From Internet of Things to System of Systems

Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS

An Artemis-IA Whitepaper

ARTEMIS
Industry Association

From Internet of Things to System of Systems

Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS

An ARTEMIS-IA Whitepaper

April 2020

Paolo Azzoni
Research Program Manager
EUROTECH Group
Chairman of ARTEMIS Working Group "From IoT to SoS"

Table of Contents

Table of Figures

Executive Summary

Digital transformation is shaping our world in unprecedented ways, at a rate of change never seen before, potentially improving our daily life and our society, disrupting the traditional businesses and representing a must to secure companies' competitive edge. Digitalisation creates a link between the physical and the digital worlds and the dynamic interaction between these two worlds constitutes one of the strongest driving forces that will shape the evolution of future markets, potentially in every vertical domain.

The Internet of Things (IoT) has come today a long way from the prototype of the Coke machine at Carnegie Mellon University in 1980s, and it will play a crucial role in the digital transformation: IoT is essentially everything that sits between a sensor and the destination for the data it generates. From the initial machine-to-machine features and capabilities adopted in the manufacturing and utilities domains, IoT has rapidly evolved, "colonising" almost every vertical domain, with any kind of natural or man-made objects. These "Things", that become connected, are provided with significant computing power, advanced sensing capabilities and a continuously increasing level of intelligence and autonomy. The resulting information networks generate a shift from the classical linear value chains towards non-linear value networks, where every relationship between stakeholders could potentially generate new business and revenue streams, new business combinations, improve the existing business processes and create new additional value propositions. This shift represents a historical change in the structure of the current economic system, opening the way to the creation of an integrated and self-regulating system of systems (SoS), beyond brands, industries and vertical domain boundaries.

Today, beyond the hype, IoT has become a reality, with increasing technological maturity, global hyper connectivity, new flexible business models, more awareness about trust and sustainability, and specific European Research Programmes. Potentially, for every company involved in ICT, irrespective of its size, now is the time to understand the positioning in the evolving IoT value chain, analyse the adequacy and sustainability of the business model, define the product offer and play a pivotal role in European digitalisation process.

Embracing upcoming IoT trends, influencing and shaping them represent a crucial part of European digital strategy for the future and it is the key to driving continuous innovation and staying ahead of the competition in the years to come. Recently, European Commission President Ursula von der Leyen identified[1] specific strategic priorities for a "Europe fit for the Digital Age" to "ensure that Europe fully grasps the potential of the digital age and strengthens its industry and innovation capacity" to achieve technological leadership and sovereignty. From this perspective, boosting the adoption of IoT in Europe represents a keystone for the European Digital Age, because

- IoT is a technology game changer in the digitalisation process;
- it promotes the transformation of existing business models and the creation of new innovative ones based on the convergence of IoT, Big Data, AI and Cloud computing;
- many barriers preventing the uptake of IoT in Europe require immediate solutions, particularly regarding the lack of trust, market fragmentation, the proliferation of standards hindering interoperability and the general uncertainty around IoT investments.

[1] *https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-margrethe-vestager_2019_en.pdf*

The ARTEMIS and ECSEL community have always devoted significant interest in IoT and SoS that is such a central topic for scientific and industrial research: IoT covers a large part of the Electronic Components and Systems (ECS) value chain.

This white paper provides a global overview of the IoT market, identifying the key factors that are currently enabling the uptake of IoT, providing a panorama of the market dimensions and of the opportunities offered by IoT in significant vertical domains, identifying the IoT trends and providing insights on the structure of the IoT value chain, the respective stakeholders, the positioning of the value across the value chain and its evolution.

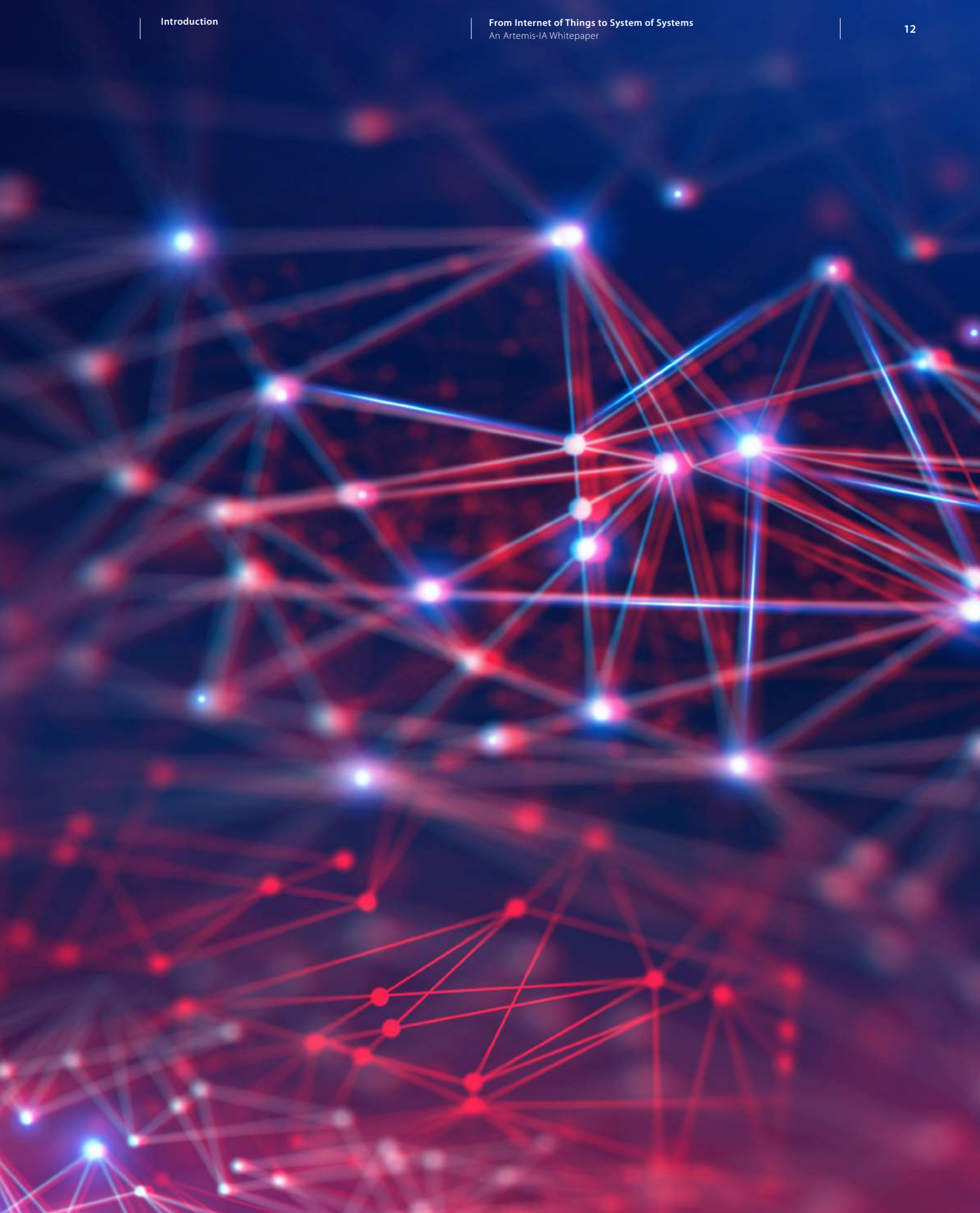
The white paper reports the results of the extensive analysis and assessment backtrack of ARTEMIS and ECSEL projects related to IoT and SoS and developed by the community during the last decade: the study has been elaborated in the last two years with the intention of identifying the projects' achievements, illustrating the interdisciplinary technologies involved in IoT and SoS, identifying the barriers that are hindering the uptake of IoT and the challenges confronting future ECS SRAs, providing insights on economic, business and societal aspects.

The study highlights the huge effort spent by the community in IoT and SoS innovation and allows the ARTEMIS and ECSEL initiatives to be positioned in the European and international panorama. The identification of IoT and SoS research streams allows an evaluation of the alignment of the research activities and of the projects' objectives/results with the Strategic Research Agendas and with the market trends: this alignment demonstrates that we are heading in the right direction, with the right long-term vision of IoT towards SoS. At the end, the investments analysis draws a "map" of investments and provides an estimation of the financial effort in IoT and SoS research, spent to develop technological solutions that overcome obstacles and address challenges.

This study is intended also to stimulate further reflections for the ECSEL community and for the wider digital community, that are currently focused on planning the future of ECSEL, and it provides useful insights for the European Member States, for European companies and decision makers, hoping to promote a coordinated and constructive strategy for the European Digital Era.

With my best regards,

Paolo Azzoni



Introduction

Billions of devices and systems are getting connected, offering new services and applications that improve consumers' lifestyle and companies' efficiency, minimising the operational costs, increasing the utilization of assets and improving the quality of the final products. The Internet of Things (IoT) is the interdisciplinary solution adopted to integrate these heterogeneous and distributed objects in a single system of systems (SoS), efficiently managing the collection and processing of vast amount of data, generating added-value services and applications to achieve common goals.

The original concept of IoT was to connect "Things" to the Internet and eventually to each other. Today, IoT represents a wider conceptual approach adopted to efficiently solve classical problems at a massive scale with a new recipe based on smart objects, connectivity, interoperability, embedded intelligence, actionable data streams, delocalised computation and agile business models.

The word IoT was coined in 1999 by Kevin Ashton, executive director of the Auto-ID Center at MIT[2], but it is widely recognised that the first steps in IoT were taken in the early 1980s with David Nichols, a graduate student in Carnegie Mellon University's computer science department, which modified a Coke vending machine, located very distant from his office, to enable its remote control through a network. That Coke machine is considered the first IoT device.

From those early stages, the IoT evolution has gone through two main phases, the *monolithic and the cloud-based phases*. During the monolithic phase (until 2010) IoT solutions rarely left the stage of advanced prototypes, with the development and deployment of *monolithic and closed systems*, characterised by limited scalability, limited support for communication protocols, low level of intelligence and automation, and built on software middleware capable of managing just a few hundreds of devices.

The cloud-based phase (2011-2016) is characterised by *integration and convergence between IoT, hyper-connectivity and cloud computing*, capable of generating IoT solutions which enabled the delivery of IoT services and applications on a massive scale with a Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) business model. During this phase, we assisted in the progressive creation, growth and consolidation of the IoT market, of the IoT value chain and ecosystem, and of vertical markets in which IoT generates value. We assisted as well in several waves of Big Data, of increasing dimensions, that allowed IoT investments to be monetised and new horizons to be opened to data-driven intelligent applications and new business opportunities. In this period, IoT solutions had a centralised architecture, offering large-scale computing and storage platforms. Data collected from sensors are sent directly or via gateways to centralised platforms, typically in the cloud, that aggregate, process, store, analyse and visualise data, create insights, extract knowledge, improve the operational efficiency of processes and generate new added-value services and applications.

[2] *http://www.rfidjournal.com/article/view/4986*

FIGURE 1 — *The first IoT device.*

The third phase in the IoT evolution (2016…to date) is based on *artificial intelligence* that is becoming embedded and pervasive and, coupled with ubiquitous connectivity and real-time communication, is enabling the exponential growth of IoT that we were expecting. This phase is characterised by edge connected devices that are shifting the paradigm from central clouds to decentralised, ubiquitous intelligence. Indeed, centralised architectures are characterised by high latency of data, delays in acting on actionable information, slow decision processes, low resilience to environmental disasters and to security hacks. They are generally more difficult and expensive to scale up and are designed to work with commodity hardware which may lack versatility for IoT operations. Distributed or decentralised architectures based on edge computing and *embedded intelligence* are intended to avoid these shortcomings. Embedded intelligence allows machines and products to communicate and cooperate autonomously together without any human intervention, leaving the real value of data to emerge spontaneously and giving the possibility to manage it more effectively through better and faster decision-making, predictive analytics and automation. The Kurzweil curve[3] predicts an exponential growth of intelligence and estimates that advanced computing platforms will be capable of simulating a human-like intelligence by the end of the next decade. The embedded intelligence represents a key factor in transforming data collected from the IoT infrastructure into insightful knowledge, which is the real value obtained adopting IoT and the factor that generates new business opportunities and commercial benefits.

> *From collecting data to collecting knowledge: organisations will use AI to transform collected data into insightful knowledge and will derive a real commercial benefit.*

A series of long-term technological trends will shape the future evolution of IoT: hyper- connectivity, low-cost hardware and embedded intelligence are the main key factors that are bringing the IoT at the massive scale we were envisioning. There is no better time to examine a business to understand which opportunities IoT could generate: we should think of IoT as an intelligence tool capable of improving the business efficiency but, more importantly, of unlocking new opportunities that, with a suitable business model, could generate high-value revenue streams. Following this evolution, the IoT value chain will be able to deliver interdisciplinary-based new services and applications on top of the IoT enabled data layer with the potential to generate vast opportunities for entire ecosystems.

---

[3] *https://www.kurzweilai.net/the-law-of-accelerating-returns*

To capture these opportunities, ARTEMIS-IA community focused the attention on IoT and SoS since the very beginning of the ARTEMIS initiative: IoT and SoS represent two fundamental components of embedded intelligence and are fully covered by the six ARTEMIS-IA focus areas (Figure 2). Today, the entire ECSEL community is reserving a significant scope to IoT and SoS, as this study demonstrates.

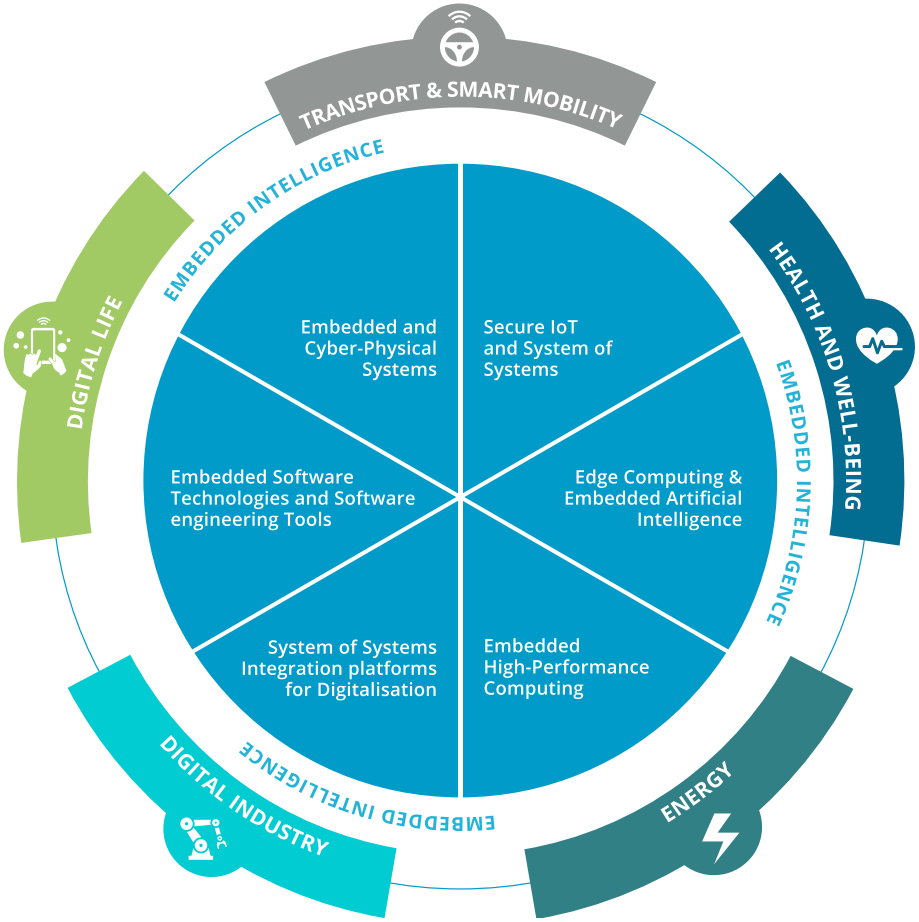


FIGURE 2 — *ARTEMIS-IA focus areas.*

IoT market enablers

IoT has been struggling to flourish for a long time: it attracted a massive interest and as much investments, but *the market was negatively influenced by the value chain unreadiness, fragmentation, inadequate technologies, lack of interoperability and trust in IoT*. Some of these key factors still represent significant barriers for the IoT uptake, but the market analyses demonstrate that the market is consolidating and many of the stakeholders of the value chain are already making significant revenues. The consolidation is due to some *market enablers* that unleash the real potential of IoT and allow its practical viability (Figure 3), leading the market uptake.

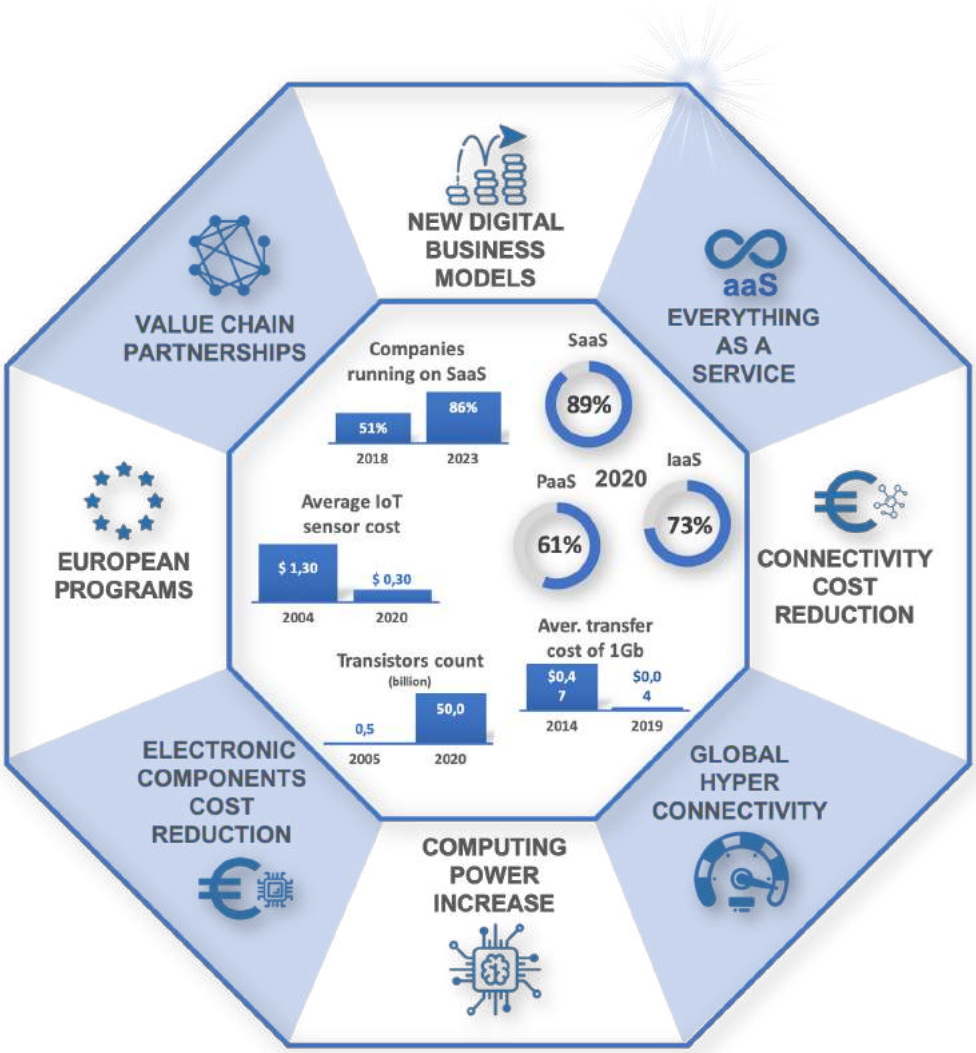


FIGURE 3 — *The diamond of IoT enablers (SaaS - Software as a Service, PaaS - Platform as a Service, IaaS - Infrastructure as a Service).*

1. **Decrease of sensors and electronic components costs.**
The average cost of IoT sensors and electronic components has been steadily decreasing since 2004, with a reduction of more than the 40% in the last 15 years, according to Goldman Sachs and BI Intelligence estimates. The reduction of the price of the fundamental building blocks of IoT represents a crucial first step to make IoT affordable and increase the possibility of a massive adoption. The cost reduction is due to three main factors: 1) the demand for IoT-oriented electronic components is massively increasing, 2) more semiconductor companies are focusing their business on IoT, 3) sensor technology is continuously evolving towards optimal solutions that can be easily and seamlessly integrated with the existing IT infrastructures.

2. **Increase in computing power.**
For a long time, computing power represented a limitation for IoT and in general for distributed systems, confining the large part of the processing in data centres or in the cloud, increasing the amount of data transferred and the related costs. The availability of computing power in almost all the nodes of the IoT infrastructure enables the processing of information on site and exactly when it is required. In particular, it satisfies the necessity of computing power on the edge, where a large part of the data processing will shift. Edge computing is unleashing unprecedented business opportunities. Moreover, the "ubiquitous" availability of computing power allows the adoption of artificial intelligence in embedded and resource-limited devices, increasing the autonomy of the nodes of the IoT infrastructure, their decisional capabilities and the knowledge/value extracted from data.

3. **Global hyper-connectivity.**
Connectivity is a fundamental factor for the existence of IoT, but it is not sufficient for its massive diffusion. Global hyper-connectivity ensures the possibility to support and manage the avalanche of information collected from globally deployed sensors, and let it flows in real-time to the processing nodes of the IoT infrastructure, up to the cloud or data centres. The communication system will have to efficiently manage hundreds billion of connected devices, generating tens or hundreds of zettabytes of data per month. Although edge computing could significantly contribute to reducing the amount of transferred data, the scalability of connectivity remains a critical aspect for the uptake of IoT. Support of a rich set of protocols, geographically driven switching capabilities, strong service delivery and pricing customisation are key factors that hyper-connectivity will have to provide.

4. **Connectivity costs reduction.**
The inner nature of IoT is data transfer, and for a long time connectivity represented one of the most impacting costs of an IoT solution. Firmware updates, log uploads and, in general, massive data collection were not always limited or even impossible due to technical reasons, but rather very frequently due to the unsustainable and unreasonable costs of connectivity. Reducing the price of connectivity means demolishing a historical barrier to IoT uptake. The richness of wireless and wired connectivity solutions available today, the convenient scaling capacity of their performance depending on the application, new flexible business models and pricing solutions are reshaping the connectivity market and significantly reducing the cost of connectivity.

5. **"Everything" as a service.**
IoT is pushing the stakeholders of the value chain to stop considering their products as fixed artefacts with fixed-in-time features and functions. They are starting to think and act like service providers, constantly delivering new value to their customers in order to satisfy their evolving needs. The power and flexibility of software are the fundamental elements at the heart of this change: software allows hardware technologies and artefacts to be transformed into solutions and services, converting this new value proposition into revenues.

6. **Value chain partnerships.**

The real value of IoT lies in data and assets with their digital footprint, which can be shared in real time between the different stakeholders of the value chain. This exchange of information brings IoT to life, but it also generates indirectly an overall improvement of the value chain, end-to-end. While it is possible, but unrealistic, that a single stakeholder implements its own IoT solution, if we consider the intrinsic interdisciplinarity of IoT, a winning IoT solution can be developed only when the stakeholders cooperate together sharing data and expertise. Frequently, many systems, like navigation, manufacturing, warehousing, condition monitoring, etc. operate in their silos, as well as the companies that developed and operate them: in such conditions, the scope of the business and the associated benefits are very limited. Sharing data and insights throughout the IoT value chain in real time enable the creation of partnerships and alliances between the stakeholders that join their forces to create an ecosystem, with a wider business horizon and a more stable, reliable, scalable, open, secure, evolvable and globally more affordable IoT solution. The data shared in this ecosystem, in turn, allows new business opportunities to be revealed, new business models and new revenue streams introduced and, eventually, value to be brought to the end user.

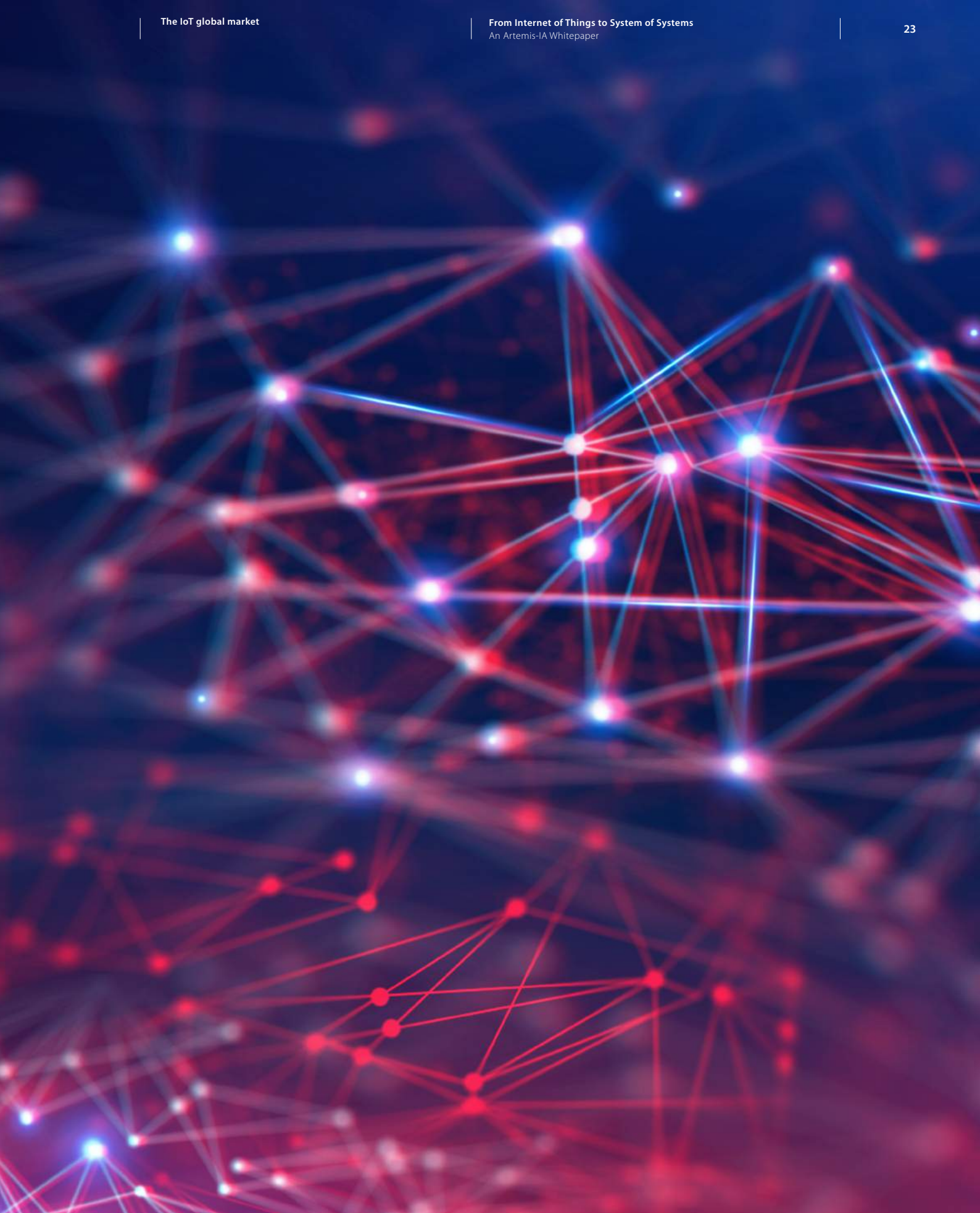
7. **New digital business models.**

IoT generates value in many ways, but emerging business models are really unleashing the real potential of IoT. A business model in the IoT domain must firstly identify where it can capture and deliver value and subsequently define how to leverage the unique characteristic of IoT solutions that connects, monitors and controls 24/7/365 the customer's environment to produce innovative and differentiated value. The "subscription model", for example, adopts a software as a service (SaaS) approach to monetise the product, with a monthly subscription, but also with periodic paid upgrades or a "freemium" model, if possible. The "asset sharing model" tries to maximise the usage of the IoT product across multiple customers, reducing the single partner price and ensuring faster market penetration, if compared to the traditional approach where a single customer pays entirely for the IoT product. The "data monetisation" model proposes to provide value to the customers with the IoT solution and to collect from the customers valuable data that can be sold to third parties. The "service offering" model distinguishes from the "as a service" model because it uses an IoT solution to offer a new service, intended more in the traditional way (e.g. an IoT solution to monitor machinery for preventive maintenance, allows the selling of a maintenance contract). The "pay per usage" model consists of charging the customers for the exact amount of time they have used the IoT product/solution: monitoring the customers' environment allows indirectly also to know how much the IoT product/solution is used. With the "razor blade" model the IoT product/solution is an excuse to sell other products: the IoT product/solution can be sold at cost or even at a loss but, in turn, the customers will buy other products that generate more revenues (e.g. this is the typical example of a device manufacturer that converts to an IoT solution provider, without leaving its core business). And, eventually, the "outcome model" is based on the idea that the customer pays for the outcome or benefit that the IoT product/solution delivers: e.g. when the customer wants to buy a car, probably he/she is not interested in the car but only in moving from point A to point B, and IoT generates a benefit not in the car but in the travel.

8. **European programs.**

The European Commission has been involved in several strategic investments specifically focused on IoT and included in the larger policy of European Digitalisation. These investments are conceived to accelerate European digitalisation, fill the digital gaps existing between European countries and industries and maximise the impact of digital technologies in Europe. The investments allow the consolidation of the existing IoT market and simplify the market entry for start-ups and SMEs, creating an open ecosystem with equal opportunities that avoid the creation of commercial monopolies. From

the technology perspective, the objective is to develop IoT solutions based on common architectures, interoperability and standards, privacy and security by design, and exploit the IoT interdisciplinary expertise of the stakeholders in the value chain. Initiatives such as ARTEMIS, ECSEL, AIOTI and the IoT-EPI have been possible thanks to the investments of the European Commission that generated solid communities focused on the IoT and on the ECS value chain, and that are contributing to European sovereignty in the IoT market.



The IoT global market

IoT and SoS play a fundamental role for digitalisation, they can be considered as the backbone of digitalisation, both from the technical perspective, providing scalable technologies capable of managing billions of connected devices, and from the business perspective, generating potentially more than USD3 trillion worth of revenues in the next 3-5 years. IoT and SoS could play an important role for EU economies in accelerating their slow GDP growth and avoiding stagnation in productivity. *Economic growth can be represented by the sum of the demographic growth and of the aggregate efficiency*[4]. The demographic growth is a factor that is expected to remain very low in Europe, so the only possibility is to improve the aggregate efficiency, on which the impact of IoT is decisive: IoT has been conceived to improve productivity, fault resilience, fault tolerance, to reduce operational costs, optimise the supply chain, etc. Furthermore, IoT is one of the four pillars of a new General-Purpose Technology (GPT)[4] platform able to support European economic growth and really open the path of the 4th industrial revolution. The GPT is composed of:

1. A digitalised and communication-oriented Internet
2. A shared, connected, automated and CO_2-neutral transportation network
3. An energy-oriented sustainable Internet
4. **A smart and automated world based on IoT**

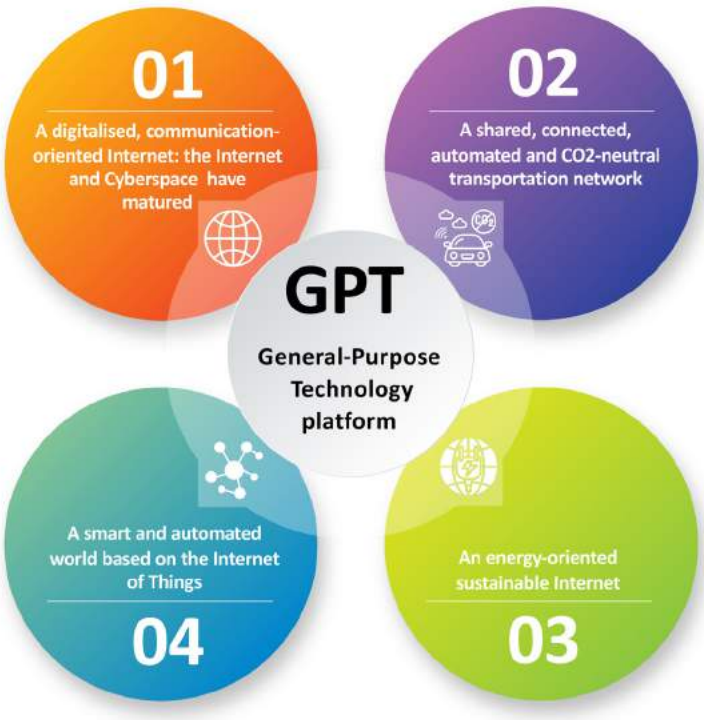


FIGURE 4 — *General-Purpose Technology (GPT) platform.*

[4] *Embedded Intelligence: Trends and Challenges - A Study by Advancy, Commissioned by ARTEMIS Industry Association, March 2019.*

IoT can be considered as the "load-bearing" pillar of the GPT, because of the deep dependencies with the other three pillars: Internet is the primary enabling technology of IoT (1.), while IoT is a primary enabler of the transportation network (2.) and of the Internet of energy (3.), specifically for decentralised energy production units. As the backbone of the digitalisation process, *IoT becomes also an aggregator and, frequently, an enabler of vertical value chains*, simplifying the creation of new partnerships between the stakeholders and consolidating the existing ones: *the economic growth becomes more solid and steady because it is based not only on a disruptive and endless resource, the data, but also on a cohesive ecosystems of companies, RTOs, governmental institutions, etc.* Thanks to IoT, the GPT becomes the virtual counterpart of the physical economy, introducing a radical change in the production process towards decentralised operation (thanks to edge computing and embedded intelligence), collaborative and open solutions (thanks to a solid ecosystems) and laterally scaled value chains, able to demolish the barrier between vertical silos.

The *global IoT market* is complex and dynamic and is evolving very quickly with unprecedented dimensions and opportunities. The IoT market is a subset of the wider Electronic Components and Systems (ECS) market on which ECSEL focuses. According to the Advancy report[4] and to a McKinsey analysis, the ECS market is expected to grow from two to ten times, respectively for the low part of the ECS value chain (electronic components and devices) and for the higher parts (systems, services and applications). The significant growth of the higher parts demonstrates that the vision the ARTEMIS community since the beginning was oriented in the right direction and justifies the large investments of the community on IoT and SoS.

> *The global internet of things (IoT) market was valued at USD 190.0 billion in 2018 and is projected to reach USD 1,102.6 billion by 2025, exhibiting a CAGR of 24.7% in the forecast period* [5] .

IDC (International Data Corporation) and Fortune Business Insights[5] estimate that the IoT global market revenue will reach approximately USD1.1 trillion by 2025. The number of connections related to IoT operations is estimated to increase from 7 billion to 25 billion approximately from 2017 to 2025, with a CAGR[6] of the 17%. The increase of IoT connections (both cellular and non-cellular) will be due in large part to the growth of industrial IoT, responsible for more than 50% of the connections, and to a significant increase of consumer connected devices (e.g. smart home). From a regional perspective, the Asia-Pacific region is expected to lead the global growth of IoT market in terms of size, followed by North America and Europe: the estimated IoT connections for the Asia-Pacific region is about 10.9 billion by 2025. In terms of trend speed, Europe and Middle East (EMEA) represent the fastest growing regions in the period 2017-2025, with a CAGR of 15.7%. *The number of connected devices is an important parameter to measure the dimensions of the IoT market, in all its components.*

Considering the role of IoT in the digital transformation and the complexity of IoT, it is extremely difficult to estimate the impact of IoT on the global economy. Starting from the data available until 2015 and considering the number of connections, Frontiers Economy[7] estimates that a rise in only the 10% of connections could lead to a growth of the United States' GDP of USD2.3 trillion in the next 30 years. More recently, GSMA Intelligence[8] reached a more cautious estimation about the economic impact of IoT on business productivity, evaluating the operating cost savings, the IoT business adoption rate and the sector value added. The study estimates an average growth of USD370 billion by 2025, equivalent to the 0.34% of the global GDP. North America and Asia/Pacific are expected to lead the growth, with a respective 0.46% and 0.34% of the regional GDP, while for Europe the impact is expected to reach 0.27% of

---

5 *Internet of Things (IoT) Market Size, Share and Industry Analysis, Fortune Business Insights, July 2019.*
6 *Compound Annual Growth Rate.*
7 *The Economic Impact of IoT, putting numbers on a revolutionary technology, Frontiers Economy, March 2018.*
8 *The contribution of IoT to economic growth. Modelling the impact on business productivity. GSMA Intelligence, April 2019.*

the regional GDP by 2025. A recent study[9] tends to increase these figures, estimating a potential annual average contribution to the GDP of USD849 billion by 2030, which is growth of 0.99%.

Regarding the *intellectual property landscape*, many studies[10] [11] [12] clearly highlight that the top patent holders belong to diverse sectors like consumer electronics (Samsung, LG, Sony), telecom (Huawei, Ericsson, Korea Electronics Telecom, ZTE) and software (IBM, Microsoft). The patent-filing trend is characterised by steady growth until 2015-2017, with a consistent reduction in the following years that is coherent with the IoT hype cycle. China, the USA, Korea, Europe and Japan account around the 75% of the patents filed. With more than 10,000 patents, Samsung is the major patent holder, covering many technological areas of IoT and many IoT vertical applications. The second position is occupied by Qualcomm, with around 9000 patents: Qualcomm is the major patent filer in multiple jurisdictions and the major PCT filer. A group of large companies, including Qualcomm, LG, Huawei, and Intel, follows with a number of patents between 2200 and 1700 patents while a larger group, including Sony, Ericsson, Nokia, Siemens, NEC, Panasonic, Philips, CISCO, Microsoft, IBM, Fujitsu, is positioned in the range of 1700-600 patents. The largest vertical application domain addressed by patents is consumer electronics, followed by industrials and telecom, and automotive right behind. From the technology perspective, networking is the most addressed topic (with more than 80,000 patents), followed by sensing (around 50,000), security (40,000), energy management (30,000), data analytics (25,000), data storage and IoT CPU (around 7000) and cloud computing (5000).

From the IoT value chain perspective, the estimations of market growth, spending and potential revenues are more difficult to predict and remain more vague. Below is a synthesis of the estimations currently available in several studies published by the most accredited analysists[13]. Figure 5 illustrate a summary of these estimations.

The *share of the revenues in the IoT value chain* depends on the players, their role, on where they create the value and how they interact: the share is largely localised in the upper part, with platform providers and systems integrators totalling 35% each, while all the stakeholders involved in the process and production of electronic components and devices reach the 25% and only a limited part, 5%, is associated to telecom operators and connectivity providers. As estimated by many analysts, the share of the value chain confirms the shift of value from the area of the electronic components and devices (embedded chipsets, IoT modules, transponders, smart thermostats, smart meters, smart parking sensors, IoT gateways, etc.) towards the integration platforms (software for aggregating, processing, securing, storing, analysing, visualising, controlling and understanding data and integrating, monitoring, managing and remotely controlling the IoT end-to-end infrastructure), services, applications and solutions (software, domain-specific applications and services that leverage IoT data). The stakeholders are starting to capitalise on the growing convergence towards the upper part of the IoT value chain and on the increasing number of partnerships and alliances, extending their portfolio beyond their core offerings. The traditional boundaries in the IoT value chain are also more blurred, with all the stakeholders trying to expand their core expertise into new areas and to offer services across the value chain.

---

9 *The Internet of Things and economic growth in a panel of countries, Harald Edquist, Peter Goodridge & Jonathan Haskel, December 2019.*
10 *Internet of Things Technology Landscape and IP Commercialization Trends, Relecura Inc., May 2017.*
11 *IoT Patent Landscape Reference Report, Moeller Ventures LLC, September 2019.*
12 *Leading Internet of Things (IoT) patent owners worldwide as of 2019, Statista, 2020.*
13 *Gartner, McKinsey, IDC, Statista, IoT Analytics.*

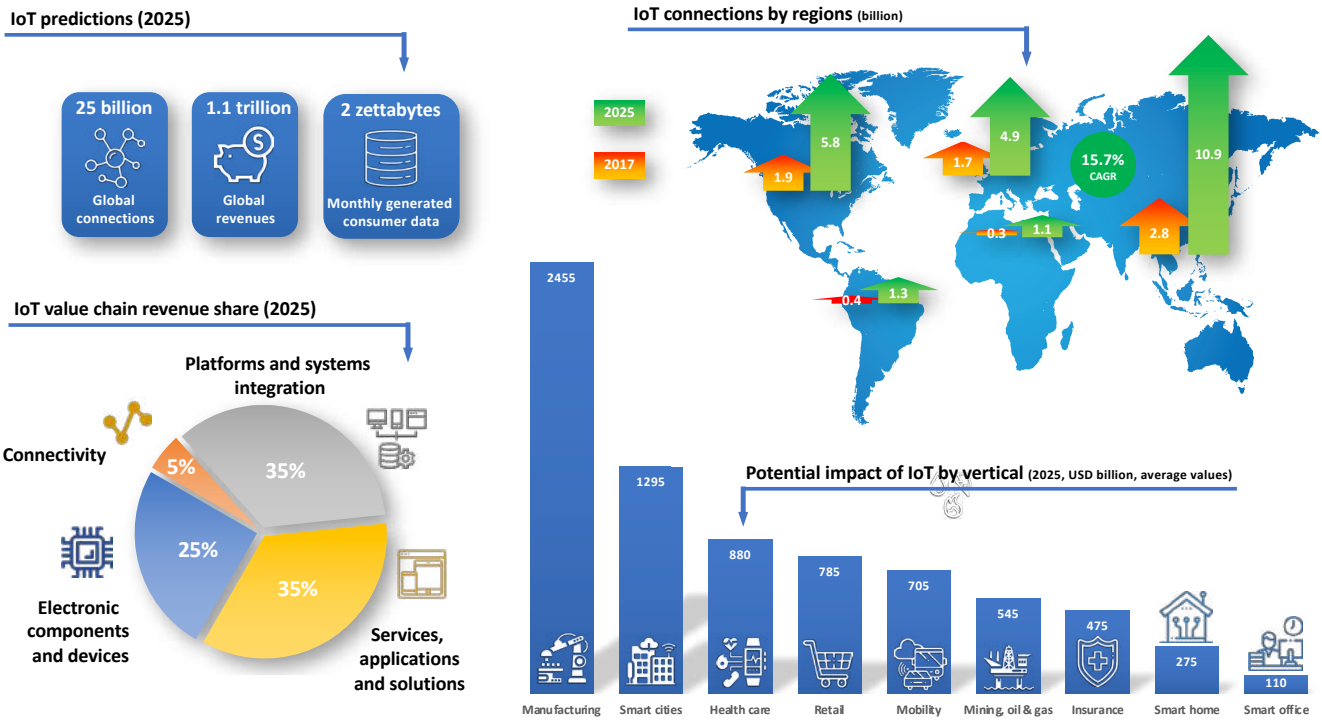


FIGURE 5 — *2025 IoT global market estimations.*

Figure 5 provides an illustrative and non-exhaustive estimation of the potential of some vertical IoT markets by 2025.

Manufacturing will be the largest potential market, with spending concentrated mainly on IoT solutions to support manufacturing operations and production asset management. Industrial IoT provides to manufacturers equipment and machinery remote monitoring, controlling and servicing, with the possibility to scale up these functionalities to the dimensions of a large and geographically distributed industry. Many plants are already utilising connected control systems for monitoring and supervision, and the vast majority of companies in the manufacturing domain consider the IoT implementation as a way to further reduce costs and improve products. Moreover, the benefits of IoT adoption starts from factory, facility and asset management, but extends to security and operations, logistics, customer servicing, etc. *Five drivers are influencing this huge potential market: predictive maintenance, remote production control and optimisation, asset tracking, logistic management and asset/product virtualisation.*

> *IoT vertical markets are strictly linked and interdependent: thanks to IoT, the demolition of vertical silos will be a natural step in their evolution.*

Maintenance information allows the condition of the machinery to be estimated, warning signs to be identified, alerts sent and the maintenance process automatically triggered: IoT allows this information to be collected and maintenance to be transformed into an efficient and automated process, able to foresee failures before they happen. IoT-based maintenance takes traditional maintenance processes a step forward because it optimises costs, limiting maintenance actions exactly and only when they are necessary and required. IoT is also able to prolong equipment lifetime, contribute to plant safety and significantly reduce the risks of accidents.

Remote production control, enhanced with IoT, allows the centralised supervision of all the machinery in the manufacturing process. The information collected through the IoT infrastructure from remote machinery and equipment quickly provides a much clearer understanding of the actual production status. IoT simplifies and speeds up the analysis of data at enterprise level and supports real-time decision making. *Remote control is the prominent driver of the IoT manufacturing market.*

Manufacturing control implies also the adoption of asset practices to track, monitor and oversee all the components of the supply chain (raw materials, containers and finished goods). IoT allows the *real-time collection of asset information* that can be visualised and analysed with web or mobile applications, allowing personnel to quickly make reasonable decisions: similar applications can significantly optimise logistics, ensure the availability of the assets required in the manufacturing process, disclose thefts and violations. Moreover, IoT-based asset tracking allows the usage of movable equipment to be calculated, their idle period to be reduced and their utilisation enhanced.

When the manufacturing process "interacts" with the *logistics domain*, IoT helps to reduce inefficiencies, specifically when the company has to manage a fleet of vehicles. Logistics managers can exploit logistics information collected with IoT to reduce repairs, monitor fuel costs, optimise delivery costs, diagnostics, and also monitor drivers.

The *virtualisation of manufacturing* is a strong driver of the IoT manufacturing market. Through the availability of digital twins, companies simulate robust digital copies of both the manufacturing plant and of the physical objects manufactured. This kind of IoT application has been demonstrated to replicate very accurately the characteristics and behaviours of physical artefacts, allowing the calculation of machine lifespan, checking the correct operations after updates, and predicting potential issues and bottlenecks. The digital twin allows producers to work on a replica of machinery and goods to monitor and test them in a virtual environment, before putting them on the market. This approach significantly improves the product quality, improves the efficiency of supply and delivery chains, brings customer service to a higher level and generates new business opportunities.

Smart cities represent the second area in terms of market potential, probably because of the large number of use cases in a city that could take advantage of IoT technologies and because of the variety of stakeholders potentially involved. The adoption of IoT technologies is emerging and/or consolidating in many key sectors of a smart city, including:

- *Governance:* IoT contributes to the flexibility of the governance structure and to the decision mechanisms, but requires new regulations linking local laws to the new digital environment.
- *Economy:* IoT promotes viable and sustainable business opportunities, generally contributing to improve the economic status of the city.
- *Mobility:* IoT ensures the infrastructural elements and the management solutions at the base of future public transportation network and more generally city mobility (including parking, electric cars, car sharing, limited traffic areas, cycle paths, etc.).
- *Environment:* IoT contributes to the creation of a cleaner and greener environment for the citizens, providing smart objects and infrastructures for monitoring the environmental conditions (e.g. air pollution) and for the efficient and sustainable management of waste disposal, water treatment plants, etc.
- *Living:* the possibility to collect and analyse vast amount of the data from the urban issue allows the provision of services that improve the living conditions in many areas, such as healthcare, childcare, cultural events, entertainment, etc.
- *People:* the IoT infrastructure is fundamental to improve the notification and information channels and media directed to citizens (e.g. information regarding traffic, air pollution, safety, governmental news, events, etc.).
- *Public safety:* IoT enables many advanced and more efficient solutions for city surveillance, emergency response and disaster management that represent key components of smart city modern life.

The urban environment is also well suited for *cross-vertical applications*: consider, for example, the potential application that could result connecting different sectors – like health, social, transport, education, housing, water, energy, security, retail, tourism etc. – that by becoming digitalised could interact and cooperate exchanging information and services to improve the general quality of life in the city and ensure its environmental sustainability. IoT platforms will play a crucial role in the smart city context, having to manage complexity and heterogeneity, ensuring interoperability, flexibility, scalability and security.

The global IoT market size related to **healthcare** is estimated to be the third area of major spending by 2025. The key factor for this significant market development is the *increasing penetration of connected IoT devices in various healthcare sectors* that can take a significant advantage from the adoption of IoT infrastructures and software solutions. Also in this domain, the list of potential applications is endless. An IoT-based solution allows monitoring, taking readings, observing patients' behaviours, and notifying them in the case of potential risks. The real-time capabilities of these solutions allow real-time patient monitoring, extending the treatments also to at-risk patients, making informed decisions, and preventing emergency situations. Moreover, the combination of remote monitoring, mobile devices and analytics could cut the rate of hospitalisations of patients suffering from heart failure, diabetes, blood pressure, etc. *The healthcare market is attracting large investments because, in significantly reducing the costs of the healthcare system, it indulges the trend of public institutions that are dramatically reducing the budget available for public healthcare.* Geographically, North America is expected to be the largest healthcare IoT market.

The IoT **retail market** is expected to be very close to healthcare in terms of dimensions and seems to focus primarily on five sectors where IoT solutions could provide significant advantages: *store analytics, loss prevention, supply chain optimisation, inventory optimisation and surveillance*. Retailers are strongly pushing the adoption of IoT solutions, because they allow them to understand everything about their customers, they contribute to reducing and preventing thefts and optimise almost every process adopted for retail management. According to a report from Microsoft[14], 87% of retailers consider the adoption of IoT connected solution a critical step for their success, and 92% of them have already implemented some form of IoT in their store. However, the IoT retail market is also characterised by a high level of project failure and it is hindered by privacy issues, customers' concerns and inadequate/inefficient regulations[15].

The **smart mobility and transportation** markets are apparently moderately competitive, if compared to the previous markets, but it is difficult to estimate the market potential because of its complexity and because of the evanescent boundaries between smart mobility and smart city markets. The growing world population, rapid urbanisation and the handling of vast amounts of freight, creating congestion and safety issues on the road network, represent the main motivations for establishing a smart mobility market. The availability of IoT and cloud technologies, the advances in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are making smart mobility a reality, creating a global pull. Smart mobility applications are the result of the vertical adoption of IoT technologies, integrated with the existing transportation systems and supported by specific management strategies. Typical use cases are traffic management, road safety and security, parking management, public transport, automotive telematics, freight management, etc. Europe is expected to reach the largest share by 2025, due to the government support and the large investments in the automotive sectors. More than 200 million connected cars are estimated to be already on the road in Europe and this market is rapidly increasing. The congestion of the road networks is pushing the research of solutions for urban transportation that are becoming essential for quality of life: IoT connected technologies in the automotive sector are boosting the adoption of IoT solutions also in the transportation sector. In this sector, more than half of IoT spending

[14] *https://azure.microsoft.com/en-us/blog/iot-signals-retail-report-iot-s-promise-for-retail-will-be-unlocked-addressing-security-privacy-and-compliance/*
[15] *https://www.wired.com/story/stores-must-tell-you-how-theyre-tracking/*

may be invested in freight monitoring, followed by fleet management. The smart transportation market is also positively influenced by government organisations that find in IoT-based solutions the way to create safer, more efficient and greener transportation.

The **mining, oil and gas** sectors have been initially resilient to the penetration of IoT technologies because they have to deal with harsh and challenging environments that require extremely reliable and robust solutions. The evolution of these markets is also strongly influenced by key factors that are independent of technology: political sensitivity, governmental regulations, resource nationalism, limited access to capital and rising costs.

The adoption of IoT technologies in the *mining sector* is expected to generate USD200 billion by 2025 with a CAGR of 8.2%. The mining industry is looking for new technologies able to support the increasing product demand and the parallel reduction of costs. Smart mining exploits the possibility to connect in real-time machinery, collect information, speed up decision-making and optimise the mining business processes, to ensure a considerable optimisation of costs. Connected mining provides real-time visibility in the various phases of the mining and production process, accurately monitoring output, machinery, equipment, the workers' location and their safety/security. The value chain is composed by few major players that leverage IoT to create new partnerships and alliances, increasing their market share and profitability. North America will hold a major share in this market.

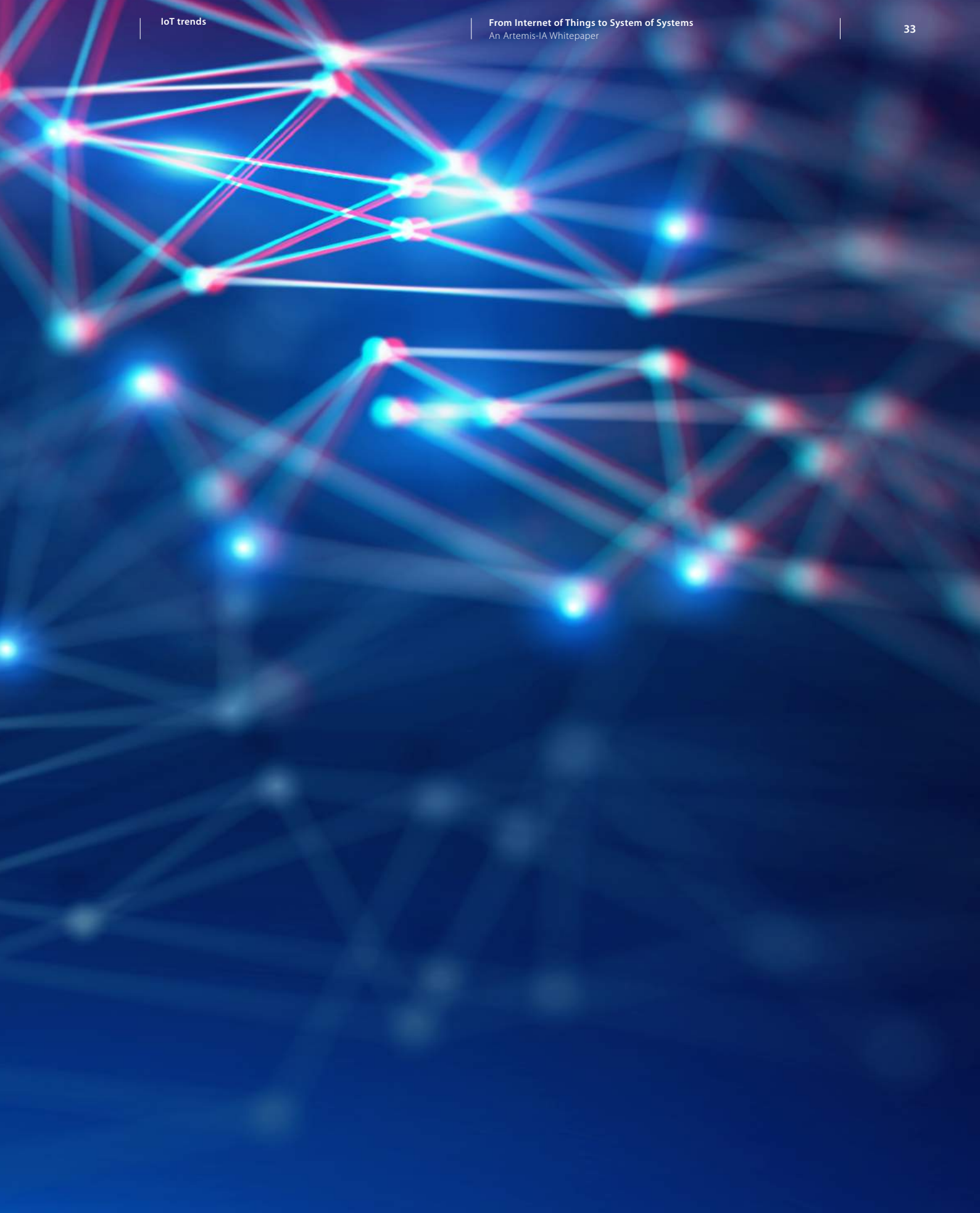
The *oil & gas industry* is expected to exploit IoT technologies in a similar way, connecting assets, people, products and services and streamlining the flow of data to enable fast decision-making, increase asset performance and improve the production process. The adoption of IoT technologies is expected to increase profits of USD100-200 billion by 2025, with an increase in oil production of 10% every two years. The proven abundant availability of oil and gas reserves, the growth of the product demand and the availability of industrial IoT across drilling and production assets are driving the market growth. Many oil & gas companies are already heavily investing in IoT, because they are historically sensitive to the topic of remote management of distributed assets, so they are more open and faster in the adoption of new technologies. IoT solutions are intended to increase asset uptime, provide predictive maintenance, minimise compliance costs and improve the general return on innovation, which is a dominant aspect for oil & gas companies. Remote control and preventive maintenance based on IoT are fundamental to safeguard extremely expensive assets and equipment in-field that are typically integrated in complex systems: a company in the oil & gas market has to manage typically more than 50,000 wells. At this scale, even a slight maintenance delay or inefficiency potentially leads to huge financial losses. IoT solutions enable oil & gas companies also to effectively monitor the environmental conditions in which they operate and ensure the compliance with regulations on emissions and waste: e.g. in the case of a plant failure that generates a leakage of oil, prompt intervention could avoid the payment of penalties that, added to the loss of material, doubles the company loss. Eventually, oil & gas companies live in a market of highly commoditised products and the implementation of IoT helps them to improve their operational efficiency and minimise costs by connecting their internal process with the supply chain.

Insurances represent an underexploited but quickly developing vertical domain for IoT that has been focused until now mainly on improving the interaction with the customer to improve the helpdesk and to simplify and accelerate contract signatures, claims processing, reimbursements, etc. The global IoT-based insurance market was estimated at approximately USD 33.23 billion in 2018 and is expected to generate revenues exceeding USD 400 billion by end of 2025, with one of the highest CAGRs at around 70%. *Insurers are currently attracted by IoT because of the possibility to partner with other stakeholders in the value chain to provide improved or new cross-industry products and services.* IoT technologies allow insurance companies to accurately determine the risks: the use case of connected vehicles that contribute to define and monitor the driver profile to align the related insurance have already demonstrated excellent ROI and costs savings, although this kind of service is still largely underexploited. But IoT can also contribute to *improve the interaction with the customer*, the area where ICT has already significantly reshaped the market: the data collected

from the customer allows a more intensive, qualitative and focused interaction with the customer via telematics apps, limiting direct contact with an agent to customised contract extensions or to handle insurance claims. This digital networking based on IoT generates additional revenues, allowing monetarisation from data analysis (e.g. driving behaviour) and introducing a usage or demand-based service offer. IoT also introduces significant benefits in terms of costs reduction, through automatic maintenance, active prevention and automatic fraud identification. The insurance market will focus mainly on four use cases that can significantly benefit from IoT technologies: smart mobility, smart housing, healthcare and commercial lines. These use cases present very different characteristics, in terms of technologies, involved stakeholders, regulations, etc. requiring completely different business strategies, IoT solutions and insurance products. The development of their markets differs, as well as the dynamics influencing their evolution. Frequently, these use cases are strictly linked together, offering several new opportunities to generate cross-vertical business. Geographically, Asia and the Asian-Pacific region, followed by North America, are estimated to hold the maximum market share, due to the growing awareness and increasing adoption of IoT technologies in these regions.

Homes represent one of the best environments for IoT connected products, which are intended to make our lives easier, more convenient and more comfortable. A **smart home** is a residence where IoT connected devices enable the remote monitoring and management of appliances and systems. It provides improved security, safety, accessibility, comfort, convenience, cost effectiveness and energy efficiency by allowing homeowners to control smart devices and the entire home environment simply using app on their smartphone. The global smart homes market is experiencing consistent growth driven primarily by *safety and security applications, followed by operational & energy efficiency services*. The market enablers are exactly the internet infrastructure and the IoT technologies but, despite the availability of technology, some limiting factors have prevented market uptake to date. Indeed, consumers' hesitance in accepting IoT technologies, concerns related to security issues, privacy protection and governmental regulations represent important barriers to be quickly removed for market uptake: statistics show that, currently, only 12-16% of US residences can be considered smart homes, due to these mass adoption barriers. The global smart home market was estimated at around USD 56 billion in 2016 and is expected to exceed USD 250 billion by 2025, growing at a CAGR of around 14%. Amazon and Google dominate the market, providing a wide set of smart appliances and products for the home automation, from smart thermostats to smart lighting. IoT is also playing an important role in the entertainment domain. A large market share is represented by smart meters and smoke detectors, which present a high penetration rate. Smart meters are perceived by homeowners as a good solution to hinder the increasing cost of electricity that is becoming a major concern. Moreover, the increasing popularity of smart plugs, smart lights, smart hubs and smart locks is also pushing the adoption of home automation systems.

The use of IoT extends to both commercial and residential buildings, creating not only smart homes but also **smart offices**, and eventually smart buildings and smart cities. The smart office market is estimated today at around USD 28 billion and is expected to reach USD 110 billion by 2025, at a CAGR of 16%. The IoT technologies involved in a smart office include smart lighting, security and access control systems, heating and cooling systems, energy management systems, connected and intelligent cameras, audio-video conferencing systems and fire and safety control systems. *The market is mainly driven by the increasing demand for intelligent office solutions, energy efficiency, safety and security at the workplace.* Large companies also tend to adopt IoT-based solutions directly for new building because the ratio between the solution costs and the offered functionalities is very favourable. However, the smart office market is more affected than smart homes by the consumers scepticism about smart technologies and by the concerns about security and privacy: this market is vulnerable because large companies are more frequently becoming the target of cyber-attacks, raising concerns over the deployment of smart office systems.



IoT trends

Several IoT trends are shaping the evolution of the global IoT market and the way IoT impacts on the vertical domains where it is adopted as a solution.

Computing on the edge – With the disruptive increase of collected data, the solutions for processing information based on a centralised approach (e.g. cloud, data centres) will not provide the necessary performance levels to process data in real-time and react adequately. The increasing processing power on the edge of IoT and in the "intermediate" nodes of the IoT infrastructure allows the processing, in real-time, of a large amount of information directly at the source, optimising the IoT connected applications, increasing the intelligence of IoT devices, improving their level of autonomy, reducing the connectivity costs, introducing a level of dynamicity and flexibility that reduces the ROI, etc. IDC estimates that 40% of all data created by IoT devices will be stored, processed and analysed close to or at the edge of the IoT infrastructure already by 2022[16].

> *The shift of computing to the edge, hyper-connectivity, artificial intelligence, security awareness and sustainability are the short-term linked trends influencing the IoT evolution.*

Hyper-connectivity – Global and high-performance connectivity is a crucial factor for the uptake of IoT and SoS. According to Cisco, five quintillion bytes of data are produced every day and efficiently transferring just a part of them from the field, through the IoT infrastructure, to the cloud or data centres for data analysis, will clearly require hyper-connectivity. Moreover, where hyper-connectivity is the key to support global and connected IoT value chains in the different countries where the stakeholders operate, the products must be always connected and globally deployed and operated. A large part of telecom operators, in collaboration with IoT platform providers, are moving towards *global connectivity platforms*, able to ensure high performance and seamless connectivity, supporting very different cellular networks and providing user services for the connectivity management, performance evaluation, usage profiling, etc. 5G technology is in the spotlight, with great expectations that are currently only partially satisfied by the networks currently available. The 5G rollout was meant for 2020 and will probably happen quickly, with fast-growing, wide-scale deployment of 5G networks, providing meaningful coverage of wide

[16] *IDC FutureScape: Worldwide IoT 2019 Predictions, IDC FutureScape 2019.*

areas, and with the availability of lower-priced chipsets. A recent IDC report estimates that global 5G services will drive 70% of companies to spend USD1.2 billion on connectivity management solutions[17]. *Satellite-based communication* is a complementary approach to connectivity that is reaching a hype: more than 2500 satellites will be launched before the end of 2020. This marks a new era of broadband internet that is expected to rely on a satellite network composed of more than 12,000 satellites by 2023.

Artificial intelligence – Artificial intelligence is becoming available to a large set of new embedded systems, with significantly improved capabilities: this is one of the faster growing trends in the AI domain. The interaction and cooperation between humans and AI will increase and, considering the capability of embedded intelligence to disappear in the environment around us, *we will probably not know and recognise it is an artificial intelligence*. Virtual assistants represent a good example of this trend: the algorithms have been shrunk and optimised to fit a large class of low-resource devices and provide extended functionalities that go beyond simple voice-based assistance, extending to autonomous cooperation with other devices in the environment for home security, user safety, better entertainment, environmental monitoring, etc. This trend also influences other domains, like industry with more intelligent traditional robots involved in manufacturing but also with software robots, able to monitor and automate processes, by automatically filling forms, generating reports, producing documentation, etc. Autonomous driving is a very hot topic for embedded intelligence, because AI is the primary and crucial enabling technology for this domain, with around 2.3 USD billion of investment for autonomous vehicle software and 5.6 USD billions for sensors and systems[18].

Security awareness – All the actors involved in the IoT value chain are becoming more and more sensible and aware of the security risks associated with the adoption of IoT, because it represents a playground for hackers with unprecedented opportunities to mine the entire IoT market. *Security is perceived more as an opportunity, rather than a burden.* IoT security not only protects the digital dimension of a vertical application but enhances and strengthens the security level of the physical infrastructures associated with the IoT vertical application. The approach of selling an IoT solution now and patching the security issue later paves the way to the concept of security by design and on its continuous improvement, looking towards end-to-end security solutions. In this perspective, the development process is also evolving from an approach based on single developer expertise to the inclusion of *security support in the entire engineering process across the product lifecycle*.

[17] *https://www.idc.com/research/viewtoc.jsp?containerId=US43161517*
[18] *Start me up: Where mobility investments are going, McKinsey, April 201*

> *The nature of IoT and SoS is forcing a reconsideration of the concept of lifecycle, frequently limited to engineering, and requires to extend it to the operation, maintenance, retirement, recycling and evolution phases. A deep and comprehensive knowledge/control of the entire lifecycle represents the baseline for sustainable products/solutions and for the achievement of European Green Deal objectives [19].*

Sustainability – New awareness for sustainability reached millions of individuals with climate change concerns but is also leading large corporations to reprioritise their top-level strategies: sustainability is becoming a global key governmental[19] and business priority and the adoption of digital technologies like IoT could really contribute to accelerating the process of reducing global emissions. The 2019 Exponential Roadmap[20] identifies 36 solutions to cut 50% of worldwide greenhouse gas emissions by 2030 and large part of them are linked directly or indirectly to IoT. The whole IoT value chain plays a fundamental role in achieving a high level of sustainability, providing an ecosystem of stakeholders (from semiconductor companies to applications, service provides and the final user) that must combine their efforts to develop, deploy and operate IoT solutions in a seamless and environmental-friendly way. Sustainability must be ensured across the entire product lifecycle, from when the product is conceived until its retirement and recycling, at product end-of-life.

All these trends influence and depend deeply on each other. IoT devices need more computing power to process a large amount of data on the edge in real-time, to make information meaningful. But all the data they are transmitting risks supercharging the communication networks and new solutions for high-performance connectivity become a requirement. Moreover, to make information meaningful, we need a more powerful and embedded artificial intelligence that, in turn, could also rationalise the amount of transmitted information. The pervasiveness of IoT and the nature of data transmitted expose many vertical domains to unprecedented security risks that urgently need to be addressed with reliable and scalable solutions. And eventually, processing power, embedded intelligence, hyper-connectivity and security must be ensured in a sustainable way, in order to coherently make IoT the perfect solution to improve the sustainability of vertical domains.

---

[19] *https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_e*
[20] *https://exponentialroadmap.org*

The IoT value chain

During the last decade the ARTEMIS and ECSEL projects covered all the phases of the IoT value chain, from the physical world to the final services and applications generated through the digitalization process, demonstrating a deep comprehension of the IoT nature, a sensibility for aspects that go beyond the pure technical domain and the importance of partners cooperation for the existence and evolution of the IoT market. Probably, the *value chain* is the most important aspect of the business model because, considering an IoT end-to-end solution, it identifies the involved stakeholders, it defines how they cooperate to provide the end-to-end solutions, which business model they adopt and how the final service and application is delivered. *IoT has a very complex value chain*, due to the complexity of the IoT solutions, that requires the joint engineering effort of multiple stakeholders, belonging to different technological domains, with different business models and, depending on the vertical application, impacting on a large number of different processes.

The *cooperation* is, indeed, a key factor for the success of an IoT solution on the market, because it is unrealistic that a single vendor is capable to deliver and manage a complete end-to-end IoT solution, due to its technical and business complexity, its heterogeneity, its diversity, etc. In a similar scenario the spontaneous formation of partnerships between stakeholders is not an easy process, but the increasing comprehension of the mechanisms that govern the IoT allows the stakeholder to identify its role in the value chain and, depending on its business area, to create partnerships with other stakeholders.

> *One of the roles of ARTEMIS/ECSEL projects has been exactly to allow partners to reach a better understanding of IoT from many perspectives, technical, engineering, operational, vertical applications and consequently also from the business perspective.*

A clear view of the IoT governing mechanisms is a competitive advantage for the partners of ARTEMIS/ECSEL projects, because it provides more chances to easily identify their best role and position in the IoT value chain, understanding their relevance for the value chain, the available business opportunities and the business strategy to adopt.

Every stakeholder has a specific relevance for the value chain, depending on its business, but it is difficult that a single stakeholder will entirely lead the IoT value chain. The players covering the large part of the value chain and capturing most of the opportunities it offers should ideally take a lead position and define partnerships and alliances. *It is clear that the platform providers are best positioned to lead the IoT value chain as they capture the large part of the opportunities IoT offers.* Unfortunately, a similar configuration where platform providers could apparently control the entire value chain, offering complete end-to-end solutions that hide the other stakeholders, exposes the IoT market to fragmentation, one of the strongest barriers for the IoT uptake.

The integration of the value chain

The *integration of the value chain* is the key factor to guarantee an optimal final result and it should consider the following aspects:

- **Data collection.** An IoT solution is not just the sensors-based instrumentation of materials, of packages, of products or the instrumentation of their manufacturing, delivering and servicing process. IoT is primarily data collection from a four-dimensional environment (a 3D space plus time), subsequently filtered and processed for downstream actions, applications and services across the value chain.
- **Connectivity and storage.** Connectivity is the key enabling technology to ensure the flow of information in the value chain and to maximize the information value. For this reason, the value chain must support multilingualism and interoperability, through the adoption of platform capable to be hardware, communication protocols and information agnostic. But the flow of information is not enough: the stakeholders in the value chain need one or more storage "points" to archive, retrieve and share the collected information. Shared storage solutions like the cloud platforms allow operational insights from the collected information, that can be stored, integrated, processed, synthesized, and made available for the services and final applications.
- **Data processing and knowledge creation.** IoT is generating and will generate an avalanche of information but, to unleash the real value of the information, we need to find a rationale in this huge amount of data if we want to clearly understand the situation and take the most appropriate decisions/actions. Currently, most of the IoT collected data are not used or are in general underexploited: frequently the usage of data is limited to anomaly detection and real-time monitoring and control, rather than for optimisation and prediction that provide significantly more added value. The inability to fully exploit the data captured through the IoT infrastructure is due to technical aspects, but also to organisational and commercial barriers. Analytics is fundamental to leverage collected data for actionable insights, while automation is fundamental for the conversion of insights in actions. Data processing and knowledge creation are two fundamental factors for the IoT value chain, being part of the IoT infrastructure from the edge to the enterprise level and, consequently, involving almost all the stakeholders of the value chain.

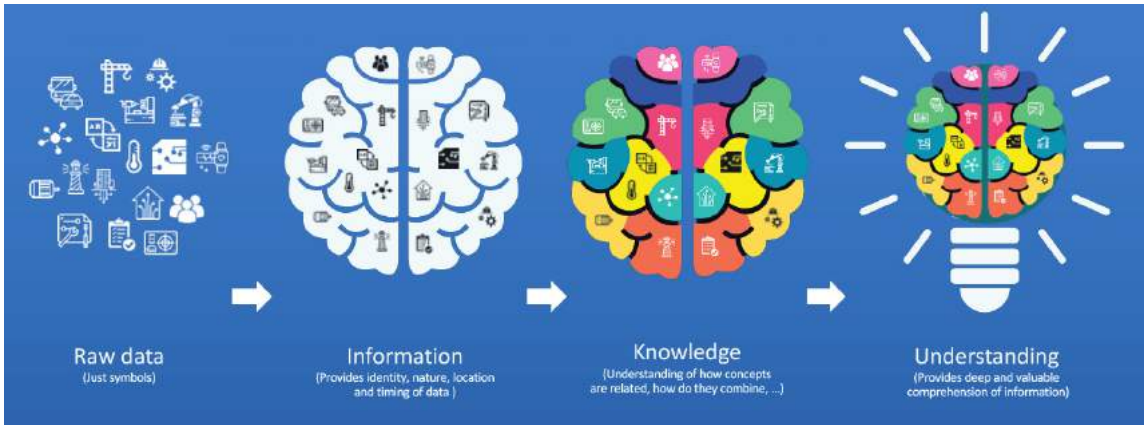


FIGURE 6 — *From data to knowledge.*

- **Trust.** The impact of IoT on the final user, on society and on the value chain is unprecedented and, considering the scale of IoT and the complexity of an end-to-end solution it consequently requires end-to-end trustworthiness, including security, privacy, safety, dependability, device and information control and management, etc. The end-to-end trustworthiness is fundamental from a technical perspective but also for the existence of the value chain itself, in order to allow the creation of alliances and partnerships based on trust between the involved stakeholders.
- **IoT beyond operations optimization.** The immediate and extremely valuable application of IoT is operations optimization, considered in its widest meaning and applied to a huge set of vertical domains. This IoT application is enough to justify the entire IoT market and to ensure the existence of an IoT value chain. But the focus of IoT solutions is quickly evolving beyond the operations optimization, trying to provide new services, new cross domain application, new ways to engage the final user, new business models (e.g. pay per use), new ways to monetize data, etc. The IoT value chain plays a fundamental role to ensure this evolution.
- **Stakeholders role and positioning.** The variety of technologies adopted in an IoT end-to-end solution is enormous and the complexity of the vertical (and cross-vertical) domains they try to support is as well enormous. This complexity reflects also in the value chain required to manufacture, deploy and operate an IoT end-to-end solution, therefore it is fundamental that each stakeholder involved in the value chain has a clear and well defined role and business positioning.

The stakeholders of the value chain

In the large majority of vertical domains, the stakeholders involved the IoT value chain belongs to six main categories:

- Electronic components and device providers
- Telecom operators
- IoT platform providers
- System integrators
- Application or service providers
- Final users

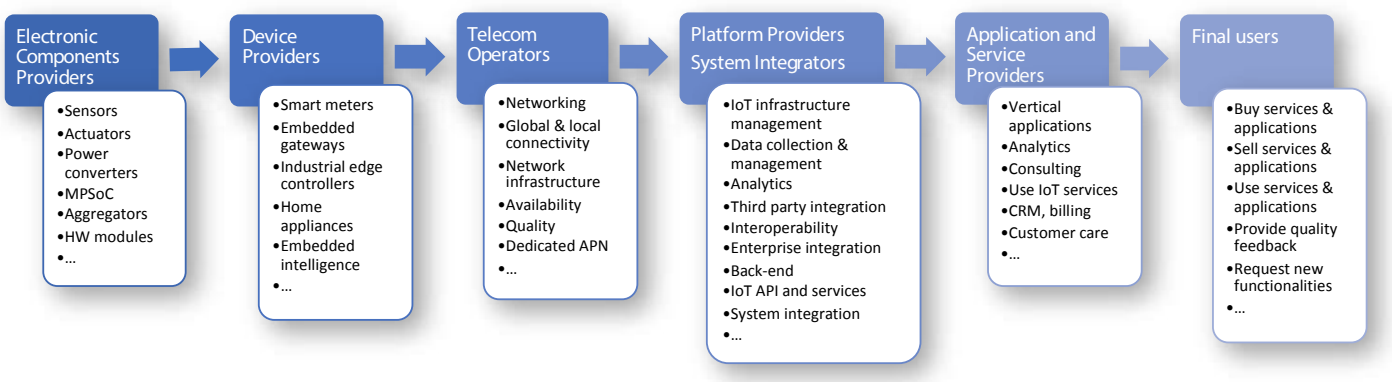


FIGURE 7 — *Simplified example of the IoT value chain.*

Every electronic device around us depends on semiconductors, included the IoT, where sensors, actuators and devices play a critical role: **semiconductor companies** represent the basement of the value chain. According to Gartner the semiconductor spending in the IoT market is expected to reach USD$34 billion already in 2020[21], but if we consider IoT electronic solutions the projection rises at USD$572 billion[22]. For semiconductor companies the IoT market is a huge opportunity to reinvent themselves, to significantly increase profitability and to provide new value to their customers. But to make a profit on low margin products and create value in this market, semiconductor companies can no longer remain simply component providers: they must consider the entire IoT ecosystem and understand the requirements of the entire IoT stack in order to provide solutions based on integration, software and services. In some cases, they are trying to provide end-to-end solutions that facilitates the uptake of the IoT market.

Device providers are positioned closely to semiconductor providers, and they also share with them the necessity to increase the current "share" of the value chain. Device providers represent the second pillar of the IoT market, with an important role for edge computing but, remaining just vendors, they could capture only a limited part of the market value (e.g. around 10%), without exploiting the full benefit that the hype around IoT offers. Device vendors must develop a service-based model for IoT and create vital partnerships with the value chain lead player. In some cases, device vendors try to capture a larger part of the value chain offering also an IoT framework and an integration platform, intended to provide a seamless and open solution for the IoT infrastructure (e.g. Eurotech ESF and EC[23]).

The third pillar of the IoT value chain is represented by **telecom operators** that are critical for providing the internet connectivity. They consider themselves as a primary player, but the large part of their revenues (80-90%) comes from annuity business, that is, from a stable business environment that unlikely adapts to the quickly evolving nature of IoT. Telecom operators are crucial for an IoT solution, but they require partnerships and alliances with other players of the value chain to go to the market: in a business driven by data usage, connectivity on its own risks to become the non-added value part of the IoT value chain, relegating telecom operators just to the role of communication channels providers.

IoT platform providers play a central role in the value chain, a role that reflects the function of the platform in the IoT architecture: an IoT platform is the core of the IoT infrastructure, orchestrating its parts, managing them and bringing together hardware, software, connectivity and services in a specific IoT end-to-end solution. Similarly, in the value chain, platform providers become the centre of partnerships and alliances intended to create the synergies, to provide the complementary expertise, the assets,

---

21 *Gartner, Forecast: IoT endpoints – Sensing, processing and communications semiconductors, worldwide, 2016 update, January 9, 2017, https://www.gartner.com/doc/3565023/forecast-iot-endpoints--sensing.*

22 *Gartner, Forecast: Internet of Things – Endpoints and associated services, worldwide, 2017, December 21, 2017, table 3-1, https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.*

23 *https://www.eurotech.com/en/products/iot*

the business support, the management and operational capabilities required by the IoT end-to-end solution. To achieve this leading position in the value chain, the platform must cover and combine a wide set of functionalities: device and fleet management, information storage, processing, visualization and analytics, developer support to simplify the integration with third party systems (e.g. API, SDK, etc.) and strong legacy support.

System integrators role is twofold, because they significantly contribute to manage the intrinsic heterogeneity of IoT and they ensure legacy support, that is fundamental to valorise already existing digital assets. One of the obstacles for the IoT uptake is the lack of interoperability and, very frequently, many potential components of an IoT infrastructure are not "plug & play", therefore system integrators are crucial for the IoT value chain in order to ensure the seamless integration of these components and systems. The positioning of system integrators in the value chain depends on the vertical domain and on the partnerships they establish with platform providers. In some cases, their extensive and multidisciplinary expertise allows system integrators to become also platform providers.

Application or service providers position almost at the end of the value chain, where the large part of the added value offered by IoT lays. They are typically too small players to lead the value chain and their positioning depends on the partnerships they establish with system integrators and platform providers. Frequently, with the evolution of the specific IoT vertical market in which they are involved, they are acquired by platform providers that aims at consolidating and widening their market share. Except for some large industry players, capable to manage an entire vertical IoT application, application providers cannot in general operate independently but strongly depend on partnerships with the other stakeholders of the value chain. The application and service domains are expecting to totalize the largest share of the revenues in the IoT market, due to the shift of the value towards the higher parts of the value chain.

Last but not least, the **final user** that is a central point for the entire value chain: at the end, the technology, including and primarily IoT, should be conceived to simplify and improve human life. Indeed, a large part of the effort in the value chain is spent for the final user, be he/she consumer or industrial. The final user has also an active role in the IoT value chain, because of the penetration of IoT technology in the everyday life, of the interactivity level of IoT and of the possibility for the final user to provide extremely valuable direct or indirect feedback to the other stakeholders of the value chain.

The value chain as a whole

Looking at the IoT value chain as a whole, *the value and the interest is shifting towards the platform, application and service parts of the value chain*[24] [25] [26] [27]. The stakeholders involved in these parts will have the largest opportunities: the Advancy report[28] estimates that the market related to electronic components, electronic boards & packaging and embedded electronic systems will double, from €1.7 trillion in 2016 to €3.2 trillion in 2025, but the market related to integrated systems, SoS, applications and solutions will grow tenfold, from €500 billion to €3.9 - €11.1 trillion.

Moving up the value chain means *the stakeholder has to leave partially its business comfort zone*, diversify the existing portfolio and offer products and services that position at the higher levels of the value chain. Moving up the value chain means also adopting new strategies and taking a completely new path to embrace more sophisticated roles in the value chain, to develop new capabilities and new business models. *The shift in the value chain carries more risks, but generates also higher revenue and, typically, higher margins.*

The ECSEL community covers the entire value chain of the Internet of Things, from semiconductors, to devices, connectivity, platforms, services, applications and final users. *This coverage and the synergies it could create are a fundamental factor to ensure the success of European strategies aimed to reach the sovereignty in the IoT market.* IoT plays an important role in the European digital economy, providing concrete solutions and the world class infrastructure for the establishment of a single digital market and of digital supply chains.

Following the estimated trends and positioning in the fastest-growing parts of the IoT value chain represents a challenge for Europe and, if we consider the rapidity and the scale at which the IoT market evolves, *it is not guaranteed that Europe will be able to concretize the estimated revenues growth, particularly in the higher parts of the IoT value chain.* To win this challenge, a large effort in research and innovation must be planned for the next decade, trying to capitalize on the existing European strengths in terms of technologies, players and ECS ecosystem.

The value chain evolution

IoT is characterised by a deep networked nature that reflects in the value chain, or better in the value "network", which requires an appropriate ecosystem. *A single company is not capable to offer an all-inclusive solution, covering the entire value network, while an ecosystem of companies, with complementary competences and businesses is the appropriate solution.*

In this ecosystem, new and existing stakeholders will be able to integrate both vertically and horizontally encompassing all stages of production. In a value network, hardware providers, software providers, service providers, brokers and end-users may collaborate in a flexible manner for the creation of the final product: the conventional boundaries between industries, technologies and vertical domains fade away.

The value network has an impact on competitivity. Indeed, the complexity of IoT/SoS pushes companies to bring all competencies under a single umbrella, forging alliances and partnerships, which in turn will compete against each other.

---

[24] *https://www.mckinsey.com/featured-insights/china/chinas-fast-climb-up-the-value-chain*
[25] *Globalisation in Transition: the Future of Trade and Value Chains, McKinsey Global Institute, 2019*
[26] *https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/shaking-up-the-value-chain*
[27] *Study on the electronics ecosystem - Overview, Developments and Europe's Position in the World, Decision Etudes & Conseil, 2018.*
[28] *Embedded Intelligence: Trends and Challenges - A Study by Advancy, Commissioned by ARTEMIS Industry Association, March 2019.*

> *IoT generates a radical change in the structure of the current and future economic system, transforming the linear value chain in a nonlinear value network. Any business combination in the network could potentially generates new revenue streams.*

In a value network the traditional roles and responsibilities can mix, shift and change: customers can act as designers for their products, machine manufacturers can become service providers, selling both machine and aftersales, new service providers could emerge, etc. But the most important advantage of the value network for a company is the possibility to extend its business model from its nearer environment (direct suppliers, clients, etc.) to the entire ecosystem: any business combination between stakeholders in the network could potentially work, generating additional value propositions and potentially new revenues streams.

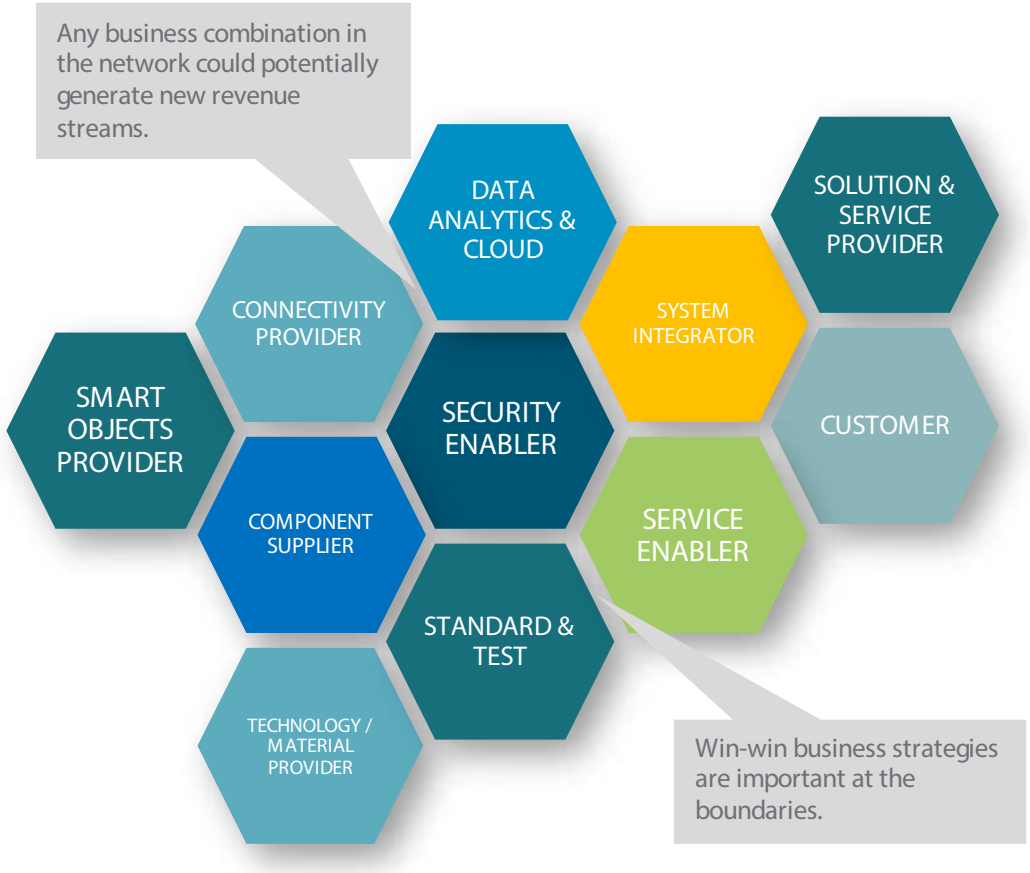
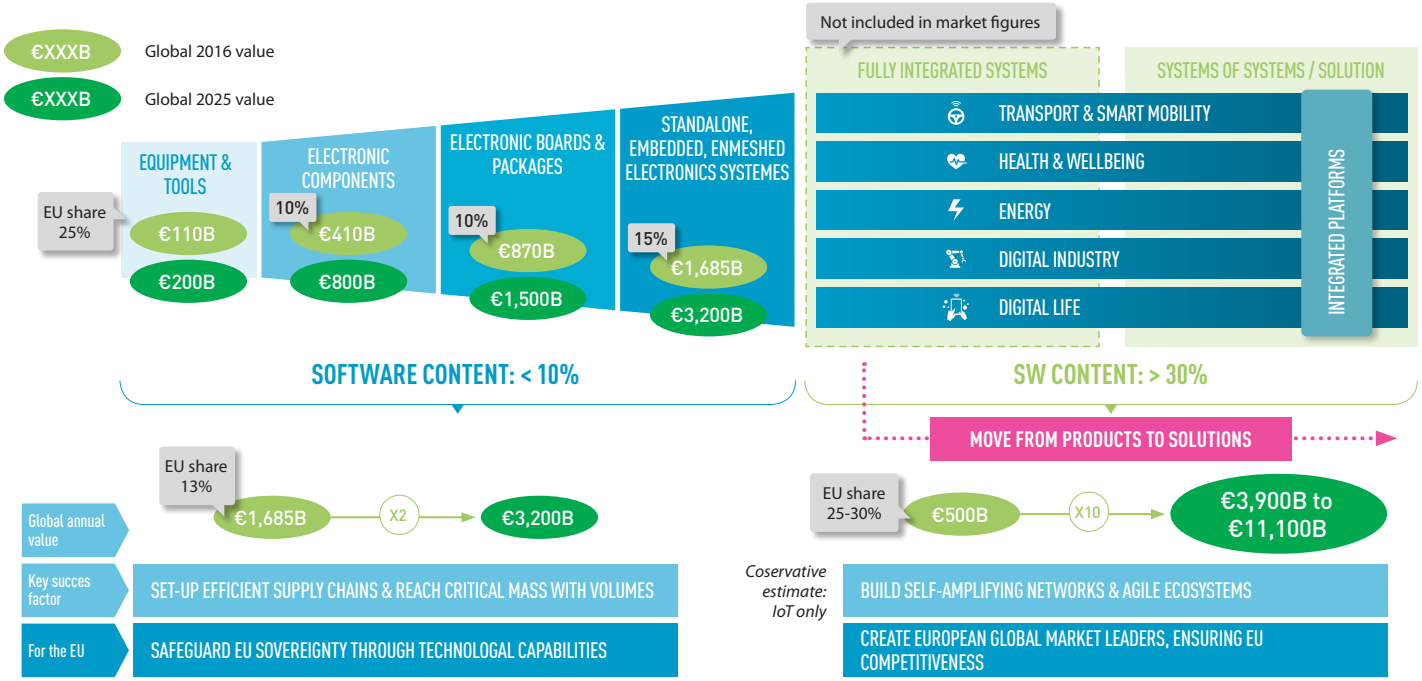


FIGURE 8 — *The IoT value network.*

The coverage of the value chain in ARTEMIS and ECSEL projects

The concept of the value chain always represented, directly or indirectly, a reference factor for ARTEMIS and ECSEL projects, that devoted a large effort to ensure its coverage, both in terms of technologies and stakeholders. In these projects, the investments that intended to provide IoT solutions in specific vertical domains, embracing large parts of the value chain, demonstrated to be correctly planned and anticipated the trends that the analysts are currently envisioning for the next decade.



Note: rounded figures. (1): 2025 estimate value potential for the Internet of Things, not the full potential for ECS end-applications. Source: Decision, IDC, MGI, Advancy research & analysis

FIGURE 9 — *Global and European value chain (source Advancy report).*

Figure 10 illustrates the coverage of the IoT value chain obtained in some ARTEMIS and ECSEL projects. The six projects mentioned represent just an example that demonstrates the attention has been made to the coverage of the value chain in the last ten years and how the shift towards its higher parts was largely anticipated. For example, in the first ARTEMIS call, SOFIA addressed the *value chain of smart buildings* providing smart sensors connected by a multiservice gateway and capable of orchestrating different systems in a building (e.g. lighting, air conditioning, surveillance, etc.). The SOFIA Semantic Information Broker was the core of the solution, collecting the data from the network of sensors and providing support for the final application, that was oriented to the maintenance operators and to the office tenants. A couple of years later, ME^{3}GAS addressed the *value chain of utilities*, with a specific focus on gas consumption monitoring, based on a smart gas meter and an energy-aware middleware, enabling remote management applications, multiple tariffs and payment optimisation for the end user. In the same call, IoE addressed the same value chain focusing on the smart grid and on electric vehicles: in this case the end user was the utility itself.

The Arrowhead project devoted a specific pilot to the value chain behind the heterogeneous domain of electromobility. The pilot intended to remotely manage a distributed recharging infrastructure composed of three different recharging stations, developed by three distinct manufacturers, and aimed at providing monitoring services for maintenance applications and cross-domain apps for the final user. The integration and control of the distributed infrastructure was possible thanks to Eclipse Kura and Kapua platforms, while the added value services and application were built on top of the Arrowhead Framework.

More recently, Productive 4.0 focused on the optimisation of the supply chain management, covering the entire product lifecycle. A common architecture has been devised, which supports interoperability, security, data sharing and solution integration along a multi stakeholder supply chain. A reference implementation for the architecture has been defined and applied to a wide range of production use cases in e.g. semiconductor, automotive, consumer goods and manufacturing.

AFarCloud addresses the agriculture value chain, focusing on crop and livestock management. The proposed solution covers the entire value chain, offering farmers an end-to-end semantic-based management system that improves farming productivity and efficiency. The management system provides mission management tools and a decision support system to improve daily farming activities. It orchestrates the entire IoT infrastructure, from sensors, actuators and smart objects deployed in the field to edge computing IoT gateways, multi- protocol connectivity in the field and to the cloud, to the cooperative mission management of complex systems, such as autonomous drones and ground vehicles for farming.

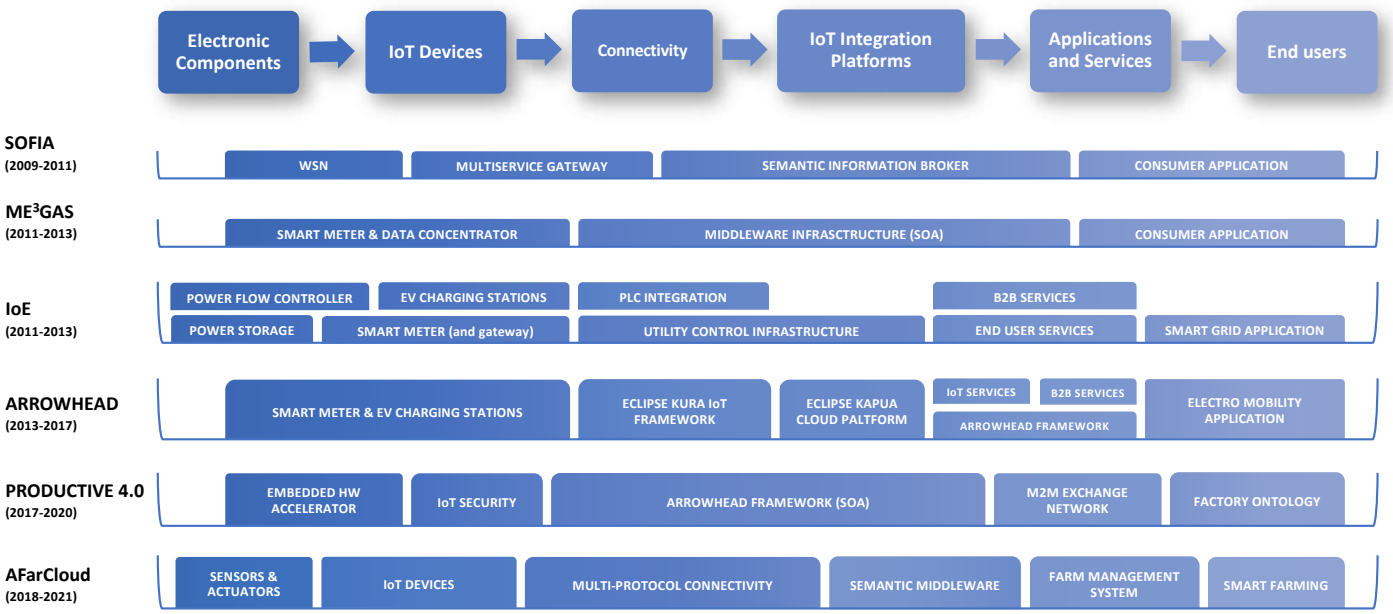


FIGURE 10 — *ARTEMIS and ECSEL projects coverage of the IoT value chain, some examples.*

Recently, SECREDAS has been addressing a value network in the automotive domain, focusing on automated vehicles application and driver monitoring. The linearity of the previous examples leaves space to a more complex network of stakeholders that, with the creation of multilateral partnerships and alliances, jointly contribute to the creation of the final application. This example demonstrates **the real possibility to create an integrated and self-regulating system**

of systems (SoS), beyond brands, industries and vertical domain boundaries. SECREDAS focuses in particular on the development of a network within the car (In-Vehicle Networking, IVN), a control unit in the car (Vehicle Control Unit, VCU) and the driver monitoring system, including connection to IoT. The project provides the hardware and software foundation for running the selected user scenarios and 3 field demonstrations. The key elements that are addressed are: data security, functional safety, privacy, network and processing performance, use of resources and robustness. The value network also includes a stakeholder from an "external" value chain/network, which acts as a platform provider offering a smart traffic solution that is treated as a "black box" in the SECREDAS end-to-end solution. The value network originates from real-life situations encountered by vehicle users during traffic and potential external threats to data and connectivity integrity. More in general, any partnership between two or more "close" stakeholders could potentially generate new value propositions, business opportunities and revenue streams.

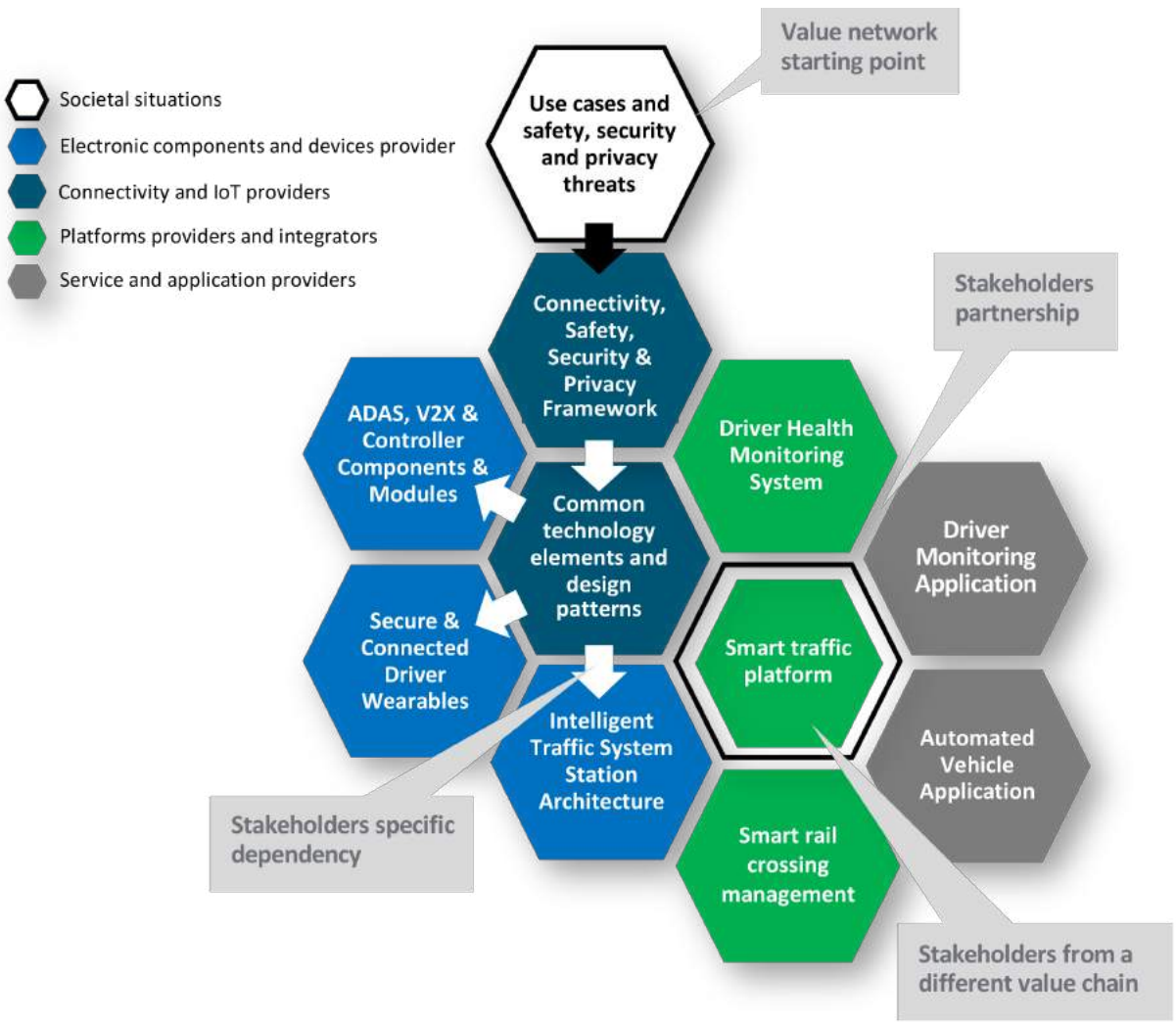
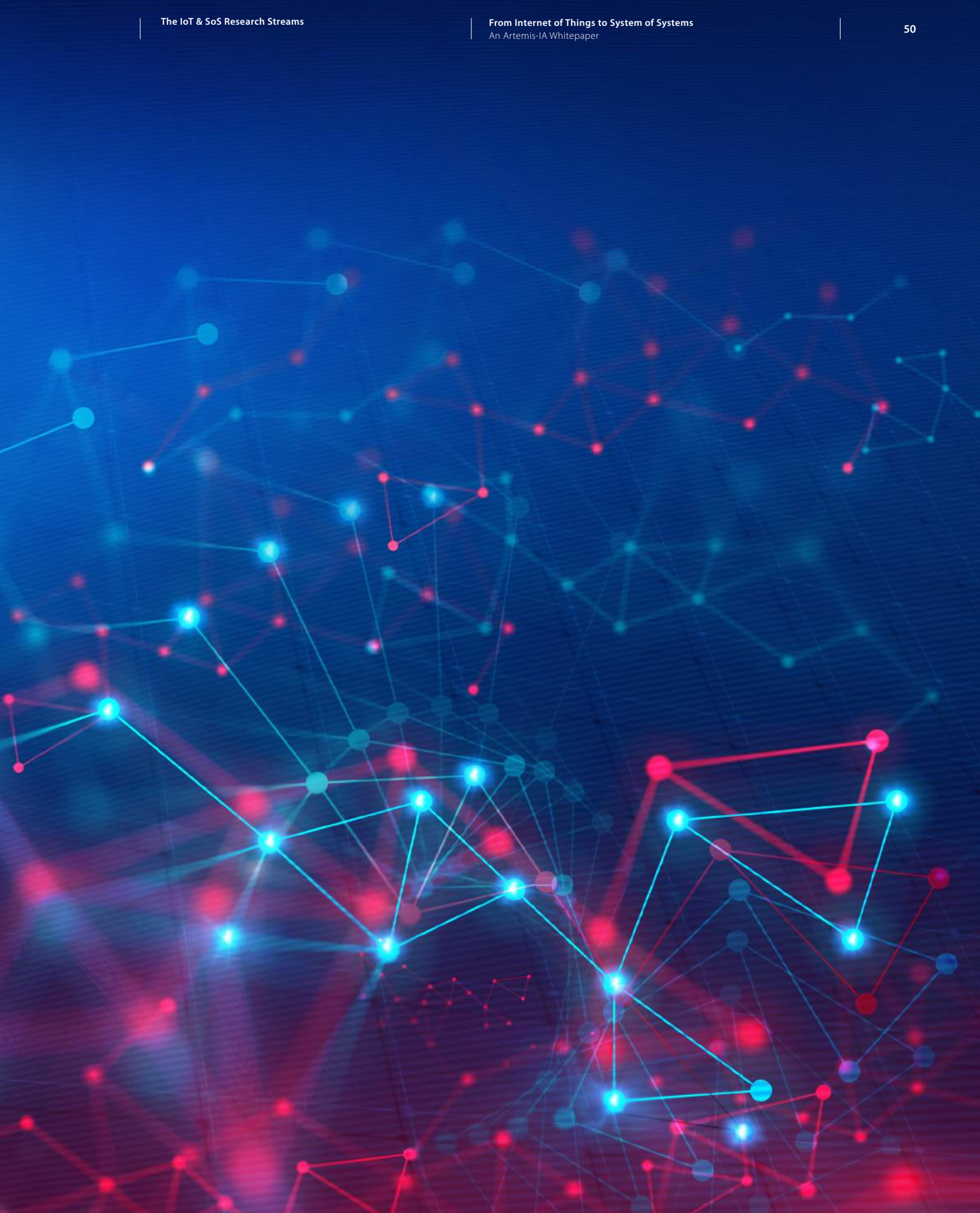


FIGURE 11 — *Example of IoT value network from SECREDAS.*



The IoT & SoS Research Streams

ARTEMIS and ECSEL initiatives are focused on industrial research with projects located at high TRL levels (typically at level six or more), if compared to fundamental scientific research. ARTEMIS and ECSEL projects investigate how to gather knowledge, develop innovative technologies and solutions for the creation of new products, processes, services and applications or to improve the existing ones. Industrial research includes the creation of components of complex systems (e.g. of IoT and SoS infrastructures), possibly tested initially with real demonstrators and subsequently in large pilot deployments, which are necessary for technology validation and eventually for final products/solutions engineering. Inspired by this industrial approach, the evolution of ARTEMIS and ECSEL projects related to IoT and SoS is driven by *four primary research streams* (see Figure 12):

- enabling technologies for IoT and SoS,
- IoT and SoS Architectures,
- IoT and SoS Platforms,
- engineering support for IoT and SoS,

and by *two transversal research streams*:

- interoperability and
- trust.

The research streams are the *macroscopic research domains* that have been identified by the analysis of the IoT/SoS related projects developed by the ARTEMIS/ECSEL community during the last decade. The research streams also represent the *conceptual steps of the evolution of IoT/SoS*: they have no strict chronological order, but they mix, merge, sometimes they run independently, sometimes they influence each other, following the maturity level of the technology, of the community and of the ecosystem. Depending on their objectives, project activities have been focusing on the research streams with various levels of intensity and effort, and this analysis discovered that the projects have not been running in isolation but developing along coherent project lines, across technologies, vertical domains and time.

The initial ARTEMIS IoT-related projects reserved a large part of their research activities on **enabling technologies**, because they were driving the first steps in IoT and SoS. The research of enabling technologies lays the foundations of IoT solutions and allows one to focus on specific aspects of the IoT, evaluates technologies in an early stage of development, elaborates new ideas and evaluates them through technology demonstrators. This research stream is still very active, because of the inherent nature of IoT and SoS that is strongly based on innovation, requiring the continuous development of new technologies.

The integration of different enabling technologies, following a wider design, typically an **architecture**, represents the first step for the creation of an IoT end-to-end solution. Enabling technologies provide the first glimpse of the IoT vision, while architectures represent the attempt to rationalise and "organise" this vision. Architectures define the structure of the IoT solution, how it is composed and organised, how IoT nodes interact, etc. Architectures can be defined only when a certain level of comprehensive knowledge and visibility of the domain is available and, for this reason, projects dealing with architecture appeared later.

A **platform** is the core, the backbone of an IoT end-to-end solution. A platform realises the integrated approach adopted to leverage data from devices, assets and environmental/contextual conditions that, depending on the vertical domain and on the specific business logic, are processed to create added value. An IoT platform can be typically considered as the instantiation/implementation of an IoT architecture, which makes it rather difficult for IoT/SoS platforms to appear without having in mind a clear architecture.

But enabling technologies, architectures and platforms cannot be designed and developed without solid **engineering support**. Research development and, in particular, the engineering of research results to create new products require the support of design methods and tools, across the entire product lifecycle: from the product conception, to development, deployment & commissioning, operation, maintenance and final retirement and recycling of the product. The complexity and interdisciplinarity of IoT and SoS require engineering support more than "conventional" products. The sensibility and consciousness of the important role played by the engineering support have been evident since the very first ARTEMIS call, but it is only in the last ECSEL calls that specific projects have been devoted entirely to this fundamental research stream.

The two transversal research streams have no temporal binding with the evolution of ARTEMIS and ECSEL: the community has been always sensitive to interoperability and trust and, considering the interdisciplinary of these two research streams, they have been developed transversally with respect to the other four research streams. For their importance and complexity, both interoperability and trust have been addressed since the first ARTEMIS call in 2009.

Interoperability is the key element to inherently control IoT intrinsic diversity and avoid fragmentation. Diversity in SoS is not something to be solved, but an aspect that must be embraced and managed: diversity means richness and added value, diversity is an indicator of innovation, but fragmentation is an IoT/SoS enemy.

Eventually, **trust** represents the strongest barrier to IoT/SoS uptake. Not only customers and end users, but the whole IoT value chain and the entire society must trust the security, safety, integrity and privacy of the massive transformation that IoT is generating and will generate. And like interoperability, the complexity and interdisciplinarity of trust make this a transversal research stream.

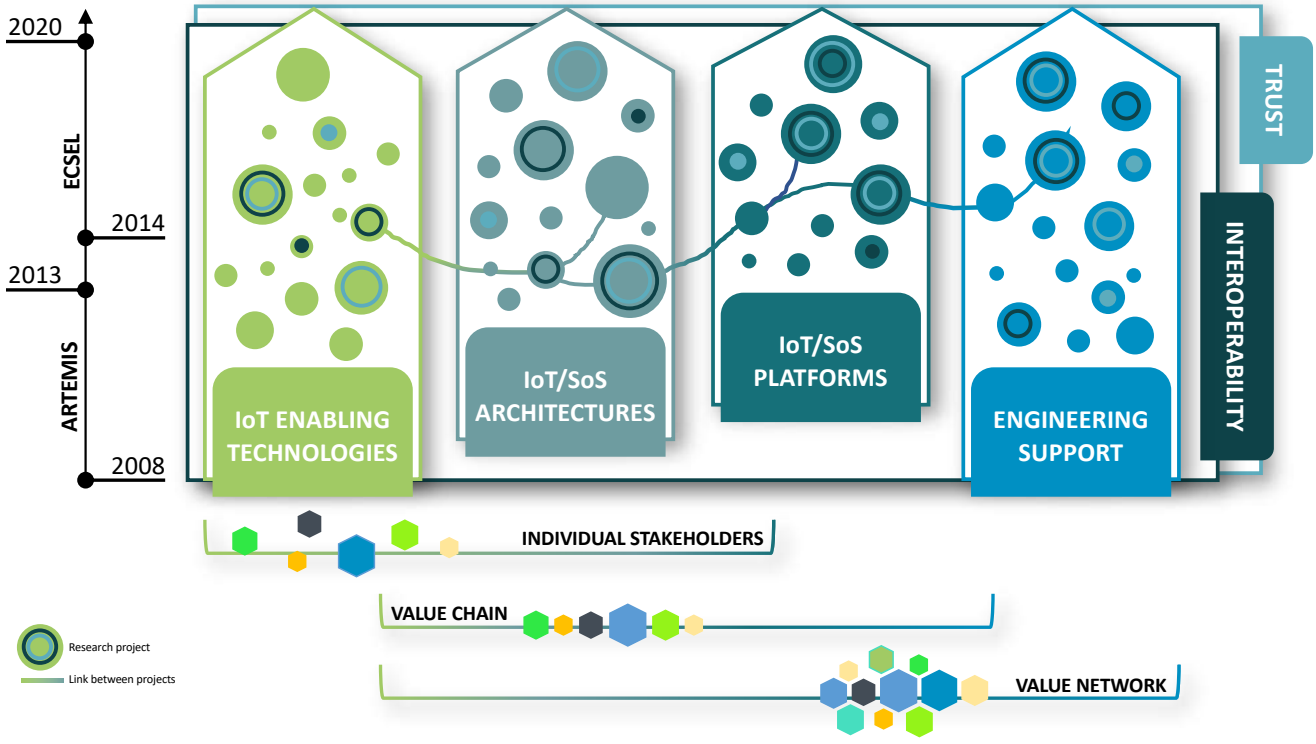


FIGURE 12 — *IoT and SoS research streams.*

For each research stream, the analysis identified several *focus areas of research*, as illustrated in Figure 13. The results of the analysis are reported in the following chapters providing, for each research stream, a description of the stream and of the related focus areas, a summary of all the projects' contributions to the stream and a list of potential evolutions of the research stream.

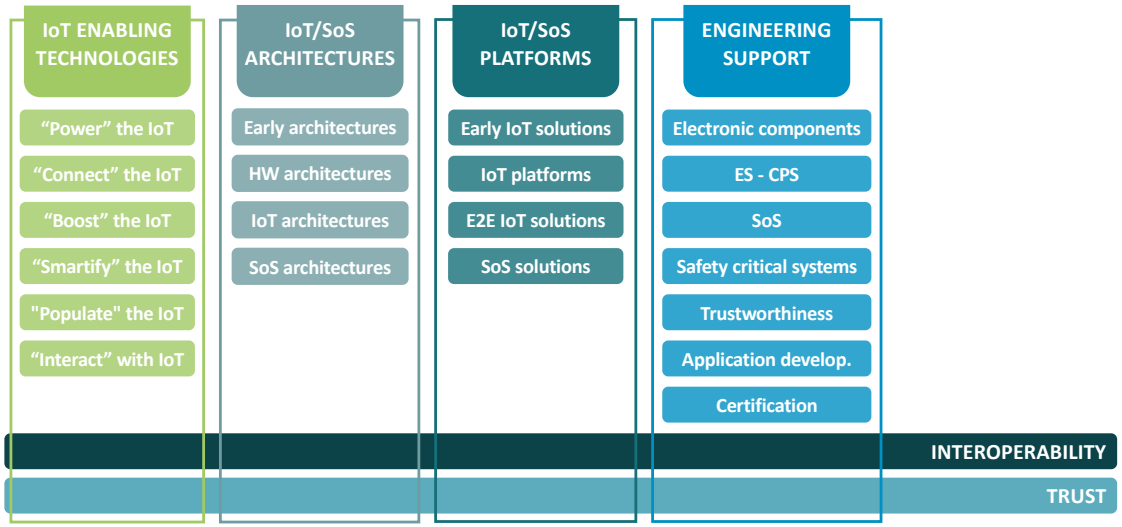


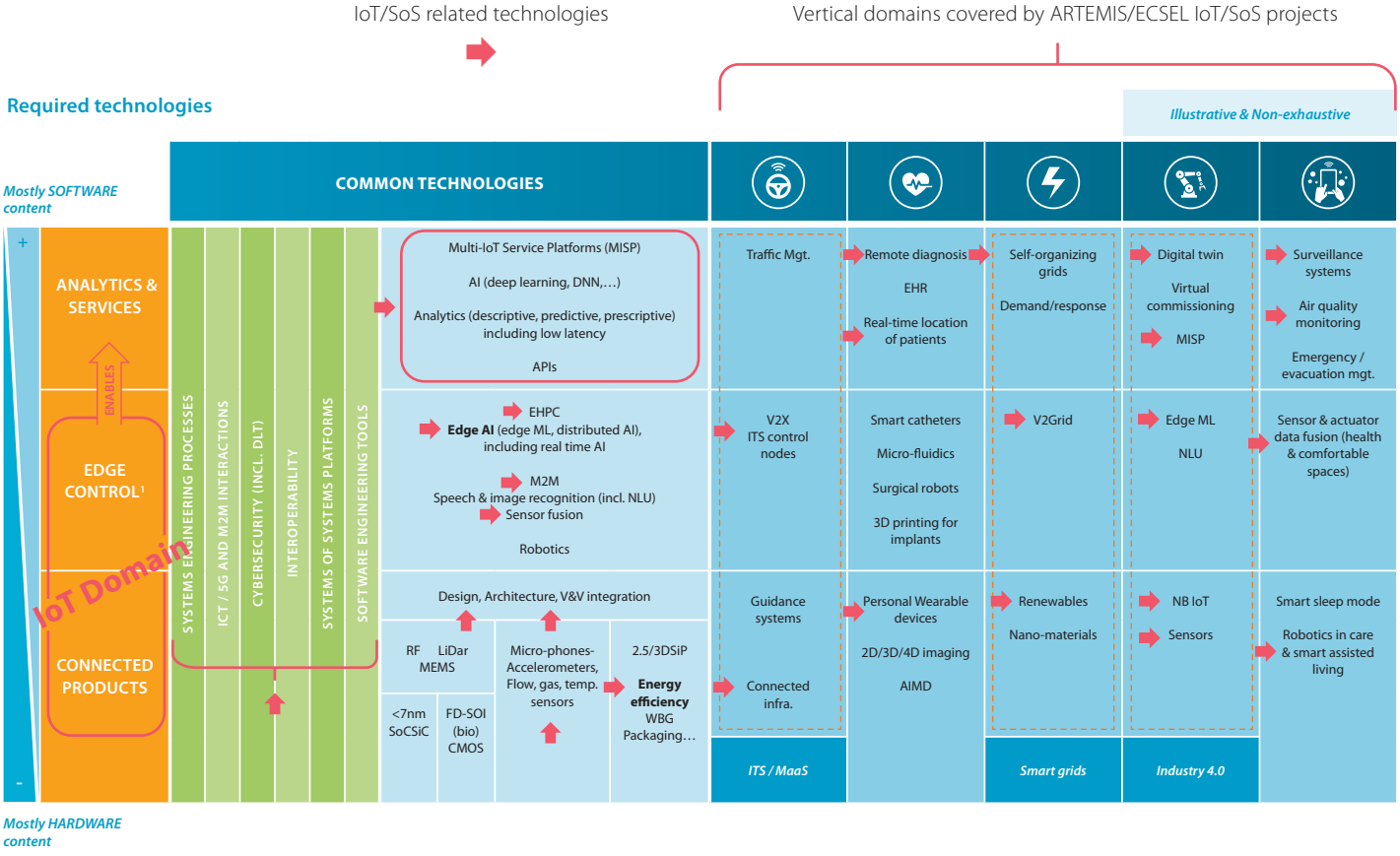
FIGURE 13 — *Detailed summary of IoT/SoS primary and cross research streams.*

The analysis of the research streams also highlighted that:

- in the last calls the concept of "digital transformation support" and "life cycle support" appear very frequently, demonstrating that the IoT proposed solutions are getting more mature and complete in terms of requirements coverage and available functionalities.
- Similarly, the solutions oriented to the management of SoS appear more frequently in the last calls.
- The most important projects for the research streams cover all the aspect of IoT, introducing reference designs and architectures, addressing connectivity, providing platforms/frameworks/middleware to manage the IoT infrastructure and provide design methods and tools. These projects intend to implement end-to-end solutions, specifically in the last calls.
- Projects focused on reference designs and architectures very frequently provide also solutions for software development and frameworks for the management of the new design and architectures.

The research streams address technological topics that have been considered strategic in the ECSEL ECS Strategic Research Agenda (SRA), a tool to implement the industry-driven, long-term vision of the ECS ecosystem. The document aims at promoting the digital transformation by developing technologies and solutions in the domain of electronic components and systems and, focusing on strategic priorities, it is intended to align and coordinate the European research policies and match the allocation of programmes and resources to different technology and policy challenges.

The ECS SRA focuses on the entire ECS value chain, while this analysis is focused specifically on IoT and SoS, that is, on the largest "sub"-value chain in the ECS domain. Indeed, a vast majority of the technologies addressed in the ECS-SRA are either fundamental parts of IoT, or directly adopted in IoT (as well as in other domains) or indirectly linked to IoT. Starting from the ECS SRA, the Advancy report identified the new technologies that are expected to affect all the stages of the ECS value chain (Figure 14): in the figure, technologies are positioned according to their role in the ECS architecture, according to their nature (technologies belonging to the physical world, to the digital world or positioned at the boundary/overlap between them) and considering the final application in which the technologies are adopted.



[1] An edge control is any piece of hardware that controls data flow at the between the CPS and the network. Serving as network entry (or exit) points : transmission, routing, processing, monitoring, filtering, translation, computing and storage of data.

Source: ECS SRA, Advancy research & analysis

FIGURE 14 — *IoT positioning in the ECS wider domain.*

Starting from this mapping, it is possible to highlight the technologies, directly or indirectly, related to IoT and SoS (see red arrows), clearly visualising the central positioning of IoT and SoS in the ECS domain. IoT is entirely based on connected products and it is the main enabling technology for edge control. Hence, remotely controllable products generate the data stream that is the primary food for analytics and services. Moreover, the six common technologies marked in green are widely overlapped with the research streams of ARTEMIS and ECSEL project focused on IoT/SoS that have been identified in this analysis. Eventually, the research streams (red arrows) demonstrate the high level of coverage of the ECS value chain by IoT and SoS, both in terms of single technologies and considering their adoption in the vertical domains.

IoT/SoS Project Lines

The classification of IoT/SoS projects based on their topics allowed the identification of the research streams and understanding of the relationship between the projects. It emerged clearly that many of the projects were following their own objectives, but also considered these objectives in a wider perspective, following a wider vision, across technologies, consortia and calls for proposals. Indeed, it has been possible to identify **project lines** that are composed of groups of projects approved in different calls for proposals, having a "forefather" and being coherent in terms of research area, macro-objectives and technologies. Typically, the forefather project focuses on a specific research topic, investigating it for the first time, studying and developing new technologies, and proposing a first solution, frequently in the form of a technology demonstrator. Subsequently, the project follow-ups focus on the same research topics and, starting from the results of the previous projects, extend and enhance the previous solutions and improve the TRL, frequently applying them to specific vertical domains and larger pilots. The annual SRAs certainly contributed to the existence of project lines because they promote the coherence of topics in time and drive the research activities ensuring continuity in the long term.

The existence of project lines that started in the first call and are still currently active highlights important qualities of the research carried out by the ARTEMIS/ECSEL community in the last decade. Project lines:

- started from visionary ideas that are still extremely relevant today,
- are focused on macro-objectives that were and are significant for IoT and SoS,
- ensure research continuity in terms of focus areas, major objectives and technologies,
- are associated with an improvement of the TRL level in time,
- demonstrate the maturity of the community that looks beyond the lifetime of a single project,
- indicate that investments have been targeted correctly.

Starting from 2009, the analysis highlighted that 20 of the 58 projects related to IoT/SoS form five different project lines, two of which are currently active. It is relatively complex to identify the relationships between different projects; therefore, the results of the analysis are not exhaustive and certainly represent a conservative estimate. Figure 15 illustrates the five project lines.

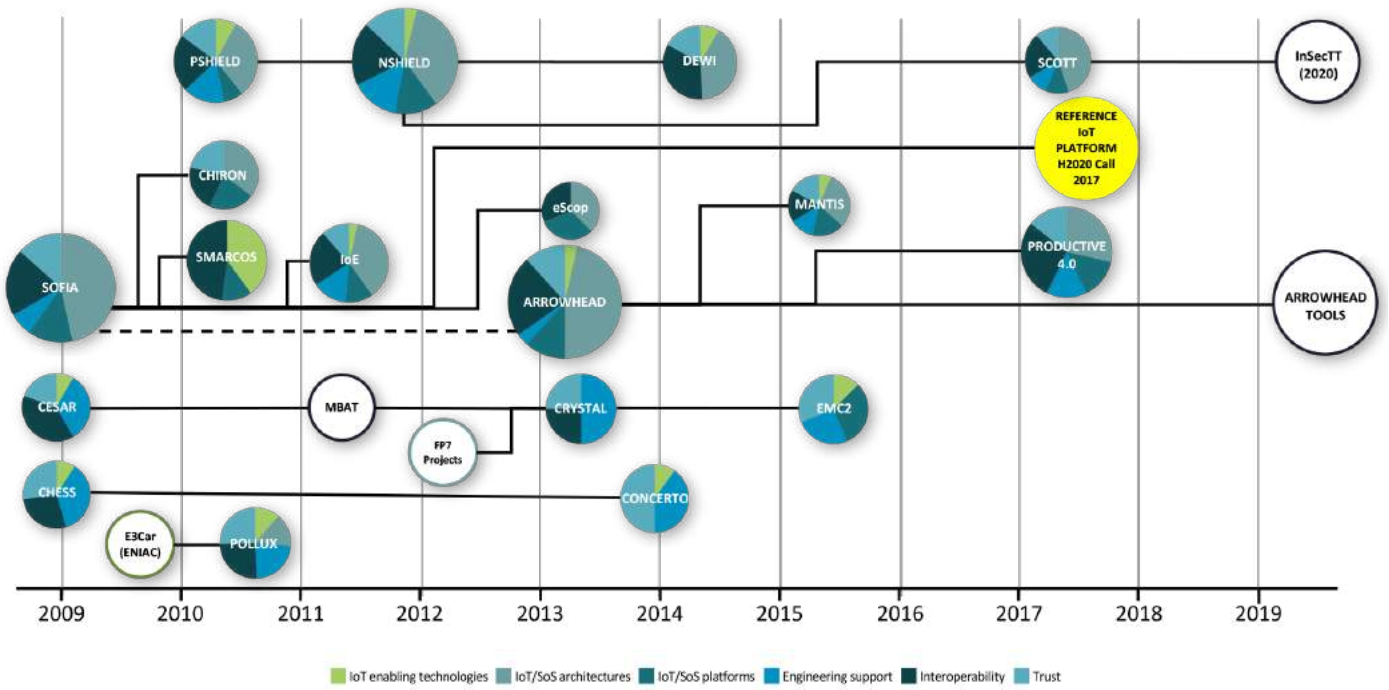


FIGURE 15 — *IoT/SoS ARTEMIS and ECSEL project lines.*

Two of the identified project lines deserve to be mentioned because they influenced the entire evolution of IoT and SoS projects at European level: SOFIA and Shield (p and nSHIELD).

SOFIA largely anticipated the general concept of IoT, introducing a semantic-based solution to manage smart objects deployed in a smart space. The concept of smart object was central to the project and was considered the main building block of a smart space, which can be considered a precursor of the wider concept of IoT. For SOFIA, the value of data was already very clear and, more importantly, the idea that data could generate knowledge and revenues was one of the primary drivers of the project. The project defined an architecture to structure and organise a smart space and implemented a semantic platform conceived to collect data from the smart space, control the smart space and the smart objects composing it, generate knowledge from data and simplify the development of application built on data and knowledge. With SOFIA, the ARTEMIS community addressed all the research streams from the first call, and a long crucial project line started. In 2017, SOFIA was mentioned as a reference platform for IoT in the H2020 IoT-03-2017 call for proposals. Some project follow-ups focused on specific vertical markets, such as Chiron and IoE, while other projects established important milestones for the development of the original concepts of SOFIA to higher TRL levels, such as Arrowhead, Productive 4.0 and recently Arrowhead Tools, where the concepts of SOFIA have evolved in a SOA IoT platform (the Arrowhead Framework[29]) and the focus is on the engineering support across the entire lifecycle of the platform. In 2020, the Arrowhead Framework will become an Eclipse[30] IoT open source project.

[29] *Delsing J., IoT Automation - Arrowhead Framework, CRC Press 2017, ISBN 9781498756754*
[30] *Eclipse Foundation, IoT Working Group, https://iot.eclipse.org/*

The ARTEMIS/ECSEL community has always been characterised by a sensitivity to trust and this topic has been addressed in almost every project at different levels, with different interests and criticality levels, investigating different technologies, different approaches and proposing different solutions: in the case of Shield the research activities found a long continuity and developed in a project line. Shield[31] project line addressed the concept of trust in IoT as a built-in feature rather than an add-on. pSHIELD and nSHIELD were specifically focused on security, privacy and dependability, a subset of trustworthiness, but they were already building on the idea that trust must be a core element of an IoT solution, a requirement possibly satisfied by design and, when not possible (e.g. when legacy system must become part of IoT), supported natively by the IoT platform. nSHIELD developed a general architectural framework and common metrics to ensure modular, composable and expandable security, privacy and dependability. The project follow-ups DEWI and SCOTT have been more focused on the evolution of these concepts when applied to specific vertical applications, such as the management of secure connected facilities, secure cloud services for mobility, trustable wireless in-vehicle communication, secure car access, secure wireless avionics, safe freight and traffic management, etc.

[31] *Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems: The SHIELD Methodology, Andrea Fiaschetti, Josef Noll, Paolo Azzoni, and Roberto Uribeetxeberria, CRC Press, December 22, 2017, ISBN 9781138042759*

Enabling technologies for IoT and SoS

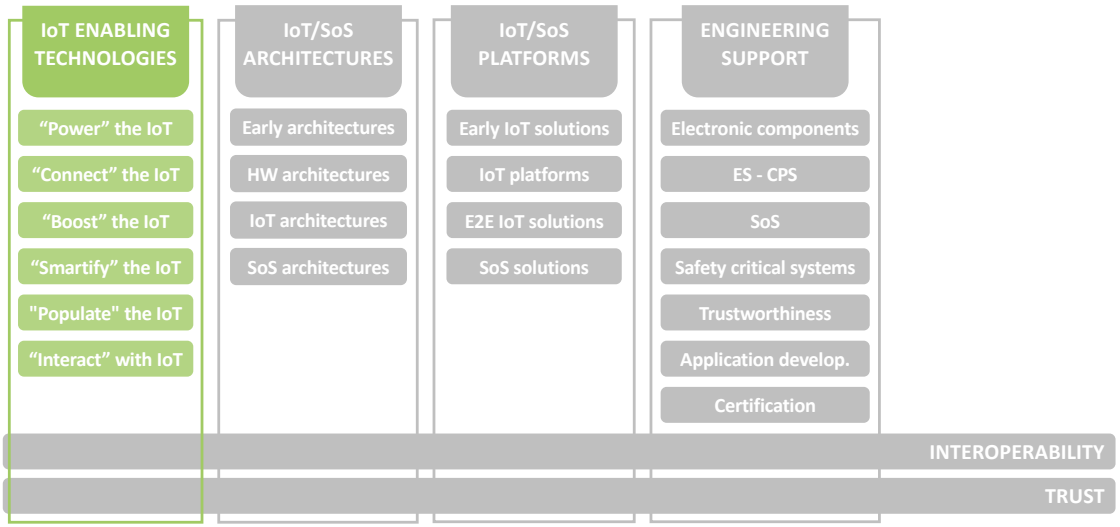


FIGURE 16 — *IoT Enabling Technologies research stream.*

IoT cannot be considered a single technology, having an inherently interdisciplinary nature based on a mixture of technologies that find their roots in both hardware and software domains. IoT is rather a solution resulting from the integration of the hardware and software technologies, adopted to retrieve, store, process data, and of the communication technologies, which ensure the flow of information between the various parts composing the IoT infrastructure, including the enterprise level. These four functionalities – retrieve, store, process and share information – appear apparently very simple but hide a large set of heterogeneous and interdisciplinary domains of science, technology and engineering.

Just to mention a few examples, retrieving data requires advanced semiconductor technologies that allow the creation of low-power sensors, able to interface with multiservice IoT gateways or to autonomously connect to an enterprise-level platform, that will process the collected information. Storing information on the edge requires the ability to efficiently manage time series of data collected from the environment, finding a good compromise between the limited resources of the embedded systems in which the information will be stored, their real-time capabilities and the right amount of information required by the specific business application. Processing data on the edge is really becoming a challenge, driven by opposite trends in terms of available computing power, energy consumed and offered functionalities, a challenge that can only be overcome with the interdisciplinary contributions from micro/nanoelectronics, low power hardware and software technologies, efficient and intelligent software for data processing. And finally, IoT connectivity, which requires the support of a rich set of heterogeneous field

protocols to ensure the integration of sensors, actuators and legacy systems, as well as the support of secure WAN communications required by data collection, machine-to-machine interactions, command and control of the IoT infrastructure, etc.

Even without considering transversal aspects like security, privacy, dependability, interoperability, autonomy, …, domain specific requirements, standards, … architectural and engineering aspects … the previous simple examples give a clear idea of the multidimensional complexity of IoT.

Each single technology is clearly not enough to create an IoT solution but, in this complex puzzle, it becomes a fundamental tile that composes the whole picture, that is an **enabling technology.** Single enabling technologies allow the implementation of specific IoT features/functionalities: e.g. self-adaptation and configuration are specifically conceived to allow a device to react autonomously to changes in the context – they solve a specific issue. Further examples of IoT enabling technologies include: electronic components, hardware platforms, sensing and actuation, identification and recognition, positioning technologies, low power and energy storage solutions, communication technologies, software framework for edge computing, virtualisation, cloud platforms, embedded intelligence, data processing solutions, security mechanisms, etc. (see Figure 17).

But the integration of multiple enabling technologies allows the convergence of the IoT evolution process to a final end-to-end solution. E.g. multicore technologies depend on the properties and capabilities of materials, low-power technologies, process technologies that, combined with design methods, tools and APIs availability, allow the development and execution of complex and potentially power-consuming algorithms on low-power devices, that become the real smart nodes of the IoT infrastructure.

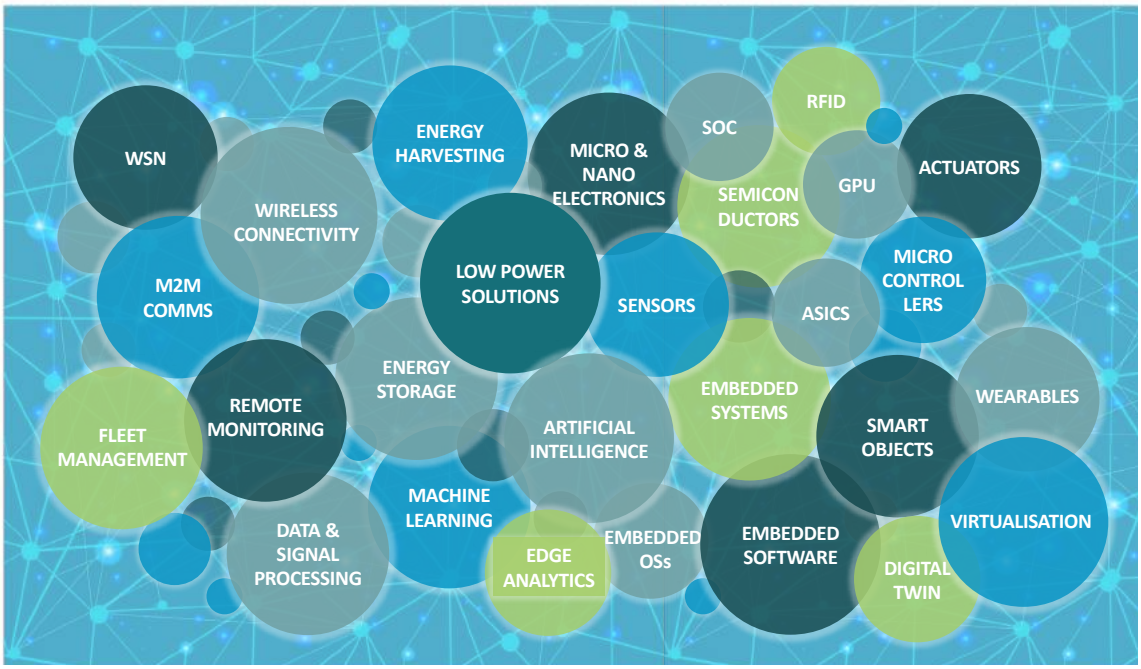


FIGURE 17 — *The landscape of IoT enabling technologies.*

Enabling technologies lay the foundations of IoT solutions and allow one to focus the scientific and industrial research on specific aspects of IoT, on the evaluation of technologies in an early stage of development, on the elaboration of new innovative ideas and their evaluation through technology demonstrators. The study of enabling technologies

started in the first ARTEMIS call and generated important anticipations, creating milestones that influenced the future evolution of IoT and set the initial point for entire project lines. In this research stream, the community started investigating the main challenges of IoT and SoS, including:

- manage complexity and heterogeneity;
- improve autonomy (power, connectivity, embedded intelligence);
- solve interoperability and integration issues;
- ensure security, privacy and dependability;
- ensure reliability and availability;
- QoS and scalability;
- processing and intelligence capabilities;
- sensing and actuation;
- promote cross-domain reusability;
- etc.

This research stream is not chronologically linked with the ARTEMIS/ECSEL annual calls, as demonstrated by many recent projects that addressed IoT enabling technologies and will certainly also be present in future projects due to the continuous evolution of technologies and to their progressive adoption in IoT/SoS solutions.
In the "IoT Enabling Technology" research stream six focus areas have been developed, depending on the specific technology issue they intend to address:

- "Power" the IoT,
- "Connect" the IoT,
- "Boost" the IoT,
- "Smartify" the IoT,
- "Populate" the IoT,
- "Interact" with IoT.

The contribution of ARTEMIS/ECSEL projects to the six focus areas is depicted in Figure 18.

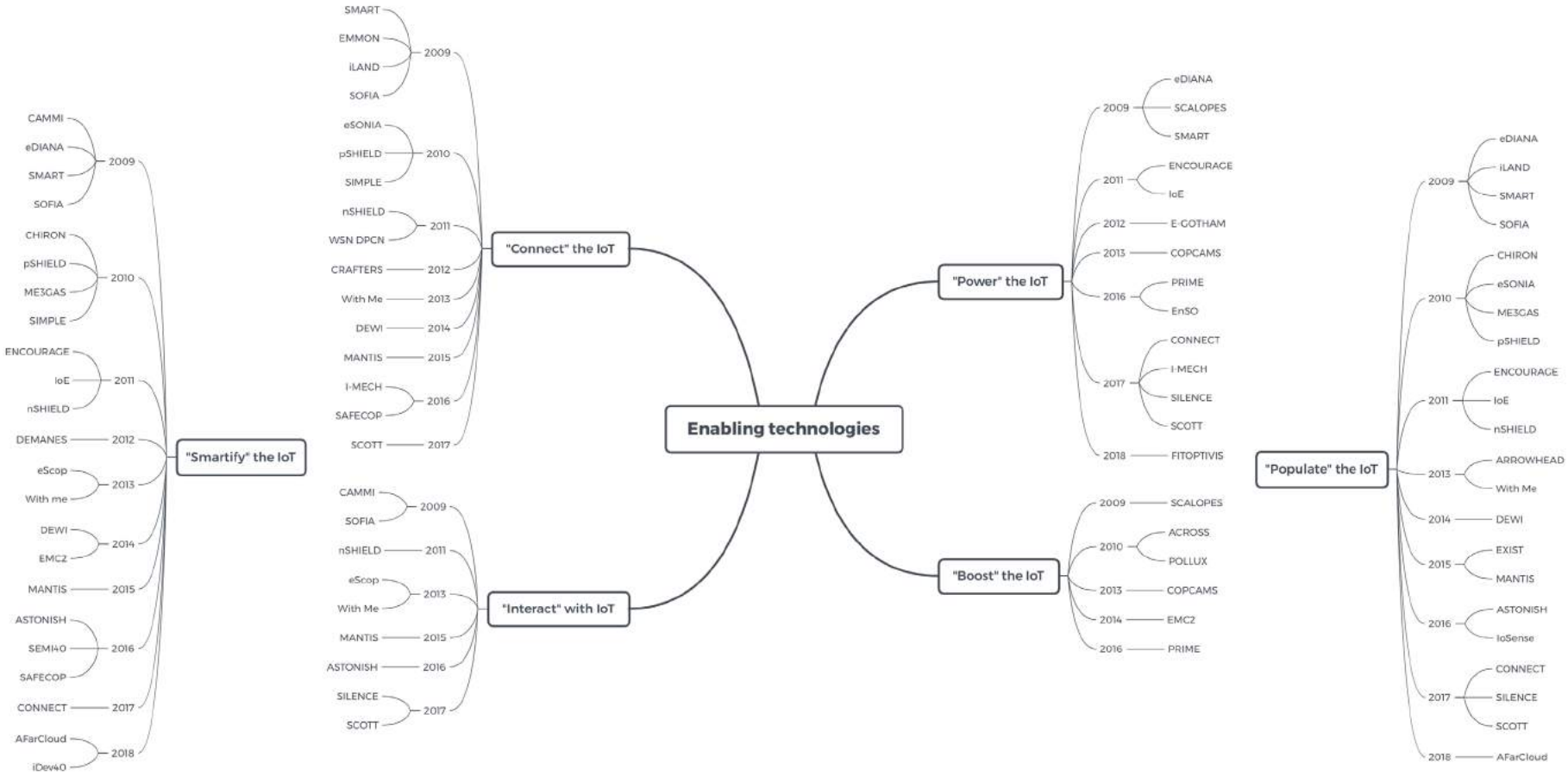


FIGURE 18 — *ARTEMIS/ECSEL projects that contributed to IoT Enabling Technologies, by research focus area and call.*

"Power" the IoT

The pervasive nature of IoT generates *power consumption constraints* with a significant impact on the autonomy, diffusion and sustainability of IoT. The IoT physical infrastructure is composed of devices and sensors that in many cases will function entirely on batteries. In many IoT applications, where batteries are difficult or even impossible to recharge or to change, the solution adopted to power the device/sensor limits its functionalities, impacts on the maintenance costs, influences the business model and the sustainability or even the overall feasibility of the IoT application.

According to a recent study from Juniper Research, the growth trend of service revenues from low-power IoT technologies will reach 800% over the next five years and will exceed USD2.6 billion by 2024[32].

In this focus area, the research activities in ARTEMIS/ECSEL projects have been oriented to:

- Reduce/optimise the power consumption of the electronic components adopted to manufacture the *things* composing IoT (electronic components, sensors, actuators, multicore CPUs, SoC, …).
- Reduce/optimise the power consumption of the *things* composing IoT, at the embedded or cyber-physical level.
- Improve the autonomy of *things* in terms of energy, adopting energy harvesting and storage solutions that benefit both from hardware and software technologies.
- Enabling IoT and SoS level power monitoring and optimization:
  - E.g. a new sensor conceived to measure energy consumption of appliances, enables the possibility monitor and control the appliances in the entire home.
  - E.g. a smart object that autonomously provides information about energy consumption, enables the creation of an energy monitoring and optimisation service at IoT level.

The reduction and optimisation of the power consumption of the electronic components, sensors, actuator, multicore, system on chip, etc. that are used to produce an IoT device has been addressed both from the perspective of *single low-power technologies, in terms of complete hardware platforms and also considering the manufacturing process*.

In the domain of **low-power electronic components**, CONNECT developed *high efficiency, low-cost, low-weight, compact high-power density converters with embedded communication capabilities*. The converters can be adopted in different application levels of the electrical grid, allowing bidirectional power exchange with the grid and supporting the extended integration of local storage and renewables, such as photovoltaic. The solution also enables smart energy management. I-MECH developed a *low-power solution for smart sensors*, trying to facilitate the reliable inclusion of wireless sensors in real-time feedback control, ensuring the reliability of the wireless data, low-energy consumption of the wireless nodes and high update rates / low latency. PRIME developed an *ultra-low power solution for a System on Chip and System in Package memory banks and processing implementations for IoT sensor nodes*. This solution has been conceived for IoT applications in the medical, agricultural, domestic and security domains. SILENSE developed *low-cost and low-power micro-acoustic transducers* and the related IC design with improved performances (e.g. directivity, fractional bandwidth, dynamic range, frequency range, sensitivity and efficiency…) that can be exploited in IoT applications.

[32] *Low Power IoT, Impact Analysis, Vertical Assessment & Forecasts 2019-2024, Juniper Research, 2019.*

Several **hardware platforms oriented to low-power solutions** have been proposed. The open Ultra Low Power (ULP) Technology Platform developed by PRIME contains all the necessary design and architecture blocks and components needed to support the supply of products for the IoT. The platform is oriented to provide a high-performance, energy-efficient and cost-effective solution for IoT hardware. The COPCAMS platform focused on more efficient usage of the silicon area, on improved performance to sustain complex vision analytics and video encoding functions, but with attention to power consumption, thanks to the reduced area of processors and aggressive power management. COPCAMS also developed open and standard APIs to simplify application development.

The **reduction and optimisation of the power consumption** has also been addressed from an **holistic point of view**: SCALOPES tried to identify an industrially sustainable path for the evolution of low-power, multicore computing platforms, providing solutions for energy and resource management, low-energy design methods and associated runtime methods as well as standard interfaces (API) between hardware and low-level software. This approach provides energy awareness at the upper layer of the IoT stack.

From the **manufacturing perspective**, ASAM focused on the automation of the construction of the SoC and processor designs through an advanced design-space exploration, including the combined macro- and micro- architecture exploration necessary for SoCs based on adaptable ASIPs. Starting from the actual constraints of modern SoC design (power, performance and area), the architecture of the SoC, its interface and memory structures are automatically instantiated or customised. The design space exploration includes also aspects like parallelization, partitioning, scheduling and mapping, needed to deliver applications running efficiently on heterogeneous multi-processor platforms. In the context of the Ultra Low Power (ULP) Technology Platform, PRIME developed *22nm FDSOI low-power technologies with logic, analogue, RF and embedded new memory components* (STT RAM and RRAM), together with innovative design and system architecture solutions (providing a flexible design ecosystem), used to build macros and demonstrate the functionality and power reduction advantage of new IoT device components. Finally, SILENSE also developed the package and assembly technology for low-power micro-acoustic transducers.

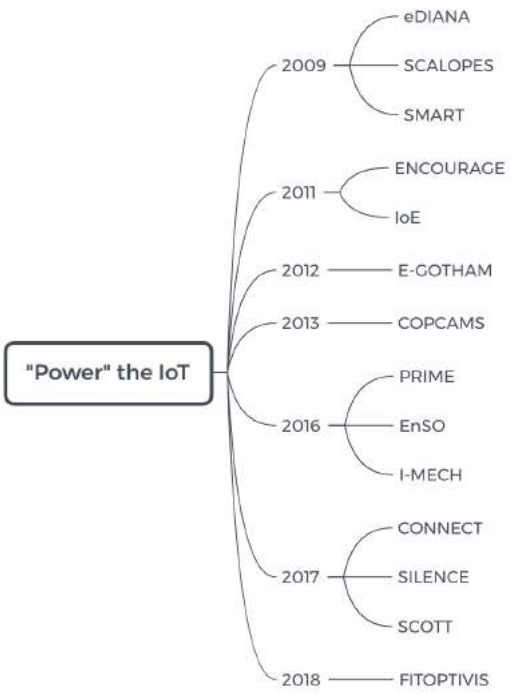


FIGURE 19 — *ARTEMIS/ECSEL projects that contributed to energy related technologies by call.*

The future of a power-aware and power-autonomous IoT will be driven by new technologies that will affect all the levels of the IoT infrastructure, including:

- New materials and electronic components oriented to low power solutions.
- 3D-based device scaling for low energy consumption.
- Strategies for self-powering nodes/systems.
- Physical integration at system level, targeting energy autonomy.
- Low and ultra-low power communications.
- Ultra-low power computing and storage, network, sensing, actuation and power management functionalities.
- Policies and operational algorithms intended to reduce the power consumption at IoT/SoS level.

"Connect" the IoT

Digitalisation and connectivity are the two drivers of the historical change in the structure of the current economic system, *from a linear value chain to a non-linear value network*, where every "connection" between two stakeholders could potentially generate a new business opportunity.

Investing in research and engineering activities focused on communication technologies is fundamental for the evolution of IoT because connectivity determines the existence of IoT itself. And considering the current growth rate that cannot be supported properly by the legacy communication infrastructures, the necessity of new efficient, secure and scalable connectivity solutions is becoming a key factor: according to McKinsey[33], more than 100 new devices are connecting to the internet every second. With a similar trend, new challenges will rapidly emerge because the existing connectivity solutions are not conceived to support real-time communication of high-volume, latency-sensitive and bandwidth-demanding information that also have to respects an application-specific quality of service: the new solutions will face an avalanche of data generated by IoT but also ensure the control and management of large ecosystems of connected devices.

The future of IoT is entirely wireless and, to a large extent, mobile but the connectivity landscape in this sector is still very uncertain and rapidly evolving. According to Ericsson[34], the number of cellular IoT connections is projected to reach 5 billion by 2025 and the number of all types of wireless IoT connections to reach almost 25 billion by 2025. Even though 5G and Wi-Fi 6 standards have been almost completely defined, the related networks are still not available, either for the consumer and or the industrial markets. Many local pilots have been set up, but real-world deployments of an infrastructure and of enabled devices, as required by large-scale IoT application, will reach critical mass only in 3-4 years. According to Ericsson[35], 5G has the potential to cover up to 65 percent of the world's population only by 2025. The diffusion of 5G has been recently negatively affected by the inclusion of Huawei in the US government's companies blacklist: although other countries (including the European area, where Huawei investments are rapidly shifting) has not adopted the same decision, this international case is influencing 5G rollout.

[33] *What's new with the Internet of Things?, McKinsey & Company, May 2017*
[34] *IoT connections outlook, Ericsson, November 2019*
[35] *Ericsson Mobility Report, November 2019*

It is evident that there isn't a single form of network and data technology that satisfies the requirements of all IoT vertical applications. *Connecting billions of devices will probably require hybrid solutions, representing a vertically-driven trade-off between different networking technologies, with embedded intelligence to optimally exploit the network capabilities, network function virtualisation and software-defined solutions to make the overall connectivity solution more flexible, available, faster and smarter.*

Satellite-based communication, especially nano-satellite services, represents a complementary approach to connectivity that is reaching a hype and aims to provide ubiquitous connectivity even in very remote areas. In November 2019, Eutelsat, in partnership with Sigfox, announced that it would launch 25 satellites to serve specifically the IoT market across 65 countries. In February 2019, Fleet Space reported that 1 million devices were registered to be connected just 24 hours after launching its Lora-based satellite network called "Project Galaxy". In April 2019, Amazon announced a plan to launch a constellation of 3,236 satellites into low Earth orbit to provide internet connectivity in uncovered areas. Similarly, SpaceX has plans to launch 12,000 satellites as part of its Starlink constellation, OneWeb wants to launch 650 satellites, and Facebook is also developing an internet satellite programme.

IoT connectivity protocols will also play an important role because the choice of the networking protocol impacts the design of the connected products and the entire IoT infrastructure of which they are part. Many factors have driven the research activities, trying to provide a rich set of possible solutions for an heterogenous set of IoT vertical applications: the connectivity range, the available bandwidth, the interoperability level, the data rate, the security level, the power consumption and the scalability.

From the connectivity perspective, the ARTEMIS/ECSEL research projects tried to lay the foundations of future IoT/SoS integration platform, taking account of the low-power requirements of IoT, focusing from the first projects on wireless and mobile communications and keeping always in mind the infrastructural and system level dimensions of IoT:

- Enable remote control on *things*, fundamental for the management of the entire IoT infrastructure, and of the vertical application.
- Low-power communications.
- Wireless solutions scalability.
- Improve trust in wireless communication.
- Wireless communication support in IoT platforms and solutions.
- Wireless Sensor Networks (WSN):
  - simplification of WSN adoption;
  - improve the integration of heterogeneous wireless devices and of different WSN;
  - wireless sensor networks conceived for specific vertical domain.
- Non-standard communications (e.g. smart grid inclusion).

Although connectivity is largely seen as a *commodity*, a de facto available asset, it remains a relevant topic for research because of its role in IoT/SoS and because of the challenges it still presents in terms of security, scalability, interoperability, etc.

Apart from the obvious role it plays for data collection and delivery, connectivity is a key factor for enabling **remote control and the related added-value functionalities and services**. The simplest approach is to start from traditional devices, such as a gas, water or electricity meter, and design new smart objects provided with sensors, actuators and connectivity, enabling their remote management. ME^{3}GAS, for example, developed *a smart gas meter* based on

embedded electronics, an electric shut-off valve and connectivity, enabling remote management features that can be used to create intelligent services, including management of multiple tariffs and payment modalities, remote gas cut-off, security alarms, etc. Another completely different example is I-MECH, which tried to facilitate the reliable inclusion of *wirelessly connected sensors* in the real-time industrial feedback control, allowing the possibility to improve the reliability and the efficiency of industrial processes by remote control.

Research has been focused for a long time on **Wireless Sensor Networks** (WSN) and many ARTEMIS and ECSEL projects have investigated the potentialities of this technology for application in specific vertical domains. In the context of smart buildings and home automation, SOFIA tried to improve the *automation of large buildings* with a WSN that collects the main environmental information needed by a cooperative system that integrates the HVAC system, the lighting system and the maintenance activities. SIMPLE and ME^{3}GAS focused more on *home automation*, with respectively a cross-domain self-organising WSN able to integrate also smart tags and a new generation of smart gas meters. In the smart factory domain, SIMPLE's WSN solution was adopted to overcome the current difficulties of *monitoring the state of shipments* in large groups of companies and, more generally, of tracing goods along the whole supply chain (manufacturing, logistics, consumption). eSonia proposed a solution to improve the *predictability of plant behaviour* and visibility by realising the asset-aware plant, while I-MECH developed a WSN intended to facilitate the inclusion of this technology in an industrial environment and offering low energy consumption, high update rates / low latency and reliability of transmitted data. pSHIELD and nSHIELD focused on the transportation domain, providing a *WSN-based solution for safety and security* intended for tracking carriage transporting hazardous materials. SCOTT adopted WSN to provide new wireless communications capabilities to the *on-track infrastructure and of the onboard equipment of trains*. And eventually, in the healthcare domain, CHIRON adopted WSN technologies to build patient-centric and continuous healthcare at home, in the hospital and in nomadic environments, while With Me proposed a similar solution more focused on well-being.

However, the diffusion of *WSN has been limited by many factors* that prevented their massive distribution, including the absence of a standard and the heterogeneity of the available WSN, the difficulties in their adaptation and integration, installation, maintenance and usage. To address these issues, WSN-DPCM developed a full platform composed of a middleware for heterogeneous wireless technologies and an integrated engineering toolset for development, planning, commissioning and maintenance activities for expert and non-expert users. While SIMPLE focused on the dynamic inter-working of ultra-heterogeneous sensors and tags able to autonomously organise in hierarchies and thereby simplify the integration of heterogenous WSNs. The same topic was studied in DEWI that developed a solution for smart composability and integration of WSNs.

The *inclusion of WSNs* in wider IoT ecosystems has been addressed by many projects, mainly providing native WSN support in IoT middleware and platforms by means of seamless connectivity: SOFIA, Arrowhead, CRAFTERS, e-GOTHAM, SMARCOS, IoE, Productive 4.0, etc. EMMON also addressed the *scalability issues* that could arise in real IoT deployment: the project developed and tested a simulation tool and a functional prototype for large-scale wireless sensor networks, with the aim of increasing tenfold the number of devices deployable in a common WSN.

In similar large IoT deployments, the presence of wireless communications is already predominant, and, with 5G connectivity, it will certainly increase, exposing the IoT infrastructure and the related applications to unprecedented security risks. **Trust in wireless communications** has been considered a central research topic for many projects: DEWI, MANTIS, SAFECOP, SCOTT, etc. DEWI provided a *secure solution for wireless seamless connectivity and interoperability* in smart cities and infrastructures: locally adaptable wireless "sensor & communication bubble" ensure locally confined wireless internal and external access, secure and dependable wireless communication and safe operation, fast, easy and stress-free access to smart environments flexible self-organisation, re-configuration, resilience, adaptability and interoperability. SAFECOP targeted cooperating CPS, that is systems that rely on wireless communication, have multiple stakeholders, use dynamic system definitions and operate in unpredictable environments: in this context, the project developed a runtime manager to detect abnormal behaviours at runtime,

triggering, if needed, a safe degraded mode. SCOTT tried to create *trust in wireless solutions and increase their social acceptance*, a limiting factor that is preventing the full potential of IoT from being unleashed. The project provided a comprehensive cost-efficient solution for wireless, end-to-end secure, trustworthy connectivity and interoperability to bridge the last mile to market implementation. The solution was applied to several industrial domains including building and home / smart infrastructure, automotive, aeronautics, rail and healthcare.

Particular attention has been devoted to the **connectivity in the vertical domain of energy**, focusing on electro-mobility, the smart grid and microgrid. IoE proposed innovative solutions for interfacing the Internet with the power grid, with potential applications in the areas of electric mobility, contributing to making transport more sustainable, efficient, clean, safe and seamless. IoE promoted the development of the future electric grid by using data communication to move electricity more efficiently, reliably and affordably and the development of the future Internet by using the electric grid to facilitate and speed-up the communication amongst the various energy nodes and domains. e-GOTHAM designed an open reference architecture and develop a middleware with seamless connectivity that provides the communications and decision support tools needed to optimize and manage microgrids in the residential, services and industrial sectors. CONNECT develop solutions for high-interoperable, high-data rate for local and wide area communication in the grid with enhanced security in order to protect this critical infrastructure against attacks.

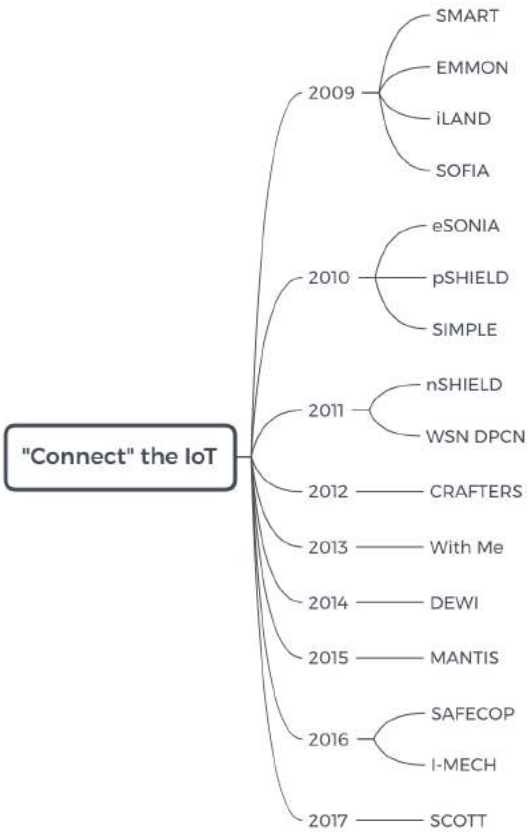


FIGURE 20 — *ARTEMIS/ECSEL projects that contributed to connectivity related technologies by call.*

Connectivity is really a challenging sector, in continuous evolution, with pressing demand from new technologies and a significant potential impact on IoT application feasibility and business model sustainability. The ECSEL community will have to widen the scope of the research activities, including:

- Low-Power Wide Area Networks (e.g. LoRa and LoRaWAN systems).
- Provide effective solutions for 5G network infrastructure and enabled devices, from IoT to backend (HW, control, envelope tracking, system integration, …).
- Define the requirements for 6G and beyond.
- Provide solutions to move towards Wi-Fi 6 and Bluetooth 5.
- Investigate new connectivity medium.
- Intelligent connectivity switching.
- Machine-to-machine software technologies that extend intelligence at IoT/SoS level.
- IoT applications with a high degree of distribution and processing at the edge of the network, and networking services between edge devices and computing data centres.
- SoS connectivity architectures and frameworks.

"Boost" the IoT

The digitalisation process enables a massive flow of information from the digitised environments to the cloud platforms or to the enterprise software, where big data processing and analytics take place. Unfortunately, *this avalanche of data is already and will continue to be difficult to process with the computing power available in the cloud or in classical data centres, with the collected data very soon becoming too slow to process in real time*. Moreover, with the traditional centralised approach to data processing, digitalisation could become unsustainable due the *costs for transmitting and storing a huge amount of raw data* in which, for the large majority of vertical applications, only a small subset of transmitted information is meaningful for the final application or service. A similar approach would also be extremely expensive in terms of energy required for the useless transmission of the data, with an *unsustainable impact on the environment*.

A significantly more sustainable and efficient solution is represented by *edge computing* that consists of selectively shifting the data processing from the enterprise to the intermediate node of the IoT infrastructure or, preferably, directly to the edge of IoT. With this approach, the *things* at the edge of IoT become richer in terms of functionalities, more performant, able to adapt to the context, to elaborate information and take decisions, to cooperate and, more in general, become computationally autonomous and independent.

> *Edge computing and high-speed connectivity, combined with artificial intelligence and machine learning, will allow enterprises to sustainably support IoT applications, learning from the collected data, dynamically adapting and changing their internal process with a positive impact on their business and on the related ROI.*

In addition, a strong motivation to provide real-time analytics and faster decision-making on IoT devices (or near to them) is represented by the increasing number of companies that are starting to use IoT-based solutions also for the management of mission-critical, latency-sensitive or industrial applications (see e.g. autonomous cars).

Edge computing requires enabling technologies to "boost" the processing power of sensors, edge controllers, embedded control units, multiservice gateways etc. at the edge of IoT. Multicore technologies, for example, are rapidly developing the parallel computing environments whose improved performance, energy and cost characteristics will allow the effective and adaptive processing of information on the edge. With this technology, splitting the workload on low-frequency simple cores (instead of a single high-frequency and energy-consuming CPU) allows to increase the parallelism of computation, preserving a low-power budget. Multicore technologies play a strategic role in the markets of *high performance embedded systems, CPS and IoT*.

Many ARTEMIS and ECSEL projects focused on technologies aimed to improve the capabilities of edge computing, contributing to shift the centre of gravity of data processing and analytics from the enterprise to the boundaries of the IoT infrastructure and of its nodes. The research and engineering activities tried to:

- Conceive new multicore technologies for the embedded systems of the IoT infrastructure.
- Provide new solutions for parallel computing.
- Increase the computing power of devices on the edge.
- Increase the independence of the devices from the rest of the IoT infrastructure and from the enterprise/cloud platforms.

The design of **new computing platforms** is the first step towards improving the processing capabilities and the computational autonomy of the nodes composing the IoT infrastructure. In this regard, SCALOPES focused on cross-domain technology and tool *developments for multicore architectures*, with particular attention on reaching a sustainable trade-off between computing power and energy consumption. The development was driven by the requirements of four different application domains and proven with specific demonstrators: communication infrastructure appliances, surveillance systems, smart mobile terminals, stationary video and entertainment systems. POLLUX aimed at the creation of a common architecture and design platform for *advanced multicore hardware and middleware solutions*, enabling the flexible and evolvable interoperation of systems (including sensors, actuators, energy storage and conversion devices, information systems and control systems across multiple domains). The architecture was adopted for the deployment of advanced electric vehicles and powertrain management algorithms and strategies. COPCAMS focused on a *many-core architecture*, provided with a flexible programming model, as a more effective solution to support the processing requirements of large scale IoT deployment, such as surveillance systems or perception/vision-based manufacturing control. The new solution resulted in lower costs because of more efficient use of the silicon area, more power in terms of processing power, less energy demand and easier programmability, thanks to the use of standard APIs. The solution has been adopted to power a new generation of vision-related smart cameras and gateways, providing better in-situ image/video analysis for the improvement of goods quality and productivity, specifically in large deployments characterised by reduced communication requirements, where the decisional autonomy of a device could be a relevant application requirement. A wider approach that also considers the *upper layers of the IoT stack*, has been followed in ACROSS, where a MPSoC-based framework for the component- based development of safety-related embedded systems was developed to support composability, robustness, integrated resource management, diagnosis and model-based development. The approach was domain-independent and offered an integrated solution, composed of IP cores, tools and a middleware, intended to reduce development costs and accelerate time to market, simplify the introduction of new cross-domain applications, enable the exploitation of the economies of scale in the semiconductor industry and give the end user more robust products.

The immediate positive effect of increasing the processing power in the nodes of the IoT infrastructure, especially on the edge, is the possibility to **execute more complex and demanding algorithms**, thereby improving the analytical and decisional autonomy of the nodes. All the projects mentioned indirectly contributed to this objective,

but COPCAMS is a particularly good example to this regard because it addressed the *autonomy of a demanding application*, such as image and video processing on the edge. A different approach was proposed in EMC^2, that focused on developing and evaluating *hardware techniques that enable multicore processors to execute applications with mixed criticalities*. The objective was to find solutions for dynamic adaptability in open systems, provide handling of mixed criticality applications under real-time conditions, scalability and utmost flexibility, full-scale deployment and management of integrated tool chains, through the entire lifecycle.

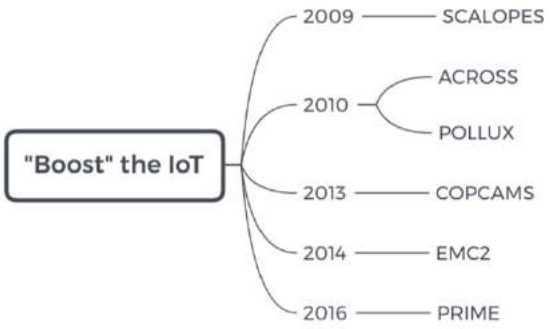


FIGURE 21 — *ARTEMIS/ECSEL projects that contributed to improve computing power on the edge by call.*

The increasing demand of processing capabilities on the edge will require the continuous evolution of embedded computing technologies that are currently focusing on:

- New solutions for integration and packaging of SoC, including 3D integration, chiplet technologies, smart System-in-Package (SiP), heterogeneous and hybrid SoC and sensors integration.
- Non-volatile memories that enable embedded AI processing. Near/in-memory computing.
- Embedded (or Edge) High-Performance Computing (EHPC), conceived to provide classical HPC processing capabilities of the edge, satisfying the energy constraints and the environmental requirements.
- Emerging computing technologies like neuromorphic and quantum computing.
- Bio-inspired computing.
- Solutions to enable new edge computing technologies, like cloudlets, micro data centres and cloud of things.

"Smartify" the IoT

Embedded intelligence is a key factor for IoT market penetration in many vertical domains and allows IoT to disappear in everyday life, offering functionalities and services seamlessly integrated with human activities. A large amount of effort in research projects is typically focused on data collection and on the management of the IoT infrastructure and its resources. Although these are the most popular topics, significantly enhancing the IoT capabilities, *extracting knowledge and reaching some level of awareness from the interaction with human and smart objects are becoming important enabling technologies.*

The concept of "smart object" has been investigated in research projects since the beginning of the ARTEMIS initiative, and for several years it has been a buzzword in the community. However, this enabling technology, that is intended to increase the decisional autonomy of the *things* of IoT, is still in its infancy, with concrete results only in specific areas of artificial intelligence. *Embedded intelligence allows smart objects to learn from experience, adjust and adapt according to new inputs and accomplish specific tasks without human intervention.*

> *Embedded intelligence allows IoT to evolve from simple data collection to a more valuable knowledge collection.*

Artificial intelligence has repeatedly failed under the weight of its own unrealistic expectations. Unfortunately, this negative heritage and the inherent limitations and constraints of IoT further increase the complexity of embedding intelligence in IoT. "Nevertheless, artificial intelligence has a big impact on computing and remains a fundamental enabling technology for the evolution of IoT: *embedded intelligence and IoT should be tightly connected to create new value for organisations across a large spectrum of vertical domains.* The ability of an intelligent IoT to "learn" from massive volumes of data and quickly take decisions on the edge makes AI an essential form of analytics for any organisation that has to expand or move the processing resources into the IoT infrastructure. Gartner estimates that by 2022, more than 80 percent of the enterprise IoT projects will rely on embedded intelligent components[36], while IoT Analytics estimates a growth of the industrial AI market size from USD11 billion of 2018 to USD72 billion by 2025, with a CAGR of the 31%[37].

Such enabling technologies as deep learning, computer vision, natural language processing and machine learning make embedded intelligence a complement of IoT. *Machine learning for edge devices* is currently a hot topic: it allows patterns to be identified and anomalies discovered in the information collected from smart sensors and devices, without being previously programmed to recognise them. *Neural engines* in modern smartphones accelerate machine learning algorithms, software frameworks for machine learning have been optimised for embedded devices (e.g. tensorflow-lite) and hardware accelerators for machine learning are becoming standard products (e.g. edge TPU). An energy-efficient machine learning solution running close to the data collection point ensures a substantial scaling of IoT, although the identification of the optimal place within an IoT infrastructure for running it remains a research challenge. In the long term, machine learning algorithms will be able to deliver more accurate results and make operational predictions many times faster and more accurately compared to traditional business intelligence solutions.

Embedded intelligence brings many benefits to IoT, including the capacity to:

- Filter and validate raw data collected from sensors.
- Analyse raw data on the fly.
- Monitor aggregated information, detect events and trigger the appropriate actions.
- Predict events, complex situation and trends in real-time.
- Optimise operation in real-time.
- Improve edge computing enabling high-performance stream analytics.
- Manage interactions and connectivity in real-time.
- Reduce the bandwidth required for IoT communications.
- Improve autoconfiguration, auto-calibration and adaptation of device and of the entire infrastructure.
- Enable active and adaptive cooperation between devices.
- Directly and indirectly improve security, privacy, dependability.

---

[36] *The Business Value of Artificial Intelligence Worldwide, 2017-2025, Gartner Inc. Forecast.*
[37] *Industrial AI Market Report 2020-2025, IoT Analytics, December 2019.*

Three levels of embedded intelligence have been developed in ECSEL/ARTEMIS projects:

- In sensors, in actuators and in more complex devices.
- In the communication (see "connecting the IoT" when we talk about interoperability).
- Distributed embedded intelligence, that is, intelligence distributed in the various parts of the IoT infrastructure (in the edge, in the "internal" nodes of IoT infrastructure, in a data centre, on the cloud, etc.).

The ARTEMIS and ECSEL projects have contributed to improve the "awareness", the decisional autonomy and the analytics capabilities of IoT, addressing several research challenges:

- Increase the decisional autonomy of the devices on the edge.
- Self-adaptation and configuration (e.g. context awareness and adaptation, increased possibility to develop custom solutions …).
- Enable the creation of added-value services (smart services):
  - E.g. a smart sensor is seen simply as a service at higher layers of the IoT stack.
  - E.g. information processing and fusion from the whole IoT infrastructure generate added value services that can be adopted to develop the vertical business logic, and can be reused at application level in different vertical domains, demolishing silos and creating unforeseen business opportunities.
- Simplify the management of heterogeneity, one of the most destabilising intrinsic aspects of IoT:
  - Embedded intelligence introduces the fuzziness required to automatically manage diversity.
  - Simplify the management of heterogeneity and complexity treating them with AI at a higher level of abstraction.
- Distributed embedded intelligence.
- Improve cooperation between the *things* of IoT.

Increasing the processing power of IoT devices is just one of the enabling factors to improve their analytical and decisional autonomy, but a rich set of different technologies, including AI, can be further considered. SOFIA, for example, largely anticipated the need for extracting insightful information that could be used on the edge and entirely based its solution for smart environments on **semantics**. The creation of knowledge in a smart object provides the ingredients required for reasoning that, in turn, allows to formulate decisions and to actuate them through the smart object capabilities. Semantics is a good solution for the creation of a shared knowledge-base and the publish-subscribe-notify approach, proposed in SOFIA, allows the smart object to be always up to date about the information it is interested in, and keep its internal knowledge base up to date, which becomes a solid foundation for the execution of a reasoning algorithm in a smart object. Semantics was also adopted in eScop that proposed to combine embedded systems with an *ontology-driven service-oriented architecture* (SOA) for realising a fully open, automated manufacturing environment. Semantics improve the autonomy of embedded systems responsible for the operational control of manufacturing equipment. It allows flexible re-configuration and knowledge updates, specifically for newly plugged or unplugged equipment ("plug & produce" inclusion of new equipment), reducing time and cost related to conventional manual reprogramming, ensuring easy and fast commissioning of new plants, replacement of traditional control with an IoT inspired infrastructure.

Self-adaptation and configuration represent indeed another important form of embedded intelligence that introduces the possibility to create more personalised solutions. CHIRON and WithMe, for example, proposed the idea of *proactive computing* for healthcare and well-being, making the embedded systems composing the IoT infrastructure capable of anticipating the needs of people and self-adaptation, thereby enriching the quality of life, personalising patient assistance and fostering their empowerment. In the medium to long term, the impact of self-adaptation and configuration is expected in terms of fewer visits to doctors and hospitals, shorter hospitalisation periods, increased longevity with improved quality of life and increased support to interdisciplinary care teams. SIMPLE and DEMANES focus more on industrial applications. SIMPLE addressed the *self-organisation and cooperation* of wireless sensors and smart tags for federated, open and trusted use in the manufacturing, logistics applications and domestic use. Based on these concepts, the project developed a complete manufacturing plant solution, a complete logistics supply chain and a domestic case. DEMANES developed a framework and a component-based methods and tools for the development of run-time adaptive systems, enabling them to react to changes in themselves, in their environment, in user needs and in contexts. The primary objective was to develop novel technologies to support the cost-effective and timely realisation of large-scale networked systems embedded in the physical world, which are capable of a high level of evolution to follow internal and external changes and manifest a high level of dependability. pSHIELD, nSHIELD and DEWI addressed the *security aspects* related to self-adaptation and configuration. pSHIELD and nSHIELD designed entirely the framework for security, privacy and dependability (SPD) of IoT devices and systems on the concept of built-in self-diagnosis of the SPD status and self-adaptation depending on the current SPD threats. While DEWI, developed a locally adaptable wireless "sensor & communication bubble", providing locally confined wireless internal and external access, secure and dependable wireless communication and safe operation, flexible self-organisation, re-configuration, resilience and adaptability.

Improving the intelligence embedded in IoT devices contributes to **simplifying the management of the heterogeneity**, one of the most destabilising intrinsic aspects of IoT: providing intelligence to an IoT device implies giving it a certain level of fuzziness, exactly the key element that humans adopt to better manage the diversity and heterogeneity of everyday life. For example, in nSHIELD the *management of threats at system level* is based on embedded intelligence in order to treat a larger number of threats that a hard-coded algorithm could not efficiently and dynamically manage. Indeed, the embedded intelligence also allows heterogeneity and complexity to be managed at a higher level of abstraction: *intelligence combines simple information and generates more abstract concepts, allowing management at a more complex level of heterogeneity*. Again, in nSHIELD, complex security threats that cannot be identified by just monitoring a single port or a service can be detected and managed only by combining simple events and using reasoning to recognise a more complex threat.

The previous example, which combines information collected from different sources, introduces the concept of **cooperation between IoT devices**, a concept that is strongly based on embedded intelligence. eDIANA, for example, developed a middleware infrastructure based on novel algorithms, protocols and software tools that enable *collaborative and context-aware interaction among heterogeneous devices*. The addressed vertical domain is urban electricity distribution and monitoring, where electricity can be accessed, read, profiled, curtailed and managed with various devices that can cooperate to provide not only the previous functionalities but also an increasingly precise response to changes in weather, user comfort, security criteria, demand and price. In a similar context, ACCUS aimed at providing an integration and *coordination platform* for urban systems, in order to optimise their combined performances. ACCUS addressed the *efficient composition of system of systems in dynamic environments*, providing an integration and coordination platform for urban subsystems. An adaptive and cooperative control architecture was developed to optimise their combined performance, and methodologies and tools for creating real-time collaborative applications for system of systems were introduced. The Arrowhead project was entirely focused on *cooperative automation*, addressing the technical and applicative challenges associated with cooperation between devices and more complex systems through the provision of a technical service-oriented framework, the Arrowhead Framework, that simplifies and standardises their interaction. Recently, AFarCloud intends to provide a distributed platform for autonomous farming, which will allow the integration and *cooperation of different CPS in real-time* for increased

agriculture efficiency, productivity, animal health, food quality and reduced farm labour costs. The project aims to make farming robots accessible to more users by enabling, for example, farming vehicles to work in a cooperative mesh. Eventually, SafeCOP investigated the safety aspects related to cooperation between devices, defining a runtime manager to detect abnormal behaviours at runtime, able to trigger a safe degraded mode. The project developed methods and tools to *certify cooperative functions* and offer new standards and regulations to certification authorities and standardisation committees. The proposed solution was applied to cooperative moving of empty hospital beds, cooperative bathymetry with boat platoons, vehicle control loss warning, vehicle and roadside units interaction and vehicle to infrastructure cooperation for traffic management.

Cooperation between IoT devices that are typically distributed implies that also the embedded intelligence is distributed, increasing **the intelligence of the entire IoT infrastructure**. ENCORURAGE addressed the issues of distributed intelligence at different levels, in the context of smart buildings. At device level, the project developed an intelligent gateway with embedded logic supporting inter-building energy exchange, facilitating direct communication with other buildings and local producers so that the potential use of the electricity produced locally on their premises can be negotiated. At infrastructure level, the project developed *supervisory control strategies* to coordinate and orchestrate larger sub-systems (heating, ventilation, air conditioning, lighting, renewable energy generation, thermal storage, etc.). At platform level, the project developed novel virtual *sub-metering technologies and event-based middleware applications* to support advanced monitoring and diagnostics concepts. Similarly, in the domain of energy, IoE proposed efficient *dynamic and self-reconfigurable topologies* for the aggregation of the nodes of the Internet of Energy (e.g. electric vehicles, distributed renewable energy generation, distributed storage, etc.) addressing sustainable mobility and urban life quality. MANTIS focused on the industrial domain, developing a proactive maintenance service platform that enables the *collaborative maintenance of ecosystems*. The objective was to improve companies' asset availability, competitiveness, growth and sustainability by improving the quality of maintenance and reducing its impact on productivity and costs. The platform is based on *distributed sensing and decision making*, performed at different levels in a collaborative way: the solution considers local nodes that pre-process raw sensor data and extract relevant information before transmitting it, intermediate nodes that offer asset-specific analytics to locally optimise performance and maintenance, and cloud-based platforms that integrate information from ERP, CRM and CMMS systems and execute distributed processing and analytics algorithms for global decision making.

Eventually, embedded intelligence represents a key factor for the creation of **added-value services (smart services)** in the higher levels of the value chain: for example, a sensor that is able to process the collected data locally, generate more abstract information, take simple decisions and, when required, *make this information available as a service*. The smart gas meter, developed in ME^{3}GAS, was able to provide added-value services to the final user (e.g. management of multiple tariffs and payment modalities) and to the utility company (e.g. remote gas cut off, security alarms, etc.). Recently, CONNECT proposed a similar solution based on advanced smart metering and sensing approaches to reduce the power demand by providing consumption/generation data to the users. CHIRON and WithMe developed healthcare and well-being personalised services to patients, that were possible thanks to the intelligent integration of information in personal information spaces. In MANTIS, the development of smart sensors, actuators and cyber-physical systems capable of local pre-processing, as well as robust communication systems for harsh environments, allowed the provision of high-level services to improve the availability of assets in industrial applications.

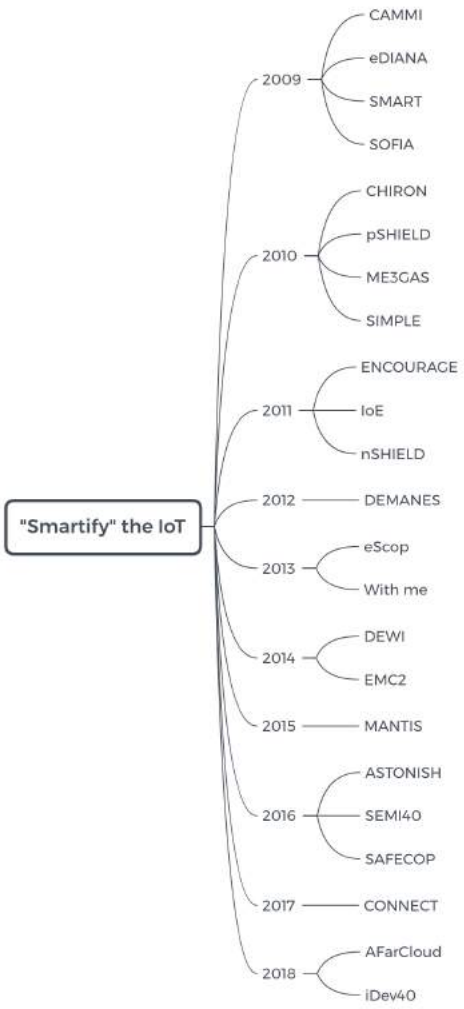


FIGURE 22 — *ARTEMIS/ECSEL projects that contributed to improve the embedded intelligence by call.*

Embedded intelligence is a research domain in an early stage of development. In recent years significant progress has been made, but the wide adoption of this enabling technology still requires significant investments in scientific and industrial research. Potential areas of future development include:

- Integration of artificial intelligence, featuring self-X technologies (self-organisation, self-adaptation, self-reconfiguration, self-healing) and truly cognitive functionalities.
- IoT edge analytics, embedded analytics, geospatial and local intelligence
- Machine learning on the edge.
- Distributed algorithms for cooperation among co-located nodes.
- Embedded intelligence for distributed sensing based on machine learning.
- Realtime classification on resources limited devices.
- Collective intelligence.
- Neuromorphic computing.

"Populate" the IoT

The IoT is a system primarily composed of a *heterogeneous set of artefacts*: sensors, actuators, simple embedded systems, complex smart objects, consumer devices, multi-service gateways, industrial edge controllers, vehicles embedded control units, edge high-performance systems, adapted legacy devices, etc. A large part of these artefacts is the result of the integration of different enabling technologies that provide them sensing capabilities, good power autonomy, significant processing power, a certain level of embedded intelligence, connectivity and cooperation capabilities, etc. With such a rich set of features and capabilities we refer to these artefacts as "smart objects". They are the result of interdisciplinary research and must be considered an enabling technology being *the main building blocks of IoT*. Without them, IoT simply would not exist.

> *Smart objects transform the physical environment around us into a digital world: they represent the bridge between the physical world and the digital world, becoming the fundamental elements on which the entire digitalisation process is built.*

Depending on the vertical domain, a smart object carries part of the application business logic and interacts with other artefacts of the IoT infrastructure and with human users. A smart object senses, processes, logs, interprets and communicates. It is typically able to execute the business application in a semi- or fully autonomous way, becoming decoupled from the rest of the IoT infrastructure. Bridging physical and digital worlds, these objects also increase the volatility, dynamism and complexity of IoT infrastructure, which will lead to new cyber-security challenges and expose the collected information to security and privacy risks. Therefore, new ideas for safeguarding security and privacy in this emerging landscape will be needed.

From the functional point of view, the most basic level of intelligence they host consists of triggering alerts depending on the data collected from the environment or from other devices. This autonomy already represents an added value, but the real value of the embedded intelligence of smart objects is found at a different level and consists of learning from their specific use or from each other and then automating actions. At this level they can adapt, change behaviour over time, make decisions, take actions and tune their responses based on what they have learnt.

Smart objects are typically connected to the edge of the IoT infrastructure, becoming fundamental for the adoption of the edge computing paradigm in IoT: they simply *make edge computing physically possible*, hosting the data-processing algorithms and the analytics migrated from the enterprise/cloud to the IoT infrastructure.

The artefacts typically populating the IoT belongs to three different macro categories:

- *Consumer* connected devices, including speakers, wearable devices, personal assistants, smart appliances, smart TVs, smartphones, healthcare devices, etc.
- *Social and enterprise* connected devices, including smart meters (e.g. energy, water or gas meters), multi-service gateways, smart city devices for traffic monitoring, pollution monitoring, weather forecasting devices, smart lighting, smart thermostats, wireless sensor networks, etc.
- *Industrial* oriented artefacts, including edge controllers, smart cameras, smart sensors and actuators, robots, smart production machine, wireless sensor networks, smart engines, pumps, etc.

A fourth transversal category collects all the *legacy artefacts* that are not IoT-enabled but that can become part of the IoT infrastructure directly through an existing interface, or indirectly through an adapter. *The huge category of legacy devices, connected or non-connected, with or without processing capabilities, sensing and actuation functionalities and some level of intelligence, represents an almost endless market for IoT.*

> *Legacy system support is fundamental for the uptake of IoT, representing a sustainable and profitable way to refresh, add value, promote and improve the ROI of existing businesses.*

Indeed, the "rip-and-replace" approach that implies a complete substitution of the legacy IT infrastructure with IoT-ready equipment, is expensive and very frequently doesn't represent the most profitable and attractive solution. Replacing legacy systems with new equipment is certainly more viable in the long term, due to its improved reliability, better performance, low power consumption, scalability, etc. But replacing a legacy system remains a challenge because of the time and the costs required for the replacement: *trying to set up a future-ready business, the "throw everything away" approach is typically extremely costly and time-consuming, with the potential risk of being wasteful and without any ROI if it fails to satisfy the initial expectations.*

Instead of a full replacement, the *augmentation of a legacy system* is more affordable and faster, also allowing an incremental approach. Progressively upgrading a legacy system with smart objects reduces the time to market, provides IoT capabilities that contribute to optimising the business operations, limits the investment and ensures ROI. The augmentation process, for example, consists of upgrading legacy machinery with smart sensors and actuators, driven by an industrial edge controller that runs the local business logic and bridges the machinery to the IoT infrastructure. This approach doesn't require the complete replacement of the old equipment.

In the context of smart objects, the ARTEMIS and ECSEL projects contributed to:

- The creation of new smart sensors and actuators.
- The study and the creation of new secure, flexible and adaptable Wireless Sensor Networks.
- The creation of new smart objects.
- Providing support for the integration of legacy systems, following the approach of *don't "throwing anything away" but augment, adapt and include.*

The next 20 years will see an enormous increase in the total number of IoT devices, which will permeate our homes, workplaces and outdoor environments. The availability of a **new generation of electronic components** (e.g. sensors and sensor systems), specifically conceived for IoT, is one of the primary drivers of this trend. In this context, IoSense developed *frontend and backend sensor technologies for both discrete and integrated innovative sensor devices*, suitable for high volume production required by the IoT market. The project provided electrical and mechanical security and software resources for integration of sensor system components into IoT systems and IoT enabling systems. A rich set of sensors were developed, covering the requirements of many vertical domains: a sensor for lighting products with performance monitoring, a dust, air quality and gas sensor for environmental monitoring, a force/pressure sensor and flow sensor for smart production, a sensor system (including sensors for temperature, pressure/vacuum, mass, optical detection, force) for manufacturing, and a spectrometer-on-a-chip for smart health. In the same research area, MANTIS developed a new wireless sensor for fine measurements of torque forces for the heavy industry, based on a transducer built on torque oriented gauges, a signal conditioning circuit and a signal processing software, allowing a local pre-processing of the collected data, by means of intelligent functions.

By creating smart objects, **IoT can be enriched, domains can be expanded and quality of life can be improved for end-users**. An example of these intersecting forces is ILAND, which has facilitated remote monitoring and infrastructure-free email services in poorer regions with no communication infrastructure. ILAND also demonstrates the strong overlap between the four artefact macro-categories and the smart object contexts to which ARTEMIS and ECSEL projects have contributed, as WSN-based products and applications (such as home and environmental monitoring) can also benefit from this project. Several other solutions have been developed in the *WSN domain*, including SMART. This supports application-specific features – such as security, power consumption, video capabilities, auto-configuration and self-organization – by altering the processing tasks of reconfigurable devices according to their sensor network's environment. WSNs represent a very flexible category of smart objects that have been frequently adopted to improve security in many vertical domains. For example, in pSHIELD and nSHIELD a WSN has been adopted for the localisation and tracking of railway carriages transporting hazardous material. While DEWI envisioned a 'sensor & communication bubble' based on WSNs and featuring local security, resilience, flexibility and interoperability. This solution has been adopted in twenty-one industry-driven use cases in the aeronautics, automotive, rail and building domains. Recently, MANTIS extensively investigated the technologies required to develop a mote (a connected sensor node), based on the state of the art of MEMS, contactless sensing, embedded local processing and wireless bidirectional connectivity. MANTIS analysed the sensing strategies in manufacturing processes, trying to understand how a sensor-based monitoring system could improve the manufacturing processes in terms of maintenance.

IoT and SoS hold great promise in terms of **energy management**, for which eDIANA has developed a *real-time power consumption sensor and embedded energy controller* for urban and domestic environments. This combines consumer, enterprise and industrial smart objects as it allows utility companies to effectively manage energy load while empowering consumers to adjust consumption and make data-based decisions. CONNECT focused on an efficiency, low-cost, low-weight, and compact *high-power density converter* with embedded communication capabilities for different application levels in the smart grid and conceived for example to avoid unnecessary energy flows. ME^{3}Gas developed a new generation of *smart gas meters* providing intelligent features, such as management of multiple tariffs and payment modalities, remote gas cut off, security alarms, etc. IoE's interface-based smart meter system could support this through advanced demand response and load shedding. ENCOURAGE aims to enable energy optimization in buildings at the device, building and district levels via the development of supervisory control strategies, an intelligent gateway with embedded logic, novel virtual sub-metering technologies and event-based middleware applications.

Healthcare is also becoming increasingly digitalized; sensors therefore feature heavily in the population of IoT within this domain. ASTONISH, for example, has improved *personal wearable monitoring systems* for immediate health feedback. On a larger scale, the With-Me ecosystem is an open solution which integrates an embedded platform for *multivendor nomadic sensors*, *interoperable intelligent sensors* to monitor wellbeing and an open architecture for persuasive electronic services. This collection of embedded devices is a gateway to customizable health services. In recognition of IoT's multidisciplinary nature, SCOTT combines long- and short-range monitoring and analysis systems to create *hybrid WSN monitoring solutions* for IAQ (Indoor Air Quality). Starting from simple existing sensors (e.g. temperature, relative humidity, CO2 / CO / NO2 concentrations) and integrating them in this WSN solution, it is possible to enable sensor data fusion and analytics and new trustable services that ensure lower energy consumption and a healthy indoor environment.

A wide range of **more complex smart objects** have been developed in SOFIA: a smart gateway for heterogeneous system integration in smart buildings and smart manufacturing, a "family bonding" smart device, a smart lock system, a smart camera for surveillance applications, etc. In this context, also nSHIELD, EXIST and COPCAMS proposed *smart cameras* for security, surveillance and smart manufacturing applications. ENCOURAGE provided an *intelligent gateway* with embedded logic supporting the integration of large systems in buildings, including heating, ventilation, air conditioning, lighting, renewable energy generation, thermal storage, etc.

A great strength of IoT is its flexibility, giving **new life to legacy devices and systems** while using them to speed up digitalization and dramatically reduce costs. This is an important basis on which future IoT and SoS can be enriched. SOFIA used *adapters*, running on a smart multiservice gateway, to link these systems, describing them with semantics and publishing their features and functionalities in the entire smart environment. In ARROWHEAD project, smart charging stations for electric vehicles based on a similar multiservice gateway were able to expose their own functionalities to IoT in the form of services. *As almost all technology eventually becomes a legacy system in its own right, reusability is also vital.* This has been demonstrated by AFarCloud, for instance, which enables farming vehicles to work in a cooperative mesh that combines their capabilities.

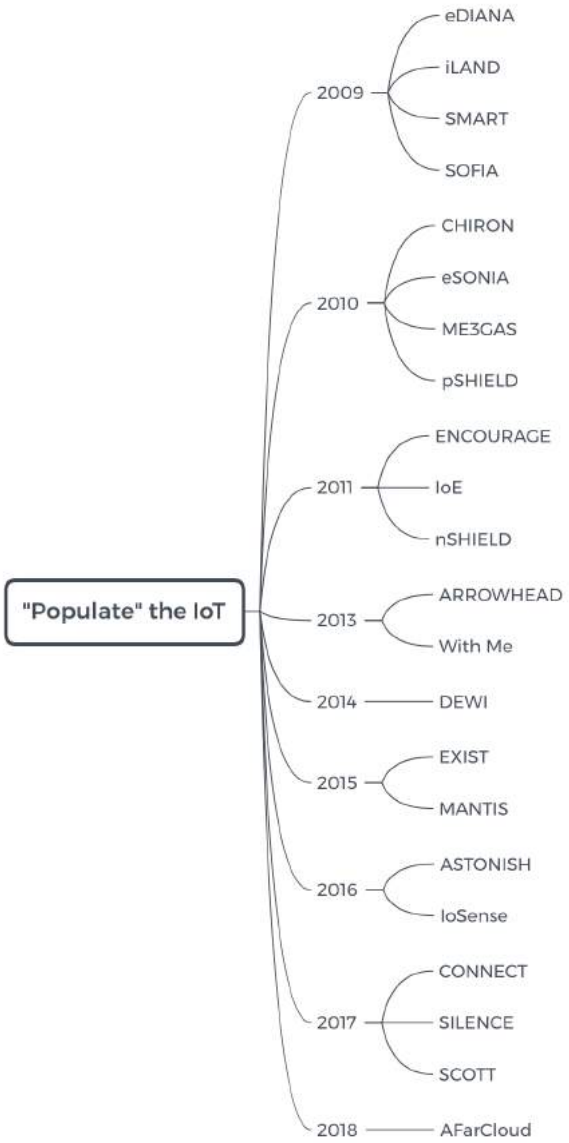


FIGURE 23 — *ARTEMIS/ECSEL projects that contributed to "populate" the IoT by call.*

The evolution of research and innovation in this focus area will contribute to populating IoT with intelligent artefacts provided with better sensing capabilities, improved autonomy and cooperation capabilities:

- Improve the capabilities of smart sensors and actuators. Bio-sensors and bio-actuators. Quantum sensors.
- Create new autonomous devices (e.g. robots, drones and autonomous vehicles, etc.).
- Improve security, reliability, privacy and dependability of smart objects.
- Decoupling smart features from smart objects and design modular and extensible smart objects.
- Decoupling smart objects from the business application and making them reusable for different vertical domains.
- From "smart objects" to "social objects", providing social-like capabilities to the objects in the IoT.
- Improve support for the inclusion of legacy systems, at any level.

"Interact" with IoT

Technology is primarily oriented to create a better life and should be made with a human dimension: from this perspective, IoT is not an exception and, considering the heterogeneity of devices composing the infrastructure, the potential vertical applications and the variety of users involved, significant effort should be spent on this focus areas.

IoT can improve how users interact with almost everything in everyday life, helping businesses to create personalised experiences that are accessible on many devices at their personal convenience. But the adoption of IoT in the consumer world, in industry and, more generally, in organisations has a significant and diversified impact on how common activities and work is done, requiring appropriate, customised and efficient interaction models and human-computer interfaces.

Human interaction with IoT can basically involve four categories of users:

- Inexperienced users (e.g. a person that uses health care monitoring devices at home).
- Experienced users (e.g. a maintenance operator that repairs an industrial machinery).
- Super users (e.g. the administrator or operator in charge of managing the IoT infrastructure).
- The designers and developers of the application and of the interface with IoT.

These four categories of users need *different interfaces with the IoT world*, depending on the application, on the type of interaction, on the duration of the interaction, on the type of information displayed, etc. Many different technologies can be adopted to satisfy these requirements and to develop the interface that provide the best interactive experience with IoT.

Depending of the vertical domain, the right interface can improve sales, reduce the time required to carry out a task, improve shopping, simplify maintenance activities, simplify inventory management, etc.

A very common solution to simplify the interaction with users is based on the use of *natural language and voice-based interfaces*: it is a mature technology that is gradually transforming the way people search information, perform simple tasks, shop and express their preferences. Although being a mature technology, it is more common in the consumer market and almost absent in the industrial applications. The use of voice to control an interface is powerful for its simplicity and effectiveness but it is also a delicate technology that is still not enough reliable for the industrial world: user's voice is subject to frequent changes that are difficult to manage but also the input modality adopted for the interaction (e.g. use of command versus use of requests) could negatively affect the final user's experience and the efficiency of the interface.

Recently, *augmented reality* has been developing rapidly, and provides immersive solutions to enhance user experience in many vertical applications, including IoT. Augmented reality provides an ideal interface to IoT applications, by overlapping virtual information from smart objects and services on the user's view of the real world. The physical interaction with the object is augmented with additional information about the object, the context, the process, information about nearby objects, about the IoT infrastructure, etc. The advantage of using augmented reality is that the physical interaction with the object is not strictly necessary. The interaction happens primarily in virtual reality and, in terms of functionalities, it significantly extends the physical possibilities offered by the object (e.g. buttons, levels, keyboards, etc.) with software-based functionalities available only in the virtual interface (e.g. overlapped information, menu, symbols, etc..).

The integration of IoT and augmented reality is still in an early stage but, considering the enormous potential, it will be a very important research area. It will enable a vast set of vertical applications, including:

- Education and professional training based on augmented reality.
- Augmented site inspection (e.g. safely guide operators to a faulty equipment).
- Simplified maintenance operations (e.g. augmented reality hardware facilitates hands-free operation and the IoT connections during repairs provide access to reference sources, like live diagnostic feeds, technical manuals, co-workers and help desks).
- Human-assisted robotic manufacturing (e.g. augmented reality helps the operator in the selection of the parts to pick-up and assemble, then IoT takes over and starts the full robotic-based manufacturing process).
- Simplified fleet management (e.g. augmented 3d-based asset management, windshields that provide traffic data, weather alerts and cargo status, etc.).
- Improved worker safety and efficiency (e.g. safety helmets that provide task lists, safety instructions, workers surveillance, monitoring vital signals, etc.).
- Support for emergency responders.
- Etc.

The research activities carried on in ARTEMIS and ECSEL projects have been focusing both on technological aspects and on the role of humans in the loop:

- Improve human-machine interaction.
- Improve human efficiency, reduce workload, simplify human tasks, …
- Promote the adoption of a "human centric" vision.
- Use of IoT as a mean for creating and keeping human relations.

Humans communicate predominantly using speech and gestures, which runs counter to the methods that have traditionally been used to interact with machines. In order to engage non-experienced users in new technologies (opening up both market opportunities and quality of life improvements), it makes sense to **extend natural human communication to machines**. SILENSE, for example, is researching *acoustic technologies and concepts* for device management via gestures, audio sensing, data communication and indoor positioning. In making machines easier to use, such innovations can also improve safety (such as touchless navigation in vehicles), security (through new authentication scenarios) and hygiene (via reduced usage of touchscreens). In SILENSE's case, the aim is to develop and improve smart acoustic technology blocks at the hardware, software and system levels, including smart algorithms, low-power IC design and transducers for voice/speech, digital sound modulation and gesture control. Projects like this hold potential in fields as diverse as healthcare, automotive and smart homes: a connecting factor is user interfaces, which are currently one of the key differentiators in the mobile market. These are also a *prominent enabler of increased efficiency*, as indicated by CAMMI's joint cognitive approach to operator console control: whenever

the workload exceeds the operator's capacity, time-consuming yet non-critical tasks are automated or offloaded, allowing the operator and the system to share control. Like in SILENCE, nSHIELD proposed a new *people identification technology* for security applications. A user-friendly and assistive HMI allowed to automatically manage the entire process of people identification (facial images acquisition and analysis, person recognition and authentication) to ensure security in large public infrastructures (e.g. stadium, airport, train stations, large buildings, etc.) and improve the reliability of security operators' tasks.

Efficiency through improved human-machine interactions is reflected at both the macro (industrial, economic, societal) level and the micro (individual) level. In all cases, a human-centric approach is required; in CAMMI's case, this involved identifying a core of cooperative work across different domains and developing technologies for *intelligent multimodal interactive systems* that address user interaction with adaptive context-aware systems. A wide range of applications are envisaged, ranging from (un)manned aircrafts to civil protection to agricultural machines. ASTONISH, on the other hand, simplifies complex clinical tasks by combing advanced user interfaces with smart algorithms, multimodal fusion techniques and biomedical signal processing of the acquired data. MANTIS investigated the design of *scenario-based and context aware HMI* design, analysing in different scenarios the activities that maintenance people are conducting during everyday work. The objective was to identify the best human-machine interface (personal computers, tablets, wearable devices, etc.) to simplify, improve safety and efficiency of maintenance activities in an industrial environment (e.g. maintenance of a protrusion line, a press machine, a sheet metal working machine, a conventional energy production system, etc.). Human-centric IoT also shows enormous promise in the field of *healthcare*, in which ageing populations require affordable treatment by fewer and fewer medical professionals. The approach adopted by CHIRON is to shift from healthcare to ensuring that people remain healthy for longer; it does this through an integrated system architecture for a 'continuum of care' from the home to the hospital and everything in between. The reference architecture will ensure interoperability between heterogeneous devices and services, reliable and secure patient data management and a seamless integration with the clinical workflow.

Personalization is another crucial element of human-centric technology and encompasses aspects such as tailored treatment and personal assistants. In terms of healthcare, this should result in fewer hospital visits, shorter hospitalization periods and improved quality of life. The With-Me project, for instance, aims for an adaptive, assistive and secure training/supporting platform based on user preferences and needs and a personalized virtual assistant that provides guidance on physical activity and healthy living. SCOTT applies a similar logic to at-risk individuals such as stroke patients. By applying advanced wireless sensor technology, their health and wellbeing can be monitored and their location and possibly activity can be determined. If something is amiss, a caregiver can be notified.

Humans are fundamentally social and IoT should therefore be a means to **create and maintain human relations**. Another aspect of SILENSE, for example, is sign language interpretation for individuals suffering from speech or hearing impediments and wider accessibility options for disabled or elderly individuals. Others, such as SOFIA, focus on family bonding. In short, ARTEMIS and ECSEL's IoT interaction projects are not just about bringing natural human communication to machines but also about advancements in communication between the humans who use these.

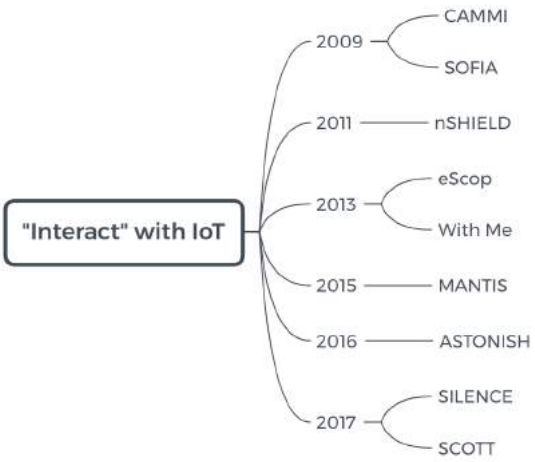


FIGURE 24 — *ARTEMIS/ECSEL projects that investigate the human-machine interaction in IoT by call.*

The interaction between IoT and users is a fundamental research focus area because it is from this interaction that we firstly perceive the benefits of IoT presence around us. The importance of interaction for the acceptance of IoT requires investments in many technological fields, including:

- Multimodal Interactions between human and machine (e.g. spoken and gestural interaction, brain computer interface, etc.).
- Automation vs interaction (considering critical issues as for example safety, feeling of control, privacy etc.).
- Improve speech and image recognition.
- Augment reality, in all the aspects and technology areas.
- Recommendation systems.
- Human-computer interfaces that ensure clear appearance and pragmatic transparency of the information.

IoT/SoS architectures

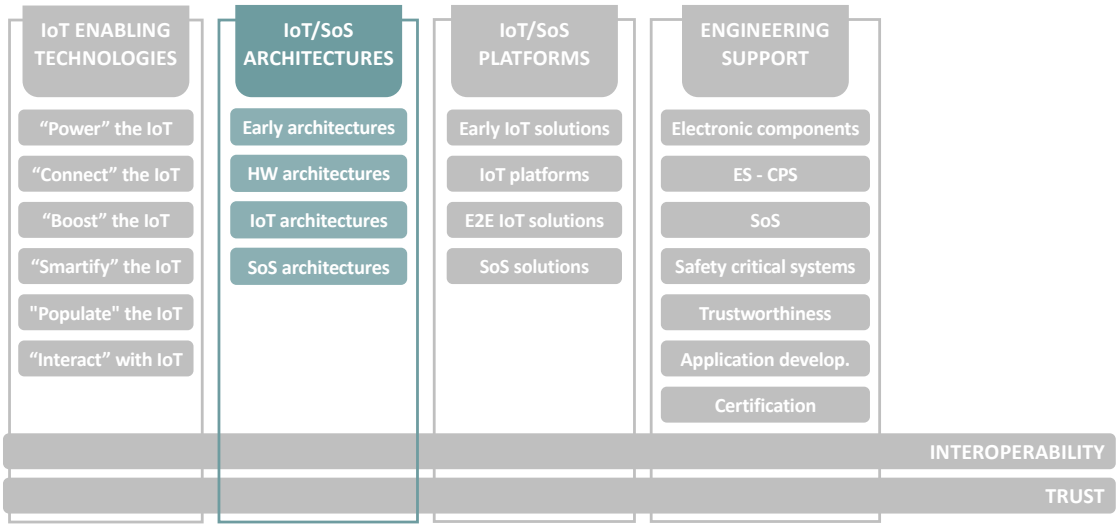


FIGURE 25 — *IoT/SoS architectures research stream.*

Enabling technologies provide the first glimpse of the IoT vision, while architectures represent the attempt to rationalise and "organise" this vision. *Architectures define the structure of the IoT solution, how it is composed and organised, how IoT nodes interact, how they can be managed, how information flows, etc.* The IoT architecture represents one of the main challenges of the evolution towards a sustainable product and requires considerable investments in research and innovation.

The IoT architecture must support the heterogeneous and fragmented nature of IoT/SoS, made of different devices, subsystems, systems, networks, information flowing between them and applications using the information. Key elements to support a similar level of heterogeneity are interoperability, openness and standardisation, which become fundamental requirements of the architecture design. Considering potential vertical domains, these initial requirements are extended and complemented by scalability, modularity, extensibility, security and flexibility.

An architecture defines how the integration of multiple systems, the cross-domain interaction, the simple, secure and scalable infrastructures management, the optimised data acquisition and management, data analytics, added value services and applications will be possible.

Eventually, the presence of *virtualisation, automation and intelligence represent* a guarantee of evolvability of the architecture. Virtualisation allows the architecture to be abstracted from specific solutions at physical level (e.g. sensors, actuators), ensuring with virtual objects (e.g. fog/cloud services, communication layers and protocols) the possibility to confine future significant changes only in the lower layers of the IoT/SoS stacks.

Containers technology is also influencing the evolution of IoT/SoS architectures, bringing a rich new set of flexible and performant functionalities conceived for deployments, both for centralised and edge-computing based IoT solutions. Docker is the most popular container runtime environment, while Google's open-source platform, Kubernetes, can be considered the winner of container orchestration race. In August 2019, VMware launched Tanzu, a cloud platform that manages Kubernetes container distribution and allows applications to be built and deployed. In October 2019, Siemens acquired Pixeom, a software-defined docker-based edge platform, with the goal to embrace container technology for edge applications in factories. In 2018, Cisco launched the "Cisco Container Platform" and, in the last two years, it established three important partnerships related to container technology to support Google Cloud, AWS and Microsoft Azure Kubernetes Services.

Architecture must also consider the automation that is a key factor to constructing the engineering support required for a sustainable IoT/SoS solution that aims to become a real product. And finally, artificial intelligence represents the only way to fully unleash the potential of modern digitalisation approaches based on IoT/SoS, giving the possibility to autonomously monitor and manage selected information flows, support decision making, etc.

There is no consensus about the IoT architecture, which is reasonable considering the vast amount of vertical applications and the flexibility required to satisfy them. However, there is a widely adopted model that is flexible and comprehensive enough to cover 90% of IoT applications. The model proposes to structure the IoT architecture in five layers, as follows:

- *Sensing and actuation layer*: the physical layer where sensors collect data from the environment, including physical parameters or information obtained from other smart objects in the environment. In this layer commands are sent to actuators.
- *Transport layer*: in this layer the collected data are transported from the sensor to the processing layer and vice versa, from the processing layer to actuators. The transport happens through a network, including WiFi, Ethernet, 4G, Bluetooth, RFID, NFC or other field communication channels.
- *Process layer*: is responsible to store, analyse, and process the data collected from the transport layer. It provides and manage services for the lower (hardware abstraction) and upper layers and, typically, relies on databases, IoT frameworks, artificial intelligence, cloud computing, and data processing modules (e.g. OpenIoT, Eurotech ESF, Hydra, FiWare, Oracle Fusion Middleware, etc.).
- *Application layer*: it is responsible for executing the vertical application and for providing the related functionalities/services to the user. This layer depends entirely on the vertical domain in which the IoT solution is adopted.
- *Business layer*: this layer is responsible for the management of the entire IoT solution, across its entire lifecycle (deployment and commissioning of the solution, user applications, security, privacy, business and profit models, operation monitoring and management, maintenance activities, etc.).

ARTEMIS and ECSEL projects have investigated IoT architectures at both hardware, software and system levels, in order to build solid foundations on the edge of IoT (e.g. for sensing, actuation, processing and connectivity), defining the IoT/SoS stack and providing integration solutions to create and manage the entire IoT/SoS infrastructure. The research areas include:

- Hardware architectures:
  - E.g. functional to simplify & rationalize platform design/implementation and improve features/ capabilities.
  - E.g. functional to develop virtualization technologies.
- Architectures for modularity, composability, interoperability and scalability.
- Architectures that address the heterogeneity and dynamicity of the IoT:
  - Facilitate the integration of IoT/SoS.
  - Frequently based on SoA oriented architectures.
- Architecture oriented to ensure trust.
- Wireless Sensor Networks architectures.
- Architecture oriented to SoS.

In regard to ECSEL and ARTEMIS projects which have sought to address these six research areas, it is important to remember that a large degree of *overlap exists*: the flexibility of IoT architecture naturally creates thematic intersections which one or more projects aim to address. SCOTT, for example, focuses on all of these areas (besides hardware architectures) through a standardised multi-domain reference architecture and compliance with ISO 29182. A specific focus on cross-domain use-cases and heterogeneous environments encourages reusability, scalability and interoperability, allowing digital ecosystems to be built up for broader market penetration.

In a similar manner, eDIANA tackles both architectures for modularity, composability, interoperability and scalability and architectures oriented toward SoS via the integration of a cross-sector solution composed of systems of systems from multiple domains, vendors and service providers. The final result is a reference *architecture for a network of composable, interoperable and layered embedded systems* that has been instantiated to several physical architectures dealing with variable sets of location- and building-specific constraints. Due to its focus on hardware architectures and architectures for modularity, composability, interoperability and scalability, ACROSS is therefore an example which 'completes the loop', demonstrating how all *six areas are logically connected*. ACROSS solution with a minimal set of core services offers domain-independent technology through a component-based architecture, supporting both composability and robustness.

Like all IoT- and CPS-related projects, SCOTT, eDIANA and ACROSS require special attention to **trustworthiness**. If this can be guaranteed, there is a great potential to provide mature, cross-domain technologies at lower costs while accelerating the time to market of new applications.

Having established similarities across the research areas, it then becomes possible to group projects according to domains at the heart of their innovations, such as healthcare or wireless communication. **Hardware architectures**, for instance, are particularly important to the automotive domain, where security or connectivity issues may have lethal consequences. In recognition of this, electric vehicle project POLLUX addressed novel safety and security schemes as its first priority, offering new approaches to standardisation, certification and qualification in order to accommodate new embedded system architectures. By creating a common architecture and design platform for advanced multicore hardware and middleware solutions, POLLUX envisions the convergence of computer and automotive architectures: future cars will be mechatronic systems comprised of a multitude of plug-and-play and self-configurable peripherals.

In order to be comprehensively effective, automotive innovations also need to address the design stage. ASAM, for instance, defined a unified design methodology, automated synthesis and prototyping toolchains to allow the rapid exploration of high-level algorithm and architecture design spaces. The ensuing vertical integration and horizontal cooperation between OEMs and hardware, software and silicon suppliers are crucial when it comes to building a solid European embedded systems industry and establishing standard designs and distributed real-time embedded-systems platforms for electric vehicles. POLLUX has also played a key role in this new industry by developing spin-offs aimed at energy savings and sustainable production (particularly in terms of scarce raw materials).

In addition to **opening up new markets**, IoT/SoS should play a role in **revolutionising existing production domains**. In the field of IoT heterogeneity and dynamicity, PRODUCTIVE 4.0 is one example of an architecture which can be used to manage supply chains, product lifecycles and digital production by simulating manufacturing processes to optimise real workflows. CRAFTERS, meanwhile, expands previous design approaches through the development of a multicore architecture and early estimation techniques, performance estimators, verification frameworks and parallelising coilers.

On the subject of **energy usage** in general, **sustainability** has become an increasingly pertinent issue for organisations at all stages of the IoT/SoS value chain. Some projects, such as ARROWHEAD, have recognised that this can actually bring a competitive advantage and have worked to enable collaborative automation in the energy domain. e-GOTHAM serves as a functional example of this: through an open reference architecture and a middleware with communications and decision support tools, the energy-related parameters of residential, service and industrial microgrids can be dynamically and autonomously measured to match demand and supply. In turn, IoE has worked to create a real-time interface between the smart energy grid and devices/loads at the edge (such as electric vehicles and domestic appliances) that can be charged to any source of energy. This is achieved through an underlying architecture of distributed embedded systems combining power electronics, integrated circuits, sensors, processing units, storage technologies, algorithms and software.

The flipside of attention to **sustainability** is **lower power** usage within the architectures themselves. FitOptiVis, for instance, demonstrates the importance of low latency image processing to CPS autonomy and environmental interactions and focuses on multi-objective optimisation for both performance and energy use. Its reference architecture therefore supports design portability, online multi-objective quality and resource management and runtime adaptation based on platform virtualisation. Additionally, COPCAMS shows that many-core architectures and flexible programming models can be more power efficient through reduced processor areas and aggressive power management, as well as more affordable thanks to efficient use of the silicon area (again saving on material resources). In the medical, agricultural, domestics and security domains, PRIME has established an open Ultra Low Power (ULP) Technology Platform containing all necessary design and architecture blocks and components needed to support the supply of IoT products and strengthen European competitiveness in this field.

While the aforementioned projects hold great potential for industry, **end-users** are crucial to the success of IoT/SoS. Smart environments are one area with obvious implications for individuals, and these should be intuitive and easy to manage – in other words, largely autonomous. SOFIA, which proposed an architecture based on the semantic information broker and a publish/subscribe/notify model, accomplishes this by remaining information and vertical domain-agnostic, allowing heterogenous devices to publish themselves in the smart environment. From CHIRON's perspective, such interoperability is the gateway to personalised healthcare via reliable and secure patient data management and seamless integration with the clinical workflow. Architectures which clearly apply to e-health can also find cross-domain applications: SMART includes sensor network hardware for smart environment monitoring but is independent of the sensors and actuators used, allowing it to be flexibly applied to industrial and transport systems, amongst others.

Given the inherent connected nature of IoT, **Wireless Sensor Network architectures** – one of the key research areas – also have an overarching impact on projects in other fields. DEWI, for instance, tackled four industrial domains (aeronautics, automotive, rail and building) by bringing together fragmented research results into one harmonised architecture for dependable wireless systems development with both domain-specific and domain-independent standards. This ensures dependable, auto-configurable and secure short-range communication and smart composability and integration for WSN. EMMON then develops network planning and deployment tools to facilitate the deployment of such large-scale networks via a scalable and dependable horizontal network architecture. For additional flexibility, wireless and cabled networks may be combined, as indicated by eSONIA's optimised platform to connect production machines and equipment for a complete plant solution.

Returning to the ever-present issue of security, **architectures oriented towards trust** have a vital role to play in allowing solutions to achieve societal acceptance. Two related projects set out to realise this. pSHIELD aimed to address security, privacy and dependability (SPD) as 'built in' rather than 'added-on' functionalities: it provided built-in SPD via a reference architecture that allows flexibility and composability of enhanced SPD technologies acting at every level (node, network and overlay). Building on this, nSHIELD developed new SPD functionalities for railway security, voice/face recognition, dependable avionic systems and social mobility and networking. With the creation of an innovative, modular, composable, expandable and highly dependable architectural framework, and with the use of common SPD metrics, nSHIELD was capable of improving the overall SPD level in any specific application domain with minimum engineering effort. Root problems caused by the convergence of safety and security in embedded systems are addressed by SESAMO, which models and analyses their cross-influences and specifies enhanced building blocks (architectural design principles, communication protocol definitions, etc.) to balance their requirements more easily.

To once again highlight the interconnected nature of the six research areas, all of these IoT systems form parts of **larger Systems of Systems** in which integration and coordination must be optimised for maximum performance. As an architecture oriented towards SoS, ACCUS makes it possible to build monitoring, management and control systems that traverse the border of individual subsystems through many of the concepts previously discussed: a reference system architecture, platform software, design tools for information extraction and control, a model-based design environment and validation tools for application development and monitoring and visualisation tools to track the system-level operations. Such smart combinations of innovations from diffuse domains are what give architectures the power to make IoT and SoS systems a resounding success.

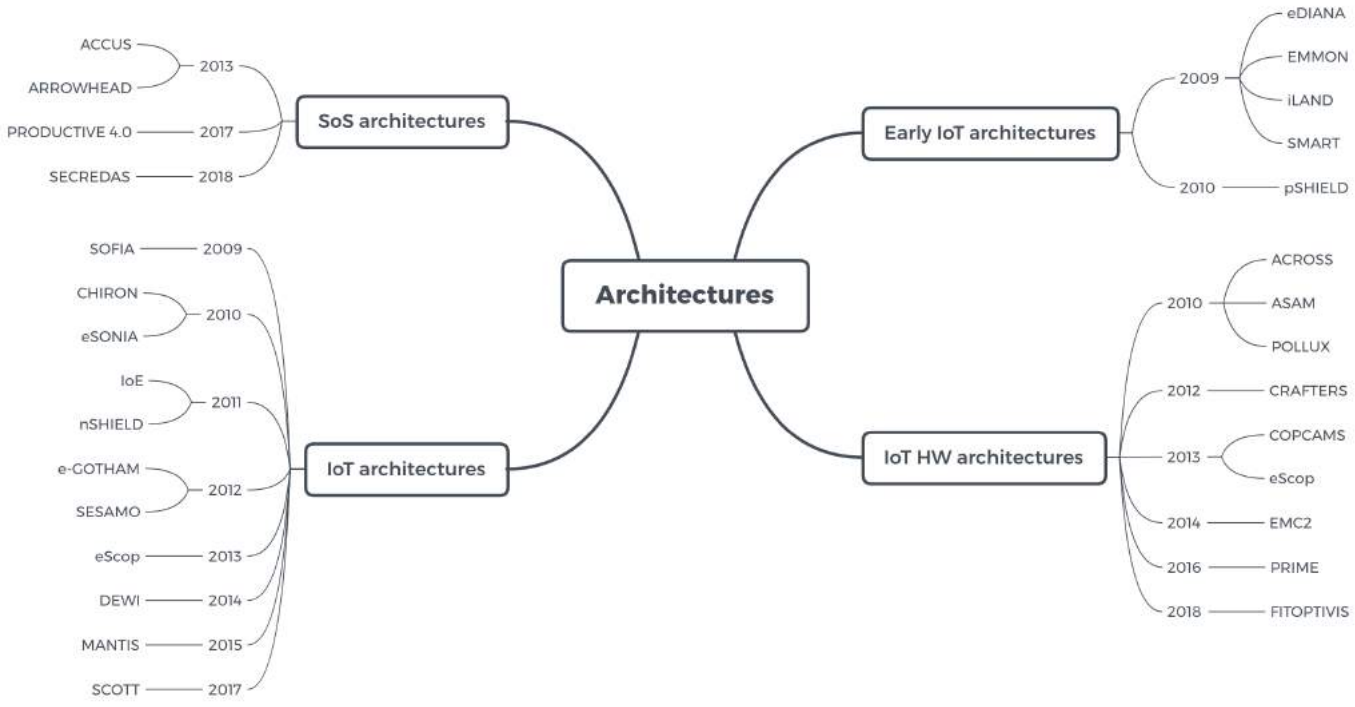
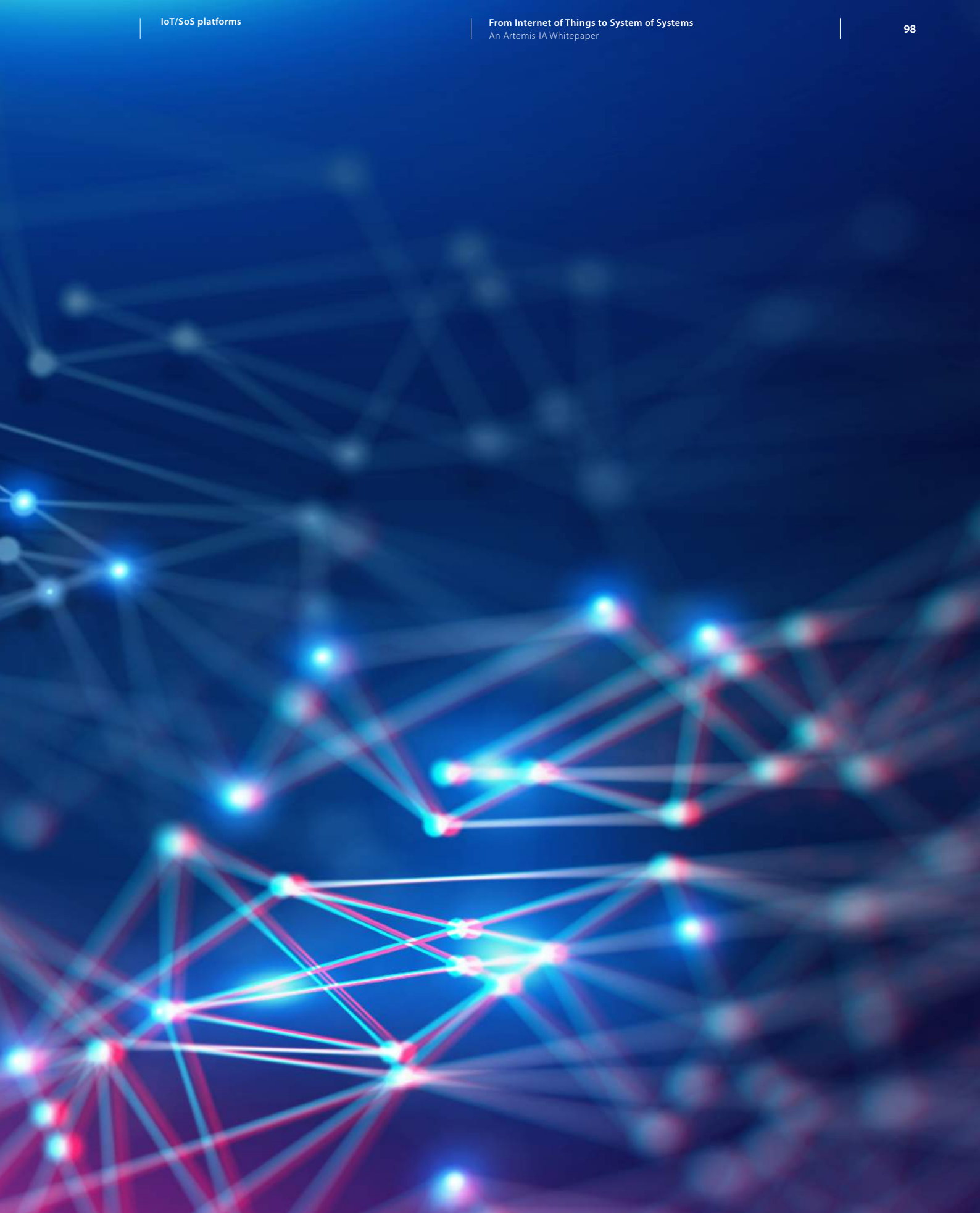


FIGURE 26 — *ARTEMIS/ECSEL projects that contributed to the definition of IoT/SoS architectures, by research focus area and call.*

The architecture of an IoT solution is a fundamental element to conceptually command and control a complex system of systems. It is a vague topic that, thanks to is flexibility, can be adapted to many vertical domains, allowing IoT to achieve the outstanding market results estimated by the vast majority of analysts. The uptake of IoT will strongly depend on the adequacy of its architecture and future research should consider three important aspects:

- IoT and SoS cannot be a mere assembly of disparate improvements issued from previous steps but need to be a smart combination of them to provide efficient solutions.
- Growing number of devices, massive amount of generated data, mission critical apps requiring low latency … are drivers for decentralisation, embeddable computational intelligence and edge computing. IoT architectures must reflect and embrace these trends.
- "Security by design" should be considered also in the definition of the architecture, because of the increased attack surface exposed by IoT.



IoT/SoS platforms

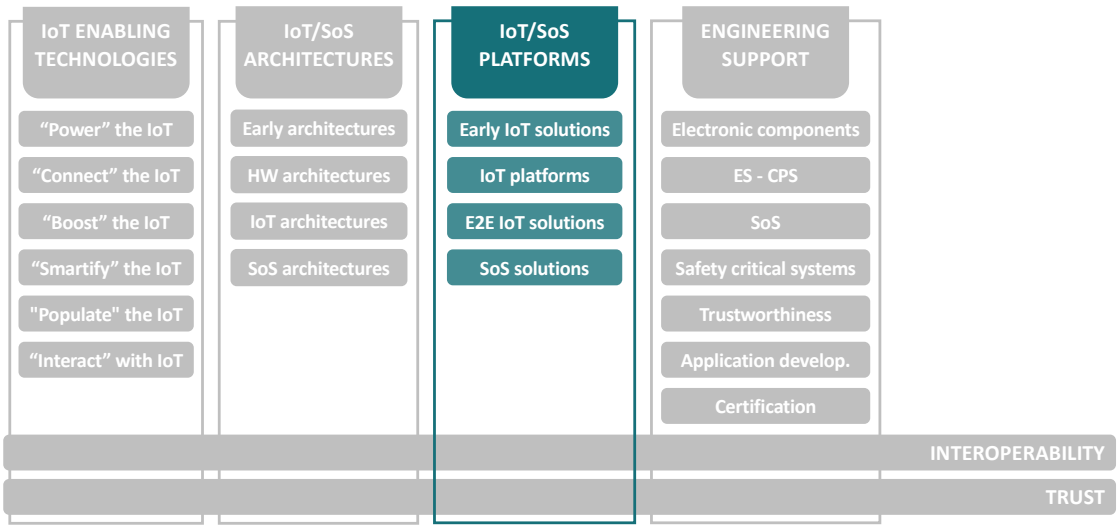


FIGURE 27 — *IoT/SoS platforms research stream.*

IoT end-to-end solutions are the result of an integrated and interdisciplinary approach to leverage data from devices, assets and environmental conditions that, depending on the vertical domain and on the specific business logic, are processed to create added value: *IoT/SoS platforms are the core of end-to-end solutions and represent the backbone of IoT/SoS deployment*. The definition of an architecture is propaedeutic for the design and implementation an IoT/SoS platform that can be considered an instance of the architecture. IoT/SoS platforms allow IoT end-to-end solutions to be realised faster, cheaper, better and, combined with the engineering support, platforms ensure the maintenance and evolution of the IoT/SoS solution across its lifecycle.

The existence of a value chain directly depends on the availability of IoT/SoS platforms that represent the bonding element which keeps the entire ecosystem physically and virtually together, allowing a controlled information flow from sources to consumers, enabling new added-value services and applications, creating and consolidating the relations between the involved stakeholders and generating business opportunity from relations and information. *Platforms promote IoT adoption*, specifically in the case of stakeholders that are approaching a digitalisation process for the first time. Typically, the value creation emerges from the adoption and specialisation of platforms in specific vertical domains, where the adoption of an IoT approach valorises existing assets, generates new sources of information and provides new innovative ways to exploit them from a business perspective.

IoT hardware, software, applications and services are the macro-components of end-to-end solutions, combined in different ways depending on the vendor and on the vertical domain. *Very seldom can a vendor directly sell an end-to-end solution because of its complexity and of the high level of interdisciplinary expertise required.* But selling the IoT platform, which is the core component of an end-to-end solution, it becomes a strategy to also sell the rest of the

components of the end-to-end solution: in this approach the value chain/network plays a fundamental role because this selling strategy is possible only through alliances, partnerships, agreements, that is, through an ecosystem. *The platform "competition" will probably require a long convergence process, without a single winner, because a unified IoT platform is unrealistic and senseless.*

Although the IoT market is growing rapidly, with more than 600 platforms already in 2019, this is a fledgling market that is still taking shape and a large proportion of the players will not be able to really deliver an IoT platform, specifically when it aims to be a complete end-to-end solution. Despite a significant number of company failures and acquisitions in the last three years, which apparently decreased the number of IoT platforms (around 450 in 2017), more than 250 new platforms have emerged since 2017. The fragmentation of the market is increasing, due to the presence of many niches, of many vertical custom solutions sold as IoT platforms and of many SMEs driving small market shares based on a very limited customer portfolio (5-10 customers). From the vertical domains perspective, the largest share (50%) of IoT platforms focus on manufacturing, followed by industry (34%), energy (32%), mobility (32%), smart cities (23%), healthcare (19%), retail (18%), smart homes, etc. Considering that IoT platforms are characterised by a certain level of domain independency, the same platform can therefore be adopted in different verticals. *The market of SoS open (non-proprietary) platforms is almost completely non-existent: in this context the research is still in a very early stage and significant investments will be required.*

Platforms provide a wide range of essential and advanced features and capabilities, on at least six different levels: device, connectivity, data acquisition and storage, data analysis, system integration and application. An IoT platform enables IoT device and endpoint management, connectivity and network management, data collection and management, processing and analytics, data visualisation, application development and deployment, security and access control management, infrastructure and assets monitoring, event processing, subsystems interfacing and integration, etc.

Depending on the positioning in the IoT stack and on the offered functionalities, IoT platforms can be classified mainly in the following categories:

- **Connectivity:** these platforms provide solutions intended to ensure IoT devices connectivity, managing and orchestrating communications, managing data streams, billing and provisioning communication services to the fleet of IoT devices deployed in the environment.
- **Device management:** these platforms enable device deployment configuration, device monitoring, command and control, firmware, operating system and software updates, and generally edge computing management.
- **IaaS/Cloud backend:** the focus in this category is on scalable enterprise grade backend for data management required to provision IoT applications and services, including IoT hub, scalable storage, wide data base support and data processing.
- **Application enablement:** these platforms enable developers to easily and quickly design, develop, test and deploy an IoT application or service. This category provides functionalities such as digital twins, rules engine and event management, integration with the enterprise software and engineering support.
- **Advanced analytics:** this category focuses on the processing of data streams, and includes analytics tools and embedded intelligence, adopted to extract actionable insights from the collected IoT data.

Very frequently, IoT platforms cover many of the previous categories, following an integrated approach aimed at providing a seamless environment for connectivity, IoT infrastructure management, data processing and application/service support.

When referring to IoT/SoS platforms the focus is most commonly on software technologies, but hardware platforms also play an important role in the final end-to-end solution: hardware platforms provide a standard, modular and open approach to create a solid physical infrastructure on the edge (made of sensors, actuators, smart objects, multi-service gateways, edge controllers, etc.), simplifying its integration, deployment, commissioning, operation

management and ensuring its future evolution. For example, in October 2019, Microsoft launched the Azure Sphere microcontroller (MCU), a new platform that allows any device manufacturer to create equipment with native, highly secure cloud integration. The new solution allows the secure and easy connection of billions of MCU-based devices which cannot currently be connected in a secure way due to their limited computing and storage resources. MediaTek, NXP, Qualcomm, Avnet and others are already adopting this technology. In December 2019, following the strategy of reducing the network heterogeneity, Cisco announced Cisco Silicon One, the first networking chip designed to be universally adaptable across service provider and web-scale markets, designed for both fixed and modular platforms.

The ARTEMIS and ECSEL projects have dedicated a lot of effort to the development of the IoT/SoS platforms research stream. A 360-degree overview of the research and innovation activities covered and currently covering this topic includes:

- Middleware and platforms for WSN.
- Legacy systems integration/inclusion.
- Control and manage the IoT infrastructure and its nodes.
- Enable the information flow and processing.
- Promote service creation.
- IoT/SoS integration platforms.
- End-to-end IoT solutions.
- SoS oriented solutions.

The perception that a heterogeneous, distributed, more or less complex system requires specific solutions for its orchestration, management and evolution has been clearly present in the ECSEL community since the initial ARTEMIS calls.

From this perspective, IoT/SoS platforms have been preceded by **early IoT solutions** based on middleware and conceived to simplify the management of the interaction and integration of smart objects. The eDIANA project, for example, developed a *middleware infrastructure* providing algorithms, protocols and software tools to enable interaction among heterogeneous devices, supported by collaborative and context-aware solutions, cross-domain connectivity and interoperability. Similarly, SIMPLE tried to deliver an *intelligent, self-organising embedded middleware*, designed for the integration of manufacturing and logistics based on wireless sensors and smart tags. IoE proposed a *middleware to enable the seamless connectivity* between the different domains of power grids, power plants, electric vehicles and smart buildings. Running on efficient gateways, the middleware was intended to control connectivity and to analyse, interpret and react to the large amount of data flowing through the IoT infrastructure. CRAFTERS realised a *common middleware layer* designed to support new wireless communication standards while being portable across different hardware platforms: the project represented the first tentative to produce a *holistically designed ecosystem*, from application to silicon. E-GOTHAM focused on smart environments composed of smart and heterogeneous devices (an early acceptation of IoT) in the energy domain and proposed a communication model and *middleware to allow interaction among the devices, the environment and the users*. To handle the problem of power grid modernisation, the project proposed to divide the overall power grid into localised microgrids, increasing the communication capability between producers and consumers and enabling both autonomous actions on the microgrid and operations in cooperation with the overall power grid. E-GOTHAM designed an open reference architecture and developed a *middleware with seamless connectivity* that provides the communication and decision support tools needed to optimise and manage microgrids in the residential, services and industrial sectors. This solution facilitates the integration and management of microgrid elements through a large-scale network of embedded systems that use real-time measurements of energy, enabling the dynamic management of power demand and supply.

The necessity to manage the **dynamicity and evolvability of systems** is another aspect that these IoT oriented middleware tried to address. iLAND, for example, developed the enabling technology and the infrastructure of a modular component-based middleware for network embedded systems having strong requirements in terms of deterministic dynamic functional composition and reconfiguration. Similarly, in SIMPLE embedded middleware, the self-organising capabilities were introduced to support highly dynamic vertical applications, such as manufacturing and logistics supply chain.

Heterogeneity and seamless integration have also been addressed in specific technology domains, such as the domain of WSN, initially with middleware and subsequently with more feature-rich and comprehensive platforms. SMART, for example, provided a complete framework composed of sensor network hardware, middleware and software for WSN applications. The proposed solution, being independent from the used sensors and actuators, ensured a high level of flexibility, easily adapting to several application areas (e.g. industrial systems, home networks, e-health, transport systems, avionics, environmental monitoring etc). WSN-DPCM and SCOTT developed complete *platforms for WSN management*. WSN-DPCM developed a full platform to address the adoption of WSN in smart environments: the platform was composed of a middleware for heterogeneous wireless technologies and an integrated engineering toolset for development, planning, commissioning and maintenance activities for expert and non-expert users. By contrast, the SCOTT platform was built upon the standardised multi-domain reference architecture created in DEWI (i.e. the "Bubble concept") and is fully compliant with ISO 29182, which fosters the reusability, scalability and interoperability of WSN.

The necessity to manage the **interaction and integration of a heterogeneous set of devices** is still a primary objective for IoT/SoS platforms. The Arrowhead Framework, for example, was conceived exactly to automate as much as possible the interaction and integration of IoT devices and systems, while transparently publishing, sharing and consuming their functionalities and services. Similarly, the With-Me project created an ecosystem composed of embedded devices made up of multi-purpose consumer electronics, dedicated health equipment and external information sources, and provided with a computational environment to manage device integration, services and applications.

The heterogeneity in IoT and SoS also includes **legacy and existing systems** that don't integrate natively in IoT but, with IoT technologies, could experience a renewed life, generate new value and improve the ROI. The integration/inclusion of this category of systems represents a huge opportunity for the IoT market, shared in different ways by almost all the stakeholders of the IoT value chain, and can significantly improve the market penetration of IoT solutions. A large number of ARTEMIS and ECSEL projects provided and are providing strong support for the integration/inclusion of legacy systems, including SOFIA, eDIANA, nSHIELD, Arrowhead, WithMe, eSCOP, Semi40, Productive 4.0, Arrowhead Tools, etc.

One of the primary functionalities of an IoT/SoS platform is to allow the **remote monitoring and control of the IoT/SoS infrastructure and of the nodes composing it**. This fundamental functionality has been considered since the initial IoT solutions proposed in ARTEMIS projects. eSONIA middleware, for example, was capable to run *remote continuous monitoring, diagnostics, prognostics and control* of industrial assets. ENCOURAGE virtual sub-metering technologies and event-based middleware were designed to support *remote advanced monitoring, orchestration and diagnostics* of large building sub-systems (heating, ventilation, air conditioning, lighting, renewable energy generation, thermal storage, etc.) to optimise the energy consumption of building in a smart grid environment. Similarly, E-GOTHAM middleware was conceived to optimise and manage microgrids in the residential, services and industrial sectors: the objective was to facilitate the *integration and remote management* of microgrid elements through a large-scale network of embedded systems that use real-time energy measurements to dynamically optimise power demand and supply. The DEMANES solution provided system self-awareness by means of performance monitoring, runtime functional contract checking, monitoring of real-time properties and reconfiguration, enabling the *intelligent remote management* of vertical application in industrial systems, nomadic environments, private spaces and public infrastructure.

A significant advancement in **remote control and management has been focused on SoS**, which presents the highest level of complexity and heterogeneity in terms of components, connectivity, applications, involved stakeholders, etc. SAFECOP, for example, proposed a solution for systems that rely on wireless communication, have multiple stakeholders (but without a leading player), use dynamic system definitions and operate in unpredictable environments. The proposed solution was based on *cooperating CPS and provided a runtime manager able to detect abnormal behaviours at runtime*, triggering, if needed, a safe degraded operation mode. In the Arrowhead project, the Arrowhead Framework was adopted in conjunction with Eclipse Kura and Kapua to develop a *remote management solution*, intended to ensure the full remote control of a fleet of heterogeneous charging stations for electric vehicles. The remote control and management functionalities were published on the framework as Arrowhead standard services and made available to third parties for the development of electromobility and cross-domain applications. By contrast, eScop proposed the adoption of semantics to improve the remote management capabilities of the IoT platform and developed a modular, fully open solution for the *operational remote control of manufacturing equipment*. The objective was to ensure the simple and fast commissioning of new plants, promote the "plug & produce" model for the inclusion of new equipment and replace the traditional remote control, based on hierarchical hardware architecture, with a single level fleet of embedded systems and an interoperable set of services semantically described.

Another fundamental functionality of IoT/SoS platforms, which is complementary to the remote control and management of the IoT/SoS infrastructure, is the **management and control of the data streams** flowing from the edge of IoT or from intermediate sources that are processed in the nodes of the IoT/SoS infrastructure and delivered to other nodes or to the cloud/data centres at the enterprise level. From SOFIA semantic information brokers, through Arrowhead Framework services for information flow and processing, to Productive 4.0 SoS-based system architecture and platform for digitalisation, almost every ARTEMIS and ECSEL project that addressed the issues of IoT/SoS management also ensured the management of information flow.

To provide these primary functionalities, many projects developed platforms based on **service-oriented architectures**, adopted as a technical solution to manage in a standard and open way the information (both data and metadata) produced, shared and consumed in the IoT/SoS infrastructure (e.g. SOFIA, eSONIA, ME^{3}GAS, Arrowhead, eScop, Productive 4.0, etc.). Shifting to a more abstract level, almost all the ARTEMIS and ECSEL projects that contributed to this research stream spent a significant effort for the creation of high-level and added-value services that *valorise the collected information and transform it in potential revenues*. The implementation of high-level services that can be directly used by the end-user or that can be composed to develop single- and cross-domain applications highlights the importance reserved in ARTEMIS and ECSEL projects for the final impact of technologies and solutions, specifically in the area of the value chain that is expected to generate the largest profits.

Similarly, attention to **trustworthiness at platform level** has been present since the very beginning of ARTEMIS initiative. From SOFIA security features of the semantic information broker and nSHIELD security, privacy and dependability centred solution, to DEWI/SCOTT secure and dependable "communication bubbles", Arrowhead core service for security and Productive 4.0 platform … almost every project involved in this research stream addressed trust, in its different aspects.

But the real advantages of IoT/SoS platforms emerge from the *seamless integration of different IoT technologies, devices, connectivity, deployment support, operation support, etc.* in a single **end-to-end solution**, across all the levels of the IoT stack and across the product lifecycle. Many ARTEMIS and ECSEL projects tried to develop end-to-end IoT solutions, initially and tentatively focused on WSN, which represented a good playground to test technologies and solutions that could be further developed to scale-up to entire IoT or SoS infrastructures. EMMON, for example, covered the technology chain from the operating system to middleware and from protocols to system integration in order to support *large geographical deployment of thousands of wireless sensor nodes*. SMART was focused on WSN-based smart environment and developed a complete framework composed of a sensor network hardware, a middleware and

software for WSN applications. With a similar approach, ME^{3}GAS focused on the specific sector of energy management and proposed solution based on a connected smart meter, a service-oriented energy-aware middleware and services/applications for multiple tariffs and payment modalities, remote gas cut off, security alarms, etc. With IoE, the research started looking to more general, *heterogeneous and complex systems*: starting from a novel smart electricity meter with multiple interfaces, the IoE end-to-end solution included a middleware running on multiservice gateways, to enable the seamless connectivity between the different domains of power grid, power plants, electric vehicles, smart buildings and services for advanced demand response and load shedding.

In the domain of **end-to-end solutions for IoT**, eScop aimed to realise a modular, fully open solution for the *operational control of manufacturing equipment*, composed of a hardware platform, an ontology-driven service-oriented architecture and a software for remote management and control, covering the entire value chain of the production automation industry. With-Me developed a complete solution for *personalised assistance*, from lifestyle improvement to primary, secondary and tertiary prevention and care: the solution was intended to manage a heterogeneous ecosystem of embedded devices (including multi-purpose consumer electronics, dedicated health equipment), external information sources providing sensor input from the environment, general information, personal feedback, and servers providing the necessary computational environment for services and applications. MANTIS focused more on *proactive maintenance*, and proposed a platform including new sensing devices for maintenance monitoring, virtual plug & play, configuration and deployment functionalities, secure wireless connectivity, remote control and management, distributed (local) decision making, cloud platform integration and data aggregation, processing and analysis. Recently, AFarCloud provided a distributed platform for *autonomous farming*, which will allow the integration and cooperation of CPS in real-time for increased agriculture efficiency, productivity, animal health, food quality and reduced farm labour costs. The platform enables farming robot cooperation, is integrated with the farm management software and supports monitoring and decision-making, based on big data and real time data mining techniques. While Productive 4.0 is entirely focusing on *Industry 4.0*, with a multi-sided cross-domain platform for manufacturing networks that includes IoT enabling components (e.g. smart sensors and actuators), an SoS-based architecture supporting automation and digitalisation for sustainable production, simulation models for digital production, supply chain networks and product lifecycle management, solutions for production planning, virtualising, operating and controlling, distributed data analytics services to handle big data in real-time and reference implementations.

Some projects decided to focus specifically on **trust** that, being a transversal and interdisciplinary aspect of IoT and SoS, requires end-to-end solutions that cover the entire IoT/SoS stack. nSHIELD, for example, proposed an *end-to-end solution for modular and composable security, privacy and dependability*, covering both the node, network, middleware and overlay layers of the IoT stack, providing system maintenance and evolution support, in cross-domain environments. DEWI and SCOTT research activities generated nearly *50 technical building blocks for security/safety*, distributed cloud integration, energy efficiency/autonomy of devices and reference architecture/implementations, smart wireless devices which, combined with a standardised multi-domain reference architecture, facilitate composability of systems as well as cross-domain sharing of trustable wireless technologies and services.

> *SoS are large-scale integrated and collaborative systems which are independently operable on their own, but are networked together for a certain period of time to achieve a higher goal (e.g. costs, performance, robustness, etc.) They are operationally and managerially independent, and typically evolve, changing their behaviour, but trying to remain interoperable.*

Eventually, some projects tried to address the domain of **SoS**, considering a super set of technologies, solutions and vertical applications that include but are not limited to IoT. In this context, ACCUS aimed to provide an *integration*

and coordination platform for urban heterogeneous and distributed systems in order to optimise their combined performance and manage their evolving behaviours. In addition, the project developed an adaptive and cooperative control architecture and corresponding algorithms for urban subsystems. The ACCUS platform made it possible to build monitoring, management and control applications across urban systems. The platform provided methodologies and tools for creating *real-time collaborative SoS applications* and included a reference system architecture, a software platform, design tools for information extraction and control, a model-based design environment for application development, validation tools for application development, monitoring and visualisation tools to track the system-level operations. Arrowhead focused on *SoS collaborative automation* and developed a SOA oriented framework, a technical framework, solutions for integration with legacy systems, and the implementation and evaluation of cooperative automation through real experiments in five applicative domains: production (manufacturing, process, energy), smart buildings and infrastructures, electro-mobility, energy production and the energy virtual market. The Arrowhead Framework improves SoS interoperability and makes it possible for new systems, new devices and legacy systems to integrate and interact based on a loosely coupled service-based approach, thus enabling service-based collaborative automation. SAFECOP targeted safe cooperation based on wireless communication in SoS, providing a runtime manager to detect abnormal behaviours at runtime, triggering, if needed, the appropriate countermeasures. The proposed solution was oriented to provide *safety assurance for SoS* in the healthcare, maritime, vehicle-to-vehicle and vehicle-to-infrastructure sectors. Recently, Productive 4.0 adopted and extended the Arrowhead Framework to develop an *SoS-oriented architecture and platform*, supporting automation and digitalisation for sustainable production: the objective is to combine and manage a collection of dedicated systems and pool their capabilities to generate new and more efficient complex systems. The domain-independent platform enhances automation and digitalisation, application development, deployment, operation and maintenance. Covering fields like seamless integration of design, manufacturing and lifecycle management, the platform boosts the overall SoS efficiency. Eventually, like nSHIELD, DEWI and SCOTT, the AQUAS project investigates the challenges arising from the *inter-dependence of safety, security and performance in SoS*. AQUAS proposes solutions for a holistic approach to safety, security and performance co-engineering through a domain-flexible framework, supporting the entire product lifecycle.

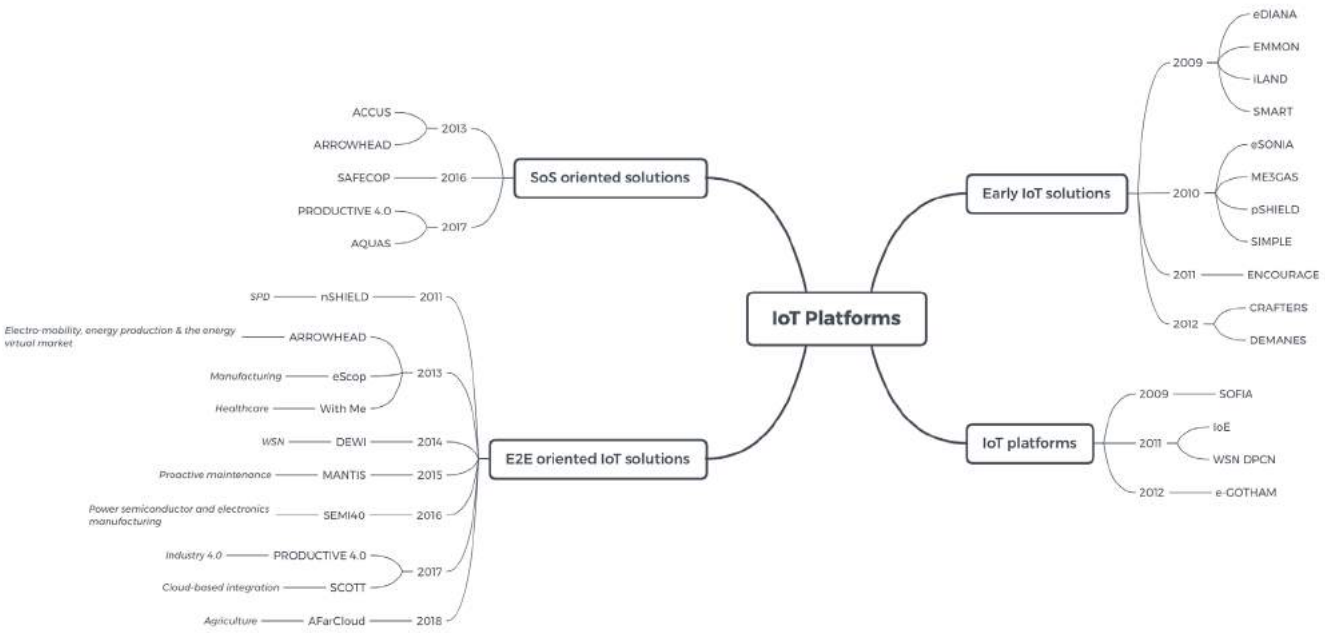


FIGURE 28 — *ARTEMIS/ECSEL projects that contributed to the IoT/SoS platforms research stream by research focus area and call.*

Considering the complexity of IoT/SoS platforms, their evolution will touch many technology areas, including:

- Decision management and support systems.
- Integration of IoT services into business processes.
- Process design, implementation and automatic deployment. Process choreography.
- Open SoS Integration platforms.
- Distributed control & simulation, including predictive models, real-time and non-real-time simulation.
- Cross-domain service and applications creation.
- Automatic added-value service creation.
- Integration with enterprise level functionalities.

Engineering support

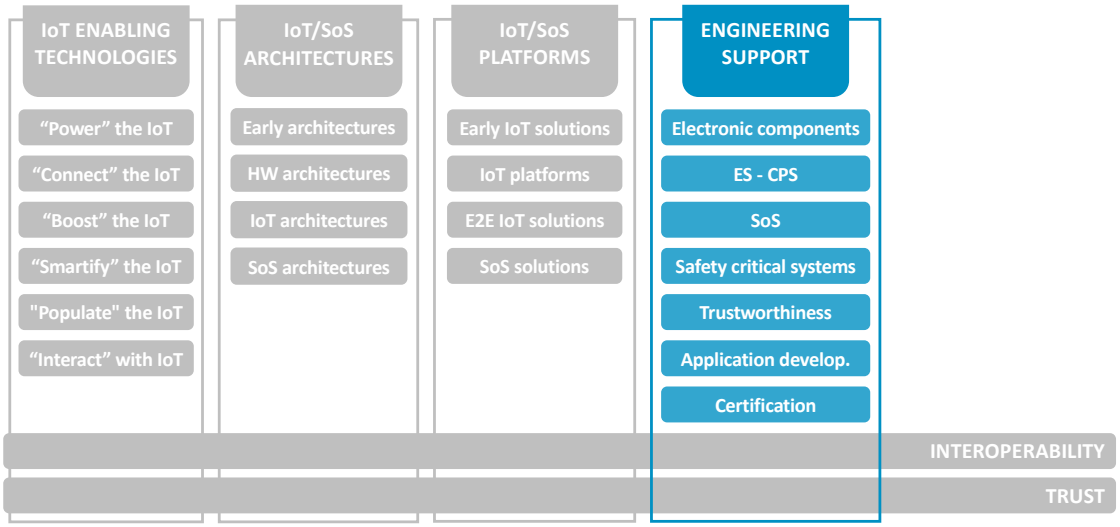


FIGURE 29 — *Engineering support research stream.*

Engineering support is a key element for successful market, for the value consolidation of products and for the sustainable evolution of an IoT/SoS solution. Adequate support in each phase of the lifecycle is a mandatory prerequisite to consider the IoT/SoS solution a real product. Lifecycle support impacts on the manufacturer of the solution, on the customers, on third parties, on the final user and represents a fundamental factor for the existence of a healthy value chain/network.

> *The complexity and interdisciplinarity of IoT and SoS require more engineering support than "conventional" products.*

Moving from research results to real products requires engineering support, across the entire lifecycle: from product conception, to development, deployment & commissioning, operation, maintenance and final retirement and recycling.

Figure 30 illustrates the typical engineering process adopted in industry automation, a process flexible enough to also be used in other vertical domains. For several aspects engineering is the point of convergence of the value chain and of the design methods & tools adopted in the engineering process itself. IoT end-to-end solutions are rarely developed by a single vendor; their complexity and the interdisciplinary expertise needed to build, sell, operate and maintain similar products requires a multi-stakeholder approach, that implies the partial or full involvement of the value chain. *The engineering process clarifies how the stakeholders cooperate to develop, sell, operate and maintain the IoT/SoS solution, in which phases they are involved, which activities they share, what are the boundaries between them, etc.* The engineering process "naturally" orchestrates the value chain and the stakeholders involved, across the entire life of the IoT end-to-end solution. The design methods, toolchains and tools adopted by the stakeholders represent the inner "spine" of the engineering process, the operative dimension of each engineering phase.

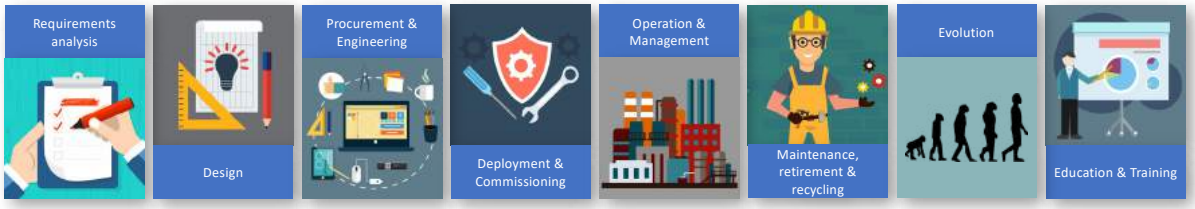


FIGURE 30 — *Example of engineering process model (IEC 81346 extension for IoT/SoS automation of lifecycle management).*

The availability of tools that support and automate the **requirements analysis and functional design** speeds up the iterative process required to enter and understand the customer domain, improve the quality of the analysis and of the subsequent functional design, help limit potential issues at contractual level, reduce the number of development cycles and, therefore, globally contribute to reducing costs and time to market.

Design methods and tools represent a fundamental counterpart of IoT/SoS solutions, and their importance is progressively pushing to integrate them in the solution itself: it is rather difficult to ensure lifecycle support without a tight integration of design methods and tools in the engineering process and directly in the final product. For example, the cyclical process of firmware updates in a fleet of devices, based on the assisted/automated bugs identification, correction and firmware provisioning, is a mandatory requirement for an IoT solution and represents a clear example of a fundamental functionality only available through the engineering automation.

Procurement and engineering automation allow also a strict and productive integration between these two phases of the engineering process. The integration is required from the early stage of product development and is crucial to ensure the best selection of suppliers regarding both technical and economic aspects, to avoid the use of costly self-made components that, instead, can be found directly in the market, to promote global sourcing and to allow engineers to focus on innovation.

Considering the complexity of IoT/SoS solutions, of the respective artefacts and the adopted technologies, we cannot imagine the design and development phases without a certain level of automation: IoT and SoS solutions would not exist without *continuous engineering*. Engineering automation improves the quality of the product, allows engineers to be creative while satisfying the technical requirements of a product, optimises teamwork, significantly reduces the time to market, etc. The availability of engineering tools promotes modularity and reuse, simplifying the process of design partitioning, module identification, design and development, creating new products and solutions based on the reuse of existing modules, optimising costs, etc.: *the concepts of modularity and reuse are fundamental in the IoT and SoS domains.*

Deployment and commissioning are critical phases of the product lifecycle, specifically for IoT and SoS, which are geographically distributed and networked, characterised by a rich diversity of artefacts and subsystems, multi-layered, multi-brand, etc. Engineering tools allow this complexity to be kept under control, simplifying and optimising the configuration and installation, and automating the test and tuning process that are brought to the final acceptance test before operations.

Engineering tools play a fundamental role in selecting and planning resources, defining targets, configuration, customisation and planning and executing installation, the definition of the test set and debugging procedures, failure identification and quick solution before entering the "go-live" final process. As for the design & development phases, real IoT/SoS solution cannot exist without the automation and support of deployment and commissioning.

Operations support, management and maintenance of the IoT/SoS are required to ensure the delivery of cost-efficient high-quality services/applications to customers. Operation and management can be considered from two very different perspectives:

- IoT/SoS as a solution to improve operation and management of a specific vertical application, e.g. an IoT infrastructure used to monitor and manage the operation of a manufacturing plant.
- The IoT/SoS infrastructure itself considered as a system that must be monitored and managed, e.g. a multi-service gateway in charge of telemetry activities must be continuously monitored and sometimes requires reconfiguration, updates, etc.

As a tool IoT/SoS becomes part of the engineering process and is adopted to enable the digitalisation of a wide spectrum of vertical domains, introducing functionalities like intelligent assets and equipment management, connect assets to processes, improve the integration of plants, increase productivity, ensure the continuity of the cognitive process efficiently collecting and storing information, optimise resources, etc. IoT is an engineering tool that becomes crucial for *maintenance activities* because its sensing capabilities allow detection of problems in an early stage, limiting their effect on safety, security, productivity and efficiency. IoT enables predictive and preventive maintenance, avoiding production delays and improving production line performance, reducing equipment downtime, increasing process efficiency and speeding up equipment repairs and, finally, retirement and recycling.

As a system, IoT and SoS requires engineering tools and integrated functionalities to manage their operation and maintenance: device/asset onboarding, enrolment, provisioning and deployment, configuration, control, management and maintenance, IoT infrastructure control, fleet management and maintenance, repairs and, finally, retirement and recycling.

Evolution means that the IoT/SoS solution is modified during or after operations to meet changing customer requirements, correct bugs and issues, architectural changes, technology evolution, etc. The automation of the engineering process and the availability of design methods and tools that support the entire lifecycle is a key element to ensuring the evolution of IoT and SoS. Engineering support ensures evolution at different levels of complexity and abstraction: hardware and software modularity, layered and abstraction-driven design, re-configurability, automation of bug identification and correction process, automatic provisioning, etc. *The evolution step is extremely important for consolidating the achievements obtained in the IoT domain and progressively move to the wider context of system of systems (SoS).*

Finally, the overall competitiveness of the IoT/SoS domain is strictly dependent on labour costs, on the competencies of professionals and on their productivity: investments in knowledge play a key role in this delicate equation. The digitalisation process implies massive changes and requires a large number of engineers and other professionals with appropriate competencies: in this regard, **training and education** currently represent a major concern because the evolution rate of technologies is not mirrored by a similar preparation of professionals. Unfortunately, the uptake of technologies strongly depends on professional expertise, and a similar loop has a negative impact on the final success of IoT/SoS solutions. The availability of training material on IoT/SoS and about the engineering process is fundamental to ensure the fast adoption of technologies, the creation of communities, the efficiency of engineering and globally to reduce the investment costs of digitalisation. The costs of education and training are definitely lower than the effects of losing competitiveness and business opportunities.

Almost every ARTEMIS and ECSEL project has devoted some resources to providing a certain level of engineering support for the developed technologies, therefore it is impossible to report here every contribution to this research stream: *the receptiveness to the importance of the engineering support reflects the industrial-driven DNA of ARTEMIS and ECSEL*. The engineering support provided in the projects focused on several topics, including:

- Design methods and tools for semiconductors, electronic components, multicore and SoC.
- Design, implementation, simulation, test, validation, operation management, etc. for:
  - Embedded and Cyber Physical Systems.
  - IoT and System of Systems.
  - Services and applications.
- Engineering tools for safety critical systems.
- Engineering tools intended to ensure trust.
- Certification process simplification.
- Education & professional training.

In ARTEMIS and ECSEL projects, specifically in the initial calls, a large space has been reserved to ensure adequate **support to the new computing architectures** adopted in smart sensors, IoT devices, multiservice gateway for edge computing, etc. Considering the increasing computing requirements of IoT, specifically on the edge, it is indeed a key factor to introduce new multicore CPUs, accelerators, SoC, etc., but it is fundamental also to provide the engineering support to simplify their design and integration in IoT devices and, in particular, to enable the development of applications that take advantage of their potentialities. For examples, the SCALOPES project tried to enable an industrially sustainable path for the evolution of low-power, multicore computing platforms for communication infrastructure, surveillance systems, smart mobile terminals, stationary video & entertainment. The project developed solutions for energy and resource management, low-energy design methods and runtime methods, as well as *standard API between hardware and low-level software*. ASAM project focused on a uniform process for the automatic architecture synthesis and application mapping of heterogeneous multi-processor embedded systems based on adaptable and extendable ASIPs. The project defined a new unified design methodology, as well as, related *automated synthesis and prototyping toolchains*, allowing rapid exploration of the high-level algorithm and architecture design spaces as well as efficient automation of the final system synthesis and, consequently, quick development of multi-domain high-quality designs. The project provided *support also for application parallelisation, partitioning, scheduling and mapping*, needed to facilitate the design-space exploration and to deliver applications running efficiently on heterogeneous multi-processor platforms.

> *The study of engineering support and the development of methodologies, toolchains and tools followed the chronological evolution of the ECS domain, focusing initially on the support for specific technologies and gradually becoming more comprehensive, towards the full support for end-to-end IoT and SoS solutions, across their entire lifecycle.*

A similar **flexibility in the engineering process** is what is required to support rapidly evolving and demanding markets like IoT and SoS. SMECY focused specifically on the support for multicore technologies by developing new *programming technologies enabling the exploitation of many (hundreds of) core architectures*, introducing massively parallel computing environments whose improved performance, energy and cost characteristics are fundamental for many IoT vertical market. CRAFTERS further extended the engineering support proposing a holistically designed

ecosystem, from application to silicon, that provides a tightly integrated multi-vendor solution along with a tool chain that complements existing standards. The projects implemented a *complete multicore development environment* that allows the selection of the best implementation strategy depending on the specific application. The development ecosystem included the extension of model-based specification standards (such as MARTE) and the development of hardware profilers, early-estimation techniques, performance estimators, verification frameworks and parallelising compilers, but also tools at middleware level including runtime environment, scheduling and hardware management. The project also addressed the development of a multicore platform that includes support for the runtime environment. The development ecosystem covered many areas of engineering, such as compiler-generated parallelism and high application portability, holistically optimised system services through technology aware hardware/software co-design, and system-wide real-time support and timing exposure through abstraction levels. With a similar approach, PRIME aimed at supporting an open *Ultra Low Power (ULP) Technology Platform*, containing all necessary design, architectural blocks and components required in IoT devices. EMC^2 extended the focus to mixed criticality applications in real-time conditions, with scalability and utmost flexibility, full-scale deployment and management of integrated tool chains, across the lifecycle. The project intended to promote the adoption of multicore technology in many vertical domains, including avionics, space, automotive, railway, shipping, medical, energy, industry automation, etc.

More generally, shifting to the area of **engineering support for the creation of SoS**, iFEST specified and developed an *integration framework for establishing and maintaining tool chains* for the engineering of complex industrial embedded systems with specific emphasis on open tool chains for HW/SW co-design of heterogeneous and multicore solutions, and life cycle support for an expected operational life time of several decades. The proposed solution allows engineers to explore the architectural design space at a high level of abstraction, select a cost-effective design, and, from the abstract models, produce semi-automatically the hardware and software implementations in a cost-effective balance. iFEST integrated tools from the world of model-driven engineering with traditional HW/SW co-design tools. WSN-DPCM represents an example focused on a different IoT enabling technology: WSN. The project developed a full platform that includes a middleware for heterogeneous wireless technologies and an *integrated engineering toolset for development, planning, commissioning and maintenance activities* for expert and non-expert users. It offered an end-to-end integrated toolchain to promote a true model-driven architecture in all design and operational views of a WSN. The integrated toolset extends beyond the graphical user interface and ensures tool interoperability, and supports model-based functionality composition, propagation and back-annotation of changes among the various tool views. The integrated environment is supported by the middleware that provides a multi-level framework including functionality composition and adaptation. Leveraging on the middleware, the integrated environment allows the WSN application developers to raise the focus of their efforts from hardware, platforms, tool details and implementation to the application business logic.

The complexity of an IoT device requires specific solutions to **simplify and make its design and development more efficient**. Frequently, to manage this complexity the solution relies on component-based design, development and execution. The CESAR project, for example, developed a seamless tool chain (CESAR Reference Technology Platform - RTP) based on the integration of methods and tools for requirements engineering, methods and tools for component-based development providing multi views and multi criteria, and for system design engineering. The objective was the significant reduction of costs by up to 50% for the development of safety-critical systems while ensuring the quality and safety properties. The CHARTER project developed concepts, methods and tools for embedded systems design and deployment, conceived to manage their complexity and substantially improve the development, verification and certification of critical embedded systems. This category of systems is gradually penetrating our lives, therefore it is fundamental to ensure they satisfy governmental regulations, certification, verification, security and safety standards, etc. CHARTER proposed a *Quality-Embedded Development (QED) approach*, based on real-time Java, model-driven development, rule-based compilation and formal verification that, when combined, can bring embedded systems certification to a new level. CHESS developed model-driven solutions, integrating them in component-based execution frameworks, assessing their applicability from the perspective of

the telecommunications, space, railways and automotive domains, and verifying their performance through the elaboration of significant use cases from industry. With this approach, CHESS aims to boost the control of complexity, reuse, robustness and quality as well as simplified maintenance. Building *languages to model and tools to evaluate extra-functional properties* will reduce the costs and risks of development and deployment. *Combining component-based development and model-driven engineering*, CHESS intended to simplify the development of components that can be certified or qualified individually to guarantee the required level of service in operation, preserve this level also when the components are assembled and address extra-functional characteristics (i.e. safety, reliability, performance).

The complexity of providing support for the engineering of IoT further increases when we consider the entire IoT infrastructure, entering the domain of **IoT platform engineering**. The necessity of design methodologies and tools for IoT platforms, in their widest meaning and forms, as well as the necessity of the design and development of services and applications based on the functionalities offered by IoT platforms, has been always considered extremely important for the ARTEMIS and ECSEL projects. For example, the *SOFIA Open Innovation Platform (OIP) architecture and Application Development Kit (ADK)* was conceived to simplify the development of devices, services and applications that can interact across vendors and industry domain boundaries. The SOFIA Application Development Kit was multivendor, multiplatform (Windows, Linux, Android, etc.), multilanguage (C, C++, C#, J2SE, J2ME, etc.) and offered a set of engineering tools conceived to simplify the design and development of the smart devices and applications composing the smart environment. The eSONIA project aimed at defining reference models and develop tools to implement a services-oriented architecture in a factory environment for the continuous monitoring, diagnostics, prognostics and control of assets, regardless of their physical location. Similarly, DEMANES intended to provide a framework as well as component-based methods and tools for the development of runtime adaptive systems, enabling them to react to internal changes, changes in their environment, in user needs and in contexts. DEMANES developed a smart integrated tool chain, reusable components and a framework for the design, implementation, testing, validation and operation of adaptive networked embedded systems. The project also delivered a model-driven design methodology and reference designs for dependable, real-time distributed systems and a pilot implementation of a runtime platform for applications designed according to the methodology developed. Following a similar approach, ACCUS implemented a development platform offering methodologies and tools for creating real-time collaborative applications for SoS: the platform allowed to build applications across urban systems like monitoring, management and control, that can extend beyond the borders of the individual subsystems. The methodologies and tools included a reference system architecture, a software platform, design tools for information extraction and control, a model-based design environment for application development, validation tools for application development, monitoring and visualisation and tools to track the system-level operations. In a more focused vertical application, FitOptiVis tried to find a solution to balance the power demand and the performance of the increasingly complex distributed SoS, reflected in the growing number of sensors, actuators and other smart devices, their growing autonomy, and the increased need for performance. In the domain of low-latency image and video acquisition and processing, FitOptiVis developed a cross-domain approach covering a reference architecture, supported by low-power, high-performance smart devices, and by methods and tools for combined design-time and runtime multi-objective optimisation within system and environment constraints. More recently, Productive 4.0 is *examining methods, concepts and technologies for service-oriented architectures* as well as for components and infrastructure in IoT. The proposed solution is intended to be used in three interlocked process pillars for managing the supply chains, the product life cycle and the digital production, providing companies with fundamental tools necessary for the digital transformation.

The IoT components modelling and simulation methods as well as tool chains for cross-lifecycle and cross-domain digitalisation are suitable solutions for **linking all stages of a product lifecycle in a sustainable way**. MegaM@Rt project is developing a framework including methods and tools for *continuous development and validation* leveraging the advantages of scalable model-based methods to provide benefits in significantly improved productivity, quality and predictability of large and complex industrial systems. The project planned to develop scalable methods and tools for modelling of functional and non-functional properties such as performance, consumption, security and

safety with mechanisms for representation of results of runtime analysis; methods and tools for application validation at runtime including verification and online testing; an infrastructure for efficient handling and management of numerous, heterogeneous and large models potentially covering several functional and non-functional domains.

The engineering support for IoT and SoS platform typically involves the entire engineering process and highlights the problem of creating **integrated and interoperable tools and toolchains**. Currently, the ad-hoc integration of tools by creating proprietary interfaces between each pair of tools does not scale, since the number of required interfaces grows exponentially with the number of employed tools: this simple approach is not suitable for IoT and SoS engineering. Moreover, the resulting toolchains become extremely vulnerable to common changes, like version upgrades from tool vendors, requiring a significant effort to maintain the interfaces. The *lack of open and common interoperability between tools* plays a critical role from this perspective. In this context, CRYSTAL tried to push the Interoperability Specification towards standardisation. Within and across the application domains of aerospace, automotive, healthcare and rail, CRYSTAL covered the entire software product life cycle and supported product line development towards ready-for-use industrial tool chains. The objective was to enable the processes of developing, governing and operating modern embedded systems to become effective and efficient, through collaboration among the respective stakeholders and interoperability between the tools they are using. The aim was to create a user platform across value chains and industries, thus promoting the digital networking of manufacturing companies, production machines and products. In iFEST, an integration framework and two tool chains permit efficient tool replacement within the toolchain, addressing issues such as tool obsolescence and tool lock-in: the intention is to shift from low efficiency in tool usage to a much more effective tool chain.

The importance of these concepts emerged clearly in Arrowhead and Productive 4.0 projects that, in the development of the Arrowhead Framework, experienced the issues *emerging from the lack of automation in the engineering process*: recently, the Arrowhead Tools project has been focusing primarily on digitalisation and automation solutions for European industry, enabling the IT/OT integration with the introduction of an open source platform for the design and runtime engineering of IoT and System of Systems. The project will provide engineering processes, an integration platform, tools and tool chains for the cost-efficient development of digitalisation, connectivity and automation system solutions in various fields of application.

Engineering trust in IoT and SoS is a mandatory requirement and, being trust a transversal aspect of IoT and SoS, **design methods and tools should provide trust support at any level of the stack and across the product lifecycle**. *Trust by design* represents a crucial factor to improve the acceptance of IoT technologies and speed up the market penetration. Adopting good practices, following guidelines and respecting standards oriented to trust[38] is a prerequisite for the creation of a trustworthy IoT ecosystem, but this prerequisite must be complemented with adequate engineering support specifically conceived to ensure the level of trustworthiness required by the vertical application. Considering also the complexity of the IoT ecosystem whereby almost every part of the IoT infrastructure is exposed to a rapidly evolving panorama of threats related to security, privacy, dependability, integrity, …, *it is crucial to ensure the continuous engineering required to improve the product and set up the countermeasures that make it resilient to these evolving menaces*: **continuous engineering of trust represents an important challenge for IoT and SoS**. The engineering support for trust has a central position in this research stream, as confirmed by the large number of ARTEMIS and ECSEL projects directly involved in it. Starting from the initial ARTEMIS calls, pSHIELD and nSHIELD projects played a significant role in sensitising the community about security, privacy and dependability (SPD), considered as *built-in functionalities rather than add-on elements*, that frequently lack of a system level perspective. The projects developed an SPD-native reference *architectural framework*, supporting all the levels of the IoT stack, with *integrated and composable SPD metrics* that simplify the development cycles of SPD in IoT because the qualification, (re)certification and (re)validation process of a SHIELD framework is faster and easier. In this solution, the

[38] *https://www.internetsociety.org/iot/trust-framework/*

native support for composability of SPD introduces a system level perspective, allowing the improvement of the SPD level of the overall IoT solution with minimum engineering effort. In the SESAMO project a *component-oriented design methodology* based on model-driven technology addressed the safety and security aspects of networked embedded systems in multiple domains (e.g., avionics, transportation, industry control, mobile medical). The project provided design guidelines, an effective toolchain and decision support strategies that allow critical situations to be solved during system operations. The core of the proposed solution was a rigorous framework that enables joint reasoning about the required safety and security properties and the resolution of any conflicting constraints. SESAMO expected to produce a 15% reduction in development cycles and the re-validation and re-certification of systems after changes. The adoption of *model-driven engineering* also characterised the CONCERTO project that proposed practices, technologies, iterative and incremental development to better address safety, reliability, performance, energy usage and other extra-functional properties of embedded applications, while guaranteeing correctness as component-based systems are assembled. The CONCERTO framework integrated *correctness-by-construction* for multicore systems with innovative model-to-code transformation techniques and a multi-view, hierarchical cross-domain design space, able to enable a compositional approach for the next generation of complex, heterogeneous embedded systems. The framework supported simulation and early model-based analysis, with fully automated backward propagation of results to the user model, runtime monitoring of mission- and operation- critical, non-functional properties, such as energy consumption, on partitioned and multicore processor architectures. The objective was to provide advanced modelling capabilities to capture the full potential of new multicore platforms, while providing tools to ensure high quality and highly reliable systems. The AQUAS project investigated the challenges arising from the interdependence of safety, security and performance of systems and aims at efficient solutions for the entire product lifecycle. AQUAS addressed the issue of meeting the continuously growing requirements on security and performance while maintaining safety, with coordinated engineering based on a *holistic approach to safety, security, performance co-engineering* through a domain-flexible framework, supporting the entire product lifecycle. The SCOTT project focused more on creating trust in wireless solutions and increasing their social acceptance to exploit the full potential of IoT. SCOTT used a *standardised multi-domain reference architecture*, created in the predecessor project DEWI and being fully compliant with ISO 29182, and provided methods, tools and reference implementations capable of satisfying the project use case requirements for reliability, robustness, security and functional safety even in harsh and/or not trusted environments. A final example is the iDev40 project that introduces seamlessly integrated ECS development processes, safe and secure digital automation workflows, interoperable and inter-organisational network solutions as well as an enhanced transparency of data and intelligence that will lead to a reduction in the time to market race for ECS solutions.

Finally, the promotion of **standards development and adoption, the simplification and improvement of the certification process, specification assurance**, etc. could significantly benefit from design methods, toolchains and tools that provide support to these phases of the engineering process. AMASS, for example, focused on reducing time, costs and risks for assurance and (re)certification by adopting an *evolutionary compositional certification and cross-domain reuse approach*. The objective was to create an open tool platform, ecosystem and self-sustainable community for assurance and certification of CPS in industrial vertical markets characterised by rapidly changing features and needs (e.g. automotive, railway, aerospace, space, and energy). The goal is to lower certification costs adopting a novel holistic and reuse-oriented approach and supporting tools for architecture-driven assurance (fully compatible with standards such as AUTOSAR and IMA), multi-concern assurance (for co-analysis and co-assurance of e.g. security and safety aspects), and for seamless interoperability between assurance and engineering activities along with third-party activities (e.g. external assessments and supplier assurance). POLLUX proposed new approaches to standardisation, certification and qualification of new embedded systems architectures for high-efficiency, innovative mechatronic systems for electric vehicles. Another example is the CHARTER project that focuses on the critical embedded software systems that are commonly found in cars, aircraft, medical instruments and major industrial and utility plants. Since this category of software will be increasingly pervasive, it is vital that it *respects governmental regulations, international standards and certifications* in order to prevent any potential risk due to any malfunction, bug, etc. CHARTER proposed a solution to ensure the compliance of this software with the highest standards of

performance through formal certification procedures, using a Quality-Embedded Development (QED) approach, real-time Java, Model Driven Development, rule-based compilation and formal verification. This approach also enables the costs of cyclical and iterative software certification to be significantly reduced. Recently, SECREDAS started developing software for validating methodologies, reference architectures, components, suitable integration and verification approaches for automated systems in different domains. The project aims at *developing and enhancing trustworthiness*, particularly for the future European transportation and medical industries, and addresses also cross-domain cybersecurity and safety related technologies in the areas of automated systems in the medical, railway & aerospace sectors, as well as support cross-domain actions.

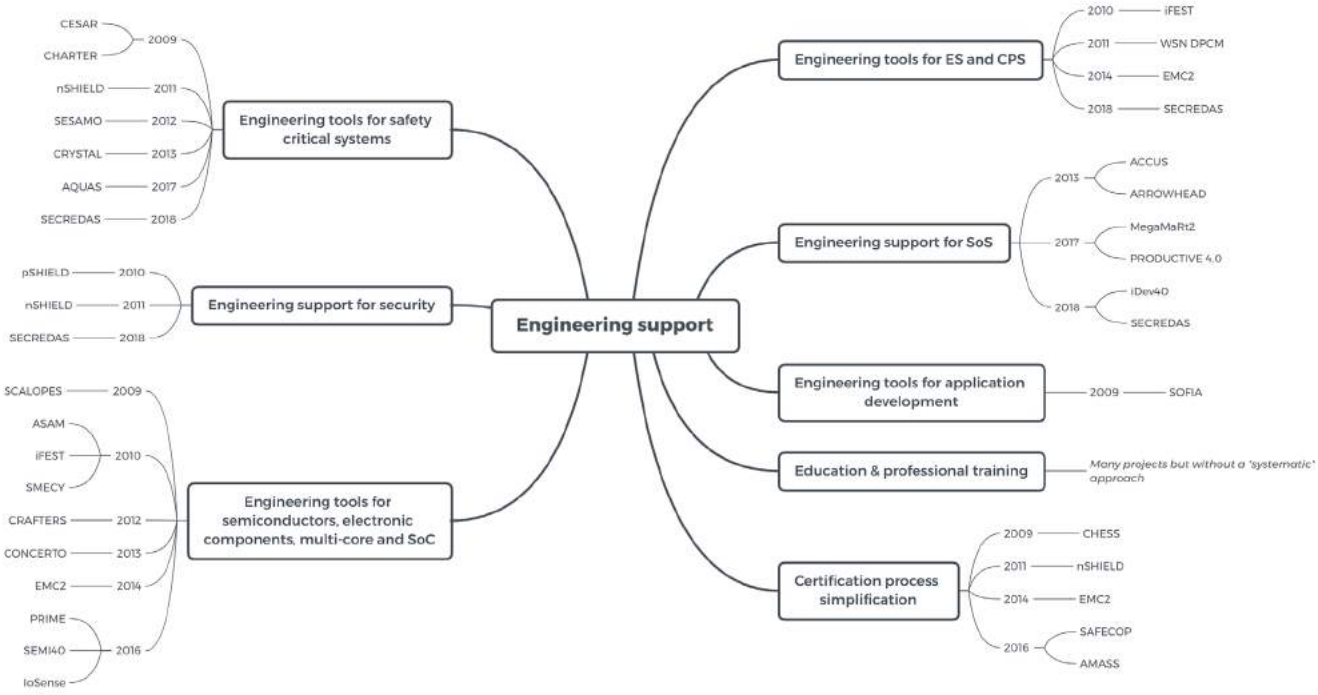
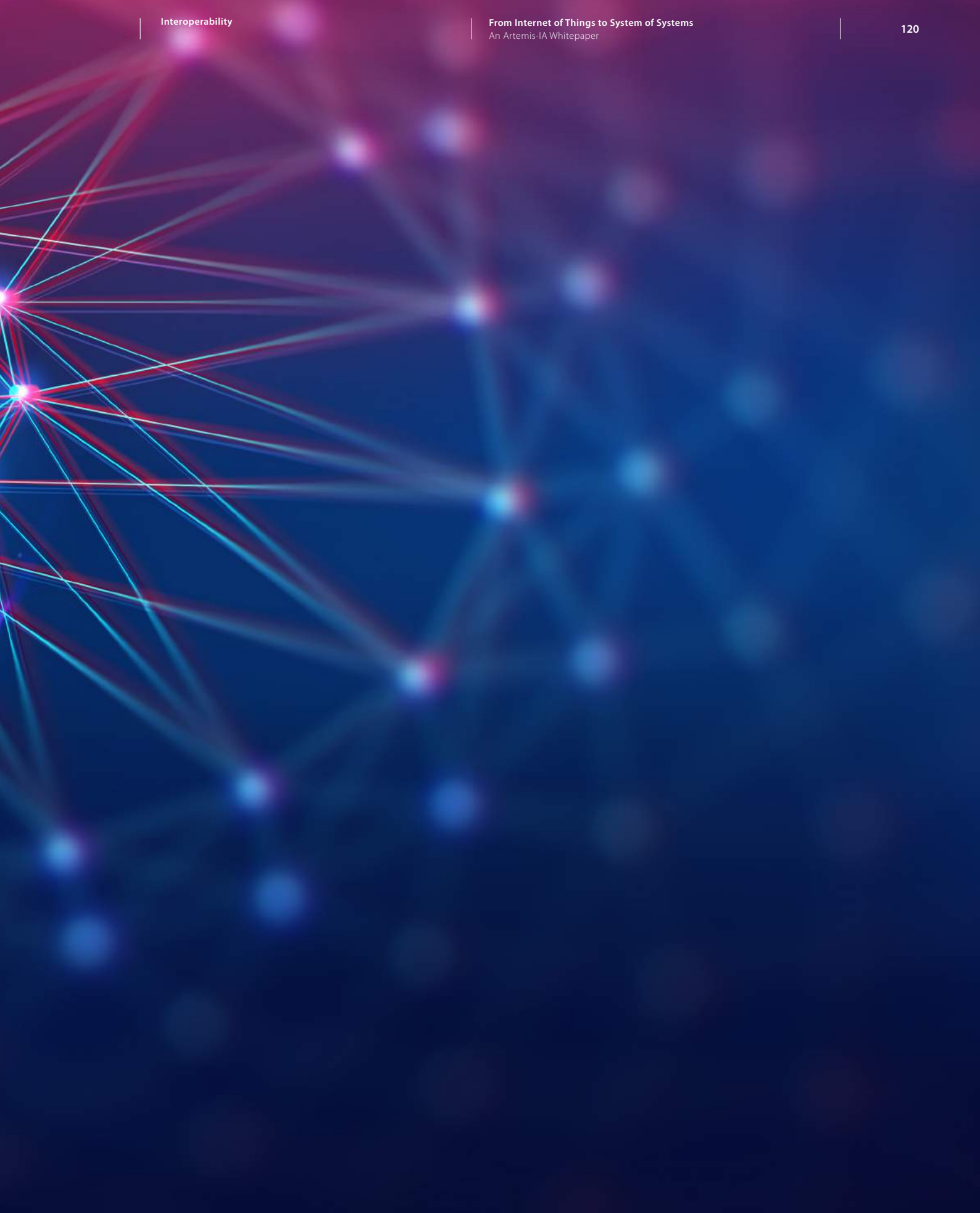


FIGURE 31 — *ARTEMIS/ECSEL projects that contributed to engineering support research stream by research focus area and call.*

Engineering support requires continuous evolution in order to follow the technology trends and to allow the adoption in future products of the results of research and innovation. In this research stream, many focus areas will require significant investments, including:

- Support for digital twin and digital thread. Virtual systems engineering.
- SoS engineering and management of multidimensional SoS solutions.
- Methods & tools, quality assurance, testing, validation & verification techniques and methods to support the engineering process on all levels of the systems hierarchy.
- Tools and toolchains interoperability.
- Engineering of automation and digitalisation solutions.
- Engineering support for large-scale embedded application.
- Introduction of machine autonomy in the engineering process, including AI driven autonomy.
- Model based software engineering.
- Shift to more agile, flexible and trustable design methods (agile development, continuous engineering, continuous certification, etc.).
- Methods and tools for development, integration and operation of IoT and SoS.



Interoperability

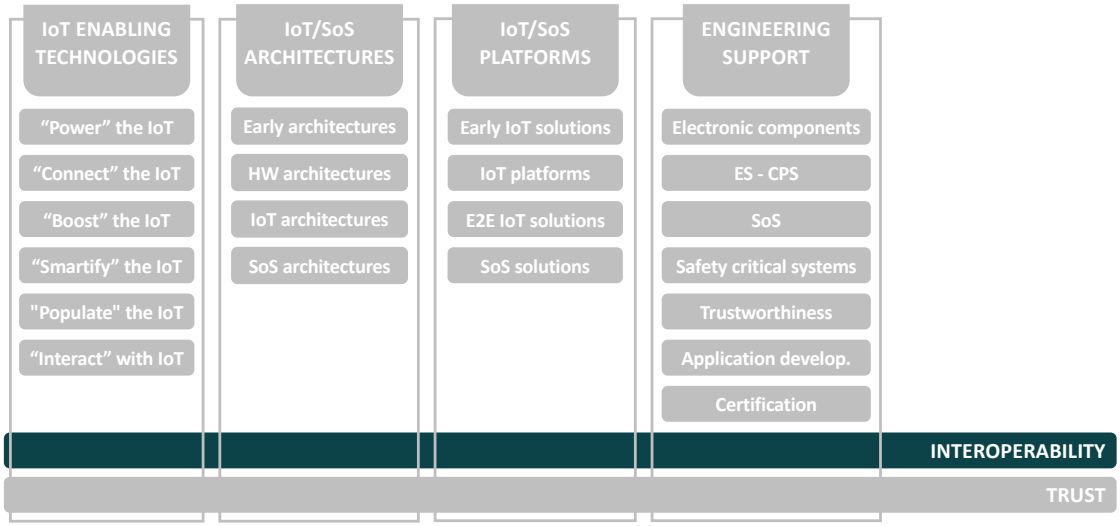


FIGURE 32 — *Interoperability research stream.*

Interoperability is the key element to inherently control the diversity that characterizes IoT and SoS and avoid the market fragmentation. The landscape of IoT solutions is overpopulated, with more than 600 platforms already in 2019[39] and a trend oriented to a further proliferation. In this landscape, each vendor tries to promote its own IoT solution, based on proprietary protocols and interfaces, low standards compliance, proprietary application frameworks and business logics that generate closed and vendor-specific ecosystems. However, the evolution of global connected markets is pointing in a different direction, highlighting the need to reduce the level of isolation of different silos, to increase the amount of shared information and to adopt IoT solutions that can seamlessly work together. In this regard, McKinsey[40] estimates that 40% of the potential benefits of IoT can be obtained with the interoperability between systems: **interoperability is an IoT technology enabler**.

> *Diversity in SoS is an indicator of innovation, richness and added value, it is not something to be solved, but an aspect to be embraced and managed. On the contrary, the technological fragmentation impacts on the market solidity and represents an obstacle for IoT/SoS uptake.*

[39] *IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally, IoT Analytics, December 2019*
[40] *Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) The internet of things: mapping the value beyond the hype. McKinsey global institute.*

IEEE provided a general definition of interoperability, as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged"[41]. *Interpreting this definition in the IoT domain, interoperability can be defined as the ability of two or more systems to communicate and share information and services.* The definition reveals also that interoperability is a transversal research stream because it affects the IoT/SoS at different levels: device, connectivity, architecture, data syntax, data semantic, platform, application and also at design and development level. *Interoperability also affects the developer, the vendor and the users in different ways*. The development of an IoT application is influenced by the data model and by the API or framework provided by the IoT platform(s) because the developer has to adapt both the programming model and the application to them, with a significant increase in complexity when the application is cross-platform and cross-domain. A lack of interoperability translates in higher development costs. From the vendor's perspective, this lack of interoperability appears initially as a protection of the IoT solution and of the investments required to develop and deliver it. But in the longer term, it is revealed to be a binding limitation that forces the vendor to always adopt the same devices, the same software and the same services, regardless of their quality, their stability, their adequacy, their costs, etc. In this case, an apparent protection of the IoT solution potentially reveals higher operational costs in the longer term, particularly for small and medium enterprises whose limited resources make it difficult to manually manage the lack of interoperability.

A general misconception tends to *reduce interoperability to standards*, intended as a definitive way to overcome interoperability issues. Standards could be beneficial for IoT and SoS but, in general, an interoperability solution does not necessarily have to be certifiable and standard, particularly for software and for the open-source community, where *standards are very frequently considered obstacles to innovation*. The basic starting point for interoperability is the identification of "common definitions" allowing components, products or entire systems to work together, regardless of whether these definitions respect a standard or not. In recent years, defining a standard for interoperability in IoT has been subject to many tentative efforts, but the market has neither accepted nor adopted any specific solution yet.

The difficulty in identifying a widely accepted solution is certainly also due to the different "personalities" of interoperability: indeed, interoperability can be considered at multiple levels, including technical (basic connectivity and network connectivity), syntactic (data exchange interoperability), semantic (understanding in the meaning of the data), pragmatic/dynamic (applicability of the information) and conceptual (shared view of the domain). Moreover, these levels transversally affect the components of the IoT solutions, devices, the information collected, the connectivity, the platforms and also the developments tools.

At device level, interoperability is primarily focused on the integration of heterogeneous artefacts, smart sensors, actuators, gateways, edge controllers, wearables, etc., which typically communicate with different protocols and which must coexist in the IoT infrastructure. The objective is to ensure the exchange of information between them and the ability to integrate new devices.

At network level, the IoT infrastructure relies on field communications and on wide area network connectivity. On the field, IoT devices typically rely on a plethora of wireless (for the large part short-ranged) and wired communications to connect the IoT devices on the edge of infrastructure. The multiplicity of connectivity options slightly reduces in the wide area network, allowing devices to connect to the enterprise level of the IoT infrastructure (cloud platforms, data centres, etc.). At network level, interoperability allows the seamless information exchange between different devices and systems, through different communication channels and with different protocols, ensuring performance, quality of service, scalability, security etc. of the network.

Entering the information domain, **syntactic and semantic interoperability** ensure that data exchanged between the components of the IoT infrastructure are correctly interpreted and understood. *Syntactic interoperability* ensures that

[41] *Radatz J, Geraci A, Katki F (1990) IEEE standard glossary of software engineering terminology.*

the data format and structure are interoperable: data is encoded and decoded following specific syntactic rules and, if the two parts of the IoT infrastructure that are interacting respect these rules, the interoperability is guaranteed. But this is not enough to ensure the information interoperability: the data model, the adopted units, the schema, that is, the meaning of information could not be understood by the interacting parts, although it is syntactically comprehensible. When the meaning of information is considered, *semantic interoperability* comes into the game: W3C defines semantic interoperability as "enabling different agents, services, and applications to exchange information, data and knowledge in a meaningful way, on and off the Web"[42].

Moving to **platform level**, interoperability is affected by many factors, ranging from the architecture of the IoT solution, the mechanism adopted for data and device management, the security requirements, the programming environment adopted to develop the solution and the data storage technologies, etc. Very frequently, platform interoperability is ensured by the IoT application because the developer takes the responsibility to mediate between the various API, libraries, information models, operating systems, storage solutions and programming languages. This approach brings us to the development of more complex application, one that can barely survive, and to the dynamicity of IoT, leading to higher engineering costs. To ensure more effective and inexpensive solutions, the interoperability should be taken into account from the very beginning of the platform development, from the architecture and its component, from the programming environment adopted, from the data model and from the data access/sharing mechanisms (e.g. Service Oriented Architectures, Open APIs, Semantic Web technologies, etc.).

Cross-platform interoperability is becoming even more important because the high-level services provided by different IoT vertical applications can be combined to create new and unforeseen cross-vertical applications, maximising the profits from information and providing added-value services to the final user.

Finally, interoperability also plays a fundamental role in the engineering process, with a significant impact on the reduction of engineering costs. **Interoperability in the engineering process** allows the automation of the engineering phases, reducing the human effort involved in the engineering process, reducing the engineering costs, both during the design and development phases and during operation and maintenance, improving the quality of the engineering process and its overall efficiency. Interoperability in a toolchain allows engineering tools to automatically and reliably exchange the information, reduces the effort required to manage the engineering process, enables continuous development, ensures the evolvability of the toolchain, reduces deployment, operational and maintenance costs.

ARTEMIS and ECSEL projects focused an all these levels of interoperability, trying to find solutions for:

- Hardware native interoperability or hardware support for interoperability.
- *Things* interoperability (e.g. highly distributed devices, complexity and heterogeneity management).
- Middleware/platform level interoperability.
- Software interoperability (e.g. application, user interface interoperability).
- Service level interoperability.
- Interoperability between systems.
- Engineering tools interoperability.

[42] *W3C, "W3C Semantic Integration & Interoperability Using RDF and OWL.", https://www.w3.org/2001/sw/BestPractices/ OEP/SemInt/.*

As anticipated, interoperability is an interdisciplinary research area and the technological solutions for interoperability result from the integration of the single technologies available in the various levels of the IoT stack. It is complex to provide **interoperability at the hardware level** but keeping in consideration interoperability during hardware design contributes to improved interoperability in the upper levels of the stack. For example, starting from off-the-shelf sensors and the RASIP processor, SMART developed a middleware for the seamless programming, configuration and management of the WSN infrastructure that improve the *interoperability of WSN*. Similarly, the CONNECT project developed solutions for *interoperability of smart grid communication infrastructures* with a particular emphasis on the enhanced security in order to protect this kind of infrastructure against attacks. Moreover, the improved interoperability level simplifies the development of advanced control algorithms to monitor renewable energy sources, local storage and electric vehicles for peak demand reduction and optimisation of local generation, consumption and storage of energy.

Considering the **interoperability of IoT devices** (*things* interoperability), different sectors and domains have been addressed in the ARTEMIS and ECSEL projects. For example, ME^{3}GAS developed and validated an initial instantiation of a new architecture and the corresponding communication platform to enable the *flexible and evolvable interoperation* of smart gas metering systems (gas Advanced Metering Infrastructure), including the smart meters, end user displays, data concentrators, and utilities information and control systems. In the same domain, eDIANA focused on cross domain connectivity and communication capabilities, working on the *interoperability of highly distributed devices*, providing a reference architecture for a network of composable, interoperable and layered embedded systems. eDIANA adopted the architecture to connect the building as a node in the producer/consumer electrical grid. eSONIA proposed to adopt the SOA paradigm and deploy *composable and interoperable web services* in a multitude of different computing platforms, including embedded devices and low-power wireless devices. DEWI contributed to establishing a standard for wireless systems engineering in the certification and security context, which improves *interoperability through conformity with both domain-specific and domain-independent standards*. Finally, CHIRON tried to identify the information required by IoT device manufacturers to build *devices and services that are interoperable* and user-centred (sensors, home networks, health computer platforms, 3D and virtual reality solutions and contents). Starting from this analysis, the project defined a reference architecture for personal healthcare ensuring the interoperability between heterogeneous devices and services, reliable and secure patient data management and seamless integration with the clinical workflow.

At a higher level, **IoT middleware and platforms** ensure adaptation, context awareness, device discovery and management, scalability, the management of a large quantity of data, ensuring the privacy and security of the IoT infrastructure. But their *primary role is to manage the heterogeneity of IoT in an interoperable way*. For this purpose, an Open Innovation Platform was created in SOFIA to provide *interoperability between multi-vendor devices*: SOFIA was largely devoted to interoperability and the Semantic Information Brokerage (SIB) was the core of the smart environment, centralising the knowledge at the base of interoperability and making it uniform. Adopting a publish-subscribe-notify architecture, the smart objects were able to register to specific topics in the SIB, modify them and receive notifications, creating an ecosystem where the IoT devices exchange information in an intrinsically interoperable way. Also other projects proposed middleware based on *semantics to improve interoperability*, such as eDIANA, nSHIELD and SCOTT. nSHIELD security, privacy and dependability middleware adopted a specific ontology of threats and countermeasure that was available for all the IoT devices connected to the middleware, ensuring interoperability in the IoT infrastructure in terms of security, privacy and dependability. SCOTT proposed a reference architecture that enables interoperability at semantic level, secure and trustable cross-domain application development, and technology building block reusability for heterogeneous wireless sensor and actuator networks. By contrast, IoE adopted an integrated approach based on hardware, software and middleware for seamless and secure interoperability, allowing the Internet to connect with the energy grids, with a specific focus on connecting electric vehicles and smart home applications to the smart grid.

Moving to the **application level**, in the SOFIA project, the knowledge processors were the applications running in the smart environment and made intrinsically interoperable through the interaction with the SIB, where the shared semantic knowledge base was stored. Also the platform developed in ACCUS was intended to ensure semantic interoperability among connected subsystems and applications that, once plugged in the platform, "understand" and "share" the same ontologies, integrating and interoperating seamlessly. Smarcos provided solutions for enabling true seamless interoperability at application level: the project focused on the development of interoperable user interfaces (UI) of distributed UI elements in selected application domains (smartphones, home appliances, health and wellness, professional displays and beamers, multimedia, control & automation).

At **service level**, interoperability simplifies the publication of services and their usage, providing a shared way to declare what an application or system makes available and understand what the consumer receives when the service is called from the application or system itself. SOFIA invested a lot of resources in the study of services and in the identification of a solution for service interoperability, comprising a *semantic-based web service* running in the SIB. eSonia focused on a *SOA paradigm implemented as web services*, made available and interoperable in a multitude of different computing platforms, including embedded devices and low-power wireless devices. Following the SOA paradigm, Arrowhead also proposed a *service-based framework*, the Arrowhead framework, that enables collaborative automation in an open-network environment connecting many devices through natively interoperable services. Also eScop focused on process automation replacing traditional control, based on hierarchical hardware architecture, with a non-hierarchical set of embedded systems and *semantically interoperable and expandable set of services*.

At the highest level of the IoT stack, the **interoperability between entire systems** can be considered, entering the domain of SoS. In this context, CHIRON focused on the *interoperability and integration of subsystems* along with seamless management of multi-source data to support the creation and growth of a horizontally structured healthcare market. With CHIRON's solution, heterogeneous devices and services can interact and exchange patient data in a reliable and secure way, also ensuring seamless integration with the clinical workflow. POLLUX aimed to reduce the development time and cost of the complex, high-reliability mechatronic systems needed for the mass deployment of electric vehicles. The proposed solution enabled the *flexible, evolvable and networked interoperation of systems* (sensors, actuators, batteries, converters, ECUs) plus the deployment of advanced electric vehicle (EV) and powertrain management algorithms and strategies. Meanwhile EMMON and ACCUS considered a wider notion of system characterised by a high level of heterogeneity of its subsystems and by the geographical distribution. ACCUSS developed a platform that allows monitoring, management and control across urban systems, enabling cross-domain and cross-layer cooperation and exploiting the interoperability aspects of semantics, pragmatics, information and knowledge discovery, as well as situational awareness within information, resource and time constraints. ACCUS integrated, coordinated and controlled urban subsystems (horizontal interoperability) and converged applications (vertical interoperability) that can "understand" each other and "share" the same ontologies. At the same level of system complexity, with the Arrowhead Framework, Arrowhead enabled the IoT-based automation of multiple systems in the energy domain, such as energy production systems, the virtual energy market, a production line, smart buildings and a fleet of charging stations for electric vehicles.

Finally, considering the importance of providing efficient engineering support to IoT, it becomes crucial to also ensure the **interoperability in the engineering process** adopted to manage the lifecycle of an IoT product/solution. CRYSTAL, for example, was an ARTEMIS Innovation Pilot Project (AIPP) that, starting from the Reference Technology Platform (RTP) and Interoperability Specification (IOS) developed in CESAR and MBAT, tried to push the Interoperability Specification towards standardisation. CRYSTAL focused on the technical challenge represented by the lack of open and common interoperability technologies supported by the different tools used in the engineering process. Within the application domains of aerospace, automotive, healthcare and rail, CRYSTAL covered the entire software product life cycle and supported product line development towards ready-for-use industrial tool chains. Recently, the Arrowhead Tools project focused entirely on improving the automation of the engineering process: *the Arrowhead Framework is adopted as a service bus to allow the interoperability between the tools used in the various phases*

of the engineering process. This solution improves the level of automation of the engineering process, speeds up the development, reduces the time to market, improves the quality of the final products and reduces the engineering costs.

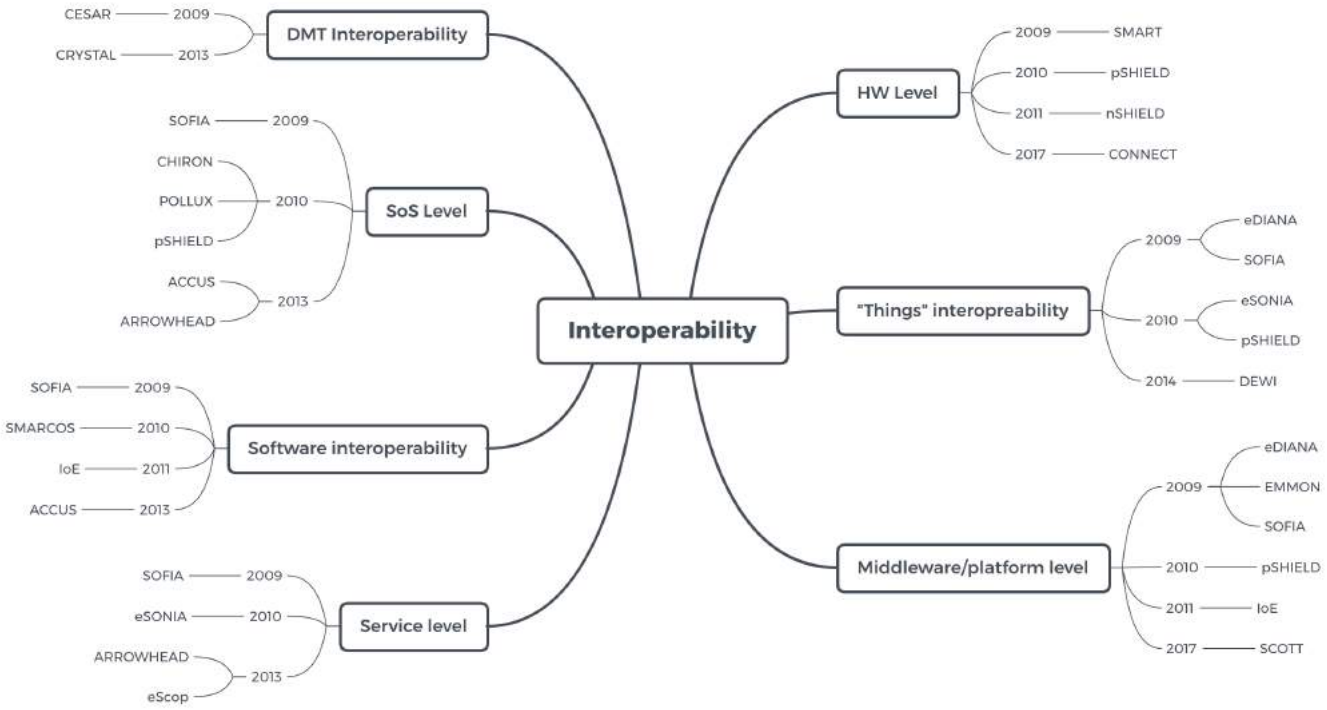


FIGURE 33 — *ARTEMIS/ECSEL projects that contributed to interoperability research stream by research focus area and call.*

The lack of interoperability clearly represents an obstacle for IoT and Improving interoperability is fundamental for the uptake of IoT. Although a huge effort has been spent on this research stream, the available solutions don't provide the expected levels of interoperability yet and they don't contribute enough the reduce IoT market fragmentation. *The definition of widely adopted communication standards for IoT, semantic interoperability and platform interoperability could significantly boost the diffusion of IoT technologies and should find concrete solutions.* This research stream is still developing, and significant investments should be dedicated to it, covering many technological areas:

- Interoperability with legacy devices and systems.
- Definition of IoT device communications standards.
- Machine to machine interoperability.
- Autonomous translation solutions in IoT/SoS (including protocols, encodings, security and semantics).
- Semantic interoperability.
- Improve cross-domain interoperability support.
- Solutions for the engineering process interoperability (e.g. tools and toolchains interoperability).

"Trust" in IoT

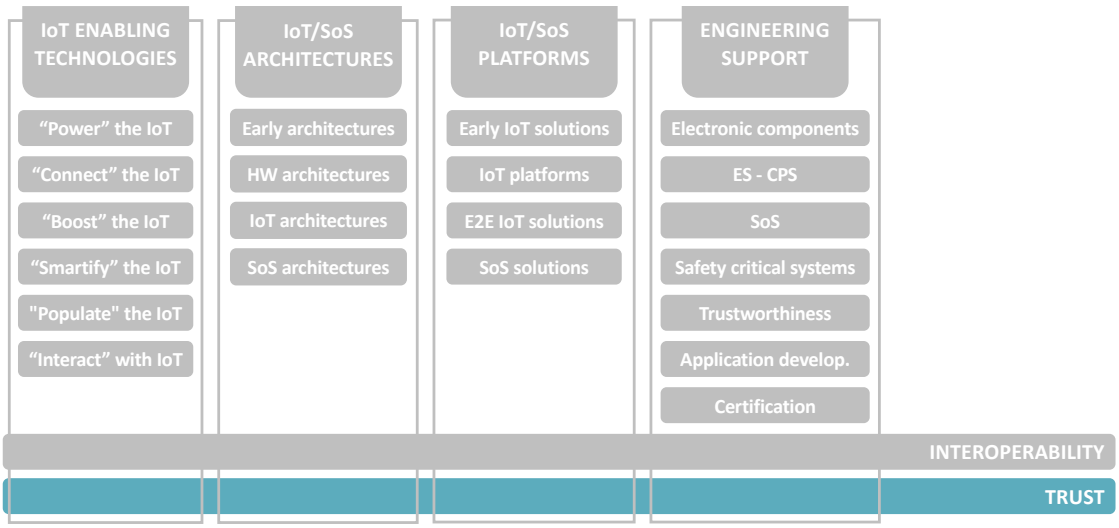


FIGURE 34 — *Trust research stream.*

There is no shared and standard definition of trust: it can be considered as the application-specific aggregation of different aspects of IoT and SoS, including security, privacy, reliability, dependability, safety, confidence, comfort, control, etc. (see Figure 35). Trust is an interdisciplinary and transversal research stream that applies to IoT/SoS devices, to the entities involved in IoT/SoS (e.g. services, application and people), to the communications and to the data flowing through the IoT/SoS infrastructure.

The IoT is a connected ecosystem that offers a new way to solve everyday problems promising simplicity, efficiency, convenience and knowledge as well as representing a shared environment for *an unprecedented multitude of risks*. Vendors of IoT solutions are pushed to deliver products and rush to market without sufficient prior consideration for the security, privacy and dependability that are required for trust in IoT. In a recent survey, Trustwave reported that 61% of surveyed organisations have already experienced an IoT security incident, but only 28% consider their IoT security strategy to be "very important"[43]. The global IoT security market was evaluated at USD 8.2 billion in 2018 and is estimated to grow to USD 35 billion by 2023[44], with a constant CAGR of the 35% until 2026, when it is estimated to reach USD 74 billion[45]. North America and Europe are expected to drive the market, which is progressively shifting the focus from the energy & utility sector (2018) to the manufacturing domain. *IoT offers unprecedented opportunities, but are we aware of the associated technology risks? Do we trust IoT?*

[43] *IoT Cybersecurity Readiness Report, Trustwave, 2018.*
[44] *IoT Security Market, Markets and Markets, April 2019.*
[45] *IoT Security Market Statistics – 2026, Allied Market Research, January 2020.*

> *The ubiquity and pervasiveness of IoT, the heterogeneity of devices and their capabilities expose both industrial and consumer domains to a huge set of security risks. In IoT any computing device is a potential target for hackers.*

Recent alarming studies report that cyberattacks on IoT devices are literally booming. The studies were based on the technique of "honeypot", a tool used by many security experts, *a decoy used to mimic typical targets of attack and subsequently attract hackers*. Recent attacks against the communal critical infrastructures clearly show the importance of having trustworthy IoT and the consequences if it is lacking.

During the first six months of 2019, Kaspersky[46] deployed more than 50 honeypots worldwide and detected 105 million attacks on IoT devices from 276,000 unique IP addresses. The number of attacks in 2019 was nine times greater than in the first half of 2018, which totalled 12 million attacks. Three types of honeypot were deployed: low-interaction, high-interaction and medium-interaction. The first simulates services such as Telnet, SSH, and web servers; the second mimics real devices, and the third is a mixture of the two. 50 honeypots were deployed for more than one year, resulting in 20,000 infected sessions every 15 minutes. Mirai and Nyadrop malwares were responsible for more the 80% of the attacks, exploiting unpatched vulnerabilities and using password brute-forcing attacks respectively. In 2016, the Mirai malware family was responsible for the largest internet blackout in US history, and its persistence in 2019 indicates that an adequate countermeasure is not available yet. The complexity of IoT provides a rich and inspiring playground for hackers that successfully use even the most primitive methods.

According to Symantec[47], *worms and bots* remains the main protagonists of IoT attacks, but the threats are evolving rapidly. Routers are a very frequent target of attacks, being the access point to the internet and representing a jump-off point for further attacks. Routers and connected cameras were the most infected devices, accounting respectively the 75% and 15% of the attacks. A serious emerging trend is represented by the attacks against industrial control systems, but also attacks to satellites for internet communications (e.g. Thrip hackers' group) and to industrial safety systems (e.g. Triton hackers' group). The report also points out that the emergence of VPNFilter in taking an important role in the evolution of IoT threats. VPNFilter was the first widespread persistent IoT threat, representing a new approach with respect to traditional attacks like DDoS. VPNFilter is able to survive a device reboot and to completely remove any trace of its presence, making it very difficult to remove.

We have and will have to live with the need to tackle security threats on a daily basis, considering both the technological aspects, their effect on the digital/physical worlds and their geographical impact. *Attacks potentially affect every technological domain*, from hardware and software, to communications, energy distribution infrastructures, mechatronics, space technologies, industrial security and safety systems, etc. *Attacks potentially have a duality*, because they typically happen in the digital world, but they seriously affect also the physical world: consider the destructive malware used in a cyber-attack to a Ukrainian power plant, for example, or the Internet blackout in 2016, or the remote hijacking of vehicle's digital systems over the Internet that caused the recall of 1.4 million of cars. *Attacks have no geographical boundaries*, starting from any part of the world and affecting every country in the world: the Karspesky report evidences that attacks came from China, Brazil, Egypt, Japan etc.

> *The IoT attack surface is the sum of all potential security vulnerabilities in IoT devices, in associated software and in the infrastructure of a given IoT deployment, both local or globally distributed over the Internet.*

---

[46] *IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019, Kaspersky Labs, October 15, 2019.*
[47] *Symantec Internet Security Threat Report 2019, Symantec a division of Broadcom, ISTR 24, February 2019.*

The large variety of IoT vulnerabilities is instigated by the heterogeneity of IoT components and of the communication channels, by the multiplicity of data managed, by the mechanisms adopted to access data, by the complexity of IoT platforms, etc.: every layer of the IoT architecture is affected. These vulnerabilities must be addressed to ensure that all the components of an IoT solution become trustworthy. *"Trust" indeed summarises in a single concept the absence of all these vulnerabilities and trust management becomes a fundamental feature for an IoT solution and for all the stakeholders involved in the related value chain.*

Collected and exchanged data need to be trusted, therefore solutions to secure data can be considered as trust management systems. In addition, entities within an IoT ecosystem need to communicate using trusted relationships, therefore identity controls and authorisation systems have to be established to build trust between entities to share information reliably. Furthermore, data and application have to be accessed from only trusted entities. Hence, access control solutions have to be established based on trustworthiness. Eventually, identification, authentication and authorisation, as well as access control systems and other existing security protocols and processes, should be integrated in a trust management system.

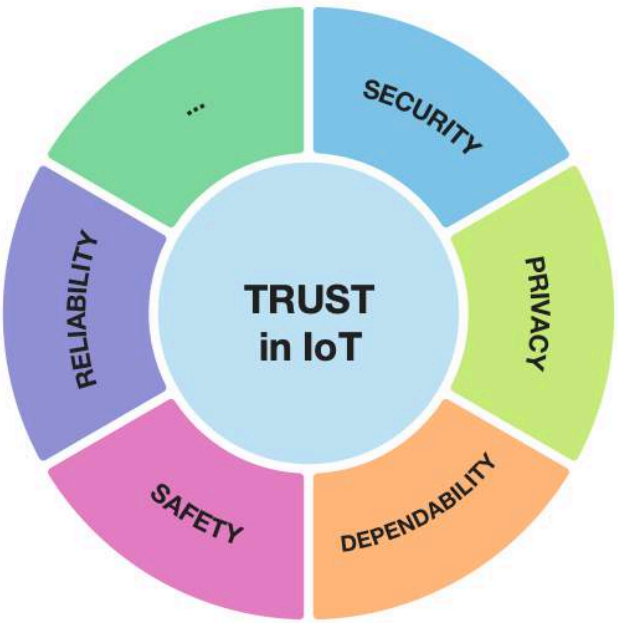


FIGURE 35 — *Aspects of IoT that contributes to trust.*

Currently, there is no reliable and complete inventory of threats that could affect IoT, and it is very difficult to identify, classify and prioritise them as well as understand how they impact on trust.

The simplest aspect that affects trust is the **lack of updates**: with 25 billion IoT devices expected by 2025 that could lack of sufficient security updates, or that could not be updated at all, the problem of ensuring device security becomes a big challenge. *The technology evolution makes a device that was initially secure completely vulnerable and insecure*. Over-the-air solutions allow a regular and automatic update of devices but, very frequently, the updates stop when a new device is produced, leaving the previous version exposed to attacks. Lack of updates significantly and seriously impact on legacy devices that, for the large part, are difficult or even impossible to update.

Another simple but severe security threat is the **use of default passwords on IoT devices**: device owners do not change the default credentials, which tend not to be safe, making the device a good candidate for brute-force attacks. This bad practice also represents an indirect risk for companies and their business.

Focusing **on the data flowing through the IoT infrastructure**, trust must be ensured from many different perspectives. IoT devices that have been compromised can become the source of untrusted, unreliable or even false information, translating in simple spam activities, fake data sources (e.g. sending fake signals with machine phishing could harm the safety of a manufacturing plant) or even generating traffic for conducting DDoS attacks when the device falls into a botnet. Hackers can exploit the vulnerabilities of an unsecured device that generates a leakage of data to steal the user's personal information (e.g. the address, phone number, credit cards, etc.). Data theft becomes an extremely serious problem when the vulnerable device is connected to an organisation network, allowing hackers to steal large amount of sensitive information. Moreover, considering that IoT devices collect any kind of data, privacy concerns emerge because the device is collecting personal information without having any proper protection or simply the user's consent. Consider, for example, the smartphone application that typically "forces" the user to accept potentially risky permissions on data collection.

Unsafe communication represents one of the biggest IoT security challenges and affects trust in many different ways. For example, many devices simply still do not encrypt the messages they send to the network, both in machine-to-machine communications and with the enterprise IoT levels. End-to-end encryption is fundamental to ensure data security and privacy. Unsafe communication also opens up the opportunity to deviate information traffic from the correct destination to a hijacked recipient, that is typically called sinkhole. Sinkholes are able to compromise the confidentiality of information and of the related IoT services.

Connectivity allows **remote access to the device** that can be fraudulently obtained, leveraging numerous vulnerabilities in the operating system (e.g. Linux, Android, iOS, etc.): the hacker has full control of the device and of the data it contains, allowing the camera/microphones to be turned on without the user's knowledge, the installing of applications, stealing of information, etc. Imagine the potential consequences of remote vehicle access that exposes the drivers, the passengers and other vehicles to extreme dangers: car manufacturers are making huge investments in IoT security but, in some cases, it has not been enough. Similar serious consequences could affect compromised IoT medical devices, industrial safety systems, industrial plants, sensitive sites, etc. A very widespread and effective threat enabled by remote control is *ransomware* that, in the simplest implementation, allows an IoT device to be locked and a ransom demanded for unlocking it.

Trust also involves the **intelligence embedded in IoT devices**. AI algorithms are more and more frequently incorporated in IoT solutions in order to increase their level of automation, but automation intrinsically implies absence of human control and without any supervision a single mistake in a line of AI code potentially represents a serious vulnerability that could be used to control a device or, depending of the role of the AI algorithm, entire portions of the IoT infrastructure.

At platform level, trust affects many aspects. Poor authentication mechanisms, both for devices and for users, represent the largest threat to platform level security. Many platforms currently provide very poor (or don't even provide) provisioning services, device-reliable authentication mechanisms, certificate-based authentication, lack of encryption and insecure password recovery, secure fleet management. And the same applies to the user/owner of these devices and to the IoT administrator and operators.

The severity of all the previously mentioned threats to IoT **trust increases with the number of deployed devices** and, more in general, with the dimensions of the IoT solution. Before the IoT revolution, security was basically supposed to take care of personal computers, while today the edge of IoT, the intermediate nodes and the communications present an unprecedented and continuously increasing level of heterogeneity, representing a rich and inspiring

playground for hackers. *The dimensions of the IoT solutions allows large-scale attacks* that are potentially devastating but also small-scale and targeted attacks represent a serious risk: they are difficult to identify in a large IoT deployment and could anticipate subsequent large-scale escalations.

Trust also depends strongly on **physical aspects** that, if not considered in trust management, allow the hackers to gain direct access to the IoT infrastructure: the mapping of the physical world in the digital world creates a bidirectional relationship, with reciprocal effects and consequences. Physical weaknesses allow the hacker to disassemble a device and fully re-program it, re-configure it, install malicious software, steal information, intercept and alter communication (e.g. man in the middle attack), install ransomware, etc.

Eventually, the **human factor** represents a large concern for trust management. IoT is largely intended to improve everyday activities and this requires human interaction. The awareness and knowledge of cyber risks is not adequately dispersed, and it does not represent a concern for most people. People either do not know much about IoT trust or don't care, and this lack of knowledge and interest could represent the cause of massive damage both to corporations, society and individuals. *Significant investment in communication, marketing, education and professional training should be planned.*

> *The common sentiment "who cares about my personal data, why someone should spy on me, hack my smartphone... I am just an individual in a multitude" is largely widespread and demonstrates a deep lack of knowledge of trust-related topics.*

Knowledge and expertise sharing are the first line of defence against such IoT threats and, in this perspective, the joint effort of three driving factors is fundamental:

- Manufacturers and suppliers of IoT solutions should implement and adopt common and shared trust frameworks.
- End-users and consumers should be aware about and should be involved in the definition of the trust capabilities of an IoT solution.
- The European community should promote an ecosystem and regulations where the stakeholders cooperate in IoT innovation and market development, ensuring trust in IoT.

To ensure trust it is also necessary to **fight the diffidence towards IoT**, clarifying the meaning of buzzwords, educating customers and end-users, improving marketing, clarifying the commercial offer, evidencing the price reduction and the return on investment, targeting financial decision-makers and identifying enthusiastic early adopters to be involved in promotional initiatives.

From the **trust management perspective**, a human-centric model could be the starting point to clarify responsibilities and identify the processes that trust in IoT. An effective and widely adopted trust model to guide IoT device designers, service providers and common users is not available yet. A trust model defines how each entity in an IoT ecosystem relies (or could rely) on other entities. *A human-centric model aims at defining an effective way to manage security, regardless of having the responsibility of a professional operator or being an average user.* A similar model could be focused on several aspects that contribute to trust management, including:

- Identify the security, safety, privacy, reliability, etc. of the intrinsic properties, functionalities and capabilities of a device and of the hosted application that make them trustworthy.
- Define how to govern the device and control how the resources (typically data) on the device are used and by whom.

- Classify which data are sensitive, non-sensitive, can be anonymised and can be merged to generate higher level information that could be sensitive, non-sensitive or can be anonymised.
- Define when trust can be delegated and to whom and identify what are the implications.
- All the previous points are considered for any physical device but must be analysed also for any virtual representation of the device itself.
- Identify processes and tools that allow the previous points to be scaled at system level (e.g. an IoT platform providing the right functionalities that ensure trust).
- Define strong and reliable identity management processes, mechanisms and systems.

From the technical perspective, ARTEMIS and ECSEL projects have been involved in this research stream since the first call for proposal, trying to develop enabling technologies, architecture oriented to trust and also holistic approaches for security, privacy and dependability. Trust by design has been an important focus of many ARTEMIS and ECSEL projects. Research have been oriented to the following focus areas:

- Electronic components providing "built-in" support for safety and security in *things*.
- Ensure safety in the inclusion of legacy systems.
- Ensure data safety, security and privacy.
- Embedded systems safety, security, reliability and dependability.
- Composability of safety, security, privacy, dependability, etc.
- Communication security and dependability.
- Application security.
- System of systems level security, privacy and dependability.
- End user safety, security and privacy.
- Design methods and tools to support trust.

The electronic components providers are facing new challenges similar to what happened when we moved from a closed phone world to the era of smart phones. The easiest attack vector was someone with overalls and a key to a distribution cable. Suddenly there were legal interfaces to the phone system revealing possible vulnerabilities. Understanding safety and security and that they are now even more tied together is becoming even more important (see the analysis carried on by SCOTT project[48]). These paradigms changed recently when safe systems got connected to the outside world. Safe systems suddenly became open to attack. Serious steps have been taken towards providing support for **safety and security "built-in" in things**. The ACROSS MPSoC offers a predictable on-chip interconnect that is free of interference. SMART had provided the RASIP processor which tolerates sideband attacks by encryption. Another approach has been to develop more robust components (e.g. IoSense). Since IoT devices are connected and have also more interaction with each other, the data transmission needs to be secured and guaranteed (CONNECT).

There have been different levels of approach in the ARTEMIS and ECSEL projects geared to ensuring **data safety, security and privacy**. Semi40 aimed to interconnect production systems, mobile production support systems and production plants along the supply chain, while maintaining *safety, security (confidentiality, integrity, availability) and* reliability and availability in order to increase efficiency and enable agile production processes. SOFIA aimed at developing an Open Innovation Platform (OIP) which could provide the interoperability allowing interaction between multi-vendor devices: the platform was based on a semantic information broker that included functionalities for *data security and access control*. Similarly, in the healthcare sector, CHIRON provides a reference architecture for personal healthcare ensuring the interoperability between heterogeneous devices and services, *reliable and secure patient*

[48] *https://scottproject.eu/security-and-safety/*

data management and seamless integration with the clinical workflow. In the energy sector the ENCOURAGE project, while providing solutions to optimise energy consumption via IoT, allows comfort and security via the inclusion of additional information sources such as personal context-aware information, i.e. ambient intelligence. In the same domain, IoE provided guidelines for the implementation of *security, privacy and dependability*, which have been validated in selected cases using models and simulations. The project also provided security and privacy solutions to maintain the confidentiality of sensitive data and protect personal identification. DEWI introduced the concept of the "sensor & communication bubble", a locally adaptable wireless network, offering locally confined wireless internal and external access, secure and dependable communication and safe operation. Recently, Productive 4.0 tried to ensure *security and data confidentiality*, adopting authorisation and authentication processes as well as data encryption in real-time industrial environments.

Embedded systems are investigated from their safety, security, reliability and dependability point of view in **different application areas**. In the automotive environment, SILENCE provided *enhanced safety by touchless control*: sound/voice activation/control of systems in the car (e.g. navigation, entertainment and climate control) and control of machinery in industrial applications. POLLUX concentrated on electrical vehicles and defined reference designs and architectures, to reduce computational effort and ensure high levels of reusability, *reliability and dependability* of systems, thus reducing development time and costs.

To tighten **physical safety**, new and more reliable sensors are required. EXIST improved safety through more sensitive and versatile gas detection systems for industrial applications. Similar results have been obtained in ME^{3}GAS and IoE.

The challenge of harnessing current environment and available components to provide **safe and secure installations** was also investigated. *Composability of safety, security, privacy and dependability* were researched, for example, in iLAND and SESAMO. iLAND aimed to realise new dependable and secure products and services resulting from the composition of existing ones: e.g. trusted environments (video monitoring), untrusted environments (wireless transport), and mixture of both (home health care). SESAMO focused more on the protection of security and critical infrastructures, addressing the issues emerging in the convergence of safety and security in embedded systems at architectural level. A component-oriented design methodology based upon model-driven technology addressed the safety and security aspects of networked embedded systems in multiple domains (e.g., avionics, transportation, industry control, mobile medical). The project developed a rigorous framework that enables joint reasoning about the required safety and security properties and the resolution of any conflicting constraints.

With the era of 5G even the smallest IoT devices will have the possibility to be part of the network, so more attention needs to be paid to **communication security and dependability**. These have been addressed in several ARTEMIS and ECSEL projects. eSONIA, for example, developed a solution that allows suppliers to remotely connect their devices in the factory through *secure connections*. IoE's main objective was to develop hardware, software and middleware for seamless, *secure connectivity* and interoperability by connecting the Internet with the energy grids. *Secure and dependable wireless communication* and safe operation have been the focus of DEWI and SCOTT, and MANTIS looked especially at reaching the inaccessible places for a wired network. On a protocol level the combination of *safe and secure wireless cooperation* was studied in SAFECOP. In industry, the weakest link needs to be harnessed and, in this context, Productive 4.0 developed a data analytics framework and a *secure communication environment* for the full value chain of the production domain to meet the demands of the industry.

Each application domain has its own special trust requirements. These have been investigated from the application point of view in almost every project that contributed to this research stream. For example, energy applications were looked in eDiana, ME^{3}GAS, IoE, SESAMO, CONNECT, etc., healthcare and assisted living in iLAND, CHIRON, SESAMO, AQUAS, SCOTT, SECREDAS, etc., automotive and transportation in POLLUX, nSHIELD, SESAMO, DEWI, AQUAS, SCOTT, etc., surveillance and public environments in nSHIELD, DEMANES, E-GHOTAM, COPCAMS, DEWI, SCOTT, SECREDAS, etc., production in eSONIA, Productive 4.0, AQUAS, SCOTT, etc.

The study of trust in ARTEMIS and ECSEL projects also covered the **wider perspective of the system level**, with the identification of potential end-to-end solutions covering the entire IoT/SoS infrastructure and the application built on it. SCOTT, for example, aimed at creating trust in wireless solutions and increasing their overall acceptance, which represents a major challenge in increasing the market penetration and achieving the full potential of IoT. Therefore, SCOTT extended the concept of DEWI's "sensor & communication bubble" to the wider idea of Secure COnnected Trustable Things and, starting from a standardised multi-domain reference architecture, it developed an *end-to-end composable and cross-domain solution providing 50 technical building blocks* for security/safety, distributed cloud integration, energy efficiency/autonomy of devices and reference architecture/implementations. The InSecTT project, recently accepted, will start in 2020 and develop this research further.

At SoS level, a significant contribution to security, privacy and dependability (SPD) is represented by pSHIELD and nSHIELD projects that developed a solution for *SPD by design, providing SPD functionalities as "built in" rather than as "add-on".* The projects developed an architectural framework for modular and composable SPD in IoT, adopting it in four different strategic scenarios: railways security, voice/face recognition, dependable avionic systems and social mobility. The end-to-end solution covered the different levels of the IoT stack, node, network, middleware, overlay and application. The framework included integrated SPD metrics able to dynamically monitor the SPD levels of the system and, depending on the system status, trigger the most adequate countermeasure to maintain the desired level of SPD. This methodology has an impact on the development cycles of SPD because the qualification, (re) certification and (re)validation process is faster, easier and widely accepted. With the creation of this innovative, modular, composable, expandable and highly dependable architectural framework, and with the use of common SPD metrics, the SHIELD solution is capable of improving the overall SPD level in any specific application domain with minimum engineering effort, across the system layers, across vertical domains and across the entire system lifecycle. On urban environments, ACCUS provided an adaptive and cooperative control architecture and corresponding algorithms. ACCUS focused on stable closed-loop systems, *controllability* of networks of dynamic systems, *robustness* of control, robust topologies and *dependable* networked control. More recently, the Arrowhead Framework introduced the concept of *secure local automation cloud* for the management of SoS. The framework was developed in the Arrowhead project and adopted in Arrowhead Tools, Productive 4.0, EMC^2, Far Edge, Opti, MANTIS for multiple vertical applications within smart production, smart buildings, smart energy and electro mobility. A secure local cloud is defined as a closed group of industrial things within a physical proximity and provides a number of basic core services enabling fundamental service-oriented properties like service registration, service discovery, authentication and authorisation plus the orchestration of system of systems.

Also **end user safety, security and privacy** have been considered highly important in ARTEMIS and ECSEL projects and were given even greater emphasis with regulatory action by the EU (e.g. GDPR). The CAMMI project focused on human safety and aimed to develop a *joint-cognitive system* that balances and optimises operators' workload and thus improves the safety of complex systems such as industrial plants, airplanes or cars operated by people under demanding conditions. This solution enables control to be shared between the operator and the system, allowing the operator to focus specifically on critical tasks. In the healthcare context, With-Me developed a customisable, adaptive, assistive and yet secure training/support solution aligned to user preferences and needs. The car and industrial control needs were researched in SILENCE. It provided *enhanced safety by touchless control*: sound/voice activation/ control of systems in the car (e.g. navigation, entertainment and climate control) and control of machinery in industrial applications. The proposed approach considered also *gestural authentication*: in the context of the need for stronger authentication process, gestural identification appears as a new factor, increasing the diversity and, hence, the robustness of authentication scenarios.

Regarding the **design methods and tools to support trust**, these have been investigated from the perspective of safety critical system in industry, from the regulatory point of view (e.g. providing certification) and from the modelling point of view. CESAR addressed the industrial needs for the development of embedded systems for *safety related applications by improving methods, processes and tools, specifically promoting a holistic view on system*

engineering. CHARTER developed concepts, methods and tools for embedded systems design and deployment that manage their complexity and substantially and improve their development, *verification and certification processes*. The CHESS approach was to build modelling languages for extra-functional properties and develop tools for evaluation of these properties to reduce the costs and risks of development and deployment, in terms of *safety, reliability, performance and robustness*. The nSHIELD architectural framework and methodology provided metrics and tools to *assess and monitor the SPD levels* of the system, identify the system states in term of SPD and define, for each state, the countermeasure to potential SPD threats. Recently, SECREDAS has been developing software for validating methodologies, reference architectures, components and suitable integration, as well as verification approaches for automated systems in different domains: the objective is to combine *high security and privacy protection* while preserving functional-safety and operational performance. The project aims at developing and enhancing trustworthiness, as well as, at addressing cross-domain cybersecurity and safety of automated systems in the transportation, aerospace and medical domains.

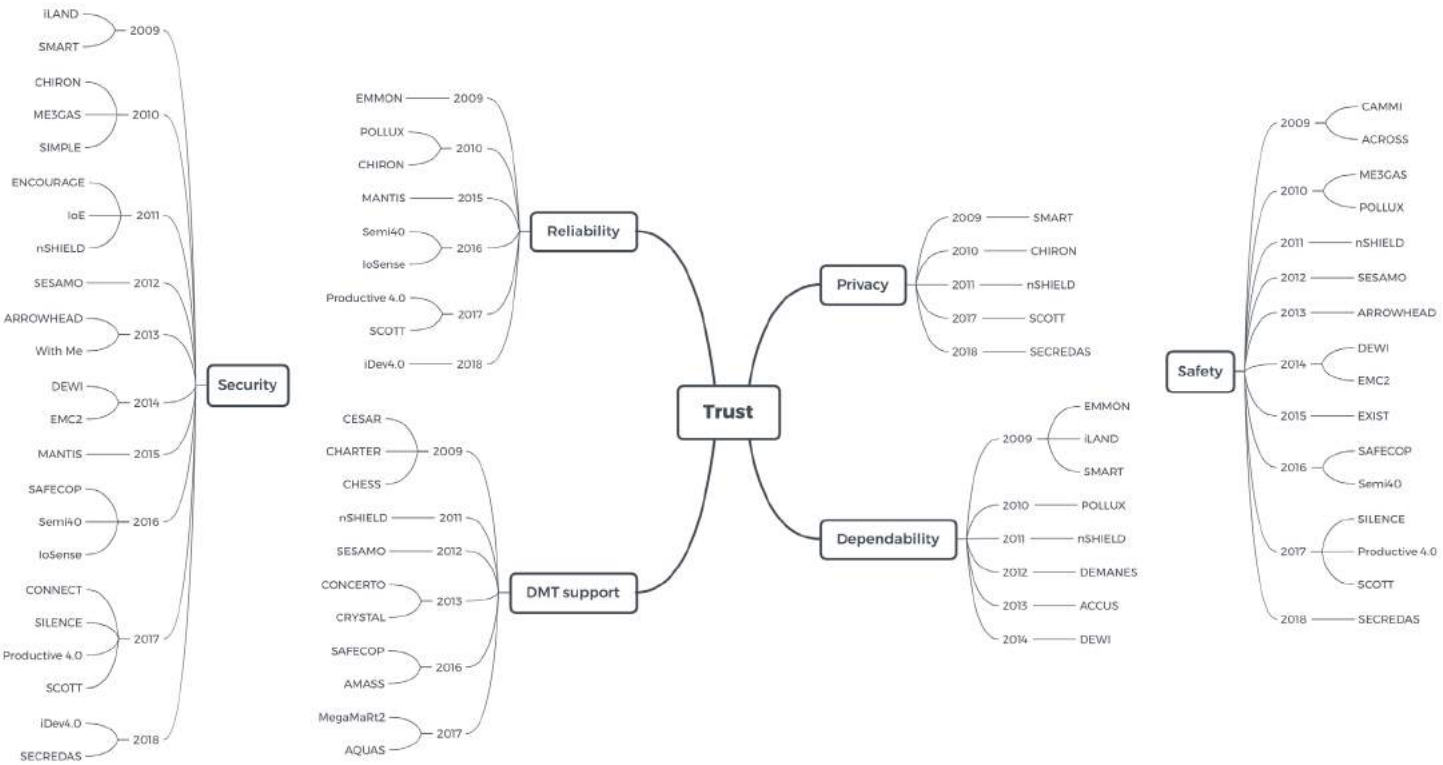


FIGURE 36 — *ARTEMIS/ECSEL projects that contributed to trust research stream by research focus area and call.*

Figure 36 clearly demonstrates the huge effort that has been spent on "trust in IoT" research stream. This effort has produced important results, consolidated the European expertise in topics related to IoT trustworthiness and provided some solutions that have already become part of IoT products in the market, but is very far from having identified definitive answers to IoT trustworthiness. IoT and SoS domains are evolving rapidly, with unprecedented opportunities and challenges, and the trust in these pervasive technologies must be keep continuously guaranteed. Many technological issues remain open, including:

- Hardware solutions for trust.
- Protection of IoT devices to prevent IoT entry doors to systems for hackers and identity theft.
- Security, privacy protection, safety, reliability, human interaction and societal acceptance of IoT and SoS.
- Promote a "Trusted IoT label" defined by the European Commission.
- Solutions for trustworthy AI-based systems.
- "Trusted IoT label" as identified by the European Commission.
- Blockchain for decentralised IoT application and SoS.
- Blockchain based solutions, blockchain-enabled integrated access management.
- IoT trust awareness and training.
- Distributed M2M business platforms, nano payments, trusted logs and secure monetisation.
- Self-X trust technologies.
- Trust by design.
- Trust composability. Trust in SoS integration.

Vertical Domains

In terms of vertical domains, connected products, IoT devices, platforms and systems are the "enablers" underpinning the "**Digital Transformation"** of many sectors of the global economy into a **"Digital Economy"**. In order to stay competitive, this transformation imposes the reshaping of activities and business models but opens up also new market opportunities. The availability of the digital information from the physical environment is a unique opportunity for the industry. The information base collected from systems will be larger than ever before, resulting in more optimised, accurate and efficient realizations and operations.

In the world of tomorrow, a myriad of smart products and systems will be connected via all kinds of networks, including the Internet, and will be able to exchange information. At the very beginning, the research and development on the Internet of Things (IoT) started from wireless sensors and connectivity, from the enabling technologies. Today, research is looking at IoT from the opposite viewpoint, that is from the system perspective: considering an **IoT vertical application**, today we have a complete overview of the information "lifecycle", from the data collected by the sensors and transported over networks in a smart fashion to the actuation based on the processing of that data. This system perspective will be key to unlocking value to users and society. And those synergies between sensing and actuation need to be extended to the complete value chains and application areas, at all levels, considering embedded software, hardware and microelectronics: this process will change the eco-system around the "verticals" and will generate subsequent sales and revenues. To enable those synergies, interoperability, particularly semantic interoperability, will be a key factor because users of physical IoT artefacts and their embedded intelligence may use the different languages of different domains but nevertheless must still "understand" each other. The emancipation of embedded information with semantics creates possibilities for completely new types of applications that have not been possible to date.

Hyper-scalability of business models

The platform concept that is now quite common in the Internet economy is also a characteristic of the Digital transformation as explained in the ARTEMIS SRA 2016. For the embedded software development and in Cyber-Physical Systems (CPS) based application building, this *Platform concept* is cost efficient, as it provides facilities to experiment and test innovative products and services. It helps companies to scale up their development activities with limited effort and minimal investment to rapidly deliver such products and services to the market. Standardization efforts in CPS and IoT technologies are required to fully exploit this Platform concept and open the generic concept to various industries and application domains.

The GAFA (Google, Apple, Facebook and Amazon) business model has shown an unprecedented and tremendous growth with economic and financial impact, together as large as the economy of a mid-sized country *but realised with only one tenth of the people*. The GAFA business model focuses on getting customers to commit. *Its innovative approach comes from earning money from product uses, not from their production or the products themselves.* Such business models are built on the concepts of open platform and networks, leveraging connections and interactions as a source of knowledge and, therefore, performance. The platforms/infrastructures they apply generate a variety of actors in the Internet economy, attracting other companies to connect, participate and create value. *And business (hyper-)scaling is implemented at almost zero marginal cost.* The GAFA model proves that there is no future for closed systems in a networked economy, specifically in IoT and SoS. It should be adapted to the core areas of European

markets that mainly address the Business to Business (B2B), Business to Machine (B2M), and Machine to Machine (M2M) segments.

A set of generic user-centric platforms can be used to help developers boost their design capabilities, validating their options and offering creative and innovative products and services. The platform owner can run the platform as a lab, letting people create, innovate and compete, and pick up the best product with the opportunity to capture the highest value.

Vertically integrated companies

In the domain of consumer electronics, companies that have gained **control over the complete value chain** (from hardware to end-user applications) have recently shown a high success rate. Google, Amazon, Apple and others tend to extend their range of smart products to devices, and even silicon design to retail or Internet shops. Supported by a platform, these companies are creating an ecosystem over the complete value chain with a customer lock-in. These companies are well positioned to take advantage of the opportunities provided by IoT technology.

The software value

The Digital Transformation implies a need for improvements in software quality, a higher productivity in software development including maintenance, as software complexity increases with growing connectivity and (system-of-)system complexity, stricter operating requirements on safety and security and with growing expectations of continuous performance and functionality improvements.

The free and open source model has been effective in getting investment from companies and engaging with developer communities through mutual effort. For Europe it is a major challenge to take advantage of the disruptive technologies created by IoT and to realise the digital transformation of European businesses, and the need for a stronger software ecosystem to nurture sustainable, interoperable CPS and IoT software development.

Projects viewed from the vertical axis

The 58 ARTEMIS and ECSEL projects selected in this study, together, cover a range of *eleven application domains or verticals*. The study classified the projects according to which of these eleven applications domains they were active. Figure 37 shows the totals of investments made by ARTEMIS and ECSEL projects in IoT technologies for each of the different application domains. A project may be active in several of the vertical application domains and, in this case, the investment of the project was equally divided over all of its application domains. This equal division of investment is an assumption that may induce some errors since it may not hold true for all projects.

> *The cross-domain proposition made in the ARTEMIS SRA 2016, that is the inclusion of more than one application domain, is supported by the majority of the projects (48) considered in this study.*

For the *cross-domain analysis*, that is the number of verticals in which a project is active in, we observed that on average each project is or was active in about 3 application domains. For seven projects we observed activities in six application domains (SOFIA, nSHIELD and Demanes, EXIST, IoSense and SCOTT). Only one vertical or application domain is observed for ten projects (CESAR, Charter, eSONIA, iFEST, SMECY, WSN DPCM, CRAFTERS, ACCUS, eScop, With Me and MANTIS).

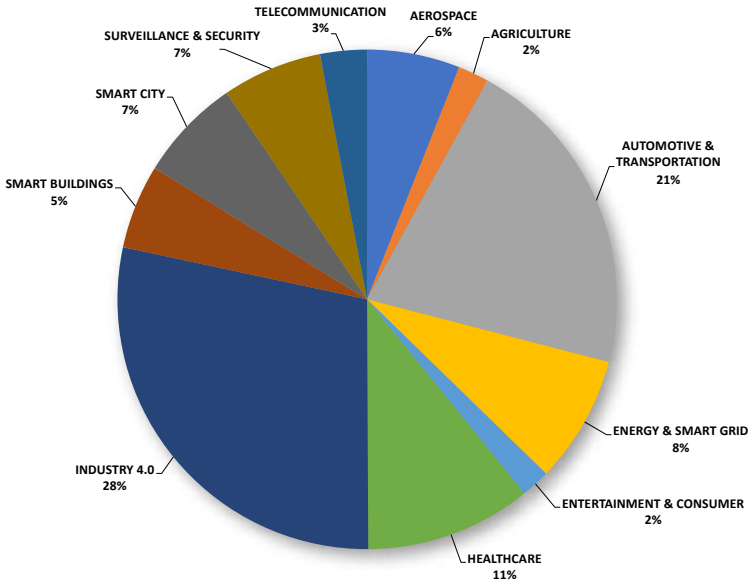


FIGURE 37 — *Investments devoted to IoT in ARTEMIS/ECSEL by vertical domain.*

The larger investment in Industry 4.0 is mainly due to larger projects and not due to the larger number of projects active in that application domain.

A distribution of projects activities (not investments) over the four Key Application areas of the ARTEMIS SRA 2016 was also made and is shown in the chart below. Again, projects may be active in several Key Application areas (Figure 38).

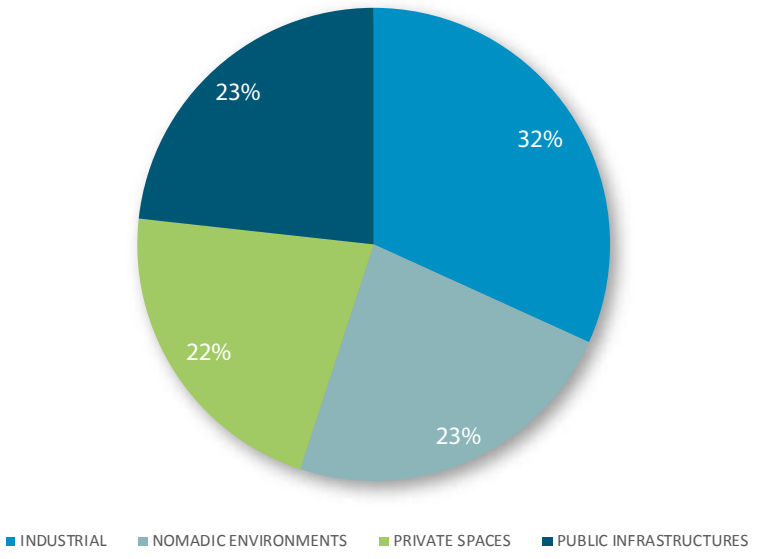


FIGURE 38 — *IoT-related ARTEMIS and ECSEL projects by key application area.*

Apart from the slightly larger size of the industrial domain, the other three domains are quite evenly sized. As projects can be active in one or more of the four Key Application domains, one can also consider the distribution of projects active in only one domain (see Figure 39).

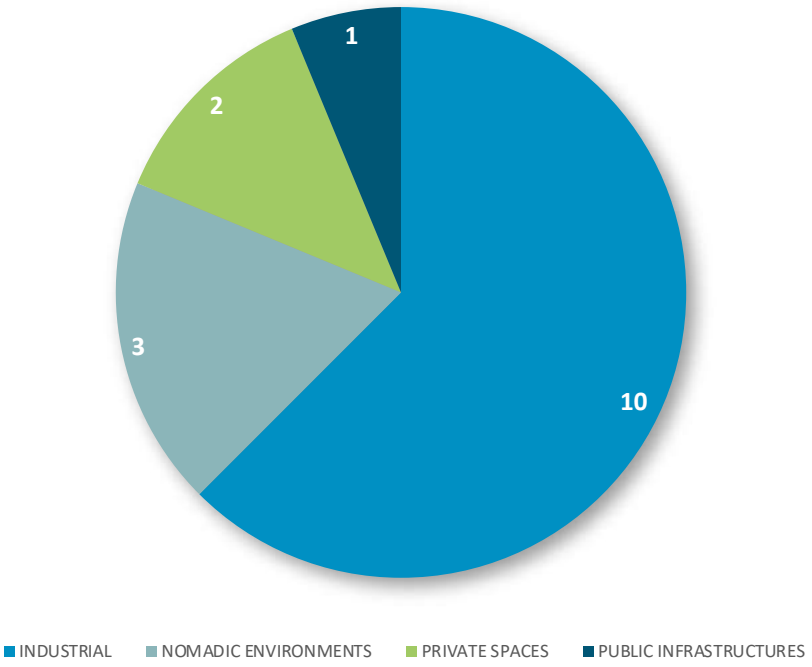
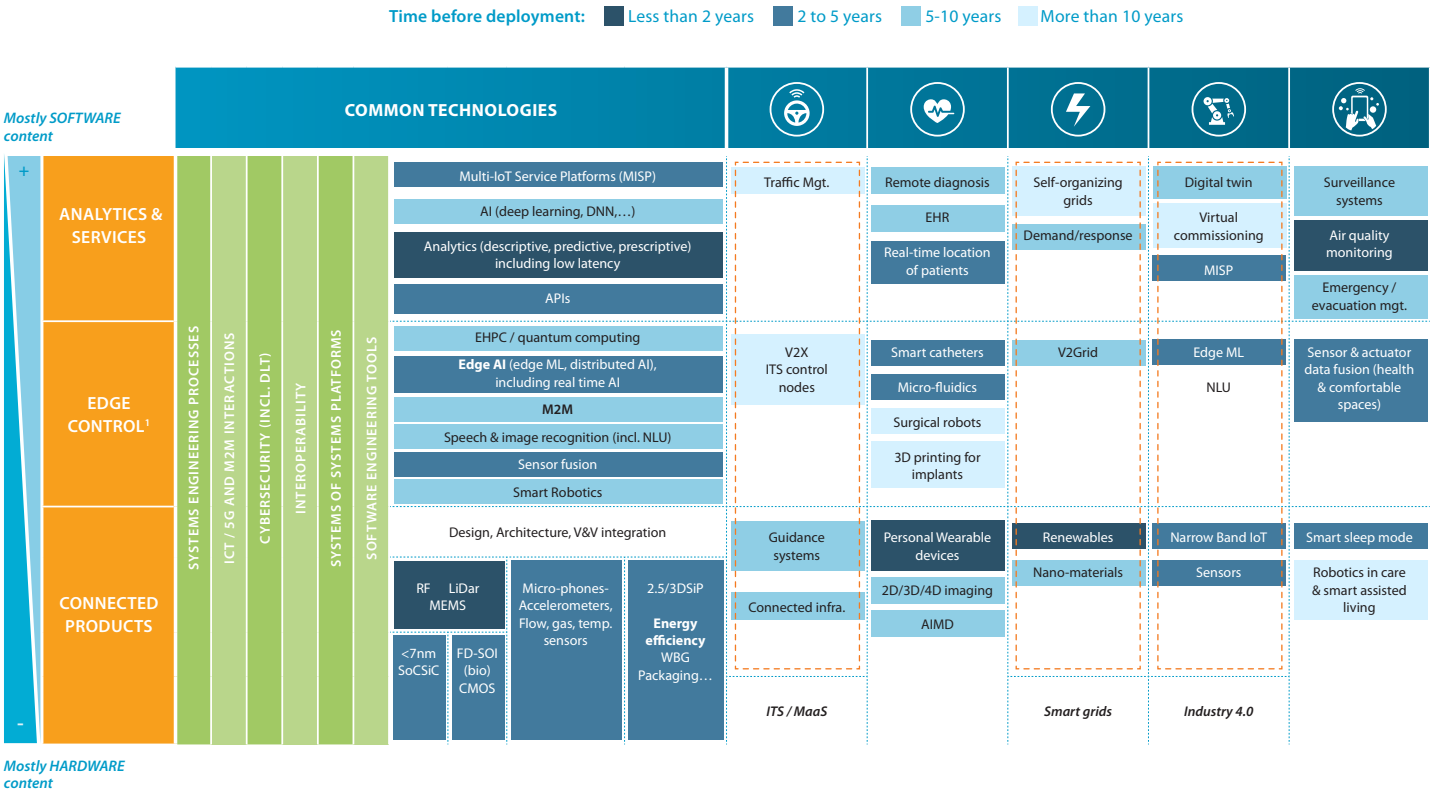


FIGURE 39 — *Number of IoT-related ARTEMIS and ECSEL projects by key application area.*

Apparently, industrial projects span multiple Key Application domains less frequently than other projects. However, when we consider projects active in 2 domains, which is the case for 22 projects, the distribution over domains is already quite similar to the picture for all the key application domains.

ECS-SRA Verticals

In the ECS-SRA five verticals are considered as engines for innovation on electronic components and systems. In this study, we do not go into the details of these verticals, but refer to figure 7 from the report: "Embedded Intelligence: Trends and Challenges". This figure shows a mapping of technologies onto the application domains and is presented in Figure 40:



[1] An edge control is any piece of hardware that controls data flow at the between the CPS and the network. Serving as network entry (or exit) points : transmission, routing, processing, monitoring, filtering, translation, computing and storage of data. - Source: ECS SRA, Advancy research & analysis

FIGURE 40 — *Time before deployment of required technologies, "Embedded Intelligence: Trends and Challenges", Advancy.*

This chart shows the important innovations in the verticals, together with the common or horizontal technologies required to drive these innovations. An indication is given for the time before deployment.

> *The positioning of IoT as element of Multi-IoT Service Platforms with a time before deployment of 2-5 year (Figure 40) supports the position of IoT as key enabler to the development of end-application solutions and confirms the role of IoT as value chain enabler.*

Investments in IoT and SoS research

There is a widespread opinion among analysts that IoT has passed the hype stage: according to Gartner[49], in 2016 IoT was at the peak of inflated expectation, while today the market is stabilising and consolidating. A more focused and continuous influx of investments and the steady growth of the market are confirming this opinion.

During the period 2009-2020, ARTEMIS and ECSEL initiatives have seen significant investments in IoT and SoS. Globally, the investments are characterised by an upward trend that is gradually shifting from the exploratory nature of the initial projects, to a more cautious, rationale and market driven approach of the last calls.

The analysis of the investments represents the second part of the assessment of the IoT and SoS projects promoted and developed by the ARTEMIS and ECSEL community. *The investments analysis is intended to identify the research streams that attracted more investments and estimate the "ballpark figure" of financial effort in IoT/SoS required to develop technological solutions to overcome obstacles and address challenges.* It is in summary, the estimate of the global investment devoted to IoT and SoS in the last decade of ARTEMIS and ECSEL calls.

Investments analysis

The analysis of the research activities and of the related investments considered 107 projects, accepted in the ARTEMIS and ECSEL calls for proposals during the period 2008-2017 and corresponding to the projects active between 2009 and 2020. To ensure the coherence of the analysis between ARTEMIS and ECSEL, the ECSEL projects focused on semiconductor process technologies, equipment, materials and manufacturing (for a total of 23 projects) have been excluded from the analysis, because these research areas were not covered in ARTEMIS calls. Potentially, many of these projects could have an indirect impact on IoT and SoS, but it is extremely difficult to evaluate it. For this reason, the investments estimations will be conservative. The analysis is based on the identification of the projects related to IoT/SoS and on the estimation of a correspondent **relevance index** that measures, for each selected project, the fraction of the project that has been focused on IoT and SoS research areas. The relevance index has been subsequently applied to the project costs to estimate the investments devoted specifically to IoT and SoS. The estimation of the relevance index is based on the information collected during the study of the six research streams, on the project research activities, on the project results and on the following three **relevance criteria**:

1. IoT stack macro-components,
2. IoT developed assets,
3. Addressed barriers and challenges.

[49] *https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/*

The methodology adopted for the analysis was organized in four steps (see Figure 41):

1. **Projects analysis**
   The project documentation has been analysed searching for any potential, direct and indirect, relationship with IoT and SoS. The analysis included project deliverables, scientific papers, projects fliers, website documentation, multimedia material and, when possible, direct interview with the project coordinator or with project partners. *This step has been applied to all the 107 projects.*
2. **Project selection**
   The evaluation at the end of the project analysis allowed the identification and selection of only the projects that contributed to the study and development, directly or indirectly, of any technology, architecture, platform and, more in general, any solution related to IoT and SoS. The evaluation also considered the activities focused on the engineering support and the implementation of IoT-based demonstrators, vertical applications and pilots. *Starting from the 107 projects, the selection process identified a subset of 58 projects related to IoT/SoS. 23 projects were excluded because they belong to the area of semiconductor process technologies, equipment, materials and manufacturing, and 26 because they not related to IoT and SoS.*
3. **Criteria evaluation**
   The selected projects have been further analysed to isolate their concrete outcomes, identify which parts of a generic IoT stack are available at the end of the project and which hardware, software or system-level assets have been developed. This step of the analysis also tried to evaluate how the project addressed the barriers that prevent the IoT/SoS uptake and the IoT/SoS challenges. *This phase allowed the values of the relevance criteria to be calculated for each selected project.*
4. **Investments estimation**
   Finally, the results of the relevance criteria evaluation have been used as weighting factors to estimate an IoT/SoS relevance index that, applied to the project costs, made it possible to calculate the investments devoted specifically to IoT and SoS.

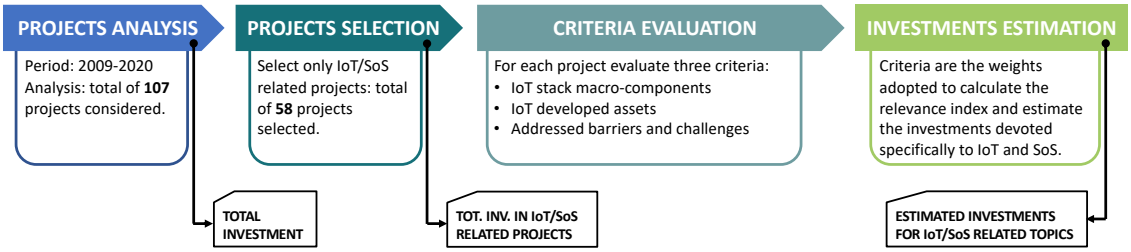


FIGURE 41 — *Methodology adopted for the investment analysis.*

The IoT/SoS relevance index for the selected projects is available in Annex 1, IoT Relevance Index.

The relevance criteria

The **relevance criteria** are the components of the IoT/SoS relevance index and represent three key factors for the uptake of the IoT market that allow an evaluation of whether the project really generated new IoT/SoS technologies and/or solutions, and how they contribute to overcoming IoT/SoS barriers and addressing challenges. *The relevance criteria are intended to estimate the projects' achievements from a practical perspective.*

IoT stack macro-components

Research and innovation in IoT/SoS require comprehensive visibility of the IoT/SoS stack: the intrinsically integrated, interoperable and connected nature of IoT/SoS implies that everything in an IoT solution is interdependent. Therefore, in order for results to be really innovative and effective, research should always keep an end-to-end visibility of the IoT solution, whether research is focused on a specific technology, or on the architecture, or on a platform, etc. For this reason, a relevance criterium that *measures the "coverage" in the project of the concepts related to the IoT/SoS stack* has been introduced.

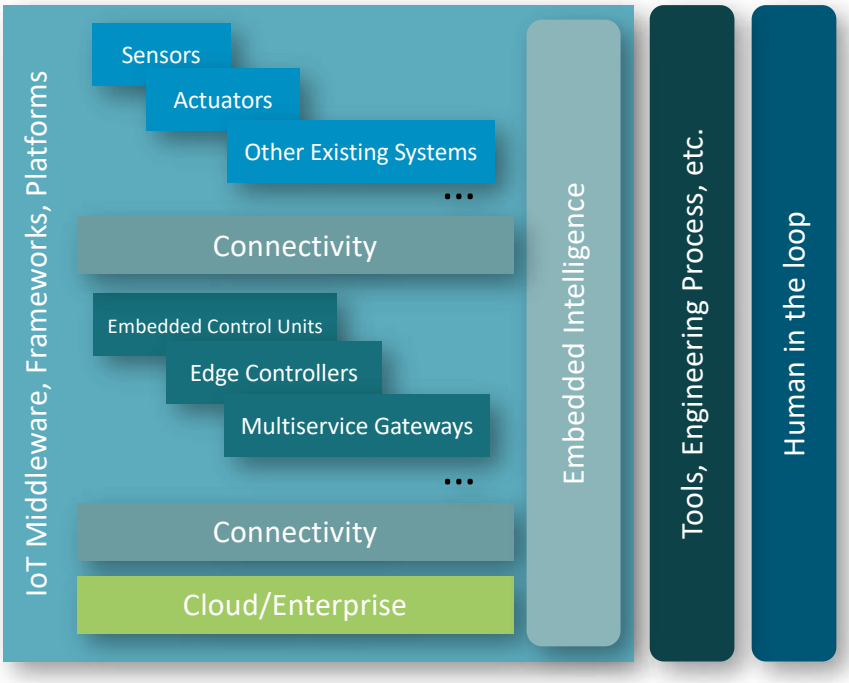


FIGURE 42 — *A common IoT stack.*

Figure 42 provides an example of a generic IoT stack. This example, which can be commonly found in the largest part of IoT solutions, has been used as the reference stack for the evaluation of this relevance criterium. It includes the following elements:

- Sensors, actuators and legacy systems, considered as the very edge of the IoT infrastructure, collecting and processing data, and executing commands.
- Computing nodes on the edge, provided with increased processing power and I/O resources, that act as gateways, bridges or hubs for the data collected from the environment and flowing through the IoT infrastructure (embedded control units, edge controllers, multiservice gateways, existing CPS, legacy embedded systems, etc.).
- All the aspects related to connectivity, field communications, machine to machine connectivity, wide area network communications, etc.

- Software middleware, frameworks and platforms that, depending on the architecture of the IoT solution, represent the load beam of the IoT infrastructure, offering functionalities for hardware abstraction, edge computing, data management, remote control, fleet management, trust, etc.
- Cloud platforms or enterprise-level solutions for data storage, big data processing, fleet remote control, IoT infrastructure monitoring, security, etc.
- The embedded and distributed intelligence, resulting from the integration of hardware technologies, embedded AI, semantics, deep learning, etc.
- The technologies and solutions conceived to make the interaction with humans more simple, friendly and effective.
- The design methods and the engineering tools required to ensure the full lifecycle support for an IoT solution.

The evaluation of this criterium demonstrated a complete alignment with the IoT market analysis and with the current trends, confirming the focus of the research activities on edge computing, on embedded intelligence, on IoT software solutions and the great sensitivity for the engineering support. The limited effort spent on connectivity demonstrates that connectivity is perceived as a commodity, while for cloud and enterprise-level solutions it can be explained with the focus of the research activities on the integration of the IoT with existing enterprise-level software, rather than the creation of new cloud platforms and enterprise solutions that are outside the scope of ARTEMIS and ECSEL initiatives.

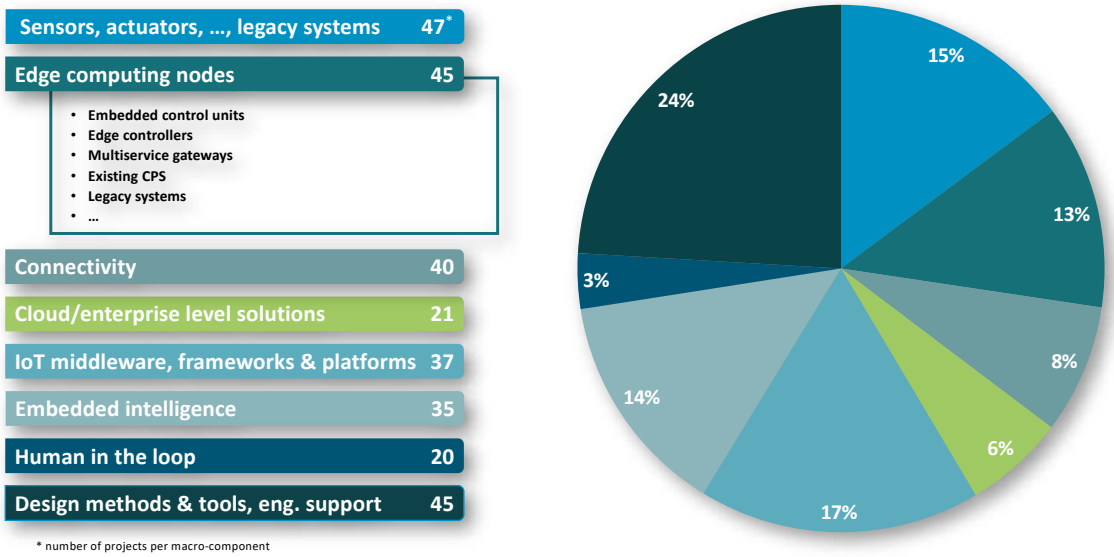


FIGURE 43 — *Percentages of investments by IoT stack macro-components.*

IoT Developed Assets

After having clarified the level of visibility of the IoT stack and having identified the components of the stack addressed by the research activities, the second relevance criterium allows identification of the **assets developed in the project**, both from a hardware, software and system level perspective and with reference to the IoT stack. *This criterium allows the practical achievements obtained in the project to be evaluated.* This relevance criterium considers the following assets:

- Enabling technologies for IoT (including computing architectures, low power solutions, connectivity, embedded devices, WSN, smart objects, sensing/actuation, HMI, etc.).
- Early IoT solutions (HW platforms, SW platforms, early IoT frameworks).
- Design methods, toolchains and tools for the lifetime engineering support.
- IoT-oriented hardware platforms.
- IoT software frameworks and platforms.
- IoT end-to-end solutions.
- Technologies and solutions conceived to support the evolution towards SoS.
- Standards and certifications.

The results of the evaluation of this relevance criterium are aligned with the previous one and demonstrate that the real and concrete results at the end of the projects are positioned in the correct research areas, according to the analysis of IoT/SoS key enablers and of the IoT/SoS trends. The analysis highlighted the importance of enabling technologies that represented a fundamental research topic since the first ARTEMIS calls. 37% of investments devoted to IoT solutions is extremely significant, because it includes both IoT specific hardware platform (7%) and IoT software framework/platforms (15%), allowing the convergence towards complete end-to-end solutions (15%). The 31% of investments devoted to the engineering support is a clear indicator that the community is looking towards results characterised by high TRL levels, engineering support being fundamental for the transformation of scientific and industrial research results into products. The 8% of investments devoted to standards and certification confirms the tendency of the community and of the market to abandon proprietary solutions in favour of open, interoperable and standardised ones. Eventually, the 7% of investment devoted to technologies and solutions conceived to support the evolution of IoT towards SoS demonstrates that the community has a long-term vision of IoT/SoS and is actively working on its implementation.

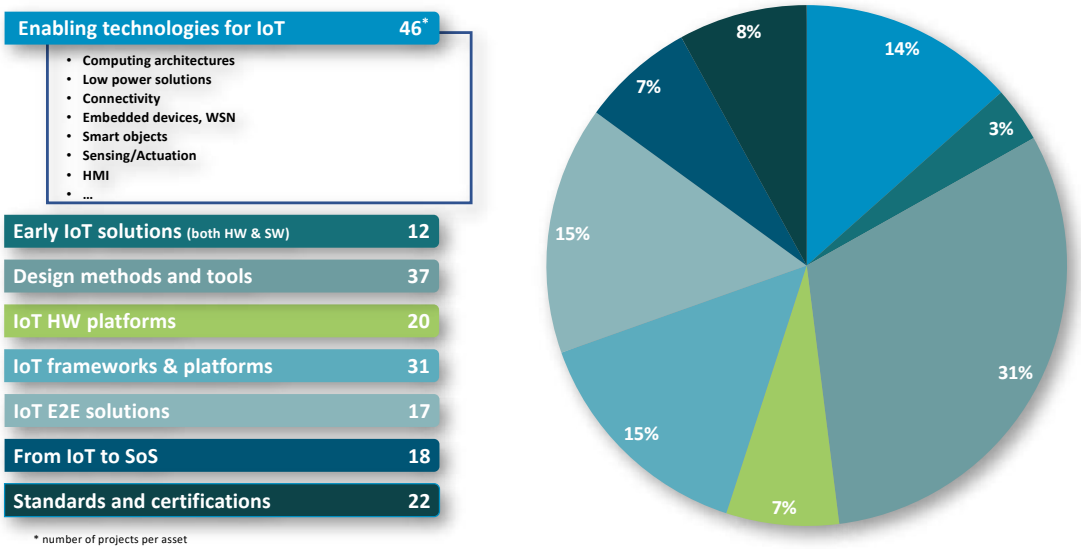


FIGURE 44 — *Percentages of investments by IoT assets.*

Addressed barriers and challenges.

The third relevance criterium is intended *to evaluate the consciousness of the barriers that are preventing the IoT/SoS uptake and the challenges that research has to face*. The criterium has been introduced to measure how much the projects addressed barriers and challenges, and to evaluate the relevance of the proposed solutions. Four **barriers/challenges** have been considered:

- Trust, all its components (security, safety, privacy, dependability, reliability, etc.).
- Interoperability.
- Lack of standards and certifications.
- Availability of IoT/SoS platforms.

Trust, interoperability and IoT platforms are considered fundamental topics of the IoT/SoS research, as demonstrated by the research streams the ARTEMIS and ECSEL community developed in the last decade.

Also, for this criterium the results of the analysis are perfectly aligned with the IoT market study. Trust is really perceived by the community as a critical obstacle and 37% of investments demonstrates the firm resolution to find adequate solutions. A similar importance is reserved for the availability of IoT/SoS platforms that, representing the core technical component of an IoT solution, is crucial for the entire existence of IoT/SoS. Interoperability, standards and certification have been considered extremely seriously in ARTEMIS and ECSEL projects, confirming the intention to valorise the heterogeneity of IoT/SoS, while minimising the market fragmentation and increasing the openness and standardisation of the final solutions.

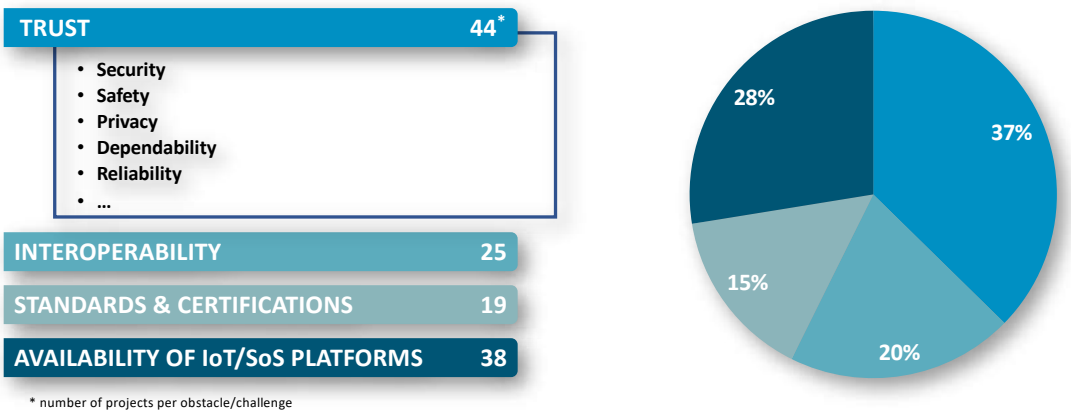


FIGURE 45 — *Percentages of investments by barriers and challenges.*

The relevance index

The IoT relevance index is an estimation intended to quantify the component of the project that has been devoted to IoT and SoS: for each project selected in the second step of the analysis, the index collects the results of the evaluation of project objectives, research topics, technologies, achievements, vertical applications, etc. Numerically, the IoT relevance index is the result of the weighted sum of the single indexes calculated for the relevance criteria. *It provides a numerical value that can be applied to project costs and calculate the estimated investment on IoT and SoS* (see Annex 1 IoT Relevance Index).

On average, the selected projects present a relevance index over 40%, with 39 projects devoted to IoT and SoS for more than 30%, of which 23 are over 40% and 15 over 50%. In the last smaller subset, we find all the projects that represented important milestones for ARTEMIS and ECSEL project lines.

The index appears to be increasing across the ARTEMIS and ECSEL calls for proposals, suggesting that the interest is continually growing, projects are more focused on IoT and SoS topics and, indirectly, indicating an increasing involvement of the community.

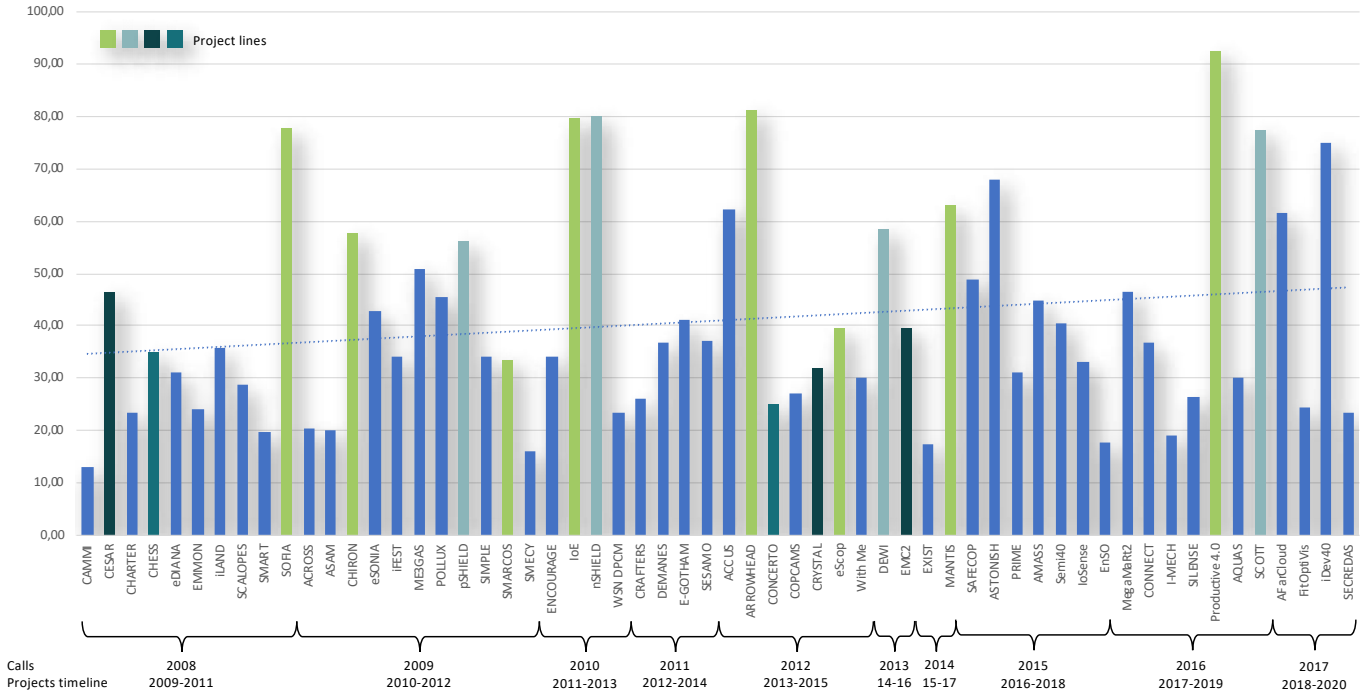


FIGURE 46 — *Evolution of the IoT relevance index across ARTEMIS and ECSEL calls for proposals.*

Investments analysis results

The analysis of the investments highlighted that around **1/3 of the total investments**[50] during the period 2009-2020 has been devoted to IoT and SoS: the total investment for all the projects of the calls 2008-2017 (i.e. the projects active in period 2009-2020) has been estimated at €2082 M, of which €1524 M is the total investment estimated for the projects that directly or indirectly focused on IoT and SoS and, in these projects, the investments devoted exclusively to IoT and SoS research, innovation and development has been estimated at €716 M (Figure 47).

[50] *In the ECSEL calls, the investments of the projects related to semiconductor process technologies, equipment, materials and manufacturing have been excluded from the total for coherence with ARTEMIS calls.*

	Tot. 2009-2020	Artemis (2009-2016)	ECSEL (2014-2020)
Total investments for all the calls 2008-2017[29]	2082 M€	1062 M€	1020 M€
Total investments for IoT/SoS related projects	1524 M€	779 M€	745 M€
Estimated investments only for IoT/SoS topics	**716 M€**	**359 M€**	**357 M€**

FIGURE 47 — *Summary of the investments analysis.*

During the period under consideration, the investments progressively increased with a AAGR[51] of 31% for the investments of the entire calls, of 48% for the investments of only those projects related to IoT and SoS, and of 59% for the investments specifically devoted to IoT and SoS in these projects (see Figure 48, Figure 49).

The evident increase of investments of the last three calls in IoT related projects is mainly due to the presence of very large projects.

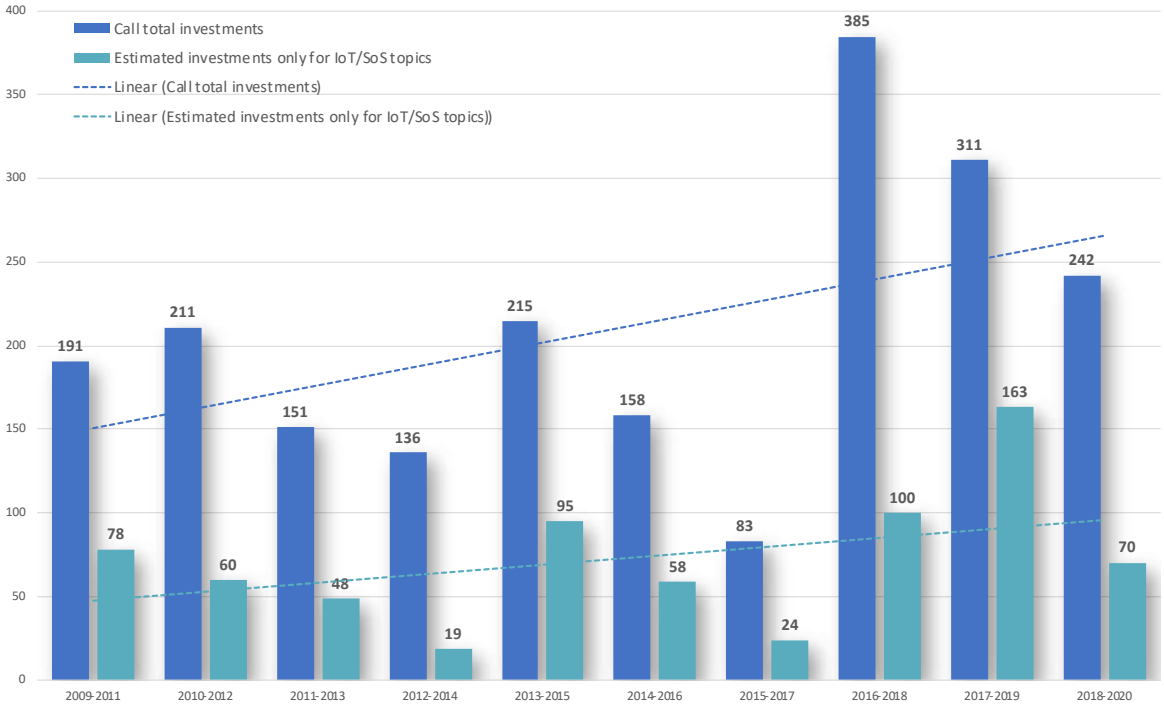


FIGURE 48 — *Total investments of the ARTEMIS and ECSEL calls compared to the estimation of the projects investments specifically devoted to IoT/SoS categorised by calls.*

Starting from 2009, the investments seem to follow a cyclical trend with a period of around three years. These cycles are partially due to the projects' typical duration (three years) and partially to the call management that tends to avoid the replication of the same research topics in subsequent calls. A cycle starts with a call characterised by projects significantly focused on IoT and SoS, followed by two or three calls characterised by a decreasing trend both in terms of research activities and investments.

[51] *Average Annual Growth Rate*

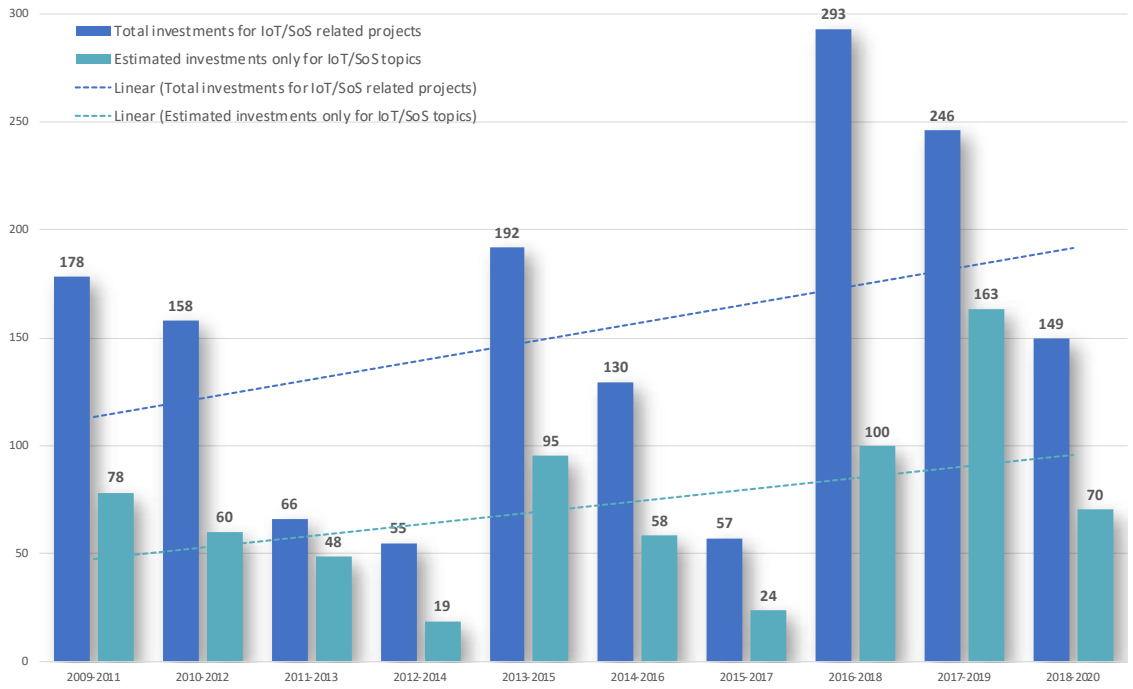


FIGURE 49 — *Total costs of the ARTEMIS and ECSEL projects related to IoT/SoS and estimation of the projects investments specifically devoted to IoT/SoS categorised by calls.*

The number of projects related to IoT/SoS is, in general, decreasing across calls, although the investments are increasing in the aggregate (Figure 50): this trend reflects the market evolution, that is shifting from a large number of small projects, centred on IoT enabling technologies specifically in the first calls, to a smaller number of bigger projects focused more on platforms and end-to-end solutions. This trend reflects the natural evolution of scientific and industrial research, that starts with a widespread investigation, intended to create the initial knowledge base, and gradually converge on specific research streams.

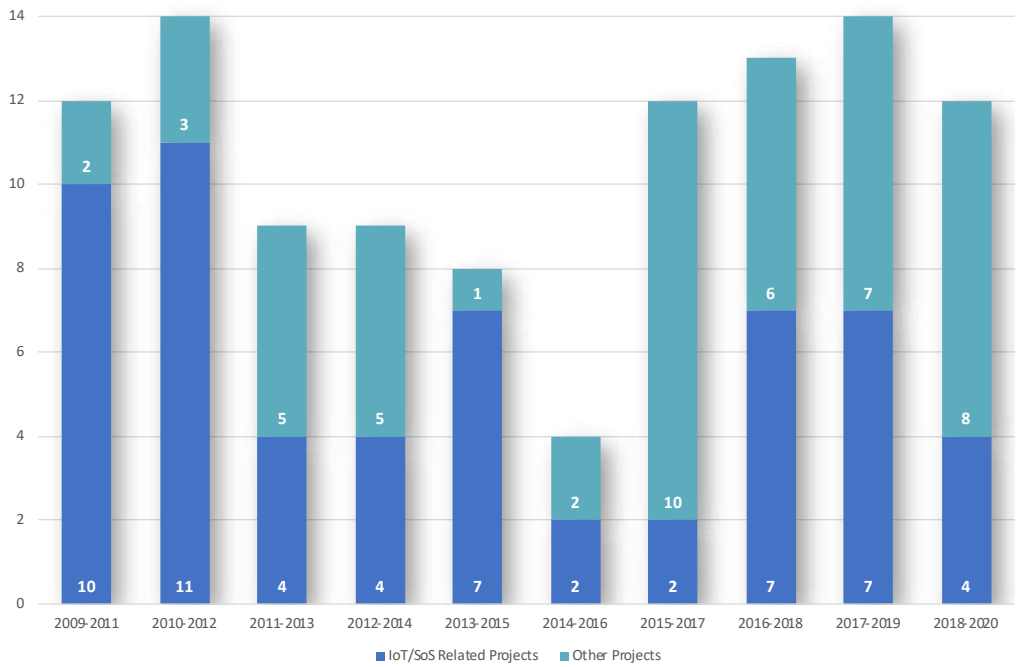


FIGURE 50 — *Number of IoT/SoS related projects.*

As anticipated, the value is shifting along the ECS value chain and the market is expected to grow tenfold in the steps of the value chain focused on fully integrated systems, IoT, SoS, application and solutions. The significant growth in these steps represents a good reason to invest in IoT and SoS, also because IoT becomes a key enabler of the value chain itself.

The analysis of the estimated investments by research stream, asset, obstacle and challenge highlights that the investments are aligned with the shift in the value chain, being largely devoted to its final steps. Moreover, the analysis demonstrates attention to the market trends, to the sensitivity for the potential impact of the technologies and for an increase in the return of investment.

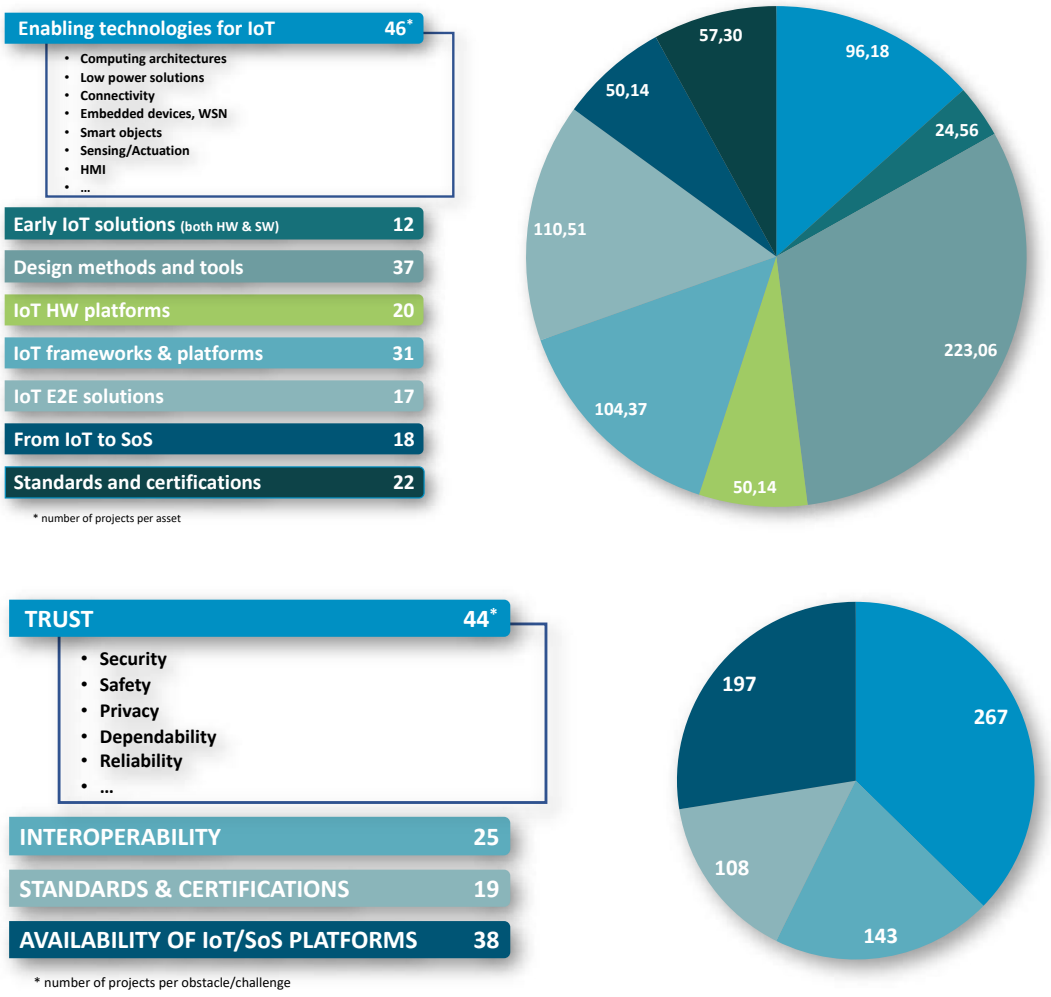


FIGURE 51 — *Estimated investments by asset, obstacle and challenge (€M).*

Conclusions

The Internet of Things has become a reality, with a market that is constantly growing, on a massive scale and with unprecedented opportunities in almost every vertical domain. IoT covers a large section of the ECS value chain and represents a key factor for Europe's future competitiveness and for the realisation of the European Digital Era. IoT will play a crucial role in securing companies' competitive edge, in providing a positive economic impact and ensuring long-lasting societal benefits. For some of the stakeholders involved in the value chain, technology is already generating the first wave of revenues, but a huge effort in research and innovation is required to enable the market scale up to the expected dimensions. To ensure the growth of the IoT market, and its potential evolution towards SoS, we have to identify the right solutions to overcome the existing barriers and face future challenges, with a European ecosystem of companies, RTOs and public institutions committed to competing on a global scale with the fastest growing regions (e.g. Asia) through innovation and with significant private/public investments.

This study demonstrates that the ARTEMIS and ECSEL community have been heading in this direction since the beginning, with concrete projects that devoted and are devoting a large effort to scientific and industrial research in IoT and SoS. The community will play a key role in Europe's digital transformation, providing solutions that are able to capture the upcoming market opportunities in a structured and profitable way, with a combination of academic and industrial research that is capable of maintaining a clear long-term vision and addressing fundamental research, industrial research and eventually efficiently facilitating the adoption of research results in market applications.

The six identified research streams appear fully aligned with IoT market trends, focusing on the most promising (for revenues) and impacting (for society) technologies and vertical applications. The research streams demonstrate the existence of a long-term, wide and shared community vision that is oriented towards the development of solutions to overcome IoT and SoS barriers and tackle the related challenges. The research streams have significantly contributed to the development of the market enablers that are currently transforming IoT in a consolidated reality. From this perspective, the continuous support of the research activities in the last decade is demonstrated by IoT/SoS project lines that have ensured a continuous and coherent evolution of the research streams with rational investments focalised on specific research topics and objectives. The project lines are aligned with the IoT market trends and started in the first ARTEMIS call with visionary ideas that are still extremely relevant today. They involve more than one third of all the ARTEMIS and ECSEL projects related to IoT and SoS, ensuring an improvement of the TRL level over time and demonstrating the maturity of the community that looks beyond the lifetime of a single project.

The investments in IoT and SoS research have been and still are considerable, with a continuous growth that must be supported and consolidated in order to be able to compete at a global level with the fastest and massively growing areas (e.g. Asia and North America), ensuring at least alignment or, even better, a competitive advantage. Investments are also fundamental to preserve the IoT market enablers and the acceleration of strategic areas such as IoT platforms, trust, interoperability and engineering support. Investments should also cover the entire IoT value chain with a progressive increase towards SoS, applications and solutions, as the value is already significantly shifting towards the higher levels of the value chain that are expected to grow tenfold: electronic components and devices are fundamental for IoT and SoS but the overall market and society uptake are driven by applications and solutions for the final user.

This study demonstrates that the direction in which the ECSEL community is heading is the right one, but this is just the first set of a difficult match, in an international arena full of strong competitors. If the estimates are correct, in 3-5

years Europe will have to be able to support three times the number of devices connected today. How will this work? What companies, governments and standards organisations need to support this growth? Devices don't just connect by themselves and the impact of such a number of connected devices is not trivial. A single digital market in Europe, supported by standards and a strong digital infrastructure are key for successful deployment.

Connectivity is the first key factor for the uptake of IoT and SoS, but is not yet uniformly available in Europe and future coverage represents a challenge for businesses and governments. Fortunately, the inherent nature of the solutions based on IoT will simplify the coverage of these areas, but the IoT solutions must be able to scale up to the enormous numbers that the predictions estimate. Scalability is at the heart of this problem. The number of connected devices will generate massive amounts of data. Will the proposed solutions be capable to collect, transport, store and analyse this avalanche of data? Will they be able to efficiently search information through it? How will information be kept secure and private? Each of these issues requires an immediate answer. Because finding timely actionable information within these vast data stores could be difficult and expensive. Because the costs of data collection, storage and analytics could become unsustainable and require the identification of adequate business models. Because a similar amount of data makes trust an enormous issue and concern.

Five major challenges have to be addressed to provide solutions adequate to the societal needs and to the market demand, ensuring also the evolution of IoT towards SoS:

- Fill the lack of trust in IoT technologies with end-to-end human-centric solutions that cover the entire IoT stack and the entire lifecycle of the product as well as with investments in communication, marketing and training, and with specific regulations that extend largely beyond the GDPR. Europe should define a common "Trust" strategy and a strong coordinated policy, involving the stakeholders and all member states.
- Ensure an adequate level of interoperability, the right trade-off between confidentiality required from companies and the level of openness required by IoT/SoS value networks to flourish beyond brands, industries, technologies, standards and vertical domain boundaries.
- Develop open IoT/SoS platforms that are more ubiquitous with hyper-connectivity, more pervasive with miniaturised and low-power physical nodes, more autonomous with embedded intelligence, more light and sustainable through edge computing, and more open through cross-brand and cross-domain interoperability, etc. IoT/SoS platforms are fundamental to securely and efficiently orchestrate and manage the entire IoT/SoS infrastructure. They represent an enabling factor even for the existence of IoT/SoS value networks.
- Provide engineering support for the entire lifecycle of the IoT solutions. Engineering support allows the research results to be capitalised, valorised and transformed into real products. But it also ensures the continuous engineering of trust, sustainability, scalability, evolvability, flexibility, etc. of IoT/SoS solutions, across all the phases of their lifecycle, from product design to development, deployment, operation, maintenance, evolution, retirement and recycling.
- Define a pan European strategy to bundle forces and develop a solid European IoT ecosystem, able to support IoT/SoS innovation and market development. An ecosystem emerging from the cooperation of European industries, RTOs and institutions, able to support the IoT value networks with European policies, common strategies, roadmaps and standards, and with joint public-private funding.

To address these challenges and ensure the IoT uptake, the ECSEL community must evolve in a wider ecosystem of stakeholders really conscious of the interdisciplinarity and heterogeneity of IoT and SoS, committed to sharing and joining their forces and expertise to fully cover the future IoT and SoS value networks, with end-to-end trustworthy solutions able to sustainably manage the entire lifecycle of IoT and SoS.

The ARTEMIS Working Group "From IoT to SoS"

Internet of Things and System of Systems represent central topics for the ARTEMIS Industrial Association and for the ARTEMIS community, which has invested significant resources for scientific and industrial research in these areas and played an important role in the definition of a strategy that, during the last decade, has written part of the IoT and SoS history. In 2017, the ARTEMIS-IA established a specific Working Group, called "From IoT to SoS", to track the achievements from ARTEMIS and ECSEL programmes, to promote interdisciplinary research in IoT/SoS, to contribute to the ECSEL SRA regarding IoT/SoS topics, to monitor and study the evolution of IoT/SoS, in terms of pervasive technologies, digital platforms, global standards, data governance, engineering tools and business models.

CHAIRMAN OF THE WORKING GROUP

Paolo Azzoni

EUROTECH Group

Paolo Azzoni is the Research Program Manager at EUROTECH Group. He is responsible for planning and directing industrial research projects, investigating technologies beyond the state of the art in the areas of cyber-physical systems, intelligent systems, machine-to-machine distributed systems, edge computing, internet of things and digitalization solutions. Since 2007, he represents EUROTECH in the ARTEMIS Industrial Association. He is currently member of the ARTEMIS-IA Steering Board, of the ARTEMIS-IA Presidium and he is the Chairman of the Working Group "From IoT to System of Systems". In 2006 he joined ETHLab, the EUROTECH Research Center, as Research Project Manager and he has been responsible for the research projects in the domains of embedded and pervasive systems. Previously, he was involved in academic lecturing and research in the areas of hardware formal verification, hardware/software co-design and co-simulation, advanced hardware architectures and operating systems. He participated in several European research projects in the contexts of FP7, ARTEMIS, Aeneas, ECSEL and H2020, and he is a European Community Independent Expert. He holds a Master Degree in Computer Science and a second Master Degree in Intelligent Systems.

MEMBERS OF THE WORKING GROUP

Ad ten Berg

ARTEMIS-IA Office

Ad ten Berg has the MSc degree in Electronic Engineering from the University of Twente. From 1983 to 1988, he was with Philips Semiconductors and later Stork Brabant, both in software engineering functions. From 1988 to 1995 he was Assistant Professor at the Faculty of Informatics at the University of Twente in Computer Architecture. He moved in 1995 to Philips Research where he headed a software engineering group on Computer Aided Design. In 2001, he switched to lead the research group on VSLI Design and Test and went on in 2006 to NXP Semiconductors when it spun-off from Philips. At NXP, he formed a new research group on Embedded Systems. In 2009, he moved to ARTEMIS-IA where he became Office Director in 2011.

Patrick Blouet

ST Microelectronics

Patrick Blouet is an electronic and computer science engineer. He holds a Master degree from ENSERB in 1981 in France. He worked in different companies before STMicroelectronics, where he was in charge of designing and developing systems in the area of telecommunication, image processing, hard real time, multi processors systems with a very strong background in software development. He then joined STMicroelectronics where he had several responsibilities in the domain of development tools and applications around DSP and complex processors chips. He also had marketing responsibilities for telecom products and was in charge of the architecture group for mobile application processors in ST. He then moved to the corporate partnerships and public affairs where he created and managed several big European projects. He contributed in several European clusters like Catrene, ETP4HPC and was deeply involved in the creation and set-up of the IPCEI on microelectronics in Europe.

Jerker Delsing

Lulea Technical University

Prof. Jerker Delsing received the M.Sc. in Engineering Physics at Lund Institute of Technology, Sweden 1982. In 1988 he received the PhD. degree in Electrical Measurement at the Lund University. During 1985 - 1988 he worked part time at Alfa-Laval - SattControl (now ABB) with development of sensors and measurement technology. In 1994 he was promoted to associate professor in Heat and Power Engineering at Lund University. Early 1995 he was appointed full professor in Industrial Electronics at Lulea University of Technology where he currently is the scientific head of EISLAB, http://www.ltu.se/eislab. His present research profile can be entitled IoT/SoS Automation, with applications to automation in large and complex industry and society systems. Prof. Delsing and his EISLAB group has been a partner of several large EU projects in the field, e.g. Socrades, IMC-AESOP, Arrowhead, FAR-EDGE, Productive4.0 and Arrowhead Tools. Delsing holds positions as a board member of ARTEMIS, ProcessIT.EU and ProcessIT Innovations.

Leire Etxeberria Elorza

Mondragon Unibertsitatea

Leire Etxeberria obtained the PhD degree in Information and Communication Technologies from Mondragon Unibertsitatea (Spain) in 2008. Previously she finished the BSc in Computer Science Engineering at Mondragon University (Spain) in 2004. She is nowadays working as lecturer/researcher in the Electronics and Computer Science Department of Mondragon Unibertsitatea. Her research topics include software product lines, model driven development, variability and V&V, variability/ reuse and safety, etc. in the embedded systems and cyber-physical systems domain. Since September 2016, she is the coordinator for looking European projects for the Department of Electronics and Informatics of the Engineering faculty of Mondragon Unibertsitatea. She has participated in numerous European projects (CSA-Industry 4.E ECSEL, ARTEMIS-JU nSafecer, ARTEMIS-JU Crafters, H2020-Rennovates, H2020-HiFi-ELEMENTS, ITEA3-TESTOMAT, etc.). She has coordinated the CPSBudi project within the H2020 CPSELabs project. She is the coordinator of DiManD: Digital Manufacturing and Design Training Network, Marie Skłodowska-Curie Actions (MSCA), Innovative Training Networks (ITN), H2020-MSCA-ITN-2018, 2019-2022.

Juha Röning

University of Oulu

Juha Röning is Professor of Embedded System at the University of Oulu. He serves also as Visiting Professor of Tianjin University of Technology, P. R. China. He is principal investigator of the Biomimetics and Intelligent Systems Group (BISG). In 1985 he received Asla/Fullbright scholarship. From 1985 to 1986 he was a visiting research scientist in the Center for Robotic Research at the University of Cincinnati. From1986 to1989 he held a Young Researcher Position in the Finnish Academy. In 2000 he was nominated as Fellow of SPIE. He has three patents and has published more than 300 papers in the areas of computer vision, robotics, intelligent signal analysis, and software security. He is currently serving as a Board of Director for euRobotics aisbl. He is also a steering board member of ARTMIS-IA.

Marina Settembre

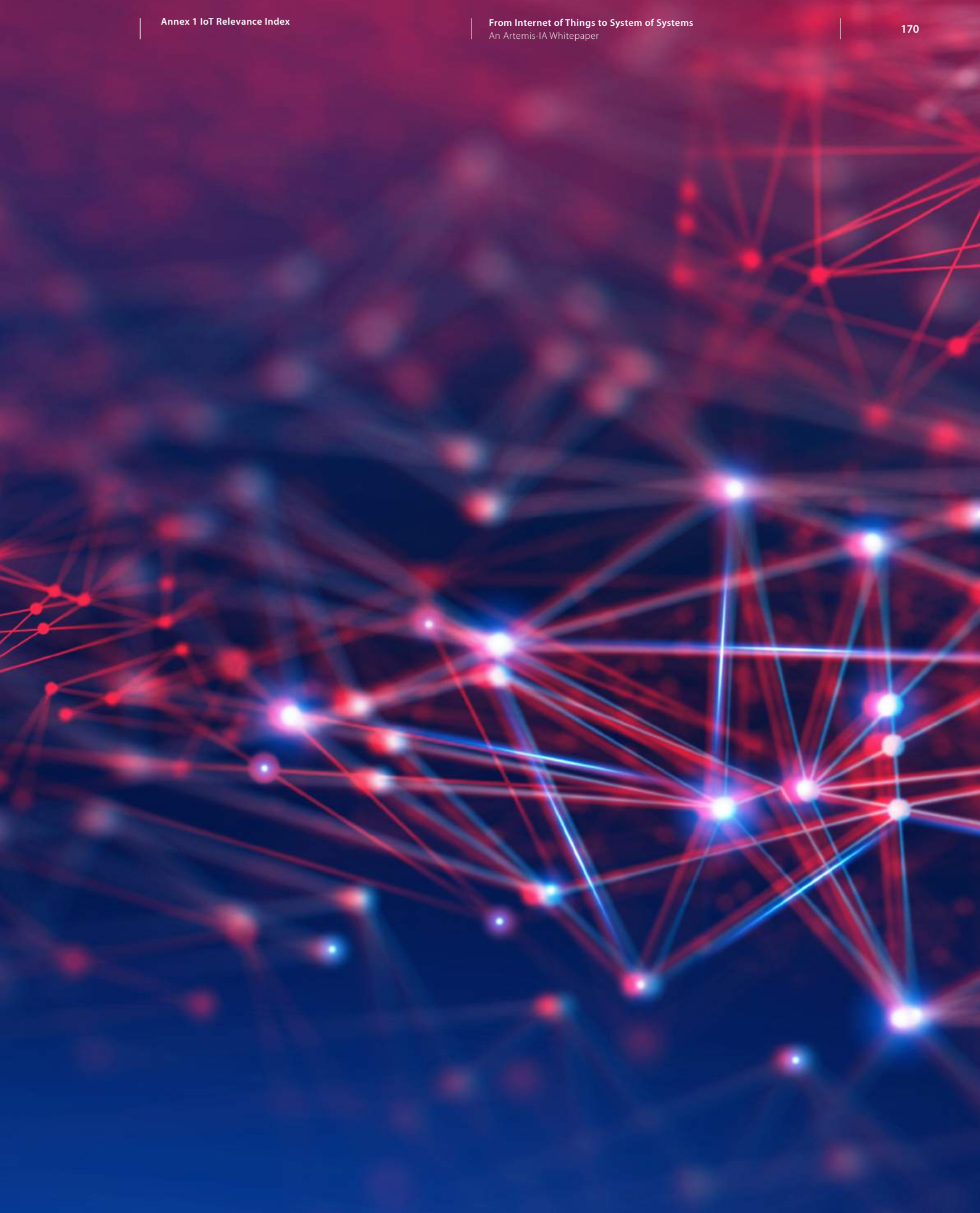
Leonardo

Marina Settembre graduated in Physics at the University of Rome "la Sapienza". For over thirty years she has been deeply interested in technology, process & product innovation and in digital & emerging technologies. From 1986 to 2000 she worked as a Research Scientist at the Fondazione U. Bordoni in the Optical Communication Division. From 2000 to 2008 she joined Ericsson Lab Italy / Marconi working on network architectures & traffic engineering and as IPR Coordinator. Since 2008 she has been part of Leonardo company (ex Finmeccanica), currently working in Cyber Division - Product & Technology Development area as Innovation & Technology Scientist. She has published more than 100 papers in scientific conference journals and proceedings and a book "Non-linear Optical Communication Networks" (ed. Wiley & Sons, 1998). She took part in several EU and National Research Projects and is member of ARTEMIS IA -WG "From IoT to SoS".

Stefan Van Baelen

IMEC

Stefan Van Baelen obtained his PhD in Computer Science at KU Leuven, Belgium. He has been active for several years as senior researcher in the field of model-driven engineering for embedded systems at the imec-DistriNet research group of KU Leuven. In 2012 Stefan became research coordinator Software Technologies and Europe at iMinds, the Belgian-Flemish strategic research centre on ICT. As of October 1st, 2016, iMinds has merged with imec into one high-tech research and innovation hub for nanoelectronics and digital technologies, under the name imec. As Funded Project Manager at imec, Stefan is responsible for the acquisition of European and national projects for the Digital & User Centric Solutions (DUCS) and Enabling Digital Transformations (EDiT) business teams. Stefan is a.o. Steering Board member and Scientific Council Member of ARTEMIS-IA, member of the Board of Directors of the Big Data Value Association (BDVA) and Core Group Member of the EUREKA Celtic-Next cluster.



Annex 1 IoT Relevance Index

Call	Project spanning	Project	Tot. cost (M€)	EU Funding (M€)	Relevance index criteria			Relevance Index (%)
					Obstacles & challenges	*Macro components*	*Assets*	
Call 2008	*Investments 2009-2011*	CAMMI	7,32	1,98	*10,00*	*1,50*	*1,50*	13,00
		CESAR	54,92	9,17	*30,00*	*6,00*	*10,50*	46,50
		CHARTER	5,24	0,87	*10,00*	*6,00*	*7,50*	23,50
		CHESS	11,92	1,99	*20,00*	*6,00*	*9,00*	35,00
		eDIANA	17,33	2,89	*20,00*	*5,25*	*6,00*	31,25
		EMMON	2,58	0,43	*10,00*	*8,25*	*6,00*	24,25
		iLAND	3,91	0,65	*20,00*	*9,75*	*6,00*	35,75
		SCALOPES	34,01	5,68	*10,00*	*10,50*	*8,25*	28,75
		SMART	4,46	0,74	*10,00*	*8,25*	*1,50*	19,75
		SOFIA	36,54	6,1	*35,00*	*22,50*	*20,25*	77,75
		Totals 2008:	178,23	30,5				
Call 2009	*Investments 2010-2012*	ACROSS	16,04	2,68	*10,00*	*6,00*	*4,50*	20,50
		ASAM	5,38	0,9	*5,00*	*7,50*	*7,50*	20,00
		CHIRON	17,77	3	*30,00*	*18,00*	*9,75*	57,75
		eSONIA	12,08	2,02	*25,00*	*12,75*	*5,25*	43,00
		iFEST	15,13	2,53	*10,00*	*13,50*	*10,50*	34,00
		ME3GAS	14,64	2,47	*22,50*	*19,50*	*9,00*	51,00
		POLLUX	32,48	5,5	*20,00*	*18,75*	*6,75*	45,50
		pSHIELD	5,37	0,9	*30,00*	*18,00*	*8,25*	56,25
		SIMPLE	7,43	1,24	*20,00*	*11,25*	*3,00*	34,25
		SMARCOS	12,38	2,07	*12,50*	*16,50*	*4,50*	33,50
		SMECY	19,38	3,27	*2,50*	*6,00*	*7,50*	16,00
		Totals 2009:	**158,08**	**26,58**				

Call	Project spanning	Project	Tot. cost (M€)	EU Funding (M€)	Relevance index criteria			Relevance Index (%)
					Obstacles & challenges	*Macro components*	*Assets*	
Call 2010	*Investments 2011-2013*	ENCOURAGE	6,29	1,05	*12,50*	*14,25*	*7,50*	34,25
		IoE	44,06	7,36	*40,00*	*20,25*	*19,50*	79,75
		nSHIELD	13,13	2,09	*35,00*	*26,25*	*18,75*	80,00
		WSN DPCM	2,57	0,43	*10,00*	*7,50*	*6,00*	23,50
		Totals 2010:	**66,05**	**10,93**				
Call 2011	*Investments 2012-2014*	CRAFTERS	15,95	2,66	*5,00*	*9,75*	*11,25*	26,00
		DEMANES	20,14	3,36	*15,00*	*12,75*	*9,00*	36,75
		E-GOTHAM	6,96	1,16	*20,00*	*13,50*	*7,50*	41,00
		SESAMO	12,01	1,97	*20,00*	*8,25*	*9,00*	37,25
		Totals 2011:	**55,06**	**9,15**				
Call 2012	*Investments 2013-2015*	ACCUS	7,79	1,93	*30,00*	*12,75*	*19,50*	62,25
		ARROWHEAD	65,69	10,97	*40,00*	*21,75*	*19,50*	81,25
		CONCERTO	9,65	1,61	*10,00*	*7,50*	*7,50*	25,00
		COPCAMS	13,35	2,23	*15,00*	*7,50*	*4,50*	27,00
		CRYSTAL	80,68	13,47	*20,00*	*6,00*	*6,00*	32,00
		eScop	5,81	0,97	*20,00*	*12,75*	*6,75*	39,50
		With Me	8,9	1,49	*10,00*	*11,25*	*9,00*	30,25
		Totals 2012:	**191,87**	**32,67**				
Call 2013	*Investments 2014-2016*	DEWI	38,5	6,43	*30,00*	*19,50*	*9,00*	58,50
		EMC2	91,05	15,22	*20,00*	*12,00*	*7,50*	39,50
		Totals 2013:	**129,55**	**21,65**				
		Total ARTEMIS:	**778,84**	**131,48**				
Call 2014	*Investments 2015-2017*	EXIST	27,385	8,77	*10,00*	*4,50*	*3,00*	17,50
		MANTIS	29,86	9,79	*30,00*	*21,00*	*12,00*	63,00
Totals 2014:			**57,245**	**18,56**				

Call	Project spanning	Project	Tot. cost (M€)	EU Funding (M€)	Relevance index criteria			Relevance Index (%)
					Obstacles & challenges	*Macro components*	*Assets*	
Call 2015	*Investments 2016-2018*	SAFECOP	11,6	3,78	*25,00*	*13,50*	*10,50*	49,00
		ASTONISH	18,33	5,89	*35,00*	*19,50*	*13,50*	68,00
		PRIME	38,85	12,2	*10,00*	*12,00*	*9,00*	31,00
		AMASS	20,53	6,2	*30,00*	*6,00*	*9,00*	45,00
		Semi40	61,97	12,23	*15,00*	*16,50*	*9,00*	40,50
		IoSense	65,27	14,65	*15,00*	*10,50*	*7,50*	33,00
		EnSO	76,44	18,73	*5,00*	*11,25*	*1,50*	17,75
		Totals 2015:	**292,99**	**73,68**				
Call 2016	*Investments 2017-2019*	MegaMaRt2	15	4,44	*30,00*	*6,00*	*10,50*	46,50
		CONNECT	17,35	5,15	*15,00*	*13,50*	*8,25*	36,75
		I-MECH	17,04	5,03	*10,00*	*6,00*	*3,00*	19,00
		SILENSE	29,33	8,7	*10,00*	*13,50*	*3,00*	26,50
		Productive 4.0	112,05	27,45	*40,00*	*28,50*	*24,00*	92,50
		AQUAS	15,5	4,61	*15,00*	*7,50*	*7,50*	30,00
		SCOTT	39,7	10,51	*40,00*	*18,00*	*19,50*	77,50
		Totals 2016:	**245,97**	**65,89**				
Call 2017	*Investments 2018-2020*	AFarCloud	28,3	8,7	*30,00*	*21,00*	*10,50*	61,50
		FitOptiVis	22,5	6,7	*5,00*	*10,50*	*9,00*	24,50
		iDev40	47,1	10,9	*30,00*	*27,00*	*18,00*	75,00
		SECREDAS	51,5	14,87	*10,00*	*7,50*	*6,00*	23,50
		Totals 2017:	**149,4**	**41,17**				
		Total ECSEL:	**745,605**	**199,3**				
		Total:	1524,445	330,78				

For the projects' descriptions, please refer to the ARTEMIS and ECSEL websites and to the following publications:

- ARTEMIS Book of projects, Volume 1, ARTEMIS Joint Undertaking, First edition, September 2010
- ARTEMIS Book of projects, Volume 2, ARTEMIS Joint Undertaking, First edition, October 2012
- ARTEMIS Book of projects, Volume 3, ARTEMIS Joint Undertaking, First edition, June 2014
- ECSEL Book of projects, Volume 1, ECSEL Joint Undertaking, First edition, October 2016
- ECSEL Book of projects, Volume 2, ECSEL Joint Undertaking, First edition, June 2018

Glossary

AI	*Artificial Intelligence*
API	*Application Program Interface*
AIMD	*Active Implantable Medical Device*
CAGR	*Compound Annual Growth Rate*
CPS	*Cyber Physical System*
DNN	*Deep Neural Network*
DLT	*Distributed Ledger Technology*
E&CPS	*Embedded Software & Cyber-Physical System*
ECS	*Electronic Components & Systems*
EHR	*Electronic Health Record*
EHPC	*Embedded High-Performance Computing*
FD-SOI	*Fully Depleted Silicon On Insulator*
GDP	*Gross Domestic Product*
GERD/GOVERD	*Gross Domestic Expenditure on R&D/Government Expenditure on R&D*
GPT	*General-Purpose Technology platform*
IaaS	*Infrastructure as a Service*
ICT	*Information and Communications Technologies*
ITS	*Intelligent Transport System*
IoT	*Internet of Things*
LIDAR	*Light Detection and Ranging*
MaaS	*Mobility as a Service*
MEMS	*Microelectromechanical System*
MISP	*Multi-IoT Service Platform*
M2M	*Machine to Machine*
NB IoT	*Narrow-Band Internet of Things*
NLU/NLP	*Natural Language Understanding/Natural Language Processing*
PaaS	*Platform as a Service*
R&D&I	*Research, Development and Innovation*
RTO	*Research and Technology Organisation*
SaaS	*Software as a Service*
SIC	*Silicon Carbide*
SIP	*Systems-in-Package*
SME	*Small and Medium-sized Enterprise*
SoC	*System-on-Chip*
SoS	*System of Systems*
SRA	*Strategic Research Agenda*
TRL	*Technology Readiness Level*
V2X	*Vehicle-to-everything*
WBG	*Wideband Gap*
WSN	*Wireless Sensor Network*

ARTEMIS
Industry Association