AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

High Priority IoT Standardisation Gaps and Relevant SDOs

Version 1.0, May 2018

AIOTI WG03 – IoT Standardisation

2018

Executive Summary

This deliverable 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 start a structured discussion within the AIOTI WG03 community and to provide consolidated technical elements as well as guidance and recommendations.

Table of Contents

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 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 largely 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

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.

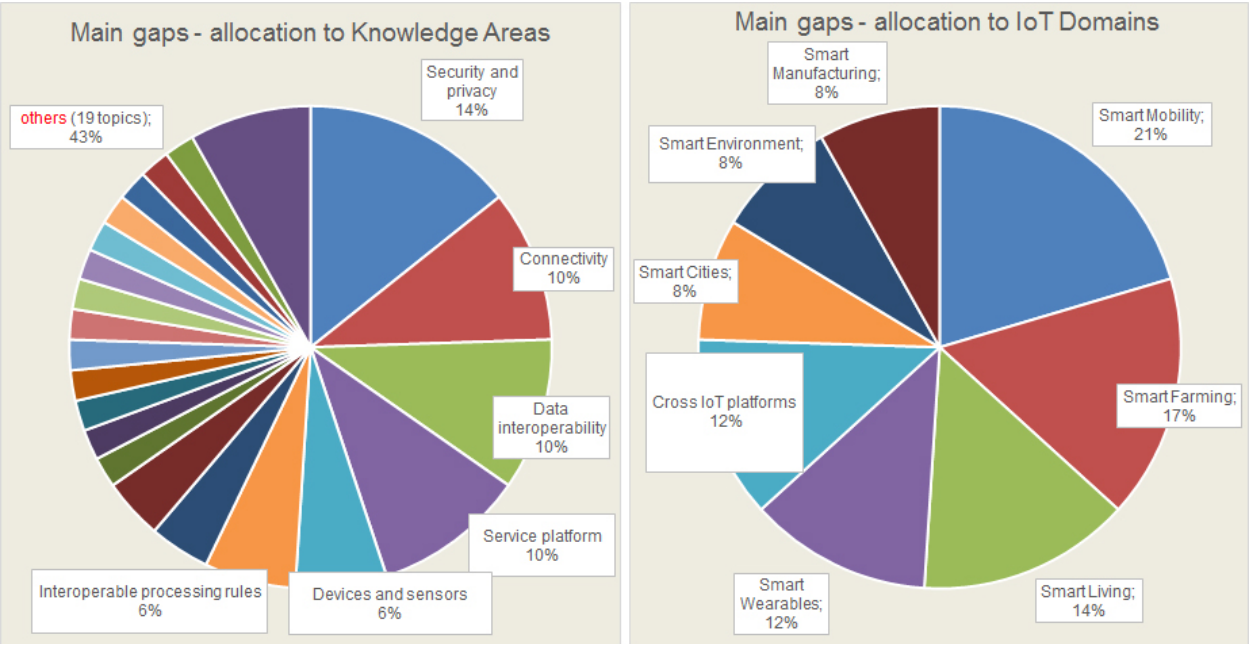

Figure 1: STF 505 gaps per Knowledge Areas and IoT Domains

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 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 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 (in an email contribution to the AIOTI WG03) related to the need to report/encode the Health of Edge Computers. The questions addressed are:

- Is data trustworthy?
  - Is this computer uncompromised?
    - Since fabrication?
    - Since Commissioning?
  - Is the running software authentic?
    - Firmware, OS, Application code
  - Is this Computer genuine?
  - Is this computer operating properly?
  - Is the data really coming from this computer?

- Using Trusted Computing techniques, device Computer vendors can assess the health of the computer
- Need to report this information 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 [3] done 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
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
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

5 Gap 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). This section addresses the work done in some of the SDOs/SSOs involved in AIOTI WG3.

In the current release of the present document, this section is very much in its early stage: most of the work for the revolution of the present document will happen in enriching it.

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):

- 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. Validation of data from sensors and control loops: there are questions arising.
- 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. Our stakeholders' interests demand clarification and identification. This urgently requires a common language and improved definitions of Users and Use Cases.

5.3 Gaps identification and resolution work in other SDOs

The corresponding sections (one per SDO) will be complemented in the next release of this document.

6 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 needs that will include: (1) identified key gaps and (2) SDOs that needs to cooperate with in order to solve these gaps.

The present document is the Release 1.0 of this AIOTI Report. It will be a living document subject to further regular updates in new Releases.

7 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

Annex Editor and Contributors to this Deliverable

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

Editor:
Emmanuel Darmois, CommLedge

Main Contributors:
The ETSI STF 505 Team
- Emmanuel Darmois, CommLedge
- Joachim Koss, JK Consulting & Projects
- Samir Mejia, CNRS
- Jumoke Ogunbekun, E2X Management Consulting Ltd
- Michelle Wetterwald, Netellany / FBConsulting

Angel Boveda, Wireless Partners S.L.L.
François Ennesser, Gemalto
Christophe Gossard, John Deere
Jurgen Heiles, Siemens
Georgios Karagiannis, Huawei Technologies
Dave Raggett, W3C (and CREATE-IoT WP06)

