# 6

# IoT Standards Landscape – State of the Art Analysis and Evolution

**Emmanuel Darmois[1], Laura Daniele[2], Patrick Guillemin[3], Juergen Heiles[4], Philippe Moretto[5] and Arthur Van der Wees[6]**

[1]CommLedge, France
[2]TNO, The Netherlands
[3]ETSI, France
[4]Siemens AG, Germany
[5]Sat4m2m, Germany
[6]Arthur's Legal B.V., The Netherlands

## 6.1 Introduction

The Internet of Things (IoT) is now more than an emerging technology, and the IoT community has started to develop ambitious solutions and to deploy large and complex IoT systems. However, this new challenge for IoT will be met only if the IoT community develops a culture of openness regarding interoperability, support of a large variety of applications departing from existing silos, and the generation of healthy ecosystems.

The role of standards is now well recognized as one of the key enablers to this open approach. There are already a number of existing standards for those who develop IoT systems. They allow to address many of the requirements of IoT systems in a large spectrum of solutions (ranging from consumer to industrial) for a large number of domains, as various as cities, e-health, framing, transportation, etc.

The objective of this chapter is to make an overview of the current state-of-the-art in standardisation, in particular regarding the new approaches that are currently addressed by standards organisations and that will rapidly enlarge the scope of current standards. On the other hand, given the

complexity of the IoT landscape, some elements are still missing and will need to be addressed as well: another objective of this paper is to provide an overview of those gaps and how they may be resolved in the near future.

## 6.2 IoT Standardisation in the Consumer, Business and Industrial Space

The IoT community has recognized long ago the importance of IoT standardisation and started to work in many directions, adapting general purpose standards to the IoT context or developing new IoT specific standards. There is now a large number of standards that can be used by those who want to develop and deploy IoT systems. This section will address the current state-of-the-art, evaluate the number of available standards and suggest ways to classify them.

When a large number of standards exist in a given domain, there is a risk of duplication, fragmentation, competition between standards organisations. In its 2016 communication on "ICT Standardisation Priorities for the Digital Single Market" [1], the European Commission notes that: "However, the IoT landscape is currently fragmented because there are so many proprietary or semi-closed solutions alongside a plethora of existing standards. This can limit innovations that span several application areas".

This is a major challenge for IoT standardisation: because IoT is a large domain, spanning across a variety of sectors (e.g., food, health, industry, transportation, etc.), many standards potentially apply that have been developed within application silos, and the risk of fragmentation exists. The European Commission also outlines an essential way-forward [1]: "Large-scale implementation and validation of cross-cutting solutions and standards is now the key to interoperability, reliability and security in the EU and globally".

Two complementary dimensions (outlined in the next subsections) are taken into account by the IoT standardisation community:

- Expansion of the reach of "horizontal layers" standards versus "vertical domains"-specific standards;
- Specialisation of general purpose standards for application to more complex and demanding domains. This is in particular the case with the convergence of IT (Information Technology) and OT (Operational Technology) in the industrial domain.

### 6.2.1 Standardisation in Horizontal Layers and Vertical Domains

The IoT landscape developed by the AIOTI Work Group 3 on Standardisation has used the distinction between the horizontal and vertical domains for the classification of the organisations that are active in IoT standardisation.

The classification of IoT standardisation organisations is done along two dimensions:

- Vertical domains (or "verticals") that represent 8 sectors where IoT systems are developed and deployed;
- An "horizontal" layer that groups standards that span across vertical domains, in particular regarding telecommunications.

In order to give an indication of the relative importance of "horizontal" versus "vertical" standards, the ETSI Specialist Task Force (STF) 505 report on the IoT Landscape [4] has identified 329 standards that apply to IoT systems. Those standards have been further classified in:

- 150 "Horizontal" standards, mostly addressing communication and connectivity, integration/interoperability and IoT architecture.
- 179 "Vertical" standards, mostly identified in the Smart Mobility, Smart Living and Smart Manufacturing domains.

One important way to ensure that "interoperability, reliability and security" aspects (outlined above as key by the EC report [1]) are handled more efficiently is to make sure that "horizontal" standards are chosen over "vertical"

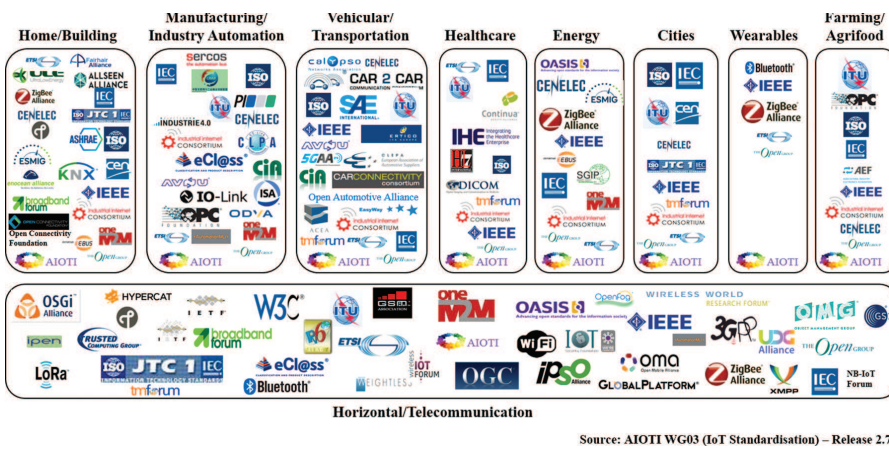


**Figure 6.1** IoT SDOs and Alliances Landscape.

ones whenever possible. An "horizontal" standard is likely to be developed to serve general-purpose requirements and better address interoperability.

In addition to the IoT Standardisation landscape, the AIOTI has developed the High-Level Architecture (HLA) that defines three layers (as depicted in Figure 6.2 below) and provides more complete ways to characterise and classify the applicable standards:

- The Application layer contains the communications and interface methods used in process-to-process communications
- The IoT layer groups IoT specific functions, such as data storage and sharing, and exposes those to the application layer via Application Programming Interfaces (APIs). The IoT Layer makes use of the Network layer's services.
- The Network layer services can be grouped into data plane services, providing short and long range connectivity and data forwarding between entities, and control plane services such as location, device triggering, QoS or determinism.

The HLA supports a more fine-grain classification of "horizontal" standards that are in general addressing only one of the HLA layers, thus offering a clearer scope for interoperability.

The IoT Standardisation Landscape in Figure 6.1 clearly shows that the "horizontal" standards are developed by organisations (SDOs/SSOs) that deal with IT technology solutions rather than by those operating in "vertical" domains. The potential of "horizontal" standards (common standards across vertical domains) will only materialize if the development of IoT standards in vertical domains is making effective use of those standards rather than reinventing similar but not compliant ones. On the other hand, collaboration and cooperation between the SDOs/SSOs involved in "horizontal" standards must be encouraged.

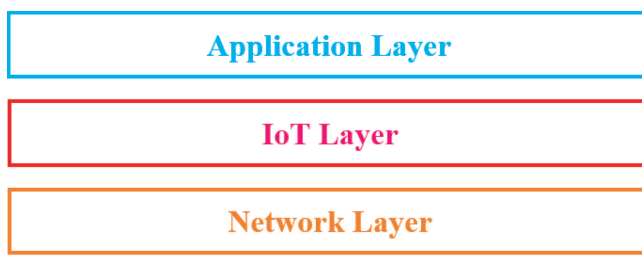


**Figure 6.2** AIOTI three layers' functional model.

### 6.2.2 Standards Addressing the Convergence of IT and OT

IoT standardisation has been a huge effort of many organisations (vendors and manufacturers, service providers, brokers, etc.). Two main kind of activities have taken place for the development of "horizontal layer" standards as well as "vertical domains" standards.

On the one hand, the "horizontal layer" standards have been mostly developed by the Information and Communication Technologies (ICT) industry with a particular focus on Information Technologies (IT), in particular those associated to communications and to new deployment models such as the cloud.

On the other hand, the "vertical" domains have started to address the requirements of IoT with the goal to expand the reach of the existing domain-specific standards. The resulting IoT standards have been coming from the massive incorporation of IT technologies, whether by adapting the existing standards or by adopting ICT standards.

IoT standardisation has addressed growing levels of complexity depending on the nature of the IoT systems concerned. Many of the ICT standards have been rapidly adopted in the Consumer space, be it for communications, security or semantic interoperability (see the example of SAREF addressed in Section 6.3.2). The requirements of IoT systems in the Business space requires an additional degree of complexity in order to be able to deal with complex data models, strict security, privacy or large scale deployments.

A new challenge for IoT standardisation is regarding industrial IoT systems (see [5]). The challenge is to massively integrate new technologies such as IoT or Cloud Computing in order to provide much more flexibility, adaptability, security and reliability. This will require achieving a transition from the current model to the "Cyber-Physical Production System" (CPPS) approach.

The current model is based on the "Manufacturing pyramid" approach, with hierarchically separated layers, where the interactions between the bottom layer of IoT devices and the upper layer of the production system are complex with supporting data models often too much specialized.

In Cyber-Physical Production Systems (CPPS), the field level (e.g., the factory, the robots, the sensors) will be connected to a wide range of applications and services – using of vast quantities of data available to plan, monitor, re-tool and maintain, etc. – together with being ensured a higher level of reliability, as well as trust and security from a redefined security architecture.

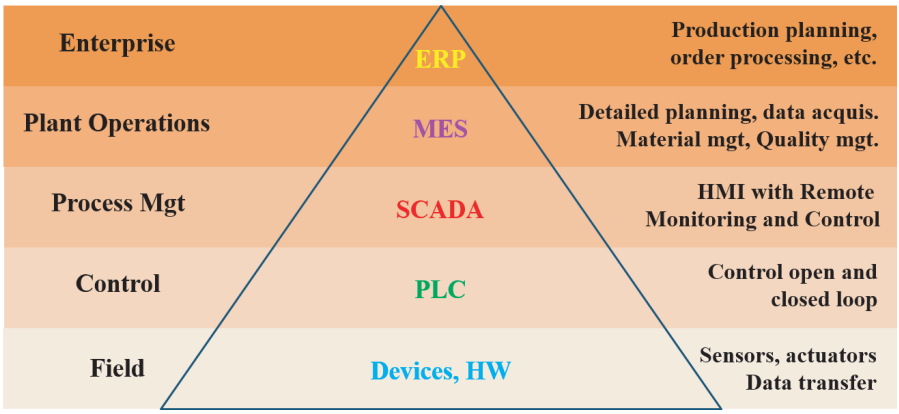


**Figure 6.3** The traditional manufacturing pyramid [6].

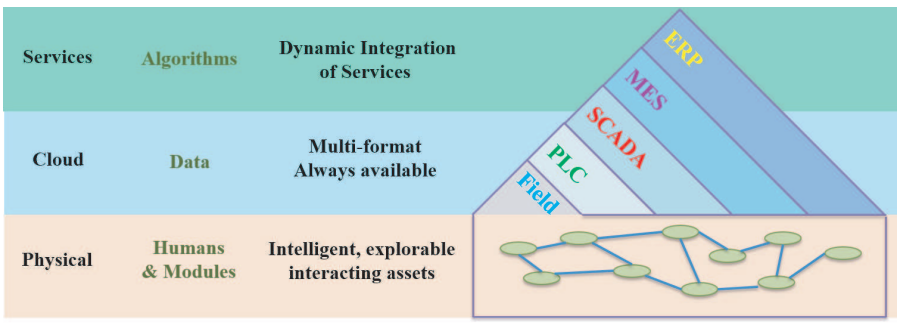


**Figure 6.4** Cyber Physical Production Systems [6].

The current model is well covered in standardization [4]. The transition towards CPPS has started and will require a major leap forward in the integration of IT (Information Technology) with OT (Operational Technology: "industrial control system and networks, hardware and software that detects or causes a change through the direct monitoring and/or control of devices, processes, and events in the enterprise [5]).

## 6.3 New Trends in IoT Standardization

IoT standardisation is a large effort with a lot of parallel undertakings. In order to address the challenges outlined above, some topics of special interest are emerging. This section intends to address some of them, in particular:

- Identification and addressing. With systems growing in size and complexity, the need to ensure that all devices are well identified and properly addressable becomes a key requirement.
- Semantic Interoperability. Many of the current systems are based on static data models. The promise of semantic interoperability is to ensure much more dynamic data models. Its challenge is to make sure that the approach is scalable and can be used in real-life IoT systems deployments.
- Security and Privacy. Though both topics are different in scope and in the solutions developed, they share a common characteristic: security and privacy are make-or-break for large IoT systems deployments and user adoption.

### 6.3.1 Identification and Addressing in IoT

In any system of interacting components, identification of these components is needed in order to ensure the correct composition and operation of the system. This applies to the assembly and commissioning of the systems, and is also relevant for system operations, especially in case of flexible and dynamic interactions between system components. In addition, identification of other entities like data types, properties, or capabilities is needed; however, that is related to semantics expressions and ontologies for such entities and not to dedicated identifiers.

IoT systems provide interaction between users and things. In order to achieve this, device components (sensors and actuators), service components, communication components, and other computing components are needed, as shown in Figure 6.5. The virtual entity plays a special role in IoT as it provides the virtual representation of things in the cyber world; it is closely linked to the thing for which identifiers are essential.

In general, an identifier is a pattern to uniquely identify a single entity (instance identifier) or a class of entities (type identifier) within a specific context. Figure 6.5 shows some examples of identifiers for IoT.

Things are at the centre of IoT and unique identification of Things is a prerequisite for IoT systems. Kevin Ashton who coined the term "Internet of Things" in 1999 linked the term with identification, specifically Radio Frequency Identification RFID. RFID is one means of identification, but many more exist, given that a *thing* could be any kind of object:

- Goods along their lifecycle from production to delivery, usage, maintenance until end of life

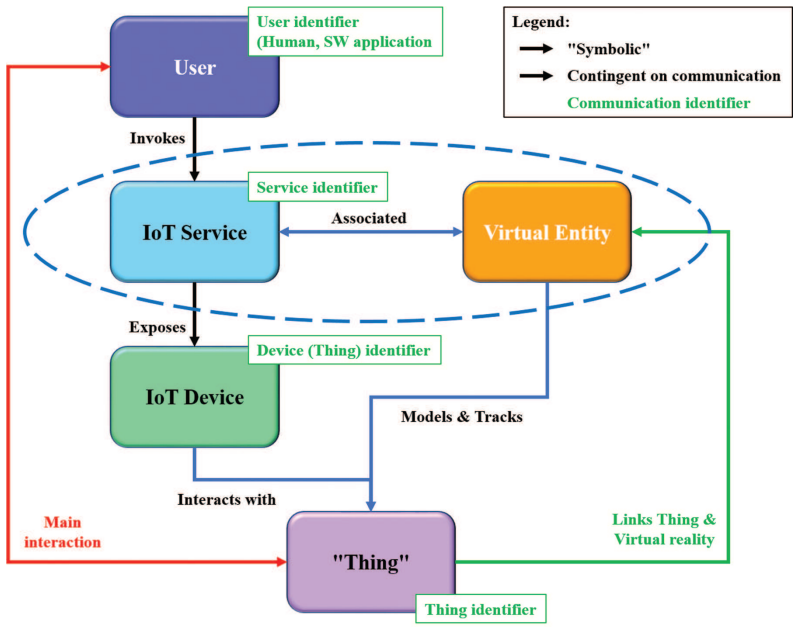


**Figure 6.5** Identifiers examples in the IoT Domain Model (according to AIOTI WG3 High Level Architecture).

- Weather conditions in a certain area
- Traffic flow at an intersection
- Vehicles and containers for tracking purposes
- Animals and field yields for smart farming applications
- Humans in case of health and fitness applications
- Digital objects like e-books, music and video files or software

Some of the things are directly connected to a communication network while others are only indirectly accessed via sensors and actuators. Identification can be based on inherent patterns of the thing itself like face recognition, fingerprints or iris scans. In most cases a specific pattern will be added to the thing for identification by technical means like printed or engraved serial numbers, bar codes, RFIDs or a pattern stored in the memory of devices. As identification applies to systems in general, many identification means already exist and are often standardized as domain specific solutions. Users may prefer different identification schemes. A property management company identifies things according to the building location, floor and room number while the producer of the thing uses its own serial number scheme.

Furthermore, the identifier might be unique within its current usage context, but new applications may result in conflicts if the same identifier is used in other systems. This raises issues of interoperability, uniqueness and linkage between identifiers which need further elaboration.

Users that interact with the things could be humans or software applications. Identification of the users is needed, especially if access is limited and/or tracked. From a security point of view, authentication requires a second step to validate the claims asserted by the identity. Privacy concerns must also be considered.

In the case of communication networks, the source and destination of the communication relationships must be identified. Here the identifiers are bound to the specific communication technology and defined as part of the standardization of the technology. IP networks use IPv4 and IPv6 addresses, Ethernet and WLAN use MAC addresses and fixed and mobile phone networks use phone numbers. Communication identifiers may not be a good fit as identifiers for *things* as the communication address of a thing may change (e.g. the communication interface or network topology may change if a different communication service provider is selected). Furthermore, some things don't have communication interfaces whilst others may have more than one (e.g. for redundancy reasons).

The AIOTI WG03 IoT Identifier task force will evaluate and classify identification needs and related requirements for IoT. As a part of this task, existing identification standards and ongoing standardization work will be examined and the applicability for the different identification needs will be elaborated. The task force has performed an open survey with various standardization bodies, research activities, industry associations, companies and individuals concerning the above topics. The results of the survey will contribute to a white paper on IoT identification needs, requirements and standards. Security, privacy and interoperability issues will also be considered and standardization gaps will be analysed. A first version of the White Paper is expected for end of 2017.

### 6.3.2 The Challenge of Semantic Interoperability

The Internet of Things (IoT) is happening all around us, not the least within the home and the (smart) city. IoT devices such as tablets, thermostats, energy meters, lamp systems, home automation, washing machines, motion sensors and personal health devices, are nowadays easily bought by consumers in the (web-) shops and are connected via the Internet to third-party service

provider's systems. In order to provide consumers of the smart home and citizens of the smart city a true and seamless IoT experience, however, the multitude of IoT devices, systems and services need to be interoperable, i.e., able to exchange information with one another and use the information so exchanged[1]. According to a recent McKinsey report, interoperability is essential to unlock 40% of the $11 trillion potential value of the IoT [7].

In the past years, standards organizations, industry alliances and consortia have focused on technical interoperability[2], which covers basic connectivity, network interoperability and syntactic interoperability, so that devices can exchange messages based on a common syntax [8]. The industry tacitly assumed that communicating devices would have a common understanding of the meaning of exchanged messages, which is true within the same ecosystem and for the same domain, as long as the design engineers and devices of the different companies speak the same technical language. However, the integration of systems for different domains with different ecosystems in the background requires a coordinated approach of the involved partners in order to agree on the meaning of the information contained in the message data structures, regardless of which communication protocol they are based on. In other words, interoperability at the technical communication level is no longer sufficient and there is a need for **semantic interoperability**.

To achieve semantic interoperability, all manufacturers involved must refer to a (set of) commonly agreed information exchange reference model(s), which not only contains the syntax, but also the meaning (semantics) of the concepts being used. By creating interoperability on the semantic level, it becomes possible to translate information to, from and between devices, thereby making it possible to control them in a standardized way. The need to address the semantics of standards has been acknowledged as an important action in the upcoming IoT standardization activities towards an interoperable and scalable solution across a global IoT ecosystem [9].

A powerful way to represent such common models and support the current standardization activities in the IoT is the use of standardized common vocabularies, or ontologies, which can formally represent the semantics

[1]Interoperability as defined by the European Information & Communications Technology Industry Association (EICTA), now called DIGITALEUROPE, also adopted by CENELEC TS 50560.

[2]Technical interoperability as defined by the GridWise Interoperability Framework, also adopted by AIOTI WG03.

of concepts exchanged by different devices and ecosystems. The Smart Appliances REFerence ontology (SAREF)[3] serves as a successful example[4].

In 2013, the European Commission launched a standardization initiative in collaboration with ETSI to create a shared semantic model of consensus to enable the missing interoperability among smart appliances. The focus of the initiative was to optimize energy management in smart buildings, as more than 40% of the total energy consumption in the European Union comes from the residential and tertiary sector of which a major part are residential houses (therefore appliances, that are inherently present in the buildings' ecosystem can be considered the main culprits of this high energy consumption). TNO was invited to lead this initiative and carry out the work in close collaboration with smart appliances manufacturers and ETSI (Jan 2014–Apr 2015). The resulting semantic model – SAREF – was standardized by ETSI in November 2015 (TS 103 264) [10]. As confirmed in [9], SAREF is a first ontology standard in the IoT ecosystem, and sets a template and a base for the development of similar standards for the other verticals to unlock the full potential of IoT.

SAREF is to be considered as an addition to existing communication protocols to enable the translation of information coming from existing (and future) protocols to and from all other protocols that are referenced to SAREF. As an example, a SAREF-enriched home gateway associates devices in a home with each other and with different service providers. The role of the network operator is to enrich their home gateways with a SAREF-based execution environment, as well as guarding the privacy of customers (as the home gateway has become an omniscient device). A study recently launched by the European Commission (SMART 2016/0082)[5] will demonstrate an implementation for interoperability for Demand Side Flexibility that uses SAREF and its extension SAREF for Energy to enrich a home gateway with additional semantics to be embedded in e.g. oneM2M resources for transportation at the underlying technical level.

Since its first release in 2015, SAREF has gradually grown into a modular network of standardized semantic models[6] that continues to evolve systematically within the SmartM2M TC in ETSI [11]. The first 3 extensions that have been standardised are SAREF for Energy [12], SAREF for Environment [13]

[3] http://w3id.org/saref

[4] https://ec.europa.eu/digital-agenda/en/blog/new-standard-smart-appliances-smart-home

[5] https://ec.europa.eu/digital-single-market/en/news/study-ensuring-interoperability-enabling-demand-side-flexibility-smart-20160082

[6] www.ec.europa.eu/digital-single-market/news-redirect/57284

and SAREF for Buildings [14] and a multitude of other domains such as Smart Cities, Smart AgriFood, Smart Industry and Manufacturing, Automotive, eHealth/Ageing-well and Wearables, are on the roadmap turning SAREF into "Smart Anything REFerence ontology", which enables better integration of semantic data from various vertical domains in the IoT.

Another relevant standardization initiative on semantic interoperability for the IoT is the Web of Things[7] (WoT) promoted by the World Wide Web Consortium (W3C) as a way to combine the Internet of Things with the Web of data in order to counter the fragmentation of the IoT through standard complementary building blocks (e.g., metadata and APIs) that enable easy integration across IoT platforms and application domains. In February 2017, W3C launched a new Web of Things Working Group[8] – as an evolution of the Interest Group that has been active in the past years – to develop initial standards for the Web of Things, tasked with the goal to counter fragmentation, reduce the costs of development, lessen the risks to both investors and customers, and encourage exponential growth in the market for IoT devices and services. The proposition of the W3C Web of Things Working Group is to describe things in the IoT in terms of actions, properties, events and metadata (as those are common aspects shared by the vast majority of connected devices), and independent of their underlying IT platforms, trying to complement the work that different organizations are doing, developing cross-domain Linked Data vocabularies, serialization formats, and APIs. An overview for implementers of the W3C WoT building blocks is published in [15], which provides an unofficial draft of the current WoT practices in a single location. While [15] is not a technical specification, it aims at helping implementers to get an overview of the WoT building blocks and includes reports from past PlugFests and follow-up discussions, which explain the rationale behind the WoT current practices.

### 6.3.3 Addressing Security and Privacy in IoT

#### Trust, Data Protection and Resilience in IoT as Key Components

Technology changes the world at a fast pace and massive scale. Digital technology makes innovation possible in our society and economy. Cloud computing, data analytics, AI and Internet of Things (IoT) will expedite this pace by hyper-connecting people, organizations and data with billions

[7] http://www.w3.org/WoT/

[8] https://www.w3.org/WoT/WG/

of objects. In such diverse physical-cyber, cyber respectively cyber-physical ecosystems, it remains to be seen how demand side, supply side, policy makers, law enforcement, authorities as well as end-users and other stakeholders are going to understand, build, deploy and use IoT ecosystems and its related products, systems and services. Trust remains one of the main challenges of any technology, and given (a) the data-centric nature of IoT products, systems and services, (b) the fact that such data is to a large extent highly sensitive, personal or otherwise valuable to individuals, companies and organisations, and (c) the fact that digital technologies are nowadays a need to have, and individuals, companies and organisations fully rely – and need to be able to fully rely – on these, security and resilience as well as privacy and data protection are key components to trustworthiness. Therewith, Trust, Data Protection and Resilience can be seen as key enablers to build, shape, monitor and optimize trust and with that successful engagement by and with all relevant stakeholders.

### Main Categories in Human-Centric IoT

There are several ways to segment and therewith make more transparent and understandable any technology, including IoT. Without such segmentation and classification, it is quite difficult to get on the same page and ensure that interdisciplinary collaboration with stakeholders with multiple backgrounds and expertise on topics such as design, engineering, architectures, governance, risk management, impact-based measures, user-adoption, standards and other policies are focussed and fruitful, especially when addressing trust, security, privacy and (personal) data protection. This obviously, while taking into account, that at the end, these segments need to be and are integrated, hyper-connected and interoperable as detailed in the other paragraphs of this Chapter. A way of segmenting IoT in four main categories is the following:

A. **Data** (including data, information and knowledge)
B. **Algorithms** (including as code, software and services)
C. **Machines** (including devices and hardware systems)
D. **Computing** (including high performance computing, systems and communication of any kind)

In Human-centric IoT, the above main categories are of course each complemented with that human-centric dimension, including for instance human rights, consumer rights, user-interfaces, identity, authentication and the Human Factor, even when there is a purely M2M layer or subdomain involved.

### Symbiosis between Security and Data Protection

There is no data protection without security. This goes for both personal data as well as any non-personal data. For instance, personal data protection and privacy is as much about security as it is about data management. Through IoT products, systems and services, organizations create, collect, process, derive, archive and (ideally and to the extent permitted) delete large amounts of data. As part of this lifecycle, digital data is also transmitted, exchanged and otherwise processed around the world, any time, (almost) any place. In short: data likes to travel. Therefore, information security nowadays is not about data ownership but about data control, access, use and digital rights management. Article 29 Working Party, the pan-European body of all data protection authorities ('DPAs') actually have recently stated this as well[9]. With appropriate and dynamic technical and organisational security measures in place it is possible to achieve a dynamic yet appropriate level of personal data protection. In other words, security is a necessary prerequisite for privacy and (personal) data protection. As a consequence, both security and privacy provide essential building blocks for trustworthiness in digital technologies.

### Conflict between Human-centric, Data-centric and Process-oriented

More and more organizations are picking up speed to explore how to benefit from digital technology, while mitigating associated risk. From an information security perspective, for more than a decade organisations (whether provider or customer) have taken steps and implemented organizational and technical measures in order to seek and obtain compliance and assurance regarding various international information security standards, such as the ISO 27000 series, SSAE 16 SOC series. However, with the user-centric General Data Protection Regulation (GDPR), just being compliant to those information security standards will not be enough from a GDPR perspective. Any organisation active within the European Union must now apply state of the art security measures (both technical and organizational) where (i) the related cost of implementation, (ii) the purposes of personal data processing

[9]BEREC Workshop on Enabling the Internet of Things of 1 February 2017: http://berec.europa.eu/eng/events/berec_events_2017/151-berec-workshop-on-enabling-the-internet-of-things

and (iii) the impact on the rights and freedoms of the data subject (also good, bad and worst case scenarios) need to be taken into account, whether one is either a data controller, co-controller, processor or co-processor. We call this the appropriate dynamic accountability (ADA) formula:

*State of the art security – Costs – Purposes + Impact*

It is important to note that other than where current information security standards aim at 'achieving continual improvement', the GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to continuously meet the ADA formula.

An organisation will not be compliant with EU rules unless it follows these user-centric and impact-based requirements. Hence, we are now in an era that where standards traditionally focus on technology-centric processes and controls, new regulation such as the GDPR – soon to be followed by the upcoming ePrivacy Regulation – is user-centric, data-centric and impact-driven. This a new phenomenon and will need to be assessed, addressed and implemented, as the GDPR is a mandatory regulation and one would want to avoid those hefty penalties, which for large enterprise can amount to several billions of Euros. Having analyzed the state of play of international information security standards and its frameworks, we can safely conclude that GDPR raises the bar for personal data protection and related security by introducing user-centric, specific data-centric and impact-based requirements as opposed to process- and technology-oriented frameworks of standards. Being compliant in the traditional way where compliance refers to linear and binary compliancy and assurance is not good enough anymore. Technology has become a highly-regulated domain in itself. The good news is that, once an organization does have those dynamic and appropriate technical and organizational measures in place, it will significantly increase trustworthiness towards customers, users, authorities and other stakeholders, and demonstrates next generation readiness.

### Principle-Based Security and Privacy

Combining the vast domain of cybersecurity, security and safety, with the even vaster domain of IoT is a necessity, yet quite complex and difficult to grasp and comprehend.

In order to come to workable and actionable frameworks and models to address the pre-requisite trust components of Security and Privacy in IoT,

come to the mandatory level of appropriate accountability (as for instance set forth in the GDPR) and enable organisations in any sector, including public and private, to assess which technical and organisational security measures it needs to consider and implement, various organisations have set up committees, taskforces and workshops. In 2016 and first part of 2017, this has resulted in about 30 papers that describe such recommendations, frameworks and other guidelines on state of the art level in Security in IoT.

The IoT Unit of the European Commission, together with relevant stakeholders including AIOTI and key IoT industrial, demand side and policy players have organised two workshops the past year, including in June 2016 the AIOTI Workshop on Security & Privacy in IoT[10] [17] and the European Commission's Workshop on Security & Privacy in IoT of 13 January 2017 [18], resulting in recommendations, principles and requirements as set forth in its respective reports in order to enable and facilitate the increase of security, privacy, identify minimum baseline principles and requirements for any IoT product, service or system, and therewith trust in human-centric IoT.

One structures and analyse these in the perspective of the following layers and dimensions, where dimensions may be relevant in one, more or all layers:

| LAYERS | DIMENSIONS |
|---|---|
| 1. Service | A. User/Human Factor |
| 2. Software/Application | B. Data |
| 3. Hardware | C. Authentication |
| 4. Infrastructure/Network | |

The two reports [17] and [18] result in a structured set of about 50 principles and requirements, and also makes visible where appropriate maturity of those principles have been reached, and where possible gaps and points of attention can be identified and how to address those.

A sample of the structured overview, in this case of the hardware layer, of the so-called State of the Art (SOTA) Layered Plotting Methodology is set forth below. The full version of the total overview hereof can be found at www.arthurslegal.com/IoT and www.aioti.eu.

[10] AIOTI Workshop on Security and Privacy in IoT of 16 June 2016: https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week

**HARDWARE**

- **Security principles:**
  - *High-level baseline:* High level baseline should be applied when safety is at stake or critical infrastructure or national safety can be materially impacted.
  - *Separate safety and security:* Manufacturers have to implement and validate safety principles, separately from security principles.
  - *Security rationale:* Manufacturers should be required to provide explanation of implemented security measures related to expected security risks from any designer of IoT device, auditable by independent third party.
  - *Security evaluation:* Manufacturers should specify precisely capabilities of device of a particular type. This could help to manage liability and evolutivity on system level.
  - *Security levels:* The industry should make use of the security scale 0 – 4 fit to the market understanding.
  - *Sustainability:* Manufacturers should ensure that connected devices as well as any IoT component as defined above are durable and maintained as per its purpose, context and respective life cycle.
  - *Assurance:* Component and system suppliers need to be prepared for security monitoring and system maintenance over the entire life cycle and need to provide end of life guarantees for vulnerabilities notifications, updates, patches and support.
- **Certification and Labelling:**
  - *Certification:* Device manufacturers should test devices and make use of existing, proven certifications recognized as state-of-the-art based on assessed risk level. Additional introduction of a classification system to certify devices for use in particular use case scenarios depending on the level of risk should be encouraged.
  - *Trusted IoT label:* Labels such as the 'Energy efficiency label' of appliances should give a baseline requirement of protection based on the level of assurances and robustness, and should be used to classify individual IoT devices.
- **Secure Performance and Functionality:**
  - *Defined functions:* Manufacturers should ensure that IoT devices are only able to perform documented functions, particular for the device/service.
  - *Secure interface points:* Manufacturers should identify and secure interface points also to reduce the risk of security breach.

## 6.4 Gaps in IoT Standardisation

Despite a large number of available standards on which to build IoT systems, the development of large-scale interoperable solutions may not fully guaranteed, when some elements in the IoT standards landscape are missing. Such elements, commonly referred to as "gaps", are subject of a number of analysis that aim at identifying them with the intent to ensure that their resolution

can be handled by the IoT community, in particular the standardisation community.

### 6.4.1 Identifying IoT Standards Gaps

Though the gaps related to missing technologies are the most commonly thought of, several categories of gaps can be identified and need to be equally addressed. In the work of ETSI STF 505 [15], three categories of gaps have been addressed:

- Technology gaps with examples such as communications paradigms, data models or ontologies, or software availability.
- Societal gaps with examples such as privacy, energy consumption, or ease of use.
- Business gaps with examples such as silo-ed applications, incomplete value chains, or missing investment.

The perceived criticality of the gaps may be different depending on the role of an actor in standardisation. The Table 6.1 below is listing some of the major gaps identified in [15]. In addition to their nature and type, it also provides a

**Table 6.1** Some standards gaps 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 | Med |
| 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 |

*Source:* CREATE-IoT.

view of their criticality that comes from an early evaluation by the European Large Scale Pilots (LSPs). This evaluation is one possible view, and it may differ if the opinion of other actors (e.g., users, service providers) is requested.

The characterization of gaps, in particular their type, their scope, the difficulties they create, and other appropriate descriptions is a first step. No listing of gaps is final and their identification will remain a work-in-progress in the IoT Standardisation community.

### 6.4.2 Bridging the Standardisation Gaps

As long as the gaps are existing, their resolution will have to be, one way or the other, taken into account of the IoT standardisation, in particular the SDOs/SSOs. The mapping of identified gaps on an architectural framework (such as the AIOTI HLA) creates a reference that can be understood by the IoT community and, in particular, that can be related to other frameworks e.g., those developed in other organizations, for instance in Standards Setting Organisations.

The Table 6.2 below shows a potential mapping of the above listed gaps on the AIOTI layered High Level Architecture (HLA). This is an indication

**Table 6.2** Standards 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 |

(*Continued*)

**Table 6.2** Continued

| Gap | Impact |
|---|---|
| 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 |

of the type of effort needed for the resolution of a gap and also of the kind of SDO/SSO that can address it in a relevant manner.

The work program of IoT standardisation is, by nature, not predictable. However, some considerations may be taken into account in order to ensure that new standards developments will foster collaboration and reduce fragmentation:

- Solutions should be transversal, with "horizontal layer" standards rather than "vertical domain" specific;
- Interoperability will be essential for the deployment of the IoT systems, to ensure seamless communication and seamless flow of data across sectors and value chains;
- New interoperability solutions should seek for integration into "horizontal" frameworks (e.g., oneM2M) rather than provide point solutions;
- Effective security and privacy solutions are key to user acceptance and should be based on global holistic approaches (e.g., security by design, privacy by design) that involve all the actors (and not just the specialists);
- Solutions are often not just technical solutions and existing standards may have to address non-technical issues.

## 6.5 Conclusions

As a technology, IoT is not isolated and it should work in conjunction with the development and deployment of other new technologies such as 5G, Big-Data, Cybersecurity or Artificial Intelligence. Moreover, the IoT systems should be more and more integrated with the complex systems of practically all of the very large vertical domains of today: Industry, Manufacturing, Robotics, Aeronautics, Intelligent Transport Systems, Maritime, Smart Living, eHealth, Farm & Food, Energy, Buildings, Environment, Cities, just to name a few.

The road to the Internet of Things (and even more to the Internet of Everything) is going to take time to travel. The role of IoT standardisation in the emergence of IoT on a largescale will be key. One of its major challenges is to help break the silos and support the integration of new, currently unforeseen, cross domain, federated applications based on open, interoperable solutions.

One clear lesson can be drawn already from the analysis of standards gaps and the definition of the program to address them: no single SDO or Alliance can address it with a one-fits-all solution. The large-scale deployment of a trusted and reliable IoT is going to be a global collaborative effort across standardisation organisations.

## References

[1] European Commission communication on "ICT Standardisation Priorities for the Digital Single Market", COM(2016) 176 final, Brussels, 19.4.2016

[2] AIOTI WG03 Report: "IoT LSP Standard Framework Concepts Release 2.7" February 2017; https://docbox.etsi.org/SmartM2M/Open/AIOTI/

[3] AIOTI WG03 Report: "High Level Architecture (HLA) Release 2.1" September 2016; https://docbox.etsi.org/SmartM2M/Open/AIOTI/

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

[5] O. Vermesan and P. Friess (Eds.). Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds, Section 3.3.7., ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016.

[6] O. Vermesan and P. Friess (Eds.). Building the Hyperconnected Society – IoT Research and Innovation Value Chains, Ecosystems and Markets, ISBN: 978-87-93237-99-5, River Publishers, Gistrup, 2015.

[7] McKinsey Global Institute, The Internet of Things: Mapping the value beyond the hype (2015), https://www.mckinsey.de/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf

[8] AIOTI WG03 – IoT Standardisation: "Semantic Interoperability" Release 2.0 (2015), https://docbox.etsi.org/smartM2M/Open/AIOTI/!!20151014Deliverables/AIOTI_WG3_SemanticInterop_Release_2_0a.pdf

[9] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs: GROW – Rolling Plan for ICT Standardisation 2016, http://ec.europa.eu/DocsRoom/documents/14681/attachments/1/translations/en/renditions/native

[10] ETSI SAREF TS 103 264 SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping version 2.2.1 (2017), http://www.etsi.org/deliver/etsi_ts/103200_103299/103264/02.01.01_60/ts_103264v020101p.pdf

[11] ETSI TR 103 411 SmartM2M; Smart Appliances; SAREF extension investigation (2017), http://www.etsi.org/deliver/etsi_tr/103400_103499/103411/01.01.01_60/tr_103411v010101p.pdf

[12] ETSI SAREF for Energy (SAREF4ENER) TS 103 410-1 SmartM2M; Smart Appliances Extension to SAREF; Part 1: Energy Domain (2017), http://www.etsi.org/deliver/etsi_ts/103400_103499/10341001/01.01.01_60/ts_10341001v010101p.pdf

[13] ETSI SAREF for Environment (SAREF4ENVI): TS 103 410-2 SmartM2M; Smart Appliances Extension to SAREF; Part 2: Environment Domain (2017), http://www.etsi.org/deliver/etsi_ts/103400_103499/10341002/01.01.01_60/ts_10341002v010101p.pdf

[14] ETSI SAREF for Building (SAREF4BLDG): TS 103 410-3 SmartM2M; Smart Appliances Extension to SAREF; Part 3: Building Domain (2017), http://www.etsi.org/deliver/etsi_ts/103400_103499/10341002/01.01.01_60/ts_10341002v010101p.pdf

[15] Web of Things (WoT) Interest Group (IG), WoT Current Practices (2017), http://w3c.github.io/wot/current-practices/wot-practices.html

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

[17] AIOTI Workshop on Security and Privacy, 16 June 2016; Final Report Workshop on Security and Privacy in IoT: https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

[18] Final Report European Commission of 13 January Workshop on Internet of Things Privacy and Security: https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report