information is sensory data collected, but not acted on, by the control system. This is used to monitor the health of plant equipment, and apply maintenance, repair or replacement as required. An example of such information is the temperature of an engine component. As diagnostic information is generally not acted on in real-time by the control system, it can also be referred to as monitoring information. Monitoring information has lower real-time requirements than control information, as it only needs to be recorded or displayed and not responded to. Monitoring information does however still require temporal consistency and minimal data loss.
- ***Safety*** information is used to implement safety related functions, such as the safe shutting down of equipment and the operation of protection circuits. As such, safety information has strong real-time requirements, and also high reliability requirements. In the past, control and monitoring were implemented in separate networks, but more recently their functions have been implemented using a single network.
- ***Historical information*** is system data which has been captured, stored and made available for off-line retrieval for example for analysis. This may include control, monitoring or safety information, which physically exists in the plant, as well as reference values that may be useful for analysis such as setpoints or calculated values.

Among the main advantages of wireless technology for industrial networks, a reduction in the amount of cabling required for communication is included, which in turn reduces installation costs. Wireless is also particularly suitable for hazardous environments or installation on moving equipment where cabling may be easily damaged or restrict the operation of the machinery to be monitored. Faster commissioning and reconfiguration can also be achieved. The industrial networks however often impose strict performance requirements in terms of latency, reliability and scalability and interoperability of the networking technology.

Latency is a measure of the delay that information takes to arrive at its destination. In terms of the Open Systems Interconnection (OSI) model, latency would be measured at the application layer. In an industrial automation system, for example, latency would be the time between a proximity event is generated by a sensor and the time knowledge of that event is received by a PLC or other controller. In an industrial control network with a safety role, tolerated latency can be often under 10μs, while order of magnitude larger latencies may be acceptable for higher level (e.g., supervision) networks.

Reliability is a measure of the likelihood of data loss within the network. It can be defined as the probability that a block of transmitted data is delayed long enough to become obsolete or lost due to noise. Similar to latency, reliability can be measured at the application layer of OSI model.

Scalability is a measure of the number of devices that may be deployed within a network without sacrificing reliability or latency. The network size will often dictate the maximum bandwidth allocated to any node. The larger the network is, the less bandwidth is available for transmissions between nodes. Protocols and architectures (e.g. mesh or star) will determine the limits of the size of a network installation. Most wireless sensor network specifications such as WirelessHART, ISA100.11a, and Zigbee (reviewed in the following sections) support large scale deployments; however, the network infrastructure must be able to cope with the throughput load of the network.

Interoperability in a factory application, for easy integration of networked devices is essential. However, while many wireless standards exist, making physical layer integration of devices within the wireless domain easier, most industrial networks fail to address the application integration well. For instance, WirelessHART describes an application layer interface, while ISA100.11a provides the constructs for such an interface. However, ZigBee and Wi-Fi provide neither the interface nor the constructs for an application layer protocol.

Coverage and Power consumption requirements relate to sensor network standards such as **ZigBee, RFID, and Bluetooth** which work over relatively short distances (i.e., tens of meters), and have low data rates and low energy consumptions. On the other hand, technologies like GPRS, LTE, WiMAX, etc., work over long distances and provide high throughput but, consume more energy and demand an expensive and fixed infrastructure of base stations that have line of sight with each other.

Owing to its low power consumption, the **IEEE 802.15.4** is a suitable standard for many IoT.. Other technologies that make use of unlicensed bandwidth (but may not be low energy) are the most popular, such as Wireless Local Area Network (WLAN) **IEEE 802.11, IEEE 802.15.1 known as Bluetooth**.

Please note that regarding the suitability of IEEE 802.15.4 facilitating communication among a large number of IoT devices or for covering large areas, the following remarks can be made:

- IEEE 802.15.4 is not only low power. IEEE802.15.4g is a flavour of this standard that covers utilities and large cities (smart metering, smart cities). Deployment of millions of devices over large countries (Canada, California and Japan) exist today. We can refer also to the Alliance WI-Sun which develops specifications and certifications for these markets and announced 66 million of deployed devices over 802.15.4.
- WirelessHart and ISA100.11a are recognized as industry standards and are also using IEEE 802.15.4 radio.

Other SDOs are working on industrial wireless technologies, e.g. IETF in the 6Tisch working group and ETSI, which published a report (GR IP6 009) on IPv6-based Industrial Internet [94]

However, following recent research and technological overviews as well as industrial requirements (CHARIOT project), standard wireless technology is even less suited to

industrial use than (wired) Ethernet, due to its inability to meet real-time communication performance requirements for the following reasons:

- **Susceptibility** to interference from a variety of sources, which causes transmission errors;
- **Multi path fading** and inter-symbol interference within the transmission channel itself;
- **Interference** from other transmission channels for example, at the boundaries between two wireless fieldbuses. Environmental electromagnetic emissions such as those produced by large motors and electrical discharges and thermal noise;
- The **Doppler-shift** induced by rapidly moving equipment. Such interference is often transient in nature, resulting in bursts of data and affecting the reliability and determinability of the transmission;
- **Environmental factors** limiting the wireless transmission range;
- **Operation at half-duplex**, as own transmissions would overpower any signal they might be intended to receive;
- **Security** of wireless transmission as physical access to the transmission medium cannot be restricted;
- **Power supply** which unlike with many wired fieldbuses that passively power field devices, existing wireless technologies have no such capability and provision for energy to remote devices is a concern, as is the energy efficiency of the remote devices;
- The **limited distance** over which wireless transceivers can operate, combined with the use of carrier sensing to determine when it is safe to transmit. This is avoided by wired networks such as Ethernet that ensures that each device has knowledge of all others to which it is connected;
- **Physical overhead** on a wireless system is also significant in comparison to wired systems, as most wireless protocols require the transmission of predetermined data sequences before or during data transmission in order to evaluate and correct the effects of noise on the received information.

In addition to difficulties in realising general reliability and timeliness requirements, the characteristics of wireless transmission can negatively affect specific **fieldbus methodologies**. Fieldbuses do not often acknowledge transitions, as the probability of unreceived data is relatively low. This approach however is unsuitable for wireless networks where the possibility of non-reception of a broadcast is significantly higher. This is especially problematic in the case of token passing networks, where the loss of the token may result in the bus needing to reinitialise to re-establish which device is the current master. Since interference is generally not uniform, some equipment may receive a broadcast while others do not. This can result in data inconsistency across a network. The half-duplex operation also means that carrier sensing with collision avoidance is not possible and a protocol such as CAN cannot be implemented. Nevertheless, several techniques can be implemented to improve the performance of wireless networks:

- Hidden node problems can be solved by adding a handshake system to the network,

in which permission to transmit must be requested and granted before transmission may occur. This allows the receiver to inform all other devices in its range, some of which may be out of the transmitter's range, that it is expecting a transmission and requires the channel to be kept open. This does however add significant overhead to the channel, especially in the case of small data packets, where the initialisation of transmission may require more time and data than the actual information to be communicated;

- Error correcting codes can be added to data that will not be acknowledged. This however increases overhead retransmission requests that can be sent for acknowledged data. This only adds overhead to the channel when a transmission fails, but the time required to retransmit may delay other transmissions;
- A combination of error correction and retransmission requests can also be implemented;
- Exploitation of spatial diversity can be achieved as interference is often localised, by using multiple, physically separate antennas;
- Advanced error mitigation strategies may also be implemented, such as deadline awareness and increased error correcting overhead for retransmitted signals. Still, each of the various technologies proposed for wireless use has its own advantages and disadvantages.

Short presentation of CHARIOT Deliverable D1.1:

This report [61] creates a baseline for the technical and/or design tasks, as well as, the work packages within the CHARIOT project, regarding the standards and guidelines in an IoT environment. With this, we include an extensive survey of industrial IoT standards which apply to the safety and security of industrial systems and are, directly or indirectly, related to CHARIOT application domains (rail, smart buildings, airports) and designed architecture.

4.4 MONICA LSP: Identification of an IoT/SRD RF standard for the stable and highly dependable transmission of sensor data

Introduction

Project MONICA (Management Of Networked IoT Wearables – Very Large Scale Demonstration of Cultural Societal Applications, http://www.Monica-project.eu) is a so-called Innovation Action, which implies, that partners must apply existing communication standards to the widest extend possible and refrain from spending granted workhours on developing "something that works". Instead eventual missing standards or gaps shall be identified and reported. Only one such identified item has been surfacing so far, and this was presented first time to ETSI, at its ERM TG 28 meeting in May 2019 in The Netherlands.

MONICA sound innovation

One of the two main areas of innovation within this (LSP) project MONICA is to seek, innovate, implement and bring to pilot demonstrations across the EU a method by which unwanted sounds from larger outdoor events can be mitigated by RF connected IoT devices, devices such that a real-time calculation of a new (mitigating) sound signal can be calculated. This mitigating signal is a sound field, which is amplified and radiated on site by a separate set of loudspeakers placed behind the audience area, such that inconvenient direct sound energy from the band on stage can be reduced for citizens living outside the event area.

The missing RF standard characteristics

This real-time calculation is executed by the ASFC (Adaptive Sound Field Controller), a fast computer system running a set of specially developed algorithms, which as parameters for calculations will need the continuous input stream from a set of RF-connected sensors, meteorological as well as acoustical, distributed throughout the event area. The proliferation of sound through the atmosphere is highly dependent on weather-parameters such as pressure, vertical pressure gradients, temperature and gradients, wind speed and so on plus of course the direct Sound Pressure Level (SPL) from the sound of the band playing. Some sensors have been mounted under a large tethered airship in order to transmit sensor data from above the band playing.

Sensor data latency and jitter

In such real-time applications of time critical sensor data, it is often of significance to have control over the latency and the latency fluctuations (time jitter) of the received data. This is in particular manageable in direct end-to-end RF links, operating on dedicated spectrum, whereas the networked IoT devices will contribute with latency and jitter characteristics that fluctuates with varying network load, and will thus introduce jitter in the data stream (see Figure 2 and Figure 3 below). This applies to all networked IoT devices if special priority is not assigned to the critical IoT devices in the network e-NodeB.

It should therefore be observed, that the mitigating signal's effectiveness drops if it is calculated from sensor data that are to "old". Then when the MONICA sound field finally reaches the spatial segment of mitigation, its effectiveness may be reduced as changes in the environment have occurred.

MONICA applies both networked IoT devices (WLAN, Operated LTE Mobile Networks) and direct end-to-end RF devices. Close study of the current ETSI portfolio of IoT/SRD standards have shown that latency and jitter has so far not been considered as an issue for applications of IoT devices.

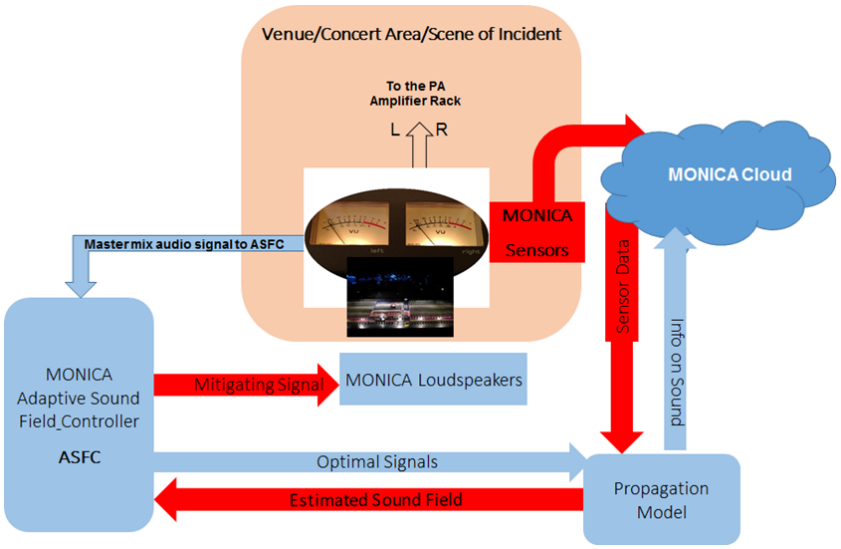

Figure 2: MONICA Acoustic Loop. The red routes are the time critical

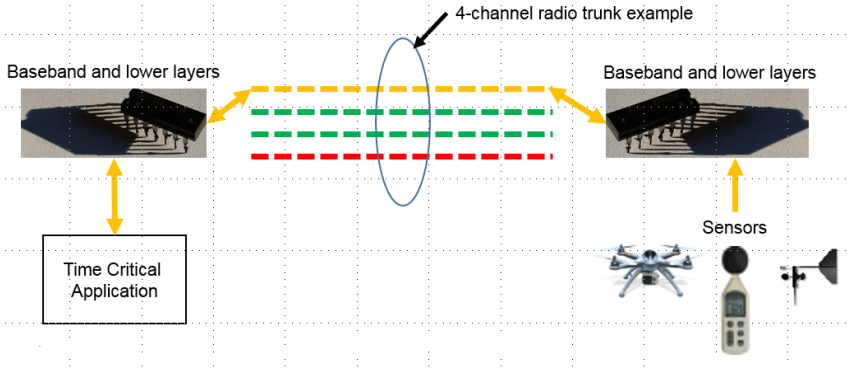

Figure 3: Example of an end-to-end RF link where latency and jitter can be controlled to be delivered within given time constraints

Figure 3 shows how latency and jitter characteristic should be part of the standard, such that connected applications should not "worry" about it. More or less a "Wireless Cable Connection".

4.5 SerIoT project

The Horizon 2020 SerIoT project (https://seriot-project.eu/) is investigating and defining solutions to improve the security and privacy of Internet of Things devices and systems. SerIoT adopts a multi-pronged approach based on different techniques and objectives. The main objectives are summarized in the following paragraphs.

SerIoT is investigating and working on the provision of a prototype implementation of (virtualized) and self-cognitive, IoT oriented honeypots, easily configurable so as to meet the standards of and adapt to any IoT platform across domains (e.g. embedded mobile devices, smart homes/cities, security & surveillance, etc.) that will be both integrally connected with the core network components

Because Software Defined Networks (SDN) are an important element of IoT based infrastructures, SerIoT is investigating and building prototypes of smart SDN routers for the dynamic (i) detection of suspicious/high risk paths, (ii) re-planning and (iii) re-scheduling of the routing paths of the transmitted information in IoT networks over secure and (per user- or per case-) preferable connections, supporting among others the interference of the human (i.e. semi-supervised approach), when needed. Furthermore, this objective will design and implement a suitable substrate of fog nodes to support secure allocation of compute, storage and network resources for i) localized processing of sensitive information, ii) define the security requirements of a path coordinated by SDN, and iii) enable secure communication with the core cloud.

SerIoT is working on the design of robust Decision Support System (DSS) and Intrusion Detection Systems (IDS), where all data and metadata from IoT networks will be collected, for the detection of potential threats and anomalies.

This can be complemented by design-driven security features monitors and validators for IoT platforms and networks based on IoT architecture and behaviour model specifications.

This work includes tasks to:

- analyse the impact of Blockchain in the Internet of Thing applications and infrastructures and to identify the potential risks and challenges to be overcome for the effective deployment of Blockchain in such a context.
- validate the aforementioned actions in both large- and small-scale representative real-case scenarios involving heterogeneous IoT platforms & devices in an EU wide testbed covering thus, a wide variety of eminent domain.

Work Package 9 (WP9) deals with the analysis of standards in the IoT context and potential gaps, which must be addressed. Such analysis has been presented in deliverable D9.5 of SerIoT. The main identified gaps and analysis of the results are reported below.

Short presentation of SerIoT Deliverable D9.5

This deliverable has surveyed the various standardization activities in the area of IoT and the use cases defined in the SerIoT project.

For each set of standards/domains, potential actions for standardization have been identified where the experience of the involved partners can be used to support ongoing standardization activities.

ITS is an important use case in SerIoT and some partners (JRC, AustriaTech and others) have been working many years in this domain in close collaboration with standardization bodies.

Extensive studies on standardization in ITS have been conducted. While many ITS interfaces and functions are well defined, some areas require additional standardization efforts where SerIoT partners can provide a significant contribution. In particular, anomaly detection, intrusion detection attacks and other techniques to identify security attacks in an ICT system can be applied to the automotive context.

Secure permissions, access control and the need to regulate trust relationships among the main entities in the ITS domain is an area where standardization effort is required. ISO TC 204 and its peer committee in CEN (CEN 278) are working on the definition of a framework (ISO/TS 21177 [91]) to support these aspects. Policy-based framework can be tailored to support the implementation of dynamic access control and control in a secure way the information flows in the ITS domain. One example is the control of the information flows to mitigate privacy risks.

SDN represents a key aspect in the SerIoT architecture to realize a more secure IoT. The integration of policy-based approaches in the SDN architecture could be useful for orchestration tasks. Indeed, orchestration represents an important aspect to be considered for an efficient resource management in IoT-enabled scenarios. In this direction, the ETSI has set up the working group ETSI NFV Management and Orchestration (MANO), which is focused on these aspects. It includes the identification of new attacks or vulnerabilities that can also be integrated with policy-based approaches for the specification of mitigation techniques. Such identification could be based on traffic analysis techniques that can be enhanced through the application of machine learning techniques.

Blockchain can be used in the IoT context, but the current standardization efforts must evaluate the trade-offs of the application of blockchain in IoT systems, which are often resource constrained. Scalability issues can also be present due to the huge amount of IoT devices and of the data which are generated and processed by them.

5G technologies are going to be used in combination with IoT in various domains. While 3GPP has various work items focused on security and privacy aspects, some elements requires further attention. Additional considerations on 5G are provided in Annex 3 " Security and Privacy aspects in 5G".

5 Gap analysis and resolution work in SDOs

5.1 Gap Resolution

The identification and prioritisation of gaps, and in particular standards gaps, has been done with the objective to ensure that they can be dealt with and resolved (and closed) by one or more organizations in the IoT community, depending on the breadth and complexity of the gap.

The resolution of the (standards) gaps is the work of the relevant organizations of the IoT community, in particular the Standards Developing Organisations (SDOs) and Standards Setting Organisations (SSOs) [42]. This section addresses the work done in some of the SDOs/SSOs involved in AIOTI WG3.

In the first release of the present document, this section was very much in its early stage.

The second release introduces in section 6 an analysis of the gaps and how they are addressed by the different SDOs.

5.2 Gaps identification and resolution work in ETSI

Some standards gaps have been identified within ETSI Technical Committees which will require further confirmation and – if needed – a resolution plan.

TC DECT

The gaps seen in IoT standardization:

- Area I: radio:
  - Low energy wireless protocols for IoT, home business and industry automation scenarios
  - Low Energy wireless IoT: Ultra Reliable Low Latency variant for industry automation
  - Low Energy wireless IoT: Ultra Reliable Low Latency streaming variant for the content industry
- Area II: low energy higher layer protocols
  - Lightweight architectures
  - Lightweight addressing and protocols
  - Lightweight transmission protocols
  - Lightweight integrated security
  - Lightweight application protocols (in general)
  - Lightweight application protocols for home automation

TC SmartBAN

Concerning the eHealth sensors/actuators low power and low energy issues, TC SmartBAN has already investigated those issues in the context of BANs (Body Area Networks) with the following two specifications:

- ETSI TS 103 326 V1.1.1 (2015-04): "Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer",
- ETSI TR 103 325 V1.1.1 (2015-04): "Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN".

EP eHEALTH

ETSI EP eHEALTH operates in tandem with ETSI TB's to address technical standards but it is always concerned with the wider, societal, environmental and ethical issues arising from technical debate. This particularly concerns interoperability and co-existence issues arising from the development of IoT.

All aspects of the operation of sensors are of prime concern, particularly where there is interaction between automatic systems, such as between intelligent transport and health related devices.

The gaps identified are:

- EP eHEALTH would welcome a clear architecture and identification of boundaries in IoT, to facilitate understanding of interfaces between value chain actors and their classification (this could be an output for an ETSI TR).
- A gap exists in classification based on functionality, control requirements, communication modes and requirements - to include all types of sensors. (Output for an ETSI TR).
- Also, a gap in classification / taxonomy for platform functions to include control / communication modes and requirements. (Output for an ETSI TR)
- eHEALTH issues require the details of AIOTI to be seen as significant elements in a huge control network. The stakeholders' interests demand clarification and identification. This urgently requires a common language and improved definitions of Users and Use Cases.

5.3 Maintaining an overview of standardisation activities and specifications related to IoT

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

AIOTI has for this report proposed an alternative approach, which is designed to improve collaboration and timeliness and re-use. The simple tool used is an excel document (contributed under CC4 licensing to SF-SSCC [33]) containing a macro and two lists (worksheets) which provide the basic information on (a) IoT organisations, (b) their specifications (see example in Figure 4). The lists are designed to show in the first few columns the public information on each organisation or specification, and then in additional

columns the added analysis, keywords or categorisation which AIOTI finds appropriate. Obviously, the list can be filtered or ordered to fit various types of analysis. The macro is able to export the key information and chosen categories into a mind map (see example Figure 5) which has been found to aid discussions and drill-down analysis.

	A	B	C	D	E	F	G	
1		Org_Short	Web	Org_Full	Abstract		SF-SSCC Category	SF-SSC
2	00295	3GPP SA2	http://	3GPP SA2 System	SA WG2 Architecture is in charge of developing the Stage 2 of the		Connectivity	Wirele
3	00174	ACEA	http://	ACEA (European	ACEA (European Automobile Manufacturing Association)		Mobility	
4	00392	AFNOR	https:/	Association	AFNOR is at the hub of the French standardization system, bringi		Organization	
5	00093	AIOTI	http://	AIOTI	AIOTI		Information Processing	IoT an
6		AREA	http://	Augmented Reality	Augmented Reality for Enterprise Alliance (AREA): global non-pro		Information Processing	Compu
7	00191	ARMOUR	www.	ARMOUR Project	ARMOUR Project		Information Processing	CyberS
8	00175	ASHRAE	https:/	ASHRAE	ASHRAE		Mobility	
9	00282	ATTM	https:/	ETSI TC Access,	ETSI TC Access, Terminals, Transmission and Multiplexing		Connectivity	Fixed
10	00173	AUTOPILOT	http://	AUTOPILOT	AUTOPILOT		Mobility	
11	00176	AVNU	http://	AVNU	AVNU		Mobility	
12	00038	BDVA	http://	Big Data Value Assoc	Big Data Value Association		Information Processing	
13	00085	Big-IoT	http://	BIG IoT	BIG IoT		Information Processing	IoT an
14	00177	C2C-CC	http://	C2C-CC (Car-2-Car	C2C-CC (Car-2-Car Communication Consortium)		Mobility	
15	00225	C40 Cities	http://	C40 Cities	C40 Cities		Smart City	
16	00178	CCC	http://	CCC (Car	CCC (Car Connectivity Consortium)		Mobility	
17	00179	CC-Link	http://	CC-Link	CC-Link		Mobility	
18	00128	CECIMO	http://	CECIMO	CECIMO: is the European Association representing the		Manufacturing	

Figure 4: Sample view of worksheet on IoT organisations

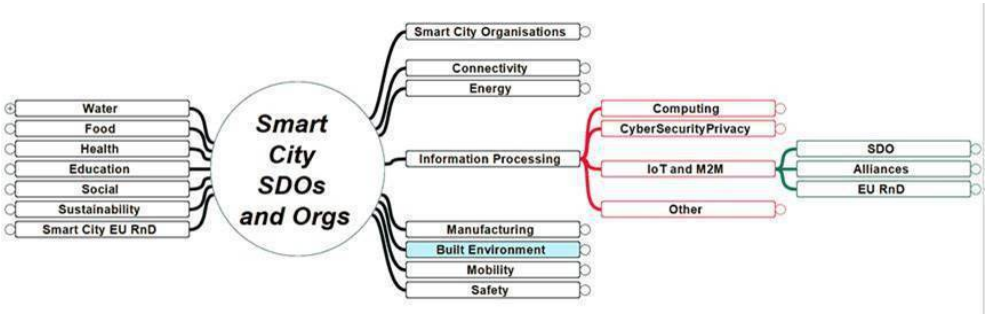

Figure 5: Sample view of the mind map

Importantly, each organisation which may in future re-use this excel sheet for other purposes can replace or add to the categories provided by AIOTI, enormously reducing the effort needed to make their own analysis or update. There is no necessity that other organisations re-publish their confidential material, but the objective is that additional public material (new organisations or specifications) will be shared. It would also be useful to collaborate with the main SDOs to similarly obtain regular updates to the benefit of all. Further information about using the excel sheet and the definitions of the categories applied in this report are provided in Annex 2.

It is possible to import specifications metadata into the excel file by e.g. copying or importing a CSV file with a few simple fields per row:

<comment>;<SDO and WG>;<title>;<url of landing page>; <optional categories>

Note: The term "landing page" is meant to indicate the overview html page (which for ETSI has the scope and publishing dates and the pdf link, and for ISO or CENELEC has similar info plus a "BUY HERE" button for the pdf). This is actually better than a direct .pdf link because the landing pages are more stable.

The excel sheet contains a list of SDO databases which are capable of exporting such CSV files, using site-specific filtering functions if desired, which is reproduced below for convenience.

Table 4: SDO Databases of Specifications

Org	Webpage_URL	Org_Full	Abstract
3GPP	https://www.3gpp.org/specifications		The 3GPP project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network and for interworking with non-3GPP networks. The different versions are named: GSM, GPRS (2G), EDGE, UMTS (3G), HSPA, LTE (or 4G), LTE Advanced, 5G.
5G-ACIA	https://www.5g-acia.org/	5G Alliance for Connected Industries and Automation	5G Alliance for Connected Industries and Automation ensures the best possible applicability of 5G technology and 5G networks for the manufacturing and process industries by addressing, discussing and evaluating relevant technical, regulatory and business aspects.
AIOTI	https://aioti.eu/aioti-wg03-reports-on-iot-standards	AIOTI WG03 Reports on IoT Standards	
CEN	https://standards.cen.eu/dyn/www/f?p=CENWEB:105	European Committee for Standardization (CEN)	Live search of CEN using title/summary but no export to file.
CENELEC	https://www.cenelec.eu/dyn/www/f?p=104:103	European Committee for Electrotechnical Standardization	Live search of CENELEC. Use "documents" tab.
CEPT-ECO	https://www.ecodocdb.dk/	CEPT Electronic Communications Office Database	The ECO Documentation Database provides an easily accessible (searchable, exportable) library of ECC deliverables (decisions, recommendations and reports) in the field of radio spectrum, numbering and networks regulation. Related documents,

			including relevant EC legal acts and ETSI technical standards are also provided for information, where applicable. All related EC deliverables, technical standards produced by ETSI and technical guidance notes developed by RED-CA, can be downloaded from their respective websites. A brief description of the features of this database is available here.
CESIP	https://webgate.ec.europa.eu/cesip/Index.aspx	Europe-China Standardisation Information Platform	The Europe-China Standardization Information Platform has information on standards in 10 sectors:
EC JOINUP	https://joinup.ec.europa.eu/collection/ict-standards-procurement/energy	Standards under Reg.1025-2012	Categorized list of specifications
ETSI	https://www.etsi.org/standards#page=1&search=smart%20city	ETSI Standards Search	The advanced search allows export of a file which includes SCOPE information for documents. It also can limit the search to keywords like OR(SAREF, IoT, SmartCity, M2M) ETSI has published TR 103 375 [1] which contains a landscape of IoT standardisation.
IEC	https://webstore.iec.ch/advsearchform	International Electrotechnical Commission	The search covers title and abstracts as well as IEC categories. No export found.
IEC	http://www.electropedia.org/	IEC Electropedia of Terminology	
IEEE	https://standards.ieee.org/search-results.html?q=smart+city		You may retrieve, download and print one (1) copy of the Materials in this Program for your personal use. You may retain one (1) additional copy of the Materials as your personal archive copy.
IETF	https://www.rfc-editor.org/search/rfc_search.php	Internet Engineering Task Force (IETF)	IETF RFCs cover many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, etc.
IIC	https://www.iiconsortium.org/vocab/index.htm		IoT Terminology
ISO	http://www.iso.org/obp		ISO Online Browsing Platform

ISO/IEC/IEEE	https://pascal.computer.org/sev_display/index.action		Joint vocabulary of computing terms
ITU-T	https://www.itu.int/net4/ITU-T/landscape	ITU-T Standards Landscape	Lists of IoT specs sorted by origin and keywords
ITU-T	http://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en#lang=en	ITU-T Terminology	
JoinUp	https://joinup.ec.europa.eu/collection/ict-standards-procurement/identified-ict-specifications-procurement	EU list of ICT Standards for Procurement	In order to allow the EU to respond to the fast evolution of technology in ICT, while also ensuring competition, promoting interoperability and innovation, the European Commission has developed a flexible approach to standardisation and can identify/cite ICT technical specifications that are not national, European, or international standards, provided they meet precise requirements. Once identified and approved, these specifications can then be referenced in European public procurement. This website displays the (short) list.
PICASSO	http://www.picasso-project.eu/wp-content/uploads/2016/10/PICASSO-D1.3-Panorama-of-ICT-landscape-in-EU-and-US-V1.4-Updated-with-new-US-5G-Initiative.pdf		Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US with Updates for Latest US Announcements on 5G Initiative'
StandICT.eu	https://www.standict.eu/standards-watch		EU project has title/scope info on about 180 standards documents, various domains
UNBIS	https://lib-thesaurus.un.org/LIB/DHLUNBISThesaurus.nsf/MultiEng/85759FD34196A99A85256AA0005FBD0B?OpenDocument	UNBIS Terminology	

The idea of using CC4.0 open license should enable any users (e.g. AIOTI) to import the lists into excel or a mind map or whatever, and annotate it according to their own ideas, as was proposed for this report.

6 Standards Gaps Analysis

This section added in version 2.0 of this report analyses the gaps identified by STF505 and the CREATE-IoT project that are listed in Section 4 and provides an analysis of their current status.

The list of gaps found in Table 1, Table 2 and Table 3 has been consolidated to enable this analysis. Tables 2 and 3 in the initial report are identical. They constitute a synthesis of Table 1. So, Table 2 was used as a basis, to recover the domain that was in Table 1. Two gaps have been merged into "platform interoperability" (Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms) and highly relevant gaps brought back in the list. Each gap has been given a name serving as header of the corresponding sub-section. This results in the following list:

Table 5: Key gaps analysed in this section

Nb	Nature of the gap [***gap name in sub-section headers***]	Domain
1	Competing communications and networking technologies. [***Connectivity interoperability***]	Connectivity
2	Standards to interpret and process the sensor data in an identical manner across heterogeneous platforms. Need of a global and neutral data model. [***Semantic interoperability***]	Service and applications
3	APIs that decouple applications from the details of specific IoT ecosystems as a means to enable open markets of services . [***Enabling Applications to Span Multiple Ecosystems***]	Service and applications
4	Safety. [***Safety***]	Deployment
5	Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms. [***Solution deployment and maintenance tools***]	Deployment
6	Standardized methods to distribute software components to devices across a network [***Software deployment***]	Deployment
7	Unified model/tools for deployment and management of large-scale distributed networks of devices. [***Scalable device deployment***]	Deployment/ Device-sensor technology
8	Easy accessibility and usage to a large non-technical public. [***Usability***]	Applications Management
9	Harmonized reference for unique and secured naming mechanisms. [***Harmonized identification***]	Applications Management
10	Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms. [***Platform interoperability***]	Integration / Interoperability IoT Architecture
11	Certification mechanisms defining "classes of devices" and ensuring quality of the devices. [***Device certification***]	Device-sensor technology
12	Data rights management: ownership, storage, sharing, selling, liability, etc. [***Data management***]	Security / Privacy
13	Risk Management Framework and Methodology. [***(Cyber-)Security***]	Security / Privacy
14	Green technologies. [***Green technologies***]	IoT Architecture

15	Ethics. Transparency and choice for citizens. [***Ethics and trustworthiness***]	Service and applications / Security / Privacy Societal
16	Standards needed to enable open markets of services. [***Open Markets of Digital Services***]	Business

Methodology for the gap analysis

- Section 6 has one sub-chapter per gap.
- For each gap, keywords are provided that would help searching for potentially available standards in the SDO databases, such as those listed in Table 4.
- A short summary of the status of the gap and recent actions since STF505 and Create-IoT contributions is then provided.

6.1 Connectivity interoperability

Short description: Competing communications and networking technologies.
Domain: Connectivity
Keywords: Wireless communication, Wired networks, LPWAN, cellular, connectivity, SDN, NFV, communication protocols, networks

Possible approaches identified to resolve this gap:

There are different wireless and wireline technologies in the IoT ecosystem, and we do not see a convergence to a single technology, therefore it is difficult to standardize a single connectivity mechanism in IoT. W3C WoT Thing Description allows to describe to IoT applications how to communicate and interact with Things. The applications therefore will automatically select the correct communication protocols pertaining to that particular Thing. Standardization activities for SDN/NFV are already going on in Open Networking Foundation (ONF), ETSI ISG NFV for QoS guarantees required for programmable networks. IEEE is standardizing Time Sensitive Networks (TSN) for latency and jitter sensitive IoT applications.

The connectivity in IoT is characterized by different heterogeneous technologies and a fragmented market. Probably, the main reason is due to the high diversity of IoT devices and IoT platforms covering a plethora of use cases. Thereby, this diversity in IoT devices, use cases and IoT platforms leads to different requirements in terms of connectivity. The market fragmentation due to the heterogeneous technologies used for connectivity can lead to interoperability problems as well. The connectivity in IoT typically refers to provide IoT devices a means of communication to the Internet, which paves the way to IoT platforms

developed at the cloud to access globally the data generated by IoT devices for data analytics and storage. To this end, the connectivity can be split in two blocks.

- Connectivity between IoT devices and IoT gateway
- Connectivity between the IoT gateway and the core network or Internet, which connect to the IoT platforms at the cloud.

Usually, the heterogeneity mentioned above, is found in the connectivity between the IoT devices and the IoT gateway. And from the IoT gateway to the Internet the connectivity is based on either the next wireless or wired technologies:

- Wireless technologies: 2G, 3G, 4G, 5G, LoRa, Sigfox, WiFi.
- Wired: DSL, Optical-based fiber (FTTX), Ethernet

Connectivity interoperability is the ability of a communication system to work with or use the components of another communication system; "work" means the capabilities to perform a certain function in a shared and agreed way as, for example, by using same file format, exchanging information via a precisely defined protocol, or using a common encoding-decoding schema. It is easy enough to achieve interoperability of different systems within the same domain or between different implementations within the stack of a specific software vendor. In the current IoT ecosystems, the various devices and applications are installed and operate in their own platforms and clouds, but without adequate compatibility with products from different brands. This platform interoperability is detailed in section 6.10.

The evolutionary vision of IoT is to provide interconnectivity between sensors, actuators, gateways and background data analytics infrastructure. IoT nurtures connectivity between physical objects through automation and data analytics to their monitoring/maintenance apps or digital twins. However, sudden increase in connected heterogeneous IoT devices takes a huge toll on the existing Internet infrastructure and introduces new challenges and gaps in both wired and wireless infrastructure such as:

- Gateway/Aggregator should be able to digest all the information coming from underlying sensors with different wireless technologies, often proprietary.
- Different stakeholders of IoT systems with different technologies pose risks in end-to-end security and privacy.
- From today's silos of sending the data to the cloud to future Any-to-Any IoT connectivity.
- Data need to be processed, acted and stored where it makes sense in the IoT connectivity perspective.
- IoT data may need different QoS properties based on its recipient IoT applications.

6.2 Semantic interoperability

Short description: First, standards to interpret and process the sensor data in an identical manner across heterogeneous platforms. Need of a global and neutral data model. Second, several standardized information models, which could be used for this purpose, already exist. But these models are not provided in a machine-interpretable form. A standard approach how to convert existing information models into a machine-interpretable form and how to create re-usable chunks of models that can be combined for different applications are needed too.
Domain: Service and applications
Keywords: interoperability, Semantic, data model, device template, ontology, cross-domain, cross-platform, device properties

Possible approaches identified to resolve this gap:

Semantic Interoperability was studied by ETSI STF547 in TR 103 535 [24]. Other organisations such as AIOTI or IEC have analysed the need for semantic interoperability as well.

AIOTI WG03 subgroup on semantic interoperability has coordinated the preparation of two white papers with the goal of advancing the adoption of semantic technologies and achieving semantic interoperability. Both whitepapers will be published under Creative Commons Attribution 4.0 International Licence. The first whitepaper "*Semantic IoT Solutions - A Developer Perspective*" [43] targets developers, who often lack a background in semantic technologies. It gives them an overview of the different aspects and steps required when developing semantic systems and it introduces the kind of tools to support these steps. The idea is to lower the entry barrier for making use of semantic technologies. The second whitepaper "*Towards semantic interoperability standards based on ontologies*" [44] targets standardization engineers and SDOs developing semantic interoperability standards. The paper focuses on best practices and the development lifecycle of interoperability specifications and underlying ontologies.

IEC Market strategy Board (looks at different topics, state of the art) has recently started a study on "Semantic Interoperability – Challenges in The Digital Transformation Age" (to be published by the end of 2019). The main contribution is the set of requirements, gaps, and recommendations, related to semantic interoperability in the upcoming digital age, i.e., the answer on question what needs to be done in order to enable semantic interoperability with respect to the state-of-the-art information models. The study also identifies the gap related to existing standard information models and their conversion into a machine-interpretable form, as well as how to create re-usable chunks of models that can be combined for different applications.

Several standards address the need for semantic interoperability to unlock the real potential of IoT, such as ETSI SAREF, ETSI NGSI-LD, OPC UA, W3C SSN, schema.org or oneM2M base ontology (see below),

Indeed, the oneM2M standards support different approaches for semantic interoperability. The main approaches are:

- Pure ontology-based solution (RDF/OWL serialization format)[25];
- Common vocabulary (basic serialization format XML or JSON): Smart Device Template (SDT) for the home domain [26];
- Resources specializations using oneM2M FlexContainer resources [27];
- Blackbox resources: Basic oneM2M resources (Container, ContentInstance and Group) extended with an external domain-specific data model [28] [29].

The Smart Applications Reference Ontology (SAREF) is a standardized ontology for IoT devices and solutions published by ETSI in a series of Technical Specifications. SAREF [30] is conceived in a modular way in order to allow the definition of any device from pre-defined building blocks, based on the function(s) that the device performs. These building blocks allow separation and recombination of different parts of the ontology depending on specific needs. The SAREF ontology supports a direct mapping with the oneM2M Base Ontology oneM2M TS-0012 and thus runs with oneM2M-compliant communication platforms. The mapping between SAREF and the oneM2M Base Ontology is described in detail in ETSI TS 103 264 [30] and oneM2M TS-0012 [25].

The SDT (Smart Device Template) data model, an initiative from HGI, hides the technology-specific, native language format of devices of different technology type from the applications. More details can be found in oneM2M TS-0023 [26].

ETSI ISG CIM (Industry Specification Group for cross-cutting Context Information Management) working group defines an API called NGSI-LD [34]. The NGSI-LD Information Model [35] prescribes the structure of context information supported by an NGSI-LD system. It is defined at two levels: The Core Meta-model and the Cross-Domain Ontology. The Core Meta-model is based on property-graph methods and allows representation of entities (things), their properties and the relationships between entities, but also allows representation of the properties of properties (e.g. the accuracy of a measured value) and properties of relationships (e.g. the duration of the relationship, which might be e.g. the date of registration of a marital relationship, or the electronic signature for validating the relationship). The cross-domain ontology is a set of generic, transversal classes which aims at avoiding conflicting or redundant definitions of the same classes in each of the domain-specific ontologies. The protocol for serialization of information is based on JSON-LD. The protocol is suitable for federated systems of context information databases.

OPC UA (Unified Architecture) is a standard for horizontal communication from machine to machine (M2M) and for vertical communication. OPC UA provides a framework that can be used to represent complex information as Objects in an Address Space. These Objects consist of Nodes connected by References. The unification of the information representation between information producers (servers) and consumers (clients) is based on the notion of type. A global OPC UA information model describes all basic types. This information model

can be used by developers as a foundation for the representation of their own specific data model. OPC UA has two recent activities that are worth noting:

- OPC UA Field Level Communications (FLC): This initiative extends OPC UA so that it can be used for field level, i.e., communication between a control level and field devices. One notable feature of this standard will be a standardized OPC UA information model for field-level devices, which can be used in online- and offline-engineering scenarios e.g. device description and diagnostics. There will be specified different application profiles for the information model, e.g., IO, motion control, safety, system redundancy, and so forth.
- OPC UA Semantic Validation: This activity has started recently by OPC UA and is related to semantic validation of OPC UA information models. As OPC UA standardizes a lot of information models, the problem of validating these models, as well as user specific OPC UA models, has been recognized. As the activity has just started more information about the activity's scope will follow. This activity can also be considered as part of a potential device quality assurance mechanism (see section 6.11).

The Semantic Sensor Network (SSN) ontology is a widely-recognized ontology published by the https://www.w3.org/2015/spatial/ of the W3C as a recommendation and currently in its Version 2.0 [31]. SSN focuses on the description of sensing devices and the observations they make of the physical world, the involved procedures, the studied features of interest, the samples used to do so, and the observed properties, as well as actuators. It follows a horizontal and vertical modularization architecture by including a lightweight but self-contained core ontology called SOSA (Sensor, Observation, Sample, and Actuator) for its elementary classes and properties.

The Web of Things (WoT) [62] is a standardization activity by the World Wide Web Consortium (W3C, see also section 6.3). WoT seeks to counter the fragmentation of the IoT through standard complementing building blocks (e.g., metadata and APIs) that enable easy integration across IoT platforms and application domains. A Thing is an abstraction of a physical or virtual entity that needs to be represented in IoT applications. Thing is represented by a Thing Description (TD), which is a machine-readable description. A TD provides general metadata of a Thing as well as metadata about the Interactions, data model, communication, and security mechanisms of a Thing. Thing's Interactions are specified in a so-called Interaction Model. The model defines three types of Interactions: Property, Action, and Event.

Schema.org Extensions for IoT: iotschema.org is a W3C Community Group for extending Schema.org to connected Things. The organization provides an open, publicly available, repository of semantic definitions for connected Things. It is an extension of well-known schema.org to enable descriptions of Things in the physical world and their data. iotschema.org can be effectively used to semantically enrich W3C Thing Description. It

provides a way for domain experts to easily create semantic definitions that are relevant to their application domain. iotschema.org reuses existing standardized semantic definitions whenever possible.

For more details: https://www.w3.org/community/iotschema

Conclusion

The previous paragraphs show that there are currently standards and directions being followed for the semantic description of systems. As the different IoT platforms often choose one of these solutions, there is a need for (standardized) entities or reference / abstract ontologies able to perform the mapping between the different existing ontologies [32]. The mapping can be realized directly between the ontologies used by the different systems or by translating each used ontology to a generic ontology that serves as a common reference. The mapping between different ontologies should be considered at the border of a system rather than internally to a system. Statistical approaches could be used additionally to define the mapping between ontologies and resolve the issues brought by incompleteness or uncertainties of the mapping.

Semantic interoperability is being addressed in different SDOs, which deliver ontology and semantics standards, but gaps remain and indeed, multiple approaches are increasing the fragmentation and confusion in the number of options. Further coordination between various groups would be needed to avoid a fragmented offer for IoT semantics.

6.3 Enabling Applications to Span Multiple Ecosystems

Short description: APIs that decouple applications from the details of specific IoT ecosystems as a means to enable open markets of services
Domain: Service and applications
Keywords: Web of Things, Thing Descriptions, Object Models, Semantic Descriptions, Metadata, Discovery, Payments, APIs

Possible approaches identified to resolve this gap:

- Web of Things

The fragmented landscape for IoT standards and platforms makes it challenging for application developers seeking to integrate across devices and information services from multiple ecosystems. To tap into the network effect, we need to establish a single European market for digital services. We need a transition plan that will take us to where we want to be some years hence.

Here are some alternatives.

- Somehow everyone switches to a single platform and standard: this is very improbable
- Client applications are written to work directly with multiple IoT protocols and standards: this is costly for developers
- Client applications are written to a single standard, and the underlying application platform maps this to multiple IoT protocols and standards: this is costly for platform developers
- Server applications act as gateways between different protocols and standards, so that client platforms and applications are decoupled from the multiplicity of IoT platforms and standards

The Web of Things focuses on the last two choices above, exploiting metadata that describes services in terms of semantic interoperability, the interfaces (virtual devices) exposed to client applications, and the communications and security metadata needed to access a server platform. A server-platform hosts application, which supply services, whilst a client-platform hosts application that consume services. Of course, a given platform could take on both roles, and likewise a single application could be both a consumer and supplier of services.

The diverse range of requirements for IoT devices justifies the corresponding diversity of IoT communication technologies at the network edge. This can be contrasted with connecting suppliers and consumers of things (i.e. digital twins) across the Internet, where the range of the requirements is much smaller. Here, it would make sense to encourage convergence on protocols for open markets of IoT services (i.e. the fourth bullet above), whilst allowing, at least for an interim period, that client platforms may need to support multiple standards, but at least this can be hidden from client applications. The downside is that this involves the need for additional metadata (a burden for suppliers of services), and an increased cost in tracking changes to the standards supported (a burden for platform vendors).

Is it possible to encourage SDO's such as ETSI, oneM2M, W3C and the IETF to work together on a convergence plan? This could start with alignment of the meta model for IoT services, and then focus on identifying the requirements for convergence on protocols. What means could the EU employ to encourage this?

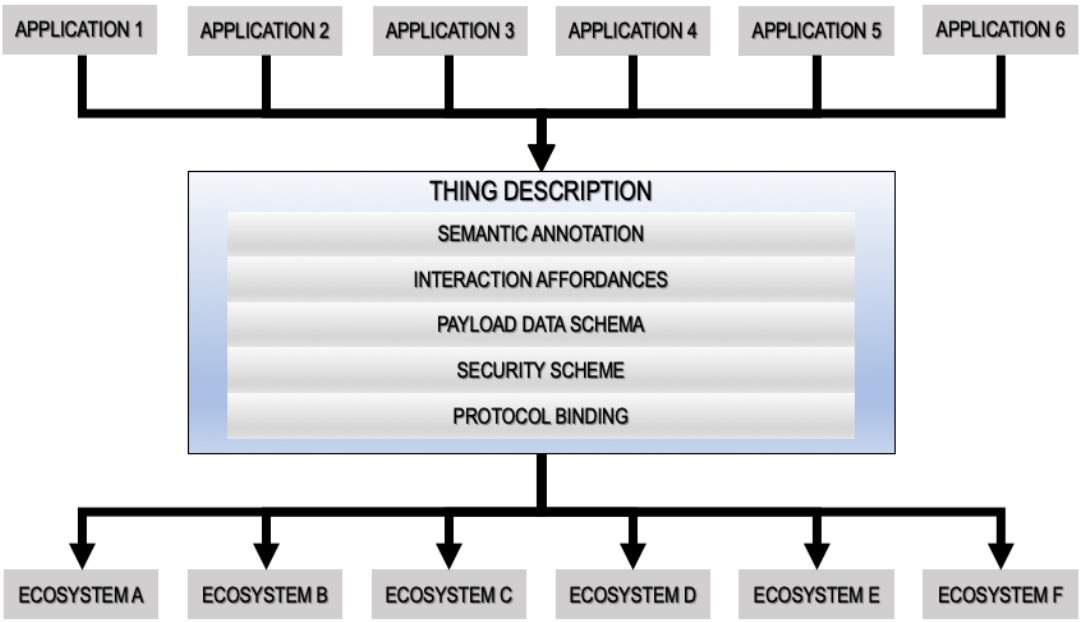

Figure 6: How the Web of Things enables applications to span multiple IoT ecosystems

For more details:

- https://www.w3.org/TR/wot-thing-description/
- https://www.w3.org/TR/wot-architecture/

6.4 Safety

Short description: Safety.
Domain: Deployment
Keywords: Provisional IoT safety, European legislation, Harmonized standards, Machinery directive

Possible approaches identified to resolve this gap:

In the domain of connected machinery, we need to ensure that performance levels regarding safety and security are fulfilled by the equipment exchanging data with the outside world. Today, the complexity for the management of all modules to be integrated into a machinery is rising substantially, and some essential health and safety requirements need first to be addressed. In this domain, because of years of experience in the risk assessment process and good lessons learned from the mechanical industry, this process should be carried out into the ICT domain, where this represents new challenges. The current Machinery Directive [66] is under evaluation for a potential extension of its scope including IoT devices or robots, and a definition at a higher level for safety, security, and

trust, before the standard definition to match the specifics of each sector, needs to be tackled. This is balanced by the objective of some stakeholders to develop an IoT specific directive with the objective to be able to integrate in the machines the IoT devices while preserving existing regulations.

The data processing must ensure that a risk assessment is carried out in order to determine the trust, security, and safety requirements, which apply to the device equipped with sensors. The device should then be designed and calibrated taking into account the results of the safety risk assessment.

By the iterative process of risk assessment and risk reduction referred to above, the device supplier should:

- determine the limits of the trusted environment, which include the intended use and any reasonably foreseeable misuse thereof,
- identify the risks that can be generated going through all the layers constituting the solution and the associated unreliable situations,
- estimate the lack of trust, considering the value that you can have in the data, that the end-user will use through organisations, operations, hardware, and software,
- evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of the actuation of the device base on the data generated or received.
- eliminate the risk of corruption or reduce the risks associated with a distributed database by application of protective measures

6.5 Solution deployment and maintenance tools

Short description: Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms
Domain: Deployment
Keywords: configuration, software management, firmware update, provisioning, diagnostics, monitoring, device management

Possible approaches identified to resolve this gap:

Device Management is a tool enabling telecommunications operators, manufacturers and service providers to make sure that smart objects installed on clients' premises are working correctly. In our environments, this invisible "masked hero" is becoming more crucial by the day, providing an ecosystem of reliable equipment for the countless services of the IoT, with the smart city, healthcare, agriculture, the smart home, or industry 4.0.

What is Device Management, and why is it so important? Device Management consists of a set of operations remotely executed on connected devices in a secure environment: provisioning, configuration, firmware updates, and diagnostics.

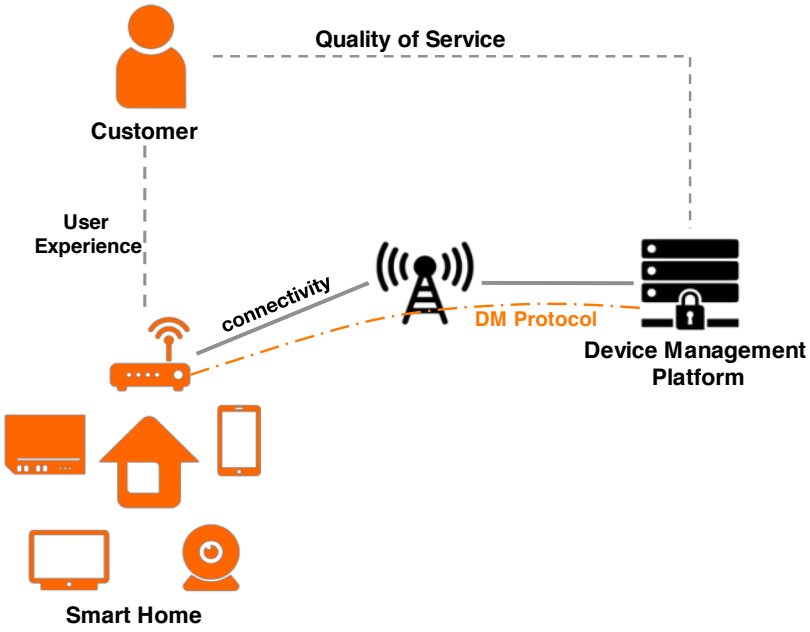

Figure 7: Legacy Device Management

1. Provisioning is the process involved when the device connects for the first time, providing the necessary credentials, right configuration and firmware version.
2. Configuration refers to the activation and setting of device services, such as Wi-Fi activation on a modem.
3. Software and firmware updates/upgrades are destined to take corrective measures and augment the device with new services.
4. Diagnostics consist in test and monitoring tasks, providing information about the device, such as events and logs, so as to detect problems and potentially trigger repair actions.

Regarding the different topics "Solution deployment and maintenance tools", "Software deployment" and "Scalable device deployment", Device Management may be the answer to all of them, but current standards addressing DM will need some evolutions to fulfil IoT needs.

The IoT does present challenges to be addressed for operation to be reliable and long-lasting: heterogeneity of devices, diversity of usages, security, confidentiality, and availability.

IoT platforms, initially designed to collect data so as to extract information and provide recommendations, are dependent on Device Management.

Current standards initiatives are at the Broadband Forum (BBF), the Open Mobile Alliance (OMA), the IETF, oneM2M and OSGi Alliance.

With TR-069 [69], the BBF had a successful deployment in Digital and Smart Homes. However, regarding IoT, TR-069 cannot scale up. BBF has specified TR-369 (USP for User Service Platform) [71] aiming at fulfilling IoT requirements. OMA with OMA-DM [73] had also a successful deployment in the mobile management domain but, as for TR-069, OMA-DM cannot scale up. OMA has specified the OMA Lightweight Machine to Machine protocol (OMA LWM2M) [72], a protocol more suitable for IoT constrained devices. It is worth mentioning that both BBF USP and OMA LWM2M propose a convergence of Device and Service management, so as to avoid the necessity for multiple protocol stacks on a device.

IETF on its side is working on two topics. COMI (CoAP Management Interface) is an initiative to transpose the IETF proposal for IT management based on NETCONF and YANG to IoT and constrained devices. SUIT (Software Updates for Internet of Things) is a proposal for defining a manifest format for software updates on IoT devices.

oneM2M has defined specifications for the interworking between oneM2M and different Device Management protocols, mainly BBF TR-069, OMA DM and OMA LWM2M, defining specific resources called Management Objects. While this interworking approach is a good approach for federating the heterogeneous ecosystems, the current proposal lacks flexibility.

OSGi Alliance specifies a standard execution environment based on Java with a SOA approach. OSGi applications are based on modules which can have dependencies and can be installed or updated at runtime. In this goal OSGi proposes a set of specifications for Device Management of OSGi devices. It mainly relies on the Device Management Tree (DMT) Admin API. The DMT is conceptually close from OMA or BBF concepts.

A new generation of Device Management platforms and therefore new standards or evolutions of existing ones may be needed to treat these challenges: capacity to scale up, capacity to hide and abstract the heterogeneous ecosystems of devices to manage (device abstraction layer with semantic descriptions), capacity to take the context of users/customers and of their devices into account whilst guaranteeing their privacy protection.

6.6 Software deployment

Short description: Standardized methods to distribute software components to devices across a network
Domain: Deployment
Keywords: see keywords in section 6.5.

Possible approaches identified to resolve this gap:

This gap has been addressed together with the "solution deployment and maintenance tools" analysis in section 6.5 (previous section).

6.7 Scalable device deployment

Short description: Unified model/tools and strategies for deployment and management of large-scale distributed networks of devices
Domain: Deployment/ Device-sensor technology
Keywords: campaign management, software management, configuration, provisioning, device management

Possible approaches identified to resolve this gap:

With the large-scale number of IoT devices, we need methods and approaches for large scale firmware and software deployment. Device Management platforms must adapt to the new volume of connected devices. To that end, "campaign management" tools allow to define operations for large numbers of devices using rules.

It is then possible to dynamically enrol devices based on their state, which triggers automatic provisioning or firmware upgrade operations. For instance, it is possible to target only devices with a specific firmware, or a specific type.

In addition to these reactive operations, pro-active operations may be required, for instance when a vulnerability is detected on a family of devices, requiring a prompt firmware upgrade. It is then necessary to hold smart inventories, storing the relevant data for an efficient targeting of devices. Moreover, the execution of these massive campaigns needs to be monitored and controlled. Rollout tools will trigger operations on devices following specific strategies balancing operational and functional risks. For example, it would be unwise to upgrade every device at the same time in general, given the fact that this operation could introduce problems such as crashes or disconnections. Thus, the targeted device population may be divided in sub-groups, whose size may increase as the operation proves to be successful in the earlier test groups to improve velocity. However, in the case of a security crisis, the small time overhead induced by this cautious strategy may prove more harmful than potential dysfunctions, motivating a more direct approach with simultaneous upgrades.

These requirements are partly described in the BBF TR-131 [70], which specifies the use cases and functional requirements for a DM solution Northbound interface, without specifying the interface itself (lack of the specification). It includes requirements for architecture, provisioning devices, device operations, file management, device grouping, events, error management, security and access control. However, these specifications may need some adaptation for the IoT context.

6.8 Usability

Short description: Easy accessibility and usage to a large non-technical public
Domain: Applications Management
Keywords: Human Factors, configuration, upgrade, accessibility

Possible approaches identified to resolve this gap:

This topic is still open. Further standardisation activities are required.

6.9 Harmonized identification

Short description: Harmonized reference for unique and secured naming mechanisms
Domain: Applications Management
Keywords: Identification; Identifier; AIDC (Automatic Identification and Data Capture); RFID (Radio Frequency Identification); Interoperability; URN; IPv6 address.

Possible approaches identified to resolve this gap:

In general, no single identification scheme fits all needs and often identification is bound to a specific technologies or governance bodies. Examples are domain names, IP and MAC addresses that are bound to specific communication technologies and car license plates that assigned by public authorities. These different identifiers might be bound to the same entity and can be assigned in a static or dynamic way. In that case resolution between the different identifiers has to be done. Examples are the Domain Name System (DNS) which maps between domain names and IP addresses and the Address Resolution Protocol (ARP) which maps between IP and MAC addresses.

Furthermore, specifically for the identification of Things various identifiers schemes are already in use and standardized for years. They are often application or domain specific like identification of freight containers (ISO 6346 [55]), books (ISBN/ISO2108 [56]) and animals (ISO 11784 [57]). These existing schemes will be used in IoT and a convergence to a single scheme is not expected. In case IoT applications have to deal with several identification schemes differentiation between them is needed in order to ensure uniqueness and correct interpretation and processing of the identifiers. That can be based on the specific context in which the identifier is used or on a meta-identification scheme like ISO/IEC 29161 [58]. ISO/IEC 29161 introduces an unambiguous wrapper based on URNs for the differentiation. The wrapper allows to identify identifier schemes based on various standards for which URN namespaces are defined (e.g. urn:epc, urn:oid, urn:isbn, urn:uuid). Also, proprietary identifier scheme could be covered by registering an urn namespace with IANA (see IETF RFC 8141 [59]) or a sub namespace with a registration entity that offers such a service.

For a more detailed discussion, see AIOTI report on Identifiers in Internet of Things (IoT) at: https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf.

6.10 Platform interoperability

Short description: Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms.
Domain: Integration / Interoperability - IoT Architecture
Keywords: IoT Platform, IoT Platform Interoperability, oneM2M Interworking Proxy Entity, IoT Data Models, Ontologies, IoT Platform Architecture, SPDI (Security, Privacy, Dependability, Interoperability), Cross-domain IoT operation, Cross-Platform Access, Cross Application Domain Access, Platform Independence, Platform-Scale Independence, Higher-level Service Facades.

Possible approaches identified to resolve this gap:

The next sub-sections provide different approaches aiming at solving the platform interoperability challenge and how they relate to existing standards.

This topic has also been subject of an ETSI report prepared by STF547, ETSI TR 103 536 [45]. This report outlines the nature, the role of IoT platforms and proposes elements for the identification of the most relevant ones. It addresses detailed examples such as Industrial IoT to outline the challenges posed to generic IoT platforms. The issues related to the interoperability and interworking of IoT platforms are explained, in particular for standardised IoT platforms, and how the way they are handled can foster their adoption by the IoT community.

The Technical Report provides an overview of the very fragmented IoT platforms landscape. At first, it describes a framework for IoT platforms outlining some requirements that should be met by the main IoT platforms in order to expand their capabilities and attractiveness to IoT systems designers and developers. The impact of two major evolutions, namely Big Data and Virtualisation, on these platforms is analysed. The overall objective is to better characterise what properties a "standardised IoT platform" should embed in order to become a major reference to the developers of IoT solutions in various business sectors.

Besides providing a classification of IoT platforms, including advantages and drawbacks for each of them, the document introduces platforms identified by UNIFY-IoT and the IoT-EPI, platforms used by the EU-funded IoT Large Scale Pilots, and the platforms standardised by oneM2M, OCF and the Open Source Software Apache platform.

The document devotes special attention to interworking across all layers of the interoperability stack (from technical to organisational). It analyses the technical approaches in support of interoperability and outlines some criteria for best support of interoperability within and between platforms. Based on these criteria, a list of "candidate platforms" is established and an evaluation of the actual support of these criteria by the identified platforms is made.

Furthermore, the report presents Industrial IoT (IIOT) as a typical case study of the many challenges that are posed to standardised platforms. Beyond the identification of major requirements, it addresses some challenges such as the role of legacy and its impact on

candidate platforms. Based on these requirements, a list of potential platforms is provided. Some of them are analysed in order to evaluate their coverage and what should be done to overcome potential limitations.

Finally, some recommendations are made towards the IoT community regarding standardisation, convergence of platforms, interoperability support frameworks.

6.10.1 Patterns of IoT Platform Interoperability

This subsection is based on the material published in the paper [48] that was elaborated as part of the BIG IoT project [49] as well as [50]and was extended in the SEMIoTICS project (https://www.semiotics-project.eu) [51].

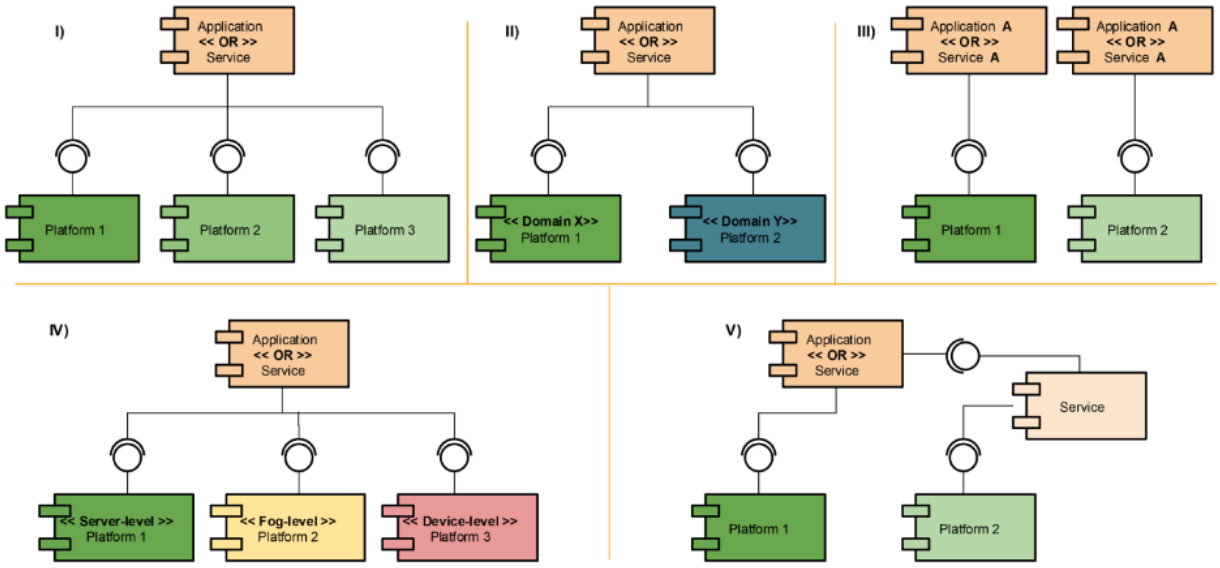

Figure 8: Patterns of IoT platform interoperability (Source [48])

Achieving interoperability on the IoT, requires a closer look at interactions of the key components in IoT ecosystems. We analyse here those interactions and we identify in Figure 8 five generic interoperability patterns for IoT ecosystems.

The "Cross Platform Access" pattern (Figure 8, I) is the basic characteristic of an interoperable IoT ecosystem. The goal of this pattern is to hide that an application or service accesses resources (information or functions) from different platforms through the same interface specification. The challenge of realizing this goal lays in allowing applications or services to discover platforms with relevant information, and enabling platforms that are potentially from different providers to have the same interface and use the same formats to communicate data.

The pattern "Cross Application Domain Access" (Figure 8, II) extends the "Cross Platform Access" pattern. The goal is that services/applications are able to access information and functions not only from different platforms, but also from platforms, which host information from multiple application domains. Thereby, it is crucial that semantic interoperability is given through well-defined and shared information models. A cross-domain application that accesses multiple IoT platforms, could e.g. air quality information and traffic data to provide green routing through a city.

The goal of the pattern "Platform Independence" (Figure 8, III) is to allow a single application or service to be used on top of different IoT platforms (e.g. in different regions). For example, these can be multiple deployments of a "smart parking" service used in two different geographic regions, which utilize different platforms with information about parking spots. This is especially challenging, when the sensors producing the IoT data are based on entirely different technology (e.g., radar-based parking spot observation, or counting in & outs of a parking lot).

The goal of the "Platform-Scale Independence" pattern (Figure 8, IV) is to hide different platform scales towards the connecting services and applications. So called server-level platforms are platforms with many devices connected (e.g. a cloud platform), whereas device-level platforms grant direct access to attached sensors, and fog-level platforms are intermediaries such as edge gateways. A platform implementing this pattern has to hide its scale from applications and services accessing it.

Finally, the pattern "Higher-level Service Facades" (Figure 8, V) extends the interoperability requirements from platforms to higher-level services. Here, services are acting similar to platforms and also provide IoT offerings via a common interface. Such a service acts as a façade towards an IoT platform and use or process the IoT offerings of the platform to provide added value.

Once the above described patterns are implemented, they ensure ecosystem interoperability and allow an easy re-usage of IoT offerings from the various platforms of the ecosystem.

Organizational interoperability can be realized by IoT platform federations formed by multiple partnering institutions that collaborate by sharing IoT resources in locations originally out of their reach. This represents an additional horizontal integration that enables "Open networked" IoT business models.

We can define an IoT platform federation as an association of a number of platforms enabling their secure interoperation, collaboration and sharing of resources. Platforms can be enabled to perform collaborative sensing/actuation tasks and to interact directly so as to trade/share resources. A mechanism for defining and monitoring Service Level Agreements should be in place, while we can also envision the emergence of roaming IoT devices, where a device registered and managed by one platform is nomadic and can interact with resources in smart

spaces managed by another federated platform (in a visited smart space). Federated platforms should of course control the terms under which a roaming IoT device is allowed to use resources in environments operated by visited platforms.

Possible approaches identified to resolve this gap:

- BIG IoT and SEMIoTICS

Figure 9 presents an overview of the BIG IoT architecture for IoT ecosystems, which has been realized and made publicly available as open source in the Eclipse Bridge.IoT project [47]. An open marketplace for IoT platforms and services as providers to trade available resources (information and functions) is at its centre. IoT applications or services as consumers of resources can use the marketplace to discover them and access them in real-time. The architecture has been specifically designed to support all of the above-described patterns of interoperability. The architecture is centred around a common set of interfaces, referred to as the BIG IoT API, that are supported both by resource providers and consumers, as well as the marketplace, where resources are traded.

During the course of the BIG IoT project, the interface specifications have influenced the standardization at W3C's Web of Things initiative [64]. In the W3C approach, the Thing Description [62] provides comprehensive metadata about the possible interactions with an IoT device, service or platform. These reflect the description of the "Access" interface in Figure 9. This is the most crucial interface, as it is the basis for communication within IoT applications. The M* interfaces of the BIG IoT Marketplace have not yet been considered by standardization activities. However, considerations regarding the "M3 Discovery" interface have been investigated in context of the W3C WoT initiative in [63].

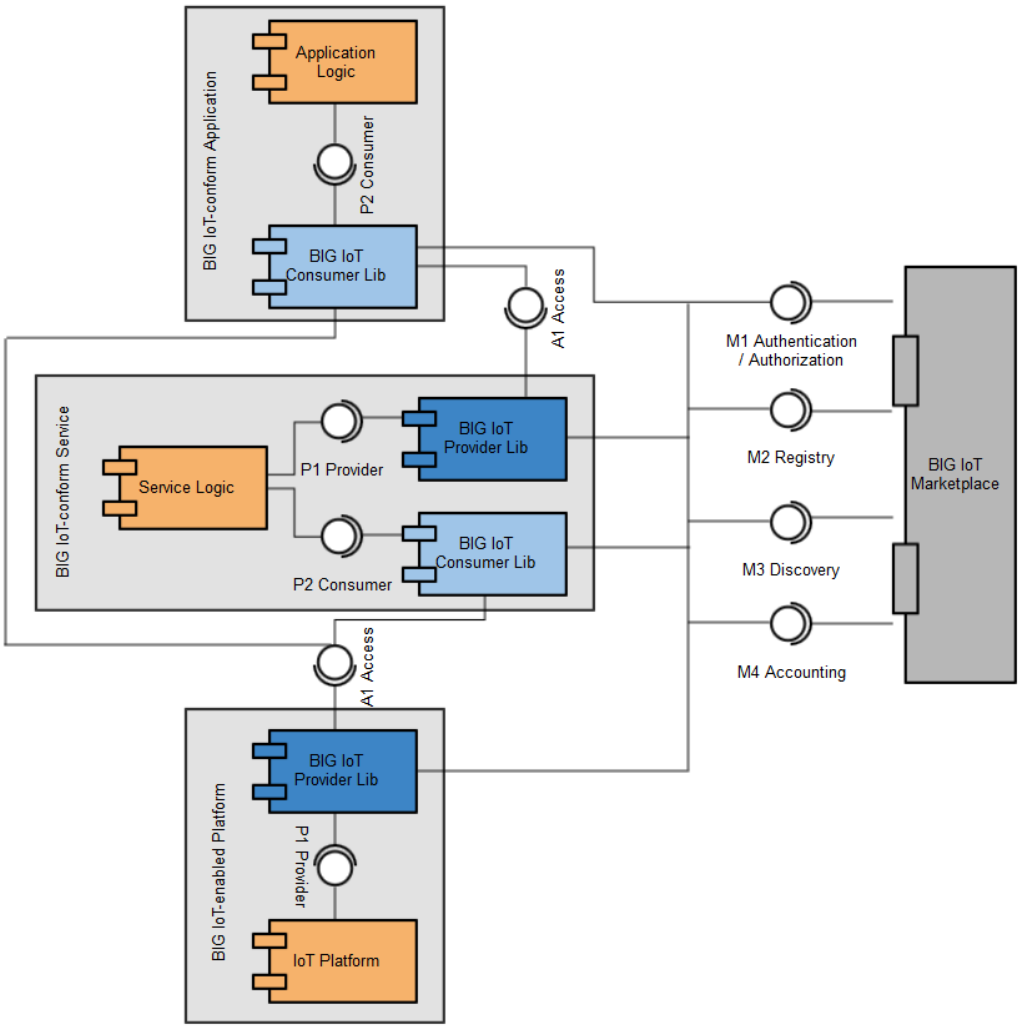

Figure 9: BIG IoT Architecture Overview

The SEMIoTICS project adopts this architecture and implements by-design cross-domain operation and interaction and enables the interplay with all layers. The overall framework is depicted in Figure 10. In addition, SEMIoTICS proposes the SPDI pattern approach. By defining pattern for IoT component interaction, the aspects security, privacy, dependability, and interoperability (SPDI) are monitored and automatically checked for violation.

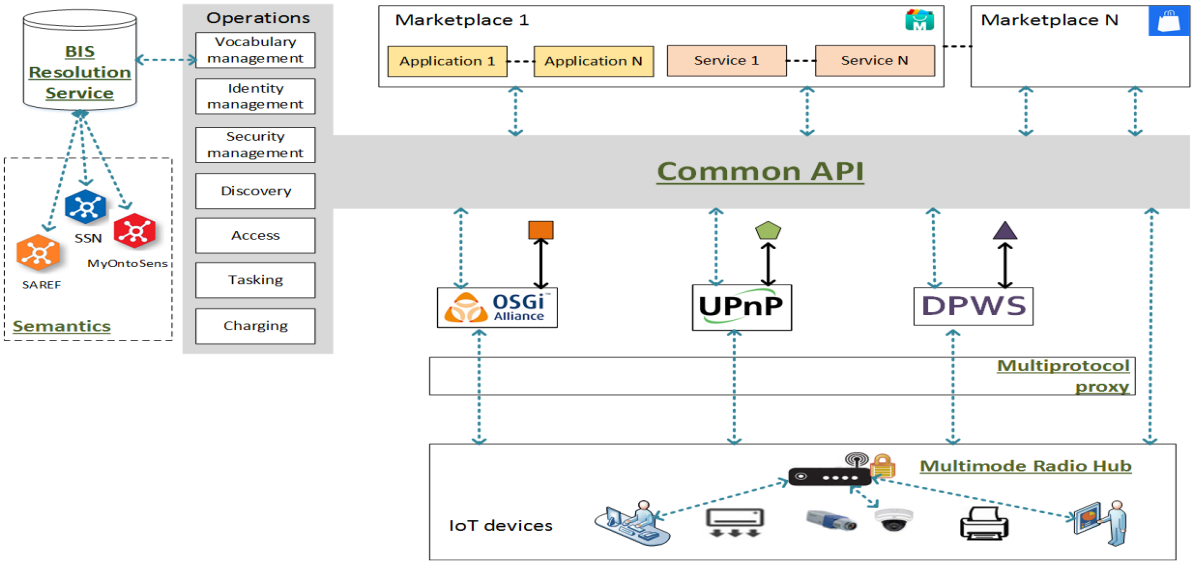

Figure 10: SEMIoTICS interoperability framework (Source: [51])

6.10.2 oneM2M: AUTOPILOT IoT platform Interoperability solution

The European Commission's Horizon 2020 AUTOPILOT (Automated Driving Progressed by Internet of Things) project focuses on creating a connected IoT ecosystem for automated vehicles.

This section provides a brief introduction of the IoT platform interoperability challenges and their solutions proposed in the AUTOPILOT project. It is based on [52] and [53].

The AUTOPILOT IoT architecture [53] is shown in Figure 11. It includes devices, gateways and in-vehicle and road-side IoT platforms exchange information with several distributed IoT platforms, which may be deployed at different levels. The AUTOPILOT project distinguishes the following two types of IoT platforms:

- **Proprietary/Private IoT Platforms:** used by some applications, organisations and services to exchange specific data with specific devices or vehicles. Such platforms that are used in the AUTOPILOT project are: Watson IoT Platform™, FIWARE and Huawei Ocean Connect.
- **oneM2M Interoperable Platforms:** considered to be the central IoT platform that acts as a hub which interconnects the proprietary/private IoT platforms (and possibly devices and services) and allows them to exchange information. This interoperability platform is based on the oneM2M machine to machine standard, which is adopted

by the project as the standard for interoperability. In AUTOPILOT the Sensinov oneM2M-based platform is used.

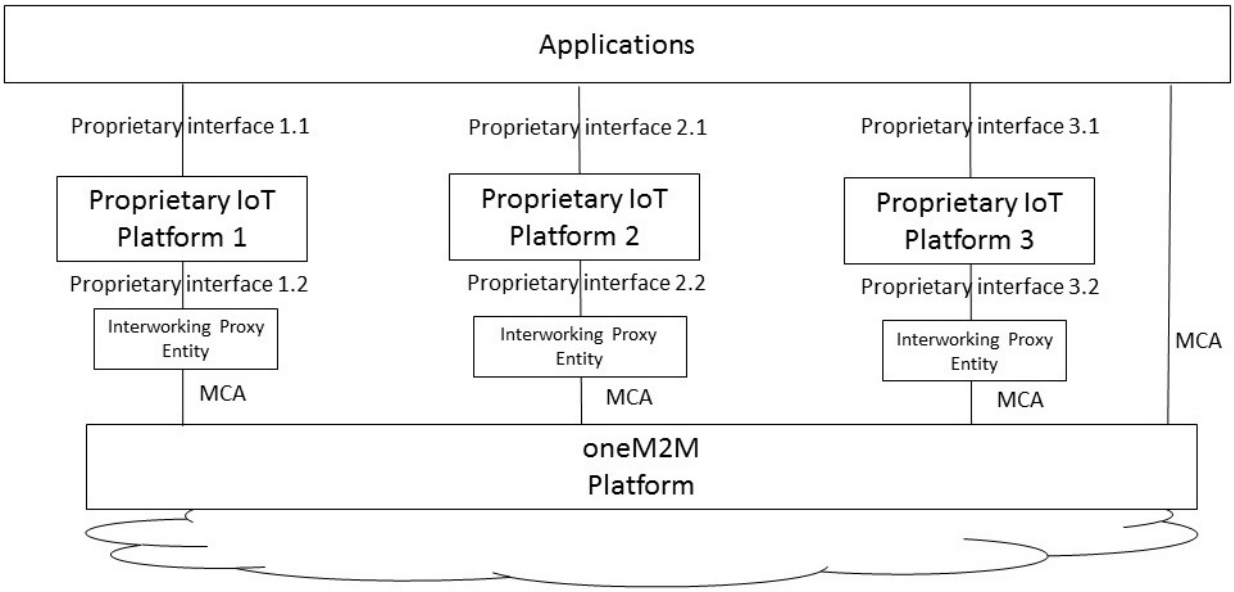

Figure 11: AUTOPILOT Federated IoT Architecture, based on [53]

The proprietary/private IoT platforms are connected to the oneM2M interoperability platform through oneM2M Interworking Proxy Entities (IPEs). Each proprietary/private IoT platform may configure the IPE to share selected data types, relevant to AD (Autonomous Driving) vehicles and applications, with the oneM2M interoperability platform. The goal of this process is that such data may then become accessible and may be shared by all the connected proprietary/private IoT platforms through the oneM2M interoperability platform.

Support for IoT Platform Interoperability

Interoperability in AUTOPILOT is achieved based on the following three concepts:

- **oneM2M IoT Standards:** Proprietary/private IoT platforms are interconnected through a standard oneM2M interoperability platform and oneM2M interworking gateways. By adopting the oneM2M standards, AUTOPILOT aims to facilitate interoperability between the various IoT platforms, sensors, and services of the architecture by using:
    - oneM2M interoperability platform to act as a central hub connecting the various proprietary IoT platforms, allowing them to exchange data and information through standard oneM2M protocols and APIs.
    - Interworking Proxy Entity (IPE) that is a specialized oneM2M AE (Application Entity) that allows the oneM2M system to interact with any non-oneM2M system, in a seamless way, through the Mca interface, see [54]. It has the

capability to remap a specific data model to oneM2M resources and maintain bidirectional communication with the non-oneM2M system.

- **IoT Data Models:** by using IoT data required to be exchanged across the IoT platforms, based, whenever possible, on existing data models and specifications (such as DATEX II for exchanging car park availability and traffic data, and SENSORIS for sharing vehicle location and object detection data). The AUTOPILOT IoT data models cover the following packages:
    - Vehicle location and detection messages, based on SENSORIS,
    - Event and object detection messages to be consumed by AD vehicles based on SENSORIS and DATEX II,
    - Traffic situations, based on DATEX II,
    - Parking availability information, based on the DATEX II parking extension,
    - Messages specific to automated valet parking, car sharing, rebalancing, and platooning.
- **Standardised Ontologies:** Semantic interoperability is supported by semantically standardising IoT data field values (e.g. hazard types, vulnerable road user types, detected object types, etc.) using ontologies.

Conclusion:

Interoperable automated driving platforms are needed for any go-to-market strategy linked with automated driving and all its complex sensor hardware. Given the many actors involved in automated driving, it becomes clear, that it is necessary to support as many different IoT platforms and sensors as possible. However, the main gap is the missing interoperability support between these IoT platforms. The H2020 AUTOPILOT project proposed an approach to solve the IoT Platform Interoperability gap, based on the following three concepts:

- oneM2M IoT Standards by using (1) oneM2M interoperability platform and (2) Interworking Proxy Entity (IPE);
- IoT Data Models;
- Standardised Ontologies.

6.10.3 Mining and construction sector

The construction and mining industry predominantly suffer from one hurdle – **the fragmentation of the standardization landscape**. The overall level of automation and digitalization is vastly different between the construction and mining sector, because of the dominance of proprietary solutions offered by a few large companies. "One brand fleet" (all machines from a single manufacturer) are much more common in mining applications than in the construction industry, where "mixed fleet" (machines from various manufacturers) are the norm. This has to do with the average length of a single operation and how contractors buy machines to get work done. While – in mining – an entire fleet is bought during mine set-up and used until it is scrap, construction equipment is typically relocated between different

sites during its useful life multiple times, typically across country boarders as used machines at one point.

Therefore, it is easy to find a mine site with a high level of automation, where, on the other hand, one would have to conduct a long (and maybe unsuccessful) search to find anything comparable in the construction sector. There are some solutions available to integrate foreign-brand machines into existing one-brand fleets in the form of very specialized aftermarket kits – for autonomy (rare) and for data collection / telematics (more common). But – to be clear – there are no standards to allow easy interoperability at this point in time, neither for sophisticated autonomy solutions, nor for the comparably simpler machine data collection and telematics. The mining and the construction sector are both running behind the agricultural sector when it comes to matters of interoperability. In mining, the customer pull is not as urging – in construction, the demand for proper interoperability is growing but currently not addressed properly.

The most global attempt to start resolving this issue is done by ISO (International Standardization Organization) with the ISO 15143-x series:

- ISO 15143-1 (2010): Earth-moving machinery and mobile road construction machinery - Worksite data exchange - Part 1: System architecture
- ISO 15143-2 (2010): Earth-moving machinery and mobile road construction machinery - Worksite data exchange - Part 2: Data dictionary
- ISO 15143-3 (2018): Earth-moving machinery and mobile road construction machinery - Worksite data exchange - Part 3: Telematics data

Part 3: "Telematics data" is currently revised by the Technical Committee ISO/TC 127/SC 3 "Machine characteristics, electrical and electronic systems, operation and maintenance".

There are also complementary efforts on European and national level, like VDMA's (Verband Deutscher Maschinen- und Anlagenbau) "Machines in Construction 4.0" or CECE's (Committee for European Construction Equipment) Working Group for Road Equipment, which tend to have a limited scope, but aim to contribute to the work of the ISO Technical Committee. Neither VDMA nor CECE is an SDO (Standardization Development Organization) – they perceive their projects as pre-standardization work to be fed into "regular" standardization later. VDMA also develops OPC UA (Open Platform Communications Unified Architecture) companion specifications together with their member companies in certain industry branches, like mining to introduce interoperability in this sector as well.

6.11 Device certification

Short description: Certification mechanisms defining "classes of devices" and ensuring the quality of the devices and the data they handle.
Domain: Device-sensor technology
Keywords: Quality, EU Directives, Harmonised standards, Data quality, conformity

Possible approaches identified to resolve this gap:

Certification has been traditionally considered as a key process for the assessment of the management, operational, and technical security controls in an information system [79].

In general, there are three possible levels of certification for devices and systems, as described in IEEE Conformity Assessment Program presentation [92]:

- Declaration of conformity by the device manufacturer
- Compliance with requirements from the device user or customer, for example a system integrator
- Certification by an independent organisation or dedicated laboratory.

IoT is considered as a core enabler of the current hyper-connectivity trend, in which certification is crucial to ensure trust in the development of new digital solutions. Beyond limitations of well-known certification schemes (e.g., Common Criteria [89]) such as cost and complexity, the massive integration of physical devices to the Internet brings new challenges to the certification process of IoT devices [80]:

- The IoT landscape is composed by heterogeneous devices, which are based on different underlying technologies and protocols. This aspect is in conflict with the need to provide objective security assessments, which should be independent on the underlying mechanisms.
- IoT devices will often require software updates/patches to react against potential security attacks. These circumstances could provoke the need to recertify the device, in order to reflect the changes in the security level. Consequently, a lightweight and cost-effective certification process is crucial to be considered in IoT environments
- Related to the previous point, maintaining an IoT device's security level up-to-date represents a challenge because of the potential changes (e.g., the discovery of a new vulnerability) through its lifecycle. For that reason, the use of blockchain could mitigate this issue by maintaining the cybersecurity information in a publicly accessible ledger [81].
- While the National Vulnerability Database (NVD) is considered in the United States to store vulnerabilities of ICT systems, there is a lack of such effort in the EU. It would enable different stakeholders (including manufacturer and end users) to share threats/vulnerabilities information among countries. Such vulnerabilities could represent the starting point of a certification process for IoT devices.
- As part of the certification process, the identification of consistent security metrics is of paramount importance to ensure objective results of the process. Such metrics (e.g., likelihood or impact) could be more difficult to be measured in the IoT context, due to scale, heterogeneity and dependencies among different devices composing a certain system.
- Indeed, a certain system could be composed by different IoT devices, which in turn, could be formed by or connected to several components with different certification

requirements. For that purpose, there is a need to define suitable approaches for *composed certification*, in order to reflect the dependencies among different components or devices composing a single system to be certified.
- Among the different stakeholders, end-users should be provided with a simple a clear representation of the certification of a certain device. Toward this end, different approaches (e.g., radar diagrams as considered by [79]) could be proposed.
- An additional aspect is the need to consider the context where the IoT device will operate. It should be noted that a certain device could be used in different scenarios (e.g., eHealth, smart homes) with different cybersecurity and privacy requirements. Indeed, this context could not be known when the device is manufactured, so such requirements could be only considered when the device is deployed in a certain environment.

Certification may apply to very different features of an IoT device: safety, security / privacy, data quality, semantics and most often its specified requirements to adhere to specific standards and regulations when available. Certification delivers trust in the devices to which they apply.

- Standards Requirements certification: Very often, industrial alliances prepare test suite specifications to promote their technology and a specific standard they promote on the market. They provide specifications for testing, certification and other related elements of conformity assessment, and ensure that the products, services or systems implemented according to the initial standards meet the standards' requirements. Examples of such alliances are EnOcean Alliance (EnOcean Equipment Profiles, see https://www.enocean-alliance.org/en/enocean_standard), Wi-Fi (Wi-Fi Test Suite, see http://www.wi-fi.org/certification/wi-fi-test-suite), Bluetooth (http://www.bluetooth.com), IPv6 Forum and the IPv6 Ready Logo Program (https://www.ipv6ready.org/), OPC UA Semantic Validation (introduced in section 6.2), etc.

- Harmonised European standards: There are market conditions that need to be fulfilled to get CE marking or USA compliance (FCC), showing that the products delivered are fulfilling the local regulations. In Europe, harmonised standards are a specific type of standards, developed by the European Standardisation Organisations (ETSI, CEN and CENELEC) in response to standardisation requests ('Mandates') from the European Commission for the application of Union harmonised legislation. The references of harmonized standards are published in the Official Journal of the European Union (OJEU); it is a precondition for legal validity of the harmonized standards and references to them, including the 'presumption of conformity' to the requirements set out in the corresponding legislation [42]. Adherence to harmonized standards carries with it the presumption of conformity with essential requirements. However, implementation of these harmonized standards remains voluntary: manufacturers, other economic operators and conformity assessment bodies are free to choose other technical solutions, but then need to demonstrate compliance with

the mandatory essential requirements. Examples of these standards are standards developed to comply with the Machinery Directive (Directive 2006/42/EC [66]) targeting safety and health of workers using the machines (this Directive applies to machinery, interchangeable equipment, safety components, lifting accessories, chains, ropes and webbing, removable mechanical transmission devices and partly completed machinery as defined in article 2 of the Directive.) or the Radio Equipment Directive (RED, Directive 2014/53/EU [67]) setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. The list of harmonised standards developed under the RED can be found at https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/red_en.

Example and lessons learnt: The MONICA LSP Project.

This project (ending March 28, 2020) is studying wearable IoT devices during (large scale) pilot tests of up to 10.000 active devices (in the shape of a wristband for each concert guest) aimed at monitoring the behaviour/movements of the large audience crowd at outdoor events, such as rock concerts (see also section 4.4).

Also, the security staff of the event is carrying a wearable (but more advanced) IoT based Tracking device, such that the event control room can have an exact screen view of the position of each security officer, should a dangerous panic be detected in the audience crowd.

These two IoT devices (both classified as Short-Range Devices (SRD)) are newly developed (ß-devices), and as such not yet carrying the CE-mark. They are both operating in the license exempt 800 MHz non-specific spectrum (863.000 – 870.000 MHz). The crowd wristband is built to comply with ETSI EN 300 220-2 [78] and the staff tracker to comply with ETSI EN 300 220-1 [77] (Technical characteristics and test methods)

Operating non-certified radio devices legally, even during a research pilot test, is not trivial. However we learned from discussions with the National Regulatory Authority (NRA) of one of the Member States, that if non-certified RF devices are to be demonstrated at the event area, one may apply Article 9 and 9.1 of the RED and define the event area as an exhibition/electronic fair in the meaning of RED Article 9 and ensure that the event area is duly gated, such that non-certified devices cannot be brought outside the gates and circulate amongst the general public with the possible interference to other RF services as a possible result. Also, the Responsible Project must ensure to clearly mark the devices: "Engineering Sample – Not for Sale" or similar, in agreement with the NRA of the country in question.

- Security / privacy certification: In March 2019, the Cybersecurity Act [65]was adopted

at EU level. It establishes an EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately intends to improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services. The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. It will attest that ICT products and services which have been certified in accordance with this scheme comply with specified requirements. In particular, each European scheme should specify: a) the categories of products and services covered, b) the cybersecurity requirements, for example by reference to standards or technical specifications, c) the type of evaluation (e.g. self-assessment or third-party evaluation), and d) the intended level of assurance (e.g. basic, substantial and/or high).
In addition to the Cybersecurity Act, certification aspects are being considered by other institutions at EU level. In this direction, the European Cyber Security Organization (ECSO) meta-scheme [79] represents an ongoing initiative to define an approach to embrace different cybersecurity certification schemes. This effort is part of a specific working group (WG1: Standardization, certification, labelling, and supply chain management).

- Data quality and homologation: The certification of data quality is an important topic, as the IoT uses sensor data to make critical decisions leveraging AI and real-time analytics, such as closing oil and gas pipes, stopping cars or sending alerts. The accuracy and quality of these data, used by the AI learning algorithms, influence the decisions of the IoT applications, as described in the AUTOPILOT project D5.4 [68]. In safety-related and eHealth applications, reliable data are crucial. The use and processing of data from reliable sources are an important element to maintain confidence and trust in the AI technology and its mechanisms. An IEEE project, IEEE P2510™ (Standard for Establishing Quality of Data Sensor Parameters in the Internet of Things Environment) [93], has been established in June 2017 to define quality measures, controls, and definitions for sensor data used in IoT environments across a multitude of verticals including power and energy, oil and gas, environmental quality, healthcare and consumer electronics. This standard is under draft approval.

- Another relevant EU initiative was the H2020 ARMOUR project (https://www.armour-project.eu), which dealt with the certification aspects of IoT devices through an automated testing methodology. Indeed, as already mentioned, a certification process should be cost-effective to cope with potential changes in a certain IoT deployment [80]. For that reason, the use of an automated testing approach could help to make the overall certification process more suitable for IoT scenarios

6.12 Data management

Short description: Data rights management: ownership, storage, sharing, selling, liability, etc.
Domain: Security / Privacy

Keywords: Data management, GDPR, data privacy, personal identifying information (PII), FAIR principles

Possible approaches identified to resolve this gap:

- Blockchain and Distributed Ledger Technologies
- ML/AI algorithms for data management
- Data anonymization/aggregation technologies
- GDPR and FAIR management policies
- Data Management Plans and related data processing

Privacy was studied by ETSI STF547 in TR 103 591 [60].

Privacy is a concept used across different disciplines. From a legal standpoint it is the ability of an individual to be left alone, out of public view, and in control of information about oneself. One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy"). The latter relates to what is known as personal data protection under EU law.

Privacy is closely linked to security. Although, privacy and security are separate concepts in the sense, for example, that privacy can be perceived independently of security, yet, they are complementary, given that in reality security is an enabler of privacy. It can be stressed that security is a basic requirement for the effective protection of privacy.

General Data Protection Regulation (GDPR) [12] provides exclusively for the protection of personal data in EU. The GDPR became applicable on the 25 May 2018 and it is directly applicable across all EU Member States.

Although the General Data Protection Regulation (GDPR) forms a technologically neutral legal instrument and, therefore, does not make any explicit reference to IoT, Recital 78 of the GDPR emphasizes the responsibility of the series of actors involved in a supply chain without exclusively focusing on a single actor.

The GDPR defines [14] the key concepts and the role of the main actors.

The GDPR introduces a series of novelties that create an impact on how organizations and, therefore, professionals, are required to process personal data. Taking into account the target audience of this document, the discussion below maps certain new requirements to actors holding diverse roles in the supply chain. The definitions below are particularly, but not exclusively relevant for the actors mentioned below.

Data protection by design

Data protection by design refers to the concept that data protection is considered throughout the design process. Data protection by design aims at building data protection and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with data protection. This is particularly relevant for organization and professionals involved in the design process of products and systems.

In relation to this new obligation, the European Data Protection Supervisor (EDPS) [16] identifies four dimensions of data protection by design.

Data protection by design, established under Article 25 of the GDPR, could be broken down into the following set of principles:

1. No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.
2. 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.
3. De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is no longer any valid legal basis.
4. Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data.
5. Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto.

The GSMA document [15], describes a range of tools and techniques that practically support the concept of data protection by-design for big data, analytics and machine learning based services in the IoT. The document provides approaches to various topics which enhance data protection. Included in the document are case studies from a number of mobile operators, illustrating the adoption of such best-practice approaches.

Data protection by default

This is related to the importance of taking technical measures to meet the expectations of the individuals whose data are processed, not to have their data processed for other purposes than what the product and service is basically and strictly meant to do, leaving by default any further use turned off, for instance through configuration settings. This is particularly relevant for organization -and professionals – involved, for example, in the development of interfaces.

Data breach notification

The GDPR provides for the mandatory notification of a data breaches provided that certain requirements are met.

According to the GDPR personal data breach is a breach of security leading to accidental or unlawful destruction. Loss, alteration, unauthorized disclosure, access to personal data transmitted stored or processed.

IoT forms a clear example of hyper connectivity and distributed control, as such appropriate safeguards are needed to ensure that individuals' right to privacy is effectively protected. As part of IoT design, the following are some of the challenges in identifying:

- the stakeholders for whom privacy is relevant;
- who is responsible for the personal data as context is relevant (e.g. in Smart Living, Smart Home), for instance for software developers, when implementing data protection by default;
- how stakeholders need to think of privacy proactively as part of design not an afterthought.

Data Protection Impact Assessment – DPIA an art of privacy assessment is a tool to help companies identify and minimize the data protection risks of new projects. They are part of their accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach.

DPIA can address a single processing operation or a set of similar processing operations.

DPIA should be carried out prior to the processing, as early as practical in the design of the processing operation.

In conclusion, there are no obvious missing gaps in standardisation, but there is a significant gap in application of privacy protection capability in general, and of standards based of privacy protection capability specifically. This was the same conclusion that was deduced by a report by ETSI in ETSI TR 103 370 [17]. The report indicates that gaps are in the appropriate application of the privacy principle which can be resolved by proper code of conduct and certification. One of the guidance to code of conduct is for technical system to consider privacy by default and by design.

The effective protection of privacy and (personal) data protection, also, within the IoT environment requires appropriate technical and organizational measures. The implementation, monitoring and optimisation of those measures are to be planned and taken both in advance as well as during the related data collecting, data processing and data

management pertaining to the life cycle of the respective IoT ecosystem. The GDPR further requires organizations not only to be able to ensure, but also to deliver documented and continuous proof of appropriate levels of compliance – defined in the GDPR as: accountability –, on a continuous basis.

Blockchain and Distributed Ledger Technologies

In recent years, Distributed Ledger Technologies (DLTs) and Blockchains have become a disruptive technology to realize a decentralized data sharing platform to be considered in many everyday scenarios. Because of its recent emergence, there is a need to define standardized approaches to foster the deployment of large-scale blockchain deployments, such as in the context of IoT.

However, several practical issues have been reported specially because of the cost associated to the process to add transactions in a certain blockchain. Moreover, in the case of public blockchains, the access model provides a certain degree of anonymity to the users that can be exploited by potential attackers. Such aspects are being considered by several researches and organizations. In the scope of IoT, the IEEE P2418 initiative aims to build a generic framework of blockchain to be used in IoT by considering scalability, security and privacy challenges (P2418.1, https://standards.ieee.org/project/2418_1.html). More focused on specific use cases, P2418.3 and P2418.4 (resp. https://standards.ieee.org/project/2418_3.html and https://standards.ieee.org/project/2418_4.html) are intended to define a framework to the use of Distributed Ledger Technologies (DLT) in the scope of agriculture and autonomous vehicles. In addition, the ITU-T FG DLT (https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx) represents another effort to identify and analyse the current landscape of DLTs approaches, in order to propose guidelines for related standardization work in other ITU-T Study Groups. An additional initiative is represented by the Blockchain Community Group (https://www.w3.org/community/blockchain/).

In the EU, the increasing interest on blockchain has motivated the establishment of the EU Blockchain Observatory and Forum (https://www.eublockchainforum.eu/), which intends to analyse the developments of the technology in order to identity potential activities in different use cases, as well as potential aspects associated to the development of legal instruments to foster the deployment of Blockchain. Indeed, this organization published in 2018 the report "Blockchain and the GDPR" [90], in which different barriers are identified for a large-scale deployment. As an example, the immutable nature of the Blockchain could represent an issue to comply with GDPR's Article 16 ("Right to rectification") and Article 17 ("Right to erasure ('right to be forgotten')"), especially in the case of personal data that are directly stored in the ledger. These aspects could be exacerbated in the case of IoT devices, which could act on behalf of users by sharing data without an explicit consent.

Another aspect related to data management is the need to provide interoperable approaches to deal with a huge amount of data coming from different sources. For that reason, in the blockchain context, in recent years, the use of *interledger* approaches is emerging as a potential solution to deal with performance, scalability and privacy aspects of a single blockchain vision [81]. In that way, different organizations (or even countries) could manage their own information in a blockchain, which is connected to other blockchains to create a cross-border platform for data sharing.

6.13 (Cyber-)Security

Short description: Risk Management Framework and Methodology
Domain: Security / Privacy
Keywords: cyber-security, attacks, countermeasures, risk analysis, threat, vulnerability confidentiality, integrity, encryption, authentication, access control, cryptography.

Possible approaches identified to resolve this gap:

(Cyber-)Security was studied by ETSI STF547 in TR 103 533 [46].

The purpose of security technologies is multi-fold:

- Confidentiality: Information shared by Party A with Party B is only visible to Party B and Party A. If Party C can access the information, it cannot ascertain the meaning of the content. Confidentiality is primarily achieved using cryptographic encryption (from TS 102 165-2 [19]).
- Integrity: Information shared by Party A with Party B can be proven by Party A not to have been manipulated by a 3rd party (e.g., Party C). Party B can verify this is the case. Proof and verification of document integrity is primarily achieved using cryptographic hash functions which have specific characteristics (from TS 102 165-2 [19]).
- Availability: This addresses the aim of ensuring that an authorized party (e.g., Party A) is able to access services or information when needed. In other words, that Party A has access only to those assets it is allowed to access and that they are available to Party A when legitimately demanded, and that an adversary, Party C, does not have access. The technologies that address this include Identity Management, Authentication and Access Control, in addition considerations in the availability domain include reliability and resilience which, whilst not strictly addressed by security technology, impact on availability (from TS 102 165-2 [19]).

One of the many characteristics of IoT is that the number of communicating entities is very large and the number of possible relationships per device is larger than, say, with cellular telecommunication.

There are a number of complexities in IoT that arise from the nature and number of both devices and connections. The most obvious of these is key management

The general purpose of security technology is to give confidence to the stakeholder that the risk of cyber-attacks, or any other attack on the assets of a system, are mitigated.

In an environment of Consumer IoT where devices can be purchased and installed by the consumer it is unlikely that the vendor, or manufacturer, is aware in detail of the way in which the IoT device is to be used. For such environments the "by default" capabilities and data minimisation approaches that are widely recommended cannot be assured to be sufficient.

By contrast in an industrial IoT environment devices may be subject to strict control before being installed and operated, at least this would certainly be expected of any organisation that has followed the recommendations of the ISO 27000 series of controls, or adopted the controls recommended in ETSI TR 103 305 [20]

As identified in the introduction of ETSI TR 103 306 [21] cyber security consists of a continuing cycle of structured actions to:

- Identify
  - Requires gaining an understanding of the system that allows the owner to state the risks to systems, assets, data, and capabilities
  - Requires understanding of the nature of attacks and the nature of change on the system
- Prevent (also termed as protect)
  - The application of countermeasures
  - At design time, at update time
- Prepare (also termed as detect)
  - Being able to react – measuring how the security of the system is performing
- Respond
  - Implement resilience and restoration of impaired capabilities resulting in an update of the system and return to the start of the cycle

All of these activities rely on the trusted, timely sharing of related structured information.

As also identified in TR 103 306 [21] effective cross sector security requires the sharing of knowledge. This has been summarised as a requirement for interoperability across each of the syntactic, semantic, mechanical, and process domains.

For IoT, there are many unknowns that have to be resolved prior to overall security being achieved. Many current standards exist for the concepts and functions to allow the problems to be resolved.

Methods for performing a risk analysis and identifying the assets of any system are described in the following core documents from ETSI:

- TS 102 165-1: CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) [22]
- TR 103 305-x: CYBER; Critical Security Controls for Effective Cyber Defence (multi-part standard) [23]

The best practices that are available on the market from a large number of standards bodies, vendors, government agencies, industrial groupings, are very similar in their intent but often understate the difficulty in determining what has to be secured and how it is to be secured. Rather there is an assumption of knowledge of the means to apply the guidelines. A danger that is not expressed in any of the guidelines is the consequence of incomplete implementation, or of incomplete knowledge. On the one hand good practice is followed, by enforcing authentication, but is then undermined by not enforcing uniqueness of the credentials that allow it to be effective.

Whilst guidelines are effective, their applicability are only as effective as the knowledge of the designer implementing them. The conclusion of this section is therefore for all designers, developers, implementers and users, to be aware of the guidelines but to recognise that without expert knowledge and care they may act to give a false sense of security.

6.14 Green technologies

Short description: Green technologies
Domain: IoT Architecture
Keywords: Sustainability, energy consumption, rare minerals and raw materials provisioning,

Possible approaches identified to resolve this gap:

In the IoT domain the impact of green technologies would be two-fold:

- using IoT technologies to improve the environment impact of other domains. This topic covers for example smart homes and buildings, pollution measurements or waste reduction in smart cities, soil moisture and weather monitoring in smart agriculture, or the smart energy domain aiming to meter and optimize overall energy consumption. There are many stakeholders' initiatives, such as the call for action that resulted from the ITU-T green standards week [74]. Standards are defined for smart metering in the domain of Utilities. For example, IEC 62056 family of standards [76] specifies "electricity metering data exchanges".
- improving the energy footprint of IoT based systems, including its use and energy consumption, the disposal or refurbishing of obsolete devices, the design and manufacturing of energy and environment-friendly new devices.

More globally in the ICT domain, ITU-T Study Group 5 has established a new Focus Group on "Environmental Efficiency for Artificial Intelligence and other Emerging Technologies"

(FG-AI4EE) [75]. Its objective is to support the development of technical reports and technical specifications to address the environmental efficiency, as well as water and energy consumption of emerging technologies, and provide guidance to stakeholders on how to operate these technologies in a more environmentally efficient manner to meet the 2030 Agenda for Sustainable Development and its 17 Sustainable Development Goals. The first meeting is planned on December 2019.

6.15 Ethics and trustworthiness

Short description: Ethics and trustworthiness
Domain: Service and applications / Security / Privacy
Keywords: Trustworthiness, IoT Ethics and Ethical concerns,

Possible approaches identified to resolve this gap:

Ethics is currently a topic in Artificial Intelligence standardization, but not really in IoT standardization. It is a general consensus in AI standardization that we will not standardize ethics or ethical values. Ethical values are defined by the societal and cultural environment and may change over time. It doesn't make sense to standardize these values and they are not a technology specific issue.

What is important is that technologies may enable and provide new applications that may impact the ethical values of a society. A negative impact on these values will decrease the trust people have in the technology and hamper its acceptance by the society. Trustworthiness, the degree to which users and all stakeholders have confidence that a product or system will behave as intended, is therefore an issue for each technology.

IoT trustworthiness aspects are mainly related to privacy, security and to a lesser degree safety. It is therefore proposed to focus this section on Trustworthiness.

6.15.1 Ethics

As the use and impact of IoT and autonomous and intelligent systems (A/IS) [36] become pervasive, we need to establish societal and policy guidelines in order for such systems to remain human-centric, serving humanity's values and ethical principles. These IoT systems must be developed and should operate in a way that is beneficial to the users and their environment, beyond simply reaching functional goals and addressing technical problems. This approach will foster the heightened level of trust between people and used IoT technology that is needed for its fruitful use in our daily lives.

Typically, IoT systems are specifically designed to reduce the necessity for human intervention in our day-to-day lives. In doing so, these new systems are also raising concerns about their impact on individuals and societies. IoT systems/Machines do not, in terms of classical autonomy, comprehend the moral or legal rules they follow. They move according to their programming, following rules that are designed by humans. This requires ethical and

values-based design, development, and implementation of IoT systems, that should be guided by the following General Principles:

- Human Rights: IoT shall be created and operated to respect, promote, and protect internationally recognized human rights.
- Well-being: IoT creators shall adopt increased human well-being as a primary success
- Data Privacy: IoT creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity.
- Effectiveness: IoT shall provide evidence of the effectiveness and fitness for purpose.
- Transparency: The basis of a particular IoT decision should always be discoverable.
- Accountability: IoT needs to provide an unambiguous rationale for all decisions made.
- Awareness of Misuse: IoT creators shall guard against all potential misuses and risks of IoT in operation.
- Competence: IoT creators shall specify and IoT operators shall adhere to the knowledge and skill required for safe and effective operation.

Providing ethics education and security awareness that sensitizes society to the potential risks of misuse of IoT. For example, provide "data privacy warnings" that some smart devices will collect their users' personal data. Applied to IoT, an interesting hypothesis one can make for humans and their interests in tandem with non-human entities about consequences of one's decisions and actions. In the context of IoT, one consideration is to wonder if developers are acting with the best

interests of humanity and human dignity in mind. This could possibly be extended to IoT whereby they are assisting humanity as an instrument of action that has an impact on decision-making capabilities, despite being based on neural machine learning or set protocols. The ethical part of IoT shall be that it provides a model for iterative learning and growth, and moral value informed by context and practice, not just as compliance with a given, static ruleset.

IEEE P7000™, "IEEE Standards Project for Model Process for Addressing Ethical Concerns During System Design" will provide engineers and technologists with an implementable process aligning innovation management processes, IT system design approaches, and software engineering methods to minimize ethical risk for their organizations, stakeholders and end users.

The main functionality of IoT systems is to transfer very large sensitive and private data. There are many ethical challenges that need to be taken into consideration by individuals and companies that use this technology. Amongst the challenges is the user awareness of attack risks [37] .

6.15.2 General IoT Ethics

IoT technologies solve many real-life problems but they create serious ethical concerns and legal challenges related to:

- Protection of privacy
- Data security
- Data usability
- Data user experience
- Trust
- Safety, etc.

6.15.2.1 State of the art IoT Ethics: Informed consent (based on [38])

This case demonstrates how the IoT intersects with existing moral concepts like informed consent: a device gathers personal information through sensors and communicates that information to some receiver, all without the user necessarily being actively involved. Informed consent has been extended from medicine to digital contexts, starting in the early 2000s; This extension has translated from the patient or research subject to the digital consumer.

- The principal application is vis-à-vis personal data, often as would be collected by or shared with a third party, such as a website or smartphone application [39].
- The applications to the IoT are initially straightforward insofar as any IoT application will similarly seek informed consent from the consumer.
- There needs to be a standard that establishes informed consent for the acquisition, retention, and sharing of personal data

6.15.2.2 State of the art IoT Ethics: Privacy (based on [38])

The intersection between privacy to the IoT starts with the observation that devices connected to the IoT collect vast amounts of user data and that data can be analyzed, shared, and so on [40].

- Simply encrypting the information is not likely to solve all the problems
- In fully-integrated smart homes area, the smart home are routinely communicating information back to manufacturers, not all of which is even encrypted [41]. Hence, not only could hackers potentially access this information, but the manufacturers themselves would start to have more information about their customer's habits, and the personal information that is derived from their habits can reveal deeply intimate aspects of a person's life like being pregnant.
- The European Union's GDPR just went into effect in mid-2018 and makes substantial strides toward increased data protection. Courts have also started to recognize rights to digital privacy.

6.15.2.3 State of the art IoT Ethics: Physical safety (based on [38])

The main difference between the IoT and the "traditional internet" is that the IoT has the potential to be active in the physical realm. In addition to sensors and communication, many elements of the IoT include actuators; (i.e. sensors: one in the smartphone and one in the door's locking mechanism, communicators: smartphone and the door's locking mechanism confirming handshakes, a smart driverless vehicle that steers, accelerates, brakes). So, any components with actuators that pose a physical risk must take those risks seriously. Key mechanisms for these issues:

- The government oversight and enforcement of minimum safety standards
- The enforcement mechanisms—particularly ones that seek to apply civil or criminal liability as a result of physical harms—generally need to be able to correctly identify the responsible parties

6.15.2.4 State of the art IoT Ethics: Trust (based on [38])

Trust is directly related to the above ethically relevant features. For example:

- if we are confident that privacy will be respected, then we have established trust
- if informed consent is respected, then we will know how our data is being used or what the risks of some IoT-enabled device are, thus furthering trust.
- In information security were compromised, then we would retain trust by expecting we be notified of breaches and that they be expeditiously patched.

6.15.3 Challenges (based on [37])

- No Way Out: The client is totally immersed in the IoT network. There is a high dependability from the user on the IoT network specially in healthcare applications.
- Miniaturization: Nowadays, PC's are diminishing in size, and new IoT devices will be in the Nano size and transparent. Thus, it will be difficult to maintain any sort of audit, quality control or traffic control, due to the Nano size and huge number of devices.
- IoT Globalization: IoT cannot be localized, especially in medical applications where the service can be offered overseas. It is a challenge for nations to deal with this new concept, because may be almost every whisper in a country is collected and sent to the country that is providing the service.
- New Business Models: Using IoT will enforce companies that offer medical services to create new business models that take into consideration the available types of data and the high stream. Virtual hospitals will take place. Therefore, the service will be offered remotely.
- Vagueness: The differentiation between physical and virtual devices and human being will be more difficult due to the ease of transformation from one category to another.
- Identification Problems: There are billions of IoT devices, each needs a unique identification in order to log in the network. Identification problems will rise up with other identity proof problems.

- Ultra-Availability: Billions of devices will be always on 24/7. This will result in massive amount of data (big data), which will be more exposed to malicious attacks.
- Autonomous and Unexpected Behaviour: Human beings will be part of IoT networks together with other devices and sensors, a hybrid network will be the result. Interconnected devices may interfere suddenly in human actions. The continuous development of IoT will lead to ambiguous behaviours not completely understandable by the users.
- Governance: Due to the considerable number of routers, switches and information, IoT control and governance will be challenging. The data exchanges will be faster and less expensive, difficult to be controlled or monitored. The accountability is an additional challenge to tackle.

6.15.4 Trustworthiness

Trustworthiness is the degree to which users and all stakeholders have confidence that a product or system will behave as intended. Trustworthiness is a major issue for the acceptance of a technology by the society especially if applications enabled by a new technology may have negative impact on ethical values of the society. Standards can support adherence to ethical principles, while supporting a with range of ethical value systems.

From an IoT point of view the following areas are of major importance when considering trustworthiness:

- Privacy; due to the fast amount of personal and related data that might be gathered by IoT applications
- Information security; due to the possibility to have access IoT devices from basically everywhere in the world in case they are connected to the Internet
- Safety; in case physical equipment and processes, which can lead to harm to humans, property and the environment, are controlled via IoT

It should be noted that these topics have to be evaluated in a holistic view for a system taking its specific functionality/use case, the environment and all deployed technologies into account. IoT may introduce specific issues, vulnerabilities and threads related to a topic.

The topics above are already specifically addressed in other clauses of this document.

ISO/IEC JTC SC41 has work items on a Trustworthiness Framework and Methodology for trustworthiness of IoT system/service. Specific IoT standardization gaps in Trustworthiness are therefore currently not seen.

6.16 Open Markets of Digital Services

Short description: standards needed to enable open markets of services
Domain: Service and applications
Keywords: open markets, smart contracts, terms and conditions, privacy, payments, discovery

Possible approaches identified to resolve this gap:

- Web of Things

The value of markets to suppliers and consumers is related to the size of the marketplace. Competition in open markets is an effective driver for the adoption of standards, and for companies to actively contribute to the development of standards. The Web of Things provides a basis for connecting suppliers and consumers of IoT services, decoupling applications from the underlying protocols, but further work is needed on standards in the following areas:

- Standards for suppliers and consumers to find each other and work together
- Standards for describing services, e.g. different kinds of sensors and actuators, and what they measure or control – this involves domain specific ontologies
- Standards for describing the software interfaces and data formats – this is fulfilled by the Thing Descriptions for the Web of Things
- Standards for terms and conditions for service contracts
- Standards for audit trails – this could be based upon block chains that record agreements on smart contracts, as well as a record of operations as required by those contracts
- Standards for payments – e.g. one off, subscription-based, or per-use payments
- Standards for security and for enabling trust between suppliers and consumers, including the regulatory framework and legal recourse

Only part of this is in place. There is an opportunity to learn from experience in EU projects and feed this into the standardisation process.

7 Conclusion

The initial discussions in AIOTI WG03 on (standards) gaps has led to the conclusion that it is an essential topic for the IoT community and to the decision to develop a new AIOTI WG03 Report that should include: (1) identified key gaps and (2) SDOs that needs to cooperate with in order to solve these gaps.

This led to the publication of Release 1.0 of this AIOTI Report. It was planned to be a living document subject to further regular updates in new Releases.

The present document is the Release 2.0 of this AIOTI Report. It continues the analysis of the gaps identified in Release 1.0 and provides an updated status of the standardization status on these topics. It demonstrates that if parts of these gaps have been addressed in new standardisation projects, there is still matter for improving the standards towards reliability, sustainability and interoperability of the systems, especially for topics such as green technologies, deployment and usability of the devices.

Annex I References

[1] "SmartM2M; IoT Standards landscape and future evolution", ETSI TR 103 375 (STF 505), 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[2] "SmartM2M; IoT LSP use cases and standards gaps", ETSI TR 103 376 (STF 505), 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[3] "20170303_MainIoTgaps_STF505.pptxV2", presentation by Michelle Wetterwald, 03/03/2017, available on the AIOTI web site.

[4] ECSEL Joint Undertaking (Electronic Components and Systems for European Leadership), www.ecsel.eu

[5] "Functional safety of electrical/electronic/programmable electronic safety-related systems", https://en.wikipedia.org/wiki/Safety_integrity_level

[6] "Strategy and coordination plan for IoT interoperability and standard approaches", CREATE-IoT Deliverable D06.01, 2017.

[7] ETSI STF 505 Home Page: https://portal.etsi.org/STF/stfs/STFHomePages/STF505

[8] CREATE-IoT Home Page: https://european-iot-pilots.eu/project/create-iot/

[9] CREATE-IoT D6.1 https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06_01_WP06_H2020_CREATE-IoT_Final.pdf

[10] AIOTI WG03 Reports: https://aioti.eu/aioti-wg03-reports-on-iot-standards/

[11] AIOTI WG03 HLA: https://aioti.eu/wp-content/uploads/2017/06/AIOTI-HLA-R3-June-2017.pdf

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[13] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

[14] Article 4 of the GDPR

[15] Protecting Privacy and Data in the Internet of Things: Considerations and techniques for big data, machine learning and analytics February 2019 GSMA www.gsma.com

[16] European Data Protection Supervisor: Preliminary Opinion on privacy by design, 31 May 2018

[17] ETSI TR 103 370 Practical Introductory guide to Technical Standards for Privacy

[18] Privacy in Mobile Apps: Guidance for app developers ICO

[19] ETSI TS 102 165-2: CYBER; Methods and protocols; Protocol Framework Definition; Security Counter Measures"

[20] ETSI TR 103 305-x: Critical Security Controls for Effective Cyber Defence (multi-part standard)

[21]ETSI TR 103 306: "Global Cyber Security Ecosystem"
[22]ETSI TS 102 165-1: "Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)"
[23]ETSI TR 103 305-x: Critical Security Controls for Effective Cyber Defence (multi-part standard
[24]ETSI TR 103 535: " SmartM2M; Guidelines for using semantic interoperability in the industry"
[25]oneM2M TS 0012: "oneM2M Base Ontology"
[26]oneM2M TS 0023: "Home Appliances Information Model and Mapping"
[27]oneM2M TS 0021: "oneM2M and AllJoyn Interworking"
[28]oneM2M TS 0014: "LWM2M Interworking
[29]oneM2M TS 0024: "OIC Interworking"
[30]ETSI TS 103 264: "SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping"
[31]SSN ontology, available at https://www.w3.org/TR/vocab-ssn/
[32]ETSI TR 103 537: " SmartM2M; Plugtests™ preparation on Semantic Interoperability"
[33]SF SSCC, Overview of Standards and Specifications relevant to Smart Cities (DRAFTv28: modified 20180419). See CEN/CENELEC pages https://www.cencenelec.eu/standards/Sectorsold/SmartLiving/smartcities/Pages/default.aspx and the provided document link ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/SmartLiving/City/SF-SSCC_Overview_of_Standards_for_SmartCities.pdf
[34]ETSI GS CIM 009: "Context Information Management (CIM); NGSI-LD API"
[35]ETSI GS CIM 006-MOD0: "Context Information Management (CIM); Information Model (MOD0)"
[36]https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf
[37]A. AboBakr and M. A. Azer, “IoT ethics challenges and legal issues,” in 2017 12th International Conference on Computer Engineering and Systems (ICCES), 2017, pp. 233–237.
[38]F. Allhoff and A. Henschke, “The Internet of Things: Foundational ethical issues,” Internet of Things, vol. 1–2, pp. 55–66, Sep. 2018.
[39]R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, “An agent-based framework for Informed Consent in the internet of things,” in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 789–794.
[40]R. H. Weber, “Internet of things: Privacy issues revisited,” Comput. Law Secur. Rev., vol. 31, no. 5, pp. 618–627, Oct. 2015.

[41]"New research: Most IoT devices can be hacked into botnets - TechRepublic." [Online]. Available: https://www.techrepublic.com/article/new-research-most-iot-devices-can-be-hacked-into-botnets/. [Accessed: 16-Jul-2019].

[42]Abdelkafi N., Lanting C.J.M., Thuns M., Bolla R., Rodriguez-Ascaso A., Wetterwald M., Understanding ICT Standardization: Principles and Practice, ETSI ed, November 2018. ISBN 978-3-7482-4742-5. Available at https://www.etsi.org/standardization-education.

[43]Semantic Interoperability White Paper: Semantic IoT Solutions - A Developer Perspective Editor Martin Bauer- Under publication

[44]Semantic Interoperability White Paper: Towards semantic interoperability standards based on ontologies. Editor Martin Bauer- Under publication

[45]ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms"

[46]ETSI TR 103 533:"SmartM2M; Security; Standards Landscape and best practices".

[47]https://projects.eclipse.org/proposals/eclipse-bridge.iot

[48]Bröring, A., S. Schmid, C.-K.Schindhelm, A. Khelil, S. Kaebisch, D. Kramer, D. Le Phuoc, J. Mitic, D. Anicic, E. Teniente (2017): Enabling IoT Ecosystems through Platform Interoperability. IEEE Software, 34(1), pp. 54-61.

[49]Bröring, A., A. Ziller, V. Charpenay, S. Schmid, A.S. Thuluva, D. Anicic, A. Zappa, M.P. Linares, L. Mikkelsen, C. Seidel (2018): The BIG IoT API - Semantically Enabling IoT Interoperability. IEEE Pervasive Computing, 17(4), pp. 41-51

[50]Bröring, A., A. Zappa, O. Vermesan, K. Fräing, A. Zaslavsky, R. Gonzalez-Usach, P. Szmeja, C.E. Palau, M. Jacoby, I. Podnar Zarko, S. Soursos, C. Schmitt, M. Plociennik, S. Krco, S. Georgoulas, I. Larizgoitia, N. Gligoric, R. Garcia-Castro, F. Serena, V. Oravec, R. Giaffreda, C. Kiraly (2018). Advancing IoT Platforms Interoperability. River Publishers. ISBN: 978-87-7022-005-7

[51]Hatzivasilis, G., I. Askoxylakis, G. Alexandris, D. Anicic, A. Bröring, V. Kulkarni, K. Fysarakis & G. Spanoudakis (2018): The Interoperability of Things - Interoperable solutions as an enabler for IoT and Web 3.0. 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2018), 17.-19. September 2018, Barcelona, Spain. IEEE

[52]M. Djurica, G. Romano , G. Karagiannis, Y. Lassoued, G. Solmaz, "oneM2M-Based, Open, and Interoperability IoT Platform for Connected Automated Driving", (submitted to) 13th ITS European Congress, the Netherlands, 3-6 June 2019

[53]D2.3 Report on the Implementation of the IoT Platform, EC H2020 AUTOPILOT, 2018, to be retrieved via (visited in February 2019) https://autopilot-project.eu/wp-content/uploads/sites/16/2018/10/AUTOPILOT-D2.3-Report-on-the-Implementation-of-the-IoT-Platform-v0.3.pdf

[54]"Developer guide: Interworking Proxy using SDT", oneM2M TR-0039-V-2.0.0, 12-03-2018, available via (seen in June 2019), http://www.onem2m.org/images/files/deliverables/Release2A/TR-0039-Developer_guide-SDT-based_implementation-v_2_0_0.pdf
[55]ISO 6346 "Freight containers -- Coding, identification and marking", 1995
[56]ISO2108 "Information and documentation — International Standard Book Number (ISBN)", December 2017
[57]ISO 11784 "Radio frequency identification of animals -- Code structure", 1996
[58]ISO/IEC 29161 "Information technology -- Data structure -- Unique identification for the Internet of Things", 2016
[59]IETF RFC 8141 "Uniform Resource Names (URNs)", 2017, Available at https://tools.ietf.org/html/rfc8141 [Accessed 15.12.2017]
[60]ETSI TR 103 591:"SmartM2M; Privacy study report; Standards Landscape and best practices"
[61]CHARIOT Deliverable D1.1, Classification and use guidelines of relevant standards and platforms, available at https://www.chariotproject.eu/uploadfiles/D1.1-v1.6-28.03.2019-FINAL.pdf
[62]Web of Things (WoT) Thing Description: https://w3c.github.io/wot-thing-description
[63]Bröring, A., S.K. Datta & C. Bonnet (2016): A Categorization of Discovery Technologies for the Internet of Things. Proceedings of the 6th International Conference on the Internet of Things (IoT 2016), 7.-9. November 2016, Stuttgart, Germany. ACM. pp. 131-139.
[64]Web of Things (WoT) website: http://w3c.org/WOT
[65]REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[66]DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
[67]DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[68]D5.4 IoT Policy Framework for autonomous vehicles applications, EC H2020 AUTOPILOT, 2018
[69]BBF TR-069: "CPE WAN Management Protocol", Issue 1 Amendment 5, V1.4
[70]BBF TR-131: "ACS Northbound Interface Requirements", Issue 1 Amendment 1

[71]BBF TR-369: "User Service Platform (USP)", Issue 1 Amendment 1
[72]OMA Lightweight Machine to Machine Technical Specification, Open Mobile Alliance, V1.1
[73]Open Mobile Alliance Device Management Specification, V2.0
[74]"Call to Action, The 9th Green Standards Week: Connecting Smart Sustainable Cities with the Sustainable Development Goals", available at https://www.itu.int/en/ITU-T/Workshops-and-Seminars/gsw/201910/Documents/9thGSW2019-Valencia-CalltoAction-EN.pdf
[75]https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Pages/default.aspx
[76]IEC 62056 standards: available at https://webstore.iec.ch/searchform&q=IEC%2062056
[77]ETSI EN 300 220-1: "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 1: Technical characteristics and methods of measurement", 02/2017
[78]ETSI EN 300 220-2: "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for access to radio spectrum for non specific radio equipment", 12/2018
[79]Matheu, S. N., F. Allhoff and Hernandez-Ramos, J. L., & Skarmeta, A. Henschke, "TheF. (2019). Toward a Cybersecurity Certification Framework for the Internet of Things: Foundational ethical issues," Internet of Things, vol. 1–2, pp. 55–. IEEE Security & Privacy, 17(3), 66, Sep. 2018-76
[80]Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, 64-83.
[81]Neisse, R., Hernández-Ramos, J. L., Matheu, S. N., Baldini, G., & Skarmeta, A. (2019). Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices. arXiv preprint arXiv:1909.07039.
[82]Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions. IEEE Communications Surveys & Tutorials.
[83]Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), 36-43
[84]"Security Aspects of Network Capabilities Exposure in 5G," September 2018, available at https://www.ngmn.org/wp-content/uploads/Publications/2018/180921_NGMN-NCEsec_white_paper_v1.0.pdf

[85]ETSI TS 103 458 V1.1.1 (2018-06). CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements.
[86]ETSI TS 103 532 V1.1.1 (2018-03). Page 43 CYBER;Attribute Based Encryption for Attribute Based Access Control
[87]ONF Principles and Practices for Securing Software-Defined Networks. Available at https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf
[88]5G PPP Phase1 Security Landscape Produced by the 5G PPP Security WG https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf. Last accessed November 2019.
[89]CCRA. 2017. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[90]Dr Michèle Finck "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Last accessed November 2019.
[91]ISO/TS 21177 "Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices"
[92]IEEE –Conformity Assessment Program (ICAP) presentation, January 2019, available at http://www.ieee802.org/1/files/public/docs2019/60802-Subramaniam-IEEE_ICAP_Overview_TSN-0119.pdf
[93]Antonio J. Jara, "ACTIVAGE: data quality", Aril 2019, available at https://oascities.org/wp-content/uploads/2019/04/2019-04-08_HOPU_AJ.pdf
[94]ETSI GR IP6 009, IPv6-based Industrial Internet leveraging 6TiSCH technology, March 2017

Annex II Readme worksheet of the excel sheet presented in Section 5.3

This .xlsm file contains a few macros (MakeMindMap) in order to generate mindmap files.

Mind maps consist of a central node with a "tree structure" of tags attached. In the excel sheet, the hierarchical string of tags starts after column E.

The formatting for the mind map file fits the open source www.freeplane.org software, but also others like www.xmind.net **Error! Hyperlink reference not valid.** can read it.

In the excel sheet, the hierarchical string of tags starts after column E and each row (until blank) creates a new branch on the mind map.

Sheet 1 in this excel file is this "ReadMe". Sheet "DefaultMM" is protected against changes because it is used to fill in default mind map initial text. Sheet "Organisations" is an example mind map for SmartCity relevant organisations, Sheet "References" is an incomplete list of references (not checked). Sheets Test1, Test2, Test3 are simple test sheets to allow users to try out different changes.

WARNING: in excel, be EXTREMELY careful (i.e. Backup before) when sorting/filtering/hiding data, to avoid scrambling rows.

The macros are started by setting the cursor anywhere inside any sheet with appropriate information, and typing CTRL-m

The name of that current sheet is used as the name of the created mind map file, ending with .mm, over-writing any previous one.

- The user is asked for some inputs when the macro runs:
- If debugging is enabled (not this version) then "DebugMsg depth" is requested (0 means no messages and is best choice. -999 outputs first 999 messages to a file .log. +999 prints to screen, so don't.)
- "First column to use" is asked for creating nodes or categories (tags) in the mind map, e.g. "j" for excel column J
- (Note that checking for tags (categories) stops at the first later column where a tag is empty in Row 1)
- The macro closes with the message "Done."

The formatting of the excel sheet of information must be:

- Row 1 contains headers describing each column. If a blank header is encountered it will stop processing of later columns.
- (That is a feature: you can insert a blank column to "truncate" the mind map so not all the depth is processed.)
- Any later rows which are "hidden" in the excel sheet will be skipped over during processing (nice for ignoring unneeded rows)
- Columns are A <optional index>, B <Name>, C <optional weblink>, D <should be full title>, E <optional abstract>, FGH etc <optional tags>
- Column A is optionally numbers, intended to remind of some consistent index

of items, independent of re-sorting etc. It is not used in the mind map.
- Column B must contain a short Name or Title to show in a box in the mind map. Preferably a descriptive one!
- (If a blank is found, processing will stop This is a feature: you can insert a blank row in the middle of the list to truncate processing for the mind map.)
- Column C, if not blank, is used as a weblink to the document or organisation described. Links are NOT checked.
- Column D is currently not used in the mind map but SHOULD contain the full official name of the organisation of title of a document
- Column E must be blank OR contain an Abstract of the reference. It is shown in the mind map as a yellow button which shows the text when the mouse is moved over it.
- Column F and later columns are all user-defined, for making your mind map. DO NOT USE '&' IN Tag NAMES !
- Note that the mind map formatting looks logical if rows are ordered so tag combinations are without gaps i.e. If you have tags in ColF and ColG then a tag in ColI will not appear on the mind map at the same place as if you had put it in ColH.

Collaboration

The excel sheet can be a collaborative tool where new material can be added, sorted, hidden, abbreviated without deleting anything unnecessarily

- Columns F and later ("your tags") can be moved and re-sorted to create whatever desired hierarchy of tags is needed, without deleting any information.
- The ordering of the "tags" columns sets how the rows are grouped together under common categories: shifting ordering can make a big emphasis change.
- Rows (except Row 1) can be hidden so that only the rows of current interest are shown

Known bugs

- Putting the character "&" inside of a tag (e.g. Water & Waste) crashes the mind map. Until the bug is fixed please use Water_and_Waste or some other way
- The algorithm to generate the mind map assumes that in the declared set of columns of categories (e.g. G-J) there will be no gaps i.e. If columns G and H have categories, and column "I" does not, then also J does not. There is no error message, and all nodes in the mind map are generated, but the arrangement is a bit mixed up. I am still considering what SHOULD the algorithm do, just jump across to the next category?

Licensing

"Creative Commons License and Disclaimer

If modified, this document was modified by Lindsay Frost on 20180924 under license as below.

The original source version v30 of this material is licensed under CCI4 (see below) and was created on 20180924 by the SF-SSCC, the Sector Forum for Smart and Sustainable Cities and Communities, a joint activity of CEN/CENELEC/ETSI (the European Standards Organizations). The latest version of this document and of the mind map described here is available at: https://www.cencenelec.eu/standards/Sectors/SmartLiving/smartcities/Pages/SSCC-CG.aspxhttps://www.cencenelec.eu/standards/Sectors/SmartLiving/smartcities/Pages/SSCC-CG.aspx
External contributions and distributions are welcomed. If you change the original version you MUST update the first line of this disclaimer and the title and central node of any exported mind map and keep this disclaimer.

This document is a living document with the aim to give an overview of useful information on work related to smart and sustainable cities, and to reference initiatives and standardization activities. Web links to original material are given, but there are no guarantees that the links are maintained or contain the same information as originally viewed. Categories and labels in the document are defined by you and previous users. The SF-SSCC has chosen as a compromise for a wide range of users and experts, and are related to naming in various UN, WHO, ESO, ITU and ISO documents... but there is no universal agreement. Please consider the categories like the shelf areas in a library: you may not agree with the topics but at least similar things are nearby.

This work is licensed under a Creative Commons Attribution 4.0 International License https://creativecommons.org/licenses/by/4.0/legalcodehttps://creativecommons.org/licenses/by/4.0/legalcode and you are free to (a) share, copy and redistribute the material in any medium or format, and (b) adapt, remix, transform, and build upon the material for any purpose, even commercially, provided that you follow the following terms: (c) you must give appropriate credit, provide a link to the license, and indicate if changes were made in the licensed material, and you can do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use, (d) no additional legal terms or technological measures are added that legally restrict others from doing anything the license permits."

Annex III Security and Privacy aspects in 5G

The next generation of 5G networks will introduce a number of new concepts in comparison to the previous generations of telecommunication networks. The novel features of 5G networks will impact different layers of the network from the physical layer to the network and applications layers. 5G networks will support IoT devices and technologies in various domains, then a study of the 5G security and privacy aspects is related to SerIoT.

A number of standardization activities are on-going in this area and various studies have reported on the new security and privacy challenges of future 5G networks.

In [82], the authors provide a survey on security and privacy aspects in 5G technologies including a review of the current standardization activities. While it is recognized that many security and privacy vulnerabilities are mitigated in 5G (e.g., authentication is more robust with 5G-AKA), the complexity of 5G networks has also created new potential threats, which are briefly summarized here from the findings in [82]. In particular, the application of 5G to IoT is investigated in detail. The identified threat areas are:

- In IoT, eavesdropper attacks, malware and epidemic attacks are considered high priority because of the large number of IoT devices, which can be present in the IoT context.
- In network slicing, communication between inter-network slices is not secure.
- Denial of Services attacks. For example, when a number of devices access the signalling plan of a 5G network simultaneously.
- Weak implementation of access control.

Along similar lines, the authors in [83] have identified a number of security threats including:

- Flash network traffic, especially in the IoT domain with numerous IoT devices connected to the 5G network.
- Signalling storms (same of threat 3 above) affecting Non-Access Stratum (NAS) layer of the 3GPP protocols.
- User plane integrity: No cryptographic integrity protection for the user data plane.

More specifically, we describe in the following paragraphs the on-going security and privacy studies in some specific standardization groups.

NGMN P1 WS1 5G

Next Generation Mobile Networks (NGMN) 5G Security Group (NGMN) P1 WS1 5G security group has been mainly gathering requirements. The alliance is comprised of many stakeholders, such as mobile network operators, service providers and device manufacturers. The security group objective is to guide standardization and implementation of 5G security features, in particular Multi-access Edge Computing (MEC). In a recent report [84], the NGMN 5G security group has defined several service scenarios and technical requirements for MEC in 5G.

ETSI (and 3GPP)

ETSI has identified Attribute Base Encryption (ABE) as a key enabler technology for distributed systems in 5G network and two access control specifications have been published. ETSI TS 103 458 [85] focuses on how to secure user identity, and to preventing disclosure to an unauthorized entity in a WLAN and cloud. Whereas ETSI TS 103 532 [86] describes trust models protocols using ABE mechanism and increases data security and privacy in untrusted environments.

Open Networking Foundation (ONF)

The Open Networking Foundation (ONF) is a non-profit organization funded by many large companies like Deutsche Telekom, Facebook, Google, Microsoft. ONF strongly supports SDN, which is one of the key components of 5G. In 2015, ONF has published a report on Principles and Practices for Securing Software-Defined Networks [87], which can also be applied to 5G.

In addition to the standardization bodies cited above, many other standardization bodies and committees like IEEE, ETSI M2M and NIST work closely with 5G standardization bodies as some areas (e.g., WLAN) impact 5G and vice versa.

To complete this overview, we also mention the 5G PPP Public Private Partnership, which is a joint initiative between the European Commission and European ICT industry. The 5G PPP initiative was initiated based on the experience of ICT infrastructure and communication networks.

5G PPP

The 5G PPP Public Private Partnership is a joint initiative between the European Commission and European ICT industry. The 5G PPP was initiated based on the experience of ICT infrastructure and communication networks.

In 5G PPP, a security working group was established to identify security and privacy risks of 5G networks. This WG was officially launched on 5/4/2016 and results from an initiative created by a Phase 1 Security Project (5G-ENSURE). Since its creation, this Working Group has been the place where the 5G Security topics and vision were discussed and also progressed. The Security working group has published the white paper 5G PPP Phase1 Security Landscape [88], which identifies (among other things) the 5G major security requirements and risks and the related 5G architecture.

Annex IV Editors and Contributors to this Deliverable

The document was written by several participants of the AIOTI WG03.

Editors (and contributors):

- Michelle Wetterwald, Netellany / FBConsulting, ETSI STF 505 & ETSI STF 547 (Release 2)
- Georgios Karagiannis, Huawei Technologies (co-editor Release 2)
- Emmanuel Darmois, CommLedge, ETSI STF 505 & 547 (Release 1)

Main Contributors:

- Gianmarco Baldini, JRC, European Commission (and SerIoT project)
- Henri Barthel, GS1
- Samuel Berlemont, Orange
- Sebastien Bolle, Orange
- Angel Boveda, Wireless Partners S.L.L.
- François Ennesser, Gemalto
- Lindsay Frost, NEC
- Christophe Gossard, John Deere
- Jurgen Heiles, Siemens
- Jose Luis Hernandez Ramos, JRC, European Commission
- Bill Karakostas, VLTN GCV (CHARIOT Project Technical Lead)
- Holger Kellerbauer Caterpillar
- Joachim Koss, JK Consulting & Projects, ETSI STF 505 & 547
- Vivek Kulkarni, Siemens (SEMIoTICS project coordinator)
- Konstantinos Loupos, INLECOM Innovation (CHARIOT Project coordinator)
- Samir Medjiah, LAAS-CNRS, ETSI STF 505
- Emna Mezghani, Orange
- Jumoke Ogunbekun, E2X Management Consulting Ltd, ETSI STF 505 & 547
- Dave Raggett, W3C (and CREATE-IoT WP06)
- Steffen Ring, Ring Advocacy ApS (and H2020 project MONICA)