ILNAS

# INTERNET OF THINGS (IoT)

## NATIONAL TECHNICAL STANDARDIZATION REPORT

Version 1.0 · June 2020

ANEC

COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRIAL
432432
675453
875654
23466
COLLABORATION
PARTNER
OFFICE

# INTERNET OF THINGS (IoT)

## NATIONAL TECHNICAL STANDARDIZATION REPORT

Version 1.0 · June 2020

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation et
l'Economie de la Connaissance

# Foreword

The proliferation of connected devices in our world is participating in making the Internet of Things (IoT) an unavoidable reality in an economy that is ever more driven by data and their exploitation for the benefit of our society. However, the multiplicity of technologies in use, the needs for interoperability, for security, for trustworthiness are some examples perfectly illustrating the vital role of technical standardization to answer these challenges and to fully unleash the potential of the IoT. Indeed, technical standardization and standards are nowadays essential to support worldwide economic development. All sectors of the economy rely on standards in their daily activities, whether it be for developing products and services respecting recognized good practices, for the governance of their business, for the assessment of the quality or safety of their products, etc. This observation is particularly true for the Information and Communication Technology (ICT) sector, where all developments lead to a smarter world where all “things” become connected, able to communicate between each other, to collect information and to use the result of a wider knowledge base to offer customized solutions in all aspects of our lives. In this context, the use of technical standards is a prerequisite to ensure the interoperability between technical solutions, to support the integration of multiple data sources of Smart ICT technologies or to guarantee the security and safety of the next digital world.

The Grand-Duchy of Luxembourg has clearly understood the importance of the digital economy and has engaged since several years in an ambitious innovation strategy for the ICT sector, considering that the development of a trusted and sustainable economy will notably rely on a data-driven approach. The *“Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services”* (ILNAS) fully supports this development through the “Luxembourg Standardization Strategy 2020-2030”[1], signed by the Minister of the Economy, which identifies the ICT sector as one of the growth sectors, with the construction and aerospace sectors. In this context, ILNAS has developed the “Luxembourg’s policy on ICT technical standardization 2020-2025”[2], which aims to promote and strengthen the use of technical standards by the national market, to reinforce the positioning of Luxembourg in the global ICT standardization landscape, particularly through a stronger involvement of national stakeholders in the relevant standardization technical committees, and to pursue the development of research and education programs in the Smart ICT standardization area. In order to carry out this policy, ILNAS benefits notably from the support of the Economic Interest Group *“Agence pour la Normalisation et l’Économie de la Connaissance”* (ANEC GIE – Standardization Department).

ILNAS is already actively involved in the domain of education about standardization, and two educational programs have been developed through a fruitful collaboration with the University of Luxembourg. The first one was the University certificate *“Smart ICT for Business Innovation”* which was delivered twice (2015-2016 and 2018-2019) and which has led to the creation of a new Master’s degree *“Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions”*[3] that will start in September 2020. This diploma will allow national stakeholders to gain familiarity with Smart Secure ICT technologies, notably from a standardization and Technopreneurship point of view, in order to seize the future business opportunities offered in this innovative area.

[1] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

[2] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/policy-on-ict-technical-standardization-2020-2025.pdf

[3] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/master-mtech.html

In parallel, ILNAS has also launched different research activities in the Smart Secure ICT domain, which are directly contributing to the success of its education about standardization developments. On the one hand, ILNAS and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg launched a research program "*Technical Standardisation for Trusted Use in the Field of Smart ICT*" (2017-2020)[4], involving three PhD students respectively working on Cloud Computing, Internet of Things and Big Data/Artificial Intelligence. This program largely considers technical standardization and digital trust aspects of these Smart ICT technologies and has already resulted in the publication of a White Paper “Data Protection and Privacy in Smart ICT”[5] in October 2018 and three technical reports[6] , in October 2019, on the gaps between scientific research and technical standardization in the three aforementioned Smart ICT areas. On the other hand, ILNAS has published a series of White Papers and reports in order to inform the market about technical standardization developments in Smart ICT. In this framework, White Papers on “Internet of Things[7] , “Blockchain and Distributed Ledger Technologies”[8] or “Digital Trust for Smart ICT”[9] have been published in recent years.

This National Technical Standardization Report on Internet of Things is intended to further inform the national market about the relevant IoT standardization developments, in the continuation of the White Paper on IoT published in 2018 with the support of the Ministry of the Economy. It provides updated information on the technical standardization landscape of IoT and gives some concrete examples of IoT implementations in different economic sectors, illustrated by use cases involving national stakeholders. With this report, ILNAS aims to encourage the involvement of the market in the IoT standards development process, highlighting an overview of different opportunities offered, for the benefit of the national economy.

**Jean-Marie REIFF**
Director
ILNAS

**Jean-Philippe HUMBERT**
Deputy Director
ILNAS

[4] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html

[5] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf

[6] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/TR-Smart-ICT-Gap-Analysis-SR-TS-ILNAS-UL.pdf

[7] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-iot.html

[8] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html

[9] https://portail-qualite.public.lu/dam-assets/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf

# Acknowledgements

The working-group (WG) involved to prepare this national technical standardization report is:

| Name of the contributor | Institution/Organization |
|---|---|
| Mr. Jean-Marie REIFF | ILNAS |
| Dr. Jean-Philippe HUMBERT | ILNAS |
| Mr. Nicolas DOMENJOUD | ILNAS |
| Dr. Jean LANCRENON | ANEC GIE |
| Dr. Shyam WAGLE | ANEC GIE |
| Dr. Johnatan PECERO | ANEC GIE |

This working-group would like to thank all the people who have helped and offered their support, in different ways, in developing this report.

- Mr. Frank ZIMMER, SES, Luxembourg
- Dr. Konstantinos LIOLIS, SES, Luxembourg
- Dr. Christos POLITIS, SES, Luxembourg
- Dr. Symeon CHATZINOTAS, University of Luxembourg
- Dr. Francesco VITI, University of Luxembourg
- Dr. Nicola MATURO, University of Luxembourg
- Dr. Ridha SOUA, University of Luxembourg
- Mr. Oltjon KODHELI, University of Luxembourg
- Dr. Maria Rita PALATTELLA, LIST, Luxembourg

# Table of contents

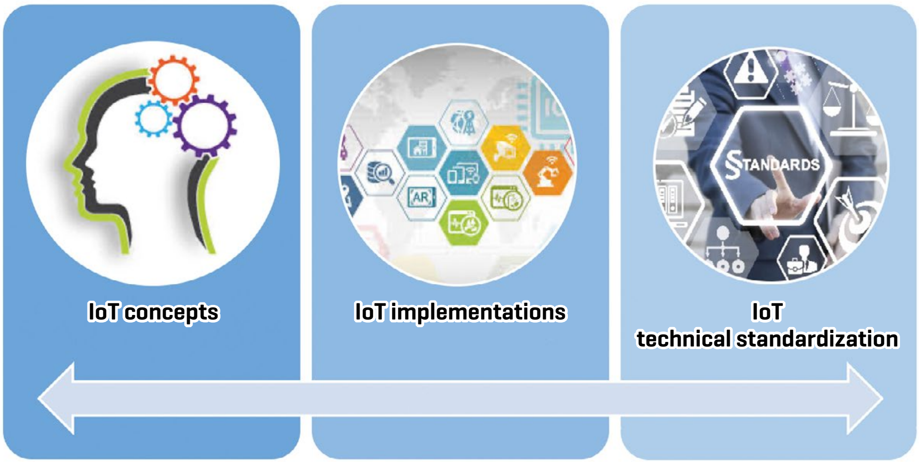
# List of Figures

# List of Tables

# Introduction

ILNAS – ANEC GIE, together with the support of the Ministry of the Economy, published a White Paper – Internet of Things (IoT) in July 2018 [1]. This White Paper mainly overviewed the concept of IoT technology, its economic impact, and ongoing technical standardization activities. Considering national public and private initiatives in IoT related implementations in Luxembourg, a study of these implementations from different perspectives, particularly those of operational efficiency and technical standardization, appears crucial to make national stakeholders aware of standardization opportunities in this sector. This National Technical Standardization Report, with an analysis of current IoT-related issues across various sectors, highlights how technical standardization is expected to help them in their IoT technology implementation plan.

In this context, this National Technical Standardization Report on Internet of Things (IoT) has been developed intending to provide a study of national-based initiatives/examples across various sectors of IoT applications linked with related standardization initiatives.



This report is broadly divided into three sections: the IoT technical landscape (overview of the IoT concepts with recent technological trends), a study of examples of IoT applications, and IoT technical standardization. In particular, these three sections are considered from three different perspectives: IoT concepts, IoT implementations and IoT technical standardization. A detailed description of this report along these three perspectives is provided as follows:

## IoT concepts

- **Chapter 1**: This chapter provides an overview of IoT technology. It extends the White Paper – Internet of Things (IoT) published in July 2018 [1], focusing more on data flow in an IoT architecture, and including trends in IoT technology as well as efforts towards secure IoT. In particular, this chapter identifies some major complexities, from the perspective of IoT deployment following recent trends of this technology, which are further detailed in Chapter 3 to see how standards development organizations and other alliances are working towards minimizing such complexities.

## IoT implementations

- **Chapter 2**: This chapter is dedicated to providing a study of national IoT-related initiatives/examples across selected sectors. In general, IoT application domains can be divided into two categories: horizontal and vertical [2]. The horizontal sector is essentially that of *telecommunications,* while *smart buildings, smart homes, smart manufacturing, connected vehicles, smart health, smart energy, smart cities, smart agriculture,* to name but a few, constitute the vertical sectors of IoT application domains. To represent both horizontal and vertical domains, *satellite and related connectivity for IoT* (under telecommunication and related sectors), and *connected vehicles* (as a vertical domain) are considered in this report:

    - **Use case sector 1: Satellite and related connectivity for IoT**

      The goal of this section is to include an analysis of a few selected national examples to cover connectivity and related activities area to support IoT-based implementations across this sector. It includes four projects, namely Light-Weight Application and Transport Protocols For Future M2M Applications (M2MSAT), Communication Algorithms for End-to-End Satellite-IoT (SATIOT), Demonstrator for Satellite-Terrestrial Integration in the 5G Context (SATis5), and 5G Verticals Innovation Infrastructure (5G-VINNI) in collaboration with several national/international organizations including SES TechCom S.A., Luxembourg.

    - **Use case sector 2: Connected vehicles**

      The goal of this section is to include an analysis of a few selected national examples to cover the connected vehicle sector including vehicle-to-Infrastructure (V2I) and vice-versa as well as intelligent transport systems to support IoT-based implementations across this sector. It includes two projects, namely the Electrified Cooperative Bus System (eCoBus) project and the Multimodal MoBility Assistance (MAMBA) project, in collaboration with several national/international organizations including the University of Luxembourg.

## IoT technical standardization

- **Chapter 3**: The goal of this chapter is to make readers aware of how standards development organizations and different alliances are addressing the problems of minimizing IoT deployment complexities identified in Chapter 1. At first, this chapter recalls the concepts of standards and standardization, along with a brief introduction of standardization bodies and alliances at the international and European level. The national context is also highlighted, providing information about Luxembourg's National Mirror Committee for the technical committee ISO/IEC JTC 1/SC 41 on IoT and related technologies, ILNAS' activities and related support provided by ILNAS & ANEC GIE. In addition to this, the technical standardization landscape related to IoT technology is also provided, giving highlights of the efforts of several standardization bodies and alliances towards IoT technical standardization. Finally, it provides the status of published standards as well as ongoing standards developed by different standardization bodies and alliances, mainly from the perspectives of complexities and use cases mentioned in Chapter 1 and Chapter 2.

# 1

# Internet of Things: Technical landscape

# 1. Internet of Things: Technical landscape

This chapter of the national technical standardization report extends the concept of the IoT provided in ILNAS' IoT White Paper [1], which provided the basics of the IoT and its driving technologies, global challenges in the domain, and economic as well as business prospects. Finally, this White Paper did a systematic review of the ongoing technical standardization at the national, European and international levels. In the context of the increasing number of connected devices to the IoT and the exponential growth in data consumption demands, the need for complex analytics to realize the true potential of a connected society [3] is growing; this chapter provides the reader with basics of IoT data insights, ranging from data generation to data analysis, in order to know how IoT data are assets of any organization. At the same time, it provides insight on how the IoT carries inherent security, storage and processing risks from data generation to data analysis, as well as creates other new challenges to professionals in the diverse IoT world. In this context, the background of IoT cybersecurity objectives, risks and threats is also discussed in this chapter to inform stakeholders who are interested to be a part of the IoT ecosystem. This chapter is organized as follows: Section 1.1 provides an overview of the IoT paradigm, giving the relations between components, systems and IoT environments; Section 1.2 provides basics on data principles, value and management in the IoT; Section 1.3 provides the current driving technologies of the IoT compared with previous technologies; Section 1.4 shows the complexities in IoT deployment from technical, business, and societal perspectives. This section further introduces the reader to the concept of how cybersecurity is emerging as a leading concern for implementers.

## 1.1 IoT paradigm

The IoT refers to business processes and applications of sensed data, information and content generated from an interconnected world by the means of connected devices that exist in the internet infrastructure [1]. In the IoT ecosystem, systems are composed of networked entities. The entities could be IoT devices, information resources or people, which can be easily interconnected to interact with the physical world. Basically, there are two essential concepts in the IoT [1], [4]:

- The presence of sensors, and/or actuators, which interact with the physical world;
- The capacity to support networked relationships between components.

The IoT can be broken down largely into major three concepts: IoT components, IoT systems and IoT environments (see Figure 1):

- **IoT components:** These are the basic building blocks of the IoT system. They interact with each other to form a system and achieve one or more goals performing some function that is necessary within that system [1]. The IoT components must have at least the following capabilities:
  - Some combination of: sensing, actuating, application interface, data collecting, processing, data storing and transferring, human-user interface; and
  - At least one network interface that can be connected in a many-to-many network [4].
- **IoT systems:** A system is a combination of interacting elements formed to achieve certain goals. ISO/IEC 15288:2015 [5] defines a system as a combination of interacting elements organized to achieve one or more stated purposes. An IoT system is a system composed of networked IoT components that interacts with a physical entity through sensors and/or actuators within those components. Such IoT systems are also part of an IoT environment.
- **IoT environments:** An IoT environment is composed of IoT systems and IoT components. In other words, it is a set of IoT components and supporting technologies that are interconnected together and can be built into IoT systems. The Internet is an example of an IoT environment.

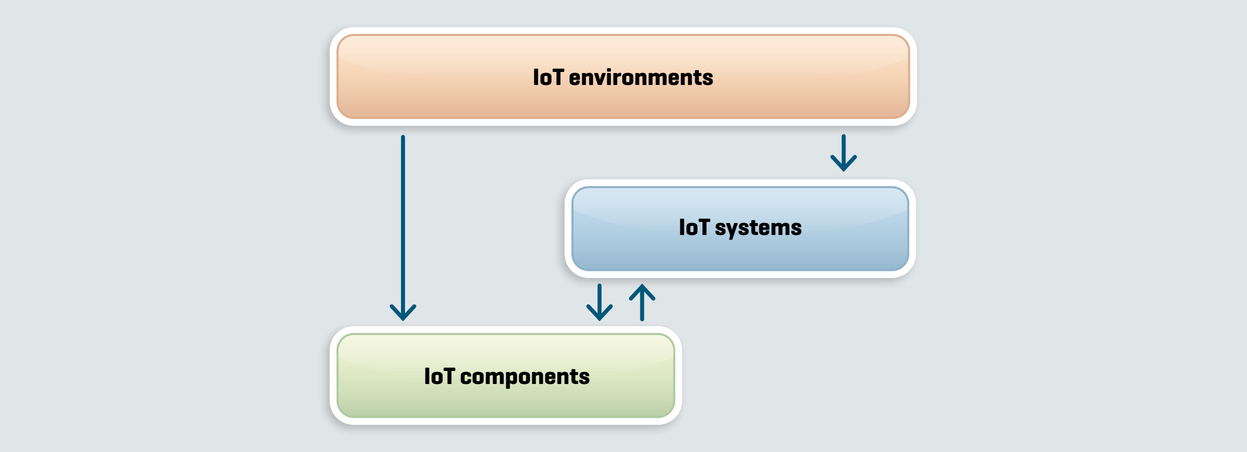


*Figure 1: Relation between IoT environments, systems, and components*

As the IoT is a key source of data and that data gives potential insights to its stakeholders, the following section is intended to provide the values of data in general and to substantiate how it is important in the IoT ecosystem, from data generation to application for business insight.

## 1.2 IoT data insights

The IoT provides open access to data from connected devices in the IoT environment by third party applications, which is the source of valuable insights to stakeholders [6]. The devices themselves range from road sensors to vehicles to energy meters to washing machines to even wearables such as fitness trackers. Any device connected to the IoT can generate and share meaningful data itself, even concerning its environment and use. This data most often is aggregated in the cloud (refer to the data flow in an IoT environment -- from the data collection layer to the process, management and utilization layer [1]), where it is further processed to yield actionable knowledge for business, government authorities, municipalities or even individuals.

Data, in its most common understanding, is a collection of numbers or characters that can be measured, collected, analyzed and presented in various formats, such as in tables, charts, graphs, histograms, etc. [7]. Information or knowledge exists on this data in some form, but this form is only accessible through appropriate processing, and is only exploitable with the correct wisdom. The concepts of data, information, knowledge, and wisdom are closely related, but distinct from each other. Data itself has little value, as it should be processed and contextualized to get an actionable insights. The DIKW model or DIKW pyramid [8] is a widely-used model to represent the relationships among data (the “D”), information (the “I”), knowledge (the “K”), and wisdom (the “W”). Figure 2 shows how data contain various information and can have higher value with the use of knowledge and wisdom. Its value increases with the intervention of computers and humans adding knowledge and wisdom.

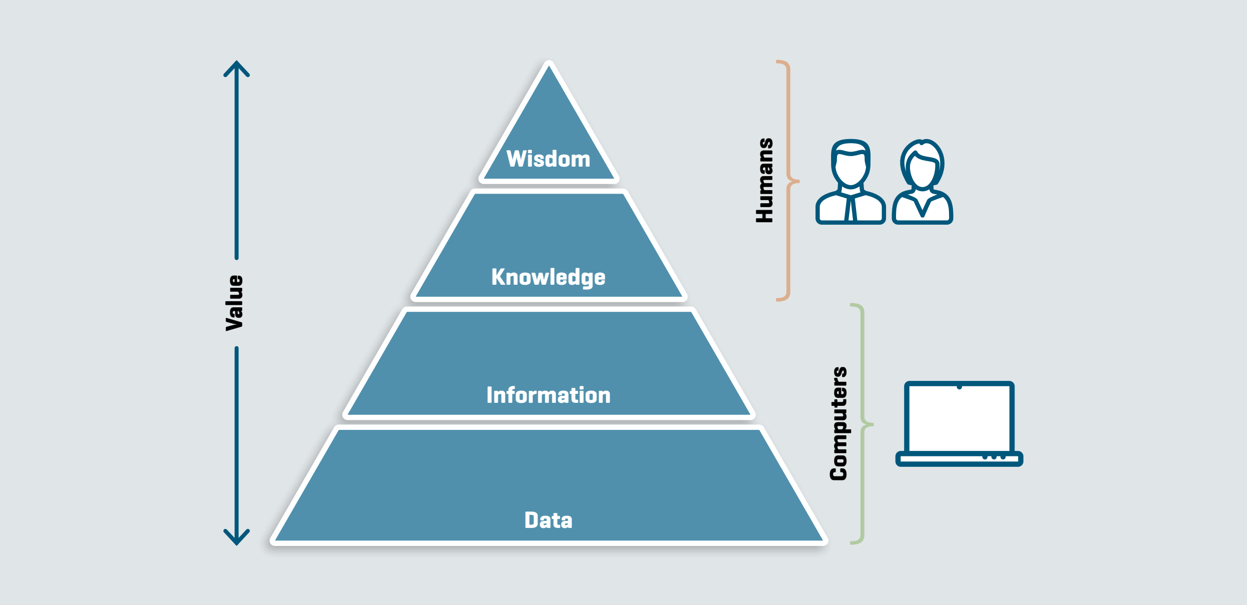


*Figure 2: DIKW model [8]*

As the use of connected devices by consumers in the IoT increases, there will be an exponential growth of data to be gathered to the cloud. This translates to the need of more discerning choices to solve the issues of data being collected, processed and communicated, not only to save time, cost and power at the edge but also to enable more efficient processors at the cloud. Figure 3 shows the increasing requirements for data analytics to realize the true potential of a connected society. For example, as the number of connected devices grows exponentially, so do the need for additional processing capacity (e.g. Cloud Computing), for standards for seamless integration of IoT devices and applications, and for related open Application Programming Interfaces (APIs). Similarly, the system demands complex analytic algorithms and tools to realize the true potential of a connected society. At the end of this chapter, the complexities in realizing this connected society will be identified (see section 1.4) and

Chapter 3 is intended to guide on how standards are important in this context, along with the standardization efforts of relevant stakeholders.

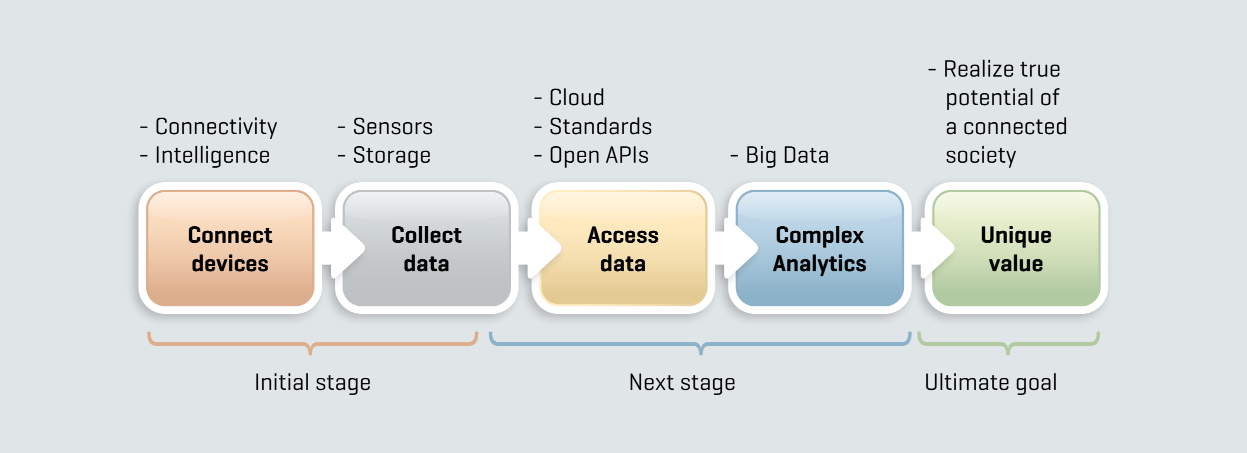


*Figure 3: Increasing requirements of data analytics to realize the true potential of a connected society [6]*

## 1.2.1 Data value principles, categories, and management concepts in the IoT

As the IoT is a key source of data, it should be managed properly to fully take advantage of it. Before providing trends of IoT driving technologies and related complexities in the current context, the basic concepts of data value principles and requirements of efficient data management will be provided below [7].

### 1.2.1.1 Data value principles

In the context of a given IoT environment, sensing elements generate data from various sources, which are key elements of business insights. There are several key data value principles that drive data assets, including, but not limited to, those in Table 1.

| Data value | Description |
|---|---|
| Increases with use | Data usage is cheap, especially compared to the cost of its collection and maintenance. Thus, high value for investment is often obtained through a high data reuse rate. |
| Decreases over time | By definition, obsolete data is no longer relevant to its context, and is useless. Usually, recent data is more valuable. |
| Increases with quality | For business decisions or other processes supported by data to be of any use, the data that they are fed should be as reliable as possible. Data reliability, or data quality, are measured in terms of accuracy, completeness, and traceability, among others. Poor quality data can actively damage anything that relies on it as input. |
| Increases through combination | Combinations of data often yield more interesting business insights than sets of data taken separately. Combining data can also mean enriching one or more data sets with metadata or indexing to better describe context. |

*Table 1: Data value principles*

### 1.2.1.2 Data categories

For effective data management, it is important to identify different data categories having different lifecycles and management requirements. The data can be globally categorized via four different concepts: structure, source, size and speed. Previously, traditional information management systems dealt with structured or semi-structured data, but IoT data are more unstructured and come from external sources in Big Data streams, which demands new architectures for managing such data. Table 2 provides an overview of data categories, from the perspective of an IoT ecosystem.

| Category | Sub-category | Description |
|---|---|---|
| Structure | Structured | This is data equipped with a pre-defined model or a schema, used to define the information such as data type, and how they will be recorded, processed, and accessed. Examples of structured data are: employee information, system logs, billing data. Structured data can be easily queried and analyzed. |
| | Semi-structured | Data in this category are only loosely organized, e.g. there may simply be tags pointing to various data elements. These are more often handled by file systems. Examples of semi-structured data are: Emails (sender, recipient and time of receipt are tagged, while actual content remains unstructured), and files encoding graphics. |
| | Unstructured | Unstructured data are generally text-heavy and may contain other types of data such as numbers, dates, etc. There is no a priori intrinsic structure. Data from social media, call center logs etc. are examples of unstructured data. |
| Source | Internal | Internal data come from some internal system, for example, within a same company, from a same application etc. |
| | External | External data come from third parties, for example social media, third party web services, data received from sensors networks (e.g. weather, traffic information). |
| Size | Small data | This is data that can fit in the memory of a computer and can be managed by traditional data processing applications. |
| | Big data | This is large data that cannot be processed by traditional data processing applications and requires advanced processing mechanisms. |
| Speed | Data at rest | Data that are static in nature, and usually stored in persistent storage (e.g. hard disk) in any digital form (e.g. database, data warehouse, spreadsheet, files), are considered data at rest. |
| | Data in motion | Data in transit, and data that are processed on the fly without long-term storage, are considered data in motion. Typical characteristics of data in motion are velocity (the rate at which the data goes from creation all the way to visualization) and variability (the rate at which data, or its processing characteristics, change). |
| | Slow data | This is data that takes a relatively long time to process. |
| | Fast data | This is data that is processed in a short amount of time. The data are created and passed on in real-time or near-real time, and are typical in the era of Big Data. |

*Table 2: Data categories*

#### 1.2.1.3 Data management

Data management is key to any organization. Typically in IoT, it helps to ensure security and privacy in the growing context of deployment across application sectors. Data management comprises all the requirements needed to securely manage data as a valuable asset. For successful data management, a data management architecture is required to enable a unified real-time view of all data assets. Successful data management should [7]:

- manage the entire data lifecycle;
- ensure data quality;
- provide accessibility;
- provide maximum value of data assets;
- provide a unified view of all data assets to enable integration across sectors, system verticals and silos;
- provide efficient processing, transformation, and enrichment of data;
- provide specific management policies and procedures to ensure the highest possible level of data security and privacy.

### 1.2.2 Foundational pillars of IoT data generation

In terms of data flow, there are mainly three layers realized in an IoT architecture, namely the data collection layer, the data transmission layer, and the data process, management and utilization layer [1]. Data generation for business innovation can be categorized basically into four phases: connect, collect, compute and create [3] (see Table 3).

| Foundational pillars of IoT data generation | Description |
|---|---|
| **Connect**<br>New connections of devices and information | Connections are the foundational component of the IoT. It is about embedding connectivity and processing capabilities into devices. Capabilities of new technologies, such as 5G, NB-IoT, satellite are expected to connect billions of devices across the globe. |
| **Collect**<br>Enhanced data collection grows from the connections of devices and information | Once the devices are connected to the Internet, they (once enhanced with sensors and storage) allow for an unprecedented collection of data (information) about the physical environment. Emerging biometrics sensing technologies are expected to provide more convenient and stronger security for the collection of data. However, there are still open questions from the regulatory perspective, and security issues at the IoT system level. |
| **Compute**<br>Advanced computation that transforms collected data into new possibilities | The feature of "everything-as-a-service" (XaaS) based on Cloud Computing is supporting the drive towards new business models and cost efficiency. The sheer volume of data generated by IoT devices can only really be handled by cloud or edge services (see [1] for more details). |
| **Create**<br>Unique creation of new interactions, business models, and solutions using data insights | Creation is the most significant step among the four phases of data movement in IoT, where new and unique solutions are developed and emerging opportunities are identified. Artificial Intelligence (AI) is expected to minimize the dominance of current technical solutions of companies in the digital assistant market. |

*Table 3: Foundational pillars of IoT data generation*

This section provided data value principles, management requirements, and fundamental pillars of data generation in the IoT. The next section is intended to provide its key trends on the basis of such foundational pillars.

## 1.3 Key IoT driving technologies

The IoT is an already existing phenomenon but the growing number of smart connected devices being added to the IoT has increased its significance in the connected society. Some of the key technologies that are driving the future IoT are depicted in Figure 4. For example, previously Machine-to-machine (M2M) protocols were used to communicate between devices but now Low Power Wide Area (LPWA), and Narrow Band IoT (NB-IoT) are already in place for connecting devices. 5G technology is going to take its place across sectors requiring deep coverage and having mission critical scenarios (e.g. ultra-low latency, high reliability, and immediate availability) in the near future compared to previous 3G/4G technology. Recent IoT trends drive towards overall system solutions rather than multiple single point solutions. Thanks to Machine Learning (ML) and Artificial Intelligence (AI) supporting IoT, businesses can reach another level of success to provide efficient insights for organizations.

Instead of using individual APIs to connect multiple applications, a single platform will be used to connect multiple applications. Blockchain technology for IoT applications is introduced to focus on asset tracking and management. It provides traceability, and health, safety, and security requirements. For example, the "cold chain" is very important in food and pharmaceutical distribution, and maintaining the appropriate temperature throughout this process is a key challenge. Blockchain technology can be used to prove each party's responsibility has been fulfilled at each step. Cloud-based data storage and processing are increasingly being used in IoT deployments. These days, the market has shifted from a single-vendor-centric approach, and more towards a manufacture-developer-service provider ecosystem approach.

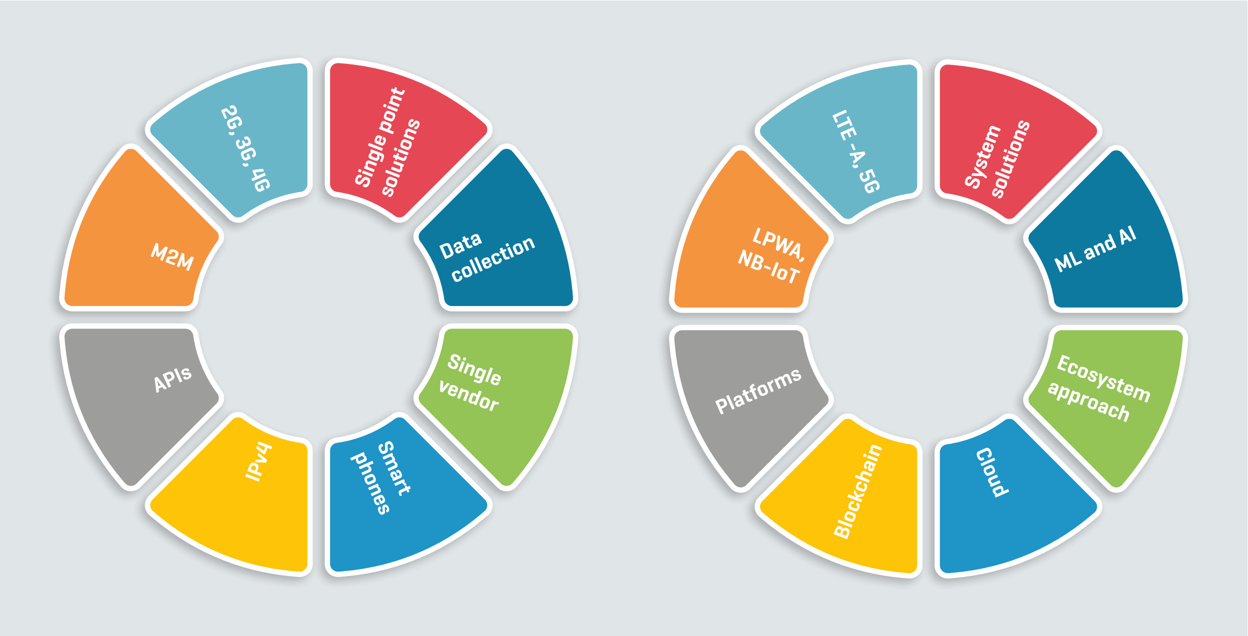


*Figure 4: Key IoT driving technologies [3]*

In particular, its key trends can be also divided into the following parameters from the perspectives of IoT data generation:

- Innovation and competitiveness
  - Connectivity standards have risen in response to the IoT opportunity. Numerous similar (sometimes redundant) wireless solutions now exist, some originating in existing technology (e.g. Bluetooth, WiFi) and others newer to the field (e.g. SigFox, LoRa);
  - The market for sensing techniques has become highly competitive. For example, the Micro-Electro-mechanical Systems (MEMS) microphone market is very fragmented. Similarly, technologies for natural speech/voice recognition are reaching the next level of success;
  - Off-premises or on-premises computing is used depending upon the scenarios. For example, off-premises computing is well suited where applications do not have stringent response time requirements. For certain low latency applications on-premises computing could be the best solution. The security of off-premises (e.g. cloud) processing remains a top concern for organizations, so combinations (hybrids) of off-premises and on-premises solutions are increasingly prevalent;
  - IoT is driving the force to create new and unique solutions across the vertical sectors. For example, 5G, NB-IoT technology will contribute to reach another level of connectivity in IoT.

- Business models
  - Investments in M2M and traditional IoT applications are expected to increase significantly across all sectors with the introduction of 5G connectivity and its cost-cutting potential, namely taking advantage of improved energy consumption and coverage. For telecom operators, smart cities are a microcosm of the IoT ecosystem;
  - Sensing helps IoT data monetization, creating new business models more focused on data management;
  - New cellular IoT gateways provide fundamental connectivity to equipment up until now considered non-connected. This is crucial to enable edge computing.

- Technology innovation and optimization
  - The sector of public safety has embraced the IoT, through licensing of the radio spectrum and with the help of the private sector actively using LTE;
  - Many IoT platforms provide highly integrated functionality for IoT applications;
  - Use of smart sensors (e.g. smart meters) for energy saving in smart home/office buildings saves millions of euros on energy bills;
  - The IoT has created a huge market for data brokering (complete with data publication, discovery, and consumption), with third-party IoT service providers and developers.

- Security concerns
  - Cybersecurity is a top issue for the IoT, mainly through the potential deployment of a huge amount of newly-connected devices added to a more traditional array of IT assets;
  - The IoT devices found in a single environment may have radically different technical profiles, physical locations, processing capabilities;
  - The potential of IoT actuation combined with IoT pervasiveness even force open considerations of physical health and safety.

## 1.4 Complexities in IoT from deployment perspective

It is seen from previous sections that the IoT has tremendous capabilities to enhance the way of current operation of any business sector. At the same time, IoT deployment faces a variety of complexities [1]. In this section, a list of some identified complexities in IoT deployment mainly from the perspectives of technology, business, and society [9], [10] will be first provided, and then cybersecurity risks will be introduced to the readers to know how these risks are emerging as leading concerns for IoT implementers. Further discussed in Chapter 3 is how standardization stakeholders are addressing these issues.

**Common language**

There should be a common understanding about the technology and an acceptable common reference architecture for implementation by stakeholders. As the IoT is broad and applicable to most of the sectors of society, there is still a lack of common understanding about the technology as well as a well-defined reference architecture acceptable from different perspectives across sectors.

**Interoperability**

The IoT is growing across sectors. Seamless interoperability with different devices operating in different technological environments is a major challenge. In addition to this, interoperation of the network protocol stacks at higher layers involving domain-specific operation, and semantic level is another challenge.

**Connectivity**

Connecting billions of devices is a major challenge in the IoT. Apart from this, various communication technologies: WiFi, Zigbee, LoRa, Low-Power Wide Area network (LPWAN), Long Term Evolution (LTE), LTE-advanced, 5G, etc. are ruling the current IoT paradigm and other technologies are yet to come. Seamless connectivity among connecting devices across the sectors and communication technologies is a major challenge.

**Reliability**

Reliability of the services is also another major concern in-specific sectors, such as in health care, or connected vehicles. These sectors require utmost reliability (99.9999 % or better) to get the appropriate service.

**Scalability and agility**

The IoT is referred to as a network of networks. The future applications or networks should be both scalable and agile to satisfy user demands. Systems should be dynamically scaled up and down without sacrificing basic requirements, such as Quality of Service (QoS), security/privacy, reliability, etc. The IoT is more heterogeneous than the Internet. The context of the tremendous challenges due to unbounded, unplanned, and unregulated growth of networks in the Internet leads to significant improvements also in IoT technology.

**Intelligence and analytics**

By nature, the IoT is to collect information and to react based on it. Information is collected at the devices and communicated to the cloud with or without the support of the edge. The factors: delay, jitter, cost, regulatory issues, etc., play a significant role in placing the appropriate analytic platform, i.e. whether at the edge/fog/roof or at the cloud.

**Sector-specific requirements**

A deployment decision can impact the vertical, horizontal or end-customer markets of the IoT. In particular, they can be industrial and/or consumer IoT. In this context, specific guidelines for specific sectors of deployment are very important; this is missing in the current context for the most sectors.

**Societal**

The services of IoT should satisfy consumers, developers, and regulators etc. as stakeholders of society. This societal challenge includes the mode of usage, energy consumption, environment impact and other related societal impacts, which play a vital role in IoT deployment.

**Trustworthiness**

Trustworthiness reflects the degree of confidence one has that the system performs as expected with regard to characteristics including safety, security, privacy, reliability and resilience, etc. [11]. Trustworthiness of IoT systems will require active management of risks for all of these characteristics.

**Security and privacy**

Today, security and privacy are prime concerns for IoT deployment. Most of its deployments are prone to security and privacy risks at the device, edge, and cloud platform levels. An appropriate deployment architecture should be considered to overcome all related issues.

However, all the issues mentioned here are equally important and have to be addressed while deploying IoT. The remaining part of this section highlights cybersecurity requirements for the IoT, as one of the most growing concerns among others for every stakeholder. Chapter 3 is dedicated to providing the details on how several Standard Development Organizations (SDOs) and alliances are working together to minimize such issues.

### 1.4.1 IoT cybersecurity

As for all ICT technologies, a secured environment is a fundamental requirement of the IoT. This requirement is present in technological, privacy and ethical aspects. An appropriate level of security of an IoT ecosystem will foster users' trust. Security, privacy and trust become particularly challenging issues when the things are connected to the global network [12]. The IoT White Paper [1] provided some of the fundamental security vulnerabilities in overall IoT ecosystem and different layers of IoT architecture, including various technologies involved in such layers. This report intends to provide related cybersecurity issues from deployment aspects across sectors.

#### 1.4.1.1 Attributes affecting IoT cybersecurity

The NIST Interagency Report [4] defines cybersecurity as follows: "it is the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems". As mentioned before, an IoT ecosystem includes a diverse set of new applications across sectors. Table 4 provides possible attributes of the IoT at components and systems for its cybersecurity considerations.

| Elements of IoT ecosystem | Attributes affecting cybersecurity |
|---|---|
| IoT components | ● Use hardware with restricted computing ability and low power consumption. |
| | ● Process data locally or remotely, but sometimes both for certain uses. |
| | ● Massive amounts of data may originate at a single device. |
| | ● Operate in highly heterogeneous networks (with respect to interfaces, protocols, operating systems). Devices themselves may also be quite different. |
| | ● Can be set up in locations that are hard to secure physically. |
| IoT systems | ● Have access to device owner and/or non-owner networks, representing an entry point for both. |
| | ● Are highly distributed, with device ownership sometimes hard to determine clearly. |
| | ● Operate with varying degrees of autonomy. |
| | ● Rely heavily on proprietary communication solutions. |
| | ● Are often deployed in very dynamic environments. |
| | ● Could be accessed remotely by third parties (e.g. manufacturers). |
| | ● Could impact different aspects of the deploying party's IT and physical environment (e.g. physical safety may be affected). |
| | ● Might infringe on Personally Identifiable Information (PII) by collecting, storing, and using data unbeknownst to the owner. |

*Table 4: Attributes affecting IoT Cybersecurity [4]*

### Cybersecurity objectives, risks, and threats

The cybersecurity objective for a traditional IT system used to mainly prioritize confidentiality first, then integrity, and finally availability. But cross-sector use cases force cybersecurity objectives in IoT systems to be prioritized differently as a function of their objectives. For example, availability and integrity are of higher priority in connected vehicles. Table 5 summarizes general cybersecurity objectives, risks, and threats in IoT systems. Sector-specific objectives, risks, and threats will be provided in Chapter 2.

| Parameters | | Descriptions |
|---|---|---|
| Cybersecurity objectives | Confidentiality | Confidentiality is the property that information is accessible only to parties to whom it is authorized. This also covers protection of personal data. |
| | Integrity | Integrity is the property that unauthorized information alteration (including destruction) is detected. By-products include providing authentication and non-repudiation. |
| | Availability | Availability is the property that information is accessible when needed. |
| Risks | | Risk measures the degree to which an adverse event can affect an asset or entity. It usually is quantified as a measure of an adverse event's impact and the probability of given threats that cause the event. |
| Threats | | A threat is any phenomenon that may cause an adverse event on an asset or entity, whether intentionally or not. [13]. |

*Table 5: Cybersecurity objectives, risks and threats [4]*

### IoT cybersecurity objectives

The specific cybersecurity objective for IoT systems in general can be articulated as follows [14], [15]:

- To control logical IoT network access and physical IoT component access;
- To protect components of IoT from misuse;
- To protect data integrity;
- To detect security events and incidents;
- To ensuring system functions and continuity during incidents or attacks;
- To ensuring system recovery post-incident.

### IoT cybersecurity risks

The risks that arise from the loss of above cybersecurity objectives (confidentiality, integrity, and availability) are called information security risks. In this context, risk assessment is a way of documenting, evaluating, and prioritizing risk, in particular to decide which risks require mitigation (risk treatment), and which ones do not (risk acceptance). It requires a careful analysis of threats and vulnerabilities (of which risk is usually the product) to decide the extent to which events or circumstances would poorly impact an environment or organization, as well as their likelihood of occurrence [14].

### IoT cybersecurity threats

As seen in Table 5, cybersecurity threats exist both to and from the IoT. The number of deployed devices continues to increase the overall ecosystem's attack surface, all while also increasing the volume of produced data which needs protection, and the physical actuation potential on society in general. Refer to Table 6 for some representative methods of threat types

| Threat types | Description |
|---|---|
| Adversarial | Exploration and information collection.<br>Develop skills for creating attack tools.<br>Installation or launching of malware or attacks in general.<br>Achieve results (i.e., cause adverse impacts, obtain information).<br>Can be set up in locations that are hard to secure physically. |
| Non-adversarial | These consist in errors that occur in the system either due to a technical mishap (component fault or software bug) or the accidental misuse of a system by a legitimate party, as well as natural events, whether severe (earthquake) or not (temporary power outage). |

*Table 6: Methods of threat types*

Further sector-specific cybersecurity objectives, risks and threats will be provided in Chapter 2. Chapter 3 is dedicated to providing related technical standardization efforts initiated by several SDOs as well as alliances to obtain identified cybersecurity objectives and other deployment complexities mentioned in the chapter.

# 2

# Internet of Things: Examples of applications

# 2. Internet of Things: Examples of applications

In this chapter, a global analysis of IoT use cases in some selected domains is provided. In general, IoT application domains can be divided into two categories: horizontal and vertical. The horizontal sector falls under the telecommunications domain while smart buildings, smart homes, smart manufacturing, connected vehicles, smart health, smart energy, smart cities, smart agriculture, to name but a few, consist in the vertical domains of IoT applications. To represent both categories, satellite and related connectivity for IoT (under telecommunications and related sectors) as a horizontal domain, and connected vehicles as a vertical domain, are considered in this report.

## 2.1 Satellite and related connectivity in IoT

### 2.1.1 Background

Connectivity is one of the most significant parts of the IoT ecosystem. On one hand, a network of billions of connected things demands an efficient scattered communications network across the globe. On the other hand, connected things across sectors produce a massive amount of data. A ubiquitous and seamless coverage throughout all sectors is not possible by only cellular and terrestrial communications, due to the geographical landscape. This leads to space-based communication to solve the problem of interconnecting things scattered across the globe. Satellite technology has the potential to support the development of the IoT ecosystem. It has the capability to handle the connectivity challenges of scattered networks in the IoT. Business operations have been already extended into unmanned sites and offshore platforms for decades using satellite communication. Examples include providing connectivity for facility monitoring and instantaneous management in rural farming, pipelines across deserts, wildlife and environment monitoring, etc. Satellite-based solutions can be easily integrated into hybrid networks that combine wired, wireless, and satellite. Once the IoT ecosystem is empowered with a global network of billions of interconnected devices via satellite communication, it will unleash the full potential of IoT technology. Some of the features of satellite-based solutions, which are ideal for the IoT traffic [16], are depicted in Table 7.

| Global Footprint | Resilience | Broad-, narrow-band and broadcast capabilities |
|---|---|---|
| Satellite networks can have global coverage allowing the IoT to be connectd to remote locations, where terrestrial connectivity is not reasonably accessible either because of cost or terrain, including at sea, in the air, or other unconnected locations. | The IoT ecosystem needs ubiquitous, resilient, and seamless connections over time to run efficiently. Satellites, in conjunction with terrestrial services, have a proven track record of resilience and provide an economic connection anywhere in the world. | Satellite communications have broadband, narrowband, and broadcast capabilities. Accordingly, the global network of satellite operations can support the needs of IoT users with different bandwidth and capabilities. |

*Table 7: Ideal features of satellite for the IoT traffic*

In addition to these features, satellite technology can deliver a variety of frequencies, orbits, and speeds for smart applications. L-band satellite services have been providing M2M connectivity for many years. Now, with the advancement in high throughput Ku-band and Ka-band, satellite connections have created a broadband superhighway in space to easily handle the potential volume of opportunities in the IoT and M2M [16]. Various sources show that more than 2.7 million devices are already supported via satellite IoT spreading across sectors, including infrastructure, smart grid, disaster monitoring, environmental monitoring, and the oil and gas industry [17]. Military support, border patrol, aviation, fleet management, etc. are the other key vertical sectors supported by satellite connectivity services.

## 2.1.2 A typical example of satellite and related communications for the IoT

Figure 5 depicts a simplified view of satellite connectivity in the IoT ecosystem. Satellite connectivity is capable of connecting various sectors of society, ranging from rural to urban coverage as well as water to air coverage [16]. As shown in Figure 5, Low-Earth Orbit (LEO) and Geosynchronous Equatorial Orbit (GEO) satellites can provide effective communications across sectors with the help of other communication technologies (e.g. 5G) to connect things anywhere in the world.

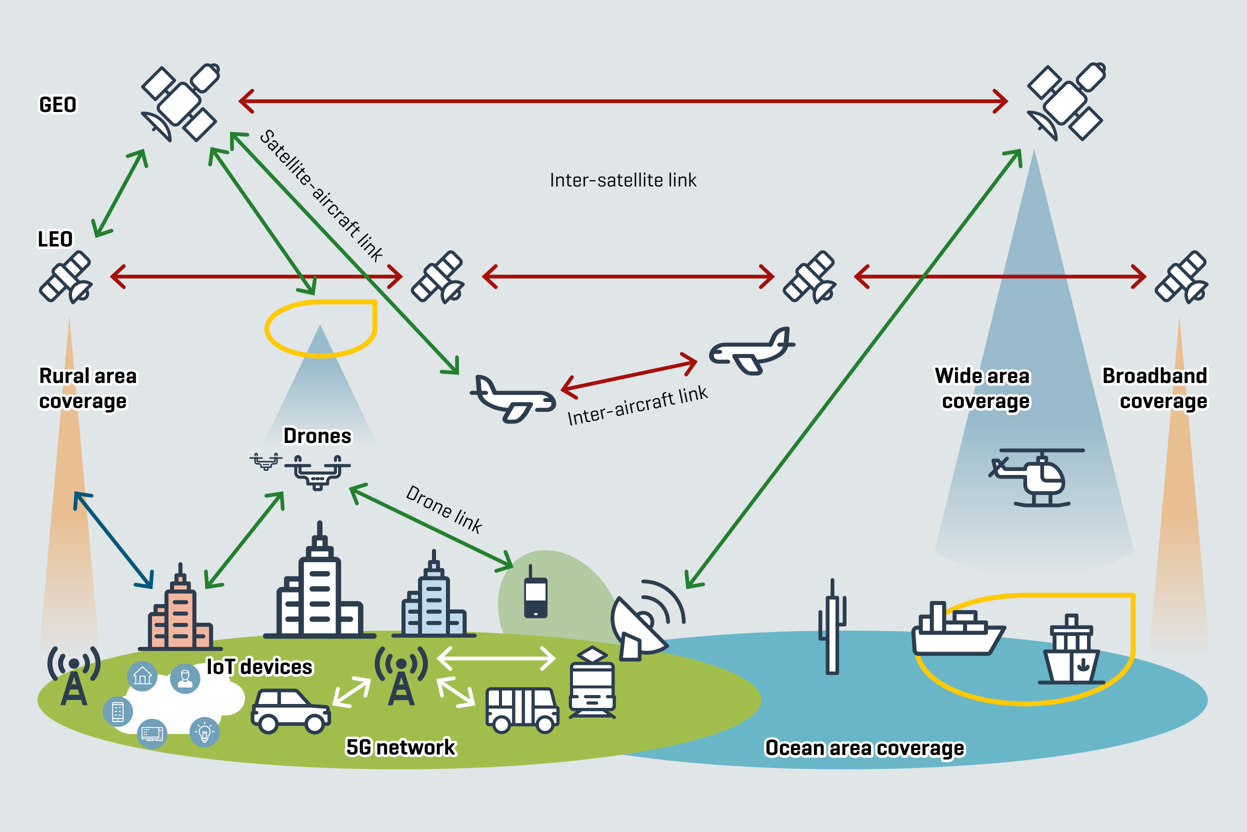


*Figure 5: Simplified satellite connectivity in the IoT ecosystem [16]*

### 2.1.2.1 The satellite-IoT ecosystem

Some players of the satellite-IoT ecosystem include, but are not limited to, those listed in Table 8.

| Key players | Examples |
|---|---|
| Hardware and related infrastructure providers. | Original Equipment Manufacturers (OEMs), platform providers, Satellite links (up/down), satellite, etc. |
| Connectivity service providers | Wireline (e.g. optical fiber), Wireless (e.g. 4G, 5G), short range communication (e.g. NB-IoT, SigFox, LoRa) |
| IoT service providers | Services related to IoT and M2M |
| End devices | IoT devices, aircrafts, drones |
| Regulators | The government, public organizations and related bodies |
| End users | IoT users, internet users, user of road vehicles, air/water crafts |

*Table 8: Key players of the connected vehicle ecosystem*

### 2.1.2.2 Typical data flow in the ecosystem

A block diagram of the typical data flow within the ecosystem is depicted in Figure 6. This section mainly covers the data flow where satellite or related connectivity is involved. Multiple sensing techniques are used to collect (real-time) information on locations, users and other components used within the system. The user interface represents the input and output devices to interact with physical ends. Particularly, in this case, IoT gateways or IoT nodes are connecting the satellite system with other networks. Monitoring systems are responsible for various detection mechanisms, such as support, incident control, verification, and incident detection. Computing and processing belong to the analysis of enormous data (Big data) received from multiple actors of the ecosystem available in stored information. Various communications take place inside and outside of the system to allow the actors of the ecosystem to interact. Table 9 shows a list of IoT-based technologies, which could be applied within the Satellite-IoT ecosystem.

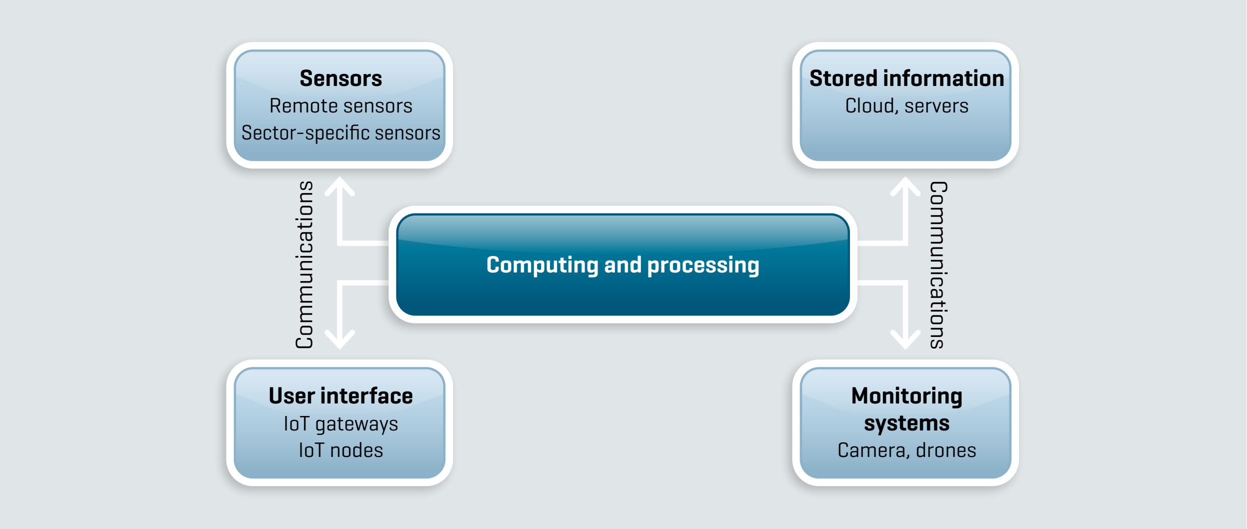


*Figure 6: Typical data flow in Satellite-IoT ecosystem*

| Technology | Purpose | Description |
|---|---|---|
| Sensing and monitoring | Remote sensors | Radar, LiDAR, ranging instrument |
| | Domain-specific sensors | Optical sensors use light to measure soil properties in smart farming |
| | Weather sensors | Sensors to detect rain, wind, snow, fog, etc. |
| Interfacing | Interface/gateways | IoT nodes, IoT gateways to be interfaces with satellite system |
| Bluetooth, Wi-Fi, NB-IoT, SigFox, LoRa, 3G, 4G, 5G, LTE etc. | Communication between the end user components | - |
| Processing and computing | Analyzing and processing real-time information and historical information | Data server, Big data, Cloud Computing |

*Table 9: Technical landscape*

### 2.1.2.3 Industry benefits

The basic requirements for the IoT are that all devices need to be connected wherever they are. As mentioned earlier, satellite can provide ubiquitous and seamless coverage across sectors. The ultimate success of the IoT will depend on the active support of satellite networks. The main value propositions of satellite connectivity for the future IoT include, but are not limited to, those in Table 10 [18], [19].

| Advantages | Description |
|---|---|
| Global coverage (Internet of Everything Everywhere) | A new breed of IoT applications will emerge from the connectivity of intelligent devices. Expected to encompass billions of devices around the world, the potential scale of the IoT demands ubiquitous network coverage even in remote locations, which are best served by satellite networks. |
| Reliability | Maintaining a high level of service reliability is a key requirement for effective IoT deployments. The low latency of L-band services holds a distinct advantage in catering to applications, such as remote asset monitoring that requires reliable, always-on connectivity. |
| Cost | Satellite technology has the potential to be a versatile and cost-effective solution to address IoT connectivity needs. The costs associated with mobile satellite services, for instance, are highly competitive with terrestrial networks, and is considered a more affordable option relative to other satellite platforms |
| Speed | The future landscape of IoT applications involve an exchange of data between interconnected objects to facilitate quicker decision-making and enhance business processes. These developments have, in turn, driven up the demand for high data speeds to support bandwidth-intensive applications in real time. |
| Continuing integration | The IoT is expected to continue driving up market demand for the integration of satellite into the overall communications mix. |
| Lowest energy | A lower energy consumption footprint and device autonomy. |
| Secure and high availability | It is capable to provide secure and trustworthy data services for professional users. |

*Table 10: Benefits of satellite connectivity in the IoT ecosystem*

### 2.1.2.4 Related issues/challenges across the sector

The demand of IoT end-device connectivity is driving the need for innovative communication techniques. In addition to the terrestrial infrastructure, satellite communication appears set to play a vital role in supporting IoT applications across sectors. Some of the challenges of the current satellite industry for supporting IoT end-device connectivity include, but are not limited to, those in Table 11.

| Challenges | Description |
|---|---|
| Interoperability | Ability to communicate despite different data format and protocols [20]<br>The growing variety of Sat-IoT connectivity will trigger the global proliferation of the IoT industry into the 90% of our globe without terrestrial networks. This will lead to the same effect as when ubiquitous broadband internet and mobile cellular brought along the "Connected Society", the shift now going from the Internet-of-People to the Internet-of-Things. We see the satellite industry responding to the IoT connectivity demand both with low cost/low power Direct-To-Satellite connectivity, as well as with various combinations of terrestrial (cellular and LPWAN) IoT access networks and satellite backhaul.<br>There are two modes of interoperability between satellite and sensors/ actuators:<br>1) direct access -- The direct access mode allows sensors and actuators to directly communicate with the satellite, in uplink with the sensors and in downlink with the actuators;<br>2) indirect access -- the sink is provided with a satellite terminal (expensive and power-hungry) and with a WSAN radio interface, while all the other nodes of WSAN are only provided with a WSAN radio interface. |
| Integration | Need to meet different networks' requirements<br>Several messaging protocols, such as MQTT, were originally designed for traditional terrestrial networks. These protocols may be used for collecting sensor data over the new IoT-Satellite emerging paradigm. Integration of IoT and satellite communication is a key issue for the smooth operation of two different networks. |
| Optimization | Need to design modification to improve QoS and system performance<br>As mentioned in Integration issues, new efficient configurations are needed. But an optimal design of such configurations is equally important on the satellite communication side. For example, reducing the amount of traffic on the satellite return channel, and delivery of critical data on time, are very important in satellite communication. |
| Cybersecurity | Cybersecurity risks and threats [21]<br>One the most significant weaknesses that is common to all satellite systems is the use of long-range telemetry for communication with ground stations. The uplinks and downlinks are often transmitted through open telecom network security protocols that are easily accessed by cyber criminals. IoT devices that utilize satellite communications pose additional potential points of entry for bad actors. Section 2.1.2.5 provides the cybersecurity objectives, risks and threats particularly in this sector. |

*Table 11: Satellite communication challenges to support IoT end-device connectivity*

### 2.1.2.5 Cybersecurity objectives, risks and threats

Most of the world's critical global-level infrastructure (e.g. air transport, world-wide communications, etc.) utilizes some form of nation, regional or international space infrastructure, including for instance satellites, data links and ground stations [22]. Service providers continue to investigate how satellites can deliver reliable, cheap and persistent abilities that can link a large variety of connected devices. Collaboration across sectors would be vital in any response to space-based cyber security threats. Some issues are at the heart of the debate due to the following reasons:

- High numbers of satellites orbit the Earth. Their downlinks and uplinks are transmitted via ground stations located all around the world;
- The satellites are used worldwide, mainly for communications, observation of Earth or specific timing and navigation capabilities;
- Nowadays, satellites are built with the components of a complex supply chain.

Some examples of cybersecurity objectives in satellite connectivity and related sectors are highlighted, but are not limited to those, in Table 12.

| Cybersecurity objectives | Description |
|---|---|
| Confidentiality | Implement appropriately strong encryption for data transferred to or from any satellite or communications network. |
| Integrity | Implement proper authentication and integrity protection mechanisms in communications. |
| Availability | The real-time nature of communications requires resilient and secure networks. |

*Table 12: Cybersecurity objectives in satellite connectivity and related sectors [21]*

Like others, this sector (satellites and other space equipment) are vulnerable to cyberattacks. Some cyberattacks in the space sector, which may pose serious risks for ground-based critical infrastructure, may include [22]:

- Spoofing, jamming, and hacking attacks on communication networks;
- Targeted attacks on mission packages or control systems; and
- Targeted attacks on the physical infrastructure (e.g. attacks on the satellite control centers of the ground infrastructure).

### 2.1.2.6 Examples of national initiatives in satellite and related connectivity in IoT

As mentioned before, considering the need of broad coverage and fast connectivity for IoT devices, satellite and 5G-related implementation initiatives at national level are covered in this report.

#### 2.1.2.6.1 Light-Weight Application and Transport Protocols For Future M2M Applications (M2MSAT)

The project "Light-Weight Application and Transport Protocols for Future M2M Applications", in short M2MSAT, was funded by the ESA under the ESA ARTES Advanced Technology Programme in October 2016 [23]. The M2MSAT project included the ESA as a contracting entity and a consortium composed of three partners: SES TechCom S.A. (Luxembourg) as the project coordinator, the University of Luxembourg (Uni.lu) – Interdisciplinary Centre for Security, Reliability and Trust (Luxembourg), and JOANNEUM RESEARCH (Austria) as SES subcontractors. The Luxembourg Institute of Science and Technology, LIST (Luxembourg) joined the consortium as well, as a Uni.lu subcontractor, providing support for the standardization-related activities.

The scope of the M2MSAT project was to propose modifications/optimizations to selected IoT application protocols to enhance network performance when adopted in integrated M2M/IoT satellite network scenarios. To this aim, first the consortium identified MQTT (Message Queuing Telemetry Transport) [24] and CoAP (Constrained Application Protocol) [25], as IoT Application Protocols suitable for IoT data collection over satellite. Selection criteria were mainly market representation, transport layer protocol, standardization organization support and available third party tools. CoAP uses the connectionless but lightweight UDP protocol, while MQTT makes use of the reliable, but more complex TCP protocol. Reliable message delivery can be selected in CoAP by using the "Confirmable message" feature. Now, the M2MSAT team has proposed an efficient configuration for MQTT and CoAP when integrated with a GEO-based satellite system [26] (see Figure 7 and Figure 8).

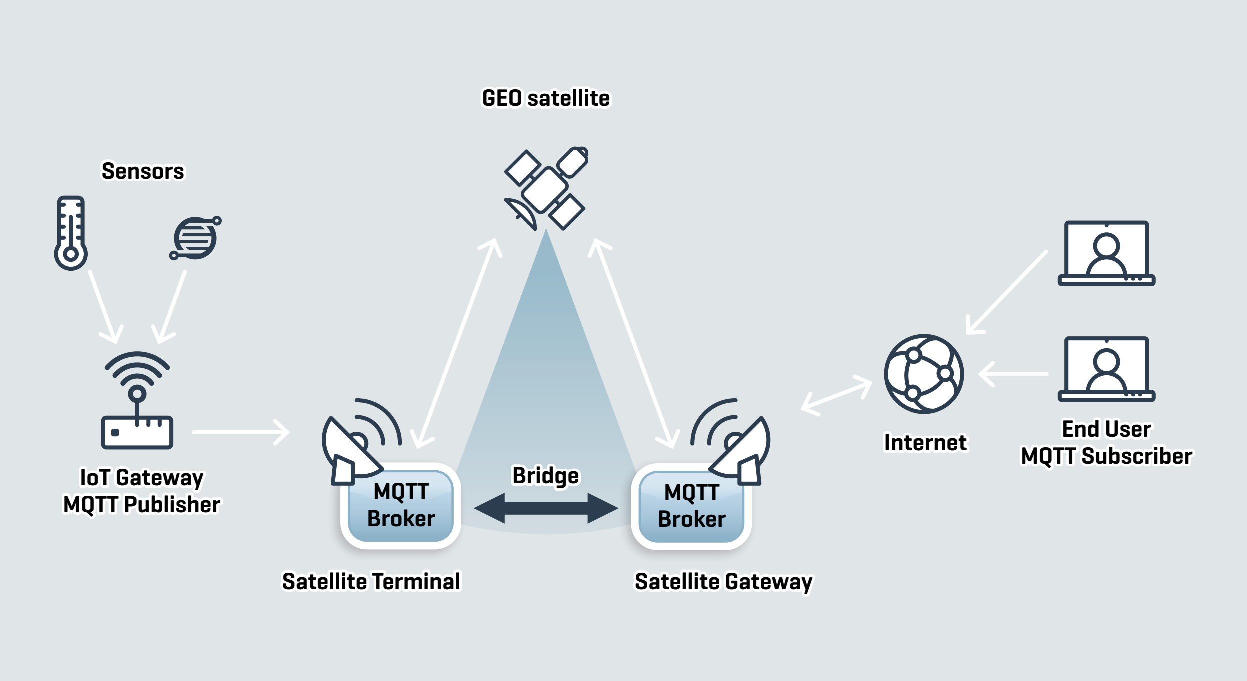


*Figure 7: MQTT Efficient Architecture*

The network architecture, which is highly scalable, includes two MQTT brokers (with bridge functionality) and two CoAP proxies, in "Observe" mode. The M2MSAT consortium designed a set of optimizations of the two selected protocols aiming: 1) to reduce the amount of traffic load over the satellite return channel, and 2) to support different Quality of Service (QoS) for traffic delivery.

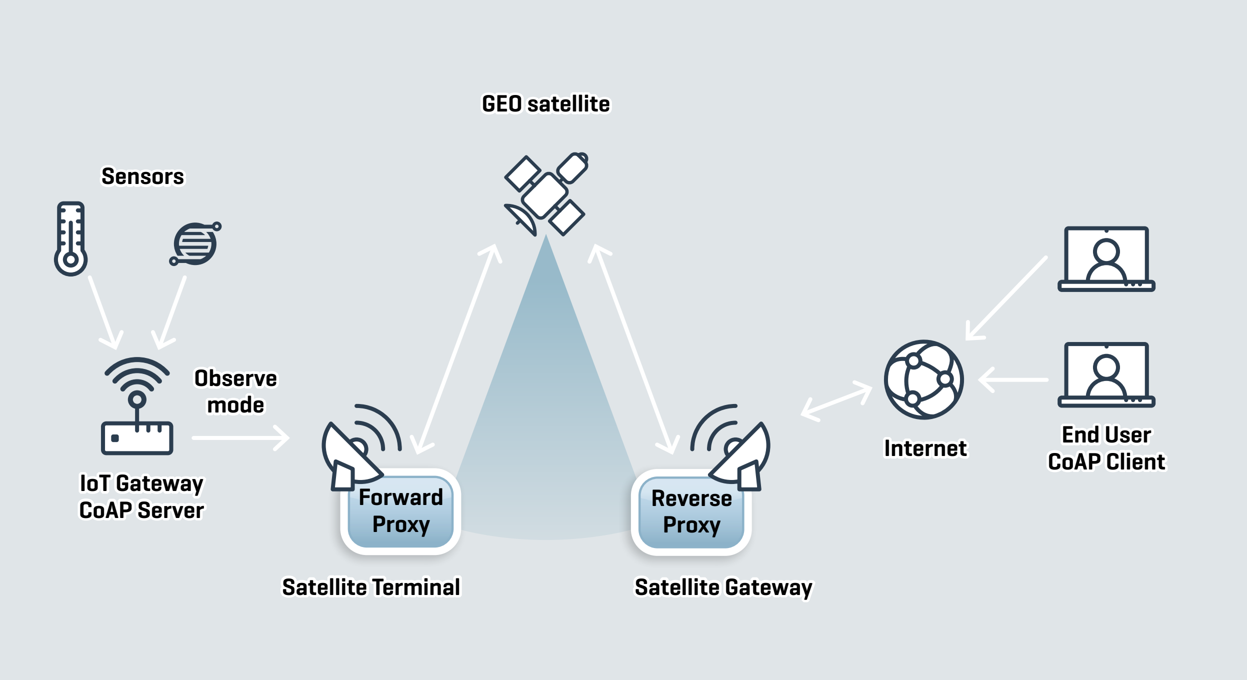


*Figure 8: CoAP Efficient Architecture*

The first optimization focuses on the aggregation of the traffic (CoAP unicast responses and MQTT topics) sent by MQTT publishers and CoAP servers on the satellite return link by making use of an MQTT filter aggregator [27], and a two-step group communication approach, respectively. The aim is to reduce the amount of traffic on the return link of the satellite segment. The second optimization aims at adding QoS classes that are linked to the reliability of the message delivery and to the timeliness of message retrieval. Implementing this optimization will ensure delivery of data according to QoS level and retrieval priority.

The proposed optimizations were implemented using a satellite emulator, called OpenSAND [28] and widely-adopted libraries for IoT messaging protocols such as Eclipse Mosquitto [29] and CoAPthon [30]. The assessment of the proposed optimization along the performance evaluation framework was done taking into account the realistic settings of the GEO satellite link. Beside the implementation of the optimization, the M2MSAT team is also planning to submit an Internet Draft to the IETF about the first proposed optimization for CoAP (aggregation of CoAP Unicast Response for Group Communication).

###### 2.1.2.6.2 Communication Algorithms for End-to-End Satellite-IoT [SATIOT]

The SATIOT research project is funded by the Luxembourg National Research Fund (FNR) under the Industrial Fellowship instrument [31]. It is a collaboration between the University of Luxembourg (Uni.lu) – Interdisciplinary Centre for Security, Reliability and Trust (Luxembourg) as the Host Institute, and SES TechCom S.A. (Luxembourg) as the industrial partner.

The main objective of the project is to define realistic architectures for Satellite-IoT. This means that it will identify where different components of the network, e.g. access point/core components, should be located, e.g. satellite/ground, and what type of satellite orbits to use, e.g. GEO/MEO/LEO. The priority will be given to the LEO orbit, which has a more relaxed round trip time (RTT) compared to MEO/GEO, but still large, and introduces higher Doppler shift. Hence, the aim of this project is to design novel and practical algorithms for the defined architectures, starting from the physical (PHY) layer up to the network (NET) layer, in order to jointly decimate the satellite channel impairments like high Doppler shift and large RTT of communication. In the PHY layer, the objective is to design a new waveform that can tolerate a higher Doppler shift and that can possess a low peakto-average power ratio (PAPR). The current waveform of NB-IoT is not resilient to high values of Doppler shift and has a high PAPR, which makes the communication through the satellite link extremely inefficient.

In the MAC layer, an advanced random access (RA) procedure will be developed. The RA procedure is very important for achieving synchronization in the uplink transmission, while in the downlink transmission the synchronization does not seem to be an issue. The recent RA procedures are optimized for terrestrial communication and cannot support the high delays in the communication link over a satellite channel. Another objective in this layer is to design novel resource allocation algorithms. The new developed algorithms, apart from taking into account the channel conditions of each user, will be able to efficiently compensate the high Doppler shift.

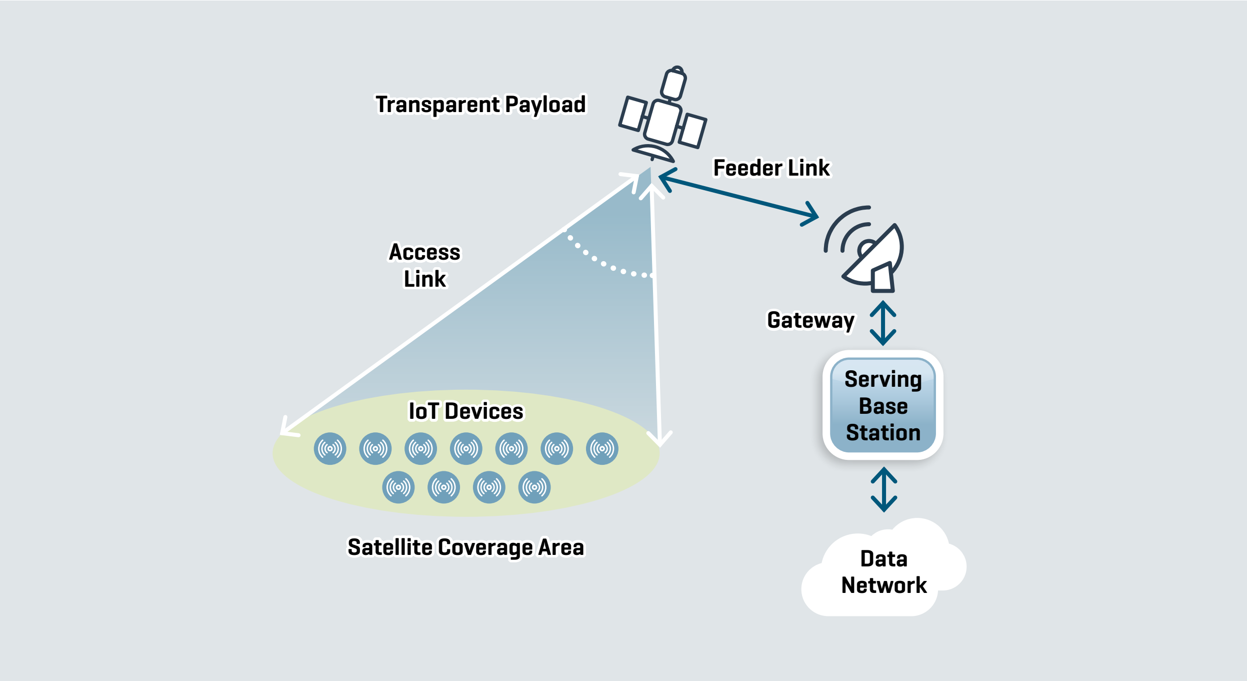


*Figure 9: Satellite user-feeder link*

An important outcome of the project is the development and design of novel communication algorithms covering the PHY, MAC and NET layers of communication, following an integrated cross-layer design approach. Another important outcome is the novel testbed with the satellite channel simulator for the developed communication algorithms, providing a real-time demonstration of IoT devices communicating through a satellite channel. It will be a helpful tool for further improvement of the algorithms and techniques before implementing them in cooperation with the industry. Innovations in Satellite-IoT technology have the potential for patenting and technology transfer. They can lead to building new standards for IoT or modifying the existing ones to match satellite requirements.

### 2.1.2.6.3 Demonstrator for Satellite-Terrestrial Integration in the 5G Context [SATis5]

The project SATis5 (Demonstrator for Satellite-Terrestrial Integration in the 5G Context) [32] is funded by the European Space Agency (ESA) under the ESA ARTES program. Its consortium comprises the following organizations: Eurescom (Prime Contractor, Germany), Fraunhofer FOKUS (Germany), Fraunhofer IIS (Germany), Newtec Communications (Germany), ST Engineering iDirect (Ireland), Technische Universität Berlin (Germany), Universität der Bundeswehr München (Germany), and SES TechCom S.A. (Luxembourg). It was kicked-off in October 2017 with a 36-month duration.

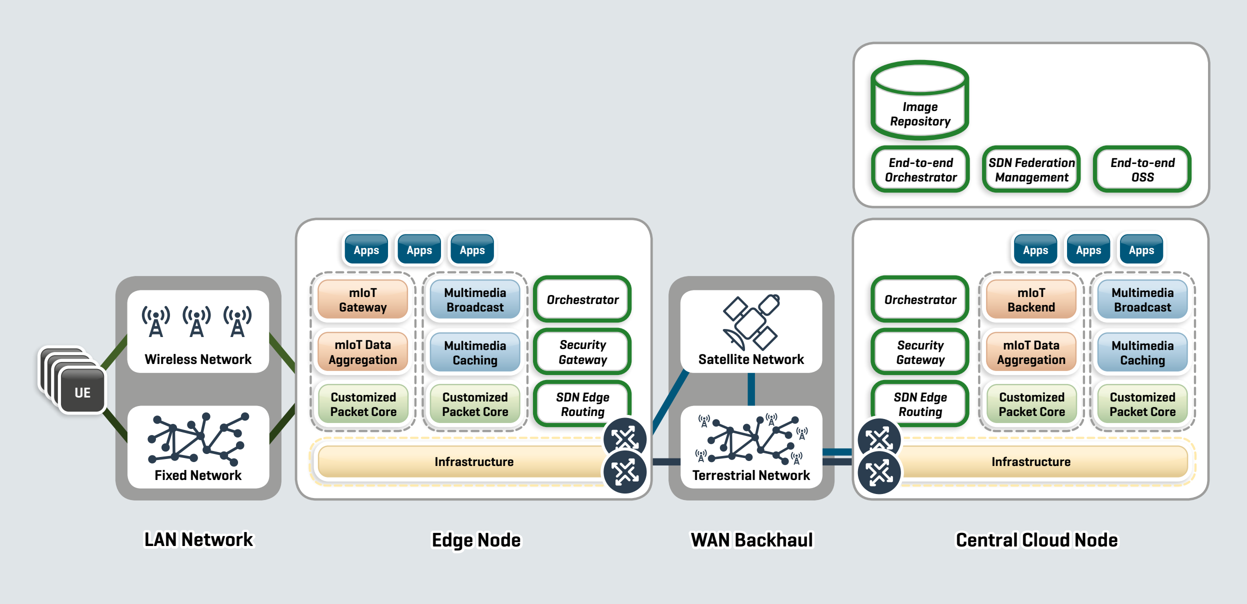


*Figure 10: SATis5 Testbed Architecture*

SATis5 builds an end-to-end 5G integrated network Proof-of-Concept testbed for satellite-terrestrial integration into 5G. The SATis5 testbed demonstrates a set of relevant satellite use cases for 5G in the areas of enhanced mobile broadband (eMBB) and massive Internet-of-Things (mIoT) deployments. The SATis5 testbed infrastructure is based on the 5G Berlin testbed and extends it with over-the-air satellite networking using SES's multi-orbit, multi-band state-of-the-art satellite fleet. It brings the level of integration of satellite networks on par with their terrestrial counterparts through end-to-end demonstrators (see Figure 10) [33], [34].

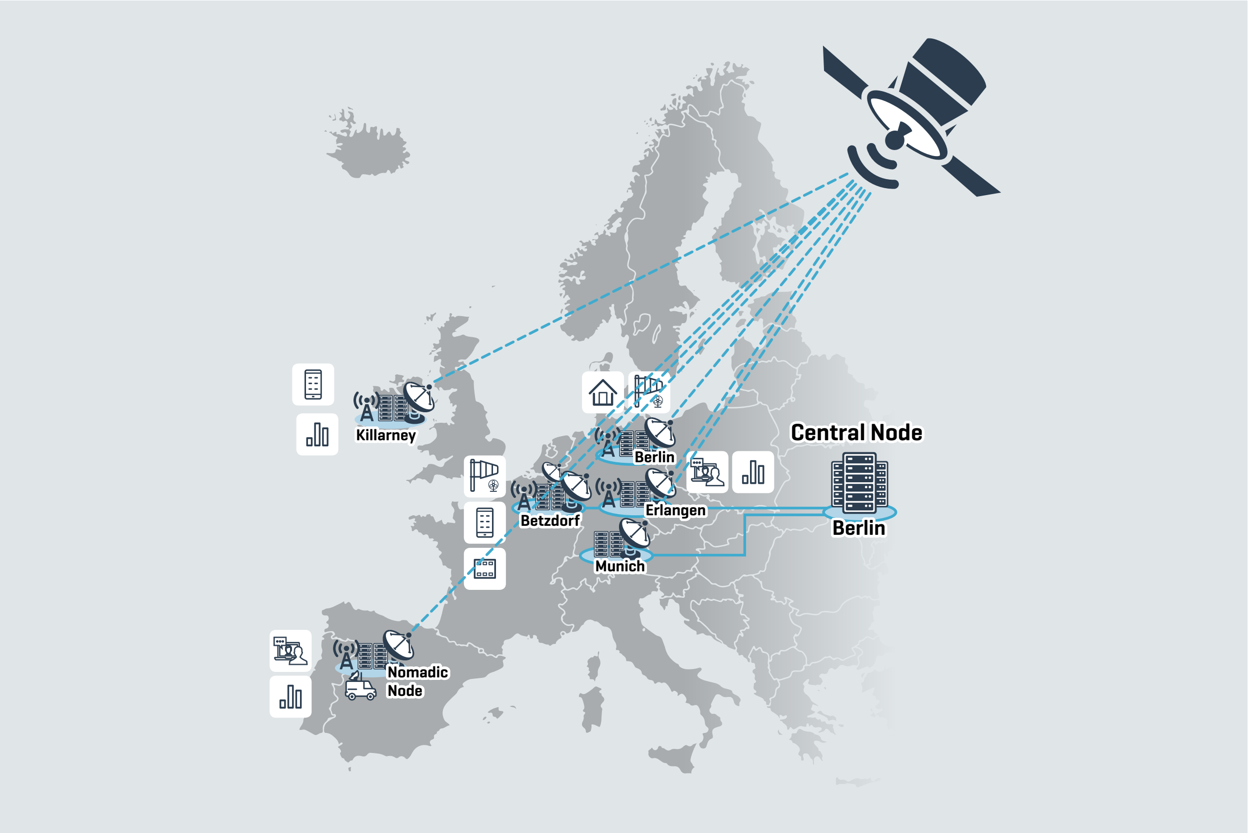


*Figure 11: SATis5 Testbed Deployment Overview*

With the central node located in Berlin, five edge nodes located in Betzdorf, Berlin, Erlangen, Munich, and Killarney, and a nomadic edge node aimed at demonstrations across Europe (see Figure 11), the SATis5 testbed includes a set of state-of-the-art toolkits and prototypes for both the terrestrial and satellite networks starting from radio network prototypes, Fraunhofer's Open5GCore and Fraunhofer's OpenBaton next to the latest satellite modem technologies, and provides a comprehensive basis for customized network deployments for the specific use cases and demonstrations acting as a best-practice path finder for the 5G trialing phase.

Apart from the multi-orbit multi-band satellite fleet provision, SES also hosts a SATis5 testbed node with prototypes of networks for satellite integration. This includes the hosting of a 5G edge node which is Software-Defined Networking (SDN), Network Functions Virtualization (NFV) and Multi-access Edge Computing (MEC)-enabled, and capable of demonstrating over-the-air eMBB and mIoT use cases, as well as the hosting of a 5G prototype hub platform which is SDN/NFV/MEC-enabled and is seamlessly integrated with the 3GPP Rel'15 compliant 5G Core Network, thus allowing the management and operation of a satellite network by telecom operators in a seamless way, as if it was a standard 3GPP 5G cellular access network.

So far, the SATis5 testbed capabilities have been successfully showcased in live over-the-air demos which took place in November 2018 in Berlin as part of the FUSECO Forum 2018 [35] and in February 2019 in Barcelona as part of the Mobile World Congress 2019 [36]. Further, SATis5 live over-the-air demonstrations took place in October 2019 in Dresden as part of the IEEE 5G World Forum 2019 and in November 2019 in Berlin as part of the FUSECO Forum 2019.

### 2.1.2.6.4 5G Verticals Innovation Infrastructure (5G-VINNI)

The project 5G-VINNI (5G Verticals Innovation Infrastructure) [37] is funded by the European Commission under the EC H2020 5G PPP Phase 3 - Grant Agreement No 815279. Comprising the leading mobile network operators (MNOs) and mobile industry vendors, its consortium includes the following organizations: Telenor (Norway), BT (UK), Telefonica (Spain), Samsung (UK), Huawei (Germany & Norway), Ericsson (Norway), Nokia (Finland), Software Radio Systems (Ireland), Lime Microsystems (UK), EANTC (Germany), Keysight Technologies (Denmark), Simula (Norway), Fraunhofer FOKUS (Germany), Eurescom (Germany), Altice Labs (Portugal), University of Patras (Greece), Universidad Carlos III de Madrid (Spain), Athens University of Economics and Business (Greece), Intracom Telecom (Greece), Cisco (Norway), Engineering (Italy), and SES TechCom S.A. (Luxembourg). It was kicked-off in July 2018 with a 36-month duration.

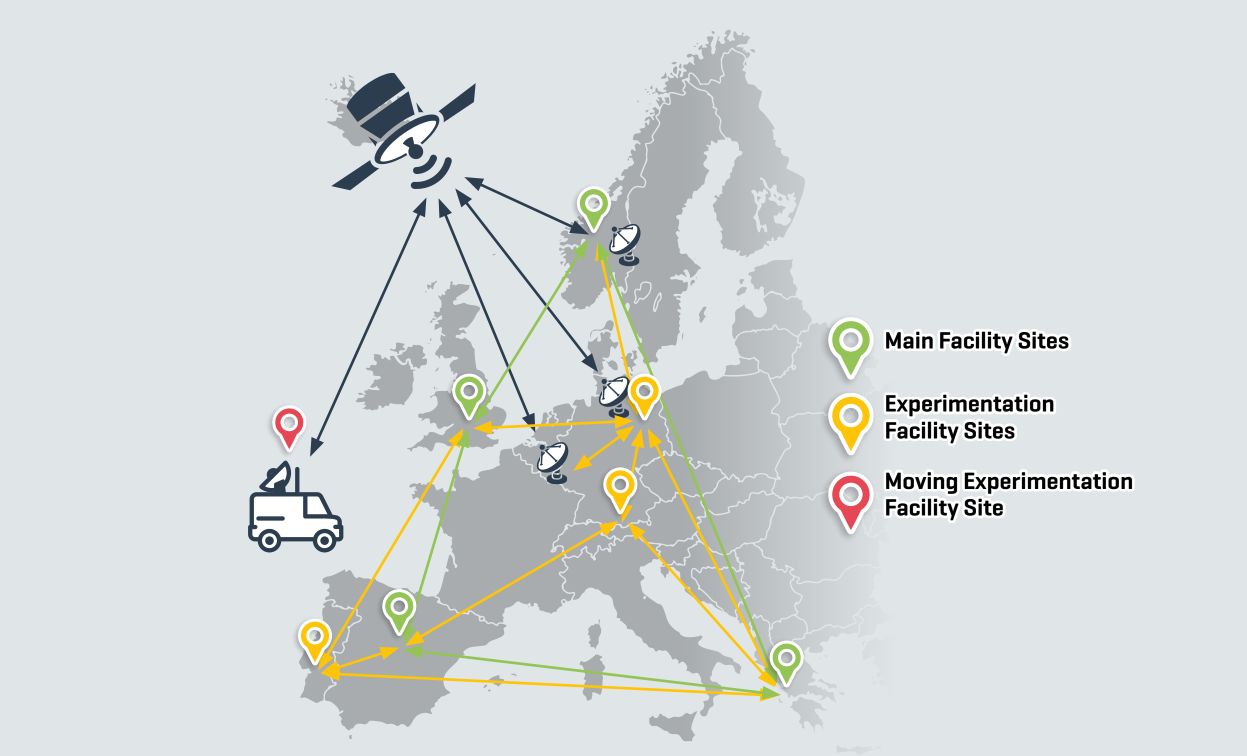

Main Facility Sites
Experimentation Facility Sites
Moving Experimentation Facility Site

*Figure 12: 5G-VINNI Facility Sites*

5G-VINNI is expected to accelerate the uptake of 5G in Europe by providing an end-to-end (E2E) facility that lowers the entry barrier for vertical industries to pilot use cases and supports the pilots as the infrastructure evolves. To achieve this, the objectives of 5G-VINNI are: Design an advanced and accessible 5G end-to-end facility; Build several interworking sites of the 5G-VINNI E2E facility; Provide user friendly zero-touch orchestration, operations and management systems for the 5G-VINNI facility; Validate the 5G KPIs and support the execution of E2E trial of vertical use cases to prove the 5G-VINNI capabilities; Develop a viable business and ecosystem model to support the life of the 5G-VINNI facility during and beyond the span of the project; Demonstrate the value of 5G solutions to the 5G community particularly to relevant standards and open source communities with a view towards securing widespread adoption of these solutions. The 5G-VINNI E2E facility include the following sites (see Figure 12):

- Main sites: E2E 5G-VINNI facilities that offer services with well-defined Service Level Agreements (SLAs). These include sites located in Norway (Oslo, Kongsberg), UK (Martlesham), Spain (Leganés), Greece (Patras);
- Experimentation sites: provide environments for advanced focused experimentation and testing. These include sites located in Portugal (Aveiro) and Germany (Berlin and Munich), as well as a Moving Experimentation site corresponding to SES' satellite connected vehicle.

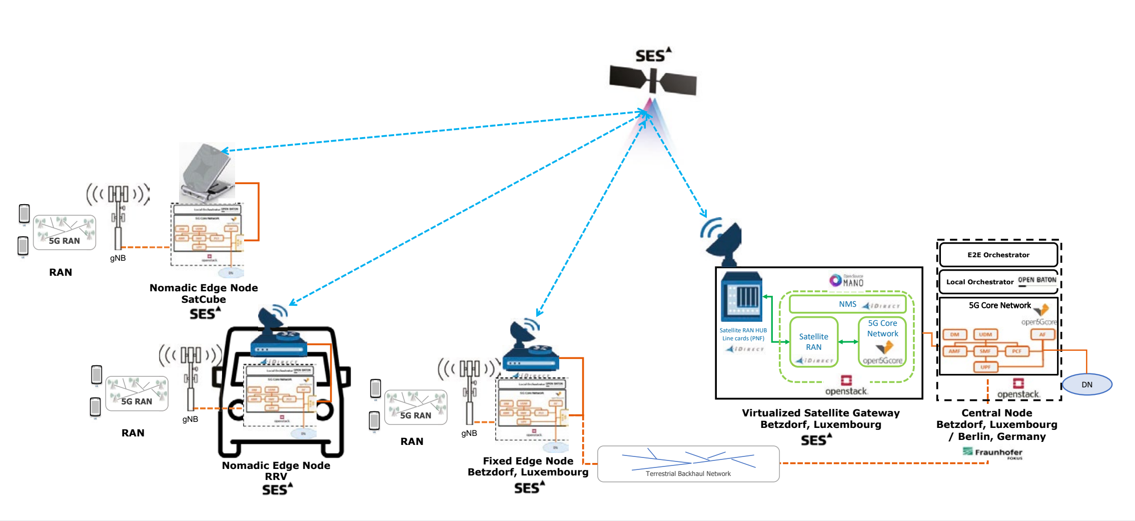


*Figure 13: 5G-VINNI Moving Experimentation Facility Site Architecture*

Particularly, the 5G-VINNI moving experimentation facility site concentrates on the research, development, experimentation, validation and demonstration of customized solutions for satellite integration into 5G, with a focus on satellite backhauling services. It is enabled by the SES' satellite connected vehicle (also referred to as "Rapid Response Vehicle" – RRV) which provides satellite backhaul capabilities and will enable the 5G-VINNI moving experimentation facility site to become a rolling lab for 5G mission-specific solutions. The 5G-VINNI moving experimentation facility site builds upon synergies with the SATis5 testbed developed as part of the SATis5 project (see section 2.1.2.6.3). Thus, it hosts the satellite 5G testbed node providing SDN/NFV/MEC capabilities and enabling both eMBB and mIoT use cases over satellite [38] (see Figure 13).

# 2.2 IoT in connected vehicles

## 2.2.1 Background

These days, the transportation system and vehicles digital journey system are moving towards a data-based mobility and transport paradigm centered on multimodal [39], low carbon, on-demand and personalized travel, enabling accurate access to information (data) in real-time. The concept of transportation is rapidly changing, overcoming the traditional approach. The concept of individual ownership of vehicles, limited insights on traffic information and journey choices, and rigid separation between public and private transport is slowly being replaced by a more modern transport system. The adoption of common data management platforms in order to cultivate an open connected vehicles data marketplace in the current transportation system, is expected to enable a faster, better and safer travel experience for commuters. Several automotive players are hugely investing in full digitalization of their products and services. According to an IDC report [40], global spending on technologies related to the transportation sector, including connected vehicles, was €71 billion in 2019. The European market is expected to double by 2021, fostering new business models and opportunities in the broader sector of the connected vehicles ecosystem. As shown in Figure 14, recent technological advancements in ICT, such as the IoT, would further enhance the quality of operation of the current system. Considering the need for increasing situational awareness on road risks and crashes, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) solutions and infrastructure are expected to be top EU connected vehicle investment priorities in the coming years. According to the IDC report [40], infotainment vehicle solutions, fleet management, vehicle security and emergency assistance, insurance telematics, V2V/V2I communications, intelligent transport systems were highly invested sectors in the connected vehicles domain.

*Figure 14: Adoption of technology in the transportation systems*

In contrast to connected vehicles, Autonomous Vehicles are vehicles with the technology system that endow self-driving capabilities. Some of the functionalities, such as self-driving, self-parking or auto-collision avoidance features, are already being deployed in current vehicles. Figure 15 shows the level of autonomy in a driving system, ranging from "No Automation" (traditional human driver) to "Full Automation" (future of automated driving system). The rest of the section intends to provide examples of some national use cases related to connected vehicles.

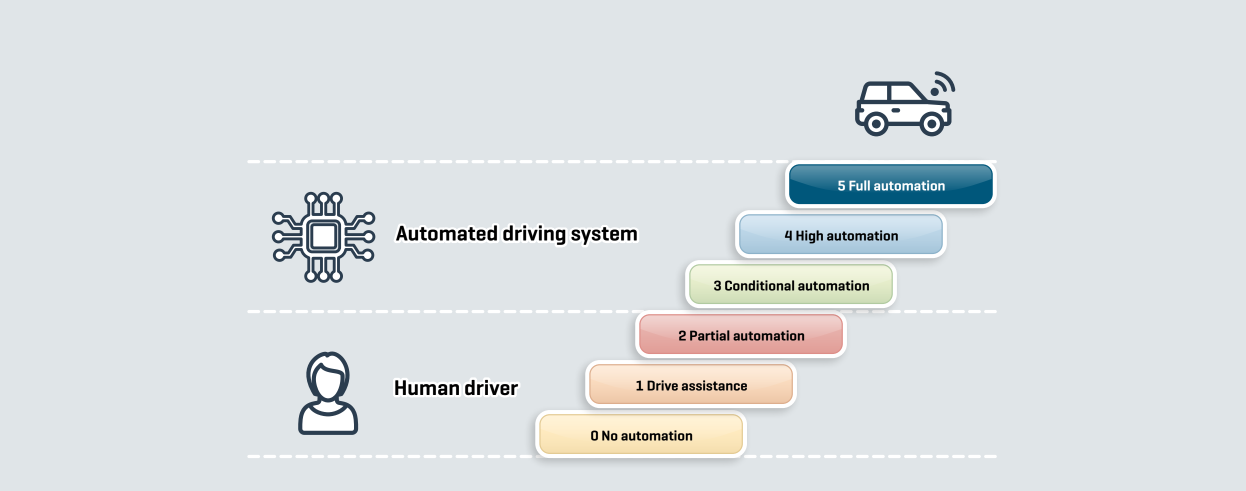


*Figure 15: Level of autonomy in a connected vehicle [41]*

## 2.2.2 A typical example of connected vehicles using IoT

Figure 16 depicts the simplified ecosystem of connected vehicles. It is an expanded view of Figure 14, which gives the technical landscape.

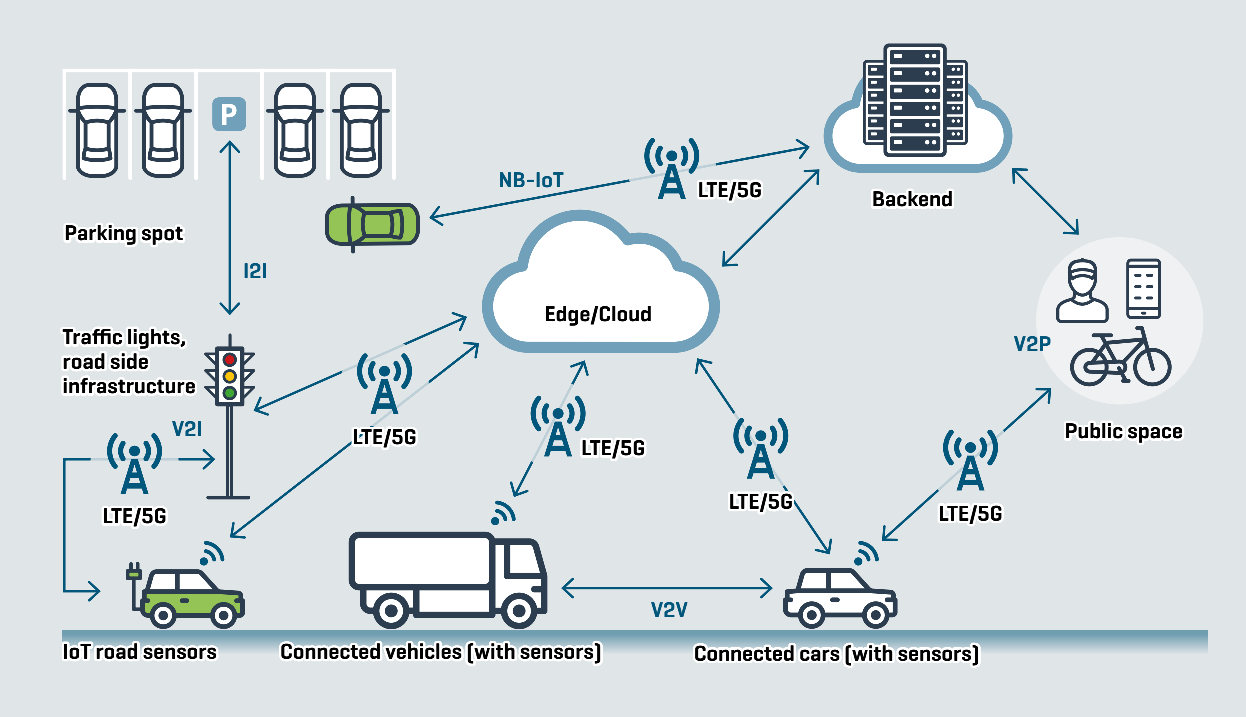


*Figure 16: Simplified connected vehicle ecosystem*

#### 2.2.2.1 The connected vehicles ecosystem

Some players of the connected vehicle ecosystem include, but are not limited to, those listed in Table 13.

| Key players | Examples |
|---|---|
| Transport infrastructure and infrastructure providers | Roads, highways, and transport providers |
| Automotive players | OEMs, Auto dealers, repair and service centers |
| Technology providers | Connectivity, hardware/software, and other related infrastructure services providers |
| Regulators | The government, public organizations and related bodies |
| Drivers/users | Personal drivers, commercial drivers, and other users |
| Service providers (support) | City information, security and safety assistance, insurance, infotainment |

*Table 13: Key players of the connected vehicle ecosystem*

#### 2.2.2.2 Typical data flow in the ecosystem

A block diagram of the typical data flow within the ecosystem is depicted in Figure 17. Multiple sensing techniques are used to collect (real-time) information of vehicles, users and other components used within the system. The user interface represents the input and output devices that interact with physical ends. Particularly, in this ecosystem, the central system provides specific instructions to bus drivers in order to best operate the bus. Control systems are responsible for various control mechanisms, such as support, incident control, verification, and incident detection. Computing and processing belong to the analysis of enormous data (Big data) received from multiple actors of the ecosystem. Various communications take place in and out of the system. Table 14 provides a technical landscape with IoT based technologies for this sector.

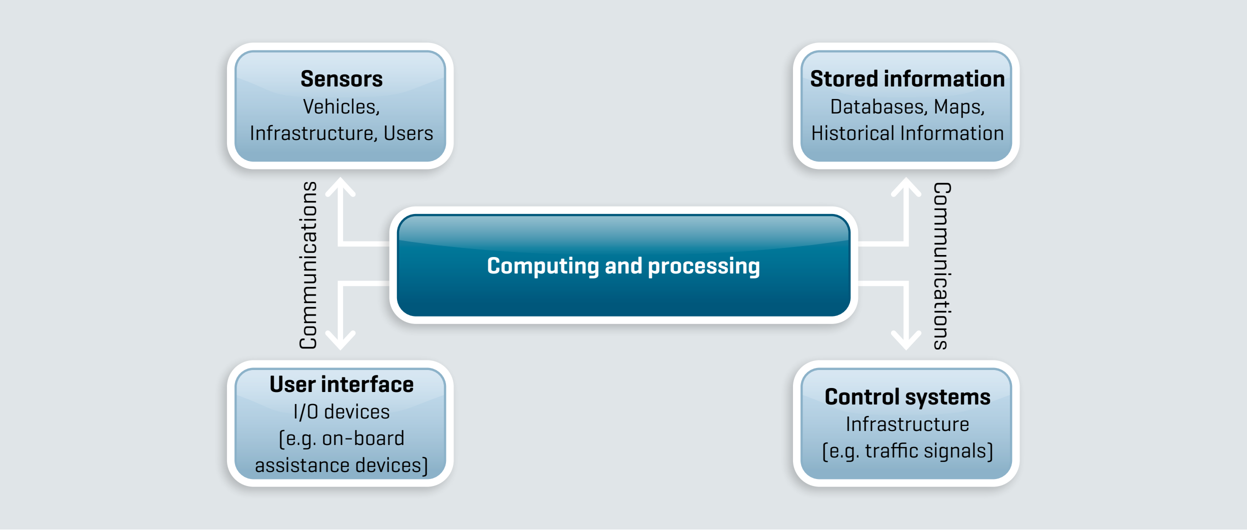

Sensors
Vehicles, Infrastructure, Users
Stored information
Databases, Maps, Historical Information
Communications
Computing and processing
Communications
User interface
I/O devices (e.g. on-board assistance devices)
Control systems
Infrastructure (e.g. traffic signals)

*Figure 17: Typical data flow in the connected vehicle ecosystem*

| Technology | Purpose | Examples of components used |
|---|---|---|
| Sensing technologies | Automatic Vehicle Location (AVL), Automatic Passenger Counts (APC), Automatic Fare Systems, Automatic incident detection system | Radar, LiDAR, ranging instrument |
| | Pedestrian detection system | Optical sensors use light to measure soil properties in smart farming |
| | Road weather information system | Sensors to detect rain, wind, snow, fog, etc. |
| Interfacing | User interface | IoT nodes, IoT gateways to be interfaces with satellite system |
| Bluetooth, Wi-Fi, NB-IoT, SigFox, LoRa, 3G, 4G, 5G, LTE etc. | Communication between the components of the ITS ecosystem | - |
| V2V, V2I, I2I, V2P | To perform prevention of collision in high-speed driving environment, traffic information providing service, control vehicle | Vehicle on-board Unit or equipment (OBU or OBE), roadside unit or equipment (RSU or RSE), safe communication channel |
| Processing and computing | Analyzing and processing real-time information and historical information | C-ITS server, Big data, Cloud Computing |

*Table 14: Technical landscape in connected vehicles*

### 2.2.2.3 Industry benefits

Some of the benefits for the players of the connected vehicles ecosystem using IoT include, but are not limited to, those listed in Table 15.

| Transport infrastructure and infrastructure providers | Automotive players | Technology providers | Regulators | Drivers/users | Service providers (support) |
|---|---|---|---|---|---|
| Insights into traffic condition to map with and infrastructure capacity | Advanced and safer products | Adoption of the latest technological trends | Ease in digital data access | Enhanced and satisfactory services | New business models and services |
| Reduced commute time, and Better safety conditions | Full use of recent technologies in customer support and after sales support services | New business models and services using IoT enabled automated vehicles | Fostering citizens' mobility, digitalization, safety and environmental benefits | Clear insights into the use of services | Clear insights into public safety and related services |
| Insights into maintenance operations and infrastructure alerts | New market players | Broad market and partnership opportunities with other technology players | Collaboration and networking opportunities with stakeholders | Safety, security, economic commutation | - |

*Table 15: Benefits due to connected vehicles ecosystems*

### 2.2.2.4 Related issues/challenges across the sector

Connected vehicles together with IoT Technologies have the potential of unleashing a more sustainable and efficient transportation system. Some challenges for integrating connecting vehicles into the IoT ecosystem include, but are not limited to, those highlighted in Table 16.

| Challenges | Description |
|---|---|
| Data collection | Uniform description and data collection mechanisms from vehicular sensors<br>Data collection using a uniform mechanism is becoming a challenge in this sector because of the increasing numbers of heterogeneous sensors and actuators found within vehicles. The collection and communication of vehicle maps and vehicle sensors' data are fundamental to enable quick reactions in highly autonomous vehicles. It relates to the challenge of data processing and actuation [42]. |
| Interoperability | Seamless interoperability of vehicular communication networks, mobile devices and deployment platforms<br>The interoperability of smart devices in vehicle and transport systems can help in also collecting the data of vehicles' environments. The combination of vehicular and environmental data in a single computing platform remains challenging due to massive data format and content differences, and the lack of a standard method for adequate data fusion. |
| Integration | A standard vehicular IoT architecture<br>The seamless integration within an IoT architecture of a vehicular network and many smart devices, complete with a storage capability and edge computing, is extremely complex as these building blocks are all heterogeneous in terms of the underlying technologies. |
| Running in real time | The ability to support real- time scenarios<br>Recent IoT platforms and services - mainly cloud-based - depend on RESTful web services and Internet Protocol (IP) technologies to guarantee interoperability. At the same time, such cloud-dependent scenarios could be prone to less QoS and higher latency. In addition, they may not be suitable for real-time applications. To provide the safety necessary to highly autonomous scenarios, edge computing platforms could be an alternative solution to support adequate real-time processing for vehicles. |
| Safety and security | Safety of the driver-passengers and secure communication<br>Safety of drivers and passengers should be the primary focus in this sector. Increased attack surface from Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications is equally critical. Data encryption (AES and SSL), authentication, and data channel access control are the major IoT data security components. With connected car, IoT developers can build point-to-point applications, where data streams bi-directionally between devices. Having the ability to grant and revoke access to user connection is just another security layer on top of AES and SSL encryption. |

*Table 16: Challenges to integrate connected vehicles into the IoT ecosystem*

### 2.2.2.5 Cybersecurity objectives, risks and threats

The safety of drivers and passengers should be the main focus of vehicle manufacturers [4]. Particularly in this sector, more attention should be paid to minimizing the new attack surface arising from V2V, V2I, and V2X communications. Apart from physical safety, privacy issues are other concerns. For example, users are connected to their vehicles through their smart phones and have access to their personal information. In this context, both vehicle and smartphone data require protection. Table 17 provides examples of cybersecurity objectives in the connected vehicle sector [4].

| Cyber security objectives | Description |
|---|---|
| Confidentiality | V2V, V2I, and V2X communications require dedicated cryptographic protection. |
| Integrity | The contents of messages requires protection from modification. |
| Availability | The real-time nature of V2I, V2V, and V2X communications requires extremely high resilience and reliability. |

*Table 17: Cyber security objectives in connected vehicle sector*

The connected vehicle sector faces many of the same risks as other IoT and cyber systems in general. Several safety concerns to vehicles and people require risk assessments to be developed [43]. The addition of Internet connectivity to "infotainment" consoles has also introduced threats to driver as well as passenger safety as a result of communications between vehicle controls and entertainment applications. Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Everything (V2X) communications introduce new attack loopholes. Thus, it is necessary to take appropriate security measures within different subsystems and any interactions among them. These project measures could be against device malfunction, user error, and device damage.

### 2.2.2.6 Examples of national initiatives in connected vehicles

Considering the market trends in implementing IoT-based technology in the connected vehicle sector, some of the national initiatives in this domain have been identified in this report

#### 2.2.2.6.1 Electrified Cooperative Bus System (eCoBus) project[10]

The Ministry of Sustainable Development and Infrastructures and the Ministry of the Economy, together with Volvo Buses, launched the first Competence Center [44] for electromobility in 2016 to develop and implement smart e-mobility projects for cities, with a strong focus given to environmental protection and noise reduction [44]. Later on, with the Electrified Cooperative Bus System project (eCoBus), the University of Luxembourg teamed up with the Luxembourg Institute of Science and Technology (LIST) to design C-ITS based solutions to increase the operating efficiency and comfort of the next generation of urban public transport systems. The Ministries of the Economy and Sustainable Development, E-Bus Competence Center (EBCC), and Sales-Lentz support this project and actively contribute to creating in Luxembourg a test arena for sustainable public transport systems. It aims to test and evaluate the system not only in extensive simulations, but also in real controlled experiments supported by public transport industry partners – EBCC and Sales-Lentz to analyze and optimize the multimodal transportation network available in Luxembourg and its surroundings. The timeline of the project is 2017 to 2020. The project considered the following trends towards next generation public transport systems:

- to introduce greener vehicles, such as electric or hybrid buses;
- to facilitate high-quality services, such as increased ride comfort via mitigation of stop-and-go driving;
- to reduce emissions and vehicle operating costs related to energy consumption and equipment wear-and-tear.

[10] https://ecobus.lu/

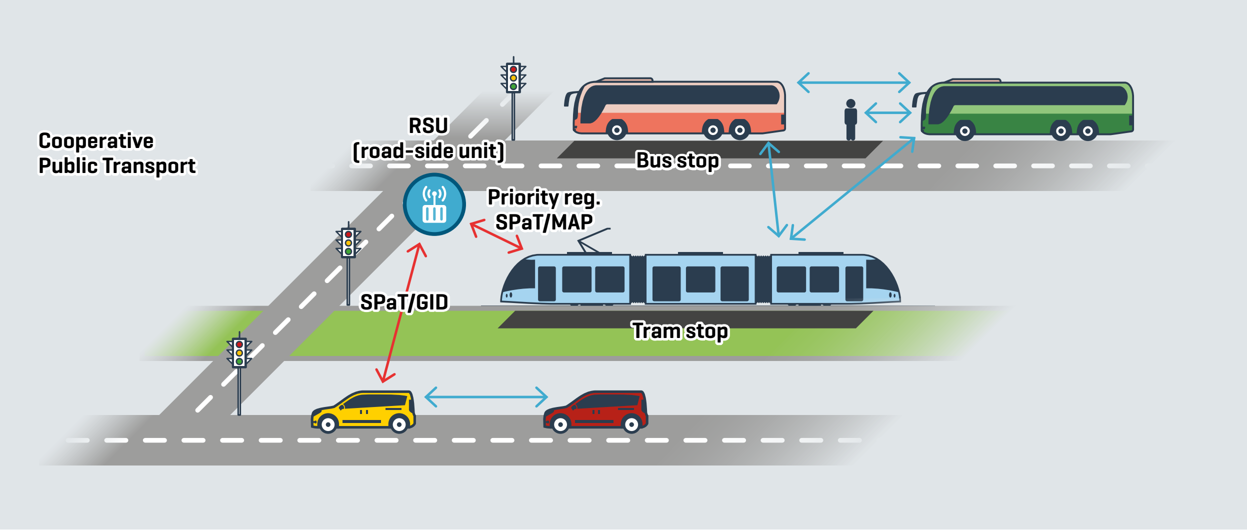


*Figure 18: Approach developed within eCoBus project*

The project aims at designing a new system approach to address the current public transport ecosystem, which consists of control signals, (e-)buses, and e-bus charging infrastructure. The IoT infrastructure modeled in the project can combine cooperation and negotiation between all actors of the ecosystem. The connectivity provided as an emerging Connected Vehicle (CV) technology allows shifting from standalone ITS systems to the C-ITS paradigm. In the C-ITS, actors of the ecosystem not only can collect and share information, but also cooperate with each other for improving safety and efficiency of transportation [45], and mutually help in achieving the overall system's goals. The new multi-layer approach designed in this project is depicted in Figure 18. On the top layer, the charging infrastructure and signal control system is assumed to provide information and to be managed by external actors (energy providers, traffic control center). They, however, provide an indication of their priorities by e.g. dynamic pricing of charging or by conditional transit signal priority. The middle layer, named Cooperative Bus System (CBS), represents the bus fleet control system. In particular, buses cooperate to achieve overall service efficiency and reliability (e.g. regularizing the headways between vehicles) and try to optimize operations taking into account constraints and costs coming from the support infrastructure layer. The CBS interacts with signal control and a centralised PT back office system that manages bus locations, electric bus energy states, and passenger data. Finally, the bottom layer represents the real (or simulated) multimodal network, where public transport vehicles interact with the other traffic flow agents (cars, pedestrians, etc.).

Existing methods to enhance public transport operations, such as Transit Signal Priority (TSP) and holding strategies, are designed only for supporting the simple objective of punctuality, and thus are not capable of handling the complex next-generation transport system. In the C-ITS, negotiation-based strategies can be used in case of conflicting objectives, such as signal optimization for public transport vs. cars. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication bring together the actors of the ecosystem that include vehicles, passengers' personal communications devices, infrastructure (traffic signal, charging stations) and the Traffic Management Center (TMC). Access to Signal Phase and Timing (SPaT) status from signal controllers are the key enablers for the new Cooperative Driver Assistance Systems (C-DAS) to improve the efficiency of conventional TSP, as well as partially replace its non-functionality in a traffic non-invasive way.

By working on an integrated approach, eCoBus pursues the following objectives to:

- improve service reliability through reducing vehicle headway variations, reducing headways between vehicles near signals and interchanges, and reducing the deviation between schedules and actual arrivals;
- improve passenger utility by reducing stops at traffic signals, by minimizing the waiting time of passengers at interchanges, and reducing crowding/bunching effects;
- decrease energy consumption and emissions by adapting speeds near signals to both avoid unnecessary stops and to reduce instantaneous consumption and emission rates;
- facilitate cost-efficient and low-impact use of e-charging infrastructure by electric buses by distributing charging in time and space according to (given) energy pricing schemes;
- The increase of PT service capacity with low or no impact on general traffic by reducing the number of calls for priority, and by reducing modification requests of phase plans.

The project advanced the research in this area in three aspects:

1. At the tactical level, new mathematical approaches have been formulated and solved to optimize the assignments of a mixed bus fleet (hybrid and electric) to the timetable, which take into consideration the time and resource constraints brought by the charging operations. Feasible and economically efficient solutions have been found, together with the optimal mix of vehicles to adopt.
2. At the operational level, new real-time control strategies have been developed, exploiting AVL information and using V2I communication to jointly reduce the number of stops for the buses at signals and for regularizing line operations. Thanks to these new hybrid strategies, buses have been shown to reduce their energy consumption and at the same time the overall quality of service of the system increased.
3. Simulation and controlled testing environments have been adopted to assess and showcase the impact of C-ITS communication in a realistic scenario involving major bus lines in Luxembourg City.

#### 2.2.2.6.2 Multimodal MoBility Assistance (MAMBA) project[11]

MobiLab[12] is the Transport Research Group of the University of Luxembourg (Uni.lu). The team performs education and research activities ranging from advanced traffic and transport data analysis, transport planning and control, mobility and traffic modelling, sustainable transport services optimization and supply chain and logistics management. This brings an interdisciplinary vision, linking Engineering, Computer Science, Human Sciences, and Economics. The Multimodal MoBility Assistance (MAMBA) project was one of the projects of MobiLab created to explore and analyze the multimodal transportation network. Considering real-time traffic conditions, the status of existing public transport services (e.g. buses, trains) and user preferences, a personalized travel assistant is developed that is expected to proactively suggest the best transportation possibility to reach a desired destination, while also balancing the load over the different transportation modes in the multimodal system. Nowadays in Luxembourg, most people prefer to use private vehicles as their main means of transportation. Consequently, the road network has become increasingly congested. Even now, its capacity is often reached during rush hour, and the situation becomes significantly worse in case of accidents or road works.

The MAMBA project was intended to explore and analyze the multimodal transportation network available in Luxembourg and its surroundings and propose new solutions to enhance individual mobility by making use of new end-user technologies such as smartphones. In the past, gathering information on how to travel between different points of interest was a time-consuming and often inefficient process, as this information was not centralized and the status of services was unknown. With growing transport demand and the expansion of the transportation network, it is crucial to better inform commuters about the existing alternatives. In particular, this project proposed a holistic mobility approach that combines different information sources that provide real-time information on the status of public transport (e.g. buses and trains).

[11] https://mobilab.lu/mamba/

[12] https://mobilab.lu/

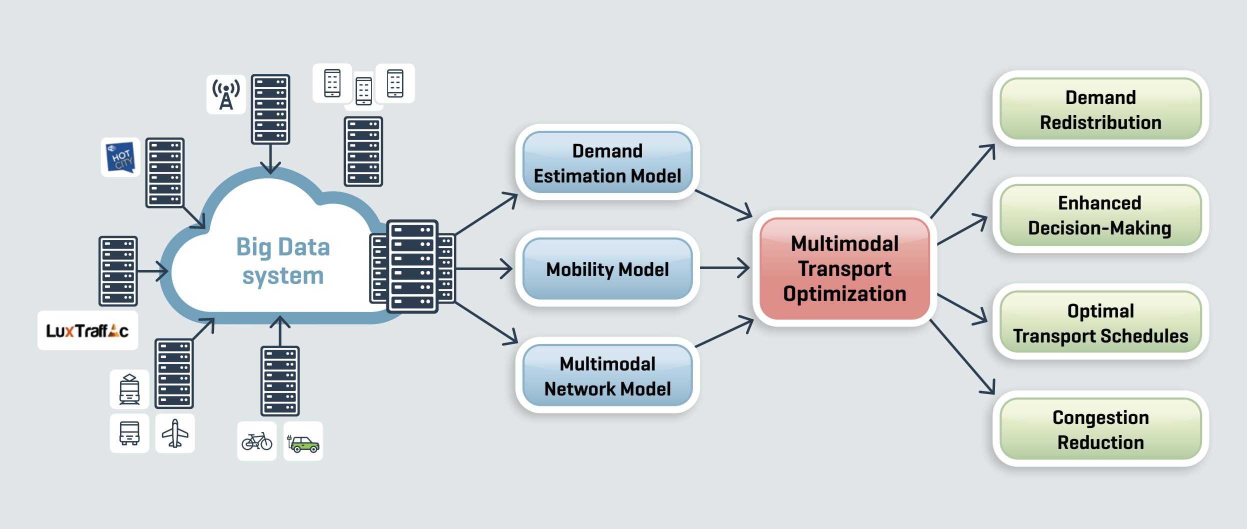


*Figure 19: System architecture of MAMBA project*

The project leveraged connected technology, in particular vehicle connectivity and location, to estimate and predict traffic conditions and analyze the mobility patterns in urban environments. In particular, new relations between connected vehicles movements and traffic flow and transport demand characteristics (speeds, travel times, mobility patterns) have been modelled.

# 3

# Internet of Things: Technical standardization

# 3. Internet of Things: Technical standardization

Information and Communication Technology (ICT) is the infrastructure and components that enable modern computing, where standards play an essential role in achieving interoperability in the complex ecosystem of ICT technologies and can bring significant benefits to both industry and consumers [1], [10], [46], [47]. Standards also guarantee that such technologies work smoothly and reliably together. Furthermore, they help to keep ICT markets remain open and allow consumers the widest choice of products. In the context of digitization of the global economy and society which affects all sectors, ICT standards are more relevant where the world tends to become all digitized and everything becomes connected.

The success of any technology is eventually highly dependent on the elaboration of such complex interoperable global standards within and across applications, and this dependence will only increase with time. For example, in the case of the IoT, more and more devices will be connected to each other ranging from cars and transportation systems, to appliances and e-Health systems. For the European market, the European Commission has proposed, in its communication "ICT Standardisation Priorities for the Digital Single Market" [48], to focus standard-setting resources and communities on five priority areas including the IoT and 5th Generation Mobile (5G) as essential technologies for wider European Union competitiveness. Moreover, both technologies are referenced as key enablers to support EU policy objectives for completing the Digital Single Market in the 2020 rolling plan for ICT standardization [46]. Before providing IoT-specific standardization initiatives, the concepts of standards and technical standardization are provided in the following section.

## 3.1 The concept of technical standardization

Standards are effective economic tools for achieving various objectives, such as mutual understanding, reduction of costs, elimination of waste, improvement of efficiency, achievement of compatibility between products and components or access to knowledge about technologies [49]. In this context, technical standardization is a keystone to ensure interoperability of complex ICT systems and it contributes to minimizing the barriers that may exist to build the future of the digital world. The European Commission's communication "ICT Standardisation Priorities for the Digital Single Market" highlights that technical standardization is an essential component of industrial competitiveness [46]. Regulation 1025/2012 on European standardization [50] sets the legal framework in which the actors in standardization (the European Commission, European standardization organizations, industry, SMEs and societal stakeholders) operate. More significantly, the role of standardization is to support the stakeholders of the various economic sectors, such as developers, researchers, government, regulators and users all over the world.

In particular, technical standards are important [48], [9], [51] to ensure i) interoperability across products, services and applications, which helps to avoid vendor lock-in, ii) inter-operation across physical communication systems, protocol syntax, data semantics as well as domain information, and iii) security and privacy of data and users including physical security of products, services and systems. Moreover, technical standards can help to establish and maintain digital trust in ICT technologies, for example by setting up appropriate information security management systems, providing common communication protocols, allowing interoperability between different applications and technologies, etc.

Technical standardization is widely recognized for its ability to provide a technical or qualitative referential for products, services or processes. Technical standards are developed within standardization bodies that bring together all interested stakeholders and are active at different geographical levels in their own areas of competency, as illustrated in Figure 20. The International Organization for Standardization (ISO) [52], the International Electrotechnical Commission (IEC) [53] and the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) [54] are the three recognized Standards Development Organizations (SDOs) at the international level. Likewise, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) [55] are the three recognized European Standardization Organizations. They develop standards, guidelines, and specifications to support stakeholders in ICT deployment. SDOs can be broadly classified into two categories from the perspective of technological offerings: generic and application-specific. On one hand, the organizations of the first category play a pivotal role in defining technology standards to cover the overall problem space. The organizations of the second category, on the other hand, are created in the interest of standardizing technologies for some specific domain of applications. This report intends to provide an overview of SDOs and alliances, which provide generic standards.

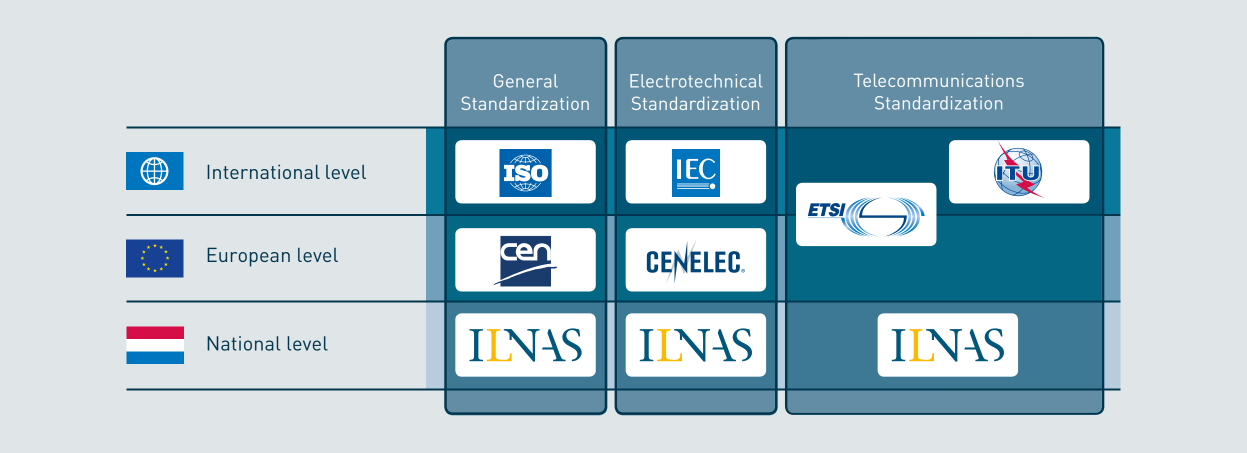


*Figure 20: International standardization organizations and their area of competence*

At national level, each country has one national standards body (NSB) that works for the interests of the country and co-ordinates with European and international standardization organizations. In Luxembourg, ILNAS is the NSB and is a member of CEN, CENELEC, ETSI, ISO, IEC and ITU-T (see Figure 20).

## 3.2 The need of technical standardization in IoT

Technical standardization is one of the most critical parts of the IoT's evolution [56], [57]. The growing complexity of devices or services that need to connect and communicate with each other will only increase without global standards [58]. That complexity is associated to interfaces, quality of service, communication, security, related addressing, and much more. In this context common standards provide guidelines for billions of connected objects in order to operate with an acceptable, manageable and scalable level of complexity. In the current model, most IoT solution providers have been building all components of the stack, from the hardware devices to the relevant services, for example cloud services. As a result, there is a lack of consistency and standards across services used in different IoT solutions. As the organization or structure of the industry evolves, the need for a standard model (e.g. IoT reference architecture) becomes more relevant to construct common IoT backend solutions, such as processing or storage [59]. In the new model, different IoT solutions are expected to work with common backend services. It provides levels of guarantee of interoperability, portability, manageability, etc., which are still missing in the current IoT [10].

Let us take an example: data is collected by sensors within IoT devices and transmitted through networks (wired or wireless), stored in the cloud, and aggregated for analysis through analytics and related intelligence applications. In this case, technical standardization is important to solve the issues of interoperability or interconnectivity. Apart from this, it is also equally important to reduce the gaps between protocols and associated security issues and other loopholes. In general, technical standardization enables more compatible components, which leads to reduce the cost of design, manufacturing, implementation and reduces time-to-market. Prior to providing the technical standardization landscape in IoT ecosystem, the composition of various components of IoT solutions will be provided to understand what the challenges are for components of IoT implementation [59] and how technical standardization is important to minimize such issues (see Figure 21). Standards lead to basic guidelines that can be followed by developers/manufacturers to minimize those challenges.

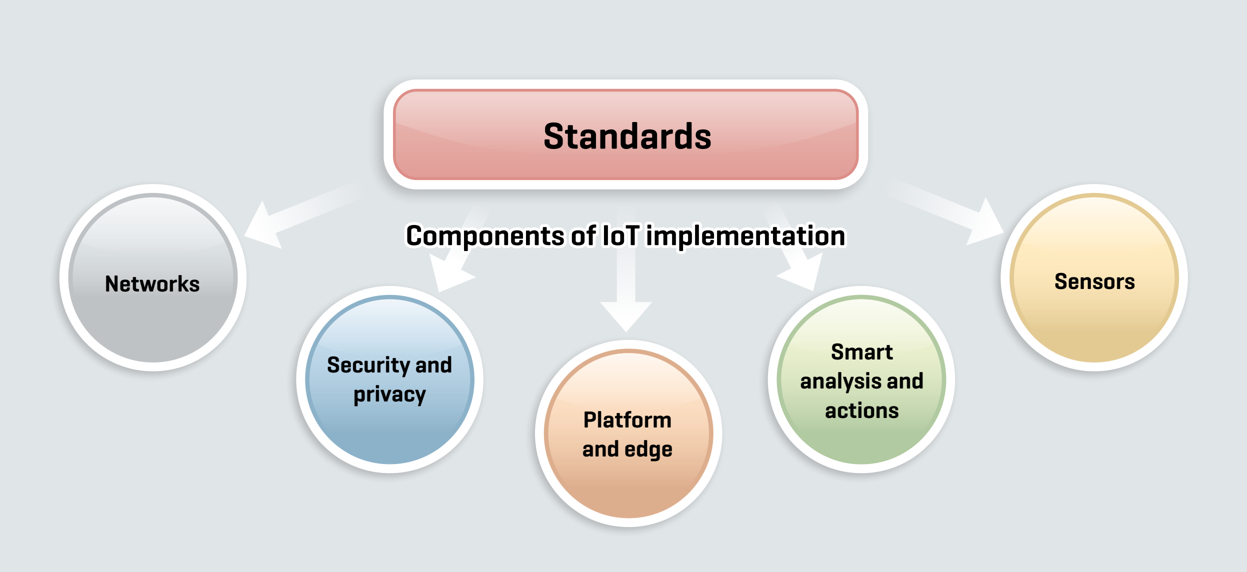


*Figure 21: Components of IoT implementation and need of Standards*

### 3.2.1 Sensors

New trends in technology help manufacturers produce sensors that are cheaper, smarter and smaller, which drives an increase in the number of sensors installed by IoT solution providers. But due to the multiple vendors and technologies used, IoT sensors face problems of interoperability, power consumption, and security and privacy.

### 3.2.2 Networks

High data rates, high availability, cheaper cost for data usage, virtualization etc. are the some of the network prerequisites for wide adoption of IoT technology. As mentioned earlier, networks are used to transmit data collected by sensors with different components including routers and bridges in different IoT implementations. Now, connecting different parts of the networks to the sensors is done by different technologies (e.g. WiFi, cellular networks). But smooth interconnectivity and heterogeneity of the networks, availability of network coverage, power consumption, security etc. are still missing in the context of the enormous growth in connected devices.

### 3.2.3 Platform and storage

The platform in the IoT includes the form and design of the products and analytics tools used to deal with the massive data streaming from all products in a secure way. Most of the IoT data (structured or unstructured) will be stored and fed to analytics functions to generate insights. The storage in the IoT should accommodate an increasing number of data files generated from sensors. Cloud-integrated storage, or cloud storage, is ideal for IoT-specific data. In addition to Cloud computing-specific issues, such as security and privacy, control, performance etc., smooth interoperability between cloud providers is still missing from a technical standardization point of view.

### 3.2.4 Intelligent analysis and actions

The components include the tools which extract insights from data for analysis. Generally, IoT analysis is driven by cognitive technologies and related models. But IoT implementation is still facing problems because of inaccurate analysis due to flaws in data sources, the limited ability to analyze and manage unstructured and real-time data, missing data extraction guidelines, etc.

### 3.2.5 Security and privacy

The IoT is not only about connecting devices, it interconnects a variety of vertical sectors, such as smart homes, buildings and cities as well as energy (electrical, gas, water) grids/networks, automobiles, etc. As mentioned in 3.2.3, the integration of IoT devices with such storage and computing power network leads to huge security challenges due to the substantial increase in the attack surface, heterogeneity, complexity and other number of resources [60]. Privacy issues are also significant in the IoT depending upon different jurisdictions. So, security and privacy are common issues for the components (Sections 3.2.1 to 3.2.4) involved in IoT implementation.

### 3.2.6 Standards

As discussed before, the IoT has a complex and fragmented landscape. The components mentioned before are inter-related, all of them are important to make the system operable. Missing one of them will break the entire system. Many stakeholders (e.g. SDOs, manufacturers, developers, researchers, governments, and regulators) have their own role to smoothly run the entire IoT ecosystem. In this context, standards help entities work together, no matter their role in the IoT implementation, by providing vendor-independent common guidelines applicable for all concerned stakeholders.

The report ETSI TR 103 376, published in 2016, provides a gap analysis of IoT technical standardization and concludes with the following priorities to be addressed:

- Interoperability is an essential for the deployment of the IoT ecosystem and for ensuring the seamless flow of data across sectors and value chains;
- Solutions should be more than technical solutions;
- Existing standards should 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.

Following this standards gap analysis, a list of challenges in the entire IoT ecosystem mainly from the perspective of technical, business, and societal [9] as well as from the view of technical standardization has been identified in Section 1.4. On the basis of those challenges, efforts of the SDOs and gaps in IoT technical standardization will be further analyzed in the next sections.

## 3.3 Technical standardization landscape in IoT

Several SDOs and alliances are involved in the process of IoT technical standardization, as illustrated in Figure 22. These initiatives are projected across two dimensions: market type on the horizontal axis, and technology/solution/knowledge area on the vertical axis.

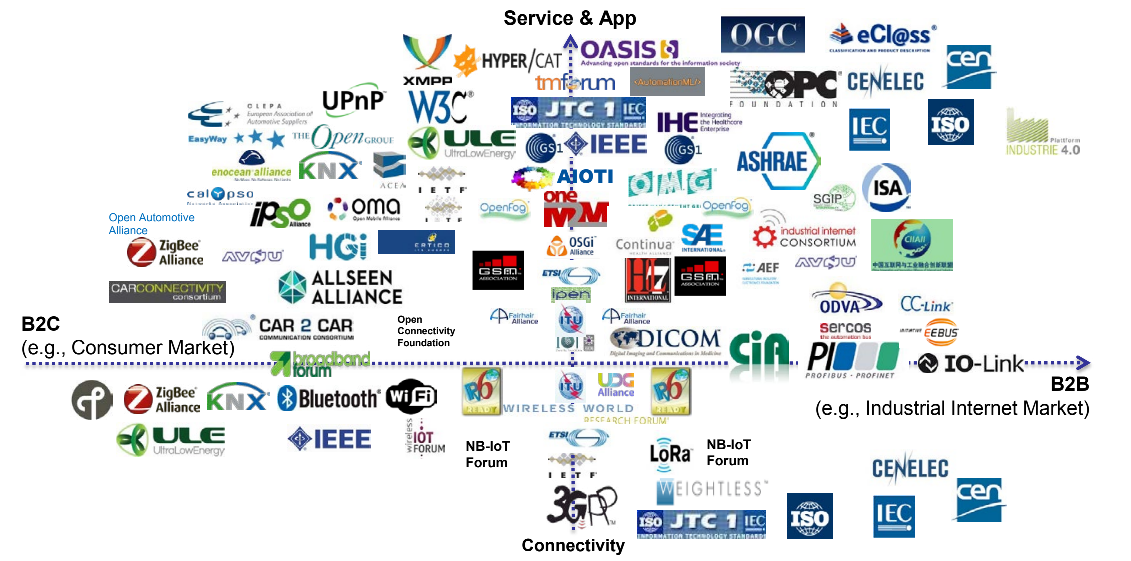


*Figure 22: SDOs and alliances landscape in IoT (technology and marketing dimensions) standardization [61]*

Figure 23 provides the landscape of SDOs and alliances involved in domain-specific standardization related to the IoT. The ILNAS IoT White Paper [1] provided a summary of major SDOs and alliances involved in IoT technical standardization. This report further considers their efforts towards technical standardization and related gaps in IoT deployment.

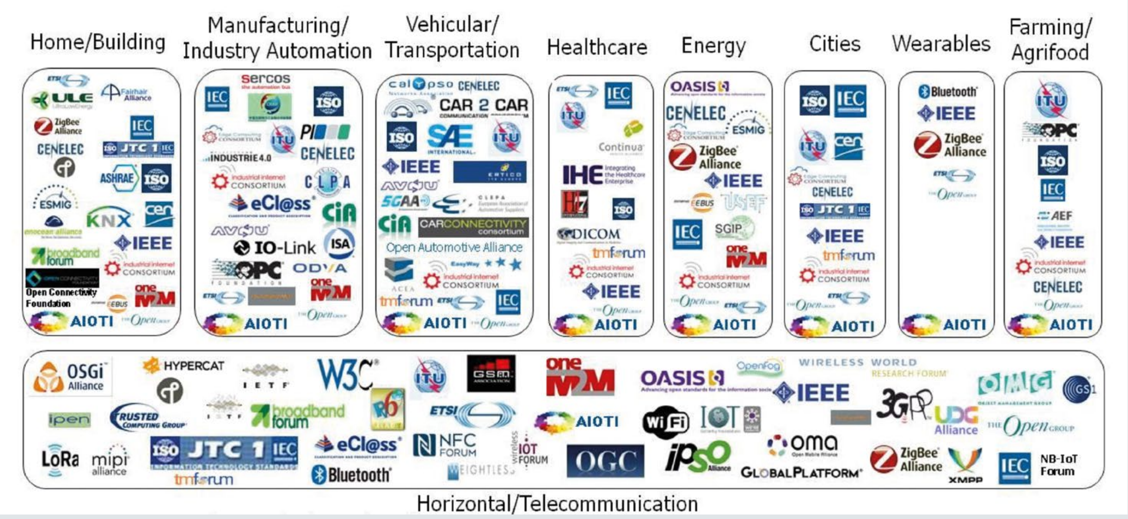

Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

*Figure 23: SDOs and alliances landscape in IoT domain-specific standardization [2]*

It is worth mentioning that the satellite and related connectivity as well as the connected vehicle sectors are covered in Chapter 2 as representative national examples of IoT applications in those horizontal and vertical domains [2] as indicated in Figure 23. The rest of the section is intended to show the overall efforts of SDOs and alliances related to IoT as well as sector-specific standardization efforts in the sectors selected in Chapter 2.

## 3.4 Technical standardization efforts for the IoT

Several SDOs and alliances are working to maintain the seamless operations of the IoT systems. As mentioned in Section 3.1, ISO, IEC and a joint collaboration between them (ISO/IEC JTC 1) [62], ETSI, ITU-T, etc. are well-known SDOs, which provide generic standards related to IoT. The rest of the section provides an overview of the efforts of SDOs and alliances working on the development of IoT standards.

Before going into the details of the SDOs and alliances, Table 18 (non-exhaustive list) provides a summary of their standardization coverage, for global understanding, in the areas of complexities in IoT deployment identified in Section 1.4 [10]. In the context of the IoT, ISO/IEC JTC 1, ETSI and ITU-T cover most of the areas in technical standardization for generic standards. Concerning other alliances related to IoT technical standardization, most of them are focused on specific areas. For example, oneM2M [63] basically addresses interoperability-related standards in the IoT and Machine-to-Machine (M2M). Connectivity, security and privacy, scalability are a secondary focus area of this organization. Similarly, the Institute of Electrical and Electronics Engineers (IEEE) [64] and the Third Generation Partnership Project (3GPP) [65] are primarily focused on connectivity-related standards. Likewise, the Industrial Internet Consortium (IIC) [66] and the Internet Engineering Task Force (IETF) [67] are primarily focused on providing related terminologies and definitions concerning IoT. The IIC has also put its effort to handle interoperability, security and privacy, and trustworthiness-related issues, whereas the IETF is focused on connectivity, intelligence and analytics related-standards, in addition to terminology and interoperability. OASIS is primarily focused on security and privacy, intelligence and analytics as well as interoperability, connectivity, reliability, and scalability-related standards. The Alliance for Internet of Things Innovation (AIOTI) [68] is primarily focused on sector-specific as well as intelligence and analytics standards. It is also involved in scalability and societal aspects. Similarly, Automatic Identification and Mobility (AIM) [69] is primarily focused on interoperability and connectivity-related standards. Providing common terminologies as well as addressing security and privacy issues related to IoT are secondary focus areas of this organization. Likewise, Global Standards One (GS1) [70] is primarily focused on vocabulary, connectivity and sector-specific standards. The primary focus of the Open Connectivity Foundation (OCF) [71] related to IoT standardization are interoperability, security & privacy, and scalability. Similarly, the World Wide Web Consortium (W3C) [72] is actively addressing the technical standardization issues on vocabulary as well as interoperability. The Open Geospatial Consortium (OGC) [73] is addressing sector-specific standards as well as interoperability, connectivity, reliability, scalability related standards.

| SDOs/alliances | Areas of technical standardization | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Common language | Interoperability | Connectivity | Security & privacy | Trustworthiness | Reliability | Scalability | Intelligence | Sector-specific | Societal aspects |
| ISO/IEC | ■■■ | ■■ | ■ | ■■■ | ■■ | ■ | ■ | ■ | ■■ | ■■ |
| ETSI | ■ | ■■■ | ■■■ | ■■ | ■ | ■ | ■ | ■■ | ■■ | ■ |
| ITU-T | ■■ | ■■ | ■■■ | ■■■ | ■ | ■ | ■■ | ■■■ | ■■ | ■ |
| oneM2M | | ■■■ | ■■ | ■■ | ■■■ | ■ | ■■ | ■ | ■ | |
| IEEE | ■■ | ■■ | ■■■ | ■■■ | | ■ | ■ | ■■ | ■ | ■ |
| 3GPP | ■ | ■■ | ■■■ | ■ | | ■ | ■ | ■■ | ■ | |
| IETF | ■■■ | ■■ | ■■ | ■■ | | ■ | ■ | ■■■ | ■ | ■ |
| OASIS | ■ | ■■ | ■■■ | ■■■ | | ■■ | ■■ | ■■■ | ■ | |
| AIOTI | ■ | ■ | ■ | ■ | | ■ | ■■ | ■■■ | ■■■ | ■■ |
| AIM | ■ | ■■ | ■■ | ■ | | | | | | |
| IIC | ■■■ | ■■ | ■ | ■■ | ■■ | ■ | ■ | ■ | ■ | ■ |
| GS1 | ■■ | ■ | ■■ | ■ | | | ■ | | ■■ | |
| OCF | ■ | ■■ | ■ | ■■ | | ■ | ■ | | ■ | |
| W3C | ■■ | ■■ | ■ | ■ | | ■ | ■ | | ■ | |
| OGC | | ■ | ■ | | | ■ | ■ | | ■ | |

*Table 18: Standardization coverage of SDOs/alliances [10]*

Note 1: ■ represents level of involvement in particular areas related to IoT standardization

Note 2: ■ low, ■■ medium, and ■■■ high

Detailed standardization efforts of SDOs and alliances related to IoT are provided in the remaining sections

### 3.4.1 National context of IoT technical standardization

ILNAS, with the support of ANEC GIE, works actively on the development of ICT technical standardization. The *National Standardization Strategy 2020-2030*[13], signed by the Minister of the Economy, aims to foster national performance and excellence in standardization activities. This twofold objective relies on four pillars including the promotion of the use of relevant technical standards and the strengthening of the national market's involvement in the technical standardization process. ICT is one of the targeted growth sectors identified in the Strategy, and the national *Policy on ICT technical standardization 2020-2025*[14] specifies the main projects dedicated to the development of this sector through three lead projects.

ILNAS delegated the management of the National Mirror Committee (NMC) of ISO/IEC JTC 1/SC 41, which will be further detailed in Section 3.4.2, to ANEC GIE, in order to foster the participation of the national market in the process of technical standardization. The registered delegates are involved in the standardization work of ISO/IEC JTC 1/SC 41 by voting and commenting on proposals of the subcommittee, and can participate in its international plenary meetings. ILNAS, with the support of ANEC GIE, also performs a broader monitoring of IoT standardization activities in order to keep up to date in the area and to inform national stakeholders on its progress.

Apart from the management of several NMCs and the creation of education and research[15] programs in the standardization area, the execution of the Policy on ICT technical standardization includes the development of reports informing the national market about current standardization developments in this sector. For instance, the annual publication of the *Smart Secure ICT Standards Analysis* [16] provides an overview of the latest standardization developments of selected Smart ICT technologies (Cloud Computing, Internet of Things, Artificial Intelligence (AI) & Big Data, and Blockchain), as well as related Digital Trust standards. This analysis is a practical tool available to national stakeholders to identify relevant standardization technical committees in the Smart Secure ICT area, with the objective to offer guidance for a potential future involvement in the standards development process to national stakeholders [74]. It is worth noting that ILNAS also published a White Paper *Digital Trust for Smart ICT* (last updated in September 2017)[17] to make national stakeholders aware of the concept of Smart ICT and related standardization with digital trust requirements for different topics of Smart ICT. In summary, it provides, among other Smart ICT technologies, a state of the art of the IoT, its economic challenges and prospects, its essential requirements in terms of Digital Trust, as well as technical standardization-related developments as one of the enablers for Digital Trust for Smart ICT [75]. As part of the University research program (ILNAS-UL) initiated in 2017, a White Paper *Data protection and privacy in Smart ICT* [76] was published in 2018, a joint work between ILNAS--ANEC GIE and the SnT of the University of Luxembourg, with the support of the Ministry of the Economy, to provide a holistic view of privacy and data protection in Smart ICT, notably IoT, Cloud Computing and Big data. This White Paper was further extended in 2019 with the publication of technical reports *Smart ICT: Gap analysis between scientific research and technical standardization* [77] intending to provide such gap analysis in smart ICT topics, specifically in Cloud Computing, AI and IoT.

Finally, as mentioned before, a White Paper IoT [1] was published in 2018 by ILNAS and ANEC GIE with the support of the Ministry of the Economy. The present report is a further extension of the White Paper, intending to include national examples of IoT-related implementations to enlighten the need of technical standardization in this field.

[13] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

[14] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/policy-on-ict-technical-standardization-2020-2025.pdf

[15] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html

[16] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/smart-secure-ans-tic-october-2019.pdf

[17] https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf

## 3.4.2 ISO and IEC

### 3.4.2.1 ISO/IEC JTC 1/SC 41

ISO/IEC JTC 1 is a joint technical committee of ISO and IEC. It was created to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT). A subcommittee under JTC 1, SC 41 [78], serves as the focus and proponent for JTC 1's standardization program on the IoT and related technologies, including Sensor Networks and Wearable technologies. This subcommittee is addressing most of the issues listed in Table 18. In particular, it has three working groups (WGs) for different areas of IoT standardization to address these issues:

- **ISO/IEC JTC 1/SC 41/WG 3** - IoT architecture provides standardization in the area of common language - IoT vocabulary, architecture and frameworks. An international standard ISO/IEC 20924:2018 IoT - Vocabulary[18] developed by this working group provides a definition of IoT for a common understanding about IoT within its stakeholders along with a set of terms and definitions forming a terminology foundation for the IoT. Similarly, another international standard ISO/IEC 30141:2018 - IoT Reference Architecture[19] provides a standardized IoT reference architecture using a common vocabulary, reusable designs and industry best practices. It has used a top down approach, deriving a high level system-based reference with subsequent dissection of that model into five architecture views from different perspectives, beginning with collecting the most important characteristics of IoT. The need of security, privacy and requirement for trustworthiness framework and methodologies while deploying IoT is also addressing by this working group forming different ad-hoc groups and liaison coordination groups;
- **ISO/IEC JTC 1/SC 41/WG 4** - IoT interoperability provides standardization activities in the area of interoperability, connectivity, platform, middle-ware, conformance and testing. This working group published an international standard ISO/IEC 21823-1:2019 - Interoperability for IoT systems - Part 1: Framework[20], which provides an overview of interoperability framework for IoT systems. It helps IoT stakeholders to build IoT systems in such a way that the entities are able to exchange information and mutually use the information in an efficient way. Apart from this, it is also working to define transport and semantic interoperability for IoT systems;
- **ISO/IEC JTC 1/SC 41/WG 5** - IoT applications deals with standardization in the area of IoT applications, uses cases, tools, and implementation guidance. A technical report ISO/IEC TR 22417:2017[21], published by this working group, identifies IoT scenarios and use cases based on real-world applications and requirements. These use cases provide a practical context for considerations on interoperability and standards based on user experience. In addition to this, it clarifies where existing standards can be applied and highlights where standardization work is needed.

Apart from it, this subcommittee also considers societal aspects of the IoT, and the relationships of the IoT with new technologies, such as Blockchain, Artificial Intelligence (AI), Cloud/Edge technology, through various ad-hoc groups and liaison coordination groups. Furthermore, ISO/IEC JTC 1/SC 41 also jointly works with ISO/IEC JTC 1/SC 27[22] - Information security, cybersecurity and privacy protection for the security and privacy-related standards. For example, an international standard ISO/IEC 27030 - Guidelines for security and privacy in IoT is being developed to provide security and privacy guidelines in IoT under ISO/IEC JTC 1/SC 27.

[18] https://webstore.iec.ch/publication/60582

[19] https://webstore.iec.ch/publication/60606

[20] https://webstore.iec.ch/publication/60604

[21] https://webstore.iec.ch/publication/60605

[22] https://www.iso.org/committee/45306.html

#### 3.4.2.2 ISO/TC 204 - Intelligent transport systems

The committee ISO/TC 204 – Intelligent transport systems was created to provide standardization activities in information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveler information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field. This committee is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work program in this field, including the schedule for standards development, taking into account the work of existing international standardization bodies. It is worth noting that this committee excludes in-vehicle transport information and control systems, which is under the responsibility of ISO/TC 22 - Road vehicles.

The committees of ISO and IEC, especially those in ISO/IEC JTC 1, cover most of the areas of standardization related to IoT pointed out in Table 18. However connectivity, reliability, scalability, intelligence and analytics as well as societal aspects are less covered areas by such committees compared to others.

### 3.4.3 ETSI

ETSI is a standardization organization for ICT standards fulfilling European and global market needs. It has long been involved in IoT related technical standardization. It develops several standards (specifications, reports) in the area of interoperability and use cases. In particular, standards related to Machine-to-Machine (M2M), IoT, Smart cities, Smart meters, Intelligent Transport Systems, Low power supplies, Radio spectrum etc. and related security issues are the main focus of this organization. Some technical committees more relevant for the IoT are highlighted below:

- **ETSI/TC Smart M2M** is responsible to provide specifications to IoT smart cities-related applications. In the beginning, ETSI's special task force 505 - IoT Standards landscaping and IoT European Large Scale Pilots (LSP) gap analysis provided two technical reports, ETSI TR 103 375 and ETSI TR 103 376 to provide a roadmap of IoT standards, and a gap analysis in IoT technical standardization. In particular, ETSI TR 103 375 - IoT Standards landscape and future evaluations is to provide the standards landscape for IoT and the identification of potential frameworks for interoperability, and ETSI TR 103 376 - IoT LSP use cases and standards gaps is to identify standardization gaps and proposals on how to address them in standardization. For cyber security guidelines related to IoT, the ETSI technical committee on Cybersecurity - TC Cyber - has released the technical specification, ETSI TS 103 645, for cybersecurity in IoT aiming at establishing a security guideline for internet-connected consumer products and intending to provide a basis for future IoT certification schemes;
- **ETSI/TC Satellite Earth Station and Systems (SES)** is responsible for standardization relating to all types of satellite communication systems, services and applications, but still needs to explore many issues, for example, the applicability of current satellite communication scenarios for the IoT, efficient M2M/IoT protocols suitable for future services, etc.;
- **ETSI/TC Intelligent Transport Systems (ITS)** is responsible for standardization to support the development and implementation of Intelligent Transport Systems (ITS) service provision across the network, for transport networks, vehicles and transport users, including interface aspects, multiple modes of transport and interoperability between systems. This committee is leading the drive to achieve international standards relevant for this sector. In addition to this, it is helping to accelerate the introduction of ITS services and applications and to maximize their benefits by developing common European standards and technical specifications to enable interoperability.

ETSI's main focus as a standards development organization is in the telecommunications industry, for example for equipment makers and network operators. It also supports to create an environment for the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services. It is significantly contributing to develop standards related to connectivity and interoperability for the IoT. Security and privacy, intelligence and analytics, and sector-specific standards are other focus areas of ETSI. As shown in Table 18, defining common language and reference architecture, trustworthiness issues, reliability, scalability, and societal aspects are less covered areas by ETSI compared to others.

### 3.4.4 ITU-T

ITU is the United Nations' specialized agency for ICTs. The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) gather experts from around the world to develop international standards known as ITU-T Recommendations, which act as defining elements in the global infrastructure of ICTs. ITU-T put forward a vision of IoT in the landmark "Internet of Things" report published in 2005 as part of a series of ITU reports on the Internet. It was defined in recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. The ITU-T has its main focus on providing recommendations defining how telecommunication networks operate and interwork. It is significantly contributing to develop standards related to connectivity, security and privacy, and intelligence and analytics for the IoT. Similarly, providing a common understanding about IoT technology, interoperability frameworks, scalability, and sector-specific standards are other focus areas of ITU-T. However, trustworthiness, reliability, and societal aspects in technical standardization issues in IoT are the less covered areas by ITU-T compared to others. A few examples of standards developed by ITU-T across sectors are listed in Section 3.5.

Some relevant study groups of ITU-T related to the IoT are highlighted below:

- **SG 20 - IoT & Smart Cities, and Communities (SC &C)** is working to address the standardization requirements with an initial focus on IoT applications in Smart Cities and communities. This study group is responsible from ITU-T to put forward the vision of IoT defined in Recommendation ITU-T Y.2060 (06/2012). A central part of this study is the standardization of end-to-end architectures for IoT, and mechanisms for the interoperability of IoT applications and data sets employed by various vertical industry sectors. This study group has also addressed the issue of defining application-specific reference architecture, such as in smart manufacturing and Industrial IoT, e-health and e-agriculture, wearable device and services, and cooperative applications and transportation safety services;
- **SG 17 - Security** coordinates security-related work across all ITU-T SGs together with a broad range of standardization issues. In particular for the IoT, it is working for the security of applications and services for the IoT and smart grid.

### 3.4.5 Other SDOs and alliances

In addition to the previous list of SDOs, several other SDOs and alliances are working for maintaining seamless operations of the IoT. There is a huge list of alliances who are actively working on IoT technical standardization, namely oneM2M, Institute of Electrical and Electronics Engineers (IEEE), Third Generation Partnership Project (3GPP), Institute of Electrical and Electronics Engineers (IEEE), Alliance for Internet of Things Innovation (AIOTI), Association for Automatic Identification and Mobility (AIM), Industrial Internet Consortium (IIC), Global Standards One (GS1), Open Connectivity Foundation (OCF), World Wide Web Consortium (W3C), Open Geospatial Consortium (OGC), are some of them, will be briefly overviewed in this section.

- **oneM2M**

  It is a joint alliance of eight SDOs active in ICT standardization including ETSI. This alliance is playing an important role in developing interoperability related standards and specifications within and out of the IoT system. Basically the specifications developed by oneM2M address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers.

- **The Institute of Electrical and Electronics Engineers (IEEE)**

  It has been producing standards for local/personal area connectivity, which play a vital role in forming a physical and Medium Access Control (MAC) layer related standards. For example, the standard IEEE 2413-2019 [79] aims to develop an architectural framework to cover the needs of different applications.

- **The Third Generation Partnership Project (3GPP)**

  Considering market growth of the IoT, the 3GPP is working on, and has already provided, sets of specifications to Long Term Evolution (LTE), NarrowBand IoT (NB-IoT), and 5G-related radio specifications and standards related for the IoT. For example, recent development of LTE-Advanced Pro is set to be used by other sectors, beyond telecoms, including Critical Communications (blue light services & other Mission Critical systems), M2M or IoT sector, Transport (Rail, ITS, etc.), education and many other areas. LTE-Advanced Pro is 3GPP's stepping stone to 5G systems.

- **The Internet Engineering Task Force (IETF)**

  The IETF is another leading organization in standardizing protocols for the Internet at different layers of the network stack. It is also working to optimize the IETF's protocol offerings for the lower level on LPWAN from SigFox, LoRA Alliance, 3GPP etc. as well as to define the upper layer exchanges and signaling of existing protocol offerings. Likewise, Message Queuing Telemetry Transport (MQTT) [24], an ISO standard, submitted by Organization for the Advancements of Structured Information Standard (OASIS) [80] provides a standardized mechanism to connect devices. It helps cloud-based architectures to be developed with common protocol semantics for inter-connectivity.

- **Alliance for Internet of Things Innovation (AIOTI)**

  In 2015, the European Commission initiated the Alliance for Internet of Things Innovation (AIOTI) with the aim to strengthen the dialogue and interaction among IoT stakeholders in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the adoption of IoT. Apart from this, its other objectives include: fostering experimentation, replication, and deployment of IoT and supporting convergence and interoperability of IoT standards; gathering evidence on market obstacles for IoT deployment; and mapping and bridging global, EU, and member states' IoT innovation activities.

  Among the 13 different working groups, WG 3: IoT standardization is dedicated to related IoT standardization activities. It identifies and, where appropriate, makes recommendations to address existing IoT standards, analyzes gaps in standardization, and develops strategies and use cases aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) semantic interoperability, and (3) personal data & personal data protection to the various categories of stakeholders in the IoT space.

- **Industrial Internet Consortium (IIC)**

  The Industrial Internet Consortium was formed aiming to bring together the organizations and technologies necessary to accelerate the growth of the industrial internet by identifying, assembling, testing and promoting best practices. Among its multiple activities and programs, it helps IoT end users, vendors, system integrators and researchers to achieve tangible results as they seek to digitally transform across the enterprise. Manufacturing, energy, heath, transportation, smart cities, etc. are some of the key areas of focus of IIC. It is intended to bring together end user organizations, product vendors, service providers and research organizations to create new Industrial IoT (IIoT) solutions, generate operational efficiencies and develop business model innovations covering most of these sectors.

- **Global Standards One (GS1)**

  Global Standards One (GS1) is an industrial consortium aiming to develop specifications to identify, capture and share data of value chain. GS1 standards are intended to create a common foundation for business by uniquely identifying, accurately capturing and automatically sharing vital information about products, locations, assets and more. These standards could be also helpful to streamline business processes, for example traceability.

- **OASIS - Organization for the Advancement of Structured Information Standards**

  OASIS develops standards for a broad range of technical areas, including cybersecurity, blockchain, privacy, cryptography, Cloud Computing, IoT, etc. Several technical committees are working on IoT and M2M-related topics, such as the Advanced Message Queuing Protocol (AMQP), which defines an ubiquitous, secure, reliable and open internet protocol for handling business messaging, or the Message Queuing Telemetry Transport (MQTT) protocol, which provides a lightweight messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is a priority.

- **Open Connectivity Foundation (OCF)**

  In the context of the need for secure and reliable device discovery and connectivity to enable IoT, OCF is intended to ensuring secure interoperability for consumers, businesses and industries by delivering a standard communications platform, a bridging specification, an open source implementation and a certification program allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem. In particular, it is contributing to the IoT society in two ways: providing specifications, code and a certification program to enable manufacturers to bring OCF Certified products to the market that can interoperate with current IoT devices and legacy systems, and making the end user's experience better by seamlessly bridging to other ecosystems within a user's smart home and ensuring interoperability with OCF-compliant devices.

- **World Wide Web Consortium (W3C)**

  The World Wide Web Consortium (W3C) aims to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. It gathers diverse stakeholders together under a clear and effective consensus-based process to develop high-quality standards based on contributions. W3C has defined two designed principles: Web for all - the social value of the Web is that it enables human communication, commerce, and opportunities to share knowledge; and Web on everything - the number of different kinds of devices that can access the Web has grown immensely. Mobile phones, smart phones, personal digital assistants, interactive television systems, voice response systems, kiosks and even certain domestic appliances access the Web. In particular for IoT, the W3C Web of Things (WoT) has been created to enable interoperability across IoT platforms and application domains. The WoT complements existing IoT ecosystems to reduce the cost and risk for suppliers and consumers of applications that create value by combining multiple devices and information services. There are many sectors that will benefit, e.g. smart homes, smart cities, smart industry, smart agriculture, smart healthcare and many more.

  The WoT Working Group has recently advanced two specifications to Candidate Recommendation status (Web of Things -- Architecture, and Web of Things -- Thing Descriptions). These specifications further aim to advance to become W3C Recommendations.

- **Association for Automatic Identification and Mobility (AIM)**

  AIM is an industry association for the automatic identification industry worldwide. It is intended to provide unbiased information, educational resources and standards to providers and users of these technologies. It mainly helps organizations to grow their businesses by fostering the effective use of Automatic Identification and Data Capture (AIDC) solutions. Standards can be also divided into technology and application. Technology standards deal with the nuts-and-bolts of how things work. For instance, in radio frequency identification (RFID), technical specifications cover issues such as frequency, data transfer and communications protocols.

They do not cover how the technology is used, only how it works. On the other hand, application standards define how a technology is used. They cover data content, structure and syntax. They typically point to a technical specification and may define a subset of it to limit how a specific technology will be used to carry or represent the data. Additional guidance, such as placement, durability and so forth is also generally included. In particular for IoT, AIM helps a diverse group of industry professionals, academics, consultants, distributors, independent software vendors, manufacturers, nonprofits, re-sellers, startups, system integrators, and end users of AIDC technologies.

- **Open Geospatial Consortium (OGC)**

  The Open Geospatial Consortium (OGC) is an international consortium of several businesses, government agencies, research organizations, and universities driven to make geospatial (location) information and services, like FAIR (Findable, Accessible, Interoperable, and Reusable). For example, the OGC SensorThings API provides an open, geospatial-enabled and unified way to interconnect the Internet of Things (IoT) devices, data, and applications over the Web. Similarly, the Sensor Observation Service (SOS) standards are applicable to use cases in which sensor data needs to be managed in an interoperable way. This standard defines a Web service interface which allows querying observations, sensor metadata, as well as representations of observed features. On the other hand, Sensor Planning Service Interface Standards (SPS) define interfaces for queries that provide information about the capabilities of a sensor and how to task the sensor.

## 3.5 Coverage of technical standardization of SDOs and alliances related to IoT

As shown in Table 18, only a few organizations cover most of the issues related to IoT standardization identified in Section 1.4: ISO/IEC JTC 1, ETSI, and ITU-T. ISO/IEC JTC 1 covers primarily common language, security and privacy, interoperability, sector-specific (for example, consumer IoT, Industrial IoT) issues, trustworthiness and societal aspects in IoT technical standardization. Similarly, ETSI primarily covers connectivity, interoperability, security and privacy, intelligence, sector-specific (for example, consumer IoT, smart cities) related standards related to IoT. On the other hand, another well-known SDO, ITU-T, primarily covers the connectivity, security and privacy, intelligence, common language, interoperability, scalability, and sector-specific (for example, smart cites) standards related to IoT. As mentioned before, concerning other alliances related to the IoT technical standardization, most of them are focused in specific areas, see section 3.4.

### 3.5.1 Some published and ongoing standards/specifications relevant for IoT implementation

This section provides non-exhaustive lists of published and ongoing standards/specifications initiated by SDOs and alliances related to the vertical sectors and issues/complexities related to IoT introduced in Chapter 1 and 2.

#### 3.5.1.1 Vocabulary and reference architecture related standards

As mentioned in Section 3.2.6, a common understanding on the terminologies and deployment architecture are pre-requisites of every technology. As seen in Table 19, ISO/IEC, ITU-T, W3C, AIOTI, IIC are working to define vocabularies and reference architectures (in some cases, sector-based reference architectures) for the IoT. IEEE focuses standardisation activities on the lower protocol layers namely the Physical and the MAC layer while IETF activities are positioned above that layer in the Networking and transport layers with some elements in the layers above [56]. The most recognizable enhancement by ISA100.11a [81] is probably the support of IPv6, which came with the 6LoWPAN header compression, as defined by the IETF. ISO/IEC JTC 1 addresses most of the challenges identified in Table 18. For example, this committee has well addressed the need of a common understanding about the technology and a common implementation architecture acceptable for related stakeholders from different aspects across the sectors providing its definition, a set of terms and definitions forming a terminology foundation for the IoT as well as a common IoT reference architecture. ITU-T, on the other hand, provided its first definition of Internet of Things in Y.2060 (06/2012). It recently published terms and definitions (Technical Specification D0.1 - data processing and management for the IoT and smart cities and communities: vocabulary) related to Data Processing and Management (DPM), which is an example of standards/specifications important for deploying IoT and Smart Cities and Communities (SC&C). IIC on the other hand provides vocabulary related to IoT technology, particularly in the IIoT domain. In each updated version, IIC adds new definitions for new technologies and related terms. The reference architecture, also called Industrial Internet Reference Architecture (IIRA), provides guidelines on how different components fit together and how they influence each other. It tries to reflect consensus on major architecture questions among participants from the energy, healthcare, manufacturing, transportation and public sectors.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| JTC 1/SC 41 | ISO/IEC 20924:2018 Internet of Things -- Vocabulary | Published |
| JTC 1/SC 41 | ISO/IEC 30141:2018 Internet of Things – Reference Architecture | Published |
| ITU-T | Y.2060 (06/2012) Overview of the Internet of things | Published |
| ITU-T | Y.2069 (07/2012) Terms and definitions for the Internet of things | Published |
| ITU-T | Y.4203 (02/2019) Requirements of things description in the IoT | Published |
| ITU-T | Technical Specification D0.1 - Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary | Published |
| W3C | Web of Things (WoT) -- Architecture | Published |
| W3C | Web of Things (WoT) -- Thing Description | Published |
| AIOTI | IoT LSP Standard Framework Concepts Release 2.8 (2017) | Published |
| AIOTI | High Level Architecture (HLA) Release 2.1 (2016), Release 4.0 (2018) | Published |
| AIOTI | IoT Relation and Impact on 5G Release 1.0 (2018), Release 2.0 (2019) | Published |
| IIC | Industrial Internet Vocabulary Technical Report Version 1.0, 2.0, 2.1 | Published |
| IIC | Industrial Internet Reference Architecture v 1.7, v 1.8. v 1.9 | Published |
| IEEE | 2413-2019 IEEE Standard for an Architectural Framework for the Internet of Things (IoT) | Published |

*Table 19: Vocabulary and reference architecture related standards*

### 3.5.1.2 Interoperability-related standards

In the context of the exponential growth of connected devices to the IoT, interoperability issues are becoming challenging. JTC 1/SC 41 puts its efforts into defining an interoperability framework. In fact, this subcommittee recommended an interoperability framework in its first standard (ISO/IEC 21823-1:2019) for IoT, which defines four facets of interoperability, namely transport, semantic, syntactic and behavioral. This subcommittee is underway to cover all facets of IoT interoperability in its standards. ETSI collaborates with oneM2M for interoperability-related standards. oneM2M provides a set of specifications that helps enable users build platforms, regardless of existing sector or industry solutions. Since recently, ETSI and oneM2M are jointly working on semantic interoperability as in the IoT world, semantic interoperability is especially important because machines are much less capable of processing ambiguous information than humans. Semantic interoperability ensures the meaning of the data to be interpreted correctly. For example, the series of ETSI TS 103 410 Smart Applications Reference ontology are examples of specifications efforts of ETSI together with other SDOs as well as alliances, including oneM2M for semantic interoperability. Similarly, recently published specifications of ITU-T (D3.2 - SensorThings API – Sensing, and D3.3 - Framework to support data interoperability in IoT environments) provide an open, geospatial-enabled and unified way to interconnect the Internet of Things devices, data, and applications over the Web. These are some examples of joint initiatives of ITU-T and OGC for IoT interoperability and closely related to each other specifications developed by OGC, such as series of SensorThings API, etc.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| JTC 1/SC 41 | ISO/IEC 21823-1:2019 Internet of Things – Interoperability for IoT systems - Part 1: Framework | Published |
| JTC 1/SC 41 | ISO/IEC 21823-2:2020 Internet of Things (IoT) - Interoperability for IoT Systems - Part 2: Transport interoperability | Published |
| JTC 1/SC 41 | ISO/IEC 21823-3 Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability | Ongoing |
| JTC 1/SC 41 | ISO/IEC 21823-4 Internet of Things (IoT) - Interoperability for IoT Systems - Part 4: Syntatic interoperability | Ongoing |
| ETSI | ETSI TS 103 410 Smart Appliances REFerence ontology<br>Part 1: Energy Domain;<br>Part 2: Environment Domain;<br>Part 3: Building Domain;<br>Part 4: Smart Cities Domain;<br>Part 5: Industry and Manufacturing Domains;<br>Part 6: Smart Agriculture and Food Chain Domain. | Published |
| ITU-T | Y.4459 (01/2020) Digital entity architecture framework for Internet of things interoperability | Published |
| ITU-T | Technical Specification D3.2 - SensorThings API - Sensing | Published |
| ITU-T | Technical Specification D3.3 - Framework to support data interoperability in IoT environments | Published |
| AIOTI | Semantic Interoperability for the Web of Things | Published |
| OGC | SensorThings API<br>Part 1: Sensing v1.0<br>Part 2: Tasking Core v1.0 | Published |
| OGC | Sensor Observation Service Interface Standard v1.0, v2.0 | Published |
| OGC | OpenGIS Sensor Observation Service v1.0, v2.0 | Published |
| OGC | Sensor Planning Service Implementation Standard | Published |

*Table 20: Interoperability related standards*

### 3.5.1.3 Sectoral/ use case-related standards

However many initiatives are ongoing to develop sector-(or domain-) based standards for IoT, it seems a lot of initiatives are needed for this case. For example, ISO/IEC JTC 1/SC 41 identified some IoT-related use cases in ISO/IEC TR 22417:2017 Internet of Things – Use cases. This subcommittee has now created an advisory group related to IoT use cases and some co-ordination groups on industrial IoT and consumer IoT to identify needs of standards relevant for such sectors. ETSI, in ETSI TR 103 376 V1.1.1 (2016-10) SmartM2M; IoT LSP use cases and standards gaps identified gaps (requirements analysis) in cross-domain sectors of IoT. Similarly, ITU-T recently published the Recommendation Y.4556 (12/2019) Requirements and functional architecture of smart residential community, which provides an IoT-based approach for residents to acquire safe, comfortable and convenient living conditions in a residential community. Similarly, in a recent version of the IoT LSP Standard Framework Concepts (Release 2.9), AIOTI has covered nine different sectors of IoT applications.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| JTC 1/SC 41 | ISO/IEC TR 22417:2017 Internet of Things – Use cases | Published |
| ETSI | ETSI TR 103 376 V1.1.1 (2016-10) SmartM2M; IoT LSP use cases and standards gaps | Published |
| ITU-T | Y.4556 (12/2019) Requirements and functional architecture of smart residential community | Published |
| AIOTI | IoT LSP Standard Framework Concepts, Release 2.8, Release 2.9 | Published |

*Table 21: Sectoral/ use cases related standards*

### 3.5.1.4 Security, privacy and trustworthiness-related standards

Security and privacy as well as trustworthiness issues in IoT are well covered topics under ISO/IEC JTC 1 (see Table 22). ISO/IEC JTC 1/SC 27 is working on a standard, ISO/IEC 27030 -- Information technology -- Security techniques — Guidelines for security and privacy in Internet of Things (IoT), which intends to provide guidance on the principles, risks and controls for IoT information security and privacy. ISO/IEC JTC 1/SC 41 is working on two standards ISO/IEC 30149 -- Internet of Things (IoT) -- Trustworthiness framework, and ISO/IEC 30147 -- Internet of Things (IoT) -- Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 systems engineering processes, focusing more on trustworthiness aspects. In addition to this, ISO/IEC JTC 1 recently created a working group on Trustworthiness (JTC 1/WG 13) to define trustworthiness concepts applicable to every field of ICT. It intends to cover a variety of deployment sectors while developing standards. Similarly, ITU-T is also active to develop generic security and privacy-related specifications for IoT. Technical specifications, D4.1 - Framework for security, privacy, risk and governance in data processing and management, D4.3 - Overview of technical enablers for trusted data, and D4.3 - Overview of technical enablers for trusted data are some examples of specifications developed by ITU-T related to general security and privacy for IoT. Likewise, ETSI is also contributing to developing security and privacy-related specifications for IoT. ETSI TS 103 645 V1.1.1 (2019-02) -- Cyber Security for Consumer Internet of Things is a recent publication of ETSI, related to consumer IoT, which specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. It is worth noting that a European standard, notably based on this Technical Specification should be published soon (ETSI EN 303 645). Similarly, IEEE and OASIS are also equally contributing to define technical specifications at protocol level.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| JTC 1/SC 27 | ISO/IEC 27030 Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT) | Ongoing |
| JTC 1/SC 41 | ISO/IEC 30149 Internet of Things (IoT) - Trustworthiness framework | Ongoing |
| JTC 1/SC 41 | ISO/IEC 30147 Internet of Things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 systems engineering processes | Ongoing |
| ITU-T | Technical Specification D4.1 - Framework for security, privacy, risk and governance in data processing and management | Published |
| ITU-T | Technical Report D4.3 - Overview of technical enablers for trusted data | Published |
| ITU-T | Technical Specification D4.4 - Framework to support data quality management in IoT | Published |
| ITU-T | X.sc-iot Security controls for Internet of Things (IoT) systems | Ongoing |
| ITU-T | Y.4806 (11/2017) Security capabilities supporting safety of the Internet of Things | Published |
| ITU-T | X.iotsec-4 Security requirements for IoT devices and gateway | Ongoing |
| ITU-T | X.ssp-iot Security requirements and framework for IoT service platform | Ongoing |
| ITU-T | Y.Data.Sec.IoT-Dev Requirements of data security for the heterogeneous IoT devices | Ongoing |
| ETSI | ETSI TS 103 645 V1.1.1 (2019-02) Cyber Security for Consumer Internet of Things | Published |
| ETSI | ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements | Ongoing |
| ETSI | ETSI TS 103 458 V1.1.1 (2018-06) Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements | Published |
| ETSI | ETSI TR 103 591 V1.1.1 (2019-10) SmartM2M; Privacy study report; Standards Landscape and best practices | Published |
| ETSI | ETSI TR 103 534 Teaching material:<br>Part 1: Security<br>Part 2: Privacy | Published |

*Table 22: General security guidelines standards related for IoT*

### 3.5.1.5 Satellite communications-related standards

Many issues need to be considered for satellite-IoT interconnectivity related standards; some of the efforts done by ETSI in the satellite sector are listed in Table 23.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| ETSI | ETSI EN 303 980 V1.1.1 (2017-12) Satellite Earth Stations and Systems (SES); Harmonized Standard for fixed and in-motion Earth Stations communicating with non-geostationary satellite systems (NEST) in the 11 GHz to 14 GHz frequency bands covering essential requirements of article 3.2 of Directive 2014/53/EU | Published |
| ETSI | ETSI EN 301 926 V1.3.1 (2017-10) Satellite Earth Stations and Systems (SES); Radio Frequency and Modulation Standard for Telemetry, Command and Ranging (TCR) of Communications Satellites | Published |
| ETSI | ETSI TR 103 297 V1.1.1 (2017-07) Satellite Earth Stations and Systems (SES); SC-FDMA based radio waveform technology for Ku/ Ka band satellite service | Published |
| ETSI | ETSI TR 103 351 V1.1.1 (2017-07) Satellite Earth Stations and Systems (SES); Multi-link routing scheme in hybrid access network with heterogeneous links | Published |
| ETSI | ETSI TS 103 246 V1.2.1 (2017-03) Satellite Earth Stations and Systems (SES); GNSS based location systems:<br>● Part 1: Functional requirements<br>● Part 2: Reference Architecture<br>● Part 3: Performance requirements<br>● Part 4: Requirements for location data exchange protocols<br>● Part 5: Performance Test Specification | Published |

*Table 23: Satellite communications related standards*

### 3.5.1.6 Intelligent transportation systems [ITS]-related standards

Many issues need to be considered for ITS -IoT interconnectivity related standards, some of the efforts done by ISO/TC 204 and ETSI in vertical sector of ITS are listed in Table 24.

| SDOs/alliances | Name of project | Status |
|---|---|---|
| ISO/TC 204 | ISO 14816:2005 Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure | Published |
| ISO/TC 204 | ISO/TR 14823-2:2019 Intelligent transport systems — Graphic data dictionary — Part 2: Examples | Published |
| ISO/TC 204 | ISO 17264:2009 Intelligent transport systems — Automatic vehicle and equipment identification — Interfaces | Published |
| ISO/TC 204 | ISO 17438-4:2019 Intelligent transport systems — Indoor navigation for personal and vehicle ITS station — Part 4: Requirements and specifications for interface between personal/vehicle and central ITS stations | Published |

| | | |
|---|---|---|
| ISO/TC 204 | ISO 17515-3:2019 Intelligent transport systems — Evolved-universal terrestrial radio access network — Part 3: LTE-V2X | Published |
| ISO/TC 204 | ISO/TS 19091:2019 Intelligent transport systems — Cooperative ITS — Using V2I and I2V communications for applications related to signalized intersections | Published |
| ISO/TC 204 | ISO/TS 21177:2019 Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices | Published |
| ISO/TC 204 | ISO/TR 24097-3:2019 Intelligent transport systems — Using web services (machine-machine delivery) for ITS service delivery — Part 3: Quality of service | Published |
| ISO/TC 204 | ISO/TR 12859:2009 Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems | Published |
| ISO/TC 204 | ISO 17429:2017 Intelligent transport systems — Cooperative ITS — ITS station facilities for the transfer of information between ITS stations | Published |
| ISO/TC 204 | ISO/TR 24098:2007 Intelligent transport systems — System architecture, taxonomy and terminology — Procedures for developing ITS deployment plans utilizing ITS system architecture | Published |
| ETSI | ETSI TS 103 613 V1.1.1 (2018-11) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems using LTE Vehicle to everything communication in the 5,9 GHz frequency band | Published |
| ETSI | ETSI TS 102 941 V1.3.1 (2019-02) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management | Published |
| ETSI | ETSI TS 103 152 V2.1.1 (2019-11) Intelligent Transport Systems (ITS); V2X Communications; Multimedia Content Dissemination (MCD) Basic Service specification; Release 2 | Published |
| ETSI | ETSI TS 103 666-1 V15.1.0 (2020-01) Smart Secure Platform (SSP); Part 1: General characteristics (Release 15) | Published |
| ETSI | ETSI TS 102 965 V1.5.1 (2020-01) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration | Published |
| ETSI | ETSI EN 303 613 V1.1.1 (2020-01) Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band | Published |
| ETSI | ETSI EN 302 663 V1.3.1 (2020-01) Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band | Published |

*Table 24: Intelligent transportation systems (ITS) related standards*

# 4

# Conclusions and outlook

# 4. Conclusions and outlook

This national technical standardization report is developed to make national stakeholders aware of IoT technical standardization, extending the White Paper - Internet of Things (IoT) published in July 2018 [1] by ILNAS with the support of the Ministry of the Economy. This White Paper mainly surveyed IoT technology from three different viewpoints: IoT basic concepts and its driving technologies, economic and business prospects, and technical standards watch. As seen in recent years, the IoT is considered a disruptive innovation to improve business processes within and across sectors. It describes a world where anything can be connected and can interact in an intelligent fashion. Therefore, it is popular to realize the scenarios, where internet connectivity and computing capability extends to a variety of connecting things. The IoT is no more a new technology but its ways of implementation are still in the center of curiosity for its stakeholders. This report provides a study of national initiatives in IoT related implementations from different perspectives, particularly operational efficiency and importance of technical standardization. Moreover, this report, with an analysis of current IoT-related issues across various sectors, highlights how technical standardization is expected to help national stakeholders in their IoT technology implementation plan.

In this frame, IoT implementations are central in this national technical standardization report to show how technical standardization helps to minimize different deployment complexities. In particular, this report addresses these issues from three different perspectives: IoT concepts, IoT implementations and IoT technical standardization.

The IoT concept chapter is intended to extend the concepts of IoT technology that were included in the previous ILNAS White Paper on Internet of Things [1]. It basically provides an insight into the true potential of IoT data from generation to analysis with recent trends of key IoT driving technologies. In addition, it shows how IoT data carries inherent security, storage and processing risks, and presents other new challenges in diverse areas of applications. For this, a list of complexities is identified from the perspectives of IoT deployment. Finally, a concept of IoT cybersecurity objectives, risks and threats as potential challenges for the IoT ecosystem, among others, is provided, showing the criticality of these issues for IoT current deployment.

The IoT implementations chapter, which is a central focus of this report, provides a study of IoT applications across different sectors of society. Globally, IoT application domains can be divided into two categories: horizontal and vertical domains. The horizontal domain is essentially the telecommunications sector, while Smart building, smart home, smart manufacturing, connected vehicles, smart health, smart energy, smart cities, smart agriculture, are examples of vertical domains. To represent both horizontal and vertical domains in this report, some national IoT related initiatives/examples in satellite and related connectivity for IoT and connected vehicles are considered as examples of IoT applications in those domains.

The growing number of devices or services in IoT has resulted in complexities for them to connect and communicate. That complexity is associated to interfaces, quality of service, communication, security and privacy, and much more. In this context, technical standardization is expected to play a key role in qualitative development, coherent source of knowledge, and continuous improvement of these technologies with common language of communication among its stakeholders. The IoT technical standardization chapter shows how standards development organizations and different alliances are addressing the IoT deployment complexities identified in this report. At first, the chapter highlights the concept of standards and standardization along with a brief introduction of standardization bodies and alliances at international and European level. The national context is also highlighted, providing information about the National Mirror Committee ISO/IEC JTC 1/SC 41 on IoT and related technologies, ILNAS activities and related support provided by ILNAS with the support of the ANEC GIE. In addition to this, the technical standardization landscape related to IoT technology is also presented, giving highlights of the efforts of several standardization bodies and alliances towards IoT technical standardization.

Finally, it provides examples of published and ongoing standards that are developed by different standardization bodies and alliances, mainly from the perspectives of complexities and use cases mentioned in previous chapters.

In Luxembourg, ILNAS, with the support of ANEC GIE, is actively following the standardization developments of Internet of Things and related technologies, building on the National Standardization Strategy[23] and the related Policy on ICT Technical Standardization (2020-2025) [24]. The main objectives of this policy is to foster and strengthen the national ICT sector's involvement in standardization work. To achieve this, ILNAS conducted three intertwined projects: a) promoting the ICT technical standardization to the market, b) reinforcing the valorization and the involvement regarding ICT technical standardization, and c) supporting and strengthening education about standardization and related research activities. These three projects are intended to allow the national market to make rapid progress and reap the benefits of technical standardization effectively.

- In line with the first project, ILNAS is drawing up a yearly national standards analysis of the Smart Secure ICT sector. This publication aims at offering national stakeholders a "snapshot" of the Smart Secure ICT standardization landscape in order to inform them about the relevant technical standardization activities in Smart ICT areas (Internet of Things, Cloud Computing, Artificial Intelligence and Blockchain and Distributed Ledger Technologies) as well as related Digital Trust standards developments. Through this overview of international standardization activities, national stakeholders can easily identify technical committees developing standards relevant for their business and decide whether they would have an interest in participating in the development of these standards. In relation with this objective, a national implementation plan for ICT technical standardization is developed by the ANEC GIE, under the supervision of ILNAS, with the aim to involve targeted stakeholders of the Grand Duchy of Luxembourg in a global approach to standardization in order to support the sector in terms of competitiveness, visibility and performance, while enhancing the international recognition of the Grand Duchy of Luxembourg at the standards level.
- Similarly, conforming to the second project, ILNAS, with the support of ANEC GIE, is following closely and directly number of technical committees. ILNAS is already participating member of ISO/IEC JTC 1/SC 41, with 18 experts [25] actively involved in the standardization work to define future international standards. In addition, ILNAS is closely following the technical standardization developments provided by ETSI as well as ITU-T, and actively transferring relevant information to the market through the organization of workshops. In this frame, interested stakeholders in Luxembourg can get involved in the standards development process by becoming delegates (e.g. of ISO/IEC JTC 1/SC 41)[26].
- Finally, in relation with the third project, ILNAS and ANEC GIE – in collaboration with the Ministry of the Economy – published a white paper in 2018 [1] with the goal of providing a comprehensive analysis of IoT from technological, economic, as well as technical standardization perspectives. Among other outcomes, such publications, including this national technical standardization report, aim to create awareness and interest concerning relevant standardization developments within the national market.
- ILNAS also has strong relationship with the University of Luxembourg and SnT in order to facilitate standards-related education and research. As part of this partnership, two editions of the university certificate program "Smart ICT for Business Innovation" have been already completed. Based on this experience, ILNAS and University of Luxembourg will open the first promotion of the Master degree "Technopreneurship: mastering smart ICT, standardization and digital trust for enabling next generation of ICT solutions"[27] in September 2020, where digital trust and technical standardization will be at the heart of the program and be taught transversal to various Smart ICT topics, including IoT.

[23] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

[24] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/policy-on-ict-technical-standardization-2020-2025.pdf

[25] https://portail-qualite.public.lu/dam-assets/fr/publications/normes-normalisation/information-sensibilisation/ilnas-oln-registre-national-delegues-normalisation/ilnas-oln-registre-national-delegues-normalisation.pdf

[26] https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html

[27] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/master-mtech.html

# References

[1] ILNAS, "IoT White Paper," https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-iot.html, 2018.

[2] "AIOTI WG3 (IoT Standardisation) – Release 2.8," 2017. [Online]. Available: https://aioti-space.org/wp-content/uploads/2017/06/AIOTI-WG3_sdos_alliances_landscape_-_iot_lsp_standard_framework_concepts_-_release_2_v8.pdf.

[3] "IoT trend watch 2018," IHS Markit, [Online]. Available: https://cdn.ihs.com/www/pdf/IoT-Trend-Watch-eBook.pdf. [Accessed 05 2019].

[4] NIST, "Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)," https://csrc.nist.gov/publications/detail/nistir/8200/final, 2018.

[5] "ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes," [Online]. Available: https://www.iso.org/standard/63711.html.

[6] P. Mannion, "Optimal Analysis Algorithms are IoT's Big Opportunity," Industrial & Medical Technology , 2015.

[7] "A White Paper on Data management, privacy, and security in connected systems," www.interact-lighting.com, 2018.

[8] J. Rowley, "The wisdom hierarchy:representations of theDIKW hierarchy," Journal of Information Science , vol. 33, no. 2, pp. 163 - 180 , 2007.

[9] A. Pal et al., "IoT Standardization: The Road Ahead," in DOI: 10.5772/intechopen.75137, 2018.

[10] S. Wagle et al., "Efforts Towards IoT Technical Standardization," in 18th International Conference on Ad-Hoc Networks and Wireless, ADHOC-NOW, 2019.

[11] "IIC definition: The Industrial Internet of Things, Volume G8: Vocabulary Industrial Internet Consortium," 2017. [Online]. Available: http://www.iiconsortium.org/pdf/IICVocabTechnicalReport2.0.pdf.

[12] D. Mendez et al., "Internet of Things: Survey on Security and Privacy," Cornell University Library, 2017.

[13] "Committee on National Security Systems Glossary Working Group, Committee On National Security Systems (CNSS) Glossary, April 2010, 160 pp.," https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf, 2010.

[14] "NIST Special Publication 800-30 Revision 1, Joint Task Force Transformation Initiative Interagency Working Group, Guide for Conducting Risk Assessments," National Institute of Standards and Technology, 2012. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-30r1.

[15] K. Stouffer et al., "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Revision 2,, 2015.

[16] "EMEA Satellite operations assiciations(ESOA)," [Online]. Available: https://www.esoa.net/cms-data/positions/1695%20ESOA%20IOT%20%20Sat%20Brochure%20Proof%204.pdf. [Accessed April 2019].

[17] "Satmagazine," [Online]. Available: http://www.satmagazine.com/story.php?number=1897443442. [Accessed 04 2019].

[18] IoT UK, "Satellite Technologies for IoT Applications," 2017.

[19] [Online]. Available: https://www.thuraya.com/content/can-internet-things-iot-survive-without-satellite. [Accessed 04 2019].

[20] H. Urlings, "Satellite IoT: Game changer industry?," [Online]. Available: http://satellitemarkets.com/satellite-iot-game-changer-industry. [Accessed 07 2019].

[21] "Cyber Concerns For The Satellite Sector," Attila Security, [Online]. Available: https://attilasec.com/blog/satellite-cybersecurity/. [Accessed 07 2019].

[22] D. Livingstone and P. Lewis, "Space, the Final Frontier for Cybersecurity?," in International Security Department, 2016.

[23] "M2M Sat Project," [Online]. Available: https://artes.esa.int/projects/m2msat.

[24] "MQTT," [Online]. Available: MQTT: http://mqtt.org/.

[25] "RFC7252: The Constrained Application Protocol (CoAP)," [Online]. Available: https://tools.ietf.org/html/rfc7252.

[26] R. Soua et al., "IoT Application Protocols Optimisation for Future Integrated M2M-Satellite Networks," in *The Global Information Infrastructure and Networking Symposium* (GIIS 2018), 2018.

[27] M. R. Palattella et al., "Aggregation of MQTT Topics: performance study over Integrated Satellite-Terrestrial Networks," in *Performance Evaluation of Satellite Networks (PESN) Workshop in conjunction with IFIP WG Performance Conference*, 2018.

[28] “OpenSAND satellite emulator,” [Online]. Available: http://opensand.org/content/home.php.

[29] “Mosquitto,” [Online]. Available: https://mosquitto.org/.

[30] “CoAPthon,” [Online]. Available: https://github.com/Tanganelli/CoAPthon.

[31] “SATIOT project,” [Online]. Available: https://www.fnr.lu/projects/communication-algorithms-for-end-to-end-satellite-iot-2.

[32] “SATis5 ESA ARTES Project,” [Online]. Available: https://artes.esa.int/projects/satis5-0.

[33] M. Corici et al., “SATis5: A 5G Testbed Integrating Satellite and Terrestrial Infrastructures,” in *Proc. 9th Advanced Satellite Multimedia Systems Conference & 15th Signal Processing for Space Communications Workshop (ASMS/SPSC 2018)*, 2018.

[34] M. Corici et al., “SATis5 Solution: A Comprehensive Practical Validation of the Satellite Use Cases in 5G,” in *Proc. 24th Ka and Broadband Communications Conference and 36th International Communications Satellite Systems Conference (ICSSC),*, 2018.

[35] F. Völk et al., “Satellite Integration into 5G: Accent on First Over-The-Air Tests of an Edge Node Concept with Integrated Satellite Backhaul,” in *MDPI Future Internet Journal – Special Issue, 2019, 11, 193; doi:10.3390/fi11090193*, 2019.

[36] K. Liolis et al., “Over-the-Air Demonstration of Satellite Integration with 5G Core Network and Multi-Access Edge Computing Use Case,” in *Proc. IEEE 5G World Forum*, 2019.

[37] “5G-VINNI Project,” [Online]. Available: https://5g-vinni.eu/ .

[38] C. Politis et al., “Design of Moving Experimentation Facility to Showcase Satellite Integration into 5G,” in *Proc. 28th European Conference on Networks and Communications (EuCNC 2019)*, 2019.

[39] “CONNECTED VEHICLES, Towards a Data -Based Mobility & Transport Paradigm,” https://european-iot-pilots.eu/wp-content/uploads/2018/06/Market-Paper-Connected-Vehicles.pdf.

[40] “Worldwide Internet of Things Spending,” [Online]. Available: IDC, Worldwide Internet of Things Spending Guide, 2019. [Accessed 07 2019].

[41] “CONNECTED V AUTONOMOUS VEHICLES. WHAT’S THE DIFFERENCE,” myvehicle.ie, [Online]. Available: https://www.myvehicle.ie/car-news/connected-v-autonomous-vehicles--what---s-the-difference. [Accessed 09 2019].

[42] S.K. Dutta et al., “Integrating Connected Vehicles in Internet of Things Ecosystems: Challenges and Solutions,” in *Available at: http://www.eurecom.fr/en/publication/4883/download/comsys-publi-4883.pdf.*

[43] C. King and D. Klinedinst, “On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle,,” Software Engineering Institute, Carnegie Mellon University, 2016. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pd.

[44] “e-bus Competence Ccenter in luxembourg,” [Online]. Available: http://www.corporatenews.lu/en/archives-shortcut/archives/article/2016/10/volvo-buses-launches-e-bus-competence-center-in-luxembourg. [Accessed 01 2020].

[45] M. Seredynski and P. Bouvry, *“survey of vehicular-based cooperative traffic information systems,”* in *14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 2011.

[46] “Rolling Plan for ICT Standardization,” 2020. [Online]. Available: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020.

[47] V. Gazis, “A Survey of Standards for Machine-to-Machine and the Internet of Things,” in *IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 482-511*, 2017.

[48] “European Commission, COM(2016) 176 final - Commission Staff working document - Advancing the Internet of Things in Europe,” 2016. [Online].

[49] “CEN-CENELEC, Standards and your business,,” 2013. [Online]. Available: https://www.cencenelec.eu/news/publications/Publications/Standards-and-your-business2013-09.pdf.

[50] “Regulation (EU) No 1025/2012 - General framework of European standardisation policy,” [Online]. Available: https://ec.europa.eu/growth/single-market/european-standards/policy/framework_en.

[51] G. Marques et al., “A Survey on IoT: Architectures, Elements, Applications, QoS, Platforms and Security Concepts,” in *Advances in Mobile Cloud Computing and Big Data in the 5G Era, pp 115-130*, 2016.

[52] “The International Organization for Standardization (ISO),” [Online]. Available: https://www.iso.org/home.html.

[53] “The International Electrotechnical Commission (IEC),” [Online]. Available: https://www.iec.ch/.

[54] "The International Telecommunication Unions Telecommunication Standardization Sector," [Online]. Available: https://www.itu.int/en/Pages/default.aspx.

[55] "The European Telecommunications Standards Institute (ETSI)," [Online]. Available: https://www.etsi.org.

[56] P. Guillemin et al., "Internet of Things standardisation - Status, Requirements, Initiatives and Organisations," [Online]. Available: https://www.academia.edu/29074933/InternetofThingsStandardisation-StatusRequirementsInitiativesandOrganisations. [Accessed December 2019].

[57] J. Saleem et al., "IoT Standardisation - Challenges, Perspectives and Solution," in *The International Conference on Future Networks and Distributed Systems (ICFNDS)*, 2018.

[58] "e-Tech News and Views from the IEC, Why the IoT needs standardization," [Online]. Available: https://iecetech.org/Technical-Committees/2017-01/Why-the-IoT-needs-standardization. [Accessed December 2019].

[59] A. Banafa, "IoT Standardization and Implementation Challenges," 2016. [Online].

[60] S. Pacheco and J. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," in *IEEE International Workshops on Foundations and Applications of Self Systems*, 2016.

[61] AIOTI WG 03, [Online]. Available: https://aioti.eu/aioti-wg03-reports-on-iot-standards/. [Accessed 01 2020].

[62] "ISO, IEC joint technical committee (JTC 1)," [Online]. Available: https://www.iso.org/isoiec-jtc-1.html.

[63] "oneM2M, Standards for M2M and the Internet of Things," [Online]. Available: http://www.onem2m.org/.

[64] "The Institute of Electrical and Electronics Engineers (IEEE)," [Online]. Available: https://www.ieee.org/.

[65] "The third Generation Partnership Project (3GPP)," [Online]. Available: https://www.3gpp.org/.

[66] "Industrial Internet Consortium (IIC)," [Online]. Available: https://www.iiconsortium.org/.

[67] "The Internet Engineering Task Force (IETF)," [Online]. Available: https://www.ietf.org/.

[68] "Alliance for Internet of Things Innovation (AIOTI)," [Online]. Available: https://aioti.eu/.

[69] "Automatic Identification and Mobility (AIM)," [Online]. Available: https://www.aimglobal.org/.

[70] "Global Standards One (GS1)," [Online]. Available: https://www.gs1.org/.

[71] "Open Connectivity Foundation," [Online]. Available: https://openconnectivity.org/.

[72] "World Wide Web Consortium (W3C)," [Online]. Available: http://www.w3.org/.

[73] "Open Geospatial Consortium (OGC)," [Online]. Available: http://www.opengeospatial.org/.

[74] ILNAS, "Standards Analysis Smart ICT - Luxembourg," 2019. [Online]. Available: https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/smart-secure-ans-tic-october-2019.pdf.

[75] ILNAS, "White Paper Digital Trust for Smart ICT," September 2017. [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf.

[76] "White Paper on Data Protection and Privacy in Smart ICT," ILNAS-UL, 2018.

[77] "Smart ICT: Gap analysis between scientific research and technical standardization," ILNAS - UL, 2019.

[78] "ISO/IEC JTC 1/SC 41 - Internet of Things and Related Technologies," [Online]. Available: https://www.iec.ch.

[79] "IEEE, Standard for an Architectural Framework for the Internet of Things (IoT)," [Online]. Available: https://standards.ieee.org/standard/2413-2019.html.

[80] "Organization for the Advancements of Structured Information Standard (OASIS)," [Online]. Available: https://www.oasis-open.org/.

[81] ISA100.11a, [Online]. Available: https://isa100wci.org/. [Accessed 01 2020].

[82] M. Seredynski and F. Viti, "A Survey of Cooperative ITS for Next Generation Public Transport Systems," in *19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016.

[83] "Intelligent transportation system (ITS)," [Online]. Available: https://logistics.public.lu/en/why-luxembourg/logistics-infrastructure/intelligent-transportation-system.html.

[84] "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, National Institute of Standards and," NIST Interagency Report (NISTIR) 8074 Volume 2,, 2015.

[85] "Zigbee Alliance," [Online]. Available: https://www.zigbee.org/.

[86] “Lora Alliance,” [Online]. Available: https://lora-alliance.org/.

[87] E. Ahmed et al., “The role of big data analytics in Internet of Things,” in *Special Issue on 5G Wireless Networks for IoT and Body Sensors*, Computer Networks, Volume 129, Part 2, 2017, pp. 459-471.

[88] Whitepaper, Interact, “Data management, privacy, and security in connected systems,” www.interact-lighting.com, 2018.

COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRIAL
432432
675453
875654
23466
COLLABORATION
PARTNER
OFFICE

June 2020 · National Technical Standardization Report · Internet of Things (IoT) · Version 1.0 · © ILNAS/ANEC GIE

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation
et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : info@ilnas.etat.lu

**www.portail-qualite.lu**