IoT Systems: Architectures, Models, Guidelines

IoT Standards: a Global Approach

The ETSI Specialist Task Force 547

Presented by: **Emmanuel Darmois** For: **IoT Week 2019**

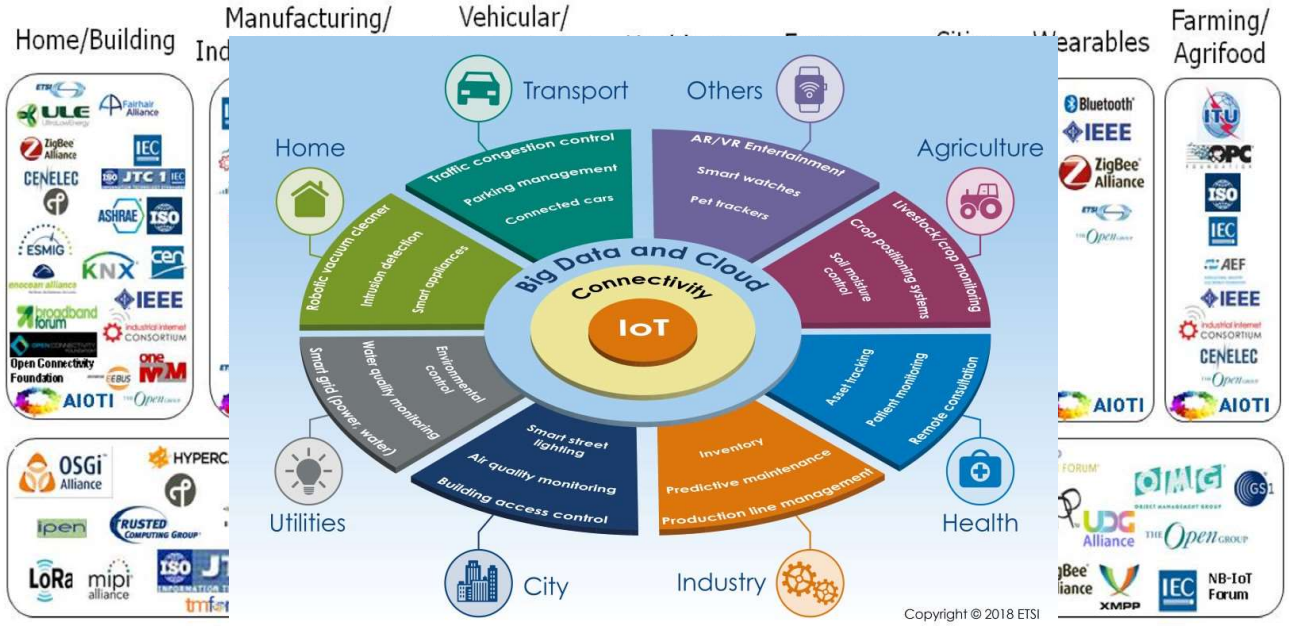
20.06.2019

A Complex Picture

The intrinsic complexity of IoT have a profound impact on IoT Standardisation and how standards are actually used

Pervasive ICT technologies, Multiple Point Solutions (e.g. protocols)

Sector-specific solutions (and silos), Cross-sector system deployment



Source: AIOTI WG3 (IoT Standardisation) – Release 2.8

How to Make Decisions in a Fragmented Standards Landscape?

Standards are only a part of the picture

Standards	Open Source	Regulation
Industry	Stakeholders	Research
Skills	Strategies	Organisations

Addressing IoT Systems Complexity

Dealing with IoT characteristics

High-level issues in support of strategy

- Extensive Stakeholders Involvement
- Technical strategy
- Deployment models
- Integration of/with legacy

Specific technical challenges

- Interoperability
- Privacy
- Security

Integrating some important aspects

Stakeholders and roles

- From diverse viewpoints
  - Strategy, empowerment, technology, …
- Potentially conflicting requirements

Reference Architecture

- Shared understanding
- Documented technical choices

Support to the non-specialist involved

- Guidelines for decision and usage
- Teaching material

ETSI Specialist Task Force (STF) 547
A global approach to IoT Systems

A framework for IoT standardisation

- Addressing interoperability across IoT domains
- Focusing on major aspects:
  - (Semantic) Interoperability
  - A end-user focused approach to Privacy
  - Methods and techniques for Secure IoT

Whose essential objectives are to

- Identify guidelines and best practices
- Build a bridge for potential designers / implementers of IoT systems
- Provide comprehensive material for information, teaching/learning and demonstration with a very practical usage and implementation perspective

Co-funded by the European Commission

ETSI STF 547
A Set of Coordinated Deliverables

Seven Technical Reports

- Privacy; Standards Landscape and best practices — TR 103 591
- Security; Standards Landscape and best practices — TR 103 533
- Guidelines for using Semantic Interoperability in the industry — TR 103 535
- Plugtests™ preparation on Semantic Interoperability — TR 103 537
- Strategic / technical approach on how to achieve interoperability / interworking of existing standardized IoT Platforms — TR 103 536
- Teaching material; Part 1: IoT Security — TR 103 534-1
- Teaching material; Part 2: IoT Privacy — TR 103 534-2

A Special Report to introduce to a complex landscape

- Dedicated to all stakeholders — SR 003 680
  - Not just for the technology happy few (and the standards literate)
  - Overall SR document and Additional Slides (including Teaching Material)
- Based on the analysis of relevant use cases

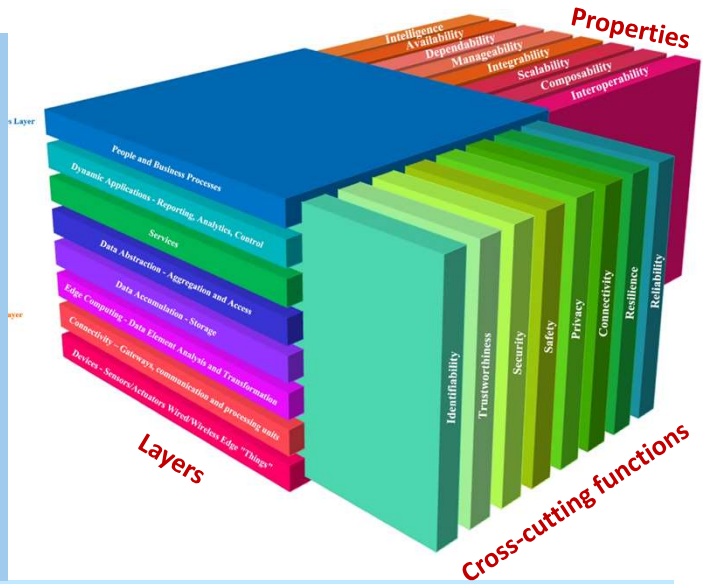
Addressing major issues

Reference Architecture
The IoT LSP 3D Reference Architecture Model

European Large-Scale Pilots Programme

The LSP 3D Architecture Model (developed in the LSP Activity Group 02) extends some of the current IoT reference architectures and is aiming at:

- Ensuring a common view of the different layers of the IoT systems from Physical up to Business;
- Providing additional viewpoints to the different stakeholders (not just to the developers) regarding some additional cross systems functions such as security, privacy or safety and the shared analysis of some properties (e.g., integrability) between different stakeholders.



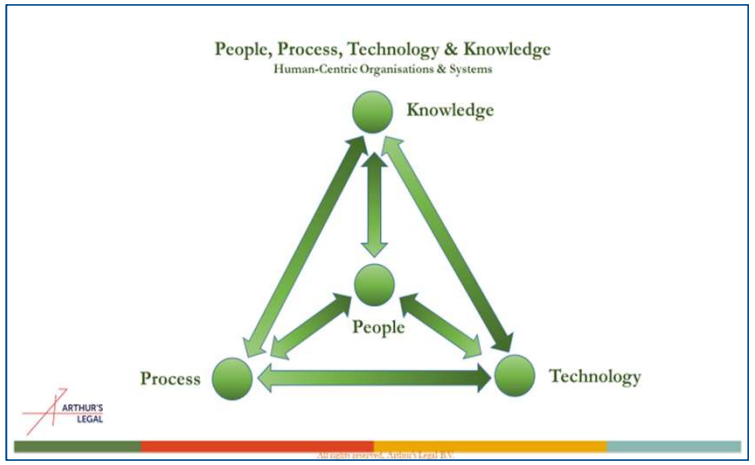
The additional dimension of properties is a new way to discuss the properties of the IoT system between different involved parties (e.g., users, contractors, designers) and identify the elements in support (e.g., functional building blocks, APIs) and those missing.

The 3D Model is meant to be contributed to standardisation (not yet another Reference Architecture)

Privacy

The challenge of Privacy in IoT

- IoT is an example of hyper connectivity and distributed control
- Appropriate safeguards are needed to ensure that individuals' right to privacy is **effectively** protected
  - Box ticking does not guaranty effective protection
- Some of the challenges in ensuring privacy in practice:
  - Identifying the entire chain of stakeholders that have responsibilities in relation to processing of personal data
  - Understanding the role of the context
  - How stakeholders need to think of Privacy as part of design not an afterthought
  - Raising awareness that protection of privacy is mandatory: GDPR forms binding law, not just a standard



The Technical Report proposes an approach that suggests

- Reinforcing the role of human users
- Putting privacy concerns at the heart of IoT

Privacy
Best Practices and Training Material

Standards Landscape and Best Practices TR 103 591

- The role of Standards under GDPR
- Use cases for IoT Privacy
- IoT Privacy Standards Landscape
- IoT Privacy Guidance and Best Practices
  - IoT Privacy Guidance pursuant to current Best Practices
  - IoT framework principles pursuant to the GDPR
  - Proposed guidelines on meeting GDPR principles
  - Existing guidelines: the paradigm of privacy by design

Training material TR 103 534-2

- Covers
  - What is Privacy and Data Protection; use cases analysis
  - The novelties of GDPR
  - Risk assessment and risk mitigation

Some take-aways

GDPR is mandatory

- An effective protection of privacy and (personal) data protection requires technical and organizational measures
- Organizations need to deliver documented and continuous proof of appropriate levels of protection

No new standards or regulation needed on privacy but:

- There is a significant gap in application of privacy protection in general
- Any new IoT standard should be adapted to GDPR
  - Standards do not mean to serve as a presumption of conformity with the GDPR,
  - New standards will have to interoperate with the rest of the legislative acts pertaining to the IoT ecosystem and beyond.
- Need for new codes of conduct and certification
  - Accountability tools embraced by the GDPR, also highly relevant for the IoT

Security
From IoT to Secure IoT

Identify where devices sit on the acceptable risk scale

- Highly risk averse:
  - All devices have to identify themselves and their function to their attached correspondents
  - All data passed from device to device has to be visible only to identified and authenticated, and authorized parties
  - All data protected against malicious manipulation (e-signature or MAC)
- Less risk averse
  - Use secure nodes as security anchors and liability anchors; Allows for devices without security processing

Apply Security Principles to IoT

- General Security Guidance and Best Practices
  - Provide security functions when required by law
  - Provide mitigations to quantified risk
  - Know who is acting on your device and why (security in depth)
- Specific (Cryptography) Security Guidance and Best Practices
  - Security should be centred on the key (and not on the algorithm)
  - Key management rigour determines system vulnerability

Security
Best Practices and Training Material

Standards Landscape and Best Practices TR 103 533

- Snapshot of IoT security (standards) landscape
- Regulatory Context: GDPR, NIS Directive, Cybersecurity Package
- IoT Specific Security Guidance and Best Practices
  - GSMA, DCMS, ENISA, ECSO and other industry guidelines
- General Security Guidance and Best Practices
  - Defence in Depth
  - Secure by Default
  - Design for assurance
  - Privacy by Design

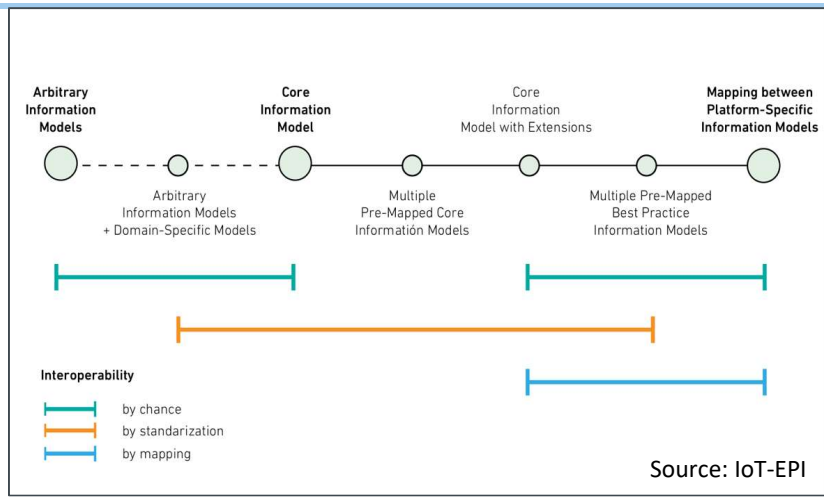
Training material TR 103 534-1

- Covers risk analysis, cryptography basics, trust modelling …
- Example of why it is useful
  - An IoT vendor is not certain to know how the IoT thing will be deployed, therefore has to make educated guesses to assure security. Hence the need to train everyone in the supply chain in security.

The IoT Security Landscape

AIOTI	oneM2M WG4
ENISA	ETSI SmartM2M
ITU-T	ETSI ITS WG5
NIST	ETSI SmartBAN
OASIS	ETSI EP eHealth
TCG Trusted Computer Group	ETSI ERM

Semantic Interoperability



Source: IoT-EPI

The Semantic Interoperability Challenge

- Adopt the most flexible adapted of many approaches
- Make sure this is used in the industry, not just labs

High expectations

- Market drivers
  - Improving existing services, providing new ones; public policy support, …
- Expected benefits
  - Continuous solution integration/operation, efficient data exposure, centralized management of heterogenous IoT infrastructure, …

Difficult road ahead

- A complex landscape
  - Glossary, Dictionary, Taxonomy, Thesaurus, Topic map, Meta data repository, Microformat, Ontology
- Various level of adoption
  - With a preference for “static” approaches, due in particular to the skills of the developers

Semantic Interoperability
Guidelines and Best Practices

Guidelines for SI in the industry TR 103 535

- State of the art of semantic interoperability
  - Semantic approaches; Classification systems; Ontologies
  - Existing solutions from academia, standards and industry
- Semantic interoperability adoption analysis
  - Need; Adoption Status; Market Drivers and Inhibitors
  - The ontology problem
- Guidelines for using Semantic Interop. in the industry
  - Strategy guidelines (for high-level decision making)
  - Technical guidelines (for IoT system designers and developers)

Guidelines for SI Plugtests TR 103 537

- Requirements for testing Semantic Interoperability
- Test configurations
- Examples of possible test scenarios

Key take-aways

Market inhibitors

- Lack of familiarity with semantic
- Lack of killer applications and successful use cases
- Complexity and immaturity
- Uncertainty regarding scalability and performance
- Difficulty to perceive immediate value

The ontology problem

- No generally accepted upper-ontology in use
- Many fragmented knowledge niches
- The ontology integration nightmare

Guidelines are proposed

- Strategic: decision, investment, promotion, …
- Technical: use upper ontology, reuse domain ontology, adapt the development process, …

Are Standardised Platforms ready for prime-time?

Definition

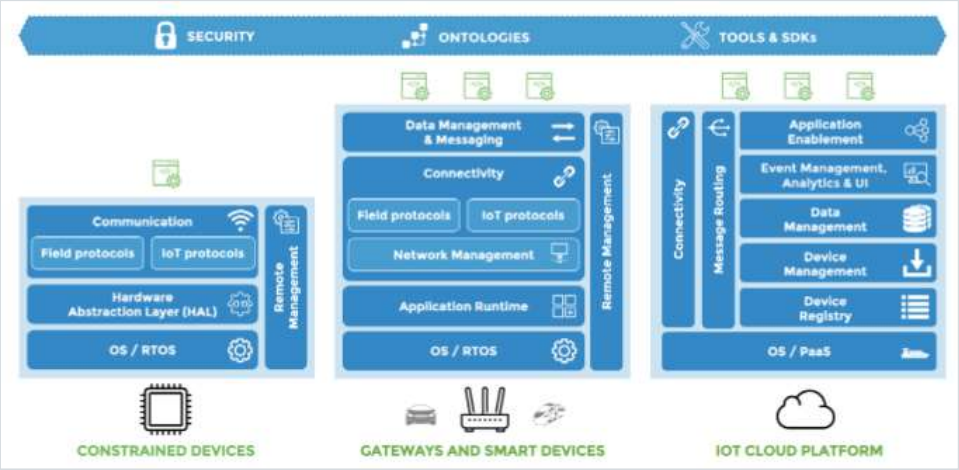
- An IoT Platform can be defined as an intelligent layer that connects the things to the network and abstract applications from the things with the goal to enable the development of services. […] An IoT platform facilitates communication, data flow, device management, and the functionality of applications. The goal is to build IoT applications within an IoT platform framework. (Source: IoT-EPI)

Expectations

- To mask the heterogeneity of devices
- To handle and simplify communication
- To support (end-to-end) data flows
- To provide generic services to the applications built on top of it

Challenges

- Versatility
- Semantic Interoperability
- Flexible deployment models
- Open and efficient implementations
- Support of non-functional properties (e.g., security)



Source: eclipse.org

Standardised Platforms
Guidelines and Best Practices

Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms TR 103 536

- An IoT Platforms Landscape
  - Analysis Framework; Maturity; Classification
  - Standardised IoT Platforms
    - Some examples: oneM2M, OCF, Apache
- Interoperability: Strategy & Technical approaches
- The case of Industrial IoT
  - Challenges of IIoT
  - Using Standardised Platforms in IIoT
    - Connectivity; Semantic Interop.; Virtualisation; Data …
  - Platform adoption
  - A review of IIoT Platforms
- Guidelines and recommendations

Key take-aways

Lessons learned

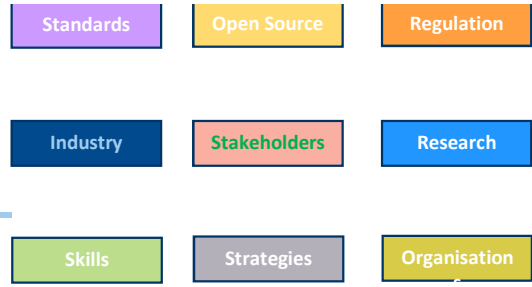
- Still fragmented & immature landscape
- Proprietary platforms are not a panacea
- Open platform adoption in the Enterprise is (even more) complex
- The key role of integration
- A growing role for standardised solutions
- Semantic Interoperability is a key issue and enabler to open platform adoption
- Many issues related to platform adoption are cultural

Conclusion

- Standardised platforms can be considered
- Strategy choices (proprietary vs standardised, development organisation, training, …) are as important as technical ones

Conclusions

The STF: a contribution to the landscape evolution



Where we are

All Technical Reports developed

- Overall publication date: 08/2019
- Presented in IoT Week 2019

Dissemination Package

- Special Report and Teaching Material
- SR Target publication date: 11/2019

Promotion / Dissemination

- Delivery Workshop in December
- Involving actors beyond standardisation

Where we go

ETSI contributions

- ETSI SmartM2M, ETSI CIM, …

Collaboration and coordination

- Fostering de-fragmentation
- Addressing technology challenges
  - Semantic Interoperability, 5G, IA, IT/OT, …

Thank you for your attention!

Contact Details: Emmanuel Darmois
CommLedge
emmanuel.darmois@commledge.com
+33 6 3151 5393

STF547: https://portal.etsi.org/STF/STFs/STFHomePages/STF547

CREATE-IoT: https://european-iot-pilots.eu/project/create-iot/