Outline

Introduction
  • ETSI TR 103 376: Content and Methodology

Results: main gaps (per knowledge area) and recommendations
  • Identified by expert team and by the survey respondents
  • For all vertical domains (Smart Cities, Smart Living, Smart Farming, Smart Wearables, Smart Mobility, Smart Environment, Smart Manufacturing)

Conclusion and summary
  • Main topics identified
Rationale for this study
• The **coverage of the IoT landscape** - and the possibility to develop large-scale interoperable solutions - is **not fully guaranteed** since some elements in this landscape may be missing.

Main Objectives
• 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.
TR 103 376: Identification of standards gaps and recommendations

Nature of gaps
- Missing standards
- Missing APIs
- Duplications that would require harmonization
- Missing interoperability profiles that would clarify the use cases
- Classified as: technical, business or societal gaps (incl. security and privacy)

Gaps identification methodology
- Survey to obtain inputs from the standardization and stakeholders community:
  - 215 answers, include gap identification as well as proposed solutions
- STF experts analysis to expand on the current standards landscape
  - For each vertical, extract requirements from the AIOTI reports and other documentation
  - Identify if SDOs/Alliances address the target requirement (using TR 103 375)

All identified gaps recorded in the TR, to serve as a reference for the LSPs

Resolution of the gaps
- Dissemination of STF 505 results: to point to gaps and allocate them
- It is left to the proper organizations of the IoT community to fill the gaps
TR 103 376 : Structure

General Considerations
- Definition, identification and mapping of gaps
- Vertical domains and Knowledge areas covered

Gap analysis in the context of:
- Smart Cities
- Smart Living environments for aging well
- Smart Farming and food security
- Smart Wearables
- Smart Mobility
- Smart Environment
- Smart Manufacturing

Cross IoT platform interoperability and harmonization

Annex: the ETSI STF 505 Gap Analysis Survey
An example of TR content: Identification of security gaps in Smart Cities

Input from the standardization and stakeholders community

• Captured by the survey

<table>
<thead>
<tr>
<th>Nature of the gap</th>
<th>Knowledge Area</th>
<th>Criticality</th>
<th>How can standardization or regulation improve this?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and security aspects not sufficiently covered, developed and not real</td>
<td>Communication and Connectivity (network and service levels); Integration/Interoperability; IoT Architecture; Security and Privacy</td>
<td>3</td>
<td>IoT and big data pose new challenges to an acceptable model of privacy and security management and rules (in terms of civil rights and &quot;industrial privacy/security&quot; guarantees: it is necessary to find out new models/approaches</td>
</tr>
</tbody>
</table>

Expanded by STF 505 experts analysis on the current landscape

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Organizations providing related standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level of trust (common good objective)</td>
<td>3GPP W3C</td>
</tr>
<tr>
<td>bootstrap authentication and key agreement for application security</td>
<td></td>
</tr>
<tr>
<td>End-to-end security</td>
<td>3GPP, Hypercat, IEEE, IETF</td>
</tr>
<tr>
<td>Confidentiality and privacy, protection of personal data; encryption</td>
<td>OASIS</td>
</tr>
<tr>
<td>Secure remote access to the system from third-parties; user authentication, access control</td>
<td>IEEE Hypercat</td>
</tr>
</tbody>
</table>
49 main gaps result from the consolidation view (TR 103 376)
Main gaps and recommendations per knowledge area
Connectivity

Fragmentation of the standardization landscape.

Large number of heterogeneous & competing communications and networking technologies

• ➔ Choose solutions with additional criteria: IPR, licensing and monthly fees, deployment cost, security, energy consumption.
• ➔ Further criteria: flexibility, prioritization of the flows, scalability, resilience to external factors and possible issues in the network, high network availability, spectrum resources availability
• ➔ May need refinement of existing standards
Upper layers: service and application

- **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
  - ➔ Develop **semantic interoperability** to enable harmonization

- **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
  - ➔ Develop **guidance for decision-making processes**, for data organization, storage and exchange.

- **APIs to support application portability among devices/terminals**
  - ➔ **Interoperability of platforms**: data level (semantic) + application level (services)
**Global-level standards (international vs. regional level)**

- **Harmonization** / Interoperability of similar messages defined at regional level

**Fragmentation due to competitive platforms and standards**

- Develop **technical guidance of compatibility** between standards
- Some clarification may be brought by **refinement of the use cases**
- Develop **interworking / cooperation between platforms**, e.g. possibility to exchange data. Manage applications heterogeneity
- Focus on the **whole value-chain** (devices, platform, etc....), not only on connectivity. Enable the support of a wide range of sensors, devices, protocols, services ... Ensure **flexibility and scalability**
Applications management (life-cycle)

**Usability** [Societal gap]

- Develop **tools to enable ease of** installation, configuration, maintenance, operation of devices, technologies, and platforms.
- Simplify the **personalization of the system.** Enable **easy accessibility and usage** to a large non-technician public.
- When suitable, allow **secure remote access** to perform device maintenance. Enable **continued support to the client** after purchase.

**Applications tailored to individual needs: evolution, flexibility of the components**

- Standardized **methods to distribute software components** to devices across a network, for life-cycle management in the field.
- Built-in **application performances' monitoring.**
Deployment tools

- Unified model/tools for deployment and management of large scale distributed networks of devices
IoT Architecture

**Identification**

- Provide a *global reference for unique and secured naming mechanisms*
- Federate existing identification schemas. Secured IoT nodes identification model

**Multiplicity of IoT HLAs, platforms and discovery mechanisms**

- *oneM2M* is emerging as a global international platform that has gained a very large support of various actors (ref. workshop held in ETSI in November 2016)
- Develop specific solutions at the Service Layer to enable communications between the platforms (e.g., offer plugins to oneM2M platform)
- Allow smart objects to move and enter different eco-systems (e.g. during an update of the system or change of provider)
Quality assurance and certification

- Building of certification mechanisms defining “classes of devices” and covering features such as robustness, consumption, accuracy, reliability, resilience over long periods of time (self-sufficient operation)
- Standardisation of test specifications and suites (hardware and software) and proper guidelines regarding the final characteristics that correspond to the expectations
- Definition of approval processes for IoT devices conformance assessment.

Device modularity

- Standardisation of the ability to add/remove hardware capabilities to a device
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

- Develop “classes of devices” and device tagging for security
- Develop mature data management, data security, data privacy and ownership standards, rules to ensure trust in a common good objective, foster security by design initiatives
- Develop data rights management (ownership, storage, sharing, selling, etc.). Define samples, good practices, regulations...
- Develop education of end users on these features

Lack of highly secure and trusted environments

- Build Risk Management Framework and Methodology
- Develop a workflow to establish trust between the players
Societal gaps [including regulations]

- **Lack of knowledge about potentialities of IoT among decision makers, users**
  - ➡️ **Dissemination** fosters awareness from the different actors
  - ➡️ Encourage the development of *education and dissemination material of IoT standards* and specifications

- **Green Technologies**
  - ➡️ Insert *low power and low energy constraints* integration in the whole value chain.

- **Liability for data privacy**
  - ➡️ Regulations to enforce the *respect of privacy* at all levels of the IoT systems and *distribute the liability* between the different providers and actors
Ethics. Transparency and choice for citizens

- Guarantee of integrity, ethical by design
- Exchange data on security breaches to raise awareness and avoid their repetition

Not everything should be smart

- Definition of what is useful to society and what is useless. Adaptation to the needs

Green Technologies

- Develop pollution management

Regulations for frequency harmonization and usage
Business gaps

Lack of a reference for business cases and value chain model to guide choices for deployment

- Define an integrated vertical business architecture, considering all actors of the value chain, from manufacturers to dealers, installers, service providers, end users...
- Clarify what is proprietary, open source, subject to IPRs
- Reduce delay of standardization to avoid proprietary solutions (vendor lock-in). But in parallel, enable the insertion of existing proprietary solutions (de-facto standards) in the architecture
- Roadmaps to market taking into account renewal cycle. Simplify early deployments
- Foster new investment paradigms to small companies, early adopters, vs. extreme competition
- Give priority to cost effective implementations, reusable solutions
Business gaps (cont.)

**Collaboration between vertical domains, siloed applications**

- ➔ Develop **communication between stakeholders** from technology and vertical domain
- ➔ Specify the **collaboration of siloed applications and services**, create a global value chain (e.g., healthcare service links with other services such as smart home for living environment, smart cities for outside activities, smart mobility)
- ➔ Develop **more transversal and common solutions** (compatibility) and business models. Aim at the seamless interoperability or plug and play of the different standardised IoT architectures and platforms
**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
Thank you for your attention!

Michelle Wetterwald
FBConsulting, member of STF505
Sophia Antipolis, France
michelle.wetterwald@gmail.com

STF 505 Homepage: https://portal.etsi.org/STF/stfs/STFHomePages/STF505
ANNEX
## Consolidated view of the main gaps

<table>
<thead>
<tr>
<th>Main Gaps Identified (by topic)</th>
<th>Number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and privacy</td>
<td>7</td>
<td>14.3</td>
</tr>
<tr>
<td>Connectivity</td>
<td>5</td>
<td>10.2</td>
</tr>
<tr>
<td>Data interoperability</td>
<td>5</td>
<td>10.2</td>
</tr>
<tr>
<td>Service platform</td>
<td>5</td>
<td>10.2</td>
</tr>
<tr>
<td>Devices and sensors</td>
<td>3</td>
<td>6.1</td>
</tr>
<tr>
<td>Interoperable processing rules</td>
<td>3</td>
<td>6.1</td>
</tr>
<tr>
<td>Autonomicity, decision-making processes</td>
<td>2</td>
<td>4.1</td>
</tr>
<tr>
<td>Data Models</td>
<td>2</td>
<td>4.1</td>
</tr>
<tr>
<td>Communication infrastructure</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Data handling</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Decision-making processes</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Devices certification</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Devices modularity</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Duplication of standards according to different regions of the globe</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Ease of use</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Fragmentation of the technology according to the target application</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Integration of a larger set of IoT devices</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Position accuracy</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Processing rules and decision-making processes</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Usability and customization of the solutions</td>
<td>1</td>
<td>2.0</td>
</tr>
<tr>
<td>Others</td>
<td>4</td>
<td>8.2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>49</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>