White Paper

IoT 2020: Smart and secure IoT platform

Executive summary

Internet of Things (IoT) market forecasts show that IoT is already making an impact on the global economy. While estimates of the economic impact during the next five to ten years vary slightly (IDC estimates USD 1,7 trillion in 2020 [1], Gartner sees a benefit of USD 2 trillion by that time [2], and McKinsey predicts growth of USD 4 trillion to USD 11 trillion by 2025 [3]), there seems to be a consensus that the impact of IoT technologies is substantial and growing.

Although a significant impact already exists, Gartner notes that both IoT and the business models associated with it are immature at this point [2], hence the huge transformation that the economy – and maybe even society as a whole – will face from the Internet of Things is still to come.

This IEC White Paper provides an outlook on what the next big step in IoT – the development of smart and secure IoT platforms – could involve. These platforms offer significant improvements in capabilities in the field of security and bridge the gaps between different existing IoT platforms, which usually consist of "legacy" systems that have not been designed for IoT purposes. Gartner predicts that by 2020, 80% of all IoT projects will have failed at the implementation stage due to improper methods of data collection [4]. Hence, one of the main objectives of the smart and secure IoT platform is to serve as a "platform of platforms".

After providing an overview of where IoT currently stands, with a particular focus on IoT system design as well as architecture patterns, the limitations and deficiencies of the current IoT framework are similarly identified in this White Paper. Such limitations and deficiencies involve topics such as security, interoperability and scalability. To derive capabilities and requirements for the next-generation smart and secure IoT platform, several use cases from the industry, public and customer domains are investigated. Based on these use cases and their different focus areas, the capabilities and requirements for smart and secure IoT platforms are deduced. Subsequently, next-generation enabling technologies for smart and secure IoT platforms are discussed, with a strong focus on platform-level technologies in the field of connectivity, processing and security.

Bringing the ambitious visions connected with the Internet of Things to fruition will require significant efforts in standardization – e.g. development of initiatives to enable interoperability – thus this White Paper presents a desired future IoT standardization ecosystem environment to address those needs.

This White Paper concludes by formulating recommendations both of a general nature as well as specifically addressed to the IEC and its committees. The principal recommendations proposed for the IEC include:

- Taking the lead in establishing an IoT standardization ecosystem environment with IEC exercizing a key role.
- Assigning tasks to the ISO/IEC JTC 1 leadership concerning key IoT standardization activities.
- Working more closely with government entities to increase their level of participation and to identify the related requirements and concerns to be addressed by IEC deliverables.

Acknowledgments

This White Paper has been prepared by the IoT 2020 project team in the IEC Market Strategy Board (MSB), with a major contribution from the project leader, SAP and project partner, Fraunhofer AISEC. The project team met four times – November 2015 (Walldorf, DE), January 2016 (Munich, DE), March 2016 (Tokyo, JP) and May 2016 (Walldorf, DE) – and held a number of online conference calls. The project team includes:

Mr. Bernd Leukert, SAP, MSB Member, Project Director

Dr. Dr. Timo Kubach, SAP, Project Manager

Dr. Claudia Eckert, Fraunhofer AISEC, Project Partner

Dr. Kazuhiko Tsutsumi, Mitsubishi Electric, MSB Member

Mr. Mark Crawford, SAP

Ms. Nina Vayssiere, SAP

Mr. Ebin Thomas Kandathil, SAP

Dr. Uwe Kubach, SAP

Mr. Anirban Majumdar, SAP

Mr. Alan Southall, SAP

Mr. Fabian Biegel, SAP

Ms. Krista Grothoff, Fraunhofer AISEC

Mr. Mario Hoffmann, Fraunhofer AISEC

Mr. Philipp Stephanow, Fraunhofer AISEC

Dr. Seisuke Kano, AIST

Dr. Hiroyuki Sawada, AIST

Dr. Kai Cui, Haier

Dr. Daisuke Matsubara, Hitachi

Dr. Motonobu Saito, Hitachi

Mr. Tadashi Kaji, Hitachi

Dr. Yun Chao Hu, Huawei Technologies

Mr. Xiangqun Liu, Huawei Technologies

Dr. Jijun Luo, Huawei Technologies

Mr. Ulrich Graf, Huawei Technologies

Dr. Sadayuki Watanabe, METI

Dr. Tetsushi Matsuda, Mitsubishi Electric

Mr. Noritaka Okuda, Mitsubishi Electric

Dr. Yasunori Mochizuki, NEC Corporation

Dr. Ernoe Kovacs, NEC Corporation

Mr. Hiroshi Takechi, NEC Corporation

Dr. Akihisa Ushirokawa, NEC Corporation

Dr. Fang-Jing Wu, NEC Corporation

Mr. Peter Lanctot, IEC, MSB Secretary

Table of contents

List of abbreviations

Technical and scientific terms

5G	5th generation cellular access
ACE	authentication and authorization for constrained environments
ADECP	autonomous data exchange control profile
API	application programming interface
ARM	architectural reference model
ASE	asymmetric searchable encryption
BCM	business continuity management
CACC	cooperative adaptive cruise control
CAGR	compound annual growth rate
CAM	cooperative awareness message
CMMI	capability maturity model integration
CoAP	constrained application protocol
COP	common operational picture
CPS	cyber physical system
CRISP-DM	cross industry standard process for data mining
CRM	customer relationship management
CT	communication technology
DENM	decentralized environmental notification message
DevOps	development and operations
DPM	digital product memory
eMTC	enhancements for machine type communications
ERP	enterprise resource planning
FCW	forward collision warning
GPS	global positioning system
GSM	global system for mobile communications
HSM	hardware security module
HSPA	high speed packet access
HTTP	hypertext transfer protocol

HV	host vehicle
HW	hardware
I/O	input/output
IaaS	infrastructure as a service
IAM	identity and access management
ICT	information and communications technology
IIRA	industrial internet reference architecture
IM	identity management
IMT-Advanced	international mobile telecommunications-advanced
IoT	Internet of Things
IoT-A	Internet of Things architecture
IoT RA	Internet of Things reference architecture
IP	internet protocol
IRI	internationalized resource identifier
IT	information technology
LAN	local area network
LPWAN	low power wireless access network
LTE	long term evolution
M2M	machine to machine
MBB	mobile broadband
MES	manufacturing execution system
MoU	memorandum of understanding
MQTT	message queuing telemetry transport
NB-IoT	narrowband Internet of Things
NFC	near field communication
NGSI	next generation service interface
OEM	original equipment manufacturer
OIDC	OpenID Connect
OODA	observe-orient-decide-act
OPC	object linking and embedding for process control
OpenIOC	open indicators of compromise

OSS	open source software
OT	operational technology
OWL	web ontology language
PaaS	platform as a service
PDCA	plan-do-check-act
PIR	private information retrieval
PKI	public key infrastructure
PLC	programmable logic controller
PLM	product lifecycle management
POS	point of sale
ProSe	proximity service
PUF	physical unclonable function
QC	quality control
QoS	quality of service
RAMI 4.0	reference architectural model industrie 4.0
RAT	radio access technology
RDF	resource description framework
REST	representational state transfer
REST API	RESTful application programming interface
RFID	radio frequency identification
ROI	return on investment
RSU	roadside unit
RV	remote vehicle
SAML	security assertion markup language
SC	subcommittee
SCIM	system for cross-domain identity management
SCM	supply chain management
SDN	software defined networking
SDO	standards developing organization
SDP	software defined perimeter
SLA	service level agreement

SMG	semantic mediation gateway
SSE	symmetric searchable encryption
SSO	single sign-on
STIX	structured threat information expression
SW	software
TAXII	trusted automated exchange of indicator information
TCP	transmission control protocol
TLS	transport layer security
TPM	trusted platform module
TSP	trust, security and privacy
UML	unified modeling language
UWB	ultra wideband
VPN	virtual private network
WAN	wide area network
WG	working group
WoT	web of trust

Organizations, institutions and companies

3GPP	3rd Generation Partnership Project
AIOTI	Alliance for Internet of Things Innovation
AISEC	Fraunhofer Institute for Applied and Integrated Security
AIST	Advanced Industrial Science and Technology
BITKOM	German Federal Association for Information Technology, Telecommunications and New Media
BMWi	German Federal Ministry for Economic Affairs and Energy
CSA	Cloud Security Alliance
IDC	International Data Corporation
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
ISO	International Organization for Standardization

ISO/IEC JTC 1	Joint Technical Committee 1 of ISO and IEC
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
METI	Japanese Ministry of Economy, Trade and Industry
MIT	Massachusetts Institute of Technology
MSB	Market Strategy Board (of the IEC)
NGMN	Next Generation Mobile Networks Alliance
NIST	National Institute of Standards and Technology
OMA	Open Mobile Alliance
SMB	Standardization Management Board (of the IEC)
VDMA	German Mechanical Engineering Industry Association
W3C	World Wide Web Consortium
WRC	ITU-R World Radiocommunication Conferences
ZVEI	German Electrical and Electronic Manufacturers' Association

Glossary

brownfield approach

business solutions approach to specific problem areas involving the development and deployment of new software systems in the immediate presence of existing (legacy) software applications/systems

Cloud Foundry® approach

an open source cloud computing platform as a service (PaaS)

cyber physical system
CPS

1. hybrid networked cyber and engineered physical elements co-designed to create adaptive and predictive systems for enhanced performance [Source: National Institute of Standards and Technology (NIST)]
2. engineered systems that are built from and depend upon the synergy of computational and physical components [Source: National Science Foundation]

edge

aspect comprising the operational domain of the overall IoT system

NOTE The edge typically consists of sensors, controllers, actuators, tag and tag readers, communication components, gateways and the physical devices themselves.

gateway-mediated edge

device that aggregates data flows and connections from all the endnodes

Hadoop®

open-source software framework for distributed storage and distributed processing of very large data sets on computer clusters built from commodity hardware

Lambda architecture

data-processing architecture designed to handle massive quantities of data by taking advantage of both batch- and stream-processing methods

semantic interoperability

ability of computer systems to exchange data with unambiguous, shared meaning

5G
fifth generation mobile networks

proposed next major phase of mobile telecommunications standards beyond the current 4G/IMT-Advanced standards

Section 1
Introduction

Much has been written about the rapidly emerging, disruptive impact being detected on every aspect of how machines and their operational technology (OT) communicate with one other, with the underlying information technology (IT) platforms that typify today's IT environments, and with the humans (consumers, operators, decisions makers) who in one form or another use, control, or are even controlled by those machines. This disruption, commonly referred to in the context of the Internet of Things (IoT), was first mentioned by Kevin Ashton, co-founder of the Auto-ID Center at MIT, where a global standard system for RFID and other sensors was created [5]. As currently defined by ISO/IEC, the Internet of Things (IoT) is "an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react [6]."

Although referred to as an "Internet of Things", in reality what is emerging is a series of consumer, industrial, public sector and hybrid networks that are collectively using today's Internet backbone to create closed loop networks for connecting the operational technology of cyber physical devices (the things) with sensors, controllers, gateways and services. The created networks can be cloud based as well as traditional on-premise based, and typically use specialized IoT platforms to provide services designed to optimize the performance of the devices using a variety of techniques and approaches. As with most disruptive technologies, these platforms are being developed by a wide range of solution providers drawing on their own experiences and promoting their own existing solutions repackaged to address new requirements.

However, to realize the true potential of this emerging technology, new approaches beyond performance optimization are necessary. This White Paper attempts to address these new approaches and the requirements involved, and to articulate them in a concise and concrete manner. The aim is to assist decision makers, architects, developers and implementers in changing the character of their IoT initiatives from ones based on simple transformation to ones involving dramatic shifts in the way that devices are identified, monitored and controlled. Also addressed is the way the devices and the networks they belong to are secured, and how multiple interdependent systems collaborate with each other.

1.1 Background

In today's IoT, applications mainly concentrate on collecting performance and environmental data from sensors attached to devices, and either performing rudimentary analyses in a proximity network close to the devices or passing the data via some form of network to an on premise enterprise or cloud platform. For many IoT applications with a limited remote device control capability, and which are largely used for data retrieval, archiving or data use limited to static or batch processes, these models often suffice.

However, such a limited approach fails to take any real advantage of this new disruptive technology, provides little return on investment (ROI), and raises doubts in the minds of executives who must make resource allocation decisions. New IoT platforms

are emerging which offer advanced services such as predictive maintenance, visualization, logistic tracking systems, home automation, public surveillance or telematics and remote device configuration and management. These services collectively offer significantly greater value to those faced with investment decisions by providing new insights into every aspect of an enterprise's core operations and by affording opportunities to reduce the company's total cost of operations, furnish new or enhanced industry, consumer and public sector services or open new markets. Nevertheless, these emerging enhancements still raise significant doubt among decision makers as to the potential ROI on IoT transformations.

Additionally, these new approaches raise almost as many issues as they tend to address. Security becomes exponentially more important as devices that heretofore were isolated and thus highly protected, are now potentially exposed to significant risk. Data privacy concerns – especially in the consumer IoT space – are significantly heightened, as more and more personal information is captured and shared by the devices and by the various networks that connect to them. Much equipment in today's industrial and public sector environment – from manufacturing to logistics to healthcare and every other industry vertical – is outdated and may not be digitized or capable of connecting to an IoT network, and thus investment in new equipment is significantly more difficult than in the typical consumer space where devices are changed out every few years.

1.2 Moving forward

Today's solution providers are making significant progress in developing advanced services and platforms designed specifically for IoT. These new platforms and services are naturally expanding the disruptive potential of IoT, however, much more progress is still required.

To realize the full disruptive opportunity that IoT offers, advances in today's IoT platforms and the IoT devices, sensors, actuators and networks they support are essential. More sophisticated data analysis techniques using deep learning and artificial intelligence will require significant enhancements employing new approaches. Autonomous devices such as self-driving cars and fully recombinant plant equipment are creating unparalleled demands for system responsiveness to support real-time behaviour. This in turn requires the ability to sift through massive amounts of data streamed in real time and stored in memory for low or zero latency access. Real-time IoT applications need real-time platform support that allows for sophisticated processing within the proximity networks as well as across the full network range. Cross-industrial application domain usage of data, (e.g. data generated in the smart home industrial application area is used in the automotive domain), can enable the development of new business models. Horizontal industries, such as telecommunication operators, and vertical industries, such as car manufacturers, can pursue partnerships and profit from such new business models.

As IoT networks become ever more mission critical, issues such as resiliency, safety, security, dynamic composition and semi- or even fully-automated recombination and/or reconfiguration of the devices become critical. Not only will responsiveness drive development of novel IoT platform architectures, it will also generate new and unimagined opportunities and requirements.

These requirements and the advanced platforms, devices, networks and architectures that support them will only be possible with corresponding new and enhanced standards for data semantics, contextualization, transformation and transmission, for analytic engine information sharing and for security, connectivity, interoperability and every other aspect of what constitutes the emerging IoT smart ecosystem. The advanced platforms

in this emerging ecosystem, hereafter referred to as smart and secure IoT platforms, require even greater capability to enhance and expand the capabilities of companion smart IoT devices and the smart networks that connect them.

1.3 Scope

This White Paper addresses the following key questions:

- Which key capabilities are offered by existing IoT architectures and which limitations and deficiencies can be identified?
- Are existing capabilities sufficient to make envisioned new applications such as Smart Cities real? If not, which additional or enhanced capabilities are required? How should a smart and secure IoT platform look?
- Are existing technologies sufficient? If not, do we only need appropriate enhancements and adaptations of existing technologies to meet the requirements of tomorrow's applications? Alternatively, do we also need new technologies?
- Which international standards are already established or are currently under investigation? Which, if any, additional standardization efforts are needed to support IoT applications?
- Who should identify the requirements for – and define, publish, and maintain – new standards?
- What should the role of the IEC be?

1.4 Structure

This White Paper is structured as follows:

- Section 2 provides an overview of the current state of IoT and describes the fundamental capabilities of existing IoT platforms to include data correlation and information retrieval, connectivity and communication, integration and interoperation, security, privacy and trust. It further describes most common architecture patterns used to build today's IoT platforms and provides a brief overview of existing reference architectures. This section concludes by providing insights into existing IoT systems, enabling the identification of the main deficiencies and limitations of those systems.
- Section 3 systematically identifies and explains encountered deficiencies related to key topics such as security, integrability and composability as well as advanced analytics and visualization.
- Section 4 highlights future IoT use cases covering three different application domains – industrial, customer, and public sector.
- Section 5 provides an overview of the smart and secure IoT platform and of smart devices and smart networks. It further explains the technical challenges expected to emerge in creating the smart and secure IoT platform.
- Section 6 focuses on several of the key next-generation enabling technologies necessary for realizing smart and secure IoT platforms.
- Section 7 addresses the current standards landscape and identifies standardization requirements for smart and secure IoT platforms.
- Section 8 rounds up this White Paper by identifying specific standards development recommendations for IEC and other standards-related organizations, such as governments.

Section 2

Today's IoT

Many "standard" definitions exist of IoT, IoT platforms, IoT architectures and the IoT "things" themselves. To set the stage properly for a shared vision of IoT in the future and the smart and secure IoT platform, it is necessary to define clearly what IEC sees as the current state of IoT, the various components that comprize IoT systems and the leading IoT architecture definitions.

2.1 IoT components

Although there are many different existing and emerging IoT architecture patterns (see Section 2.3), they all share one set of components in common – the concepts of physical device, edge and platform. The following subsections describe these concepts in detail and set the common terminology used throughout this White Paper.

2.1.1 Physical device

In today's IoT system architectures, the "things" encompassed in the Internet of Things go by many names, including cyber-physical device, device, end-point, entity and human entity. As shown in Figure 2-1, all of these things share a common attribute regardless of the domain in which they reside, namely their individual identity as a physical device. These physical devices may contain some level of computing power, either embedded in the device or directly attached in the form of their actuators or controllers. The physical devices may also be connected directly to other physical devices, edge platforms, gateways and to one or more IoT systems.

2.1.2 Edge

In today's IoT system architectures, the concept of the "edge" refers to the aspect that comprizes the operational domain of the overall IoT system. The edge typically consists of sensors, controllers, actuators, tag and tag readers, communication components, gateways and the physical devices themselves. The edge is where operational components connect, communicate and interact with each other, with the platform and in some cases directly with components in other edges. The edge can be as small as a single physical device with a direct connect to a platform, or as large as a manufacturing plant comprizing all manufacturing equipment with a comprehensive communications functional component and edge computing platform, or anything in between. Within the edge, there may or may not be a platform to support processing. The edge communication component can consist of an independent local area network or networks where the components connect using one or more protocols and zero (direct connect to gateway) or more routers to connect to an edge gateway/hub/bus, which in turn connects to larger networks or cloud-based solutions that include the platform. The local network can use hub and spoke, mesh, WiFi, cellular or other topology for internal connections and connection to the gateway/hub.

Edge processing addresses requirements and/or limitations of the edge components or system functionality. These requirements and limitations include device connectivity as devices, such as those in industrial settings, may only have local connectivity capabilities. Other requirements comprize appropriate handling of devices with

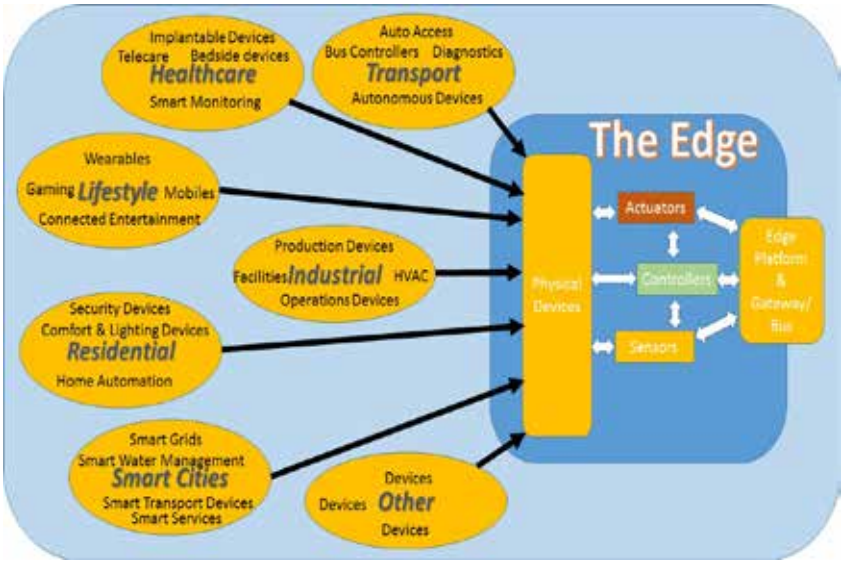


Figure 2-1 | Typical edge environment

offline operation, i.e. since certain devices may not be connected online 24x7, these devices collect data while offline and upload the data when connected. In addition, there may be a need or a desire for edge analytics, edge transaction processing or another edge functionality as an extension of, or independently of, the IoT platform. As not all data should or needs to be transferred to the platform for storage, the edge provides local storage capabilities. To reduce the volumes of data to be transferred to the platform, an edge processing is often required that enables dynamic filtering or sampling or aggregating device data.

2.1.3 Platform

In today's IoT system architectures, the concept of an IoT platform is typically expressed as referring to the central hub of domains that collectively constitute the physical realization of the functional view of an architecture encompassing one or more aggregated edge environments. The IoT platform is an integrated physical/virtual entity system employing various applications and components to provide fully interoperable IoT services and management of those services. This includes, but is not limited to, networks, IoT environments, IoT devices (sensors, controllers, actuators, tags and tag readers, gateways) and the attached physical devices, IoT operations and management, and external connectivity with suppliers, markets and temporary stakeholders of the IoT system [7]. The typical IoT platform either contains, or interacts with the following domains [8]:

- **Control** – Comprises functions executed by the controlling mechanisms to enable the IoT devices to include sensing, actuation, communication, asset management and execution. In an industrial environment, control systems are typically located in proximity to the IoT device connected to the physical device. In a consumer environment, the control systems could be proximity located or remotely located. In a public environment, the control systems will typically include a combination of proximity or remote.

- **Operations** – Typically on the IoT platform and optimizing operations across multiple control domains, it includes prognostics, optimization, monitoring and diagnostics, provisioning and deployment, and management.
- **Information** – Typically on the IoT platform but also emerging as part of the edge, it comprizes core IoT analytics and data and is responsible for gathering, transforming, persisting and modelling the data to support optimized decision making, system-wide operations and improvement of system models.
- **Application** – Typically on the IoT platform but can also contain components that are part of the business domain. Typically consists of the application program interface, user interface and logic and rules and is responsible for implementing logic that realizes functionalities for the IoT system itself.
- **Business domain** – Typically on a platform separate from those of the core IoT functions defined in the operations, information, application and to some extent control domains, it integrates the IoT functionalities with back end applications such as CRM, ERP, billing and payments.

The IoT platform itself can be located in the cloud, located on premise or involve a combination of the two. It can comprize a single server, multiple servers or a combination of physical and virtual servers. Regardless of its physical location or architecture, the domains that comprize the IoT platform – operations, information, application and perhaps even aspects of business and control – contain multiple data and control flows with one another, with the back end applications of the business domain and with the physical systems/control domain that resides in the edge. Additional services of the IoT platform can include resource interchanges to enable access to resources outside of the IoT system, network services, cloud integration services and many other services as defined by the individual platform provider.

2.2 IoT system design

A number of tools exist to assist IoT systems designers in the use of the IoT system components described in Section 2.1. Chief amongst these is the ISO/IEC/IEEE architecture description standard [9]. In addition, a number of IoT architectures/reference architectures from various standards organizations and IoT-focused consortia are available. The following subsections provide an overview of the most prominent approaches available today for better understanding the various options and potential opportunities for the IoT 2020 smart and secure IoT platform.

2.2.1 ISO/IEC 30141, Internet of Things Reference Architecture (IoT RA)

Joint Technical Committee 1 of the International Organisation for Standardisation (ISO) and the IEC (ISO/IEC JTC 1) chartered its Working Group (WG) 10 to examine and provide recommendations and develop International Standards for the Internet of Things. The first major deliverable from this group is a working draft of International Standard ISO/IEC 30141. The working draft provides key insights into the problems faced by IoT implementers and specific aspects of IoT architecture design and implementation that will help align the efforts of future IoT architects in designing seamless interoperability and plug-and-play IoT systems. The draft defines the various components of the IoT universe as well as a conceptual model, a reference model, and a reference architecture consisting of views. WG 10 has established liaison agreements with a number of groups defining the other architectures cited in Section 2.2, and input from those groups can be readily identified in the current working draft.

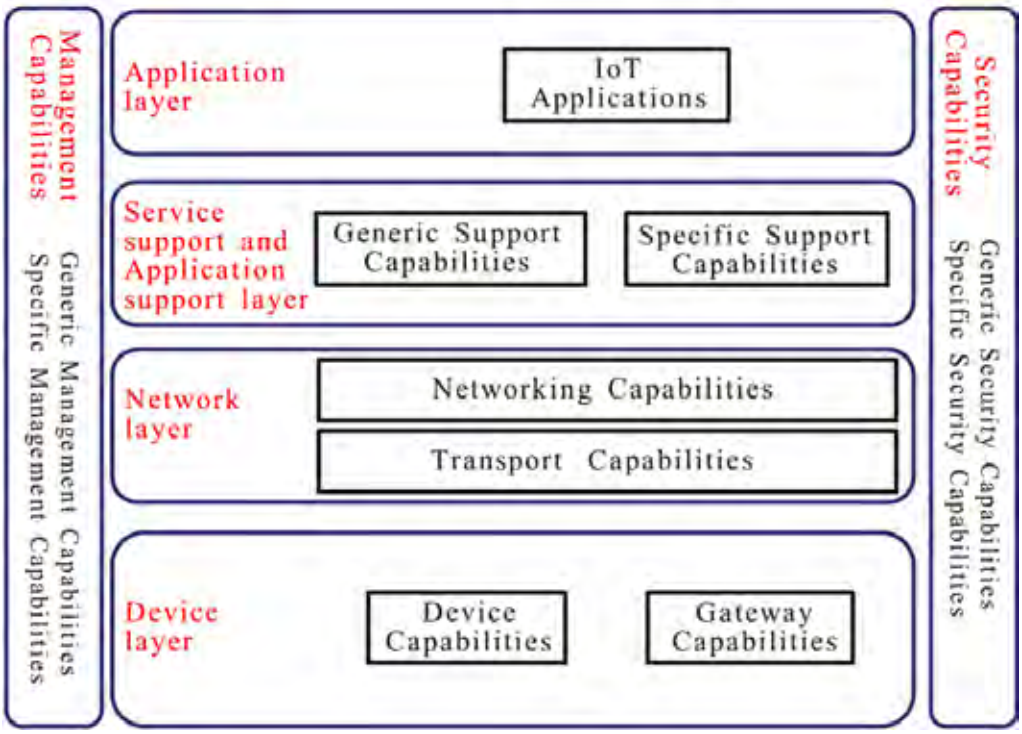


Figure 2-2 | ITU-T Y.2060 overview

2.2.2 ITU-T Y.2060

The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) Study Group 13 has produced ITU-T Y.2060. This standard identifies IoT functional characteristics, high-level requirements and an IoT reference model [10]. The identified functional characteristics include interconnectivity, things-related services, heterogeneity, dynamic changes and enormous scale. High-level requirements listed for the IoT are identification-based connectivity, interoperability, autonomic networking, location-based capabilities, security, privacy protection, high quality and highly-secure human-body-related services, plug and play and manageability.

The model formally defines the key terms "device", "thing" and "Internet of Things" as core concepts (focusing as with many models, on the connectivity of devices as the distinguishing feature for IoT). As shown in Figure 2-2, the model is divided into four layers: application, service support and application support, network, and device. The model addresses required management capabilities and security capabilities for each layer.

Security is divided into generic and specific security capabilities. Specific capabilities are bound to application requirements; generic capabilities are application independent and defined for each layer. Authorization and authentication are defined capabilities at the application, network and device layers. The application layer adds application data confidentiality and integrity protection, privacy protection, security audit and anti-virus capabilities. The network layer adds use data as well as signalling data confidentiality and signalling integrity protection. The device layer adds device integrity validation, access control, data confidentiality and integrity protection capabilities.

2.2.3 IIC IIRA

The Industrial Internet Consortium (IIC) focuses on industrial application of the IoT. The IIC Industrial Internet Reference Architecture (IIRA) defines four viewpoints: business, usage, functional and implementation, as shown in Figure 2-3. The business and usage viewpoints determine the importance placed on business concerns and business cases when implementing industrial systems, and the significance of the domain and context in which a system is used in its design. Particular technical emphasis is placed on the functional and implementation viewpoints. The functional viewpoint divides the architectural view by functional domains – control, operations, information, application and business. The implementation viewpoint focuses on general architecture (structure, component distribution, connection topology), providing a technical description of system components (interfaces, protocols, behaviours, etc.), an implementational mapping of usage viewpoint activities to functional components as well as from functional to implementation components, and an implementation map for key system characteristics. The viewpoints are guides for architects to create their own architecture views.

Security (and related security and safety issues) are both explicitly identified and discussed from the perspective of each viewpoint. This integration of security concerns with the specific viewpoints establishes an understanding that all stakeholders have a view of security-by-design. Key systems concerns – safety, privacy and trust, resilience, integrability, interoperability and composability, connectivity, data management, analytics, intelligent and resilient control, dynamic composability and automatic integration – are individually addressed.

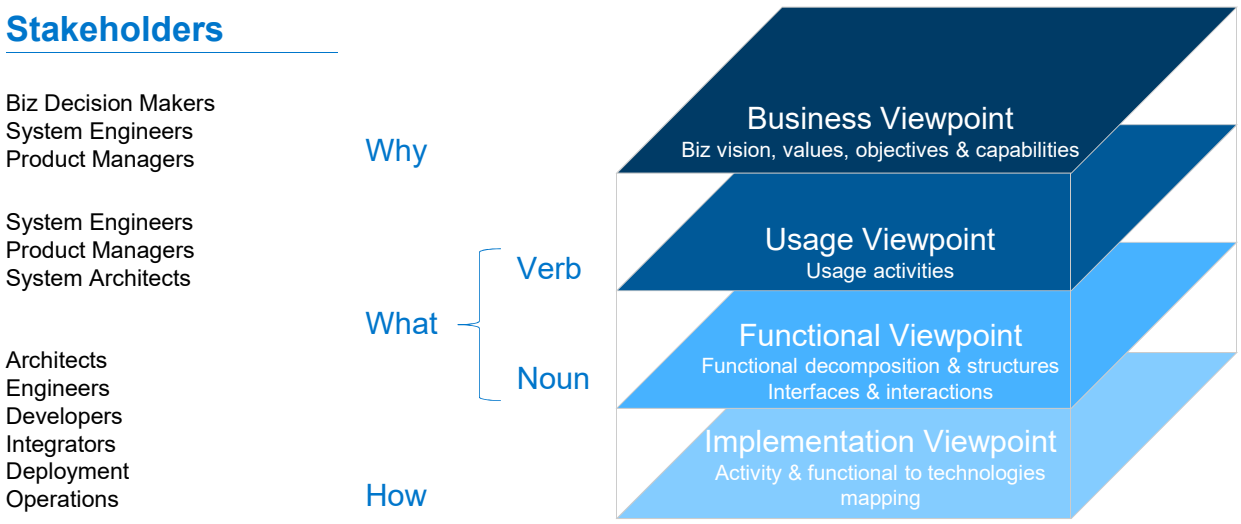


Figure 2-3 | IIC Industrial Internet Reference Architecture

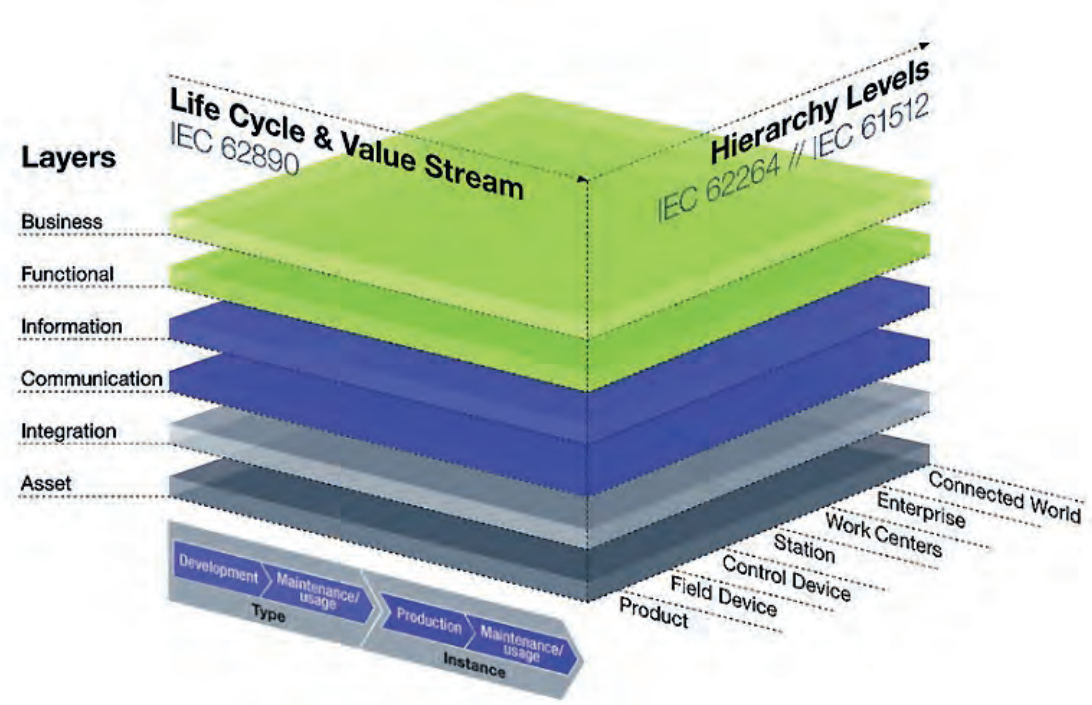


Figure 2-4 | Reference Architectural Model Industrie 4.0

2.2.4 RAMI 4.0

The Reference Architectural Model Industrie 4.0 (RAMI 4.0), currently under active development, represents a joint effort by the BITKOM (German Federal Association for Information Technology), the ZVEI (German Electrical and Electronic Manufacturers' Association) and the VDMA (German Engineering Federation) to build a reference architecture for next-generation industrial manufacturing systems [11].

As seen in Figure 2-4, the core of the RAMI 4.0 is a three-dimensional layered model used to classify Industrie 4.0 technologies. It incorporates parts of International Standards IEC 62264 and IEC 62890 to leverage established models to describe different aspects of next-generation systems.

The model defines "hierarchy levels" according to the IEC 62264 series of Standards for enterprise IT and control systems, representing the various functionalities of a factory or facility, with expansion for the purposes of Industrie 4.0 to include connectivity to the IoT and the Internet of Services (called "Connected World") as well as work-pieces (called "Product"). The model also covers the entire "life cycle and value stream" of a product, including design, production, delivery, usage, maintenance, etc., and is based on IEC 62890 as a representation of product and facility life-cycles, with the addition of the concept of "types" versus "instances" as a means of distinguishing between design and prototype phases versus production. Finally, the "layers" axis is a six-layer division of the space intended to break down machines into their component properties.

The basic RAMI-model is extended by security capabilities, that is, security is built into each layer and each dimension of the model.

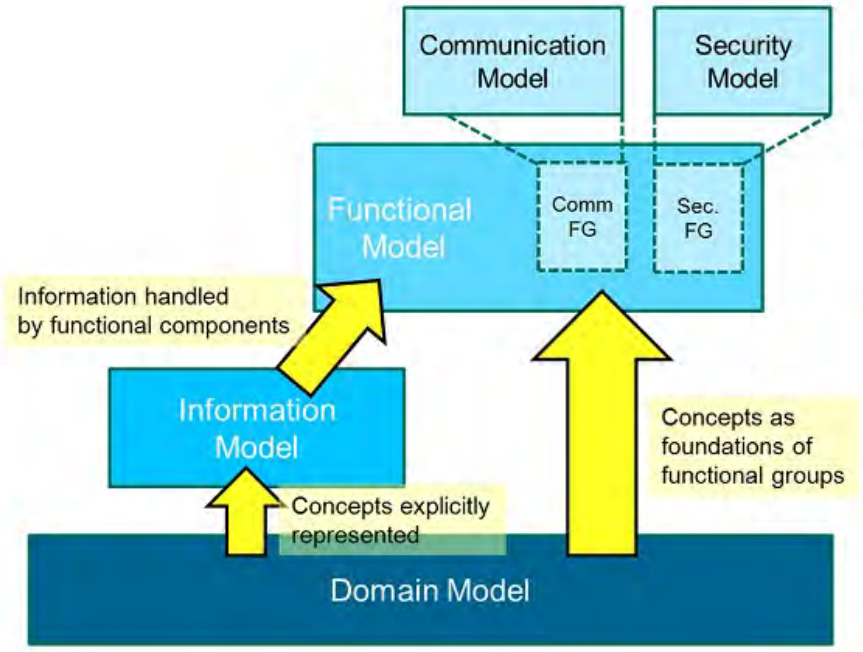


Figure 2-5 | IoT-A ARM

2.2.5 IoT-A ARM

IoT-A, a European Lighthouse Integrated Project of the 7th Framework Programme, has developed the IoT-A architectural reference model (ARM) as a foundational reference architecture document to facilitate the growth and development of IoT technologies. [12] IoT-A ARM consists of three components, with the reference model constituting the most abstract component of the ARM. As shown in Figure 2-5, the reference model consists of domain, information, functional, communication and security models. The domain model is responsible for outlining core concepts in the IoT such as "devices", "IoT services", and "virtual entities" (which model physical entities). The information model defines the generic structural properties of information in an IoT system. The functional model identifies groups of functionalities based on the relations defined in the domain model. The communications model addresses the complexity of communications in IoT environments. The trust, security and privacy (TSP) model is specifically identified by its importance to IoT use-case scenarios and each is addressed separately.

In addition to the IoT reference model, the ARM defines an IoT reference architecture, which is "the reference for building compliant IoT architectures" and includes guidelines intended to guide IoT system architects in creating actual architectures.

2.2.6 AIOTI reference architecture

The Alliance for Internet of Things Innovation (AIOTI) is a European Commission initiative launched in 2015 to develop and support dialogue and interaction amongst European players in the IoT market. AIOTI has developed two IoT models, namely the domain and functional models.

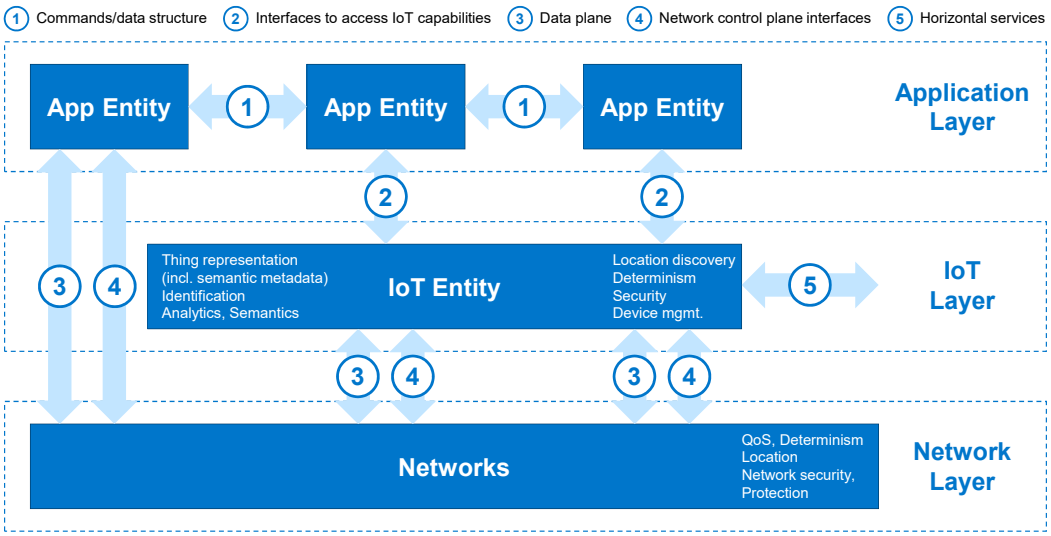


Figure 2-6 | AIOTI reference architecture

The AIOTI domain model, derived from the IoT-A domain model (see Section 2.2.5), captures the main concepts and relationships in the domain at the highest level, provides a common lexicon for the domain and is foundational for all other models and taxonomies. In this model, a user (human or otherwise) interacts with a physical entity. The interaction is mediated by an IoT service associated with a virtual entity – a digital representation of the physical entity. The IoT service then interacts with the thing via an IoT device that exposes the capabilities of the actual physical entity.

The AIOTI functional model describes functions and interfaces (interactions) within the domain, while not excluding interactions outside of the domain. As shown in Figure 2-6, the functional model is composed of three layers – application, IoT, and Network. The functional model describes functions and interfaces between functions of the IoT system. Functions do not mandate any specific implementation or deployment, therefore, it should not be assumed that a function must correspond to a physical entity in an operational deployment. Grouping of multiple functions in a physical equipment remains possible in the instantiations of the functional model.

2.3 Architecture patterns

In leveraging the various reference architectures presented in Section 2.2, a number of architecture patterns have emerged and are gaining widespread acceptance and implementation. The following subsections present the most popular of these patterns to better understand requirements and opportunities for the smart and secure IoT platform.

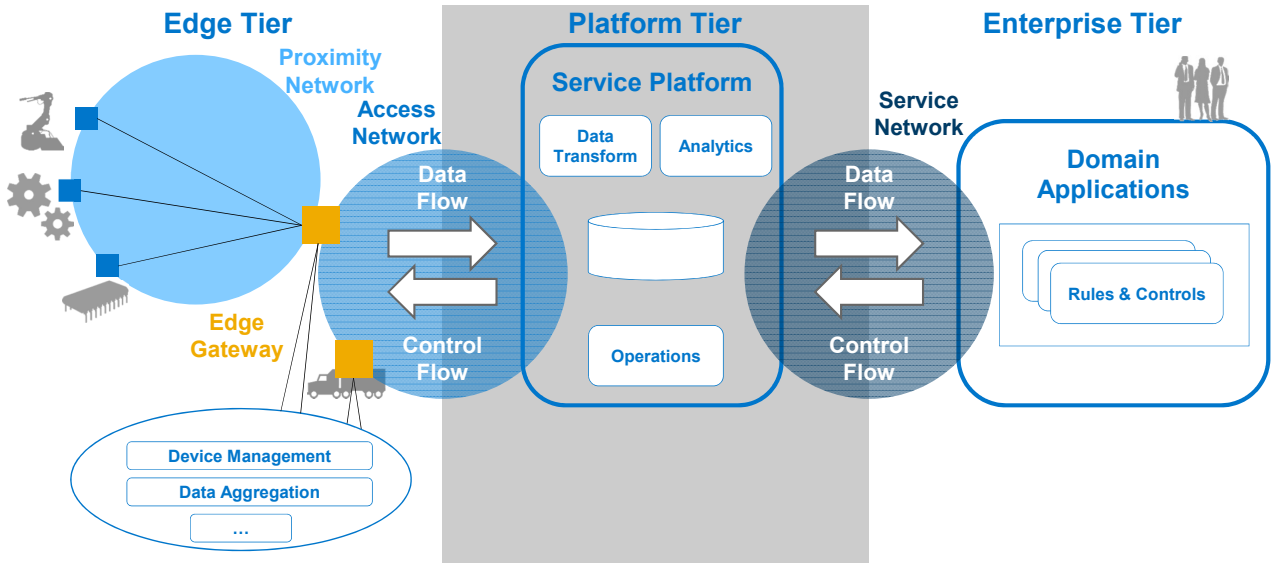


Figure 2-7 | Three-tier architecture pattern

2.3.1 Three-tier architecture

The three-tier architecture consists of edge, platform, and enterprise tiers connected by proximity, access, and service networks. The networks in this as well as in the other architectures that follow all typically use a combination of enabling wireless and/or wired technologies such as RFID, Bluetooth, Cellular, ZigBee, Z-Wave, Thread, and Ethernet. As shown in Figure 2-7, the edge tier uses the proximity network to collect data from edge nodes (at the device or "thing" level). This data is forwarded over the access network to the platform tier, which processes data from the edge tier for forwarding to the enterprise tier, as well as processing and relaying control commands from the enterprise tier back down to the edge tier (again, over the access network). The platform tier uses the service network to communicate with the enterprise tier, which provides end user interfaces, control commands and domain-specific applications [13].

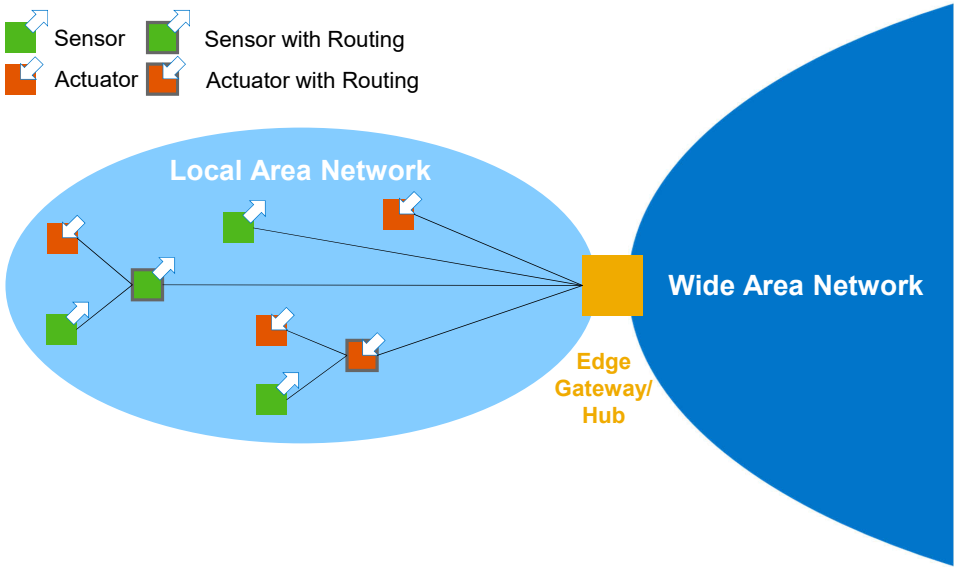


Figure 2-8 | Gateway-mediated edge architecture pattern

2.3.2 Gateway-mediated edge connectivity and management

Gateway-mediated edge connectivity and management is an architecture pattern in which a gateway acts as the mediator between a local area network (LAN) of edge nodes on one side, and a wide area network (WAN) on the other. It serves as an endpoint for the WAN network and (potentially) a management entity for the edge devices on the LAN, isolating the edge devices from the WAN. Sensors and actuators connect either directly to the edge gateway or through one or more routers, see Figure 2-8. The topology of the LAN itself may be either hub-and-spoke, in which all communications within the LAN go through the edge gateway, or mesh (peer-to-peer), in which some edge nodes have routing capability. There may be other paths of connectivity between nodes that do not go through the edge gateway itself.

2.3.3 Edge-to-cloud

The edge-to-cloud architectural pattern varies from the gateway-mediated edge pattern by including direct wide-area connectivity and addressability for devices and assets, rather than all edge assets being isolated behind the edge gateway [13].

2.3.4 Multi-tier data storage

Multi-tier data storage is a data architecture that attempts to separate storage tiers by their functionality and purpose in order to optimize performance and storage constraints. For example, storage tiers can be divided into separate tiers for performance, capacity, and archival purposes.

2.3.5 Distributed analytics

A distributed analytics architecture couples proximity analytics closer to the edge with intensive analytics at more centralized parts of the architecture. This architectural pattern is relevant,

for example, when latency or other network constraints make fully centralized processing a suboptimal solution.

2.3.6 Lambda architecture

The Lambda architecture differs from the other reference architectures presented in this section, in that it was not designed for IoT and does not address any aspect of the implementation view other than data flows for analytics. We include it here due to its widespread use and importance in designing IoT systems capable of handling the tremendous amounts of data generated by the sensors.

The Lambda architecture addresses the need for real-time processing of the massive data flows associated with IoT big data by separating such processing into two views – the batch view and the stream view. The architecture itself is separated into three layers – the batch layer responsible for the master, immutable, append-only data set; the serving layer for indexing the views of data in the batch layer for efficient retrieval; and the speed layer for real-time data to provide low-latency functionality and access to recent data for the stream view. Incoming data is sent to both layers – the batch layer for higher-latency, more complete processing, and the speed layer for immediate processing to quickly provide data or analytics the batch layer has not yet had the opportunity to incorporate in a more correct and complete manner.

This has particular relevance for IoT architectures, in that real-time applications may be faced with data coming in from hundreds or thousands of edge devices and must be able to exercize a preliminary or immediate reaction to some circumstances, in spite of the volume of data involved. Simultaneously, the same applications may need more correct or involved analysis of this data for continuing response, correction of initial results, historical or archival purposes, extended analytics, and so on.

2.4 Characteristic features of IoT

In addition to understanding IoT architecture concepts and patterns, it is also important to fully comprehend the typical characteristic features of today's IoT in order to define properly the 2020 smart and secure IoT platform. The following subsections examine key features of IoT systems that represent important considerations for tomorrow's IoT.

2.4.1 Data correlation and information retrieval

Smart data processing is a key IoT feature. The ability of today's IoT to distribute sensors widely and collect data quickly and effectively facilitates new forms of collaboration. Components of IoT systems produce different characteristic kinds of data, such as stream, batch, and asynchronous data. Data processing such as that involved in small learning tasks can often be pushed out towards the edge, where large-scale processing tends to require centralization. Such data can be processed and used for system feedback, allowing for process improvement, fault detection and incorporation of real-world context into business workflows. Today's IoT also uses semantic modelling of the data it produces to make using the data more practical and intuitive, and to facilitate interoperation. Common world models with semantic support (e.g. for Smart Cities), and virtualized entities with data abstractions that comprize all characteristic information about entities, allow for real-world entity modelling that goes beyond the sensors that provide the data. The right degree of abstraction is helpful in real-time situation handling, as all sources of information are able to agree on the semantics of the information they are providing.

2.4.2 Communication

The communication architecture of today's IoT is variable, depending on which combination of network and edge architecture is useful in a given situation. Currently, communications largely take place over VPNs or using dedicated public networks. Existing applications rely on communication that takes place between the edge and centralized servers, services and aggregation points. Today's IoT communication capabilities already span traditional silos between enterprises. While factory integrated solutions only allow for applications and improvements within a particular manufacturing area, IoT platforms permit the collection of information from multiple heterogeneous entities and support collaborations beyond traditional enterprise silos.

2.4.3 Integration and interoperation

Today's IoT solutions are characterized by varying degrees of integration and interoperation. Integration efforts often involve making systems work together that were not initially designed for interoperation. However, while not yet holistically available, within companies there can be a certain degree of integration and interoperability between products, where upper-level technologies are integrated with the technologies below them.

In many cases, integration is based on the typical hourglass model, with IP in the middle and with HTTP and REST APIs as the common denominator for communications. This is particularly useful, as enablers of IoT services are often provided by different providers, whether on-premises or in the cloud. However, this does not exclude machine-to-machine networks, which are also part of supported solutions. Additionally, there is growing support for open protocols (such as MQTT, OPC and web sockets) and for both developing and leveraging open source components in the smart product/smart services stack (e.g. Cloud Foundry, OpenStack).

Cross-industrial domain semantic interoperability is an emerging IoT characteristic that is receiving increasingly significant attention in many standards developing organizations (SDOs), alliance and open source software (OSS) initiatives. This and other emerging interoperability initiatives will enable the cross-industrial domain usage of data and will provide the means for the development of new business models.

2.4.4 Security, privacy and trust

As mentioned above, IoT consists of a multitude of different devices, sensors and actuators and may even comprize whole cloud infrastructures. Obviously, a one-fits-all solution is not feasible when it comes to security. Today's IoT capabilities with respect to security can roughly be divided into the following areas: sensor security, device security, edge security and cloud infrastructure and network security. To date, sensors with limited resources and capabilities often lack any security mechanism due to the overhead of encryption algorithms and key management needs. Depending on the application area, the same holds true for many devices, for instance industrial devices that are generally legacy devices, or consumer devices used for example in home automation environments. In today's IoT, device security is largely (and sometimes exclusively) tied to network and/or edge security, employing standard security protocols such as TLS or standard filtering techniques such as firewalls, secure gateways or edge nodes to establish encrypted communication channels. Device security is largely implemented on a case-by-case basis in connection with customer demands and capabilities. Pushing security capabilities into the edge and network gateways is the easiest way to protect endpoints and devices behind the gateway in a uniform manner. This can be done without having to change and touch each device to support mechanisms for controlling access, authenticating or detecting intrusions. However, frequently, IoT

devices are physically accessible, i.e. network security to protect them is just a first level of protection. A second level of protection within the devices and sensors themselves, as well as a third level providing security monitoring and threat analytics on the device in combination with edge as well as platform capabilities, are required. There are use cases for which more involved solutions already exist: for example, surveillance and video cameras have implemented integrity protection on the data and device levels, making them viable for use in court. Additionally, it should be noted that what needs to be secured is highly domain-dependent. For some domains, companies define the security of feedback mechanisms and control to products as a much higher security concern than any concerns about the safety of the data being produced, and solutions are geared accordingly. With respect to cloud security, a number of protection mechanisms are already in use, such as identity and access management, isolation and virtualization and intrusion detection.

Privacy considerations in today's IoT are largely managed on a non-technical level by concluding service-level agreements (SLAs) with the customer granting permission to use the data produced. On a technical level, only very simple mechanisms, if any, are employed to preserve privacy. Common capabilities comprize encryption to hide sensitive information and use of pseudonyms instead of personal identification items or aggregation to hide personal data within a crowd. Privacy protection within cloud infrastructures commonly uses well-established measures, such as storing and communicating data in an encrypted manner or employing access control to prevent unauthorized information leakages. With regard to data analytics, privacy-enhancing techniques are often lacking and are substituted by non-technical means such as SLAs and other customer agreements to ensure data processing in compliance with legal regulations. To summarize, in today's IoT privacy capabilities focus on privacy by design or privacy by default approaches protecting data privacy at data sources. To benefit from the huge potential of IoT while preserving privacy protection, more flexible capabilities are required to control data usage and data processing in an application-dependant manner [14].

To establish trust between entities of the IoT, unique device, service, and/or transaction identities and strong authentication are required. Trust establishment in today's IoT is commonly based on identities that are enrolled within certificates for users, servers and network equipment such as gateways. Certificates are generated and controlled using well-known public key infrastructures (PKI). Device identification is often delegated to a gateway that acts as an identity proxy. In some security critical environments, hardware-based trust-anchors such as the trusted platform module (TPM) are used, which provide a hardware-based root of trust and a high level of confidence that the identity attributes delivered belong to the particular device. Some devices and gateways already make use of trusted execution environments to isolate applications or use different implementations of containers, e.g. on Linux systems, to provide isolated execution environments for applications.

As IoT is a dynamic system of systems, measures to attest the trustworthiness of IoT components throughout their lifetime are required. However, this kind of integrity attestation is normally not present in today's IoT.

Section 3

Limitations and deficiencies in today's IoT

Today's IoT platforms are an eclectic mix of patched together components repurposed from existing solutions for use in specifically designed platforms that attempt to address the currently identified issues facing development and deployment of IoT cyber-physical systems encompassing both consumer and industrial end-points. Many of the current IoT solutions require trying to get disparate, stove piped applications and systems to work together. These systems use existing protocols, standards and concepts not designed for IoT. Many are built on the basis of a lack of vision concerning the real potential of IoT. Instead, such systems merely attempt to lash together the OT of the physical devices with existing IT and back end platforms and applications. All of the systems are dealing with issues of device registration, mass device on boarding, and massive amounts of potential data.

An investigation of these multiple and varied approaches to building IoT reveals the emergence of fundamental crosscutting topics in the areas of security, safety, integrability, interoperability, composability, data management, analytics, resiliency, composability, virtualization, and regulation. All of these topics drive up costs, which is as much an impediment to the functioning of today's IoT as the state of the underlying technology.

The following subsections address the more prominent issues that current IoT initiatives face with regard to each of these topics.

3.1 Security, trust, privacy and identity management

Security properties of systems are usually described by security models. These models typically describe the entities governed by a specific security policy and the rules that constitute the policy. Creating and maintaining a holistic security model able to cope with the dynamic changes of IoT systems is becoming increasingly difficult. The continual adding of devices involving different OEMs, different sensors, and different physical facility security approaches is increasing security complexity exponentially. Solutions related to issues such as customer/partner/system provider responsibilities have yet to gain consensus in the security community. Today no overall flexible, dynamic IoT security model exists capable of supporting mission-critical systems while simultaneously enabling the expected rapid advances and disruptors for tomorrow's IoT.

Today's IoT systems have usually been built in a brownfield approach connecting existing sensors, devices and infrastructure components, as well as services. The IoT is introducing new levels of exposure for each of these elements. Current IoT platforms contain technology solutions from a wide variety of vendors, each of whom focuses on providing heterogeneous components with individual levels of security. Security measures, if any, within the IoT components have not been designed to take into account the dependencies arising from the IoT's connectivity capabilities or its data correlation and information retrieval capability.

For example, industrial devices often lack proper authentication mechanisms, as they have been designed to be used in physically protected and isolated environments. As part of today's IoT they are interconnected with many other devices, especially back-end systems suffering from all the well-known security flaws inherent in today's business IT. Attackers gaining access to business IT platforms, for instance by exploiting browser vulnerabilities, will likely also gain access to weakly protected IoT industrial devices This can result in severe damages, including safety incidents. Hence, the introduction of a massive number of end-points from the consumer or industrial environment creates fertile ground for exploitation of weak links. Hardening these end-points, securing device-to-device communications and ensuring device and information credibility from what heretofore has constituted a set of completely closed homogeneous systems is presenting new challenges. Comprehensive risk and threat analysis methods as well as management tools for IoT platforms are required.

3.1.1 Trust

Security measures in today's IoT focus on network and edge security. Appropriate security concepts to provide in-depth protection are lacking, such as hardware-based trust-anchors or monitoring and threat analytics services that are properly integrated into IoT devices operated behind the edge. Proper identification and authentication capabilities and their orchestration within a complex IoT environment are also missing. This prevents establishment of trust relationships between IoT components, which is a prerequisite for security critical IoT applications or future applications requiring ad-hoc connectivity between IoT components, such as Smart City scenarios. Data validity is another issue. Trust management for IoT is needed to ensure that data analytics engines are fed with valid data.

3.1.2 Privacy

Preserving privacy in today's IoT is still an open challenge. There are thought leaders (e.g. Gartner) who see an acute need to develop and maintain digital ethics, especially when considering scandals in the press and in public discourse [15]. Facing the huge potential for data analytics in IoT, privacy-preserving technologies beyond the inflexible privacy by design principle are required. For example, usage control, homomorphic encryption or searchable encryption are potential candidates for overcoming the existing deficiencies. Besides these technological challenges, regulatory requirements are challenging as well. Vendors have to face significant regional differences in privacy regulations.

3.1.3 Identity management

Current enterprise identity and access management (IAM) solutions focus on enforcing least access policies when granting users access to applications, resources and data. However, with regard to IoT, current IAM systems are limited in their ability to adjust to storing identities and entities on a large scale. This limitation has resulted in a lack of application integration layers for IoT based applications. At this stage, there exists no overall framework for how to discover and manage IoT entities and their identities across different solutions. Current IAM systems will need to evolve in order to start covering enhanced and broader entity relationships. The enhanced IAM role will change what authentication (and authorization) means and how access is granted. The trend is on providing limited access based on expected role as opposed to least privileged access. As such, authentication from the same device may result in different access capabilities based on how the user has authenticated to the device. In addition, IoT will require traditional IAM systems to include machine-to-machine (M2M) entities. This task will be complicated, since some

of these communications will be based on short-lived entities such as virtual cloud entities. Some of these entities will use proprietary communication and identification schemes. In general, IAM platforms will need to be modified in order to cover identity in IoT-based systems.

3.2 Safety

System safety and reliability is the highest priority of many OT platforms. This means preventing the system and its components from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes. As most OT systems in the past were not networked, security and privacy was not a concern. IoT is fundamentally altering this perspective. Today's IoT lacks the sort of holistic risk and threat analysis that takes into account the dependencies arising from faults raised by intended attacks. With the current connection of OT and IT under IoT, remote attackers will be able to exploit weaknesses in industrial, consumer and public sector IoT systems in order to break into the OT system and drive it into an unsafe or unreliable state.

In addition, the employment of remote management to include reconfiguration and updating of devices as well as monitoring and operational reprogramming on the fly is creating serious next-generation security and safety concerns. The introduction of IoT systems with open ports and the potential interjection of malicious code – especially on safety critical devices and systems such as transport, city public safety and water – is creating new requirements for security and safety not currently or appropriately addressed.

3.3 Integrability, interoperability and composability

Today's IoT systems deal with how to integrate the various components into a collective whole. This integrability comprizes the capability for each system component to communicate with every other system component based on a compatible means of signalling and protocols. As shown in Figure 3-1, integrability constitutes the lowest level of the integration stack. Interoperability builds on integrability and is the capability of components to exchange information with each other based on common conceptual models and interpretation of information in context. The highest level involves composability, which is the capability of a component to interact with any other component in a recombinant fashion to satisfy requirements based on the expectation of the behaviours of the interacting parties.

3.3.1 Integrability

Integrability capabilities are enablers of IoT systems. The complexities of IoT are generating new and more complex connectivity issues that require new solutions. IoT systems are adding ever-increasing numbers of end-points, geographically dispersed information sources and new system-to-system requirements, with corresponding new demands on capability and performance. IoT systems are struggling with connectivity issues around maintaining sessions and not losing connections. Network load increases are occurring at the same time that network speed requirements – especially for safety critical components requiring virtually instantaneous event response time – are becoming more demanding. Data acquisition through multiple network resources and pushing logic back toward the edge, for example through heavily firewalled internal networks, is creating significant problems. Rules federation from the backend to the edge requires new and improved protocols.

Figure 3-1 | Integration stack

3.3.2 Interoperability

IoT systems rely on four components – syntactic transformation, domain transformation, semantic transformation and contextualization – to achieve true interoperability between and among components [13].

The connectivity framework layer (layers 5 through 7 of the ISO/IEC 7498 OSI Model) provides a syntactic interoperability mechanism using knowledge about the structure of the data and transformation rules among the various components between and among systems. IoT systems that employ presence discovery partially address this requirement. IoT systems also use domain transformation to convert one data domain to another, such as information from OT systems to IT systems. IoT system semantic transformation entails the semantic understanding between the sending and receiving components and systems. As of today, no viable contextualization mechanism exists. Although some progress has been made with data transformation at the syntactic and domain transformation levels, today's IoT systems continue to struggle with all four interoperability components. Significant effort will be necessary to ensure development of requisite standards to address these issues.

Additionally, IoT systems must deal with a lack of API dependency management. Changing one API can disrupt the entire system. Microservices and service orchestration remain difficult. Interoperability with back-end processes, i.e. end-to-end process integration is still an open issue, as different IoT silos use different non-interoperable cloud back-end or on-premise solutions.

3.3.2.1 Semantic interoperability

Today's ever more complex heterogeneous IoT systems contain a large number of different models, including real-world entity abstraction, time-series-based and location-based. Business users, data modellers, systems designers and others have built these data models over time through a variety of techniques, from simple spreadsheet analysis to more complicated UML

design. However, today's IoT systems struggle to exchange data with unambiguous shared meaning. There still remains little semantic interoperability without time-consuming manual mapping of the data models that creates brittle implementations not suitable for tomorrow's IoT. Machine computable logic, inferencing, knowledge discovery and data federation all require a sophisticated level of semantic interoperability. Ontologies are generally limited to single systems or use cases and do not have consistent naming and definition rules. International Standards such as ISO/IEC 11179 and ISO 15000-5 offer the promise of consistently named, defined, and semantically understood metadata, but this would require additional effort in order to adapt such data to be scalable and usable on the broad scale of IoT.

3.3.2.2 Context

Contextualization is the understanding of the totality of the environment at the instant of capture – to include end-point, sensor, human and environmental – and recording that information in the form of fully understandable metadata. Today's IoT systems are hampered by a lack of robust contextualization of information, especially that from the edge. Contextualization of this IoT information represents the next step in achieving true interoperability and is critical to ensuring sound analytics and safe and secure operation. There currently exists no agreed-upon standard or methodology for unambiguously identifying and sharing contextual information. In addition, context information may contain confidential data. Edge computing is useful for keeping context information isolated in the edge. However, it is necessary to protect edge computing from threats.

3.3.3 Composability

Composability is the capability of a component to interact with any other component in a recombinant fashion to satisfy requirements based on the expectation of the behaviours of the interacting parties [16]. In IoT, this translates into the ability of the IoT system to be able to be self-organized and able to adapt and reconfigure according to changes in its environment. IoT systems are currently dealing with issues of responsiveness in dynamic environments. They are transitioning beyond traditional point-to-point client-server models to meshed many-to-many models that require new approaches to handling various levels of autonomy with simultaneous responses and addressing the need for flexible compositions. Increasingly autonomous systems are struggling to deal with dynamic conditions and ensure safety and resiliency. Today's IoT systems lack mechanisms for resolving possible incompatible assumptions about their context by including such concerns as operating environment, interacting entities, user mental states and unforeseen issues. IoT systems lack the ability to support dynamic relationships in which self-forming composition handles on-the-fly activity and state changes.

3.4 Resiliency

Today's IoT systems face daunting challenges regarding their ability to deal with system or component failures and still maintain functionality. Designers of military and civilian critical systems such as military combat aircraft and civilian transport, combat operational support and emergency responses requiring the ability to deal with system or component failure and still maintain functionality, fully understand and plan for such occurrences. The purpose of this planning is to provide for system resiliency. Resiliency is "the condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties" [13]. These safety critical components and systems make resiliency a must-have capability. However, resiliency is not limited to

these use cases, but rather constitutes an equally necessary capability for many, if not all, other IoT applications as well. IoT systems and their complex relationships involve a network of subsystems that must address how to create interoperability and composability without developing a static solution and suffering its impact on resiliency. Smart platforms must develop more advanced approaches to managing the resiliency of the components their systems support.

3.5 Data collection, management and ownership

Today's IoT is dealing with unparalleled amounts, types, locations and sensitivities of data. IoT systems and the platforms that serve them are experiencing explosive growth in the numbers of end-points and the sensors that connect them in edge environments. Multiple architecture patterns further exacerbate the process of where, when, why and how the data is provided and analysed. Device- and entity-oriented data are requiring higher abstraction layers. IoT system asset heterogeneity is causing problems in gaining data access to multiple sources.

With these massive amounts of data generation, significant issues have arisen regarding data collection, storage, retrieval and query. IoT systems are struggling with how much and exactly what data to collect and store. Some systems are attempting storage at the edge for much of the raw data that is not being used by today's platform applications. Customers are demanding more and more data capture – essentially all data from all sources all the time – and yet they appear reluctant to aggregate data at the edge. As a result, some IoT systems attempt to flood the connection pipes with all data.

Much has been written regarding the general topic of data ownership and more specifically IoT data ownership. The question of who owns which data and who controls where data goes creates major issues from regulatory, ethical, and financial standpoints. Customers believe they own all the data. The original equipment manufacturers (OEMs) believe they own, or at least have access rights to, the data dealing with their endpoint. The platforms as service providers in many cases believe they own the data, as do the application providers. Issues of data ownership are increasingly compounded as more heterogeneous IoT systems with more players from divergent organizations are deployed. Further complicating the issue are the IoT system providers who outright violate, or at least circumvent, end-use license agreements by feeding both personal and operational data-to-data collectors and analytic services. Corporate entities have a significant interest in protecting proprietary business data and trade secrets, as well as limiting liability, e.g. from privacy breaches of third-party input data they may store, process, or consume. End users in particular want control over their individual data, especially privacy-related data, even when consenting to allow a system to use their data for a particular purpose. Today's IoT platforms lack robust data rights management systems to enable all parties to exercise an acceptable level of control over their data and over questions about where, how, by whom and for what it is used.

3.6 Advanced analytics and advanced data processing

The sensors and systems in today's IoT produce extremely large amounts of data. Normal processing techniques are insufficient. IoT data processing and analytics are dealing with transforming and descriptively, predictively and prescriptively analyzing this voluminous system and sensor data. Transmitting this data requires tremendous bandwidth and much of the raw data is unnecessary or unusable. As a result, we see more interest in analytics at the edge and even on the physical devices themselves – especially for safety-related systems – but this generates additional complexity

in areas such as data management, advanced analytics, and operational control. One significant issue with analytics on the physical device or at the edge is that many insights that are only revealed when the data is crowdsourced across multiple edges and/or systems would be lost. Today's environment lacks technology which coordinates edge analytics and cloud analytics. Such coordination is essential to create tomorrow's smart and secure IoT platforms.

An additional issue is the lack of time synchronization between sensors. Systems are experiencing unordered delivery of messages and are in need of universally applied time synchronization techniques. Available data for advanced analytics systems is often not useful – e.g. missed data, corrupted data, wrong data – because it has not been designed for the new approaches to predictive analytics and other forms of analytics already being deployed in today's IoT. IoT systems are dealing with significant challenges for receiving and processing clean data. Inadvertent human intervention such as end-point shutdown reduces the totality of the data and affects the data's context. Although machine generated data is generally of high quality, within today's IoT, data generated by edge computing lacks appropriate quality, as edge data continues to suffer corruption and incorrect semantic and contextual understanding. In addition, IoT systems are attempting to use data not originally designed for the purpose for which they are using it. This causes both syntactic and semantic difficulties, which results in very small intersection of useful data between and among IoT systems. IoT analytics systems are also just beginning to deal with next-generation concepts such as using social and crowdsourcing data.

3.7 Virtualization

Today's IoT platforms largely rely on legacy devices and legacy IT systems lacking virtualization capabilities. The devices are typically already equipped with most of their "smartness". Final instructions are only given through software downloads. Today's IoT devices lack embedded virtualization capabilities which allow an additional level of abstraction providing the device with a generic management layer and virtual machines that can be dynamically filled with functionality.

3.8 Scalability

The distributed nature of IoT drives creation and processing of data outside data centres as well as building massive post-process analytics systems at core data centres or in the cloud. Most current data centres rely on traditional architectures that are not suitable for these emerging requirements. Hence through 2020, 80% of all IoT projects will fail at the implementation stage due to improper methods of data collection [4]. In order to meet those requirements as well as keep pace with the expected massive growth connected with IoT (e.g. Gartner estimates that data-intensive industries will see an ~500% increase in storage by 2020), web-scale IT is required, given its ability to effectively support IoT requirements. Gartner defines web-scale IT as a system-oriented architectural pattern that enables the rapid and scalable development and delivery of web-based IT services leveraging agile, lean and continuous principles. Today's IoT lacks web-scale IT capabilities.

3.9 Regulation

The IoT can help make society more effective, safer and greener, hence government bodies strive for regulations that provide a proper balance between supporting helpful innovation and protecting consumers. Although the goal is the same, the approach between different geopolitical entities varies greatly. This is causing significant confusion in the marketplace and adding to the complexities of designing, building, deploying and operating both homo- and heterogeneous systems within and across geopolitical boundaries.

Section 4

Use cases for next-generation smart and secure IoT platforms

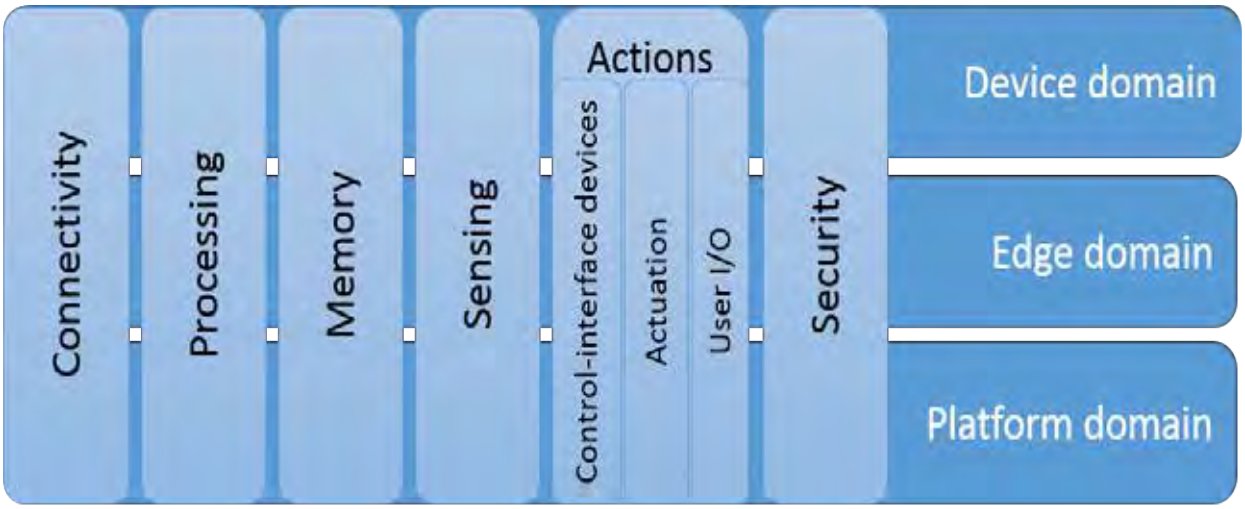


Figure 4-1 | Smart and secure IoT platform key capabilities

It is clear from the material in Sections 2 and 3 that the current IoT state of the art is both limited in capabilities and plagued by deficiencies. These combine to restrict available IoT solutions and prevent development of smart and secure IoT platforms. Furthermore, overcoming these deficiencies is in and of itself insufficient to take advantage of the full potential of IoT. Rather, a fresh look at forward thinking use cases is also required to better define the necessary capabilities. This section provides an overview of three such use cases from the industry, public sector, and customer perspectives and derives selected key capabilities, as shown in Figure 4-1, that future IoT systems and the smart and secure IoT platform must have. Smart and secure IoT platforms will certainly have additional capabilities and requirements, however we limit the remainder of this White Paper to those identified here. Greater detail regarding these three use cases, as well as the seven other forward thinking use cases listed in Table 4-1, are available in the Annexes.

Table 4-1 | Forward thinking use cases

Use case domain	Name of use case	Descriptor
Industrial	Business continuity management	BCM
	Anomaly detection system for advanced maintenance services	Anom Detect
	Collaborative supply chain management (SCM)	CSCM
	Predictive maintenance and service	Pred Maint
Public	A Smart City with a smart and secure IoT platform	Smrt Cty
	Social sensors	Soc Sens
Customer	Improvement of journey experience in public transport for passengers including those with special needs	Journ Exp
	Connected cars	Conn Car
	WISE Skiing	Ski
	Home device smart factory	Smrt Fact

4.1 Industrial domain: business continuity management for production lines

Business continuity management (BCM) ensures continuation of an organization's business processes by utilizing data collected from the organization's IT and OT systems. The objective of BCM is to provide an advanced risk assessment processed from collected IT and OT data and to implement necessary measures to mitigate the impact to the organization's business processes, see Figure 4-2.

The BCM IoT platform will gather incident information from various security systems (i.e. IT systems) as well as planned and actual production data from production control systems (i.e. OT systems) utilizing sensor fusion technology. The BCM IoT platform will import threat intelligence information from other organizations to acquire insights into the situations of other interdependent systems and cohesive knowledge of the current and future attacks. The platform will analyze the incident information and perform risk analysis of the incident. It will also create security measures such as risk mitigation plans that will minimize the effect to the production activities. The BCM IoT platform will implement security measures such as isolation of the affected subsystems or interruption of production lines. The IoT platform will analyze the production data to create an optimal production plan in response to affected capabilities of each production site.

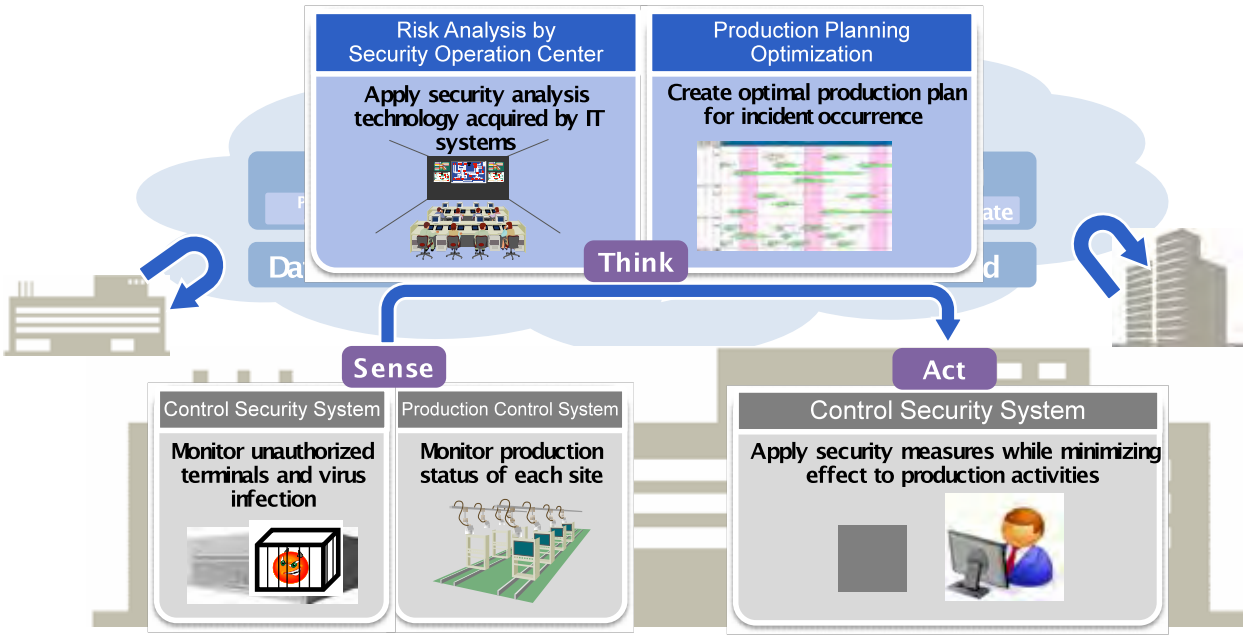


Figure 4-2 | Industrial domain use case

Existing technologies are insufficient to realize this use case and require enhancement as follows:

Connectivity	▪ Deficiencies – Network latency issues, multi-platform access and authentication. ▪ Needed enhancements – Robust networking supporting required latency and required protocols to enable multi-platform access and authentication.
Processing	*Data collection and management* ▪ Deficiency – Insufficient capacity to support the anticipated explosive growth in the number of devices and sensors and the data flows therefrom. Lack of contextualized state information. Sensor data cleansing. ▪ Needed enhancements – Advanced data storage techniques, advanced data science capabilities, in-memory databases, metadata contextualization standard for normalized state information. *Analytics* ▪ Deficiencies – Insufficient capacity in terms of memory and algorithms to support industrial level analysis. Immature distributed analytics routines. ▪ Needed enhancements – In-memory databases, enhanced algorithms with self-learning and self-optimization, artificial intelligence, semantic interoperability, data contextualization, distributed platform solutions.
Memory	–

Sensing	▪ Deficiencies – Sensor growth capacity, mediation solutions for data exchange, sensor authentication, proof of integrity. IT/OT collaboration, actuation, sensor interface, sensor recombinant capability. ▪ Needed enhancements – Advanced sensor capabilities to support distributed platforms and needed data consistent with security and related requirements. Advanced sensing capabilities with enhanced sensor reconfiguration capabilities, military grade resiliency, and dynamic composability.
Actions	*Control interface devices* ▪ Deficiency – Limited protocols for IT/OT integration. ▪ Needed enhancements – Advances in standards that fully take advantage of IoT concepts and opportunities. *Actuation* ▪ Deficiencies – Evaluation ability for scope and condition. Prioritization routines for multi-platform connectivity. ▪ Needed enhancements – Advanced actuator devices with on-board processing capabilities to support decomposition, evaluation, condition actuation.
Security	*Security models* ▪ Deficiency – Security models for creating and maintaining holistic security operations capable of coping with dynamic changes in IoT systems and the expected rapid advances in the level of system attacks. ▪ Needed enhancements – Advanced security capabilities optimized for interdependent IoT systems for implementing protection measures against system threats in interdependent systems, to include optimization of current capabilities and collaborative security across systems to realize a holistic situation view. These capabilities include optimization of existing security capabilities such as plan-do-check-act (PDCA) and observe-orient-decide-act (OODA) to match the requirements of both the IT and the OT systems, as well as new security capabilities such as collaborative security between interdependent systems to acquire a holistic view of the situation. *Secure identity and IM* ▪ Deficiency – Overall framework for discovering and managing IoT entities and their identities across different systems essential for IoT systems that consist of diverse types of devices and interdependent systems. ▪ Needed enhancements – Advanced actuation capabilities for the security enforcement functions.

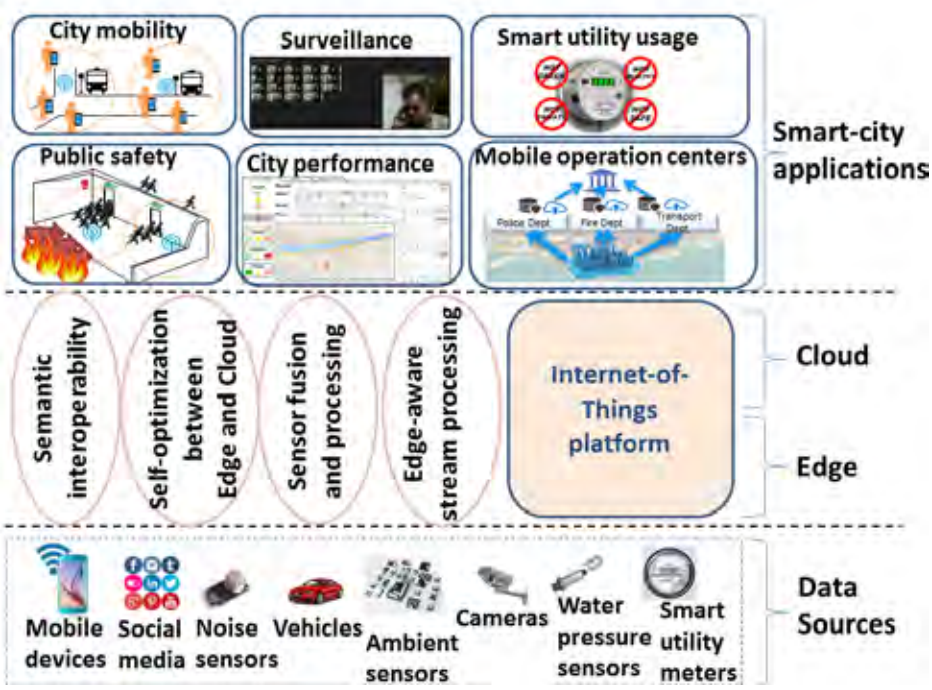


Figure 4-3 | Smart City optimization

4.2 Public domain: Smart Cities

Smart City solutions bring together a number of heterogeneous IoT platforms that collectively contain a wide variety of sensors and data sources. These include temperature, humidity, noise, gas, and motion sensors, cameras, mobile devices, network sniffers, smart meters, water meters and a plethora of others devices that collectively monitor the dynamics of a city and optimize city operations while also enhancing citizen services. The Smart City IoT platform will transform the multi-modal sensing information from these various IoT platforms into cross-domain and real-time information mash-ups, using semantic interoperability. Advanced data mining and machine learning techniques will easily access a variety of different platforms and their operating environments to provide applications for residents and multiple agencies and enable intelligent actions. The Smart City platform of platforms will include real-time applications to enhance public safety, improve city mobility, optimize utility usage and enhance the plethora of citizen services that involve physical objects. Smart City platforms and the platform of platforms will rely heavily on smart and secure sensing to optimize services. They will use a combination of data from the public, private and personal sectors (anonymized as necessary) to seamlessly gain a more holistic view of the Smart City environment. They will use cross-domain communication techniques to bring together the disparate IoT systems deployed by individual agencies in a geopolitical entity and enable cross-domain cooperation and optimization, see Figure 4-3.

The Smart City platforms and platform of platforms will rely heavily on semantic disambiguation and contextualization of information to support advanced data processing and next-generation analytics that are developed for, and focused exclusively on, optimization of citizen services. These platforms will leverage advanced connectivity

such as 5G and in-memory databases to move and process the vast amounts of data generated by the plethora of devices within their geopolitical boundary. The platforms will support edge-aware stream processing to handle processing topologies on parallel-networked systems. The Smart City platform of platforms and individual platforms will use next-generation technology to create smarter and more secure citizen quality of life environments.

Existing technologies are insufficient to realize this use case and require enhancement as follows:

Connectivity	▪ Deficiency – Adequate network bandwidth, network sessions, support for intermittent connectivity. ▪ Needed enhancements – Next-generation communications architectures and protocols such as 5G.
Processing	*Data collection and management* ▪ Deficiencies – Rigid, inflexible interoperable information structures and vocabularies. Environmental metadata mechanisms. Devices oriented with unidirectional flows from device to platform. Lack of clarity and uniformity for data ownership, data protection, and data contribution. Inability to interpret unstructured, noisy and intermittent data from diverse data sources into meaningful contextualized information-supporting real-time systems. ▪ Needed enhancements – Semantic interoperability standards for information clarity within and across domains and an overarching IoT ontology regardless of originating format. Context metadata standard for environmental context information. Support for on-demand, contextualized, multi-directional data flows between devices, sensors, actuators and platform(s). *Analytics* ▪ Deficiencies – Analytics too rigid to meet quality-of-service (QoS) requirements (e.g. emergency response) and system reconfiguration. Limited ability to address changing conditions such as weather, social preferences, and emerging conditions. ▪ Needed enhancements – Distributed analytics with algorithms and tools capable of dynamically splitting tasks between device, edge and platform for both planned and unique QoS requirements. Dynamic reconfiguration capability in support of changing system landscape for both planned changes and system resiliency. Edge-aware stream processing to handle processing topologies on parallel networked systems to facilitate and manage application execution. *System interoperability* ▪ Deficiencies – Rigid architectures devoid of support for dynamic task allocation and service migration. Operational coordination and collaboration not sufficiently mature. Inconsistent standards for ensuring interoperability in a heterogeneous platform environment. ▪ Needed enhancements – Heterogeneous entity solution (devices, sub-systems, networks, and services) for coordination and collaboration between disparate systems. Dynamic onboarding and system reconfiguration capability.
Memory	–
Sensing	–

Actions	*Control interface devices* ▪ Deficiency – Secure and safe data dissemination, remote management, actuation permission and cross-domain control. *Actuation* ▪ Deficiency – Rigid programming devoid of flexibility. ▪ Needed enhancements – Flexible routines capable of adjustment based on real-time context of the device, edge, platform and system environment.
Security	▪ Deficiency – Operation technology security and safety management. Robust lifecycle management of prevention-detection-mitigation threats to assure continuity of safe operations. ▪ Needed enhancements – Actuation permission control, authentication of data exchanges between entities, automated protection, anomaly mitigation strategies.

4.3 Customer domain: improved journey experience in public transport for passengers with special needs

This journey experience IoT system helps passengers, including those with special needs, optimize their route to destination based on personal needs and preferences. The underlying platform will monitor passenger movement, identify deviations, provide dynamic alternatives and oversee passenger safety and security. At the outset, a passenger will input travel information to the system, which in turn will find a route based on the information provided by the passenger and the passenger's needs and preferences. The journey experience IoT system will select optimized checkpoints to monitor passenger travel. The IoT system will dynamically determine expected travel time by crowdsourcing and analyzing actual user data and stakeholder related transportation services data, such as bus and railway operators, police or city agencies. The smart and secure IoT platform will support all requisite data privacy, data ownership and data use regulatory restrictions and guidelines.

The smart and secure IoT platform for journey experience IoT systems will interface with the platform for Smart City IoT systems and with solutions to adjust public transport operations such as bus and train, to better serve the special needs of individual passengers while minimizing disruption to all other passengers. For example, the bus IoT system would cooperate with the journey experience system to ensure that a bus on a given route at a given time is fully equipped to handle wheel chairs or other special needs requirements.

The journey experience IoT system will use self-learning techniques based on its operational experiences as well as those shared from other systems. It will employ situational knowledge acquisition and analysis to dynamically reconfigure both itself as well as other engaged systems, and will use advanced information sharing across disparate systems as a private system feed into a Smart City system. Adaptive selection approaches will manage the uncertainty and volatility introduced due to real-world dynamics. Management decisions and runtime adaptability will be based on security, trust, administrative, location, relationships, information, and contextual properties of things comprizing the underlying IoT system.

Existing technologies are inadequate to support this use case and require enhancements as follows:

Connectivity	▪ Deficiency – Standardization of connectivity protocols. ▪ Needed enhancements – 5G standard adoption to support needed improvements in connectivity reliability and speed.
Processing	*Data contextualization and data management* ▪ Deficiency – Robust data contextualization. ▪ Needed enhancements – Standardized contextualization mechanism for user, system, interfaced systems and anyone/anything else connected. *Analytics* ▪ Deficiencies – Focused analytics algorithms on individual use cases. Distributed analytics to support intermittent platform connectivity. Application tailored context capability. ▪ Needed enhancements – Distributed analytics to support distributed platforms. Standardized contextualization mechanism supporting dynamic contextualization of the data to enable value-added analytics. *Dynamic composition* ▪ Deficiency – System adaptability to support continuous improvement. ▪ Needed enhancements – Machine learning algorithms to support continuous dynamic composition and service improvement.
Memory	–
Sensing	–
Actions	–
Security	▪ Deficiencies – Physical sensor protection. Information manipulation. Privacy data trust. Data anonymization. Individual tracking and location. ▪ Needed enhancements – Data trustworthiness mechanisms that overcome information source risk exposure and manipulation. Secure device identification and integrity solutions that are applicable across disparate, interconnected IoT systems and platforms.

Section 5

Capabilities and requirements for smart and secure IoT platforms

5.1 General qualities of future IoT systems

Future IoT systems and their support by smart and secure IoT platforms will generate a wealth of new technical requirements for devices, the edge and platforms to enable them to realize new capabilities and deal with the effects of those capabilities. New intelligence and security functionality, for example, will require additional features in edge computing and on sensors. New APIs to manage the interaction of sensor groups and IoT gateways will need both device and platform support to encapsulate various architectural patterns and operating environments (e.g. cloud) and provide uniform views to upper layers (e.g. IoT applications, service interfaces, configuration controls, etc.).

The traditional concept of a single platform residing in the middle of an IoT architecture pattern will be replaced. The smart and secure IoT platform will realize “symbiotic ecosystems” where multiple interdependent systems collaborate with each other in a mutually reciprocal relationship to break free from traditional silos and enable value added services and business process optimizations across different IT and OT systems [17]. The integration of information and the implementation of security measures across different interdependent systems will be two of the most important challenges addressed by the smart and secure IoT platforms. Such platforms will enable both autonomous deployment of devices in the edge as well as their dynamic recomposition to support system integrability and resiliency requirements.

Smart and secure IoT platforms will use new operating systems, for example, open source-based systems that follow the Cloud Foundry® approach for development, deployment, maintenance and enhancements. The platforms will use in-memory database technology enhancing Hadoop®, Lambda architecture and emerging approaches to maximize computing power and support enhanced data science techniques.

The smart and secure IoT platform will

- support expanded sensing capabilities, sensor fusion across multiple interwoven IoT systems and tomorrow’s analytics, which will significantly enhance and expand algorithms created to support existing and new concepts for IoT productivity.
- leverage new data context mechanisms and data semantics based on new standards to provide for enhanced understanding of the information and enable fundamentally enhanced analytics.
- offer enhanced security that addresses complex issues such as maximized protection of the device and data privacy requirements from a variety of geopolitical entities.
- support the key security capabilities and policies for IT and OT systems, such as plan-do-check-act (PDCA), observe-orient-decide-act (OODA) and cooperative security

operations between interdependent systems, to cope with diverse and ever changing types of cyber and physical threats.

The smart and secure IoT platform will allow omnidirectional data flow to/from devices, products and the edge through the network, allowing the collection, storage and analysis of "thing"-related information and the integration of enterprise and IoT-specific applications. This platform will provide the means for processing and lifecycle management of the mass of endpoint data in an integrated way – across different data types and processing technologies. It will enable development of new/innovative applications by combining key platform services/capabilities, and will allow the remote management of smart and secure products and services (configuration changes, software updates, remote control) and connections. Moreover, as an important advancement in the way IoT systems work, the smart and secure IoT platform will support decentralized data (pre-)processing at the gateway, product or device (edge and fog computing).

Future IoT systems will incorporate characteristic "smartness" features that derive from IoT capabilities. Smart and secure IoT platforms, and the products and services they encompass, will be commonplace. Such features will include enhanced connectivity (to the Internet, cloud, and to one another), varying levels of autonomy, ability to collect and process data for the optimization of processes spanning several IoT entities and systems, and context awareness and self-optimized behaviour. These features will better facilitate predictive maintenance and prescriptive services, allowing owners, manufacturers and service providers to better monitor and control systems and components. They will support a maximal level of automation for standard tasks (e.g. device-onboarding), and will facilitate collaboration between entities (swarm intelligence). Discovery functionality (e.g. localization information for entities) can provide context for a system component or subsystem and describe the entities, attributes and metadata necessary for understanding generated data, as the entity moves, changes state or changes context.

At a low level, these "smartness features" will provide a "memory" that stores information about design, manufacturing, usage, or maintenance of system components. At a higher level, such features will provide the ability to ask the system specific questions (e.g. the current weather status, relevant details about crowds, etc.). In the development process, integrability and interoperability features will enable the integration of products from multiple vendors when developing complex IoT systems.

Future IoT systems will provide "holistic security capabilities" spanning the whole lifecycle of an IoT system and its components, covering design, development, operation and maintenance. These new capabilities will take into account interdependencies, for instance between business IT and OT. Thus, smart and secure IoT platforms will provide new threat analytics and risk management as well as self-healing capabilities to detect and defeat potential attacks. To improve system resilience, trustworthy security collaboration management systems will be established spanning devices, platforms and different enterprises. These security collaboration systems may run new kinds of threat intelligence mechanisms to exchange security-related information in a trustworthy manner between organizations. In addition, the envisioned smartness features of smart and secure IoT platforms require more advanced capabilities to identify the "things" involved, such as sensors, devices and services, and to ensure data integrity, data ownership and data privacy. A new federated identity and access management is required for collecting, integrating and processing heterogeneous data from different sensors, devices and systems. New capabilities to ensure controllable data ownership across enterprise boundaries must be provided by future IoT

systems, to support the envisioned future IoT use cases. To benefit from the massive volume of data while preserving the privacy of customers and/or enterprises, new data analytics algorithms and new cryptographic methods, such as searchable or homomorphic encryption are required.

Standards compliance is already a complex issue, and more dynamic, configurable and complex IoT systems will create the need to build in features for compliance with regulations in different geographical regions and regulation domains. A smart and secure IoT platform will have built-in features to help IoT systems navigate and conform to this complex regulatory landscape.

5.2 Core capabilities and requirements

The following subsections outline core capabilities of future smart and secure IoT platforms, while each capability is linked to the identified future IoT use cases (see Annexes). In addition, an outlook is provided on further requirements with regard to technology, infrastructure, organization and processes.

5.2.1 Connectivity

One of the main connectivity-based capabilities to be provided at the edge and platform levels is real-time situation handling and sense-making. For this, the ability to maintain real-time connectivity with data sources and the receiving parts of the system is crucial, while real-time processing for situation handling and sense-making at the edge level will be necessary in some cases due to lower latency of communication with the device/product, ease of access to local context information and reduction in the amount of data to be transmitted to a centralized server.

Remote access capabilities as well as secure connectivity need to be implemented end-to-end, with particular implications at the device and edge levels. Hence, reliable, secure and trustworthy connectivity is integral from device to platform, as are authentication and access control. Not only must the secure remote access functionality of devices be maintained by the platform, but secure remote access to the IoT systems themselves must be supported by the platform. The same applies to the edge level, where authentication and access control capabilities are a must, as well as the ability to ensure data integrity and reliability of data both at the device level and over the connection.

On the product level, the connectivity capabilities and demands of future IoT devices are likely to differ from current IoT entities in a number of ways. Devices and products will need the capability to connect not just to one system within a silo, but potentially to several different systems, and their functionality may not be solely contained within the device or product, but may also reside somewhere outside of the product. Adaptation to different bandwidths and protocols (since different resources may be available at different points in time), especially considering the mobility of devices, is also a necessary future capability, prompting shifts from hardware-based to software-defined networking solutions. Similarly, the ability to use software to upgrade device connectivity functionality to new and emerging standards will be an important factor in maintaining flexible and highly configurable IoT systems in the future.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Real-time situation handling	•	•	•	•	•		•	•	•	•
Multi-system connectivity	•	•	•	•	•	•		•	•	•
Remote functionality	•	•	•	•	•			•	•	•
Adaptability to any bandwidth/protocol				•	•			•	•	•
Upgradability to new connectivity standards	•			•				•	•	•
Legal intercept capabilities					•					
Remote access	•	•	•	•	•	•	•	•	•	•
Authentication and access control	•	•	•	•	•	•	•	•	•	•
Reliability and integrity	•	•	•	•	•	•	•	•	•	•

5.2.1.1 Connectivity – additional requirements

The novel connectivity capabilities described above will create a number of different technical requirements for realization, one of the most important of which will be to significantly decrease latency across the entire system. Having low latencies at both the network and device levels will be required in particular for real-time systems and for those whose configurations are expected to change dynamically, with significant churn in the member-entity sets. At the same time, existing protocols may not be sufficient for dealing with systems in which high latency is inherent, in spite of latency-reducing measures. For example, TCP has particular issues with the high latency of satellite connections, as it is not designed for high signal transmission times. Thus the new connectivity capabilities supported by the future IoT platforms will likely also require new network protocols extending beyond TCP/IP.

Latency reduction and tolerance, however, are not the only connectivity-related requirements. New communication interfaces are also needed in order to facilitate the exchange of data between multiple autonomous systems.

5.2.2 Processing

The volume and variety of data collected on the devices require extended processing capabilities at all levels of the IoT system to handle both increasingly complex and dynamic applications as well as greater device and edge processing capabilities. While enhanced pre-processing on the device and edge levels allows short reaction times and reduction of data to be transmitted to a central server, the onboard analytics capabilities also will become increasingly more powerful. In addition, machine learning will become an integral part of device, edge and platforms.

To allow advanced data processing, future IoT systems need to provide contextualized information based on the data provided by devices/products under their control and by external systems. This also affects the processing

of virtual sensor data, where multiple sensors are dynamically composed to a virtual device. Hence, dynamic composition and self-configuration of devices on the edge is seen as a characteristic feature. This also makes processing functionality for self-healing and resilience a particularly useful capability.

In order to be able to handle data ownership issues in the heterogeneous, dynamically-changing environment of future IoT systems, new capabilities for tracking data ownership and enforcing data access rules will be an integral part of future platform capabilities. At the same time, more data anonymization capabilities will exist at the edge. Low-level anonymization may not be an option for every IoT system, and different anonymization algorithms work on data at different levels. Thus, while we can expect that there may be some privacy protections added at data collection time, there is often a trade-off between information retention and anonymity, and for many applications, information may need to be retained for the purposes of data processing until it is processed at a higher, more centralized level.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Onboard analytics	•	•	•	•	•	•	•	•	•	•
Offboard analytics	•	•	•	•	•	•	•	•	•	•
Machine learning	•	•	•	•	•	•	•		•	
Contextualization	•	•	•	•	•	•	•	•	•	•
Anonymization					•	•	•	•	•	•
Information mash-up	•	•	•	•	•	•	•	•	•	•
Semantic interoperability	•	•	•	•	•	•	•	•	•	•
Dynamic composition of devices	•	•	•	•	•			•	•	•
Dynamic configurability					•			•	•	•
Tracking data ownership		•	•	•	•	•	•	•	•	•
(Swarm) awareness		•	•		•					

5.2.2.1 Processing – additional requirements

5.2.2.1.1 Scalability and operations

Given the additional requirements imposed by new capabilities at the platform and, increasingly, at the device levels, new system architectures comprizing novel operating systems functionalities will be necessary to support future IoT platforms and to deal with the complexity of future IoT data processing. As already mentioned in Section 3.8, enhanced cloud architectures and adapted high-level processes are required to adopt web-scale IT for future IoT platforms. That is, enterprise IT departments have to become more like public cloud providers, offering cloud-based technologies that are designed for economies of scale, speed and ease of management, as well as for the automation of infrastructure, facilities and processes. As IoT initiatives are “fail-fast” in nature and require rapid as well as continuous delivery,

possibly serving multiple stakeholders at the same time, the development and operations (DevOps) model of service delivery should be implemented.

5.2.2.1.2 Pricing

Additionally, the current price of computing performance for complex data processing may well be prohibitively high for many IoT system applications and implementations. Lower-cost computing performance technologies at the platform level, for instance, are required to enable new business and use cases for IoT systems. At the edge, technologies to speed up computing power and encryption capabilities are needed. To facilitate next-generation IoT systems, a better balance between price and performance has to be realized.

5.2.2.1.3 Processing data in untrusted domains

Performance requirements of future IoT systems will result in scenarios in which computations on data collected from devices will have to be executed as close as possible to devices. Often, those domains may not meet the security requirements of the data owner, i.e. the data should not be disclosed to the component of the IoT system which processes it. Thus mechanisms are required which will make it possible to protect the confidentiality and integrity of data, while still allowing execution of computations and production of meaningful results for the data owner.

5.2.2.1.4 Data science

Data scientists will be able to create models for solving specific business questions. These models will be consumed by a small group of people. If such models are not part of an IoT platform and are not consumed by applications on top of the platform for supporting business processes, the Cross Industry Standard Process for Data Mining (CRISP-DM) will not scale. IoT platforms play a major role in the model creation process and execution of actionable insights.

In the CRISP-DM process the definition of the business question is performed by the business experts. An IoT platform enables the process of data understanding, data preparation, modelling, evaluation and deployment with platform tools. Special tools are designed and available for addressing each step in the CRISP-DM process.

Data science algorithms and humans are needed to extract valuable insights and take actions. The actionable insights extracted by the data science models cannot be used by humans directly; this function has to be embedded into the IoT platform, so that the applications running on top of the platform and other connected platforms can consume the data for supporting domain experts in optimizing their business.

The future of data science is more evident now than in the past. With the rapid growth of IoT, it is expected that by 2018 the data created by IoT devices will reach 403 trillion gigabytes a year [18]. Growth is also expected in “none data” mining areas such as data mining on text, image and video. This will bring greatly increased development in the area of data science technologies. Automation of data science tasks in process areas such as data understanding, data preparation, feature selection and evaluation will become much more common.

Data science predictions will be more pervasive and will happen with zero footprint (applications which do not require end users to install any software). This will reduce the huge budget that companies need to spend on data science infrastructure. Moreover, it is expected that many open source solutions will be introduced to the market.

The success of a data science project relies on expectation management, business benefit, quality of data, team work and finally bringing the analysis into action.

5.2.2.1.5 Interoperability

A high degree of interoperability among heterogeneous types of sensors, devices and platforms will ensure that components can communicate with each other and that information can be shared in a seamless fashion. Interaction between various parts at different levels of the IoT pyramid facilitates collaboration among various partners, e.g. in a manufacturing line or a supply chain network that has a multitude of stakeholders. Hence, one particularly important characteristic capability that the platform will need is significant support for semantic interoperability. This implies that different parts of the system either share the same standards for communication (lingua franca approach) or that the IoT platform can integrate multiple standards and translate between the various languages (integrative approach).

Interoperability requirements also affect integration at the platform level. In order to utilize IoT for various aspects of society, including business, safety and welfare, it is necessary to consider not only a single platform but also a platform of platforms, that is, a system of platforms in which the platforms collaborate with each other. In general, a platform consists of various layers, each of which contains several different IT systems. IT systems based on different rules (silo systems) cannot have mutual or dense communication with each other. This leads to the need for specific mechanisms to handle and manage communication between different and separate IT systems as well as platforms.

One potential solution for construction of such mechanisms is to provide each IT system and platform with a doorway through which it can exchange data and information. Such a doorway is called a “profile”. The profile is an index of contents containing information and the properties that each IT system or platform needs or provides. It exercizes functions of access control and data provision in response to requests from other IT systems and platforms. It is classified into dual conversion and cooperation profiles: the former handles data exchange in an individual platform, while the latter manages cooperation between different platforms.

5.2.3 Memory

The availability of digital product memory (DPM) capabilities at the edge, providing information about product lifecycles, performance data, origin, and other real-world-elements will require support at the platform level as well for integration into analysis and application components. DPM will be realizable by the integration of miniaturized embedded systems in everyday objects and products [19].

Increased memories and smaller, more integrated embedded systems will also allow for much more advanced storage of performance data and for advanced pattern recognition capabilities. These can be used for machine learning and analytics both at the edge and at more abstract levels, depending upon where resources are located and the application involved.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Digital product memory		•	•	•					•	
Pattern recognition	•	•	•	•	•				•	•
Performance data	•	•	•	•	•			•	•	•

5.2.3.1 Memory – additional requirements

Developing future IoT technologies on smart and secure IoT platforms will require that the platform itself provides support for non-relational database storage technologies (e.g. Hadoop®, Spark, etc.). New data storage and processing technologies – based, for instance, on in-memory technologies – are required to support big data analytics for future IoT systems. Technologies to support cloud-at-the edge storage and processing have to be developed as well.

5.2.4 Sensing

Next-generation IoT systems will require both advanced sensing capabilities and protection of sensed data. Devices, in particular, will have increasingly complex sensing capabilities and capacities to process and exchange sensor data both with other devices at the edge as well as to other parts of the IoT systems they are included. Just as devices will be able to collect more information, the IoT system will need capabilities to cope with, communicate, and process this increasingly complex and copious sensor data and the new sensing capabilities of devices. Not only may data be exchanged directly amongst devices, but also the need arises for platform-mediated sensing data exchange capabilities. The platform, as well as the edge functions, will also need to provide support for cleansing of raw sensor data, both for accuracy, trustworthiness and for privacy purposes. The platform, but also the edge and device, will need capabilities to evaluate the trustworthiness of sensor data acquired from devices as well as ensuring the trustworthiness of data it communicates with various entities within the IoT system. Integral to ensuring trustworthiness of data is the capacity to evaluate and ensure the integrity and privacy of data used by and transmitted by platform components. While current-generation sensors largely do not require or support authentication, many next-generation sensors and devices will require authentication capabilities due to their complexity (and advanced processing capabilities), their interactions with other IoT system components belonging to diverse (and possibly dynamically-changing) entities (as opposed to within the traditional manufacturer's silo), their configurability, and the new kinds of applications that may be using them due to their increased capabilities.

Sensors will also benefit from advances in location-sensing technology, allowing ultra-precise location-based capabilities at the sensor level and providing a new dimension to the kind of data associated with the sensor. At the same time, processing of higher precision data, especially that provided by ultra-precise location capabilities, will need support from the platform, particularly for ensuring source privacy and assisting application and analysis by the IoT system. Devices at the edge which are able to collect very detailed sensor data may need filtering and generalization capabilities as well as encrypted storage and communications capabilities in order to ensure that sensitive data disclosure is kept to a minimum.

At the edge level, next-generation IoT systems can provide the capability to compose a virtual sensor by integrating information of multiple sensors under its control and information of external systems with sensor fusion technology. The capability to reconfigure sensors as both part of their functionality and, because of their complexity, is a capability that will increasingly spread to sensing devices that do not currently have such capacity.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Cope with growing number of devices with sensing capabilities	•	•	•	•	•	•	•	•	•	•
Mediated exchange of sensing data	•	•	•	•	•	•	•	•	•	•
Trustworthiness of data	•	•	•	•	•	•	•	•	•	•
Cleansing of raw data	•	•	•	•	•	•	•	•	•	•
Ultra-precise location-based capabilities		•	•		•		•	•	•	•
Privacy					•	•	•		•	
Integrity of data	•	•	•	•	•	•	•	•	•	•
Complex sensors that require authentication	•	•	•		•			•	•	•
Ability to reconfigure sensors				•	•			•	•	•

5.2.4.1 Sensing – additional requirements

One requirement for provision of characteristic sensing capabilities is the development of ultra-precise location technology. This may be facilitated through beacons, ultra-wideband (UWB), vision-based positioning, etc. Furthermore, the requirement affects both the device level and the platform itself.

5.2.5 Actions

5.2.5.1 Control-interface devices

Smart and secure IoT platforms and edge functions provide capabilities for calibrating and controlling a group of devices, comprizing both runtime and configuration. Further, the platform's capabilities support dynamic composition of devices and the management of such groups of devices and products, including the dynamic onboarding of devices.

The platform can have capabilities to help adapt the ways a device is controlled according to environment and context. A platform's capabilities extend to ensure safety requirements, e.g. in the case of predictive maintenance, in addition to supporting authentication, access control, and authorization. Moreover, future smart and secure IoT platforms will possess capabilities to enable floor control and support management of a self-controlled swarm of IoT devices, addressing both hierarchical as well as collaborative control strategies. Lastly, the capabilities of platforms can also extend to swarm control of security as well as context-aware control.

Beyond that, control operations are used to control the (technical) operation of the IoT devices itself. Actuation operations control the (cyber-) physical system to which the IoT devices are attached. Future IoT systems capabilities will go beyond micro-management of the attached

devices, leaving some degree of freedom to the operation of the devices and only controlling the general operational policies the devices have to follow. An example of such capabilities: control policies for managing a self-controlled swarm of IoT devices (hierarchical vs. collaborative control strategies), or context-aware control of devices and adaptation of their behaviour according to environment/context.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Calibration		•	•	•	•	•	•		•	
Control of group of devices		•	•	•	•			•	•	•
Dynamic composition of devices		•	•	•	•	•	•	•	•	•
Adapt the way the device is controlled according to context		•	•	•	•		•	•	•	•
Safety requirements	•			•	•		•		•	
Authentication and access control and authorization	•	•	•	•	•	•	•	•	•	•
Floor control	•	•	•		•	•			•	
Swarm/self-optimization control intelligence		•	•		•				•	
Swarm control of security		•	•		•					
Context-aware control		•	•		•		•		•	

5.2.5.2 Actuation

Actuation capabilities are operations provided by future IoT systems to manipulate the real world including the cyber-physical systems to which the IoT devices are attached. A range of different actuation tasks exists that varies in terms of abstraction and complexity. Direct actuation tasks directly manipulate the operation of a device, e.g. a simple on/off switch for a power socket or a light bulb, whereas scoped actuation tasks manipulate all devices in a given scope, e.g. a geographic range, devices with specific characteristics, or devices in a given operation condition. Scoped actuation might be transferred by an edge or platform component to a direct actuation of a device or might be forwarded to the device, which then checks the scope for itself. Conditional actuation tasks are triggered when certain conditions are met.

Actuation on the platform has to deal with a large volume of requests from many different applications that are requesting actuation tasks from the IoT system. This requires coordination, conflict resolution and a recovery procedure. For non-functional requirements, there is a need to be able to ensure secure and safe operation, to scale with the amount of applications and devices, to deal with conflicting requests and to provide error handling and diagnosis mechanisms.

Edge devices, on the other hand, need capabilities for receiving and sending actuation tasks, for controlling the progress of actuation tasks (including the quality of actuation), for announcing their own status and context to the IoT systems and for reliably executing the given actuation means. They need to deal with communication disruption to the devices as well as towards the platform.

Today, edge devices only connect to one platform. In the future, we can consider edge devices that connect to multiple platforms or applications (multi-tenant edge). In this case, we need capabilities for synchronization, floor control, conflict resolution and error recovery.

A special aspect of actuation is to influence systems which are not directly connected, but which are indirectly influenced, e.g. through optical, acoustic, wireless or other physical signals. An example of this are devices that are only allowed to operate when in the range of a wireless beacon. Keyless car systems are an example for this. All kind of systems that influence human behaviour directly (e.g. through text on displays) or indirectly (e.g. by manipulating light conditions) are included.

5.2.5.3 User I/O

Advanced user I/O capabilities are a natural part of the evolution of future IoT, and will need support at all levels of the systems. Tactile interfaces, augmented reality tools (e.g. glasses) and multi-device user interfaces will all be a part of the enhanced usability and user experience in next-generation IoT systems.

These advanced user I/O capabilities will be supported by advanced processing and analytics, virtual modelling and simulation capabilities (e.g. shop-floor layouts) on the platform, extending the actions and understanding of the user well beyond his or her immediate surroundings. However modelling and simulation of the whole IoT system in detail by platform alone can sometimes be infeasible due to the amount of data to be collected. In such a case, modelling and simulation might be moved to the edge while the platform takes over the functions to integrate and orchestrate underlying components.

Control through tactile interfaces sometimes necessitates a response to an event in a short period of time. When controlling through tactile interface from a remote location, communication latency imposed by physical distance can be a problem. In such a case, it can be effective for an edge function to have the capability to act as a proxy for a remote user to respond to an event rapidly.

Accessibility is likewise a next-generation IoT capability, supporting simpler, better user interfaces for all, as well as accommodating those with special needs (for example with advanced prostheses which respond more naturally to signals from the wearer).

	Industrial				**Public**		**Customer**			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Tactile interfaces		•	•					•	•	•
Multi-device user interfaces		•	•	•	•		•	•	•	•
Virtual modelling		•	•	•	•				•	
Simulation	•	•	•	•	•		•		•	
Accessibility		•	•		•		•			
Augmented reality				•	•				•	
Usability and user experience	•	•	•	•	•				•	

5.2.5.4 Actions – additional requirements

Future IoT platforms require system mechanisms to describe and execute the different categories of actuation tasks (direct, scoped, conditional, composed) and to support long-lasting actuation tasks (e.g. control loops). In addition, mechanisms are needed to monitor the progress and status of actuation tasks. Technologies are required for automatic and context-aware distribution of actuation tasks between devices, edge, and cloud. Technologies are required to support secure execution of actuation including proper authentication and authorization. Reliable and trustworthy actuation requires new technologies and extended system architectures to ensure reliable execution of tasks and to be able to recover from system failures, e.g. from the network or from devices. Other requirements concerning execution comprize technologies and protocols to support low-latency execution, as well as services to offer disruption-tolerant executions.

5.2.6 Security

The introduction of a platform of platforms concept for future IoT systems provides the opportunity to develop end-to-end security policy and risk management capabilities, which integrate all of the component entity and subsystem policies in an IoT system. The platform should also provide capabilities to manage and delegate the resources of edge devices in non-managed areas in order to manage security issues and events that may be facilitated by devices at the edge with similar capabilities. In principle, the platform should provide an optimized framework with respect to available physical resources and security robustness, corresponding to plan-do-check-act (PDCA) in ISO 27001.

The platform will also provide capabilities for the monitoring of devices in the IoT system and for anomaly detection. Important to these capabilities are additional capabilities for the coordination and analysis of data to determine events. This is half of the observe-orient-decide-act (OODA) cycle for detection and response to system threats. Capabilities supporting resilience and fault-tolerance (including cyber-physical attacks) are the other half of this cycle.

In addition to managing policy for the IoT system, the platform should also provide management capabilities for ID correlation between systems, federated ID management, securing the ID of devices, and authenticity management – specifically, accountability and non-repudiation of data.

Adaptive, responsive and cooperative security are additional important capabilities that should be supported at the platform level (and may have necessary functionality which needs to be supported by devices and at the edge). In short, however, systems need to be able adaptively to incorporate and learn from new threat information, plan for additional threats, and enact these plans. They also need to be able to quickly and appropriately respond to threats and attacks, mitigating as much damage as possible. Finally, they need to be able to cooperatively diagnose problems and implement mitigation and pre-emptive security plans between different subsystems in the system, which may be owned by different entities. These capabilities will distinguish future IoT systems from today's IoT [20].

At the edge level, future IoT systems need to provide the capability to authenticate and authorize devices/products and determine their identity, as well as the capability to control access to/from the devices/products based on their identity.

As edge devices are able to take greater responsibilities within IoT systems, their resources and functionality can be used both to fulfil dynamic needs within the security platform defined by the platform as well as to manage security issues and events in non-managed areas. Devices need to be able to adapt to the optimized security framework deployed by the platform with respect to physical

resources and security robustness, but will also provide detection and response capabilities for system threats.

Overall security policy management is an issue at the platform level, but more capable devices will need policy management capabilities of their own, both to deal with local policies which may be needed *in situ* as well as those that need to be managed by the platform as part of more comprehensive security policy strategies. Moreover, devices will need increased identity management capabilities to facilitate federated ID management, ID correlation between systems, etc., and devices must be designed with the capability to protect their identity. If devices themselves cannot provide these functionalities, edge functions need to act as proxy to connect them to an IoT system. This results in the edge requirement to provide proper device and product identification, the capability to confirm the trustworthiness of data obtained from them and the capabilities for managing ID correlations between systems and federated ID management.

Devices will need to have increased resilience and fault tolerance capabilities. While devices in the current IoT may provide data that is used by upper-level services and applications to perform anomaly detection, in the future IoT devices should have the capability to additionally facilitate and perform anomaly detection at the edge, possibly mitigating attacks and detecting faults where and when they occur rather than solely contributing to aggregate information which is processed remotely for this purpose.

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
End-to-end policy management	•	•	•	•	•	•	•	•	•	•
Optimized framework wrt available physical resources and security	•	•	•	•	•			•	•	
Resilience	•	•	•	•	•			•	•	•
Fault tolerance	•	•	•	•	•		•	•	•	•
Detection and response to system threats	•	•	•	•	•	•	•		•	
Monitoring of devices	•	•	•	•	•	•	•	•	•	•
Coordination and analysis of threats	•	•	•	•	•		•	•	•	•
Identity management	•	•	•	•	•	•	•	•	•	•
Securing ID of devices	•			•	•	•	•	•	•	•
Authenticity management	•	•	•	•	•	•	•	•	•	•
Anomaly detection	•	•	•	•	•				•	

5.2.6.1 Security – additional requirements

5.2.6.1.1 Secure identities and identity management

Future IoT systems will consist of numberless actors and components, embedded in heterogeneous system landscapes which have to trust each other on different levels. These things will be subjects to novel attacks including cloning devices. Correct, complete and timely data are the heart of every IoT system. Technologies are required to ensure data integrity and data authenticity as well as data delivery and processing without interferences and manipulations. This mainly requires scalable and efficient technologies beyond heavy-weight public key infrastructures (PKIs) to identify devices and smart objects in future IoT systems. New material-based scalable and efficient technologies are required to bind unique identities to things in an unclonable manner. In addition, new federated identity management systems are required for collecting, integrating, and processing heterogeneous data from different systems.

5.2.6.1.2 Preserving privacy in multifaceted and dynamic contexts [21] [22]

Privacy issues with IoT systems are complicated by the fact that a system is more than the sum of its parts. There are privacy considerations with low-level devices which may well differ from the concerns generated at an application or data analytics level, and privacy breaches at any level in the system affect the entire system.

For example, low-level RFID tags can be read without line of sight at range and at a high rate of speed [23]. This may mean that the data that discloses an object's location (and, thus, possibly a person's location) can be obtained at a distance. Even passive attacks – effectively eavesdropping on passersby – can compromise user location and data privacy by simply reading tags wirelessly in the vicinity of a reader, and the combination of RFID tags carried together on a person over time can effectively be used as a unique identifier, allowing their location and activities to be silently tracked and correlated with other pieces of information.

Once communication is introduced, even at a low level (such as in wireless sensor networks), the potential surfaces for privacy breaches increase. Because sensors usually have extremely limited computational and storage capabilities (if any at all), novel methods of securing the contents of a data stream, such as embedded and light-weight encryption, are required. Sensors often use hop-to-hop communication schemas that will not support end-to-end encryption. This necessitates the developments and inclusion of novel key exchange schemes and routing protocols.

Unintentional remote access to sensor data exemplifies one level of privacy risk, but even services with intentional access to such data present challenges to user privacy. The intended services accessing the data, whether it comes from a utility company, the device manufacturer or an application provider, furnish additional attack surfaces for breaching confidentiality of the user data, meaning that user data is only as private as the security of the entities which have access to it allows. Further, services with consensual access to user data are all potential adversaries from the data owner's point of view. With the advent of data being stored, transmitted and processed via shared infrastructure, future IoT platforms will require novel services and technologies to enforce adequate access controls and to protect stored data in case of breaches.

In addition, novel technologies, such as usage control, will be required to provide users with the ability to control what happens to their data once it is in the hands of others. This is not only a desirable property for customer satisfaction, but also a legal challenge (for companies) and a right (for end users) in many jurisdictions (e.g. the European Union). Future IoT system implementations will be forced to find ways to both

locally control data exposure and to interface with a variety of other systems while maintaining end-to-end privacy guarantees.

5.2.6.1.3 Trust establishment

Today, most technical trust establishment infrastructures aim at guaranteeing the association between a cryptographic key and the owner of the key in form of a human user or an organization. While decentralized approaches such as the Web of Trust (WoT) exist, most practically used infrastructures, such as CA-based PKIs, are organized around a set of commonly accepted trusted entities, which may establish transitive trust relationships by cross-certification. Such infrastructures have several well-known deficits, which are not limited to IoT. For example, the recent past has shown that trust put into entities (specifically: certification authorities) is not justified in all cases, as cryptographic certificates have been issued for unauthorized users. In addition, registration, certificate issuing and revocations, and especially cross-certification are heavyweight processes which require significant manual work and need to be set up upfront before communication between devices can take place. This makes central trust establishment infrastructures prohibitive for most IoT scenarios, where trust must be established *ad-hoc* with previously unregistered and unknown peers, and without user interaction. Hence, new and lightweight trust establishment algorithms are required.

5.2.6.1.4 Threat analytics and risk management

When considering security requirements and functionality, the balance between performance and security still remains crucial, even with more advanced technology supporting security implementations. Depending on the respective properties of the IoT application and platforms, there is a need to support architectures that provide security functionality corresponding to varying security requirements. Specifically, the three key requirements are adaptability, responsivity, and cooperativity [24].

Future IoT systems need to incorporate adaptability which is a capability to add pre-emptive countermeasures to the system each time a new threat is identified. This uses the PDCA cycle, a widely used technique in security management. PDCA is a way of dealing with the discovery of new threats through an ongoing process involving the identification of a new threat, determining how to counter it, planning how to implement countermeasures, and then proceeding with the implementation and assessment.

Pre-emptive security, however, is often not sufficient. Future IoT systems will also need to be able to respond appropriately for damage mitigation. The growing importance of incident response measures means that the concept of responsivity is also essential to minimize as far as possible the damage that occurs after an attack or disaster, and to speed the recovery. This can be achieved by the OODA loop of monitoring and assessing the situation, then deciding what to do and acting on the decision on a real-time or near-real-time timescale.

Finally, cooperativity is a key requirement for future IoT systems. While the growing interdependence of IoT systems provides advanced services, there are concerns that damage in a particular sub-system caused by an attack or disaster will have an impact on other interdependent sub-systems, resulting in more extensive damage across the entire IoT systems. What is needed to deal with this is to apply the concept of cooperativity by having the different sub-systems establish an accurate assessment of one another's situations.

Hence, securing future IoT platforms requires the development of dynamic security and attack models which consider both the various layers of

systems and systems as a whole as well as the whole lifecycle of the systems. They must factor in the impact of breaches of system parts on the entire system. In broad terms, there are two ways of approaching the task of establishing ongoing countermeasures against the increasingly diverse threats posed by attacks or disasters, and these relate to adaptive security and full-system coverage capabilities.

Even with the introduction of advanced security features and capabilities, there will always remain a residual risk that events occur that lead to fatal events, e.g. natural disasters. Threats due to connected systems, as well as explicit threats to physical security such as human operational errors, systems faults and natural disasters, may result in significant damage and liabilities and will require enhanced security measures as a part of the design and implementation of secure future IoT system architectures. Trading-off between the level of security and cost highly depends on individual conditions, i.e. use case and business environment. Consider for example the security level and costs of producing and deploying medical equipment with those of consumer goods. Naturally, there need to be suitable methods and models to assess individual risks and decide on the trade-off between security and cost during design and implementation of IoT system components. The increased complexity introduced by future IoT systems, end-devices, edge devices and the platform itself requires general information and support for more advanced risk analysis and management, especially when it comes to cyber-physical attacks.

Risk assessment and risk management methods (see also below the topic of continuous security management, which extends the risk management part) spanning the entire lifecycle of complex systems require new technologies to collect and process security-related data and to perform dynamic and online threat analytics based on that data. New approaches based on machine learning algorithms are required to perform real-time threat analytics that will be able to handle trustworthy as well as biased data stemming from heterogeneous and distributed sources. The required novel threat analytics algorithms must produce warnings with high accuracy and minimal amounts of false positive. In addition, they must be resilient against adversarial attacks which deliberately compromise and subvert learning data to control the behaviour of the underlying machine learning algorithms. New, cooperative risk management systems and security protocols are required to enable early warning and reaction capabilities in future IoT systems.

5.2.6.1.5 Continuous security management

Vulnerable components of IoT systems may violate the security requirements of any involved party, e.g. the platform provider or the IoT service consumer. Exploiting such vulnerabilities threatens the business model of any participant. In order to mitigate these risks, security audits of IoT components check whether the components satisfy a set of security requirements, producing a security level.

Traditionally, security audits are discrete tasks producing results which are presumed to be valid for a specific time interval, e.g. one year. With regard to IoT, this assumption of stability does not hold: attributes of IoT components change over time, with these changes sometimes being hard to detect or predict by platform providers and service consumers. Furthermore, only considering security levels of IoT components in isolation falls short of recognizing that IoT services are the result of a multitude of heterogeneous technologies, e.g. platforms and devices, interacting with each other.

Conducting security audits to IoT systems therefore requires a different approach capable

of continuously detecting ongoing changes of IoT services, and assessing their impact on the security level in real-time. In addition, such methods build the foundation of mitigative and preventative security measures which will be required to protect IoT services against attackers.

Section 6

Next-generation enabling technologies for smart and secure IoT platforms

This section focuses on several of the key next-generation enabling technologies needed to realize smart and secure IoT platforms. It addresses the necessary enhancements for the use cases described in Section 4, combining them with the capabilities of Section 5 and consequently deriving the enabling technologies.

An analysis of the three major use cases of this White Paper concerning business continuity management for production lines, Smart Cities and improved journey experience in public transport demonstrates that there is overlap in deficiencies and necessary enhancements. Security, data management in real-time and interoperability are not new in the context of IoT, however they remain crucial and require the full spectrum of next-generation technologies to be solved and applied to real-world scenarios on a daily basis.

On a more concrete level, the technology enhancements derived from the use cases are situated in the following areas, as outlined in Sections 4 and 5:

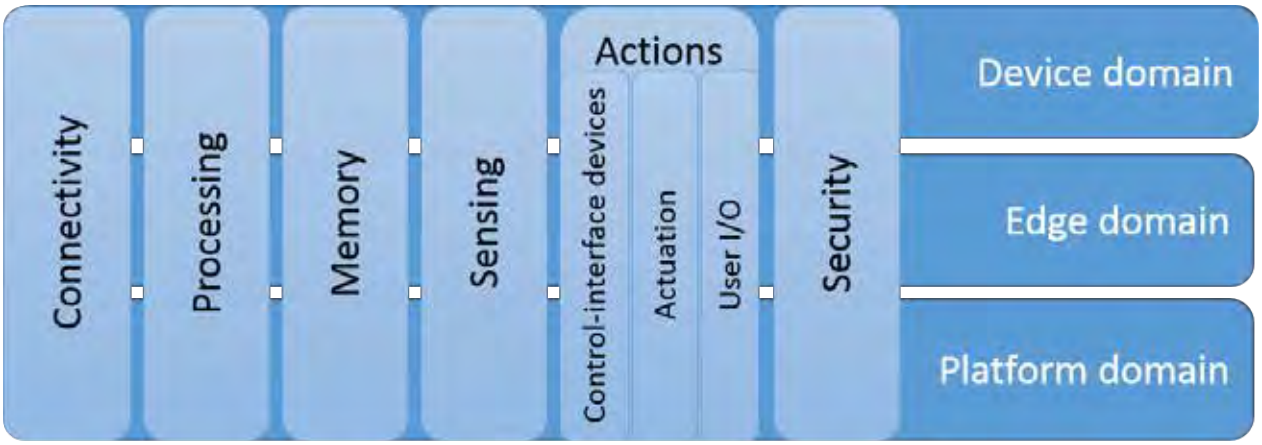


Figure 6-1 | Key enhancement areas

6.1 Connectivity

6.1.1 Transport layer protocol for the next-generation satellite connections (higher bandwidth, high latency)

The TCP (transmission control protocol), which is now widely used as a transport layer protocol in IP networks, has a congestion control function. This function is realized via a mechanism by which a sending device estimates the amount of data which can be transmitted at a time. This data is estimated by increasing the amount incrementally from a small value and reducing the amount when congestion is detected indirectly by an event such as detection of packet loss. A satellite connection usually has high bandwidth and high latency (e.g. several hundreds of milliseconds) and TCP cannot fully utilize the available bandwidth without a good estimation of the amount of data to be transmitted at a time. It takes a certain amount of time for TCP to get a large estimation value of the amount of data to be transmitted at a time, and this fact is problematic in that an end-to-end communication through a satellite connection terminates before TCP can utilize full bandwidth of the satellite connection. It can be effective to develop and introduce a new protocol technology, such as having communication equipment provide bandwidth information instead of having sending device estimates, so that the bandwidth of a satellite connection with higher bandwidth and high latency can be utilized fully.

6.1.2 Next-generation communication systems

6.1.2.1 5th generation cellular access (5G)

5G wireless networks will support 1 000-fold gains in capacity, connections for at least 100 billion devices and a 10 Gb/s individual user experience capable of extremely low latency and response times. Deployment of these networks will emerge between 2020 and 2030. 5G radio access will be built upon both new radio access technologies (RAT) and evolved existing wireless technologies (LTE, HSPA, GSM and WiFi). Breakthroughs in wireless network innovation will also drive economic and societal growth in entirely new ways. 5G will realize networks capable of providing zero-distance connectivity between people and connected machines.

The development of 5G technologies is a cornerstone for realizing breakthroughs in the transformation of ICT network infrastructure. Ultra broadband and intelligent-pipe network features that achieve near instantaneous, zero-distance connectivity between people and connected machines – no matter where they are located – are just the first step.

With regard to next-generation IoT systems, 5G wireless networks will be required to provide support for massive capacity and massive connectivity as well as for an increasingly diverse set of services, applications and users – all with extremely diverging requirements for work and life. Flexible and efficient use of all available non-contiguous spectrums for wildly different network deployment scenarios will be necessary. Mobile networks will increasingly become the primary means of network access for person-to-person and person-to-machine connectivity.

These networks will need to match advances in fixed networking in terms of delivered quality of service, reliability and security. To do so, 5G technologies will need to be capable of delivering fibre-like 10 Gb/s speeds to enable ultra-high definition visual communications and immersive multimedia interactions. These technologies will depend on ultra-wide bandwidth with sub-millisecond latencies.

The increasingly diverse and wide range of mobile services will have differing performance requirements, with latency from one millisecond to a few seconds, always-on users per cell from a few hundred to several millions, and duty cycles

from mere milliseconds to entire days. At the same time, it is expected that 5G will provide signalling loads from less than 1% to almost 100%.

The 5G HyperService Cube below gives a multi-dimensional overview in terms of throughput, latency and number of connections required for the many types of services 5G networks will need to run.

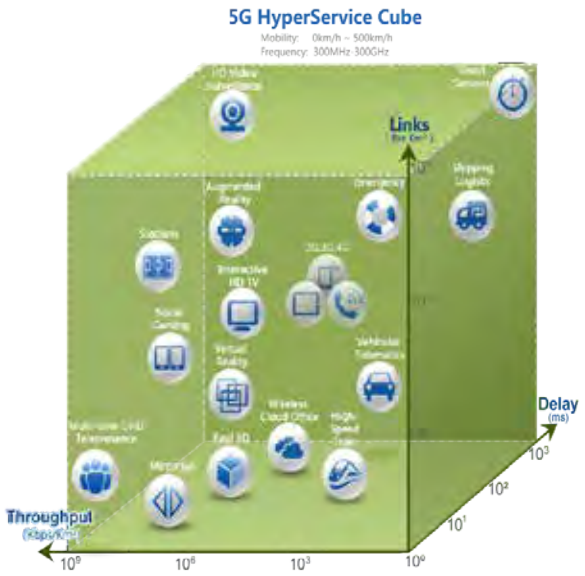


Figure 6-2 | 5G HyperService Cube

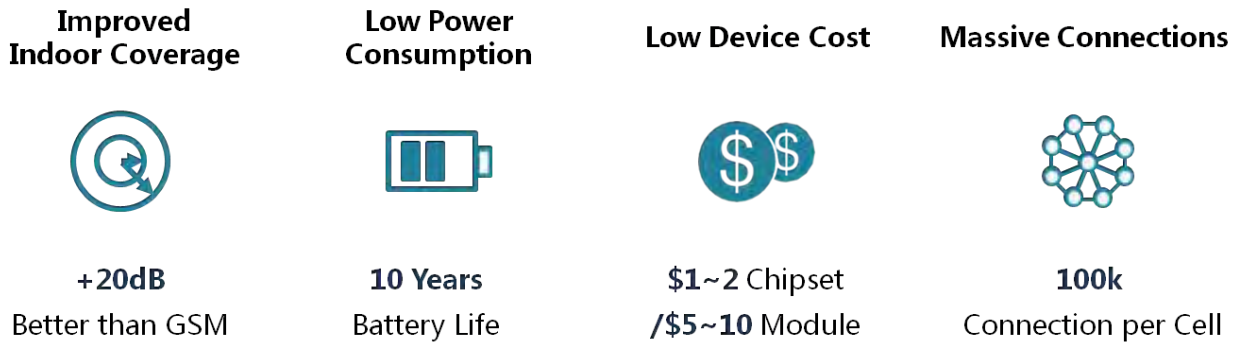
6.1.3 Low power wireless access networks (LPWAN)

The LPWAN market has existed for about 10 years. The current technologies (solutions) supporting this market are fragmented and non-standardized, therefore shortcomings exist, such as poor reliability, poor security and high operational and maintenance costs. Furthermore, the new overlay network deployment is complex.

Recently, new standards have been defined, specifically 3GPP Rel.13 LTE Cat-M1 (eMTC) and Cat-NB1 (Narrowband-IoT), which address the above defects, providing a variety of advantages, such as wide area ubiquitous coverage, fast upgrade of existing network, low-power consumption guaranteeing 10 years battery life, high coupling, low cost terminal, plug and play, high reliability and high carrier-class network security, as well as unified business platform management. The initial network investment may be quite substantial, though superimposed costs are very little. As one of the established technologies mentioned above, Narrow-band-IoT (NB-IoT) perfectly matches LPWAN market requirements, enabling operators to enter this new field, and is thus covered in more detail here as an example for LPWAN technology.

NB-IoT enables operators to operate traditional businesses such as smart metering and tracking, by virtue of ultra-low-cost (USD 5) modules and super connectivity (100K/cell), and also opens up additional industry opportunities, for example, Smart City or eHealth.

NB-IoT makes it possible for more things to be connected, but also managing the commercial value of the resulting big data is a major task. Operators can establish cooperation with related industries: in addition to selling connections, they can also sell data.



Firstly, coverage is the basic requirement for LPWAN applications, mainly because such applications can be deployed anywhere, for instance underground or deep indoors. Current 2G/3G/4G technologies are designed for human connection and fall short of coverage when applied to M2M connections. Data from one of China's cities suggests that about 2% of smart meters equipped with 2G technology cannot report data because of weak coverage. Therefore the grid company has to secure data manually for those 2% of users.

Moreover, low power consumption is a prerequisite for almost 80% of all LPWAN use cases, ranging from applications such as smart meter, smart parking and wearables to smart grid. The basic requirement for such applications is that once a device is installed, it does not need to be serviced for a few years, otherwise the maintenance cost will be increased, For massive connection applications, it would be disastrous to have to change the battery every few days.

Most LPWAN devices are sensors, such as smoke detector sensors, soil detector sensors or security sensors. For such devices, the unit price is very cheap, most of them are sold for around USD 10. In order to connect these sensors the communication module should also be very cheap, not more than 50% of the total price, otherwise price would be a major obstacle for operators to install sensor related applications.

For smart device applications such as point of sales (POS) machines and smart meters, there are already several candidate IoT technologies in use. NB-IoT oversteps those technologies in terms of coverage and power consumption, but price is also an important factor for users in selecting those smart devices. Current prices of 2G modules range from USD 8 to USD 13, while the cheapest SigFox module has already decreased to USD 9. The common view from the industry is that the ideal price for NB-IoT modules should be less than USD 5.

The growth of mobile broadband (MBB) connection numbers is limited by the human population, however IoT connections will connect a myriad number of things, such as cars, meters, animals, plants, etc., so the growth of IoT connections would be much faster than that of MBB connections in the coming few years. As predicted by Machina, the total IoT connection number will be 27 billion by 2024 [25], representing a CAGR of 18%. NB-IoT as a subset of IoT will also undergo significant growth. In order to enable the connection of everyday things, the capacity of the NB-IoT cell should be much larger than that of MBB cells. Based on the assumption that household density per square kilometre is 1 500 with an average of 40 devices in every household, it is necessary to have a capacity of 100 000 concurrent connections in each cell.

6.1.4 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Transport layer protocol for next-generation satellite connections					•			•	•	
5th generation cellular access (5G)				•	•			•	•	•
Low power wireless access (LPWAN)					•	•		•	•	•

6.2 Processing

6.2.1 System configuration and dynamic composition

New sensor fusion technologies will consider data from not only "physical sensors" but also "virtual sensors" such as social media, human inputs (so-called human-as-a-sensor), and crowdsourced data. Incorporating these sensing data in the design of new technologies will steer the advanced capacities of sensor fusion and processing, e.g. for future Smart Cities. Since collecting data in a condensed way will be expected in future IoT platforms, this new technology addresses how to maximize the data utility and minimize privacy exposure when the data is collected. Real-time DevOps technology is an agile process to develop and deploy updated software. Programmable and reconfigurable software components (e.g. algorithms of data analytics or tools of data virtualization) can be decoupled or recoupled quickly to adapt to dynamic updates and requirements in future IoT platforms.

6.2.2 Data contextualization

Data contextualization is a two-fold process. The various IoT components themselves – both individually and collectively – capture much metadata that provides context. Additionally, the data themselves can be subjected to a contextualization transformation process to extract transparent or hidden information behind the collected data. Collectively, the context represents the data in a meaningful form in certain knowledge domains through contextual mining and analytical algorithms. The emerging techniques of data contextualization will significantly enhance historical data analytics, real-time situation awareness, and situation prediction. The historical data analytics update the contextual information and features incrementally. The real-time situation awareness detects certain events and based on them discovers the contextual characteristics of unknown events. The situation prediction forecasts what is going to happen in the future. The data contextualization process can happen on any component of the distributed platform.

An example of data contextualization techniques can be seen in various Smart City applications. As the popularity of mobile devices (e.g. laptops, smartphones, and tablets) grows, the crowdedness in a certain area can be estimated based on emitted signals and location-embedded sensing data from those mobile devices. The contextual information of human mobility is hidden behind the ambient network signals. The historical data analytics finds the regularity of the mobility

patterns (e.g. weekly patterns in train stations). The real-time situation awareness detects the degree of crowdedness. Additional environmental context information is available from other sensors. Cross-referencing between platforms supporting the various services can further provide context. Situation prediction can foresee the time and locations of the crowds based on historical data and real-time data. The IoT gateways in the edge layer perform lightweight data filtering and hashing personal private information before the data is sent to the platform. The major data contextualization tasks are executed in the platform. However, as the capabilities of IoT gateways will be enhanced in the future, the real-time situation awareness can be migrated into the edge side; meanwhile, the high-level contextual information will be reported to the cloud to perform historical data analytics, as the data ages, and further to conduct situation prediction.

Since the future smart and secure IoT platform will accommodate more applications with massive data sources and users, future data contextualization technologies are expected to manage a flexible processing topology for certain quality-of-service requirements. To achieve this goal, processing tasks can be adaptively offloaded onto different entities in the edge and downstream sensing entities. Therefore, the standardization of data exchange models and interfaces needs exploration to facilitate data analytics in parallel. To facilitate meshing up information, additional standardized interfaces for collecting data, annotating situations, and appending mesh-ups from end devices, machines, edge, and platform are also expected. For example, annotating the abstraction of ultra-precise information as semantic places can be performed on data collection from mobile devices to platform in the aforementioned mobility analytics. Finally, future contextualized information models transform information into metadata of situational knowledge which can be used across the entire system.

6.2.2.1 Optimization of resource management

The amount of data and the processing workload in the future platform are increasing drastically. Moreover, the future platform needs to provide multi-tenancy support for various applications. Since the deployment and maintenance costs for large-scale and real-time IoT applications are high, sharing resources across multiple applications and users, managing resources across edge and platform and assigning processing workload across front-end and back-end entities need to be optimized in the future platform to scale up the data contextualization process.

6.2.2.2 Real-time development-and-operation (DevOps)

Since real-time data streaming, data processing and actuation will drive future IoT applications, fast development and operation of IoT services in an on-demand manner are required to steer a set of diverse IoT applications. To achieve this goal, real-time DevOps will be able to shorten the lifecycle of launching a new IoT application, where developers can directly link reprogrammable and reconfigurable components of data contextualization together and activate new services immediately.

6.2.3 Autonomous data exchange

For autonomous data exchange between entities including devices, equipment, IT systems and platforms, the profile, which manages data communication, plays an important role. In order to enable autonomous data exchange, it is necessary to establish data exchange rules. The profile has to be designed based on the data exchange rules, and must provide necessary and sufficient communication management functions. In addition, it also has to serve flexible data access control functions, which control permissions in accordance with situations, for example, purposes of the data use and the security level of the data.

Future IoT systems will enable IoT devices to exchange data autonomously, either directly between themselves (device-2-device) or with the mediation of an edge/cloud platform. Furthermore, IoT systems storing data will exchange this data with other IoT systems (hyperconnected IoT). In order to control this autonomous data exchange, a system mechanism is needed enabling IoT users as well as IoT network providers to control the autonomous data exchange. Such system mechanisms need to work autonomously on behalf of the service developer, IoT user and IoT network provider. Consequently, their needs have to be captured in a respective profile, with a system mechanism then interpreting the profile autonomously. Such profiles are called "autonomous data exchange control profiles (ADECP)". Such ADECP must contain data exchange rules that define what data is allowed to be exchanged and under which condition. Furthermore, the profiles need to contain metadata describing how long the profiles are valid and when a validity check of the profile against an online repository is needed. The profile has to provide necessary and sufficient functions of communication management. In addition, it also has to serve flexible data access control functions that control permissions in accordance with identified situations and context. For example, the purposes of the data use in the target system and the security level of the data can be taken into account. Lastly the profile needs to identify which networking mechanism shall be used during the autonomous data exchange, e.g. encrypted data, encrypted transport layer, virtual network slicing, etc.

For each of the features of ADECP profiles, system mechanisms are needed in the IoT platform. Several such system mechanisms can already be identified:

- Management of ADECP profiles (creation, changing, lifecycle, deletion)
- Auditing of ADECP profiles (monitoring the effects of the ADECP profiles and providing this information to the creator of the profile so that they understand the effects)
- Control functions to instruct devices, edge computers as well as cloud services to autonomously exchange information
- Control functions to enforce the security settings of autonomous data exchange
- Information functions that determine the current situation and context and let the autonomous data exchange functions adapt to the changing situation
- Network control function

6.2.4 Sensor fusion technology

The sensor fusion technology enables smart sensing by combining, integrating and associating data obtained from multiple different sensors to obtain more comprehensive knowledge about observed things, situations and context. Sensors may include image or vision sensors, sonic sensors, odour sensors and tactile sensors. Yet data sources are not limited to physical sensors. Social media data and statistical data collected from smartphones and mobile devices can be regarded as data from "social" sensors. In addition, network beacons can also provide sensing information that describes human mobility and network usage information in a city. In sensor fusion, the more sensors are available in both number and type, the more comprehensive knowledge can be obtained, provided the collected information is properly processed. Therefore, in future sensor fusion, sensor resources will be shared and widely used for multiple purposes by multiple parties. However, the key to applications using future sensor fusion, e.g. as Smart City applications, or applications in the context of public agencies, lies in ensuring integrity and authorization.

One example of information governance would provide both device integrity and authorization features. The device integrity feature ensures that an appliance to be installed by various agencies is not compromised and therefore that

the information accessed from the appliance is reliable. Users would only receive information on a need-to-know basis. In addition, the authorization feature enables various agencies to access information they require, while protecting it using multi-dimension access rights. This means various agencies collaborating in a situation can enforce their respective security policies to ensure access to a set of data by the right users, at the right place and on the right occasion, with the "need to know" criteria. In addition to enabling inter-agency collaboration, the sensor fusion techniques have been exploited to perform crowd estimation for realizing the vision of Smart Cities, where physical sensors such as CO_2, noise, temperature, and humidity sensors are used to extract the correlation between human mobility and environmental conditions.

6.2.5 Machine learning

IoT is creating unprecedented amounts of data. This data provides the necessary information for countless scenarios and use cases, e.g. including threat detection in security critical plants or optimized resource utilization in Smart Cities as described in Section 4. In the past such scenarios have been realized by programming rule-based systems, based on the experience and assumptions of human experts. In essence, there has been a reliance on manually created insights, while the observation of system and the triggering of actions have been automized. However, the dynamicity of future IoT systems and the amount of data they are generating on different levels of the technology stack is prohibiting humans from deriving the necessary insights for explicitly programming the necessary observers, predictors and actuators.

Machine learning enables computers to learn from large amounts of data without being explicitly programmed. Continuously monitoring the generated IoT data streams, intelligent algorithms are able to observe system states and behaviour patterns, learn to predict most probable future system states and potentially use these insights to derive proposals or actions leading to a desired future state. Thus, using machine learning it becomes possible to automate the formerly manual insight creation which is necessary to realize the complex and data-intensive IoT use cases of the future.

Machine learning could ultimately lead to autonomous business, which is a logical extension of current automated processes and services to increase efficiency and productivity rather than simply replace a human workforce [26]. As machine learning makes "things" more intelligent, such things will even gain the capacity to buy and sell in the world of digital business and the IoT. This offers new opportunities for revenue, efficiencies and managing customer relationships, but also poses risks, which need to be managed smartly and ethically [27].

6.2.6 Virtualization

To support future IoT platforms with novel virtualization technologies, virtual machines can be provisioned with logic consisting of operating systems as well as business logic. The device as produced in the factory would have just the hardware, the virtualization layer and the management layer, which connects into the cloud and can download the business logic that allows the device to perform its specific function. Because the shipped device only has logic that ties it into the cloud, device manufacturers can create a generic device that knows nothing about its eventual functionality. The device is connected to a machine, and it obtains the machine's identity through a standard interface. It reports that identity to the cloud, which has been prepared and is expecting the connection report. The cloud then provides the device with the required software content, and the device in turn downloads that

content, instantiates virtual machines and is ready to function. The management layer also makes it possible for the business content to safely communicate with the cloud.

6.2.7 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
System configuration and dynamic composition	•	•	•	•	•				•	•
Data contextualization	•	•	•	•	•	•	•		•	•
Autonomous data exchange	•	•	•	•	•	•	•		•	
Sensor fusion technology	•	•	•	•	•	•			•	•
Machine learning	•	•	•	•	•	•	•	•	•	•
Virtualization				•	•			•	•	

6.3 Memory

While modern streaming, in-memory and other storage technologies enable real time interaction and low or zero latency access for the IoT, the way information is stored is also subject to change. The concept of virtual representation of things and devices as well as storing the data decentrally on the product itself allows for higher scale and facilitates the setup of IoT business networks or supply chains that are not centrally orchestrated.

6.3.1 Digital product memory

The digital product memory (DPM) addresses the vision of the IoT, in which objects carry information about themselves and communicate this information to each other and to the world around them. Previously, with the help of RFID tags or data matrix codes, considerable amounts of data could already be stored and easily accessed. In future IoT systems, the features of semantic product memories will build on and enhance this technology. The concept is based on semantic technologies, M2M communication, intelligent sensor networks, RFID technology and multimodal interaction. Product memories can communicate among themselves and their environment using short-range radio (e.g., Bluetooth, ZigBee, NFC). Semantic technologies allow for a data exchange among various product memories with intelligent environments and for a user-friendly dialogue with the product memory itself [28].

The semantics of the DPM are domain- and industry-specific and are subject to a variety of research projects. For the manufacturing industry, the Reference Architecture Model Industrie 4.0 (RAMI 4.0) of the German Plattform Industrie 4.0 provides the concept of the administration shell, which defines a semantic description of the product master data, product origin, lifecycle, applicable processing methods and tasks that need to be executed. The administration shell can be implemented in different ways, e.g. RDF, RDF Schema or OWL [29].

6.3.2 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Digital product memory				•	•				•	

6.4 Sensing

Over the past decade, smartphones have become a sort of black hole, integrating a huge array of sensors, but mobile is now exploding back out to the environment. Sensors are expanding beyond smartphones to bodies, cars, TVs, and washing machines as well as to buildings [30].

6.4.1 Ultra-precise location technology

The Global Positioning System (GPS) is a space-based navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites [31]. It is one example of sensor technology that is already standard in mobile phones but also entering new fields such as wearables.

GPS reached fully operational capability on July 17, 1995 [32], completing its original design goals. However, additional advances in technology and new demands on the existing system led to the effort to modernize the GPS system. As of early 2015, high-quality GPS receivers provide horizontal accuracy of better than 3,5 metres. Higher accuracy is attainable by using GPS in combination with augmentation systems. These enable real-time positioning to within a few centimetres, and post-mission measurements at the millimetre level [33].

The next major evolution step of GPS – GPS IIIA – will be launched in 2017, and the project involves new ground stations as well as new satellites, with additional navigation signals for both civilian and military users. GPS IIIA aims to improve the accuracy and availability for all users – for example by replacing legacy computers and communications systems with a network-centric architecture, allowing more frequent and precise satellite commands [34].

6.4.2 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Ultra-precise location technology					•		•	•	•	•

6.5 Actions

Although IoT will require less involvement of humans in a few areas, interaction with humans will still be crucial in many areas, as important decisions and creative processes will always involve humans. In order to help humans make the best possible decisions, it is not only important to extract real and reliable information from the vast amount of available data in IoT scenarios, but also to make the data easily digestible and aggregate it to the right level of granularity.

Besides the typical two-and three-dimensional visualization of data on displays, augmented reality and virtual reality will probably become significantly more important and need new approaches on how to visualize data and information for humans to be able to process it quickly and easily.

6.5.1 Augmented reality

Augmented reality is a live direct or indirect view of a physical, real-world environment whose elements are augmented (or supplemented) by computer-generated sensory input such as video, graphics or GPS data. It is related to a more general concept called mediated reality, in which a view of reality is modified (possibly even diminished rather than augmented) by a device. As a result, the technology functions by enhancing a human's current perception of reality [35].

6.5.2 Virtual reality

Virtual reality replicates an environment that simulates a physical presence in places in the real (or an imagined) world, allowing the user to interact with that world. Virtual realities artificially create sensory experience – mainly focused on sight, but can also include hearing and touch. Most up-to-date virtual realities are displayed with special stereoscopic displays, and some simulations include additional sensory information and focus on real sound through speakers or headphones targeted towards virtual reality users. Advanced haptic systems now include tactile information, generally known as force feedback, in medical, gaming and military applications. For IoT applications, the immersive environment should be similar to the real world in order to create a lifelike experience, which requires immense computing power and implementation efforts.

6.5.3 Tactile internet

Many future IoT applications and capabilities will require extremely low latencies in order to be realized. In the realm of user I/O, one of the most anticipated developments is the emergence of the so-called tactile internet [36]. The tactile internet refers to the kind of interfaces and real-time interactions enabled by extremely low-latency I/O bandwidth, driven by the actual latency of human response times. The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) estimates that, in order to work in this real-time human context, "1-millisecond end-to-end latency is necessary in tactile internet applications." [37] This has implications for low-level devices as well as all parts of an IoT system and will definitively require support at the device and platform levels.

6.5.4 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Augmented reality				•	•		•		•	
Virtual reality					•				•	
Tactile internet					•			•		•

6.6 Security

Next-generation enabling technologies will provide secure and trustworthy system collaboration technology for exchanging threat intelligence information between entire organizations. At the same time, fusion technology also on the sensor level allows integration of IT and OT data from multiple data sources. Data science technologies are embedded for processing risk assessment information.

In communication among devices and between devices and edge or devices and platforms, respectively, secure device identification technology and next-generation cryptography technologies such as embedded encryption are major enabling technologies for IoT use cases. Privacy enhancing technology and next-generation cryptography technologies such as searchable encryption are necessary for privacy.

6.6.1 Elemental security technologies

6.6.1.1 Identity of things

When devices which used to be in a closed system get connected to an IoT system, they can be the target of cyber attacks, which are common in IT systems. Securing the identity of a device which enables the identification of each device is important in order to secure the trustworthiness of data generated by devices and the credibility of results obtained by analyzing that data in IoT systems. Hence, identifying things will be a major prerequisite for a successful realization of a secure IoT. Just as biometry for humans is becoming more and more the standard in the authentication of people, the same will be the case for things in the future. Physical unclonable functions (PUFs) are the means of biometry for things. Cryptographic keys and identities can be derived from unclonable material properties, allowing usage of PUFs with classical cryptography, which is based on secret keys. The difference is only that the key is bound to the part and cannot be separated. Additionally, new cryptographic protocols may be implemented through PUFs, which can act as security alternatives in the era of quantum computers.

A device connected to an IoT system can be located in an environment where physical security cannot be provided, and it can be attacked by dismantling or by physical cloning. For this reason, technologies to prevent the identifier of a device from being counterfeited even when the device is physically cloned, such as PUF and TPM (Trusted Platform Module) are important, including technologies to operate and manage those technologies. A PUF can be constructed even through a combination of different materials, which allows identification of combined parts, e.g. a smart card consisting of a card body and

an embedded chip. If the parts are separated the PUF is destroyed and with it the identity of the part and the associated secret keys. Based on such technology the integrity of complex products consisting of many components can be checked.

If the PUF information is inseparably combined with sensor data, such as a watermark, the integrity of sensor data can be ensured from the measurement source up to the cloud, where these data are used for making important sometimes safety-critical decisions.

6.6.1.2 Homomorphic encryption

Homomorphic encryption schemes make it possible to perform mathematical operations on ciphertexts. The results of these calculations can be decrypted and will match the results of the same operations performed on the corresponding plaintexts.

This is due to a property of cryptographic algorithms called malleability. In general, for the purposes of encryption schemes, malleability is an undesired property. If an algorithm possess this property, it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext. And in the case of homomorphic encryption schemes, malleability makes it possible for the result of a mathematic calculation to be decrypted again. Homomorphic encryption became famous in 2009 when Graig Gentry introduced the first fully homomorphic scheme. Before this, cryptographic schemes with homomorphic properties were already known. Nevertheless, having a homomorphic property only means that the ciphertexts are malleable under certain operations, e.g. ElGamal is a cryptographic scheme with a homomorphic property that makes it homomorphic under multiplication. Gentry's scheme was the first scheme that was homomorphic under both addition and multiplication, which is why such schemes are often called fully homomorphic schemes. This allows for a range of applications, such as data analytics on encrypted data or searching on encrypted data without revealing search patterns. However, the performance of the encryption scheme was too low for such applications. Gentry reported timing of about 30 minutes per basic bit operation.

Several new approaches to fully homomorphic encryption are still under development and have yet to come up with more efficient schemes. For example, schemes such as the so-called "somewhat homomorphic encryption", are still under development. They will allow an unlimited number of operations of one kind on a ciphertext and only a small number of operations of the other kind, e.g. a scheme could allow any number of additions on ciphertexts, but only two multiplications.

6.6.1.3 Searchable encryption

Another novel approach in the encryption domain which is currently being developed is called "searchable encryption". It describes encryption schemes which allow a storage provider to search for keywords or patterns in encrypted data. The provider cannot decrypt the stored data and thus – while still able to perform keyword searches – does not gain any knowledge of the underlying plaintext. There are three related concepts relevant to the discussion of searchable encryption:

- **Symmetric searchable encryption (SSE)** is based on symmetric ciphers. The data owner encrypts his data which allows him to organize the data before encryption. He may include additional data structures that allow to efficiently access relevant data, i.e. perform a keyword search on it. Having prepared his data, the owner uploads it to an untrusted server. Naturally, only those who have access to the secret key which was used to encrypt the data can perform searches on the encrypted data stored on the server. One drawback of

this approach is if a query is submitted to the server, then the search pattern is revealed to the server.

- **Asymmetric searchable encryption (ASE)** or public-key searchable encryption differs from SSE in that users who search encrypted data can be other than those who generated the encrypted data. In comparison with SSE, ASE thus supports a larger set of potential scenarios, since SSE, unmodified ASE, also reveals the queries a user makes to the untrusted server where the encrypted data is stored.
- **Single-database private information retrieval (PIR)** focuses on the retrieval of data from a server without revealing what a user is looking for, that is, his search query. In contrast to SSE and ASE, the data on the untrusted server that is queried is not encrypted. In order to hide a user's query, all data items at the server have to be touched. Therefore, PIR schemes require work that is linear in the database size, which constitutes one drawback of this approach. However, it is possible to amortize the cost for multiple queries and multiple users.

Further research and development work is needed to provide homomorphic or searchable encryption schemas that can be efficiently used in future IoT platforms.

6.6.1.4 Trust establishment

As stated above, current trust establishment architectures mainly focus on establishing trust in public keys and their assignment to users. Future IoT scenarios will require in addition trust in transactions and agreements, as well as trust in the integrity of devices and platforms.

6.6.1.4.1 Trust in platforms

In IoT, previously unknown devices will spontaneously interconnect with previously unknown peers and must establish trust with their peers in order to be included in applications. Technically, this boils down to convincing peers that a platform has certain security properties, so that peers can automatically decide to which extent a device may be included in an application, how trustworthy the data provided by it is, and which computational tasks may be assigned to it. Higher trust levels which claim protection against certain types of attacks will foster the enforcement of future usage control technologies, such as remote deletion of critical data after a usage period, or will rank sensor data provided by a trusted device higher than that of its peers. In general, two approaches on automated establishment of trust in remote platforms exist: hardware and software remote attestation. Both are however imperfect as of today. Hardware remote attestation is conceptually sound, but imposes high costs due to specific hardware modules such as hardware security modules (HSMs) or trusted platform modules, which may be prohibitive for low-cost sensor hardware. Also, additional resource consumption by such hardware is not acceptable for many battery-powered devices. As for software remote attestation, it is not possible to conceptually guarantee trust in the overall platform, though practical approaches may exist which achieve an acceptable protection level for most applications. In the future, existing technologies such as code obfuscation, whitebox cryptography, control-flow integrity and sophisticated interweaving of applications with the underlying execution environment will be further developed and integrated to provide holistic software-only remote attestations.

6.6.1.4.2 Trust in transactions and agreements

Besides establishing trust in specific identities and in platform configurations, future IoT applications will need to establish trust in transactions and agreements between peers and be able to prove them to third parties. One technology which addresses this challenge and is currently on the rise is blockchain-based protocols. Here, transactions are not stored by a central trustworthy entity but rather are distributed across any number of equal peers, which reach consensus on a common trusted ledger by making it hard for individual attackers to act against the majority of honest clients. Variations of traditional blockchains go even further by not only documenting past transactions in a trusted way, but also incorporating trusted execution of computing tasks, from which smart contracts can be created, i.e. self-executing contracts between peers for service level agreements, access control, insurance claims, etc. Smart contracts, possibly based on blockchains, will be one of the key building blocks of future IoT trust infrastructures, as they are a prerequisite for business-critical interaction between devices without direct human interaction.

However, current blockchain-based solutions such as Bitcoin, Namecoin or Ethereum still require further research and development to be suitable for security-critical IoT applications. Unbound storage requirements, large-volume data transfers for peers joining the network, the degeneration of a trustworthy peer-to-peer infrastructure to a few central entities dominating the network, and unproven security protocols all have the potential to subvert the current momentum of blockchain-based approaches. One solution might be specific adaptations of blockchain protocols, optimized for IoT applications with limited storage and bandwidth, which support provable security for specific transactions.

6.6.1.5 Secure systems collaboration technologies

Cyber threat intelligence technology that enables cooperative security measures between interdependent systems is essential for realizing secure IoT platforms. The technology aims to provide a common operational picture (COP) that captures the situations of each interdependent system included in the IoT platform. The technology provides standardized terminology that is used to indicate the situation of each organization, mechanisms for exchanging machine-readable information, and the centralized presentation and management of information from different organizations. The technology allows the operators of each system to accurately assess events such as system faults, cyber/terrorist attacks, and natural disasters in near real time manner, which will help them to evaluate the impact the event will cause to their system. The technology also allows different systems to share threat intelligence information that is acquired and managed in each system to realize more cohesive knowledge of the current and future attacks. The current related technologies include: OpenIOC (Open Indicators of Compromise), STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information) [38].

Maturity models such as one provided by CMMI (Capability Maturity Model Integration) and IEC 62443 are a critical component for realizing cooperative and secure IoT platform. CMMI provides maturity levels that define the performance of systems and their operators in regards to fulfilling the security requirements that are applied to the platform. This is crucial for operators of the interdependent systems, as it provides standardized criteria for assessing security capabilities of the interdependent systems, hence ensuring a level of security between them.

6.6.2 Security as a service

The plethora of new requirements on security architectures and services in future IoT systems must not be regarded as a hurdle, but rather as a driver for the development of promising technological enabling services, which will be at the core of future business models by themselves. Two main research streams will foster the creation of new service offerings: automating security monitoring and a paradigm shift from avoiding data collection to controlling data usage.

6.6.2.1 Privacy through usage control

One mitigation, which can also be seen as a future enabling technology, is data usage control. It is an extension from traditional access control concepts, respecting that data usage is an ongoing process, has a purpose and is not binary, but rather must be differentiated in terms of data perspectives and operations. None of these aspects are covered by traditional access control, which merely regulates accesses to data resources by subjects at a single point in time. Future data usage control technology will track and label data as it is processed by various systems and will allow definition of fine-granular usage restrictions in order to enforce privacy properties over large data sets, while still allowing the running of learning algorithms and analytics over them. One example is to enforce data perspectives at a certain aggregation level which ensures that individual users cannot be deanonymized. Another example is to grant access to raw data, but prevent combination of specific data sets in order to protect users' privacy, or to introduce perturbations in personal data without affecting the results of analysis.

6.6.2.2 Continuous security audits

Continuously reasoning about the security level of IoT systems requires automatically collecting and evaluating evidence, i.e. observable information of the IoT systems. Depending on how evidence is collected, test-based and monitoring-based methods can be distinguished. Test-based audits produce evidence by controlling some input to the IoT system and evaluating the output, e.g. calling a component's interface and checking responses. Monitoring-based audits analyze evidence which is generated as part of the productive deployment of an IoT system, e.g. log files, performance metrics, etc.

Several challenges exist that continuous security audits of IoT systems have to master. First, methods to consistently define and describe IoT system components are essential for determining which components compose a particular IoT system at a certain point in time. Moreover, these service descriptions have to be exchanged between heterogeneous IoT systems, thus supporting distributed discovery of IoT components. Secondly, provided there are IoT service descriptions available, test-based and monitoring-based security audit methods have to be developed which support dynamic assessment of real-time security levels of IoT systems. These audit methods need to be able to assess a multitude of heterogeneous IoT components, ranging from minimal-invasive, lightweight approaches required for thin devices to comprehensive security evaluations of platforms and the edge component.

6.6.3 Identity management

Modern identity and access management (IAM) systems allow for secure, integrated management of data from different devices and systems. In a future IoT system, autonomous data exchanges among different entities must be controlled based on advanced security and trust management technologies, e.g. usage control or trustworthy device identification. At the same time, applications in different domains need to be isolated and security boundary technologies need to ensure isolating for incident-affected subsystems.

6.6.3.1 IAM technologies for IoT

The modern IAM technology stack in the web consists of SAML [39], OpenID-Connect (OIDC) [40], OAuth 2.0 [41] and SCIM [42]. While SAML is popular in large organizations like multi-national corporations and academia, OpenID-Connect is a rather young but already established technology for authentication in web applications and services with large identity providers including Google and Facebook. SAML is addressing a variety of IAM needs including identity federation and SSO functionality. However, the protocol's complexity and the footprint of most software implementations limit its usefulness for IoT. OAuth 2.0 and especially currently emerging extensions like ACE [43] addressing constrained environments fit well into IoT ecosystems. Furthermore, the OAuth 2.0 protocol is compatible with constrained device protocols such as CoAP [44] and MQTT [45]. Consequently, OAuth 2.0 has even found its way into the OT world [46]. OAuth 2.0 is also highly extensible allowing use-case centred configuration and use. Features that were initially lacking in OAuth 2.0, such as proof-of-possession schemes [47], are gradually added. Beyond the traditional and established protocols and concepts, alternative approaches are emerging. For instance, blockchain-based approaches to IoT have built-in policy enforcement, device registration and accountability features. However, the viability of such a concept still remains an open question.

6.6.3.2 Application isolation and security boundary technologies

Software-defined perimeter (SDP) is a technology used to build a security boundary dynamically in order to isolate the application infrastructure in danger and to protect other application infrastructures against network-based attacks. CSA (Cloud Security Alliance) has established a specific working group to study SDP and already issued a specification [48]. The working group further initiated a study on SDP for IaaS. Software defined networking (SDN) can be used to enable SDP functionality to achieve network-level security against unauthorized access and malwares [49]. Collaborating with firewalls to detect anomalous behaviour, the system decides proper networking to isolate as well as block the target hardware and to dynamically re-route communication paths to continue normal operation with other hardware.

6.6.4 Mapping to use cases

	Industrial				Public		Customer			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Identity of things				•	•	•	•	•	•	•
Homomorphic encryption				•	•	•	•		•	
Searchable encryption					•	•	•		•	
Trust establishment				•	•	•	•		•	
Secure systems collaboration technologies	•	•	•	•	•	•	•	•	•	•
Privacy through usage control					•	•	•		•	
Continuous security audits					•		•			
IAM technologies for IoT	•	•	•	•	•	•	•	•	•	
Application isolation and security boundary technologies	•	•	•	•	•			•	•	

Section 7
Standards

In looking at the IoT standardization landscape, it becomes clear there is significant fragmentation of effort and overlapping of initiatives. This is not surprising given the current hype associated with this technology, however as with web services, cloud computing and the many other initiatives that have gone before it, the fragmentation is detrimental to achieving the smart and secure IoT platform.

7.1 Environment

To help understand the current state of standardization in the IoT space, it is necessary to look at both the current environment as well as the desired environment.

7.1.1 Current IoT standardization environment

An analysis of the current environment provides the following key takeaways:

7.1.1.1 Leading negatives

- **Initiatives** – There are a multitude of competing standards and consortia initiatives in both the horizontal and vertical spaces at every layer of the IoT stack. Although there is no set number for this issue, one IEC member reported tracking more than 50 major IoT standardization initiatives that directly affected its product offerings.
- **Requirements** – Standards development organizations and consortia are faced with a wide variety of fragmented, inconsistent, and competing requirements. This is driven in part by industry competition, which is understandable. Lack of clarity on the technology adds to the situation. A lack of clear consensus on what should be standardized versus what should remain competitive exists. Unfortunately, competition between the various SDOs and consortia themselves also adds to the problem.
- **Data ownership and privacy** – Significant issues around data ownership and privacy abound. There is widespread disagreement between all parties – end users, device or sensor owners or manufacturers, IoT system providers or the persons who contract for the system, platform providers, to name but a few.
- **Government** – Geopolitical agencies at every level are looking at IoT regulatory responsibilities and opportunities. In many cases, the resultant regulations are expected to be detrimental to IoT, as they either set unrealistic or restrictive boundaries that will negatively impact IoT innovation, or are too narrowly focused on government requirements at the expense of those of the private sector and the individual.

7.1.1.2 Leading positives

- **Emerging coalescence** – There appears to be the genesis of a coalescence around requirements and alignment of deliverables. The Industrial Internet Consortium (IIC), The Industrie 4.0 initiative, China 2025, and OpenFog are examples of IoT organizations who are defining requirements rather than standards. They are all committed to submitting those requirements to the appropriate SDO for modification of existing standards or

development of new standards. They are also starting to work collaboratively together. Good examples of this are the emerging relationship between the IIC and I4.0 groups, who are collaboratively mapping their respective reference architectures and identifying other opportunities to grow and expand their relationship, the enhancement of collaboration agreement between the Japanese Robot Revolution Initiative and Industrie 4.0, and the recently signed agreement of advancement of cooperation between the Japanese Ministry of Economy, Trade and Industry (METI) and the German Federal Ministry for Economic Affairs and Energy (BMWi) .

- **Emerging analysis** – Many of the leading SDOs and consortia are actively engaged in research and analysis around IoT and quality results are emerging. Some good examples include this IEC White Paper on the smart and secure IoT platform, the IIC IIRA & IIC security framework documents, Industrie 4.0 RAMI, the ISO/IEC JTC 1 WG 5 report on IoT, and the work of ISO/IEC JTC 1 WG 9 Big Data and WG 10 IoT.
- **Natural selection** – Some shrinking of the standards/consortia space is beginning to be visible as the hype levels begin to subside and the reality of needing to make actual contributions begins to sink in. This aspect of the cycle, however, is still in its early stages, and much remains to be done.

7.1.2 Desired future IoT standardization ecosystem environment

As shown in the previous section, the current standardization environment provides challenges to optimizing IoT standardization and opportunities to create a more positive standardization ecosystem that supports the needs of governments, the private sector and users. This ecosystem should be one of collaboration across the spectrum of SDOs and consortia as outlined below.

7.1.2.1 Standards

For the purpose of this analysis, we lump together the various deliverables from recognized SDOs without prejudice under the banner of standards.

- **Horizontal standardization** – International standards should be the preferred approach for standards activities that cross domains, geopolitical boundaries, functionalities and requirements elaborated at the international level.
  - Horizontal standards from ISO, IEC, ITU, IEEE
  - Internet standards from IETF
  - Horizontal common service standards from oneM2M
  - Modelling standards from the Object Management Group
  - Web Standards from W3C
- **Vertical and specialty standards** – Standards that are domain-specific or geopolitical should come from relevant organizations. Wherever possible, they should draw on higher-level horizontal standards.

7.1.2.2 Requirements for standards

Leading consortia should define requirements and feed those requirements to existing standards bodies. A two-tier approach similar to the standards approach above is recommended.

Horizontal organizations should take the lead for their respective areas and establish working liaison relationships for the sharing of requirements and feedback. Examples in this space include IIC, OpenFog, AIOTI, AllSeen Alliance, OMA, and NGMN.

Vertical consortia should define requirements for their respective areas and establish working liaison relationships for the sharing of requirements and feedback. Examples in this space include Industrie 4.0, China 2025, AIOTI, Robot Revolution Initiative [50], and Industrial Value Chain Initiative [51].

7.1.2.3 Suggested roles and limitations

Government	▪ Should focus exclusively on requirements for public sector IoT such as Smart City ▪ Should collaborate on sharing requirements with each other and with the open standards bodies and industry consortia ▪ Should align with private sector and push for greater alignment between competing organizations and initiatives ▪ Should not define standards or dictate statutory use of standards ▪ Should avoid dictating regional policies on data ownership, data stewardship, and data use
Private sector	▪ Should push for maximized development and use of international, open standards ▪ Should, with public sector, push for alignment between competing standards bodies and consortia ▪ Should coalesce around key standards bodies and consortia
Standards bodies and consortia	▪ Should replicate good relationships with other organizations such as IIC/I4.0 partnership as much as possible ▪ Should focus on their core standardization competency and not develop competing requirements or standards for the sake of organizational survival or expansion

7.2 Standards requirements

Sections 4, 5, and 6 identify a number of specific standardization requirements essential to realizing the smart and secure IoT platform. The following table summarizes those requirements.

Connectivity	▪ 5G – Dramatic increases in IoT network performance and data flow dictate rapid finalization of the 5G. Although research efforts and prototype deployment are ongoing, realization of the "standard" through widespread deployment is still not projected until 2020 at best. With the expected lag time in consumer uptake, IoT will have to wait too long. ▪ Next-generation satellite connections – To better support the anticipated massive increases in network loads and latency requirements, a standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and devices is required. As explained in Section 6.1, effectiveness is increased with communication equipment in network. At the WRC (World Radiocommunication Conferences) of 2015 held by ITU-R, new radio frequencies were allocated to a satellite communication system for earth stations in motion, such as airplanes and ships. Additional allocation of radio frequencies to earth stations in motion is planned to be discussed in the WRC of 2019. ▪ Flexibility – System resiliency, dynamic composition, and related capabilities require creation of standards for IoT equipment to have the capability to update to new connectivity standards as they deliver.
Processing	▪ Data contextualization technology, data contextualization standards, and semantic interoperability standards are needed for information clarity within and across domains at the device, edge and platform levels. Development of relevant standards should focus on the following areas: – Information exchange models – Semantic metadata definition standards and models – Data exchange models and interfaces and related standards – Autonomous data exchange profiles and exchange mechanisms – Metadata annotation models and interfaces – Contextualized information models – Metadata context standards
Memory	▪ Standardization of digital product memory
Sensing	▪ Metadata ▪ Abstraction for ultra-precise location-based technologies ▪ Sensor data privacy (opt-in/opt-out for end customers/consumers) ▪ Sensor fusion – Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	▪ A standard template for uniquely identifying groupings of control interface devices ▪ General standard to normalize IoT user I/O across systems ▪ Unique IoT accessibility requirements reflecting the advanced IoT services that go beyond typical human/computer I/O

Security	▪ ID federation in social systems ▪ Cyber-physical attack protection ▪ Device identifier across multiple systems with simultaneous connections, such as an IRI from the W3C ▪ Protocols for establishing trust in platform integrity ▪ Cooperative security framework that enables exchanging of cyber threat intelligence between interdependent systems ▪ Maturity models that enable security capability assessment between interdependent systems

7.2.1 Mapping to use cases

		Industrial				Public		Customer			
		BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
Connectivity	Realization of the 5G standard				•	•			•	•	•
	Standard for new transport layer protocol to support higher bandwidth-demanding latency between satellite and device					•				•	
	Standards for IoT equipment to have the capability to update to new connectivity standards				•	•			•	•	•
Processing	Information exchange models	•	•	•	•	•	•	•	•	•	•
	Semantic metadata definition standards and models	•	•	•	•	•	•	•	•	•	•
	Data exchange models as well as interfaces and related standards	•	•	•	•	•	•	•	•	•	•
	Autonomous data exchange profiles and exchange mechanisms	•	•	•	•	•	•	•		•	
	Metadata annotation models and interfaces	•	•	•		•				•	
	Contextualized information models	•	•	•	•	•	•	•	•	•	•
	Metadata context standards		•			•				•	•
Memory	Standardization of digital product memory					•				•	

Sensing	Standard for metadata	•	•	•	•	•	•	•	•	•	•
	Abstraction standard for ultra-precise location-based technologies					•		•		•	
	Sensor data privacy standard					•			•	•	
	Sensor fusion standard	•	•	•	•	•				•	•
Actions	Standard template for uniquely identifying groupings of control interface devices					•				•	
	General standard to normalize IoT user I/O across systems					•			•	•	
	Standard for unique IoT accessibility requirements					•			•	•	•
Security	ID federation standard in social systems	•	•	•		•	•	•		•	•
	Cyber-physical attack protection standards	•	•	•	•	•	•	•			•
	Standard for device identifier across multiple systems with simultaneous connections	•	•	•		•	•	•	•	•	•
	Standard protocols for establishing trust in platform integrity	•	•	•	•	•	•	•	•	•	
	Cooperative security framework	•	•	•		•	•	•		•	
	Maturity models that enable security capability assessment between interdependent systems	•	•	•		•	•	•		•	

Section 8
Recommendations

Based on the findings contained in this White Paper, a number of opportunities exist to move IoT forward and to help achieve the smart and secure IoT platform.

8.1 General recommendations

All SDOs, consortia, geopolitical entities and others involved in IoT definition, development, deployment and operation should publically adopt as a guiding principle the desired future IoT standardization ecosystem environment described in Section 7.1.2.

All SDOs, consortia, geopolitical entities and others involved in IoT definition, development, deployment and operation should look for opportunities to foster increased levels of cooperation and collaboration.

Governments should increase funding support for unrestricted research into the various technology requirements identified in Section 6.

ITU, IEEE, and 3GPP should take the lead in pushing 5G finalization and deployment until 2018.

Governments and the private sector should come together to create a joint cooperative security framework to enable the exchanging of cyber threat intelligence between interdependent systems, identification of future security enhancement opportunities, and identification of potential needed standardization activities.

8.2 Recommendations addressed to the IEC and its committees

The IEC, as one of the globally recognized *de jure* standards organizations, is in a unique position to drive the IoT forward and help make the smart and secure IoT platform a reality. Accordingly, the IEC should take the following actions:

- Publically adopt as a guiding principle the desired future IoT standardization ecosystem environment described in Section 7.1.2
- Work with recognized leaders of the organizations described in 7.1.2 to establish a formal MoU recognizing the proper roles of named SDOs and consortia, government entities such as the European Community, and individual governments. The MoU should include establishment of an overarching MoU Management Board of participants to collaborate as much as possible towards creating the desired environment
- Review the findings and recommendations contained in Sections 5, 6 and 7 and identify specific activities to be undertaken by the IEC Standardization Management Board (SMB)
- Urge the ISO/IEC JTC 1 leadership to assign responsibility to ISO/IEC JTC 1 SC 32, in cooperation with WG 9 and WG 10, to develop requirements and standards for IoT:
  - Information exchange models
  - Semantic metadata definition standards and models
  - Data exchange models and interfaces and related standards

  - Metadata annotation models and interfaces
  - Contextualized information models
  - Metadata context standards
- Urge the ISO/IEC JTC 1 leadership to assign responsibility to ISO/IEC JTC 1 SC 27 to review the security requirements identified in Sections 4, 5, 6 and 7 and initiate activities as appropriate
- Urge the ISO/IEC JTC 1 leadership to assign responsibility to the appropriate SC/WG to start a standardization activity on autonomous data exchange to define
  - the profile that control the autonomous data exchange profiles (ADECP)
  - the system mechanism to manage and enforce the ADECP
  - and the interfaces and mechanisms needed in IoT devices, edge devices and clouds to enforce the ADECP
- Work with government entities to increase the level of participation and identification of requirements so that IEC deliverables address their concerns
- Endorse greater ITU-R radio frequency allocation

Annex A – Use case

Business continuity management (BCM)

1 Description of the use case

1.1 Name of use case

Business continuity management (BCM)

1.2 Scope and objectives of use case

1.2.1 Scope

- Domain: manufacturing, logistics, supply chain management.
- Architectural levels: IoT platform, device, edge, cloud.

1.2.2 Objectives

- Advanced risk assessment by gathering and sharing incident information.
- Automated and instant implementation of security measures.
- Optimum production replanning in response to cyber threats.

1.3 Narrative of use case

1.3.1 Summary of use case

- Sense: sense field status and turn it into data
  - Gather data from various security systems into an IoT platform.
  - Gather data from production control systems into an IoT platform.
- Think: analyze data and create action plan
  - Analyze the data gathered above to perform risk analysis.
  - Analyze the data gathered above to replan optimal production plan.
- Act: implement action plan
  - Implement security measures.
  - Implement production plan.

1.3.2 Nature of the use case

- A cooperative security framework in which IoT platform analyzes data integrated from different systems and creates action plans to realize business continuance.
- A responsive security framework in which IoT platform implements necessary security measures while minimizing effect to production activities [52].

1.3.3 Complete description

- An IoT platform gathers incident information from various security systems as well as actual and planned production data from production control systems.
- The IoT platform analyzes the incident information and performs risk analysis of the incident. It also creates security measures such as risk mitigation plans that will minimize the effect to the production activities.
- The IoT platform implements security measures such as termination of communication lines or interruption of production lines.

- Meanwhile, the IoT platform analyzes the production data to create an optimal production plan in response to affected production capabilities of each production site [53].

1.4 Diagrams of use case

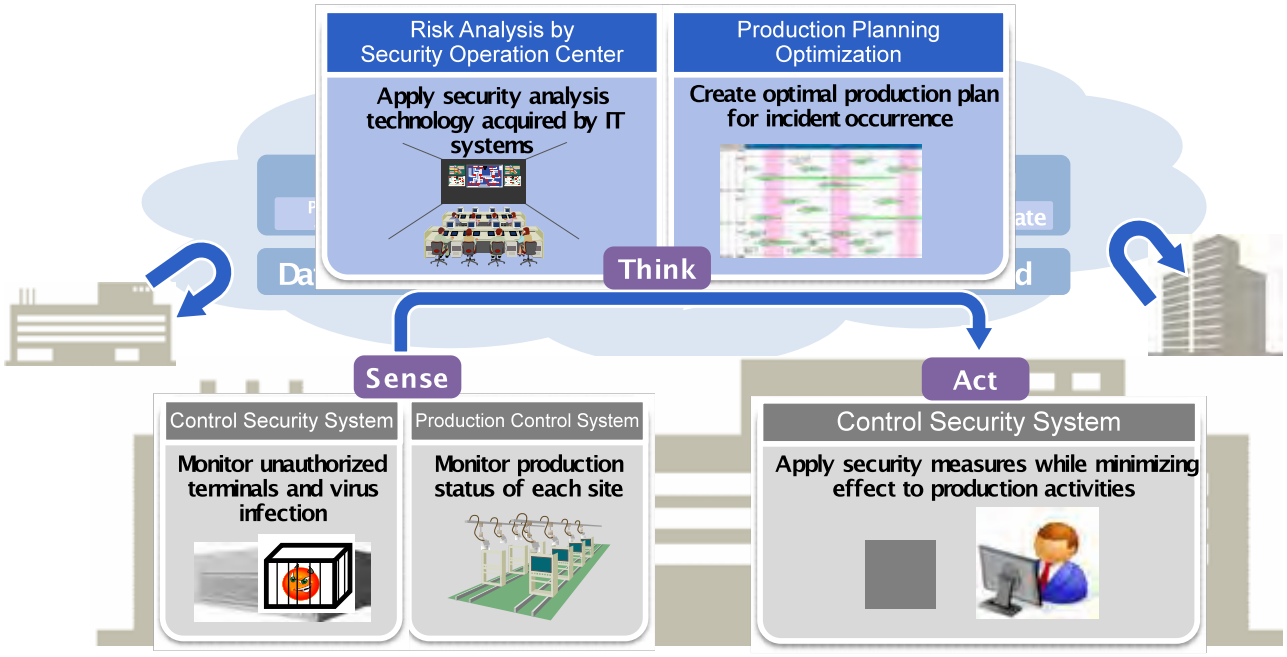


Figure A-1 | Diagram of use case – Business continuity management

1.5 Use case conditions

1.5.1 Assumptions

Involve multiple systems operated by different operators.

1.5.2 Prerequisites

None.

1.6 Further information for the use case

1.6.1 State of the art

- Status quo
  - Quasi real time data gathering and analysis (typical analysis cycle is monthly) of the production control systems.
  - Creation of security measures which is independent from the production activities.
- State of the art
  - Creates security measures based on the incident information from various security systems, which take into account the impact to the production activities by data gathering and real time analysis of the production activities.
- To switch status quo to state of the art, technologies/standards to integrate data of security systems and production control systems are needed.

1.6.2 Relation to other use cases (including sub- and super-use cases)

The use case of Collaborative SCM is related to this use case as it also focuses on integration of data from multiple systems.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol		Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards	X	Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization		
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/ resilience
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership		
(Swarm) awareness		

2.3 Memory

Capability		Remark
Digital product memory		Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities		
Privacy		
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors		

2.5 Actions

Control interface devices

Capability		Remark
Calibration		
Control of group of devices		Runtime and configuration
Dynamic composition of devices		Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context		
Safety requirements	X	
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control		

User I/O

Capability		Remark
Tactile interfaces		
Multi-device user-interfaces		
Virtual modelling		
Simulation	X	
Accessibility		For disabled people
Augmented reality		E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)		
	Low power wireless access (LPWAN)		
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology		
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet		
Security	Identity of things		
	Homomorphic encryption		
	Searchable encryption		
	Trust establishment		
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard		
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards		
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces	X	
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O

	Standards requirements		Remark
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex B – Use case

Anomaly detection system for advanced maintenance services

1 Description of the use case

1.1 Name of use case

Anomaly detection system for advanced maintenance services [54]

1.2 Scope and objectives of use case

1.2.1 Scope

- Domain: maintenance for manufacturing domain, etc.
- Architectural levels: IoT platform, device, edge, cloud.

1.2.2 Objectives

- To enable automation of equipment status diagnosis that previously required engineers with specialist knowledge.
- To help prevent losses from unexpected production facility shutdowns and to improve availability, by detecting anomaly with high accuracy.
- To lower the time and cost of maintenance management by carrying out maintenance appropriately in line with equipment status.

1.3 Narrative of use case

1.3.1 Summary of use case

An anomaly detection system (applied to compact gas engine generators) automatically gathers data from dozens of sensors for parameters such as temperature, pressure, and engine speed. It stores the data in a database, then automatically executes a diagnosis process using two functions – a remote monitoring function and a data mining function. The diagnosis result can be communicated to maintenance service personnel using a list screen of color-coded statuses for each piece of equipment.

1.3.2 Nature of the use case

- Designed to provide advance knowledge of changes to anomalous hardware statuses by using data mining technology to extract significant information from big data.
- Automatically gathering data from dozens of sensors.
- Automatically executing a diagnosis process using two functions – a remote monitoring function and a data mining function.
- Showing the diagnosis result using a list screen of color-coded statuses for each piece of equipment.

1.3.3 Complete description

- An example of an anomaly detection system applied to compact gas engine generators is as follows.
- This anomaly detection system automatically gathers data from dozens of sensors for parameters such as temperature, pressure, and engine speed. It stores the data in a

database, then automatically executes a diagnosis process using two functions – a remote monitoring function and a data mining function. The diagnosis result can be communicated to maintenance service personnel using a list screen of color-coded statuses for each piece of equipment (see 1.4).

- The remote monitoring function is a physically based diagnosis function that detects status changes after upper/lower threshold values and rate-of-change evaluation criteria for each sensor signal gathered from the equipment have been set from operator experience and knowledge. Evaluations are made by setting an anomaly detection threshold value for each sensor. Each sensor signal has a single evaluation threshold value and vice versa, making it easy to explain generated errors and failures, but making it difficult to detect status changes involving multiple sensor signals. When there are seasonal variations or differences in equipment installation environments, separate settings are also needed for each of the changing conditions. When there are many different failure types, each will have a different occurrence frequency, so it may not always be possible to determine the optimum setting value. Another difficulty is that even among failures of the same type, the process leading to the failure or the cause of the failure might be different in each case, making it impossible to determine a single setting value for each failure type.
- The data mining function is an example-based diagnosis function that is trained with normal-status data to learn statistical reference points. It detects equipment status changes on the basis of the distance between the measurement point in the statistical data space, and the reference point. The data mining function has higher sensitivity than the remote monitoring function, so could enable early detection of status changes. But a drawback of conventional data mining functions is that causes are difficult to explain when diagnosis results are derived from complex sensor signal correlations. This system has been designed to assist status monitoring and cause analysis by outputting an ordered list of the sensor signals responsible for a detected status change.
- The anomaly detection system consists of a data gathering unit that receives sensor signal data from the equipment (a pre-existing data gathering mechanism can be used if present), a data storage unit that stores the gathered data, a diagnosis process unit that analyzes the stored data, and a display unit that outputs the analysis result (see 1.4). Each of the functions above is placed where it should be in the IoT platform in consideration of application.
- Data mining technologies (diagnosis engines) used as anomaly detection algorithms perform machine learning on normal-status sensor data, create indicators of differences between the data to be monitored and the learned normal data group, and evaluate whether the result is normal (same as the normal data) or anomalous (different from the normal data).
- If the diagnosis engines are non-parametric methods, they are resilient to statistical restrictions on sensor data. And if the algorithms are model-free, they can respond flexibly without the need for model construction or simulations for each status change, even when there is a major change in a device or system operation status.
- The optimum system configuration can be created by using each diagnosis engine separately according to the device or system to be monitored, or to the characteristics of the anomaly to be detected.

1.4 Diagrams of use case

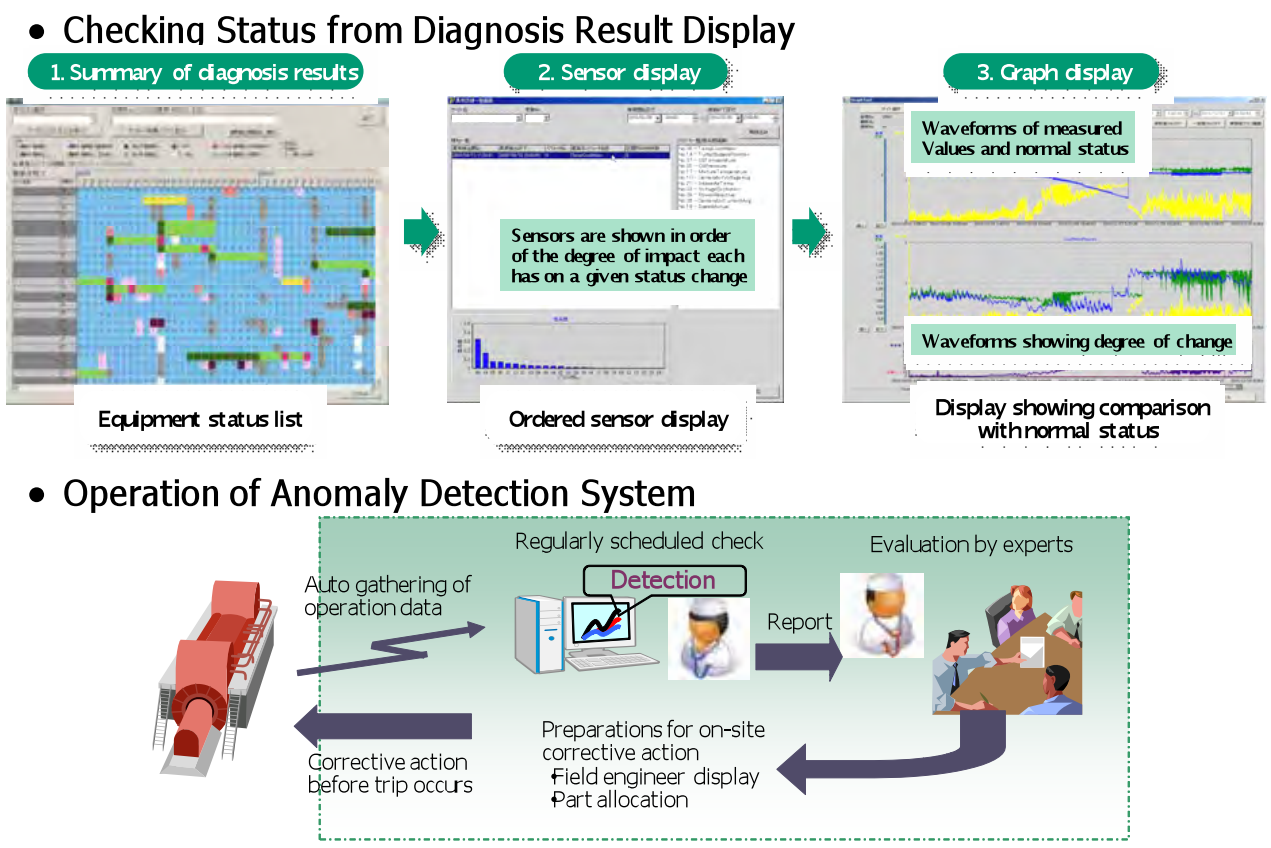


Figure B-1 | Diagram of use case – Anomaly detection system for advanced maintenance services

1.5 Use case conditions

1.5.1 Assumptions

Possible to collect and store massive amounts of operation records data and sensor data.

1.5.2 Prerequisites

None.

1.6 Further information for the use case

1.6.1 State of the art

- Status quo
  - Performing remote monitoring of compact gas engine generators throughout a country.
  - Applying the system to a limited number of what is to be monitored.
  - Performing daily diagnosis of several tens of different sensor signals measured in several tens of seconds cycles.
- State of the art
  - Performing remote monitoring of compact gas engine generators throughout the world.
  - Performing remote monitoring of various types of equipment.
  - Applying the system to a vast number of equipment.

  - Performing real time diagnosis of greater amounts of different sensor signals measured in less second cycles.
  - Analyzing stored data not only for anomaly detection but also for various other purposes.
- To switch status quo to state of the art, technologies/standards to improve performances throughout IoT platform are needed.

1.6.2 Relation to other use cases (including sub- and super-use cases)

The predictive maintenance and service use case is related to this use case.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol		Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards		Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization		
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/ resilience

Capability		Remark
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness	X	

2.3 Memory

Capability		Remark
Digital product memory	X	Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy		
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors		

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements		

Capability		Remark
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence	X	
Swarm control of security	X	
Context-aware control	X	

User I/O

Capability		Remark
Tactile interfaces	X	
Multi-device user-interfaces	X	
Virtual modelling	X	
Simulation	X	
Accessibility	X	For disabled people
Augmented reality		E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems,…
Securing ID of devices		
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)		
	Low power wireless access (LPWAN)		
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology		
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet		
Security	Identity of things		
	Homomorphic encryption		
	Searchable encryption		
	Trust establishment		
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard		
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards		
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces	X	
	Contextualized information models	X	
	Metadata context standards	X	
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O

	Standards requirements		Remark
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex C – Use case

Collaborative supply chain management (SCM)

1 Description of the use case

1.1 Name of use case

Collaborative supply chain management (SCM)

1.2 Scope and objectives of use case

1.2.1 Scope

- Domain: manufacturing, logistics, supply chain management.
- Architectural levels: IoT platform, edge, cloud.

1.2.2 Objectives

- Base management and optimum logistics planning.
- Base placement optimization.
- Global supply and demand adjustment.

1.3 Narrative of use case

1.3.1 Summary of use case

- Sense: sense field status and turn it into data
  - Gather data from PSI (product, sales, inventory) systems into an IoT platform.
  - Gather data from production control systems into an IoT platform.
- Think: analyze data and create action plan
  - Analyze the data gathered above to create a base management and optimum logistics plan.
  - Analyze the data gathered above to create a base placement optimization plan.
- Act: implement action plan
  - Implement a global supply and demand adjustment plan through creating it in an IoT platform.

1.3.2 Nature of the use case

- An IoT platform analyzes data integrated from different systems and creates action plans to realize various types of unprecedented benefits/applications.
- Beyond silos [52].

1.3.3 Complete description

- An IoT platform senses actual and predicted PSI (product, sales, inventory) data from PSI management systems, which visualize global PSI, and senses actual and planned production data from production control systems, which visualize production progress and plan the best production [55].
- The IoT platform comes up with a base management and optimum logistics plan, using a simulator to analyze the data gathered above and evaluates the business value with high accuracy.
- And the IoT platform also anticipates a base placement optimization plan to optimize factory/logistics base placement to expand to global markets by analyzing the data gathered above.
- The IoT platform acts (implements) a global supply and demand adjustment plan to place proper quantity of stocks with reacting demand

fluctuation and mutually interchange stocks with others after analyzing the data gathered above.

1.4 Diagrams of use case

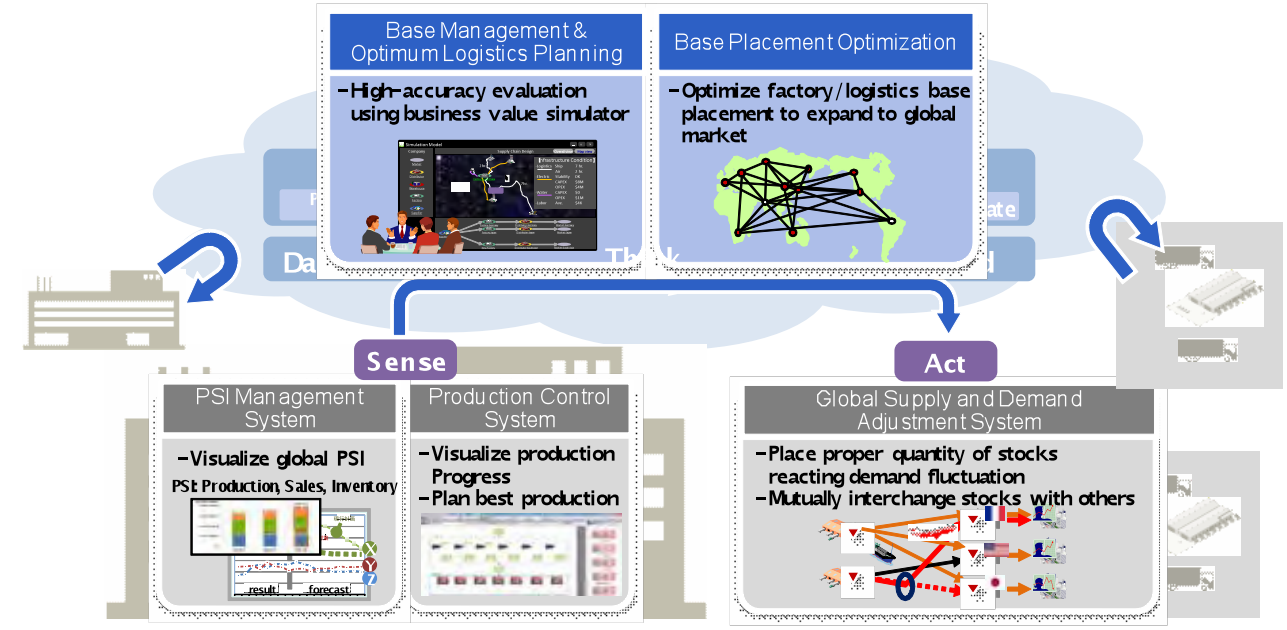


Figure C-1 | Diagram of use case – Collaborative supply chain management

1.5 Use case conditions

1.5.1 Assumptions

Involve different parties.

1.5.2 Prerequisites

Refer to 2.3, 2.4 and 2.5.

1.6 Further information for the use case

1.6.1 State of the art

- Status quo
  - Realizes collaboration between systems of a single enterprise.
  - Realizes collaboration between systems of a major enterprise and its dependent enterprises.
- State of the art
  - Realizes collaboration between systems of different enterprises, between which there have never been any previous relations.
- To switch status quo to state of the art, technologies/standards to integrate data of different enterprises and to connect with systems of different enterprises are needed.

1.6.2 Relation to other use cases (including sub- and super-use cases)

The BCM (business continuity management) use case is related to this use case. An IoT platform of the BCM use case senses, thinks and acts in a way similar to this use case.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol		Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards		Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization		
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/resilience
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness	X	

2.3 Memory

Capability		Remark
Digital product memory	X	Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy		
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors		

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements		
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence	X	
Swarm control of security	X	
Context-aware control	X	

User I/O

Capability		Remark
Tactile interfaces	X	
Multi-device user-interfaces	X	
Virtual modelling	X	
Simulation	X	
Accessibility	X	For disabled people
Augmented reality		E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems,…
Securing ID of devices		
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology	Remark
Connectivity	Transport layer protocol for next-generation satellite connections	Higher bandwidth, high latency
	5th generation cellular access (5G)	
	Low power wireless access (LPWAN)	

	Next-generation enabling technology		Remark
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology		
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet		
Security	Identity of things		
	Homomorphic encryption		
	Searchable encryption		
	Trust establishment		
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements	Remark
Connectivity	Realization of the 5G standard	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device	
	Standards for IoT equipment to have the capability to update to new connectivity standards	

	Standards requirements		Remark
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces	X	
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex D – Use case

Predictive maintenance and service

1 Description of the use case

1.1 Name of use case

Predictive maintenance and service: condition based maintenance and scheduling

1.2 Scope and objectives of use case

1.2.1 Scope

Predictive maintenance and service provides holistic management of asset health and decision support for the optimization of maintenance schedules and resource usage (e.g. spare parts). This optimization is based on health scores, anomaly detection, spectral analysis and machine learning. It runs on an extendable, high-performing data processing IoT platform that can process huge amounts of fused IT and OT data. It makes available sophisticated data science methods in combination with data from many diverse asset control and automation systems to find and mitigate previously hidden patterns of asset failures.

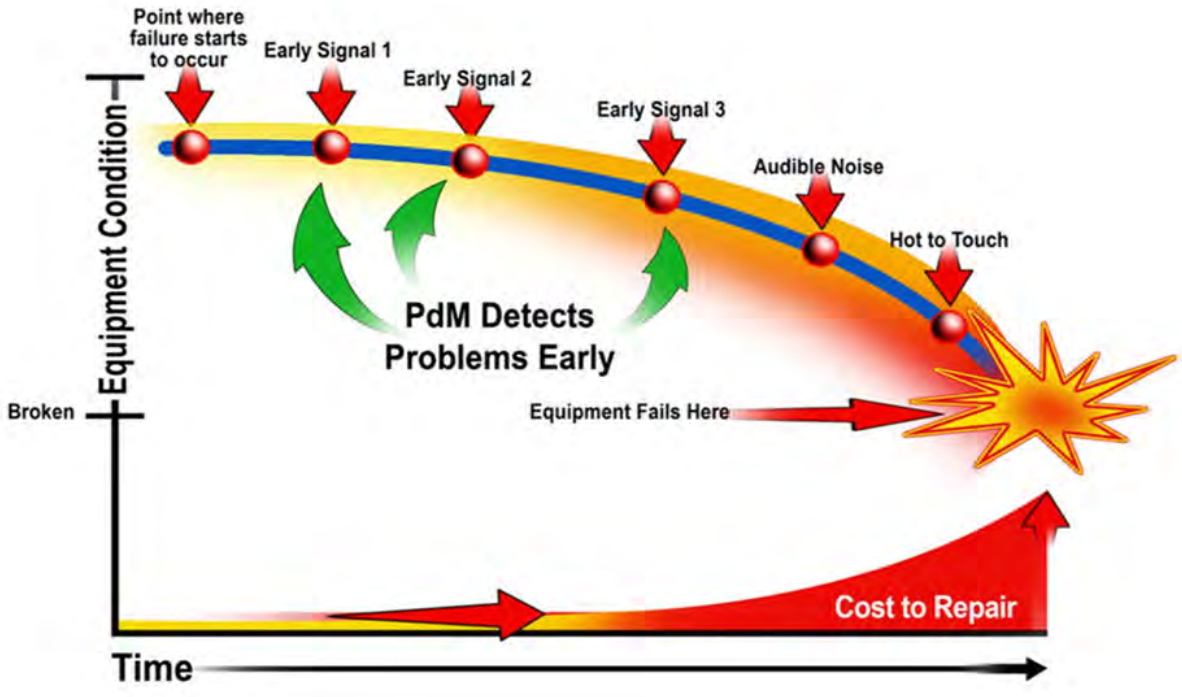


Figure D-1 | Predictive maintenance and service timeline [56]

As seen in Figure D.1, with the help of predictive maintenance and service the asset or machine in consideration can be constantly monitored and analyzed. This will help to identify future machine failures in advance and allow machine operators to take the respective actions before the machine actually breaks. This in turn will reduce unplanned downtime, improve maintenance efficiency and reduce the cost of operations.

Scope of the use case discussed in this clause is

- Data fusion of business data (IT) together with operational data generated by OT.
- Data science capabilities of an IoT platform.
- Transformation of analytical findings into meaningful actions.

1.2.2 Objectives

The main objective of predictive maintenance and service is to enable a data-driven approach to improve the quality and time lines of maintenance and service, which helps the transformation of businesses from being preventive maintenance providers into competitive differentiators, by providing innovative customer services and maintenance capabilities.

1.3 Narrative of use case

1.3.1 Summary of use case

The use case mainly highlights the capabilities of an IoT platform that can be used to face the current challenges in data fusion (one single source of truth out of the various data sources), data analytics and transformation of findings into meaningful actions. In this use case we discuss condition-based maintenance and scheduling performed by a railway operator and how predictive maintenance and service is helping it to proactively address service needs, thus improving maintenance efficiency and reducing costs of operations.

1.3.2 Nature of the use case: maintenance optimization

An important goal for the operator of an asset is the reduction of its operating costs, to which maintenance contributes a significant part. Maintenance optimization helps to ensure that the maintenance operations are as effective as possible by being able to achieve the highest availability with the least amount of budget and resources. Predictive maintenance and service can support these goals by data-driven analysis, planning and prioritization.

1.3.3 Complete description

1.3.3.1 Challenges: combining multiple data sources reduces “huge data” to “barely enough data”

One of the key capabilities and the major backbone of IoT platforms are the data fusion capabilities used to bring data from various sources together and merge it into a single source of truth. However, according to Gartner, through 2020, 80% of all IoT projects will fail at the implementation stage due to improper methods of data collection [4].

Operational data is usually captured for a specific use case, for example quality assurance, component traceability, process control etc.; it is not meant to be integrated with other operational data. Data integration (IT/OT integration) and data quality for very large data sets are a major challenge and a big cost factor for the setup of powerful IoT platforms.

If data resides in multiple sources, which is usually the case, the data needs to be analyzed in combination to create valuable insights. This includes business information such as vendor details, component master data etc. as well as operational data arising from multiple sensors, which is used for different purposes. Just combining or fusing this data will often lead to erroneous results, and as a result data will be of

no use and of lower quality. To overcome this, rethinking of data management is important. An IoT platform supporting super large-scale of data by in-memory data processing, distributed computation and human-centred data mining will be the preferred solution for overcoming performance constraints, while innovative approaches are also needed for data integration, harmonization and management.

1.3.3.2 Challenges: big data and data analytics

During projects and commercial implementations, several trends are consistently observed:

- Humans alone or even today's mid-size machines cannot process the enormous amounts of data generated by machines and sensors. This fact has been evident in all projects conducted to date, with the largest data set containing half a petabyte of machine-generated data. Without the support of high-performance computing, it is impossible for a human to process the data.
- To date, computer algorithms cannot accurately and reliably predict arbitrary machine or component failures. At the time of writing, no generic reliable and robust methods to predict faults in individual machines or groups of machines have been found that work across domains. At the same time, it is imperative that we effectively use algorithms to provide meaningful information to the human user because humans cannot process the vast volumes of data generated by machines.
- Furthermore, due to low quality and errors in the data, 50% to 60% of the machine data in the data lake is not usable for machine learning.
- There is no single cross-industry standard data model for IT/OT integration. Furthermore, customers want to view and analyze their data in their specific format.

1.3.3.3 To address the current and future needs of IoT a new approach is needed

The conceptual model to be used in the new approach should be one of adductive reasoning (tentative hypothesis → theory) and deductive reasoning (theory → hypothesis → observation → confirmation) where data science, which can supply input to this process, can be seen as inductive reasoning (observation → pattern → tentative hypothesis → theory). This interactive and, in most cases, iterative process, as shown in Figure D-2, highlights the collaboration required between domain experts and data science (observation to theory to observation).

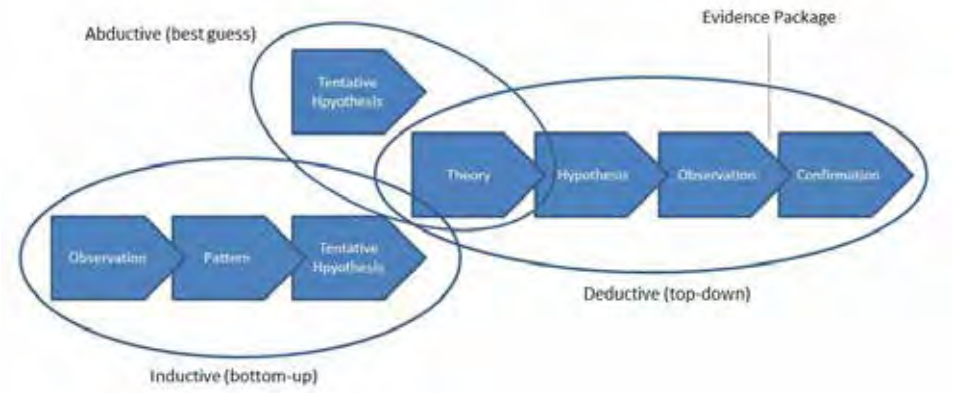


Figure D-2 | Conceptual model for new approach

The IoT platform should be ready to support a super-large-scale data set with in-memory data processing, distributed computations and cost-efficient storage. Applying advanced data science capabilities and predictive scenarios will leverage the overall process efficiency for the organization. Data management should be prepared to retrieve the data “as-is” and to defer processing of it as long as possible. Data is cleaned only when being processed, and data should be integrated into a format specific to the business problem which needs to be addressed.

The target users of a cross industry IoT platform are mainly the business users and domain experts specialized in fields such as mechanical engineering, chemical engineering or other engineering- and manufacturing-based activities. It will be the role of these individuals to manage complex processes in a company’s core business, or lines of business, such as maintenance, after sales service, quality, warranty, yield, energy efficiency, product improvement and process improvement. Another important design concept for IoT platforms is that the domain experts can be given fragments of information from data scientists or other sources of pre-processing, such as the calculation of complex key figures, which can assist in the discovery process, see Figure D-3.

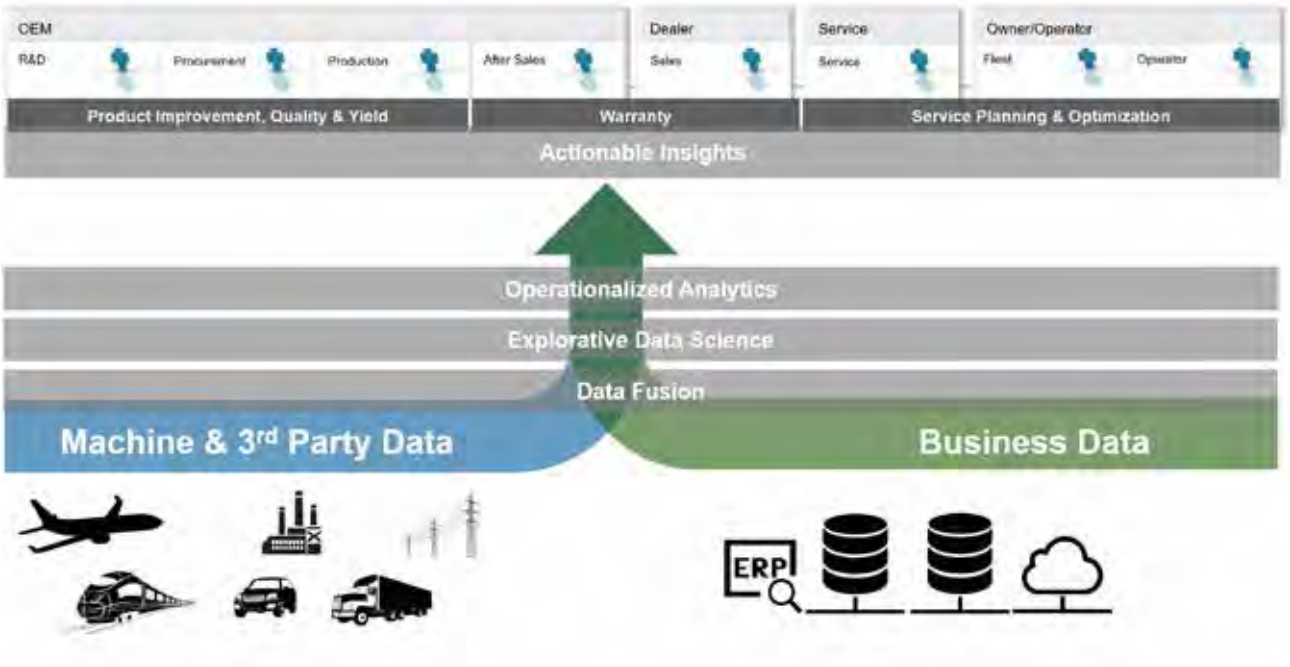


Figure D-3 | Cross industry IoT platform

1.3.3.4 Use case: maintenance optimization for railway operators

Predictive maintenance techniques provide holistic management of asset health and decision support for the optimization of maintenance schedules and resource usage (e.g. spare parts); this optimization is based on health scores, anomaly detection, spectral analysis and machine learning.

The use case discussed below provides a brief overview of how a railway operator makes use of predictive maintenance and service solutions to manage the maintenance of a fleet or a component at the locomotive level. This example analyzes a fleet of batteries used in the locomotives or specific batteries used at the machine level, such as in train lighting, engine starting, signalling, telecommunication or in multiple electronic units etc. A battery is a crucial asset in locomotives that can lead to unexpected downtimes. Early identification of malfunctioning batteries has a significant impact in reducing the downtime.

1.3.3.5 Situation today

There are over 50 000 components per locomotive, which require periodic maintenance. Currently maintenance activities for components are planned based on scheduling provided by the supplier of the rolling materials. These schedules are calculated by mileage or time, and are aimed at addressing actual or foreseen failures of specific components (corrective maintenance); no data mining is applied.

1.3.3.6 Objectives

- Establish a robust, scalable, open platform for the improvement and evolution of technology-assisted maintenance operations.
- Extend the rule-based approach with more sophisticated algorithms able to detect additional patterns and anomalies.
- Drive a new, more flexible and effective approach for maintenance scheduling, based on the specific patterns of each component.

1.3.3.7 Distance-based bad actor analysis

To perform the distance-based bad actor analysis, the equipment's sensor data needs to be extracted out of the time series storage. The extracted data then needs to be parsed, enriched and transformed for the definition of a learning model. This can be done by computing the mileage each component (e.g. battery) has already covered to a reference component, using the earthmover's distance algorithm and storing distances in time series storage. Battery lifetimes that exceed a certain threshold can be considered as being in bad condition. An alert is generated and a service notification is created in the business system for maintenance and service, see Figure D-4.

Figure D-4 | Example of extracted data for distance-based bad actor analysis

The above predictive maintenance approach will help the operator to perform all – and only – the required maintenance measures at the right time, ensuring availability of the right resources and thus reducing the costs of operations and of unplanned down time.

1.3.3.8 Future look up of the IoT platform

IoT platforms should support the real time data fusion by instantiating the data collection regardless of time, source, network and formats. Platforms should be able to integrate semantics and languages of adjacent platforms and systems. This will actualize the concept of platform of platforms by enabling the transmission of data between multiple platforms.

Platforms should also provide support for onboard analytics, self-healing and self-learning based on experiences. This will enable better handling of anomalies and prevent them from occurring repeatedly.

Platforms should have advanced machine learning capabilities, inbuilt ready-to-use applications, intuitive visualization and design concepts together with seamless transmission of data from anywhere, to perform the real time data collection, processing and data transformation needed to provide real time business insights.

Remote monitoring and remote action control capabilities of the platform focusing on safety and security enable better device lifecycle management in situations in which human beings have no or only limited access (e.g. oil rigs). The concept of device life cycle management is not only limited to the areas mentioned above but also covers the broad area of installation and configuration of new assets, their maintenance and the decommissioning of the assets after they reach the end of their operating life.

1.3.3.9 Technical requirements for the future IoT platform

Cutting-edge IoT platforms should support device connectivity and extensibility by connecting to multiple platforms that share information between themselves and easy data transmissions.

Furthermore, an IoT platform is required to have advanced capabilities, such as rules engines and modal managers. Rules engines define and set standards for learning processes from past data explorations, while a modal manager is responsible for embedding recognized or learned patterns into the analytical libraries. Artificial intelligence and machine learning algorithms can then leverage the learned patterns to derive their respective models.

Interoperability of platforms involving integrated security and remote management in edge networks enables IoT solutions to exploit processing capabilities on the edge network. This also provides an ecosystem in which IoT sensor networks can connect to one another for data transmissions and provide real-time context for insights into action on the edge networks. Acting on real-time insights on the edge will avoid the need for round-trip latency.

IoT platforms should also provide high performance messaging systems for real-time transactional data, ensuring data integrity over unstable networks. Advanced platform capabilities should also enable seamless building and deployment of analytical applications and micro services. At the same time, good user experience requires platforms to provide advanced interfaces such as virtual modelling and augmented reality.

The future and success of the platform of platforms rely on the standards set today for IoT platforms and device connectivity concepts in the edge networks.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol	X	Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards	X	Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization		
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/ resilience
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability		Remark
Digital product memory	X	Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities		
Privacy		
Integrity of data	X	
Complex sensors that require authentication		
Ability to reconfigure sensors	X	

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements	X	
Authentication and access control and authorization	X	
Floor control		Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control		

User I/O

Capability		Remark
Tactile interfaces		
Multi-device user-interfaces	X	
Virtual modelling	X	
Simulation	X	
Accessibility		For disabled people
Augmented reality	X	E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)	X	
	Low power wireless access (LPWAN)		

	Next-generation enabling technology		Remark
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization	X	
Memory	Digital product memory	X	
Sensing	Ultra-precise location technology		
Actions	Augmented reality	X	
	Virtual reality		
	Tactile Internet		
Security	Identity of things	X	
	Homomorphic encryption	X	
	Searchable encryption		
	Trust establishment	X	
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard	X	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards	X	

	Standards requirements		Remark
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces		
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems		
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections		Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework		Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems		

Annex E – Use case

A Smart City with a smart and secure IoT platform

1 Description of the use case

1.1 Name of use case

A Smart City with a smart and secure IoT platform

1.2 Scope and objectives of use case

1.2.1 Scope

The scope of Smart Cities integrates diverse ICT technologies from sensing, processing, actuating, communications and security perspectives to enhance the resource management, information transparency and efficiency of actuation in a smart and secure way.

1.2.2 Objectives

The European Smart Cities Project [57] has been considering different service sectors such as smart governance, smart mobility, smart utilities, smart buildings and smart environment to assess the level of smartness of European cities. Cross-domain technique integration and information mashups will be essential requirements in the next-generation IoT platforms with advanced smartness and security technologies. Therefore, considered here is a Smart City with various types of services, including public safety, city performance, city mobility, mobile operation centres and smart utility usage to provide concrete use cases of smart and secure IoT platforms in the next generation.

1.3 Narrative of use case

Public domain.

1.3.1 Summary of use case

In the Smart City use case, multiple types of sensors and data sources such as temperature, humidity, noise, gas, and motion sensors, cameras, mobile devices, network sniffers, smart meters, and water meters are deployed for sensing the dynamics of a city. The multi-modal sensing information is transformed into cross-domain and real-time information mashups using semantic interoperability. Furthermore, these information mashups will be easily accessible for a variety of advanced data mining and machine learning techniques, to provide applications for residents and multiple agencies so that intelligent actions can be performed. This Smart City use case reviews various representative applications in a city, including public safety, city performance, city mobility, mobile operation centres and smart utility usage. Moreover, it discusses how the advanced capabilities of next-generation IoT platforms in sensing, processing, memory, connectivity and actuating can create smarter and more secure living environments in urban areas.

1.3.2 Nature of the use case

1.3.3 Complete description

A Smart City with smart and secure IoT platforms enables many promising IoT services as shown in Figure E-1. First, for enhancing public safety, emergency response technologies estimate evacuee density and required resources from agencies for further search and rescue. Second, for building a smart environment, data on traffic, air quality, noise levels, crowd levels, etc. is provided for city performance look-up.

Third, for enabling smart mobility, crowd detection technology captures human mobility and analyzes human mobility behaviour in the city for enhancing public transport services and avoiding overcrowded travelling experiences. Fourth, for enabling smart utility usage and construction of smart buildings, smart metering systems record water/electricity usage and report to the utility agency automatically; at the same time, several recommendations for energy savings are provided. Fifth, for enabling smart government to enhance city safety, image processing and recognition technology expedite criminal investigations and help solve more crimes, for instance by identifying criminals or stolen cars. Finally, for reacting to dynamic needs in a Smart City, a mobile operation centre can dynamically exchange real-time sensor data streams between different agencies through a secure authentication process which controls data ownership among multiple agencies and users. All of the above Smart City services rely significantly on different levels of mashups on sensing data from connected objects, devices, clouds, and agencies which will be conveyed to residents and multiple agencies to enable smart services (including actuation).

A Smart City story: A concrete story in a Smart City is given to explain how these smart services cooperate with each other in a smart and secure way. A concrete example scenario is considered for critical situation detection and response as follows. When an emergency occurs in the city (e.g. a terrible explosion in a big event due to a chemical accident, or a terrorist attack), crowd detection, city mobility, and city performance look-up techniques will provide transparent information of crowd levels, people flows, usage of public transport, and traffic status for evacuating event participants. Meanwhile, dynamic mobile operation centres are set up to support on-site rescue operations. Those mobile operation centres cooperate with multiple agencies to manage and dispatch resources (e.g. ambulances, autonomous vehicles, fire engines, and police cars). In addition, search and rescue robots and autonomous vehicles are dispatched to save victims. To avoid cyber attacks during the emergency response, mobile operation centres control the access of data and data ownership. In the case of terrorist attacks, the city surveillance detects the suspicious persons and performs face recognition to facilitate inter-agency cooperation between police and emergency response agencies. Face recognition can also be used to find lost children and relatives. As it can be seen, advance technologies enable information mashups to enhance the smartness, safety, and security of the city. In the next-generation platform, to enable information mashups, the linkage between objects, devices, edge nodes, actuators, agencies and services will be many-to-many instead of existing many-to-one or one-to-one linkages. A single data source will not only provide information for a single enterprise cloud but also for multiple connected clouds.

1.4 Diagrams of use case

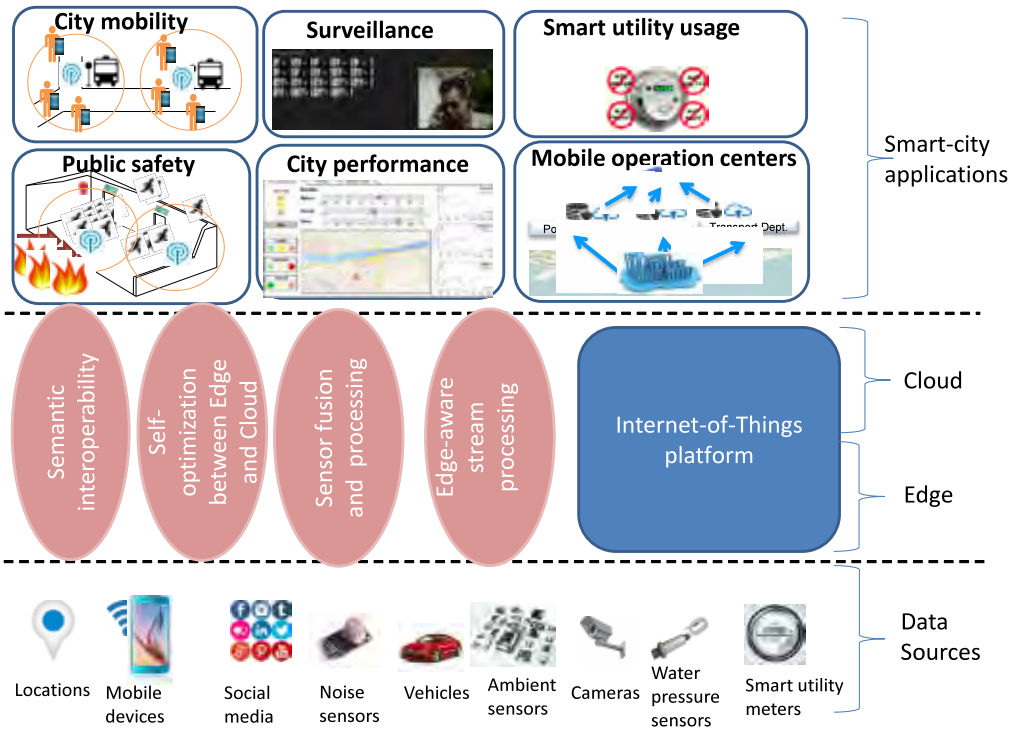


Figure E-1 | A Smart City with a smart and secure IoT platform

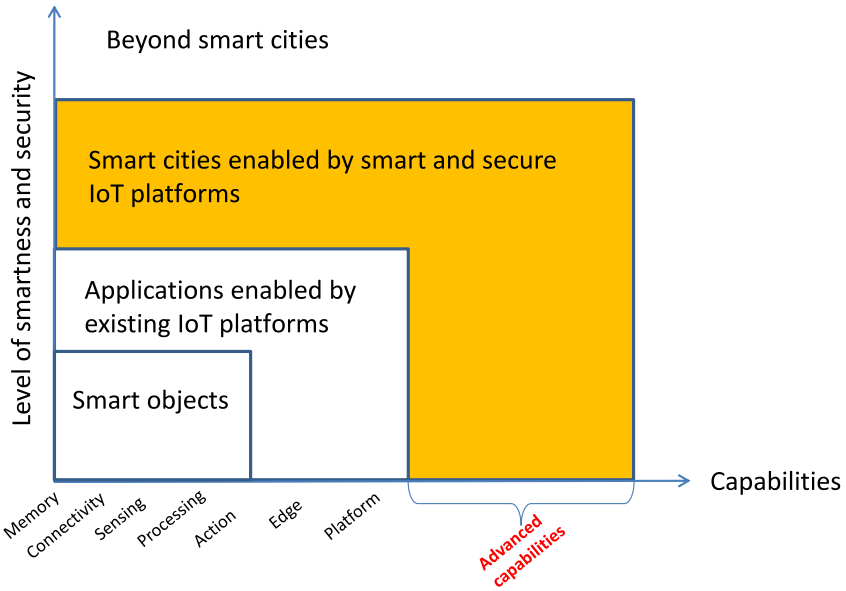


Figure E-2 | The vision of a Smart City with a smart and secure IoT platform

1.5 Use case conditions

1.5.1 Assumptions

Assume that smart objects are deployed in the future city. Those smart objects have basic capabilities of memory, connectivity, sensing, processing and action, as shown in Figure E-2. With the basic capabilities, ambient information, mobility, energy or water usage, video streams, traffic information, etc. in the city can be perceived. Meanwhile, each smart object can be connected to multiple smart objects and multiple entities, e.g. applications and service platforms for enabling a Smart City.

1.5.2 Prerequisites

The existing IoT platforms collaborate with the edge for collecting data from different sources. The evolution of the IoT platforms in the next generation will be supported by many different advanced capabilities including (1) semantic interoperability, (2) self-optimization between edge and cloud, (3) sensor fusion and processing, and (4) edge-aware stream processing.

1.6 Further information for the use case

1.6.1 State of the art

Sensor fusion and processing: The sensor fusion and processing techniques represent the process of combining observations from multiple sensors to provide robust and complete descriptions of the knowledge of interest. The typical sensor fusion techniques are based on probabilistic modelling (e.g. particle filter or Kalman filter) [58], which incorporates multiple types of sensor data streaming into a single model, and have been commonly considered in the areas of robotics control, localization and environmental monitoring. As for analyzing human mobility, image-based techniques use human shape detected in image frames to count numbers of people [59], and sensor-based approaches extract features from multi-modal sensors' data to construct data mining models for determining the level of occupancy in indoor places [60].

IoT standards: The targeted vision is to support semantic interoperability in the IoT and Smart City platforms. To achieve this vision, the information streams coming from M2M systems (probably based on the oneM2M standard) can be automatically mapped into next-generation service interface (NGSI)-based contextualized information models that are defined and used as a standard in FIWARE. The transformation process can be handled by Semantic Mediation Gateways (SMGs) to map different information models into a common model using semantic information as well as libraries of transformation routines. The transformed metadata can also be used for faster discovery of available resources, automatic information mashups, and improved big data analytics functions.

2 Mapping to characteristic capabilities

Semantic interoperability: Interoperability is "the ability of two or more systems or components to exchange data and use information" [61]. Semantic interoperability is achieved when interacting systems attribute the same meaning to an exchanged piece of data, ensuring consistency of the data across systems regardless of individual data format. The semantics can be explicitly defined using a shared vocabulary as specified in an ontology. Semantic interoperability can be applied to all parts of an IoT system, i.e. on IoT platforms in the cloud, but also reaching to edge components and IoT devices.

Self-optimization between edge and cloud: Smart City applications typically rely on various data processing tasks at different levels to extract real-time insights from geo-distributed IoT data sources. In a cloud-edge-based environment,

those tasks can be dynamically allocated to either clouds or edges, in order to meet certain optimization objectives, such as reducing the bandwidth consumption between edges and cloud, or minimizing the latency to extract analytics results from raw sensor data. The optimization of task deployment across edges and cloud can be done by the IoT platform before the deployment at the design time based on the specification given by application developers, and/or after the deployment at the run-time based on the real-time system information measured from the system platform itself. For example, in a video surveillance system we might need four processing tasks to detect suspects from camera videos: video stream reader, image extraction, face extraction, face recognition. To save bandwidth consumption, the first three types of tasks can be assigned to edges and then only the detected faces need to be sent to clouds for face recognition. However, during the runtime, some of them might be migrated from edges back to cloud if the associated edge node is overloaded.

Sensor fusion and processing: Advanced sensor fusion and processing techniques must be able to deal with real-time streaming and perform more-than-real-time prediction without too much prior training overhead. For example, a lightweight device can perform on-board learning within a small piece of observed data and provide insights to a Smart City application for further actions. Meanwhile, lightweight prediction models are preferred in the next-generation IoT platform to enable Smart City applications efficiently.

Edge-aware stream processing: Edge-aware stream processing involves software solutions that run on parallel networked systems in order to facilitate and manage the execution of applications (or “processing topologies”). The systems on which edge-aware stream processing runs are traditionally server clusters, but they can be any set of networked devices, i.e., the devices that comprize the cluster might be heterogeneous and physically distributed. The traditional scenario of server clusters stems from the fact that most big data streams were coming from web analytics applications, while the latter scenario of running edge-aware stream processing on heterogeneous and geo-distributed nodes is now motivated by the huge streams that can be produced and analyzed in IoT. An important challenge for edge-aware stream processing is the optimization of the deployment of the so-called processing topologies. Existing solutions have tried to optimize deployment based on the data traffic between the tasks of the topology and/or based on status information about the hosting servers and their network connections. However, in many IoT scenarios, critical low-latency requirements appear at the edge of the processing topology, i.e., between a processing step and external IT or IoT entities such as actuators or databases. Thus, “edge-awareness” processing techniques target some quality-of-service requirements during deployment optimization.

Standard-compliant IoT platforms: Standard-compliant IoT platforms will enable easy development of smart applications through hiding complexity of IoT installations from the applications. Thus, standard-compliant middleware components can be designed to provide applications a single point of contact and separate them from the underlying device installations. Meanwhile, they can actively communicate with large quantities of IoT devices and gateways and obtain information for the running IoT applications. Some technical standards for the efficient data model (e.g. NGSI) can facilitate the implementation of the standard-compliant middleware component.

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol	X	Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards		Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities	X	
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self-healing/ resilience
Dynamic configurability	X	Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness	X	

2.3 Memory

Capability		Remark
Digital product memory		Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy	X	
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors	X	

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements	X	
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence	X	
Swarm control of security	X	
Context-aware control	X	

User I/O

Capability		Remark
Tactile interfaces		
Multi-device user-interfaces	X	
Virtual modelling	X	
Simulation	X	
Accessibility	X	For disabled people
Augmented Reality	X	E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections	X	Higher bandwidth, high latency
	5th generation cellular access (5G)	X	
	Low power wireless access (LPWAN)	X	
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization	X	
Memory	Digital product memory	X	
Sensing	Ultra-precise location technology	X	

	Next-generation enabling technology		Remark
Actions	Augmented reality	X	
	Virtual reality	X	
	Tactile Internet	X	
Security	Identity of things	X	
	Homomorphic encryption	X	
	Searchable encryption	X	
	Trust establishment	X	
	Secure systems collaboration technologies	X	
	Privacy through usage control	X	
	Continuous security audits	X	
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard	X	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device	X	
	Standards for IoT equipment to have the capability to update to new connectivity standards	X	
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces	X	
	Contextualized information models	X	
	Metadata context standards	X	
Memory	Standardization of digital product memory	X	

	Standards requirements		Remark
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies	X	
	Sensor data privacy standard	X	Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices	X	
	General standard to normalize IoT user I/O across systems	X	
	Standard for unique IoT accessibility requirements	X	Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex F – Use case

Social sensors

1 Description of the use case

1.1 Name of use case

Social sensors

1.2 Scope and objectives of use case

1.2.1 Scope

This use case deals with data collection, data aggregation and providing data to users. This use case does not deal with analytics.

1.2.2 Objectives

To illustrate the requirements about trust, privacy, data ownership and interoperability.

1.3 Narrative of use case

1.3.1 Summary of use case

A social sensors service is intended to collect the wealth of user-generated data, which can then be anonymized and compiled to show benefits for an entire community weighed against individual behaviour. This use case is derived from the IoT scenario presented in [62].

1.3.2 Nature of the use case

Government focus.

1.3.3 Complete description

Increasingly, people have the possibility of monitoring important parameters in their homes or in the surrounding environment. An example of this is provided by the web site bwired.nl, where each user can have a number of sensors monitoring and measuring parameters related to the functioning of the home or surrounding areas (e.g. the local outside temperature, the humidity, or even various parameters related to pollution, noise and others elements).

A social sensors service is intended to collect the wealth of user-generated data, which can then be anonymized and compiled to show benefits for an entire community weighed against individual behaviour. For example, it is possible to calculate a medium or average value for some parameters and allow each citizen to compare his own set of parameters with the “average set of values”. In this way, individuals can gauge where they stand in respect to a set description of “virtuous citizen behaviour”, such as establishing a proper power consumption footprint. In fact, the availability of this type of data analysis could incentivize good-natured competition, and even encourage people to increase existing, or pursue new, practices perceived to be beneficial to the community as a whole. Another possible usage is related to integrating user-generated data in such a way as to compare data and parameters collected directly by citizens versus official data provided by public administrations. One important case could involve controlling local pollution vs. the official data monitored in a particular area of large cities. The social service can be applied to environmental monitoring, e-government and intelligent homes.

The “social sensors” service aims to aggregate measures and information collected by sensors in a specific environment (e.g. a home) and to share them in a larger context (e.g. a neighbourhood).

Data, measurements and information can be used for deriving knowledge (e.g. pattern analysis) related to how an environment is operating. An important feature is for users and owners of sensor networks to agree to share data in a larger community. The service is characterized by the need and possibility to access and use data stemming from sensors in different administrative domains (e.g. homes, companies, public administration and government, social networks). This service sets an example of how extensive independent sensor networks can cooperate in order to serve larger communities.

There are three actors in this use case.

1. The sensors provider is the actor that actually owns and manages a home or office sensor network which monitors many aspects of daily life or business. This includes things ranging from water and electricity consumption to the frequency of people knocking at the door to deliver advertising, to many other activities centred on the "home". Data represents the behaviour of the people living in a house, and storing and analysis of the data can give a very valuable description of how the social life of a family or business operation evolves over time. Data can be pushed to the aggregator by the sensor provider or it can be pulled directly by the aggregator.
2. The aggregator is the actor that actually collects and properly deals with a wealth of data. Its task is to try to govern the differences between the data representation and organize data in a meaningful manner after it has been anonymized. The aggregator could also be a provider of a distributed sensor network, or the owner of other data collecting networks, such as utilities, network operators, or public administration/ government agencies.
3. The user ultimately takes advantage of all the information. The user could also be a company or programmer that is using the sourced data in order to determine the social behaviour of citizens, or a very specific subset of individuals. (e.g. the inhabitants of a specific neighbourhood).

The service is conceptually simple (see Figure F-1): a sensor provider is a producer of information that is collected and anonymized by an aggregator in order to harmonize the diversity of the data format and information. Data collected from different sensor providers is aggregated and different views and/or inferred information can then be offered to a user. Data sets are also normalized in order to make them usable (i.e., different data formats can be generated and produced). The user can access the data or can utilize it as a benchmark for behaviour. The aggregator could also integrate its own sensors infrastructure in order to create a wider set of data. Applications range from very simple ones, such as using citizens' thermometer readings to determine the average city temperature, to very complex ones, such as using motion sensors or mobile operators' data to track a mob moving through a city.

While a social sensor service is conceptually simple, complexity is due to three factors. Firstly, there is a need to normalize heterogeneous sources (i.e., different sensors with different capabilities and different data representations and formats). Secondly, there is a need to anonymize data pertaining to the individual domain (i.e., data that allows a user to map a value of data to a specific user). Thirdly, there is a need to integrate data from and in different contexts and domains to address issues related to communication, interworking and data reliability.

1.4 Diagrams of use case

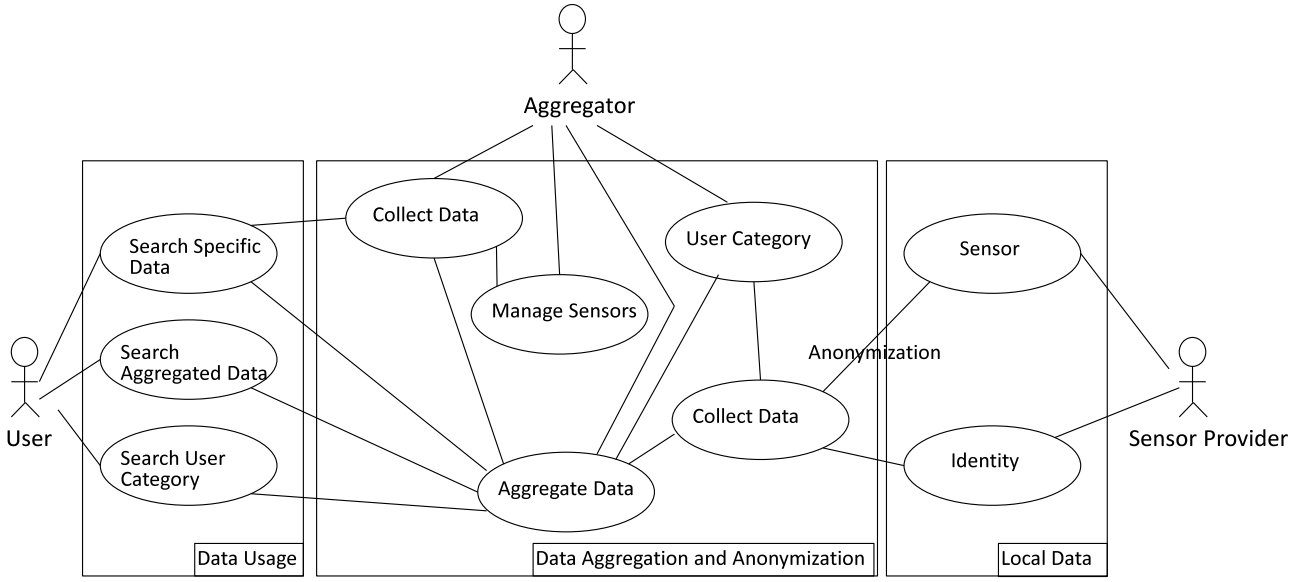


Figure F-1 | Actors and use cases of social sensor service

1.5 Use case conditions

1.5.1 Assumptions

Sensor providers are willing to provide their data honestly to data aggregator.

1.5.2 Prerequisites

- Data generated by different sensor providers can be integrated.
- Appropriate anonymization can be done to the collected data.
- Capability for sensor providers to track and control the usage of data provided by themselves may need to be provided.

1.6 Further information for the use case

1.6.1 State of the art

Communication technology to collect data from stationary sensors in homes and offices are available at present. But those communication technology may not be sufficient to collect data from other sensors such as sensors installed in a drone flying around a house or an office.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling		Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality		Functionality resides outside of the product
Adaptability to any bandwidth/protocol		Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards		Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices		Dynamic composition of devices for self healing/ resilience
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability	Remark
Digital product memory	Whole lifecycle; product pedigree
Pattern recognition	Based on artificial intelligence/machine learning
Performance data	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities		
Privacy	X	
Integrity of data	X	
Complex sensors that require authentication		
Ability to reconfigure sensors		

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices		Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context		
Safety requirements		
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control		

User I/O

Capability	Remark
Tactile interfaces	
Multi-device user-interfaces	
Virtual modelling	
Simulation	
Accessibility	For disabled people
Augmented reality	E.g. glasses
Usability and user experience	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security		Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience		Including cyber-physical attacks
Fault tolerance		Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats		
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection		

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)		
	Low power wireless access (LPWAN)	X	

	Next-generation enabling technology		Remark
Processing	System configuration and dynamic composition		
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology		
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet		
Security	Identity of things	X	
	Homomorphic encryption	X	
	Searchable encryption	X	
	Trust establishment	X	
	Secure systems collaboration technologies	X	
	Privacy through usage control	X	
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies		

4 Necessary future standards

	Standards requirements	Remark
Connectivity	Realization of the 5G standard	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device	
	Standards for IoT equipment to have the capability to update to new connectivity standards	

	Standards requirements		Remark
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces		
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard		Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex G – Use case

Improvement of journey experience in public transport for passengers including those with special needs

1 Description of the use case

1.1 Name of use case

Improvement of journey experience in public transport for passengers including those with special needs

1.2 Scope and objectives of use case

1.2.1 Scope

This use case deals with adaptability of an IoT system.

1.2.2 Objectives

To illustrate the requirements concerning analytics, machine learning and privacy.

1.3 Narrative of use case

1.3.1 Summary of use case

The IoT system helps passengers, including those with special needs, to select a route to a destination based on their needs and preferences and checks if the passengers are travelling as planned. It can also adjust the operation of public transportation such as bus and train so that the needs of passengers can be better served. This use case is an extension of the IoT scenario presented in [63].

1.3.2 Nature of the use case

Consumer focus.

1.3.3 Complete description

This use case deals with an IoT system which evolves and acts in a more autonomous way, becoming more reliable and smarter.

The IoT system helps with the handling of passengers, including those with special needs. A passenger inputs the start point, the destination, date and time of travel into the system. The system finds a route based on the information provided by the passenger, passenger's needs and preferences. The system also selects checkpoints which are used to check if the passenger is travelling as planned. If it is found that the travel is not proceeding as planned, an alarm is generated by the IoT system. To conduct checks at the checkpoints, data on average travelling time are gathered by analyzing actual user data and data obtained from stakeholders related to transportation services such as bus operators, railway operators and police. The data used by the IoT system includes schedule, location and method of transportation of passengers, which are privacy-related data. The IoT system can cooperate with public transportation systems so that the needs of passengers can be better served by such systems. For example, a bus operator can reroute a wheel chair-accessible bus to provide transportation service to a passenger in a wheel chair by cooperating with the IoT system.

The IoT system will be able to learn based on operational experiences, while situational knowledge acquisition and analysis will make the system aware of conditions and events potentially affecting its behaviour. Adaptive selection approaches will manage the uncertainty and volatility introduced due to real-world dynamics.

Management decisions and runtime adaptability will be based on security, trust, administrative aspects, location, relationships, information, and contextual properties of things comprizing the IoT system.

1.4 Diagrams of use case

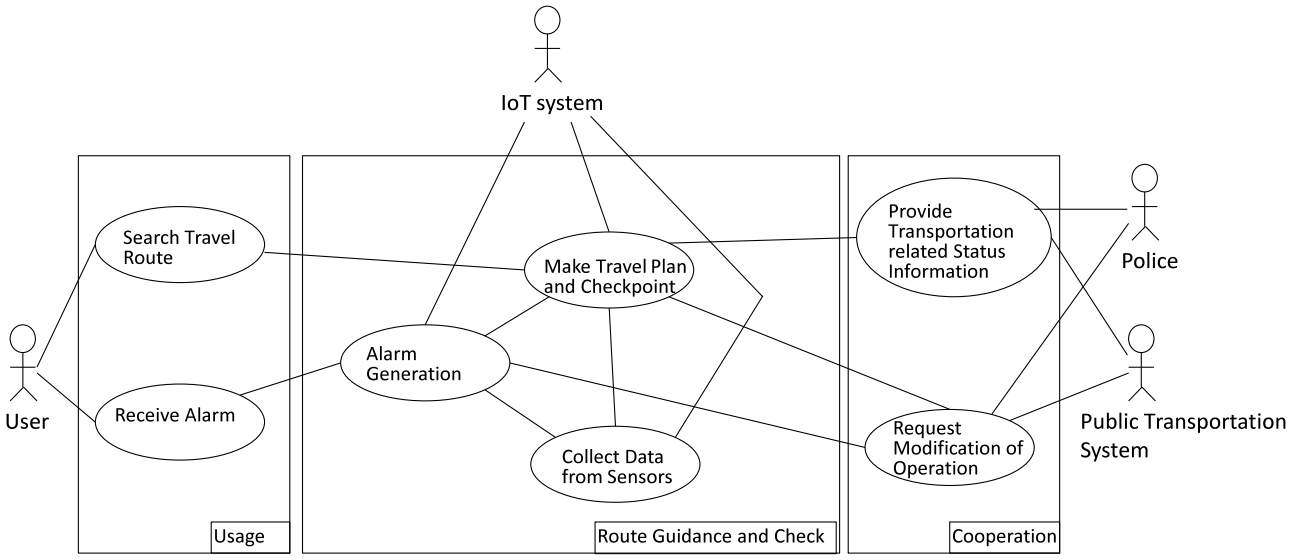


Figure G-1 | Actors and use cases of improvement of journey experience

1.5 Use case conditions

1.5.1 Assumptions

Appropriate equipment such as sensors are already deployed to detect a passenger's passing at each checkpoint. Smartphone of the passenger may suffice.

1.5.2 Prerequisites

Privacy of the passengers needs to be protected.

1.6 Further information for the use case

1.6.1 State of the art

Route navigation systems for a passenger based on a passenger's preference (e.g. lower cost, shorter travel time) already exist. We are not sure if average travelling time data is maintained by data analytics in the present route navigation systems.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity		Connection to more than one system
Remote functionality		Functionality resides outside of the product
Adaptability to any bandwidth/protocol		Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards		Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices		Dynamic composition of devices for self healing/ resilience
Dynamic configurability		Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability	Remark
Digital product memory	Whole lifecycle; product pedigree
Pattern recognition	Based on artificial intelligence/machine learning
Performance data	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy	X	
Integrity of data	X	
Complex sensors that require authentication		
Ability to reconfigure sensors		

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices		Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements	X	
Authentication and access control and authorization	X	
Floor control		Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control	X	

User I/O

Capability		Remark
Tactile interfaces		
Multi-device user-interfaces	X	
Virtual modelling		
Simulation	X	
Accessibility	X	For disabled people
Augmented reality		E.g. glasses
Usability and user experience		

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security		Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience		Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection		

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)		
	Low power wireless access (LPWAN)		
Processing	System configuration and dynamic composition		
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology		
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology	X	

	Next-generation enabling technology		Remark
Actions	Augmented reality	X	
	Virtual reality		
	Tactile Internet		
Security	Identity of things	X	
	Homomorphic encryption	X	
	Searchable encryption	X	
	Trust establishment	X	
	Secure systems collaboration technologies	X	
	Privacy through usage control	X	
	Continuous security audits	X	
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies		

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard		
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards		
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces		
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		

	Standards requirements		Remark
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies	X	
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard		Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements		Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex H – Use case

Connected cars

1 Description of the use case

1.1 Name of use case

Connected cars

1.2 Scope and objectives of use case

1.2.1 Scope

The scope of this use case is to identify use cases and associated potential requirements for V2X services, taking into account the communication access technologies.

1.2.2 Objectives

The objective is to identify use cases and associated potential requirements for V2X services taking into account communication access technologies as defined in other SDOs. The essential use cases for V2X (V2V, V2I, and V2P) to be studied and the requirements identified are as follows;

- V2V: covering wireless communication between vehicles.
- V2P: covering wireless communication between a vehicle and a device carried by an individual (e.g. handheld terminal carried by a pedestrian, cyclist, driver or passenger).
- V2I: covering wireless communication between a vehicle and a roadside unit.

This use case includes safety and non-safety aspects.

1.3 Narrative of use case

1.3.1 Summary of use case

The vehicular communication in this study, referred to as vehicle-to-everything (V2X), includes the following three different types:

- vehicle-to-vehicle (V2V) communications.
- vehicle-to-infrastructure (V2I) communications.
- vehicle-to-pedestrian (V2P) communications.

1.3.2 Vehicle-to-vehicle (V2V)

The smart and secure IoT platform allows any smart objects that are in proximity of each other to exchange V2V-related information using the smart and secure IoT platform, when the permission, authorization and proximity criteria are fulfilled. The service provider configures the proximity criteria. However, the smart objects supporting V2V Service can exchange such information when served by or not served by the smart and secure IoT platform.

The smart object supporting V2V applications transmits application layer information (e.g. about its location, dynamics, and attributes as part of the V2V Service). The V2V payload must be flexible in order to accommodate different information contents, and the information can be transmitted periodically according to a configuration provided by the service provider.

V2V is predominantly broadcast-based; V2V includes the exchange of V2V-related application information between distinct smart objects directly and/or, due to the limited direct communication range of V2V, the exchange of V2V-related

application information between distinct smart objects via infrastructure, e.g. road side unit (RSU).

1.3.3 Vehicle-to-infrastructure (V2I)

The smart objects supporting V2I applications send application layer information to RSU. RSU sends application layer information to a group of smart objects or an individual smart object supporting V2I applications.

V2N is also introduced where one party is a smart object and the other party is a serving entity, both supporting V2N applications and communicating with each other via a communication network.

1.3.4 Vehicle-to-pedestrian (V2P)

The smart and secure IoT platform allows such smart objects that are in proximity of each other to exchange V2P-related information using the smart and secure IoT platform when the permission, authorization and proximity criteria are fulfilled. The service provider configures the proximity criteria. However, smart objects supporting V2P service can exchange such information even when not served by the smart and secure IoT platform.

The smart object supporting V2P applications transmits application layer information. Such information can be transmitted either by a vehicle with a smart object supporting V2X service (e.g. warning to pedestrian), or by a pedestrian with a smart object supporting V2X service (e.g. warning to vehicle).

V2P includes the exchange of V2P-related application information between distinct smart objects (one for vehicle and the other for pedestrian) directly and/or, due to the limited direct communication range of V2P, the exchange of V2P-related application information between distinct smart objects via infrastructure, e.g. RSU.

1.4 Diagrams of use case

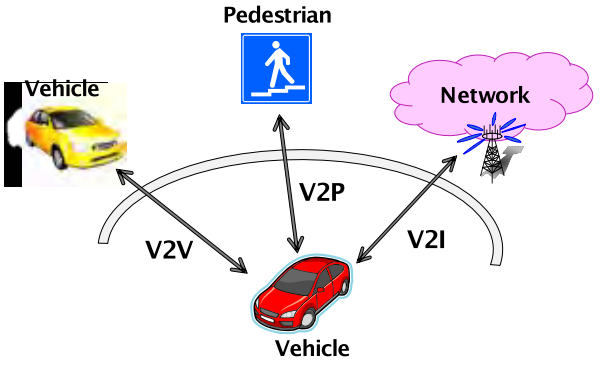


Figure H-1 | Diagram of use case – Vehicle to everything

1.5 Forward collision warning (FCW)

1.5.1 Description

The FCW application intends to warn the driver of the host vehicule (HV) in case of an impending rear-end collision with a remote vehicule (RV) ahead of it in traffic in the same lane and direction of travel. Using the V2V Service, the FCW intends to help drivers in avoiding or mitigating rear-end vehicle collisions in the forward path of travel.

1.5.2 Pre-conditions

The RV and the HV both support V2V Service and can communicate with each other using the V2V service.

1.5.3 Service flows

The RV V2V service layer periodically broadcasts a message, indicating its current location, speed, acceleration and optional estimated trajectory.

The RV makes an in-lane determination and time-to-collision determination, which is reflected in the broadcast message.

The communication access node broadcasts the different messages as requested by the application layer.

The HV receives the RV broadcasted message and determines if action need to be taken.

1.5.4 Post-conditions

The driver of the HV is alerted to the presence of an in-path vehicle and can take corrective action to avoid or mitigate rear-end vehicle collisions in the forward path of travel.

1.5.5 Potential requirements

The following potential requirements are derived from this use case:

- The service provider network shall be able to authorize a smart object that supports V2V service to use message transfer as needed for V2V services.
- A smart object that supports V2V service shall be able to transmit a broadcast V2V message periodically if requested by the V2V service layer.
- A smart object that supports V2V service shall be able to receive a periodic broadcast message.
- The smart and secure IoT platform shall be able to support high mobility performance (e.g. a maximum absolute velocity of 160 km/h).
- The smart and secure IoT platform shall be able to support a communication range sufficient to give the driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be able to support a message size of 50 bytes-300 bytes, which can be up to 1 200 bytes.
- The smart and secure IoT platform shall be able to support a maximum latency of 100 ms.
- The smart and secure IoT platform shall be able to support a maximum frequency of 10 V2V messages per second.
- The smart and secure IoT platform shall be able to support high reliability without requiring application-layer message retransmissions.
- The V2V Service shall support user/vehicle anonymity and integrity protection of the transmission.
- A smart object that supports V2V service shall be able to support transmission and reception of the V2V message from other smart objects that support V2V service in different public land mobile networks (PLMNs) and from different countries.

1.6 Control loss warning (CLW)

1.6.1 Description

The CLW application enables a HV to broadcast a self-generated control loss event to surrounding RVs. Upon receiving such event information, a RV determines the relevance of the event and provides a warning to the driver, if appropriate.

1.6.2 Pre-conditions

The RV and HV both support V2V service and can communicate with each other using the V2V service.

1.6.3 Service flows

The RV periodically broadcasts a message indicating its current location, speed, acceleration and optional estimated trajectory.

When the RV self-determines a control loss, possibly coupled with in-lane and time-to-collision determinations, it transmits this information via broadcast as an event, making use of the V2V service.

The HV receives the RV event message and determines if action need to be taken.

1.6.4 Post-conditions

The driver of the HV is alerted to the presence of an in-path vehicle experiencing a loss of control, and can therefore take corrective actions to avoid or mitigate a rear-end vehicle collision in the forward path of travel.

1.6.5 Potential requirements

The following potential requirements are derived from this use case:

- The smart and secure IoT platform shall be able to support high mobility performance (e.g. support a maximum relative velocity of 280 km/h).
- The smart and secure IoT platform shall be able to support a communication range sufficient to give the driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be able to support a maximum latency of 100 ms.
- The service provider network shall be able to support anonymity and integrity protection of communication.
- A smart object that supports V2V service shall be able to transmit an event-driven V2V message immediately after it has been triggered by the V2V service layer.
- A smart object that supports V2V service shall be able to receive an event-driven V2V message.
- The smart and secure IoT platform shall be able to support a message size of 50 bytes-300 bytes, which can be up to 1 200 bytes.
- The smart and secure IoT platform shall be able to support a maximum frequency of 10 V2V messages per second.
- The smart and secure IoT platform shall be able to support high reliability without requiring application-layer message retransmissions.

1.7 V2V use case for emergency vehicle warning

1.7.1 Description

Emergency vehicle warning service enables each vehicle to acquire the location, speed and direction information of a surrounding emergency vehicle (e.g. an ambulance) to assist a safety operation, for instance by enabling the ambulance path to be clear.

1.7.2 Pre-conditions

John is driving rapidly with his ambulance on the street. The ambulance is equipped with a proximity service (ProSe) [64]-enabled smart object supporting V2V service.

There are several cars in his vicinity also equipped with ProSe-enabled smart objects supporting V2V service.

1.7.3 Service flows

John's ambulance periodically checks if its location, speed or direction has changed for a predefined threshold compared with those notified previously. If any of the above parameters satisfies the checking criteria, a cooperative awareness message (CAM) is broadcasted containing the car's statement.

The CAM contains the basic vehicle information, including vehicle dynamic status information such as direction and speed, and vehicle static data such as dimension, status of exterior lights, path history. The size of the CAM message is between 50 bytes-300 bytes.

The emergency vehicle-warning message from John's ambulance is transmitted at a maximum frequency of 10 messages per second.

The generated CAM is broadcasted. It is expected that all cars within a 300 m-500 m range from John should be able to receive the message,

including cars at the street corner without a line-of-sight path. The latency for message reception shall be less than 100 ms.

1.7.4 Post-conditions

Cars in John's vicinity deliver the information to the car driver, who thus understands the need to free the passage way for the ambulance.

1.7.5 Potential requirements

- The smart and secure IoT platform shall be capable of transferring V2V service messages between two smart objects supporting V2V applications with variable message payloads of 50 bytes-300 bytes.
- The smart and secure IoT platform shall be capable of transferring V2V service messages between two smart objects supporting V2V applications with maximum frequency of 10 messages per second.
- The smart and secure IoT platform shall be capable of transferring V2V service messages between two smart objects supporting V2V applications with a maximum latency of 100 ms.
- The smart and secure IoT platform shall be capable of supporting a communication range sufficient to give the driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be capable of transferring V2V service messages between smart objects supporting V2V applications with a maximum relative velocity of 280 km/h.

1.8 V2V emergency stop use case

1.8.1 Description

This use case describes V2V communication used in the case of an emergency stop to trigger safer behaviour for other cars in the proximity of the stationary vehicle.

1.8.2 Pre-conditions

John is driving his car on the street. The car is equipped with a ProSe-enabled smart object supporting V2V service.

There are several cars in his vicinity also equipped with ProSe-enabled smart objects supporting V2V service.

1.8.3 Service flows

John's car engine breaks and his car suddenly stops in the middle of the street. The safety service of John's car notices this event and generates a "stationary vehicle warning" via a decentralized environmental notification message (DENM) message. The size of the DENM is smaller than 3 000 bytes.

All cars within John's transmission range are able to receive the message.

1.8.4 Post-conditions

Cars in John's vicinity deliver the information to drivers who can take appropriate action.

1.8.5 Potential requirements

- The smart and secure IoT platform shall be capable of transferring V2V service messages when requested by the V2V service between two smart objects supporting V2V applications, with a maximum message size of 1 200 Bytes.
- The smart and secure IoT platform shall be capable of transferring V2V service messages between two smart objects supporting V2V applications with maximum frequency of 10 messages per second.
- The smart and secure IoT platform shall be capable of transferring V2V Service messages

between two smart objects supporting V2V applications with a maximum latency of 100 ms.

- The smart and secure IoT platform shall be capable of supporting a communication range sufficient to give the driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be capable of transferring V2V service messages between smart objects supporting V2V applications, with a maximum absolute velocity of 160 km/h.

1.9 Cooperative adaptive cruise control

1.9.1 Description

This use case describes a scenario in which a vehicle with V2V capability joins and leaves a group of cooperative adaptive cruise control (CACC) vehicles. This provides convenience and safety benefits to participating vehicles and also has societal benefits for improving road congestion and fuel efficiency.

1.9.2 Pre-conditions

Vehicles A and B both support V2V applications.

Vehicles A and B are travelling in proximity, and are in V2V communication range.

Vehicle A is travelling outside of a CACC group, which includes Vehicle B, and wants to join the CACC group.

1.9.3 Service flows

Vehicle B and other platoon members periodically broadcast a message with the CACC group information, e.g. size, speed, gap policies, their positions in the CACC group, etc.

Vehicle A receives messages from the CACC group members and identifies acceptable CACC groups based on certain criteria (e.g. speed and gap policies, size).

Vehicle A sends a message to members of the CACC group to request joining.

Vehicle B decides that A can join the CACC group ahead of it and responds with a confirmation, allowing fora distance gap (if necessary).

All other members of the CACC group receive messages from Vehicle A and update the CACC group information they hold locally.

Subsequently, the driver of Vehicle A decides to leave the CACC group and assumes control of Vehicle A.

Vehicle A broadcasts a good-bye message to other members of the CACC group.

Vehicle B receives the message from Vehicle A and updates the CACC group information it holds locally.

1.9.4 Post-conditions

Vehicle A leaves the CACC group.

1.9.5 Potential requirements

- The smart and secure IoT platform shall be able to support a maximum latency of 1 s.
- The smart and secure IoT platform shall be able to support a maximum frequency of 1 V2V message per second.
- The smart and secure IoT platform shall be able to support high reliability without requiring application-layer message retransmissions.
- The smart and secure IoT platform shall be able to support a high density of smart objects supporting V2V services (e.g. a 4-lane motorway with traffic jam).

1.10 V2I emergency stop use case

1.10.1 Description

This use case describes V2I communication in which a Service RSU notifies vehicles travelling in the vicinity in case of an emergency stop in order to trigger safer behaviour.

1.10.2 Pre-conditions

John is driving his vehicle on the street. The vehicle is equipped with a ProSe-enabled smart object supporting V2X service.

There are several service RSUs in his vicinity equipped with ProSe-enabled smart objects supporting V2X service.

1.10.3 Service flows

John's vehicle engine malfunctions and his vehicle suddenly stops in the middle of the street. The safety service of John's vehicle notices this event and generates a "Stationary vehicle warning" DENM message.

A Service RSU in John's vicinity is able to receive the message.

The Service RSU relays the message to its surrounding vehicles.

All vehicles within the transmission range from the Service RSU are able to receive the message.

1.10.4 Post-conditions

Vehicles near the Service RSU deliver the information to drivers who can take an appropriate action.

1.10.5 Potential requirements

- The smart and secure IoT platform shall be capable of transferring V2I service messages between two Smart Objects supporting V2I applications with variable message payloads smaller than 1 200 bytes. The typical size of messages is 400 bytes.
- The smart and secure IoT platform shall be capable of transferring V2I service messages between a smart object and a roadside unit both supporting V2I applications with the maximum frequency of 10 messages per second.
- The smart and secure IoT platform shall be capable of transferring V2I Service messages between a smart object and a roadside unit, both supporting V2I applications with latency no larger than 100 ms and low delivery loss rate.
- The smart and secure IoT platform shall be capable of supporting communication range between a smart object and a roadside unit both supporting V2I applications sufficient to give driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be capable of transferring V2I service messages between a smart object and a roadside unit supporting V2I applications with a maximum relative velocity of 160 km/h.

1.11 Queue warning

1.11.1 Description

In many situations, a queue of vehicles on the road may pose a potential danger and cause a delay of traffic, e.g. when a turning queue extends to other lanes. Using the V2I service, the queue information can be made available to other drivers beforehand. This minimizes the likelihood of crashes and allows for mitigation actions.

1.11.2 Pre-conditions

Vehicles A, B, C, and D all support V2X applications and can communicate with each other using the V2V service, and communicate with an infrastructure entity, RSU, via the V2I service.

Vehicles A, B and C are queuing at a junction, with vehicle A at the queue head and vehicle C at the queue end. Vehicle D is approaching the junction from afar.

1.11.3 Service flows

The service flow involves two aspects: queue determination and queue information dissemination. The former is making use of the V2V service, and the latter is using the V2I service.

The detailed service flow is as follows:

Each of the vehicles A, B and C broadcasts a message periodically to other vehicles in proximity using V2V service. The message indicates their status, e.g. location, vehicle dimension, heading, speed, brake status, gear level, and possible environmental information.

Vehicle C receives the broadcast messages, determines that it is the end of the queue, and thus periodically informs the RSU, using V2I service, regarding the queue information, e.g. size of the queue, status of the queue, the last position of the queue, which lanes are affected, etc.

The RSU broadcasts a message about the queue to vehicles in proximity, using the V2I service, based on information received from Vehicle C.

Vehicle D, when approaching the RSU, receives the message from the RSU using the V2I service, and the driver is made aware of the queue and related information, such that his driving strategy can be formed before reaching the queue.

Vehicle D joins the queue behind vehicle C. Vehicle D replaces vehicle C to update the RSU, using V2V service, about the queue, after it determines that it has become the end of the queue.

1.11.4 Post-conditions

Driver of vehicle D is made aware of the queue ahead of time, and can take action accordingly in a timely fashion.

1.11.5 Potential requirements

- A smart object that supports V2I service shall be able to transmit a message to an RSU.
- A smart object that supports V2I Service shall be able to receive a message from an RSU.
- The smart and secure IoT platform shall be able to support a maximum relative velocity of 160 km/h.
- The smart and secure IoT platform shall be able to support a communication range sufficient to give driver(s) ample response time (e.g. 4 s).
- The smart and secure IoT platform shall be able to support a message size of 50 bytes-400 bytes, which can be up to 1 200 bytes.
- The smart and secure IoT platform shall be able to support a maximum latency of 100 ms.
- The V2I Service shall support user/vehicle anonymity and integrity protection of the transmission.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol	X	Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards	X	Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning		
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/ resilience
Dynamic configurability	X	Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability		Remark
Digital product memory		Whole lifecycle; product pedigree
Pattern recognition		Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy		
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors	X	

2.5 Actions

Control interface devices

Capability		Remark
Calibration		
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements		
Authentication and access control and authorization	X	
Floor control		Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control		

User I/O

Capability		Remark
Tactile interfaces	X	
Multi-device user-interfaces	X	
Virtual modelling		
Simulation		
Accessibility		For disabled people
Augmented Reality		E.g. glasses
Usability and user experience		

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats		OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection		

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections	X	Higher bandwidth, low latency
	5th generation cellular access (5G)	X	
	Low power wireless access (LPWAN)	X	
Processing	System configuration and dynamic composition		
	Data contextualization		
	Autonomous data exchange		
	Sensor fusion technology		
	Machine learning	X	
	Virtualization	X	
Memory	Digital product memory		
Sensing	Ultra-precise location technology	X	

	Next-generation enabling technology		Remark
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet	X	
Security	Identity of things	X	
	Homomorphic encryption		
	Searchable encryption		
	Trust establishment		
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard	X	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards	X	
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms		
	Metadata annotation models and interfaces		
	Contextualized information models	X	
	Metadata context standards		
Memory	Standardization of digital product memory		

	Standards requirements		Remark
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard	X	Opt-in/opt-out for end customers/consumers
	Sensor fusion standard		Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems	X	
	Standard for unique IoT accessibility requirements	X	Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems		
	Cyber-physical attack protection standards		
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework		Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems		

Annex I – Use case

WISE Skiing

1 Description of the use case

1.1 Name of use case

WISE Skiing with smart and secure IoT platforms

1.2 Scope and objectives of use case

1.2.1 Scope

The vision of WISE Skiing is to integrate IoT technologies into everyday activities such as skiing and especially for the sport products used during those daily activities. In order to attract people to sign-up for the system, incentive techniques and gamification are used. In an emergency case, the same information can be used for faster handling of the emergency. In the broader sense, this use case targets effective emergency handling and enhancement of public safety measures.

1.2.2 Objectives

WISE Skiing is an example application, where IoT technologies have multi-purpose use. Such technologies can be applied to public safety management in a large city-scale event, e.g. colour runs, marathons, and golf events.

To realize the vision, advanced technical capabilities in sensing, processing, communications, actuation, security, gamification and incentive schemes are needed. Furthermore, standardization efforts for transparent information sharing, discovering opportunities for information mashups, semantic interoperability and emergency management will be needed. In summary, this use case defines essential requirements of the next-generation IoT platforms.

1.3 Narrative of the use case

1.3.1 Summary of the use case

In the WISE Skiing use case, each skier carries a smartphone with various built-in sensors which will capture the person's skiing trajectories, motion information, light intensity, and levels of ambient sounds. Meanwhile, vibration sensors are mounted on skiing equipment to track the skier's motions and gestures. With these sensing data, the system will perform a variety of functions, e.g. real-time incident detection, emergency handing, and slope recommendations based on difficulty levels.

To realize the WISE Skiing scenario, some advanced technical capabilities are required because of the following characteristics in future IoT services: (a) very different equipment needs to be included into the scenario (a variety of devices), (b) data is being used by many applications (a variety of consuming applications). In the vertical domain, the future IoT platform accommodates data from very different context origins and provides connectivity management and resource-context management. In the horizontal domain, semantic-based discovery and context transformation on the edge side, as well as data contextualization and saleable data-streams management on the cloud side, are required. However, both the vertical and horizontal capabilities rely on standardization efforts to integrate information from data sources and further semantics in the future.

1.3.2 Nature of the use case

Private customers.

1.3.3 Complete description

The WISE Skiing use case with a smart and secure IoT platform is shown in Figure I-1. Each skier will wear a set of sensors (on their skiing equipment) and a mobile device with some built-in sensors. These sensors will capture skiing trajectories (by the location sensors), motion information (by the gravity, orientation and accelerometer sensors), light intensity (by the light sensor), and levels of ambient sounds (by the microphone). To encourage skiers to contribute more sensing data, there is a gamification-based incentive scheme in the WISE Skiing system, where skiers who contribute much data or provide higher quality of data will be rewarded (e.g. scores or real shopping vouchers). Once the collected data is transformed into a common form with contextual information in the next-generation IoT platform, real-time incident detection, emergency handling, and slope recommendations will be provided to skiers for enhancing their safety.

However, the WISE Skiing use case relies heavily on interoperability and internetworking in the smart and secure IoT platforms. In the vertical domain, from context origins towards IoT platform, connectivity management and resource-context management will enable the information transparency between different entities and open up opportunities for information mashups. Specifically, the connectivity management refers to the capabilities of semantic interoperability and semantic mediation, while the resource-context management refers to the capabilities of self-optimization and resource-entity mapping. In the horizontal domain, advanced capacities on edges and clouds will incorporate data streams from different resources and entities to perform search and rescue actuations (e.g. localization of incidents and injured people). Specifically, semantic-based discovery and context transformation at the edge side discover the opportunities for early information mashups, while data contextualization and scalable data-streams management on the cloud side perform sophisticated computation for enhancement of emergency response. Meanwhile, in a normal situation, the horizontal capabilities enable the slope recommendation and gamification through incentive schemes. Both the vertical and horizontal capabilities will rely on the standardization efforts to realize the use case such as FIWARE NGSI for bridging edge with cloud and oneM2M for connecting different types of devices to edge.

1.4 Diagrams of use case

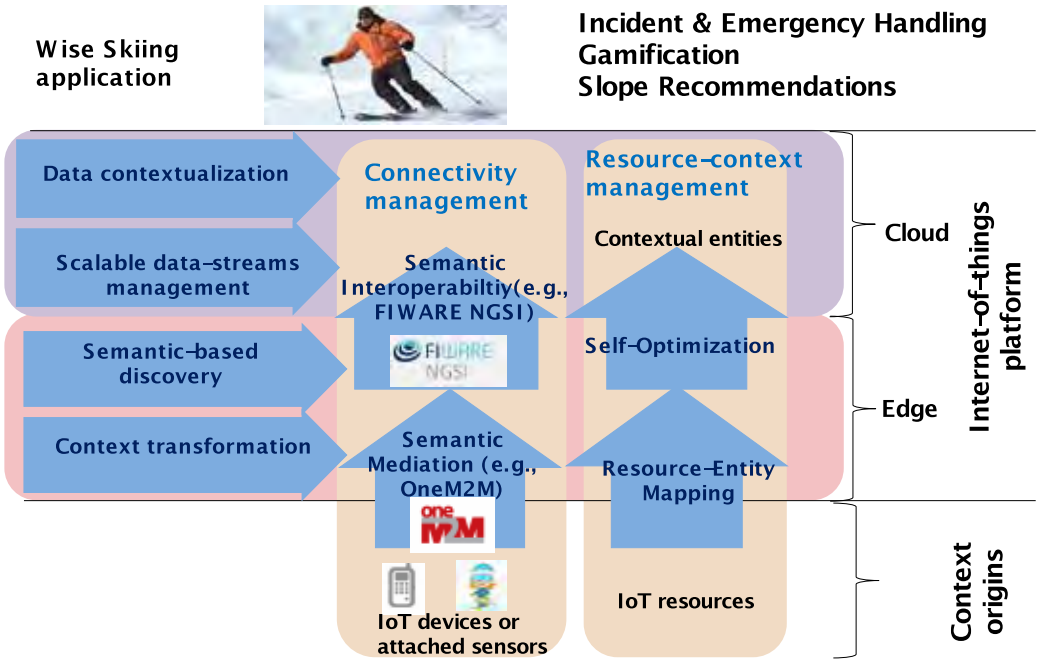


Figure I-1 | WISE Skiing with smart and secure IoT platform

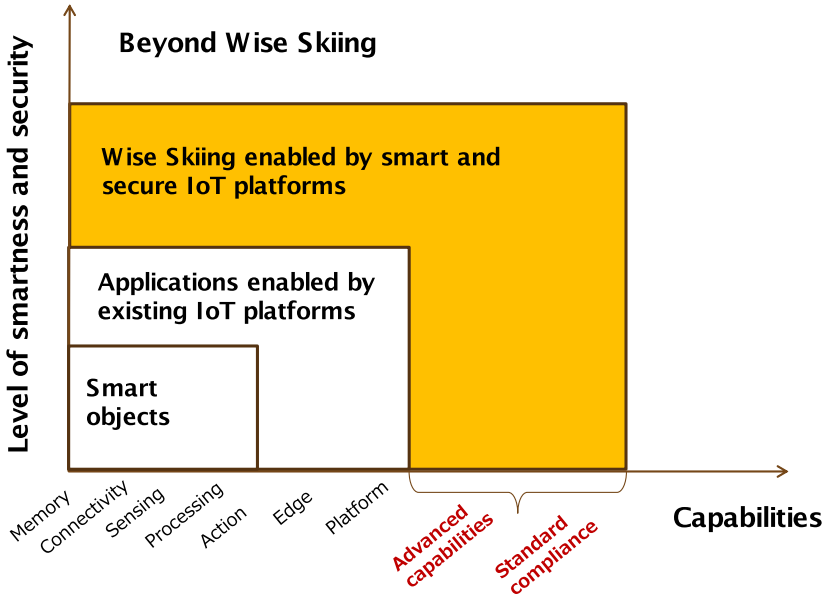


Figure I-2 | The vision of WISE Skiing with smart and secure IoT platform

1.5 Use case conditions

1.5.1 Assumptions

The WISE Skiing use case assumes that people entering the ski resort will either have the equipment already enabled with IoT sensors or they will rent/buy the devices before they start skiing.

1.6 Further information for the use case

1.6.1 State of the art

IoT standards: The use case employs the oneM2M standard for data communications. It uses the Open Mobile Alliance (OMA) next-generation service interfaces (NGSI) 9/10 APIs for providing contextualized access to the information from many applications. The vision of this use case needs additional standardized components, e.g. integration of support for semantic interoperability of data from the various systems. Information streams coming from M2M systems (probably based on the oneM2M standard) need to be automatically mapped into NGSI-based contextualized information models that are defined and used as standards in FIWARE. The transformation process can be handled by semantic mediation gateways (SMGs) to map different information models into a common model using semantic information as well as libraries of transformation routines. The transformed metadata will be used for faster discovery of available resources, automatic mashups of information, and improved big data analytics functions. Smart functions for the automatic integration of information and the generation of automatic mashups are needed. Furthermore, the data gathered and inferred is made available to multiple new applications that might come from different third parties. Strict control of security and privacy policies is needed.

2 Mapping to characteristic capabilities

Semantic interoperability: Interoperability is "the ability of two or more systems or components to exchange data and use information" [61]. Semantic interoperability is achieved when interacting systems attribute the same meaning to an exchanged piece of data, ensuring consistency of the data across systems regardless of individual data format. The semantics can be explicitly defined using a shared vocabulary as specified in an ontology. Semantic interoperability can be applied to all parts of an IoT system, i.e. on IoT platforms in the cloud, but also reaching to edge components and IoT devices [65].

Semantic mediation: Semantic mediation seamlessly transforms data coming from different devices and provides interoperated knowledge for different IoT systems. The vision of the next-generation IoT platform is to share data originating from individual verticals across a wide range of different applications and users. Therefore, intelligent semantic mediation gateways will have capabilities for connecting different devices which may have different connectivity options (WiFi, Bluetooth, ZigBee, 3GPP, LoRaWAN).

Resource-entity mapping: In existing IoT platforms, multiple resources are mapped into a single context (e.g. situations). However, in the future, the resources also can be a couple of context entities. For example, the contextual information about snowing and public holidays in the calendar also can involve shared resources which may change recommended slopes. Therefore, the mapping between resources and context entities will be more sophisticated in the resource-context management.

Self-optimization: In a cloud-edge based environment, data processing and contextual data mining tasks can be dynamically allocated to either the cloud or the edge in order to meet certain optimization objectives, such as reducing

the bandwidth consumption between the edge and the cloud, or minimizing the latency to extract analytics results from raw sensor data.

Context transformation: Context transformation performs early and lightweight data analytics on edges (e.g. data filtering and pre-processing) to enable semantic-based discovery and information mashups in the early stage.

Semantic-based discovery: Semantic-based discovery will remove the need for human involvement and assistance and allow worldwide IoT applications to complete automated installations, deployments, and information mashups in early stage.

Scalable data-streams management: The capability of scalable data-streams management is to handle real-time and large-scale data sharing and data distribution. Meanwhile, it will coordinate data flows, security, and integration with big data analytics.

Data contextualization: Data contextualization is an information transformation process which extracts transparent or hidden information behind the collected data and represents it as a meaningful form in certain knowledge domains through contextual mining and analytical algorithms. The emerging techniques of data contextualization will continue to perform the following three tasks: historical data analytics, real-time situation awareness and situation prediction.

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol	X	Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards	X	Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine learning	X	
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/ resilience
Dynamic configurability	X	Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability		Remark
Digital product memory	X	Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy	X	
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors	X	

2.5 Actions

Control interface devices

Capability		Remark
Calibration	X	
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements	X	
Authentication and access control and authorization	X	
Floor control	X	Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence	X	
Swarm control of security		
Context-aware control	X	

User I/O

Capability		Remark
Tactile interfaces	X	
Multi-device user-interfaces	X	
Virtual modelling	X	
Simulation	X	
Accessibility		For disabled people
Augmented Reality	X	E.g. glasses
Usability and user experience	X	

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security	X	Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats	X	OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection	X	

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections	X	Higher bandwidth, high latency
	5th generation cellular access (5G)	X	
	Low power wireless access (LPWAN)	X	
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange	X	
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization	X	
Memory	Digital product memory	X	
Sensing	Ultra-precise location technology	X	

	Next-generation enabling technology		Remark
Actions	Augmented reality	X	
	Virtual reality	X	
	Tactile Internet		
Security	Identity of things	X	
	Homomorphic encryption	X	
	Searchable encryption	X	
	Trust establishment	X	
	Secure systems collaboration technologies	X	
	Privacy through usage control	X	
	Continuous security audits		
	IAM technologies for IoT	X	Identity and access management
	Application isolation and security boundary technologies	X	

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard	X	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device	X	
	Standards for IoT equipment to have the capability to update to new connectivity standards	X	
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms	X	
	Metadata annotation models and interfaces	X	
	Contextualized information models	X	
	Metadata context standards	X	
Memory	Standardization of digital product memory	X	

	Standards requirements		Remark
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies	X	
	Sensor data privacy standard	X	Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices	X	
	General standard to normalize IoT user I/O across systems	X	
	Standard for unique IoT accessibility requirements	X	Reflecting the advanced IoT services that go beyond typical human/computer I/O
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards		
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity	X	
	Cooperative security framework	X	Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems	X	

Annex J – Use case

Home device smart factory

1 Description of the use case

1.1 Name of use case

Home device smart factory

1.2 Scope and objectives of use case

1.2.1 Scope

The use case addresses the factory processes within a home device manufacturer in China. It addresses the acquisition of factory process data and makes this real time data available to the back office.

1.2.2 Objectives

The objective of this use case is to demonstrate the acquisition of relevant process data from the factories' tools, instruments, sensors, PLCs and devices. It demonstrates the improved efficiency and even reduction of costs possible from making the factory process data available within the cloud and providing access to the factory-process management applications via desk cloud clients, which improves the availability of relevant information.

1.3 Narrative of use case

1.3.1 Summary of use case

The use case describes the acquisition of factory process data via an IoT gateway, which is an industrial gateway supporting different protocols to retrieve data such as device status, energy consumption, etc.

The use case also describes the provisioning of the factory process applications within the cloud and deploys cloud terminals to access the operational enterprise resource planning (ERP), product lifecycle management (PLM) and manufacturing execution system (MES) applications. Such access will provide the opportunity for real time query of information, such as quality control (QC) test results, production process information, etc.

1.3.2 Nature of the use case

The use case addresses the introduction of the concept of an IoT platform interworking with IoT agents, which is an example of the platform of platform principles.

1.3.3 Complete description

The Home Device Manufacturing Company noticed inefficiency within their production process and decided to collect more information from the manufacturing process to understand the production inefficiencies. They also noticed that accessibility to the production process information needed to be improved outside the factory within the sales and management offices.

The system collects data from the manufacturing process within the production line via an industrial gateway via wireline/bus/wireless connections from the different sensors and processes in the factory automatically. The data includes device status, energy consumption, environmental monitoring data, sensor data, and production process data. The data is provided to the IoT platform within the factory cloud infrastructure

and is distributed to the different business/ manufacturing processes, such as ERP, PLM, MES and big data analytics.

The business and manufacturing statistics and information are made available via cloud infrastructure on the cloud terminals integrated with several office applications. The manufacturer's management is now able to receive the critical process information instantly on their terminals for managerial processing and introducing necessary corrections to the business and manufacturing processes to avoid waste and/or failures. This has resulted in an increased efficiency of 30% and a reduced cost of 20%.

1.5 Use case conditions

1.5.1 Assumptions

The technology used does not require substantial new technologies in the manufacturing process but is rather focused to provide the necessary business and manufacturing information where and when it is needed. Therefore, it is assumed that the information acquired is needed to manage the business and manufacturing processes.

The use case is focused on integration of the manufacturing information within the factory in the business processes of the management, R&D and sales offices.

1.4 Diagrams of use case

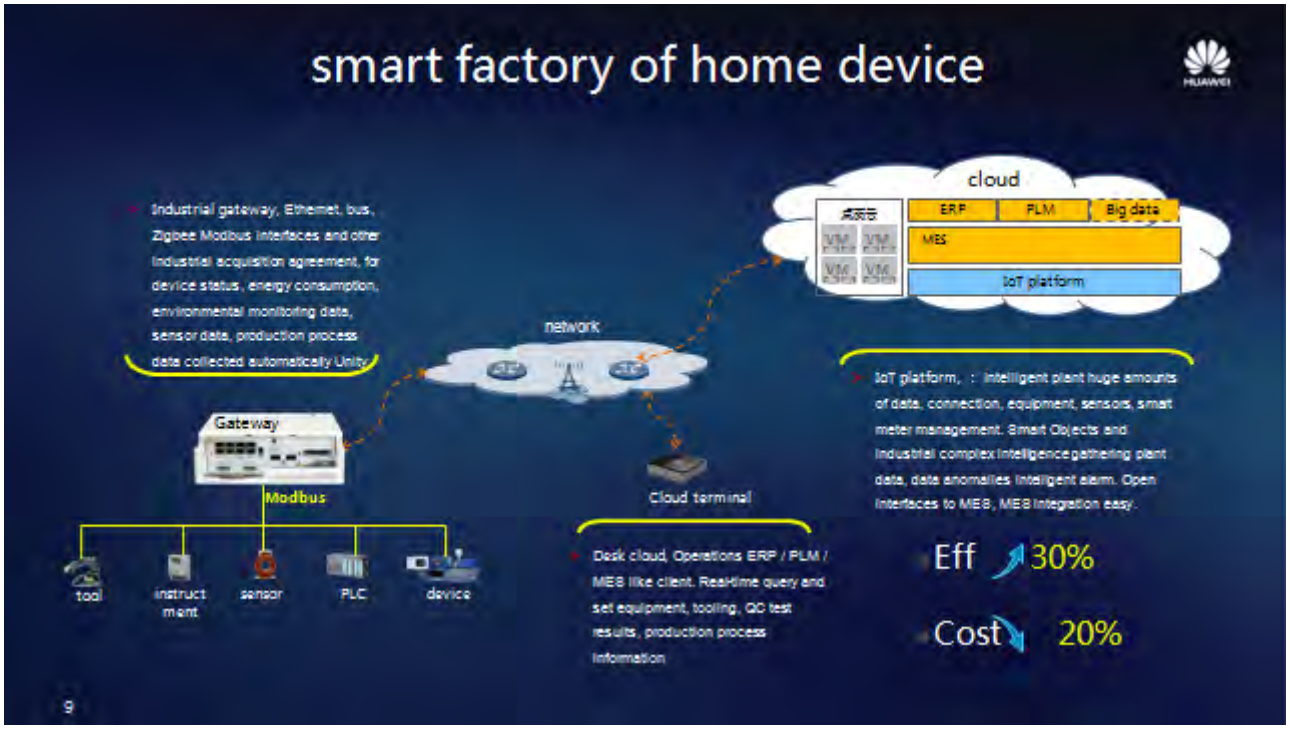


Figure J-1 | Diagram of use case – Smart factory of home device

1.5.2 Prerequisites

The solution requires an industrial gateway that is able to connect to the sensors and actuators using different communication technologies, e.g. wireless and wireline, and different protocols.

The solution requires an IoT agent integrated within the industrial gateway to include some common functions within the industrial gateway, such as security management, device management and data management capabilities.

Security management includes the basic security access functionality such as device authentication, time-based authentication, data source checking and device availability.

Device management includes basic functions such as fault management, service tracking, presence management and anti-theft/clone management.

Data management will include a rule engine that automatically can trigger an action, such as sending a notification or an alarm when specific conditions are met. The rules engine will support specific rules for devices separately or for groups of devices. The rules will be programmable using declarative programs.

1.6 Further information for the use case

1.6.1 State of the art

The transformation of introducing information knowledge within the manufacturing industry, i.e. smart manufacturing, is already ongoing. The basic technologies for industrial gateways are available within different industries, i.e. communication technology (CT), IT and OT.

However, some specific use cases will require low latency services, e.g. less than 10 ms, which will require some enhancements within wireless communication technology. Other technologies could include self-learning capabilities to evolve data management capabilities as well hardware acceleration to ensure that platform performance criteria are met.

2 Mapping to characteristic capabilities

2.1 Connectivity

Capability		Remark
Real-time situation handling	X	Includes real-time sense-making
Multi-system connectivity	X	Connection to more than one system
Remote functionality	X	Functionality resides outside of the product
Adaptability to any bandwidth/protocol	X	Reconfiguration to adapt to any bandwidth/protocol offered → shift from HW to SW solution
Upgradability to new connectivity standards	X	Ability to upgrade to new connectivity standards by SW
Legal intercept capabilities		
Remote access	X	
Authentication and access control	X	
Reliability and integrity	X	

2.2 Processing

Capability		Remark
Onboard analytics	X	
Offboard analytics	X	
Machine Learning		
Contextualization	X	
Anonymization	X	
Information mashup	X	
Semantic interoperability	X	
Dynamic composition of devices	X	Dynamic composition of devices for self healing/resilience
Dynamic configurability	X	Device needs to be dynamically configurable by itself and by the system depending on changing requirements
Tracking data ownership	X	
(Swarm) awareness		

2.3 Memory

Capability		Remark
Digital product Memory		Whole lifecycle; product pedigree
Pattern recognition	X	Based on artificial intelligence/machine learning
Performance data	X	For analytics

2.4 Sensing

Capability		Remark
Cope with growing number of devices with sensing capabilities	X	
Mediated exchange of sensing data	X	
Trustworthiness of data	X	
Cleansing of raw data	X	
Ultra-precise location-based capabilities	X	
Privacy		
Integrity of data	X	
Complex sensors that require authentication	X	
Ability to reconfigure sensors	X	

2.5 Actions

Control interface devices

Capability		Remark
Calibration		
Control of group of devices	X	Runtime and configuration
Dynamic composition of devices	X	Dynamic device onboarding/assigning to a group
Adapt the way the device is controlled according to context	X	
Safety requirements		
Authentication and access control and authorization	X	
Floor control		Who of the allowed people really controls a system and what are the handover mechanisms
Swarm/self-optimization control intelligence		
Swarm control of security		
Context-aware control		

User I/O

Capability		Remark
Tactile interfaces	X	
Multi-device user-interfaces	X	
Virtual modelling		
Simulation		
Accessibility		For disabled people
Augmented reality		E.g. glasses
Usability and user experience		

2.6 Security

Capability		Remark
End-to-end policy management	X	Integrates all policies
Optimized framework with respect to available physical resources and security		Optimized framework with respect to available physical resources/security robustness (plan-do-check-act in ISO 27001)
Resilience	X	Including cyber-physical attacks
Fault tolerance	X	Including cyber-physical attacks
Detection and response to system threats		OODA observe-orient-decide-act
Monitoring of devices	X	
Coordination and analysis of threats	X	
Identity management	X	Federated identity management, ID correlation between systems, …
Securing ID of devices	X	

Capability		Remark
Authenticity management	X	Accountability/non-repudiation of data
Anomaly detection		

3 Next-generation enabling technologies

	Next-generation enabling technology		Remark
Connectivity	Transport layer protocol for next-generation satellite connections		Higher bandwidth, high latency
	5th generation cellular access (5G)	X	
	Low power wireless access (LPWAN)	X	
Processing	System configuration and dynamic composition	X	
	Data contextualization	X	
	Autonomous data exchange		
	Sensor fusion technology	X	
	Machine learning	X	
	Virtualization		
Memory	Digital product memory		
Sensing	Ultra-precise location technology	X	
Actions	Augmented reality		
	Virtual reality		
	Tactile Internet	X	
Security	Identity of things	X	
	Homomorphic encryption		
	Searchable encryption		
	Trust establishment		
	Secure systems collaboration technologies	X	
	Privacy through usage control		
	Continuous security audits		
	IAM technologies for IoT		Identity and access management
	Application isolation and security boundary technologies		

4 Necessary future standards

	Standards requirements		Remark
Connectivity	Realization of the 5G standard	X	
	Standard for new transport layer protocol to support higher bandwidth/demanding latency between satellite and device		
	Standards for IoT equipment to have the capability to update to new connectivity standards	X	
Processing	Information exchange models	X	
	Semantic metadata definition standards and models	X	
	Data exchange models as well as interfaces and related standards	X	
	Autonomous data exchange profiles and exchange mechanisms		
	Metadata annotation models and interfaces		
	Contextualized information models	X	
	Metadata context standards	X	
Memory	Standardization of digital product memory		
Sensing	Standard for metadata	X	
	Abstraction standard for ultra-precise location-based technologies		
	Sensor data privacy standard		Opt-in/opt-out for end customers/consumers
	Sensor fusion standard	X	Standard for developing sensor meta-models for abstracting sensor observations, which can facilitate transforming unstructured and noisy data into high-level domain knowledge
Actions	Standard template for uniquely identifying groupings of control interface devices		
	General standard to normalize IoT user I/O across systems		
	Standard for unique IoT accessibility requirements	X	Reflecting the advanced IoT services that go beyond typical human/computer I/O

	Standards requirements		Remark
Security	ID federation standard in social systems	X	
	Cyber-physical attack protection standards	X	
	Standard for device identifier across multiple systems with simultaneous connections	X	Such as an internationalized resource identifier (IRI) from the W3C
	Standard protocols for establishing trust in platform integrity		
	Cooperative security framework		Enables exchange of cyber threat intelligence between interdependent systems
	Maturity models that enable security capability assessment between interdependent systems		

Bibliography

[1] International Data Corporation (IDC), *Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC*, 02 June 2015, [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS25658015. [Accessed 22 August 2016].

[2] Gartner Inc., *The Internet of Things Is a Revolution Waiting to Happen*, 30 April 2015. [Online]. Available: http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen. [Accessed 22 August 2016].

[3] McKinsey Global Institute, *Unlocking the Potential of the Internet of Things*, June 2015. [Online]. Available: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. [Accessed 22 August 2016].

[4] Gartner Inc., *Infrastructure and Operations Leaders: Prepare for the IoT Rush*, 2016.

[5] Wikipedia, *Kevin Ashton*, [Online].
Available: https://en.wikipedia.org/wiki/Kevin_Ashton. [Accessed 22 August 2016].

[6] ISO/IEC JTC 1, *Internet of Things (IoT)*, Geneva, 2014.

[7] ISO/IEC 30141, *Information technology – Internet of Things Reference Architecture*, Working Draft.

[8] Industrial Internet Consortium, *Industrial Internet Reference Architecture*, [Online]. Available: http://www.iiconsortium.org/IIRA.htm. [Accessed 22 August 2016].

[9] ISO/IEC/IEEE 42010, *Systems and software engineering – Architecture description*, 2011.

[10] ITU-T Study Group 13, *Next Generation Networks – Frameworks and Functional Models: Overview of the Internet of Things*, International Telecommunication Union, Geneva, 2012.

[11] ZVEI – German Electrical and Electronic Manufacturers' Association, *Industrie 4.0: The Reference Architectural Model Industrie 4.0 (RAMI 4.0)*, Frankfurt am Main, 2015.

[12] Internet of Things – Architecture Consortium, *The IoT Architectural Reference Model (ARM) - D1.3*, European Commission, Luxembourg, 2012.

[13] Industrial Internet Consortium, *Industrial Internet Reference Architecture (Version 1.7)*, Object Management Group, Needham, MA, US, 2015.

[14] TAKABI, H., JOSHI, J. B. D., AHN, G. J., *Security and Privacy Challenges in Cloud Computing Environments*, IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, 2010.

[15] Gartner Inc., *Digital Ethics, or How to Not Mess Up With*, 2016.

[16] Industrial Internet Consortium, *Industrial Internet Systems Volume G8: Vocabulary*, 2016.

[17] Hitachi Ltd., *Information and Control Systems – Open Innovation Achieved through Symbiotic Autonomous Decentralization*, Hitachi Review Vol.65 (2016), No.5, 2016.

[18] Cisco, *Global Cloud Index*.

[19] BRANDHERM, B., KROENER, A., *Digital Product Memories and Product Life Cycle*, in Seventh International Conference on Digital Environments, 2011.

[20] Hitachi Ltd., *Hitachi's Concept for Social Infrastructure Security*, Hitachi Review Vol.63 (2014), No.5, 2014.

[21] CHAN, H., PERRIG, A., *Security and privacy in sensor networks*, Computer, vol. 36, no. 10, pp. 103-105, 2003.

[22] McDANIEL, P., McLAUGHLIN, S., *Security and Privacy Challenges in the Smart Grid*, IEEE Security and Privacy, vol. 7, no. 3, pp. 75-77, 2009.

[23] WEIS, S. A., SARMA, S. E., RIVEST, R. L., ENGELS, D. W., *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*, in Security in Pervasive Computing, 1st International Conference, Boppard, Germany, 2004.

[24] MIMURA, M., Ph.D. ARAI, T., Ph.D. NAKANO, T., Ph.D. HATTORI, R., SATO, A., *Hitachi's Concept for Social Infrastructure Security*, Hitachi Review, 63 (5), 222-229, 2014.

[25] *Machina Research*, [Online]. Available: https://machinaresearch.com/news/global-m2m-market-to-grow-to-27-billion-devices-generating-usd16-trillion-revenue-in-2024. [Accessed 22 August 2016].

[26] Gartner Inc., *When Smart Things Rule the World – Introducing Autonomous Business*, 2015.

[27] Gartner Inc., *Internet of Things Scenario: When Things Become Customers*, 2015.

[28] RODE, J., SCHMIDT, M., O'ROURKE, J., GERDSMEIER, S., *SemProM: Semantic Product*, 2009.

[29] GRANGEL-GONZALES, I., HALILAJ, L., COSKUN, G., AUER, S., COLLARANA, D., HOFFMEISTER; M., *Towards a Semantic Administrative Shell for Industry 4.0 Components*, 2016, [Online]. Available: https://arxiv.org/pdf/1601.01556.pdf. [Accessed 22 August 2016].

[30] Forrester Inc., *Master Mobile Moments To Win In The IoT World*, 2016.

[31] The Library of the Congress, *What is a GPS? How does it work?*, 2016.

[32] U.S. Coast Guard Navigation Center, *GPS Frequently Asked Questions*, 2016.

[33] U.S. Air Force, *GPS Accuracy*, 2016.

[34] U.S. Air Force, *GPS Modernization*, 2016.

[35] GRAHAM, M., ZOOK, M., BOULTON, A., *Augmented reality in urban places: contested content and the duplicity of code*, Transactions of the Institute of British Geographers, vol. 38, no. 3, pp. 464-479, 2013.

[36] FETTWEIS, G., *The Tactile Internet: Applications and Challenges*, IEEE Vehicular Technology Magazine, pp. 64-70, March 2014.

[37] ITU-T Technology Watch, *The Tactile Internet*, International Telecommunication Union, Geneva, August 2014.

[38] SANS Institute, *Tools and Standards for Cyber Threat Intelligence Projects*, [Online]. Available: https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375. [Accessed 22 August 2016].

[39] Internet Engineering Task Force, *Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants*, May 2015, [Online]. Available: https://tools.ietf.org/html/rfc7522. [Accessed 22 August 2016].

[40] *OpenID Connect Core 1.0*, November 2014, [Online].
Available: http://openid.net/specs/openid-connect-core-1_0.html. [Accessed 22 August 2016].

[41] Internet Engineering Taskforce, *The OAuth 2.0 Authorization Framework*, October 2012, [Online]. Available: https://tools.ietf.org/html/rfc6749. [Accessed 22 August 2016].

[42] Internet Engineering Task Force, *System for Cross-domain Identity Management: Protocol*, September 2015, [Online]. Available: https://tools.ietf.org/html/rfc7644. [Accessed 22 August 2016].

[43] *Authentication and Authorization for Constrained Environments*, [Online]. Available: https://datatracker.ietf.org/wg/ace/documents. [Accessed 22 August 2016].

[44] *RFC 7252 Constrained Application Protocol*, [Online].
Available: http://coap.technology. [Accessed 22 August 2016].

[45] [Online]. Available: http://mqtt.org. [Accessed 22 August 2016].

[46] [Online]. Available: https://www.predix.io/docs#Jig2gorb. [Accessed 22 August 2016].

[47] *OAuth 2.0 Proof-of-Possession (PoP) Security Architecture draft-ietf-oauth-pop-architecture-07.txt*, December 2015, [Online]. Available: https://tools.ietf.org/html/draft-ietf-oauth-pop-architecture. [Accessed 22 August 2016].

[48] Cloud Security Alliance, *SDP Specification 1.0*, 2014.

[49] KAWAI, H. et al., *Access Authentication Solutions – Providing Flexible and Secure Network Access*, NEC Technical Journal, 2014, vol. 8, no.2.

[50] *Robot Revolution Initiative*, [Online]. Available: https://www.jmfrri.gr.jp/english/info/256.html. [Accessed 22 August 2016].

[51] Industrial Value Chain Initiative, *Industrial Value Chain Initiative Flyer English*, [Online]. Available: https://www.iv-i.org/en/docs/IVI_Flyer_English.pdf. [Accessed 22 August 2016].

[52] IEC MSB, *IEC White Paper Factory of the future*, 2015, [Online]. Available: http://www.iec.ch/whitepaper/pdf/iecWP-futurefactory-LR-en.pdf. [Accessed 22 August 2016].

[53] Hitachi Ltd., *Production Control System to Visualize Future Effects by Production Trouble*, Hitachi Review Vol.61 (2012), No.6, 2012.

[54] Hitachi Ltd., *An Anomaly Detection System for Advanced Maintenance*, Hitachi Review, vol. 63, no. 4, 2014.

[55] Hitachi Ltd., *TSCM Cloud Services for Implementing the Global Mother Factory Center Concept*, Hitachi Review Vol.64 (2015), No.5, 2015.

[56] Reliability Centered Energy Management, *Failure Mode Driven Maintenance Strategy*, 2011.

[57] *European Smart Cities*, [Online]. Available: http://www.smart-cities.eu. [Accessed 22 August 2016].

[58] SICILIANO, B., KHATIB, O., *Springer Handbook of Robotics*, ISBN: 978-3-319-32550-7.

[59] CHRIYADAT, A., RADKE, R. J., *Detecting Dominant Motions in Dense Crowds*, Topics Signal Processing 2, 4, pp. 568-581, 2008.

[60] HAILEMARIAM, E., GOLDSTEIN, R., ATTAR, R., KHAN, A., *Real-Time Occupancy Detection using Decision Trees with Multiple Sensor Types*, in Proceedings of Symposium on Simulation for Architecture and Urban Design (SimAUD'11), 2011.

[61] VAN DER VEER, H., WILES, A., *Achieving Technical Interoperability – the ETSI Approach*, ETSI, 2008, 3rd Ed.

[62] IEEE, *IoT Scenario and Use Cases: Social Sensors*, IEEE IoT Scenario submitted by IEEE, 2016.

[63] IEEE, *IoT improving journey experience in public transport for passengers with special needs*, IEEE IoT Scenarios submitted by ATOS Research and Innovation.

[64] 3GPP, *Service requirements for the Evolved Packet System (EPS), Version 13.3.0*, 2016-06.

[65] *NEC becomes first supplier to integrate semantic interoperability for IoT platforms*, [Online]. Available: https://www.fiware.org/press-coverage/nec-becomes-first-supplier-to-integrate-semantic-interoperability-for-iot-platforms-technology-to-be-demonstrated-at-the-etsi-m2m-workshop-2015-from-9-11-december-sophia-antipolis-france. [Accessed 22 August 2016].

ISBN 978-2-8322-3593-5

CHF 50.-

International Electrotechnical Commission®

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC WP IoT Platform:2016-10(en)