IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D2.2
Consolidated business needs

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

© Copyright 2019, the Members of the IoT4CPS Consortium

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Document Control

Title: Consolidated business needs
Type: internal
Editor(s): Peter Priller (AVL)
E-mail: peter.priller@avl.com
Author(s): Edin Arnautovic (TTTech), Mario Drobics (AIT), Michael Jerne (NXP), Markus Krainz (AVL), Martin Matschnig (Siemens), Katharina Kloiber (X-net), Denise Ratasich (TUW), Christos Thomos (Infineon), Omar Veledar (AVL), Heinz Weiskirchner (Nokia)
Doc ID: IoT4CPS-D2.2

Amendment History

Version	Date	Author	Description/Comments
V0.2	29.06.2018	Peter Priller / AVL	Initial version prepared
V0.3	30.8.2018	Markus Krainz / AVL	Included process description and content from asset collected
V0.4	10.9.2018	Peter Priller / AVL	Updates in multiple chapters, added missing parts
V0.5	17.9.2018	Denise Ratasich / TUW	First Review; added feedback
V0.9	10-11/2018	Edin Arnautovic / TTTech Michael Jerne / NXP Katharina Kloiber / X-Net Martin Matschnig / Siemens Peter Priller / AVL Christos Thomos / Infineon Heinz Weiskirchner / Nokia	Integrated individual chapters on business needs
V0.99	27.11.2018	Omar Veledar / AVL Peter Priller / AVL	Added automotive overview; final editing of document
V1.0	29.11.2018	Peter Priller / AVL	Integrated review feedback from Denise Ratasich und Mario Drobics
V1.1	06.03.2019	Mario Drobics / AIT	Formatting

Legal Notices

The information in this document is subject to change without notice.
The Members of the IoT4CPS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IoT4CPS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

FFG
Forschung wirkt.

Content

1. Introduction

This document was created as deliverable D2.2 by members of work package 2 (*Use-Case Objectives*) of the IoT4CPS project, with the goal to report the outcomes of Task 2.2 (Business needs consolidation).
Industrial partners of IoT4CPS defined several use cases in their domain believed to benefit significantly from advances in secure, trusted (I)IoT. A brief analysis of these use cases and derived business needs of the opportunities addressed shall allow to focus research and development activities of IoT4CPS, by this the consortium intends to maximize the impact and exploitation potential or IOT4CPS' results.
The pivotal technology requirements are identified and will be addressed further on in WP3 (Safety & Security Design & Methods), WP4 (Security Verification and Analysis) and WP5 (IoT Lifecycle Management) respectively. The use cases, business models and needs are quite diverse within the consortium. This is both challenge and opportunity, as it allows the project to cover a wide range of requirements and technologies in the IoT domain, strengthening its position as a lead project. To cluster activities appropriately, and to better understand relations to and between the desired solutions, all these business needs were categorized and mapped along (I)IoT standard architectures [1]. The outcomes will be validated in selected use cases: WP6 (Use-Case Applications in Automated Driving) and WP7 (Use-Case Applications in Industry 4.0) will host the prototypical implementation and integration of the research results in the industrial use cases and allow continued validation during the project.

1.1 Motivation

The project proposal [2] includes the main rational of IoT4CPS: to work on guidelines, methods and tools to enable safe and secure IoT-based applications for automated driving (AD) and for smart production (Industry 4.0 or I4.0). To rapidly move ahead the consortium will prioritize and address the most relevant needs. In this first phase of the project the concrete business needs and contexts are analysed and described as a base for the project work. This includes a brief summary of the use case / opportunity addressed by the industrial partners in IoT4CPS, and a refinement of the focus topic(s). The pivotal technology requirements to be addressed in WP 3..5 are highlighted, with an emphasis on security aspects. Each use case includes a brief rundown of the business case. A mapping along the IoT4CPS-Reference-Architecture / Business Viewpoint allows localizing the need along the value chain (i.e. component builder / system builder / operational user and specific role). Consideration is given to the fact that there might be different roles of an entity in parallel (e.g. a manufacturer can be operational user of production equipment, but also component builder for automated driving).

1.2 Objectives of Task 2.2 (Business needs consolidation)

Task 2.2 was structured in two steps:

In the first step, partners specified use case and context along the application areas of this project (automated driving and Industry 4.0), to be demonstrated later on in WP 6 and 7. Therefore a process and suitable supporting tools/infrastructure were defined, embodying some initial requirement engineering phase. Results of this step include a list of use cases, requirements and contexts as recommendations for WP3, WP4 and WP5.

Industrial partners of IOT4CPS described relevant use cases within the two main application domains at a high level, to be further refined throughout the project within WP 6 and 7. Each use case is complemented by its context information, including its relevant cybersecurity threats, relevant data (structure) involved and technology/implementation constraints. This shall support an efficient analysis and targeted design of solutions for these needs in the technology work packages (WP 3-5). Outcomes are described in Section 2.

During the second step, each industrial partner described the business context for the use case, including business motivation, reasoning and potential business models. Together with D2.1 (state of the art), this shall set the stage for WP3, 4 and 5 to come up with solutions that fit the needs of related users (e.g., professional user, citizens, organizations, government), regulation, business practices and markets. The findings for the addressed use cases are presented in Section 3.

2. Process Overview

2.1 Initial Requirements

WP2 / step 1 was done along the process depicted in Figure 1. The assets are defined from (1) use-cases, via (2) requirements, threats, context material and data sources, to (3) the actual building blocks. Finally, the inputs are reviewed (4), to remove potential overlaps, gaps, or ambiguities. The process was defined by WP2 partners at the beginning of the project. It is designed to be done iteratively, as use-case owners will review on a regular basis the results and update information when necessary.

2.1.1 Use case and context analysis

The main goal of the analysis was to describe exemplary use cases around Industry 4.0 and Automated Driving relevant to IOT4CPS, applying standard requirement engineering procedures. Industrial partners of the project (AVL, IFAT, NOKIA, NXP, SAGÖ, TTTech, and XNET) in their role of use case owners therefore defined project-relevant UC and *related information*.
The *related information* is structured into 3 different types:

- Implementation context

  e.g. specific technology used in the domain, like standard operating systems, software stacks etc., as well as standards that need to be met
- Requirements

  specific functional or physical needs
- Data sources

Then use-case owners and technology providers cooperated to specify known threats applying to specific use cases. WP2 does not include specific threat analysis or modelling activities, therefore known threats from previous work and/or information from available systems already in use were consolidated by the partners.

2.1.2 Relations to other work packages

In a next step, technological building blocks and demonstrators were specified in their relation to the use cases. These links shall allow traceability throughout the project, from the concrete business needs, to requirements, to development of technologies and methods, to integration and finally to verification and validation (V&V) of the solution. V&V and dissemination are strongly supported by demonstrators, which are described in WP2's process and infrastructure as well. Demonstrators are prototypes to be implemented during the project; this is typically done within WP6 and 7.

2.1.3 Process Description

The main process is depicted in Figure 1.

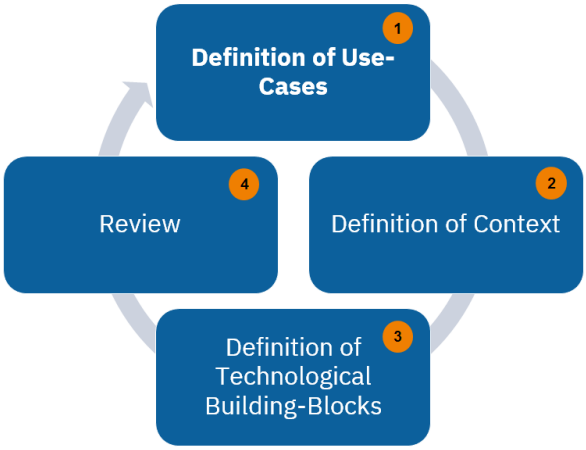

Figure 1: Iterative Requirement Engineering Process

2.1.4 Representation of Results

Results of the process described above were gathered and captured along a structure depicted in Figure 2. The use of standard requirement engineering tools normally used in industry (e.g., Atlassian JIRA, IBM Doors) was discussed in the consortium. However, agreeing on and setting up such tool in a commonly accessible infrastructure for all partners proofed to be out of scope for this project.

Thus, capture and management of WP2's results were done by specifically designed web forms and collections on Microsoft SharePoint, hosted by AIT. This proved to be well-accepted by partners. Standard features of the platform like relations and versioning allowed efficient management of the assets.

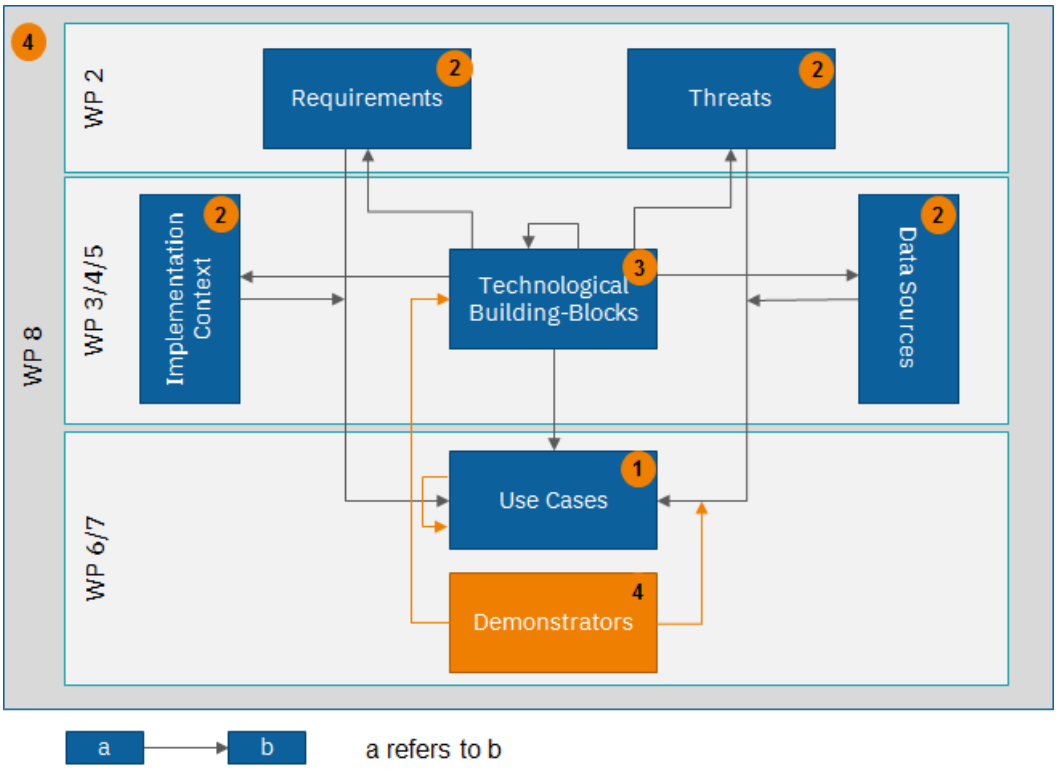

Figure 2: Structure to capture IoT4CPS assets

2.2 Reference Architecture

The consortium of IoT4CPS is comprised of multiple industrial partners active in different industrial domains. Therefor the business needs collected proved to be quite heterogeneous, covering a wide range of challenges, technologies and approaches. To better structure the input and in order to allow WP3, 4 and 5 to better understand needs and identify clusters, use case owner needed to map use case and applied technologies against standard architectural schemes.
The proposal [2] already includes an overview of current standard architectures in the IOT range. Based on this state of the art and detailed discussions in WP2 a set of reference architecture documents was defined and documented in [1]. Use case owners were requested to relate UC and context (specifically the system described with its main parts) to corresponding schemes listed in [1]. This enables the mapping to and designing of technology building blocks more easily, especially, if the UC contains many application or domain specific vocabulary and assumptions. It shall also allow gaining a more abstract view on the use cases to better understand the needs, and thus allowing to define a more detailed focus of WP3, 4 and 5.

2.3 Specific Requirements & Business Needs

In step 2 of Task 2.2, the business context was analysed and described by the industrial partners. The summary includes

- Business Motivation and Reasoning
- Alignment to Industry and Research Roadmaps
- Concrete technological needs along
    - T1) Safety & Security Design & Methods
        - T1.a) Dependability Design methods for IoT
        - T1.b) Resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT
        - T1.c) Scalable and efficient crypto algorithm for IoT
    - T2) Security Verification & Analysis
        - T2.a) Strategic Security Assurance
        - T2.b) Analytical Toolbox
        - T2.c) Operational Security Assurance
    - T3) IoT Lifecycle Management
- Related Standardization

Table 1 provides an overview of the business needs in use cases described by the industrial partners of IOT4CPS:

Partner	Described Topic
AVL	Security verification along the full life cycle of IoT-based industrial instrumentation systems
IFAT	Trustworthy radio connectivity solutions in smart production use-cases
NOKIA	Communication between CPS entities and the relevant components
NXP	Integrity and Authenticity Check of Complex Systems
Siemens	Recommender System for industrial IOT applications
TTTech	Secure and Safe Platform for Automated Driving
X-net	Security by Isolation / Production of IoT devices

Table 1: List of use cases analyzed for business needs

3. Business Needs

3.1 Initial Requirements

Results are hosted at AIT's SharePoint, see [3]; requirements are structured along the following use cases (Table 2)

Use Case Title
[Main] Industry 4.0
[Main] Automated Driving
Secure Boot for Smart Hub
Update SmartHub Kernel
Connected Vehicle
Connected Test cell
SmartHub Security Testing Methodology and Framework
Secure WSN-based instrumentation in production environment
Level 3 Automated Driving
Level 4 Automated Driving
Connectivity mechanisms for autonomous and collaborative production entities in smart manufacturing environment
Secure information exchange for production management using Digital Twins concept
Traceability of components and systems throughout life-cycle
Fleet monitoring (AVL-DRIVE)

Table 2: Use Cases

3.2 AVL: Security verification along the full life cycle of IoT-based industrial instrumentation systems

Vision: establish security verification along the full life cycle of IoT-based industrial instrumentation systems (I4.0). This includes testing accompanying development, monitoring during operation, and verification covering maintenance and system evolvement cycles.

3.2.1 Context

Automotive powertrain development needs to address global concerns, especially CO2 reduction, sustainability and commercial competitiveness. A major part in the development process takes place in test factories, to explore, verify and optimize new designs. A typical test system (e.g., a powertrain test bed), is comprised of a multitude of systems (e.g., exhaust gas analyzers, actuators, stimulation/instrumentation/automation systems), typically communicating locally via standard SCADA means like field busses. More and more such devices and subsystems provide independent, additional communication links to external systems, like smart/predictive maintenance services implemented in clouds. AVL Device.CONNECT™ provides such connectivity to a multitude of AVL products like gas analyzers, particle samplers, instrumentation systems etc. and is therefore the base of AVL's contribution to the Use-Case "Applications in Industry 4.0" in WP7.

A mapping along the IIRA viewpoints [IIC-RA] of this use case results in

1. Business: B2B products (HW and SW of devices) and services (e.g. smart/predictive maintenance)
2. Usage: professional user (e.g. test bed engineers), however not necessarily IT/Cybersec experts
3. Functional: providing secure connectivity to external (cloud) services, independent of internal (SCADA) communication
4. Implementation: AVL Device.CONNECT

Note: a detailed description of Device.CONNECT™, applying threat models and usage scenarios are not in scope of this document, and will be discussed in the respective work packages.

The business viewpoint according to [IIC-SF] can be defined as AVL being the system builder, using/integrating components of vendors (including IOT4CPS partners like NXP and Infineon), providing a product (e.g. an instrumentation system with integrated Device.CONNECT) to a customer (acting as operational user).
However, AVL's role is unique in a way that additionally its powertrain engineering unit (PTE) acts as internal customer to these products developed by the instrumentation and test systems unit (ITS). This allows to have direct access to use/operational data in house.

Trust requirements (according to [IIC-SF]) can be summarized as

1. Security: systems need to provide appropriate level of protection of hardware, software and data, as well as from disruption or misdirection of the services they provide
2. Safety: according to applicable standards, especially in the presence of human operators (see WP7)
3. Reliability: test devices need to run 24/7 in sometimes un-supervised mode; any failure in availability might result in significant cost increases (e.g., unused resources of test factory)
4. Resilience – aligned to reliability test
5. Privacy: typically of less concern, as these devices do not have access to or collect personal traceable information.
   However, confidentiality (e.g. of measurements data) is a major concern, as it might be valuable information about new innovations of an user (e.g., new engine design), considered as valuable trade secret.
6. Trustworthiness: customer/user needs to have reason to trust in appropriate security and dependability to enable and use the functionalities (e.g., smart/predictive maintenance) provided by the external connectivity of the systems.

Mapping to the IoT RA system deployment [IEC-UC] can be described as

1. Physical Entity Domain (PED): unit under test (UUT, e.g., automotive powertrain), test bed setup, media conditioning (fluids, air, energy…) etc.

2. Sensing & Controlling domain (SCD): sensors (temperature, pressure, torque,) and instrumentation systems; complex measurement devices like exhaust gas analyzer etc.
3. IoT Resource and Interchange Domain (RID): AVL Device.CONNECT
4. Application Service Domain (ASD): AVL Smart Service Framework (cloud-based)
5. Operations & Management domain (OMD): part of AVL Smart Service Framework, e.g. "Installed Base"
6. User Domain (UD): Smart Service Visualization (Web-based and mobile device apps)

From the technology perspective, the connectivity stack is comprised of (aligned with IIC-CF)

Information Layer	AVL SmartService Framework (partly using standard software tools like Cybernetes, Spark, ...)
Connectivity Layer	MQTT to/from the broker host placed in a DMZ TLS end-2-end AVL Device.CONNECT™
Networking layer (from Smart Hub to Broker)	Ethernet, mobile networks Standard IP

3.2.2 Business Motivation and Reasoning

Having a multitude of such test devices delivered and operating within globally distributed test factories of AVL customers, it is our responsibility to assure cyber-security throughout the full life cycle.
As described, devices might communicate via public networks (mobile network providers, Internet) to multiple cloud services, while at the same time having internal links to SCADA systems as well. This might expose them to serious threat scenarios, e.g. attackers from the outside trying to break through such AVL device into the internal networks of our customers. An additional constraint is the long life cycles of such industrial devices, typically increasing 10 years, in some cases even 20 years of operating time. It is therefore of major concern to

- Establish
- Monitor
- Continuously update if necessary

the security measures of these devices. This in combination with potential functional extensions/updates requires comprehensive security testing and awareness for each system and combination of HW/SW.
Failing to provide or maintain reliable security meeting appropriate standards could be a major disabler for AVL's business and is therefore a high priority in our development and QA processes.

3.2.3 Alignment to Industry and Research Roadmaps

There is a good alignment with Austria's Industrie4.0 R&D strategy, specifically with topics "Cyberphysical Systems" (CPS) and "Geschäftsmodelle" outlined in chapter 3 of [4]. In the CPS topic (chapter 3.5, p.27), AVL's use case fits into sector: Manufacturing, and follows the reasoning "requires: Design Methodology: Validation and Verification" with the focus on "Cybersystems --> {Resilience, Privacy; Malicious Attacks; Intrusion Detection}

In this category, [4] states as research needs (translated):
Privacy, trust, security: The application of CPS in different sectors raises new questions about privacy, trust and security. Among other things, the disclosure of information from the cyber-physical-social space may require new rules for the accessibility and transparency of information. In addition, new types of physical and cyber-physical attacks are possible, e.g. in the context of intelligent and networked factories. This results in a need for new concepts and tools to ensure and increase cyber security.
[..]
Verification, testing (security), certification and guidelines: CPS require new approaches for verification and for tests to detect potential events, such as physical or cyber-related errors due to comparison with defined standards to check and adjust. For this purpose, a detection, learning and argumentation module needs to be developed in order to ensure the accuracy of decisions and learning on the basis of historical data to promote the development of the country. To promote the application of CPS in various industrial sectors also requires the handling of security certifications - such as the identification of sources of danger and how to deal with them in agreement with legal requirements for health and safety at work.

3.2.4 Mapping along the Reference Architecture

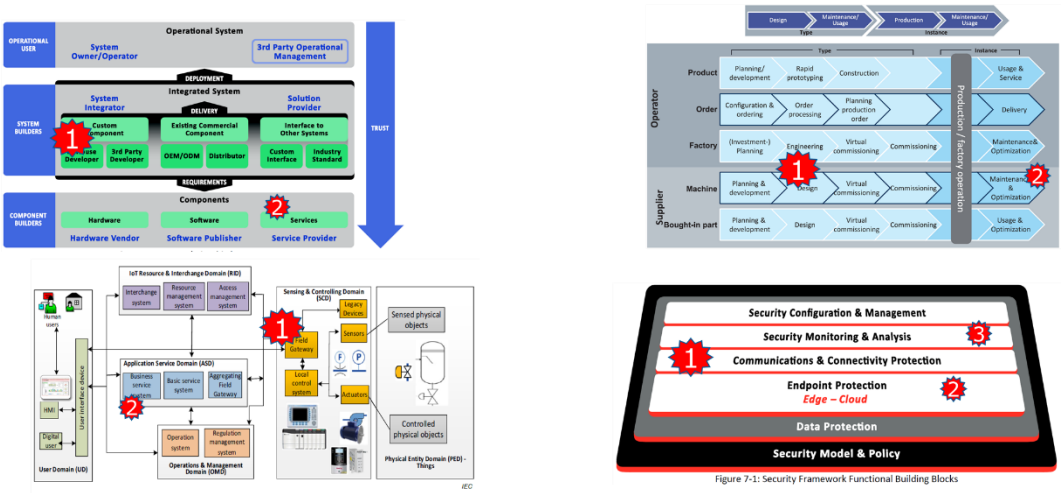

Figure 3: Mapping[1] of AVL's Scenario towards [1]

3.3 AVL: IoT for the Connected Vehicle

3.3.1 Context

The main complexity of the IoT value chain is reflected in potential internal permutations. The classic value chain examples are represented by a) the full vertical solution being provided by a single organisation and b) individual providers being responsible for each link within the chain. However, the complexity arises when organisations stop adhering to these stereotypical models and start blurring the boarders throughout the value chain. The size and complexity of the task is likely to prevent single providers from becoming experts in all necessary aspects of the value chain. Equally, the ability and interest of different providers to cross the predefined borders (especially when application development is in question) and adapt solutions to their own needs, evidently generates a multitude of possible permutations within the chain itself.

[1] number in star indicates priority, with '1' being most important

Devices either provide data or react to the input data. The *connectivity solutions (network)* control the data flow through the IoT network. The *platforms* enable system integration and data handling (storage, processing or management). They also offer interface to the *applications*, which merge the capabilities of all assets and present them to the *end user* as an IoT application.

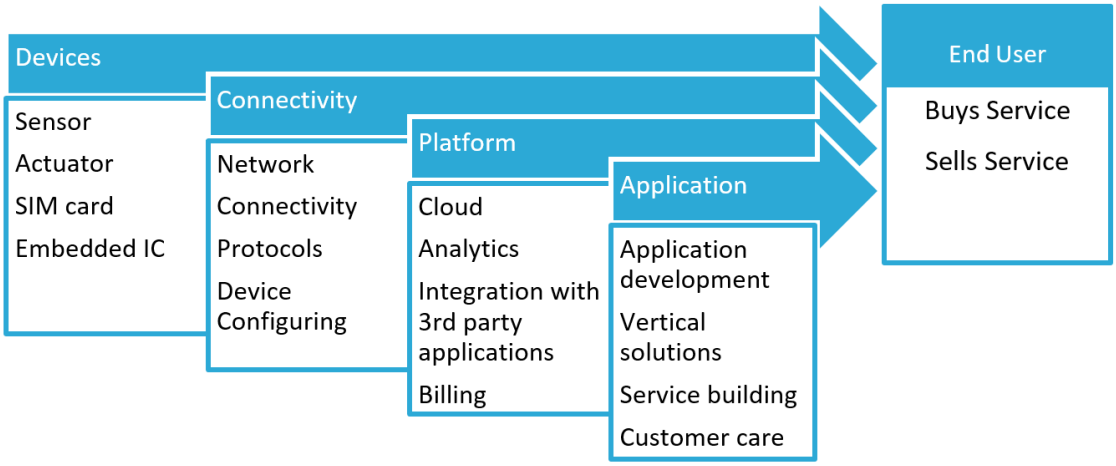

Figure 4: IoT Value Chain

Considering the potential of the IoT value chain, it is unlikely that major automotive players are going to become connectivity technology providers and such solutions ought to be left to the organisations with core competences in the field of telecommunications. IoT solutions are hence likely to either a) support the existing automotive business models by making them more efficient through faster and better-quality decision making, or b) be the means to generate innovative service-based business models capable of increasing the competitive edge and consequently capturing additional value. The obvious choices for the support of the existing business models is remote calibration and predictive maintenance in terms of mobility and support for vehicle and instrument production in terms of manufacturing.

In the case of mobility application, the gathered data could also support new customer services and business strategies. The data collected from the in-vehicle instruments should carry sufficient level of information for improving and maintaining physical assets. However, the data exchange must be protected for three reasons:

- Confidentiality (vehicle manufacturers)
- Privacy (vehicle users)
- Safety (wrong data could potentially compromise the safety)

The radical shifts in the automotive industry's mobility solutions, places an even greater emphasis on data safety, which becomes especially critical when considering the potential applications of autonomous driving. Therefore, high level of security may not be compromised when considering the data exchange that carries information such as:

- Vehicle technical status (e.g. oil temperature, technical malfunctions)
- Vehicle usage parameters (e.g. velocity, location)
- Individual preferences (e.g. patterns of usage)

Private information (e.g. driver / passenger personal information)

3.3.2 Business Motivation and Reasoning

The core value of IoT is the possibility to make decisions faster. Further detailed analysis results with identification of several external drivers, which are directly influencing the need for IoT solutions. The societal pull and consequent market needs, as well as the technology push are the main forces behind the rising expectations. From the business perspective, the IoT solutions are generally expected to provide new revenue streams while forging stronger connections with customers. The end users are moving from requiring products towards longer lasting relationships with a good-quality uninterrupted service being the core of their expectations. A consequence is that the IoT solutions are envisaged as an enabling factor for new business models, based on selling services instead of solutions. The strong bond to the end user is to support sustainable businesses future.

Simultaneously, looking inwards, the offered IoT solutions are promising to deliver improvements in terms of operations. The envisaged benefits are mainly heading through efficiency increase towards cost reduction, be it through slashing the costs of operations, introduction of predictive maintenance, optimised utilisation, creation of smart cities etc. IoT solutions are to impact the businesses, not by breaking up from the past, but by revolutionising decision-making processes. The vast information gathering activities in combination with the trained decision-making processes are expected to contribute towards (economic) growth by allowing better-quality decision making. The anticipated deliverables are to contribute to improvements in integrity, safety and security.

3.3.3 Alignment to Industry and Research Roadmaps

The market behaviour towards automotive IoT solutions is in line with the policies conducted by the European Commission. The objective of their Deployment Platform for Cooperative Intelligent Transport Systems (C-ITS) is to create a shared vision on deployment of connected vehicles [5]. Their policy recommendations are based on predicted usage of connectivity infrastructure in the future. The conclusion is that the maturing technology is creating the need for urgency as the industry is heading towards automotive connectivity [5]. The benefit maximisation is possible through the offering of full range of services and it highly depends on sufficient uptake [5].
The financial consideration of the automotive connectivity [5], [6] predicts considerable economic growth if accelerated deployment is conducted. The EC's funding activities are therefore, directed towards increased cooperation across sectors and disciplines to promote connectivity solutions. The chosen direction, which is orientated towards providing solutions to the immature market calls for subsidised commercial application. The EC's is promising to cover the gap between the current infrastructure and the network that is required for a successful commercial deployment [6]. The support is a part of Horizon 2020 'Smart Everything Everywhere' initiative, riding the next Internet wave (i.e. IoT) by integrating networked electronic components and systems in any type of product, artefact or goods [7]. The support of public funds is unlikely to fade, as the expected funding framework is aiming at maintaining the continuum for the digitalisation strategy, as "*Digitalisation enables people to get the best service at highest level of comfort and safety*" [8]. Therefore, connectivity is in high pursuit by the European policy-makers as it is a building block for future of mobility.
At the country level, the relevant Austrian roadmap prescribes connectivity reliant ADAS and AD solutions as building blocks for success within automotive industry [9]. The intelligent driver assistance functions and highly automated driving modes are singled out as the prime targets for

the mid-term research. The roadmap's long-term determination envisages driving automation geared towards safe road operation with no need for human intervention [9]. Hence, the fast and good quality decision making integrated into autonomous vehicles, in combination with the vehicle to anything communications, are identified as crucial components of future automotive development.

3.4 IFAT: Trustworthy radio connectivity solutions in smart production use-cases

This topic relates to the main Use Case 2 – Secure IoT for Industry 4.0 – Secure Connectivity.

3.4.1 Context

Trustworthy connectivity will provide the physical security to protect the information flow within an industrial network and between its endpoints. This requires low-complexity, low-cost and low-power implementations of hardware components for the transceivers (component builders) of both mobile connected manufacturing equipment and wireless backbone infrastructure (device/system builders), as well as dependable, secure, and resilient end-to-end Industrial IoT platform solutions (system builders). The latter includes enhanced industrial automation networking technologies and analytics software/services (cloud/edge) for monitoring and maintenance purposes. It shall offer an ubiquitous platform to extensively interconnect different types of industrial devices (sensors, actuators, robotics, machinery, control systems, tools, wearables, materials, etc.) with people, enterprise systems, and business processes.

Several application areas are distinguished for factories of the future, namely, factory automation, process automation, human-machine interfaces (HMIs) and production IT. These systems rely on the timely availability of large amounts of data from the production processes. Smart production use-cases that will benefit from secure and reliable connectivity solutions might include scenarios for time-critical in-factory process optimization, non-time critical in-factory communications, remote control of equipment, intra-/inter- enterprise communications and connected goods. Based on this context, business needs are multifaceted and consist of major use-cases such as condition-based monitoring, remote access and predictive maintenance based on sensor data and big data analytics, zero-defect manufacturing, industrial building automation, autonomous and collaborative robotics, manufacturing customization, plug-and-produce for production line efficiency, real-time location systems and asset tracking, inventory management, augmented reality and smart glasses, wearables, connected goods during product lifecycle etc. In any of these use cases and scenarios, the generation of vast amounts of data (not only big data but also in some cases thick data) from devices that previously have been isolated or totally unconnected will allow new and unique insights to be found that will help production optimization, productivity gains, greater flexibility, enhanced safety and offer many new growth opportunities.

3.4.2 Business Motivation and Reasoning

The strong trend of re-industrialization leveraging ICT evolution and technological innovations (IoT technology, cyber-security, cloud solutions, edge-computing, big data analytics, artificial intelligence, 3D-printing, advanced materials, etc.), the necessity for flexible and modular production systems with more mobile and versatile production assets, fundamentally requires powerful, secure and reliable connectivity in order to enable the promise of diverse smart factory use cases that will make up an Industrial IoT environment. This kind of connectivity must be offered in all types of integration, namely horizontal (inter-industrial value and supply chains), vertical (connected factories) and end-to-end (lifecycle management) integration.

As new smart factory technologies (i.e. edge computing, devices for augmented reality and wearables, enhanced networks, asset tracking technology, collaborative robotics, etc.) are also being adopted in the manufacturing environments of the component and device builders, they can also benefit from secure end-to-end industrial IoT connectivity (operational users), as long as the operational investment leveraging of such hardware, software and services solutions is not disruptive to their existing manufacturing/production operations and can be incrementally acquired. To achieve Industry 4.0 vision, a seamless and effective integration of different reliable connectivity solutions under a secure, dependable and resilient Industrial IoT platform is fundamental for efficient, connected and flexible factories that can realize true benefits and produce increasing financial and production incentives. These benefits are best achieved when they are not hindered by obtrusive security controls and checks. Security is a huge challenge due to the increased connectivity and data accessibility that comes with the industrial IoT services.
Smart production markets constitute an ocean of opportunities for building hardware, software, and services strategy. However, IoT solutions must be centered around a hybrid cloud philosophy with leading service areas of edge computing, security, and smart workforce technologies. A security architecture with different management and operational characteristics must be offered against local and remote attacks to support the deterministic nature of communication and the scalability, efficiency and low-latency requirements of the industrial processes. The management of heterogeneity and co-existence of the enabled devices and systems that consist of different media, technologies, a fragmented set of protocols and services, different vendors of networked components, different implementation platforms and tools is a very challenging task.

3.4.3 Alignment to Industry and Research Roadmaps

Refer also to IoT4CPS Deliverable 5.1

In general, this scenario aligns along the Industry 4.0 platform as defined in the reference architecture RAMI 4.0. RAMI 4.0 includes security by design in its reference architecture, highlighting security as a precondition and an enabler of industrial transformation.
Naturally, the roadmap of 5G Infrastructure Public Private Partnership (5G PPP) applies to this use case as well, as a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions).
Additional information about related initiatives and projects are summarized in Appendix A: Initiatives and Activities related to Trustworthy radio connectivity solutions in smart production use-cases

3.4.4 Concrete technological needs

This focus topic (trustworthy radio connectivity) aligns to the Communications & Connectivity protection and Endpoint protection (Edge-Cloud) layers on the functional viewpoint of the industrial internet security framework. Data access for connected manufacturing equipment needs to include all options: onsite, private clouds, public clouds.

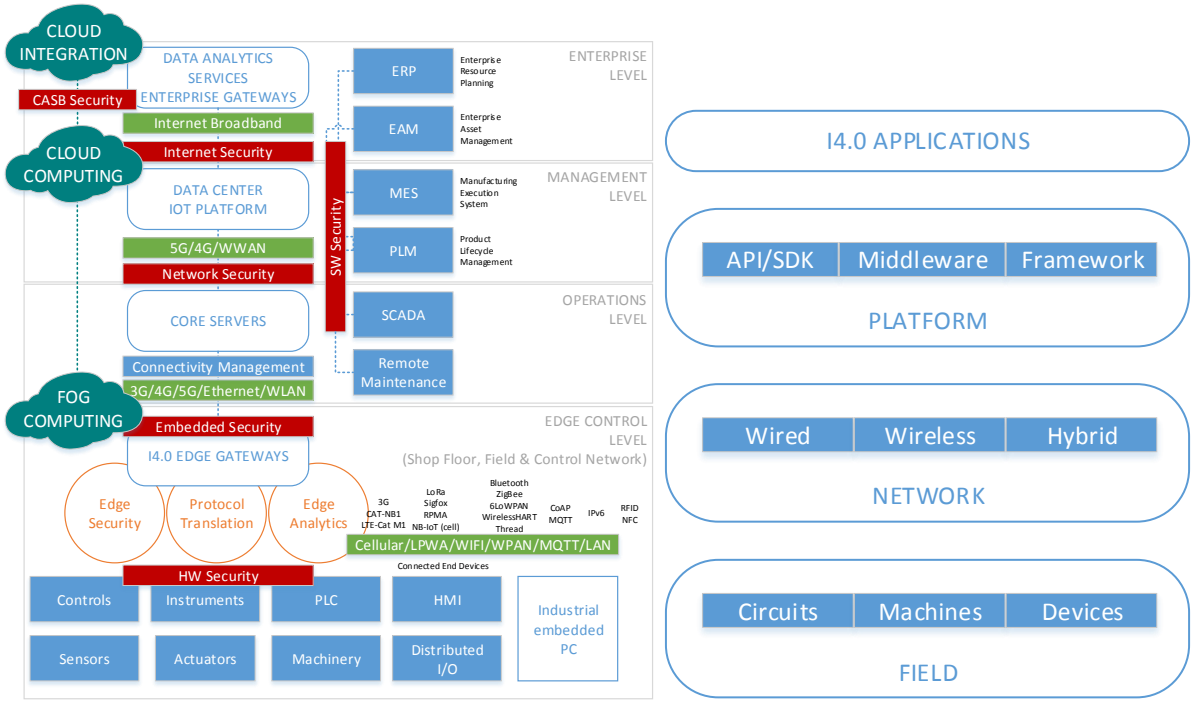

Figure 5: Trustworthy radio connectivity solutions in smart production use-cases

The requirements and the conditions for the communication system can vary from one use case to another. Such diverse requirements require high adaptability and scalability from a communication system which will have to support a seamless integration of different connectivity infrastructure and technologies depending on throughput, latency, security, dependability (reliability, availability, safety, maintainability, and integrity), scalability, accuracy, coverage, cost, flexibility and power consumption requirements. The communication network is expected to provide certain dependability guarantees independently of security. For a dependability assessment, the functions of the assets and the conditions under which these functions are to be performed must be specified. Most of the existing communication technologies fall short of the demanding requirements of industrial applications, especially with respect to end-to-end latency, communication service availability, jitter, and determinism. Real-time and continuous monitoring must be supported to avoid undesired interruption of the production processes. A communication system also must support the production facilities for a long lifetime (long-term availability). Private operation of the factory communication network should be supported and isolation from public networks must be guaranteed. Communication systems must consider the particularities of the industrial environments which is characterized of large metallic objects that cause very rich multipath conditions and potentially high interferences by the local machinery. Integrating and inter-operating typical internet technologies for constrained devices (IP, MQTT, COAP, etc.) in manufacturing specific data formats and protocol stacks (such as OPC-UA, Automation ML, OVDA, etc.) could also allow a plug-and-play concept.

HW security in the edge control level with integrated circuits, sensors and transceivers for the field devices machines must be able to address vulnerabilities of the HW such as replaying, relaying, Man-In-The-Middle (MITM) attacks, DDoS attacks, sniffing, eavesdropping, data corruption, interception, spoofing, and cloning. On the network level the risks of unauthorized access,

modification, and disruption, i.e., DDoS, MITM, malware infection, asynchronous attacks, zombie botnets, replay attacks, routing threats, SCA, and DPA must be considered. A combination of techniques such as, developing secure APIs, web, mobile and client applications, scanning and monitoring for vulnerabilities, safety and quality assurance, code reviews, security architecture evaluations, static and dynamic testing, might be needed in a platform level to reduce the risks. Automated testing for a wide range of interfaces to construct a minimal set of requirements that can be ported across applications it is also necessary to be implemented through continuous integration. On the application level, privacy and protection of data is important and issues of ownership, sharing and confidentiality of the collected data must be tackled.

Technological needs are broad and varied, from encryption, certification and key management, hardware anti-tampering security modules, embedding security, trusted computing, network security and monitoring, processes for secure software development, provisioning authentication and access control policies, trust management and secure OTA updates and patches, data protection and privacy guarantees, secure design and product development, product security through lifecycle management, secure protocols, audits and security assessments, regulatory compliance and certifications. The possibility of updating devices after sales and during their lifetime gives them many new features and capabilities since vulnerabilities can be managed and mitigated via OTA and offer a continuous monitoring for improvements. Security must form a part of the inception process through agile development, application lifecycle management and DevOps to integrate it during the design, development and testing of the Industrial IoT applications.

Edge analytics technology that can detect the early signs of equipment underperformance and potential failure is an easy investment to make and it is very necessary for networks in industrial markets to lower communication costs through less investments in networking equipment and other physical infrastructure, and lower data storage costs as less data are sent to the data center.

Considering the three main security attributes, namely, confidentiality, integrity, and availability, the main concern in industrial environments is availability, confidentiality has in general the lowest priority. This is different than the concepts and solutions developed for typical office IT systems and applications focusing more towards confidentiality. Availability in industrial environments must be guaranteed for longer component lifetimes than used in IT (typically 5-7x more). Confidentiality is low to medium for the production floor and high for business-relevant and public space operations. Integrity requirements are always very high and of paramount importance. In vertical industrial IoT use-cases, security must be also regarded as a shared responsibility between infrastructure IT and OT operators, product suppliers, and system integrators. These actors require both secure products and a secure integration of products into systems and solutions and operate the industrial infrastructure according to the associated risks. This is enforced by directives, e.g. the NIS directive for critical infrastructures, and IT infrastructure risks are typically addressed by information security management systems (e.g. ISO27000 series).
The interfaces between security process responsibilities must come with requirements and target security levels (e.g. IEC 62433 and 62351) based on the intended operational use-cases. In that sense, security functions must be optimized to lower the communication resource consumption and increase the communication service dependability. It is also important that the security mechanisms must be supported for the life expectancy of the devices which is typically ten years or

more. Long-term security is an important topic and challenges arise, since in many industrial environments, updates can be installed only during planned service periods (typically once a year and for about one week). In that sense, the devices should be upgradable (patched with firmware, security algorithms and keys). Adding or removing devices from the secure network may involve access management systems that require action both from the device as well as the network side. The general trend for authentication and verification is to be achieved using the EAP framework. Reduced lifetime of battery-powered devices and limited real-time capability must also be considered when connecting industrial IoT devices. In such deployments, security could reduce the life time of these devices or deteriorate experienced dependability parameters. Current encryption mechanisms like authenticated encryption for protecting confidentiality typically also come with integrity protection mechanisms. However, to reduce the end-to-end communication, latency encryption mechanisms may be not activated and thus communication integrity might be compromised. This must be taken also into consideration in the design of security mechanisms. Suitable solutions for cloud-based security that support scalable generation, distribution and revoking of security certificates are still missing.

3.4.5 Related Standardization

Within the IoT ecosystem, there is a drive to develop specifications to address compatibility and interoperability between the many different technologies being used, from connectivity protocols, to operating systems and hardware modules. The industrial IoT ecosystem is still at its infancy, and technical standards development will take some time. However, there are numerous IoT specifications with security elements in their design that have been standardized by internationally recognized standards bodies, such as the IETF, and other dominant specifications, which are becoming de facto standards.
On a more abstract and technology-independent level, many industrial domains have established regulations and standards, addressing integration, functional safety (e.g., IEC EN 61508), operations and IT security (e.g. 'ISO/IEC 27000 series), which apply for IIoT just as any other technology.

A detailed overview of related standardization can be found in

Appendix B: Standardization activities related to Trustworthy radio connectivity solutions in smart production use-cases.

3.4.6 Mapping along the Reference Architecture

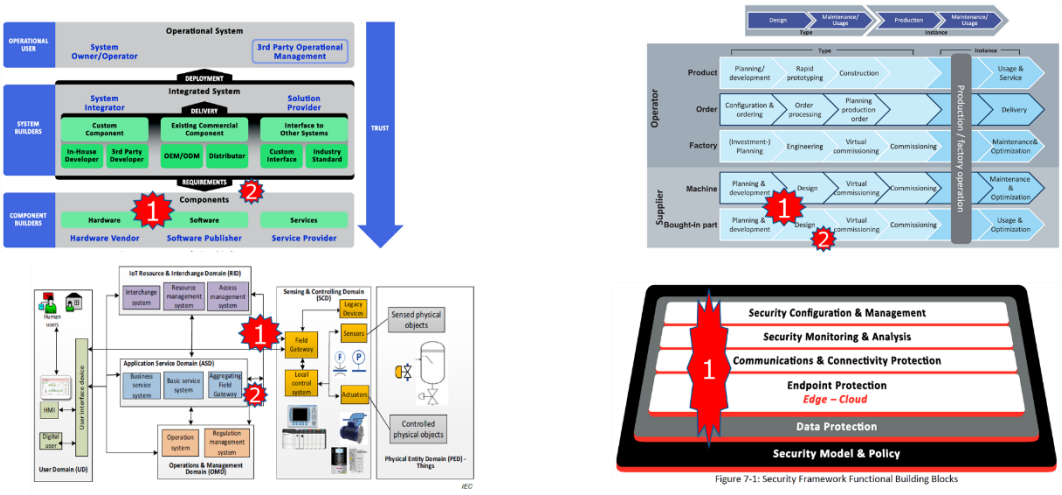

Figure 7-1: Security Framework Functional Building Blocks

Figure 6: Mapping[2] of IFAT's Scenario towards [1]

3.5 NXP: Integrity and Authenticity Check of Complex Systems

3.5.1 Context

This focus topic is related to the Industry 4.0 application domain of IoT4CPS and addressed within task T7.2 (traceability of components and systems throughout life-cycle). Results shall also be incorporated as far as possible into the overall Industry 4.0 demonstrator setup, as addressed by task 7.4.

Given the complexity of the topic and the comparably lean effort in IoT4CPS a focused involvement in WP3 – WP5 had to be chosen. Within IoT4CPS therefore a direct engagement of NXP is limited to WP4, task 4.1 (strategic security assurance). Where appropriate we also add requirements resulting from this use case towards other tasks in WP3- WP5.

From a value chain perspective results will feed into next generations of semiconductor components used for secure contactless connectivity solutions.

3.5.2 Business Motivation and Reasoning

Effective Industry 4.0 concepts build upon a set of "enabling technologies", one of them being efficient and secure traceability solutions. This applies to components and/or sub-systems and spans the whole life-cycle from production to operation and can include equipment and tooling aspects even during development. Radio Frequency Identification (RFID) has been used in the supply chain for many years and has proven to be a reliable and efficient solution for traceability and inventory purposes. Different technologies operating on various frequencies (low frequency/ high frequency/ ultra-high frequency) provide specific functionality, along with related advantages and dis-advantages in terms of environmental influences and connectivity behavior.

[2] number in marks indicates priority, 1 being most prior

Besides aspects of contactless performance and behavior (like range and speed of communication, channel characteristic…) security aspects have become more and more vital to ensure trustful implementations and broad deployment within Industry 4.0 environments. However, there are significant implementation challenges due to resource and energy constrained low power implementations of (passive) RFID systems, that are in principle controversial to the need for fast and high-level security algorithms.

Within the focus topic "Integrity and Authenticity Check of Complex Systems" a typical Industry 4.0 setup, in this case defined by a stationary test bed of the partner AVL, will be analyzed in terms of security threats, as they occur over the life-cycle. Focus will be on RFID-based integrity and authenticity checks, e.g. to conduct an initial inventory in a test bed environment to ensure completeness and authenticity of key equipment and components.
Aspects of transfer of trust (as parts will be moved and exchanged) are a vital part of the analysis.
Activities within IoT4CPS will focus on the security layer. Likely not all required combinations of security level and contactless technologies will be available at this point in time (resp. might be feasible at all). Improvements in the pure RFID-performance domain (power, range) are not in scope in IoT4CPS.

3.5.3 Alignment to Industry and Research Roadmaps

The following roadmaps and initiatives as listed at the end of this paper will be of relevance:
[4], [10], [11], [12], [13]

3.5.4 Concrete technological needs

Based on the different level of direct involvement of NXP in IoT4CPS tasks, we can define technical needs resulting from the defined focus topic resp. use case towards three groups of activities:
"Traceability of components and systems throughout lifecycle" and "Integrity and Authenticity Check of Complex Systems" shall be established and demonstrated in the industrial environment of an automotive test factory (e.g., powertrain test bed at AVL Graz). Solutions need to provide the required robustness in such "harsh environment" (e.g., interference, reflection, absorption, temperature and vibration conditions etc.)
For a holistic solution to be successful, there are several issues that need to be addressed in the context of configuration management and key management.

- Production can be done at a (semi-trusted) vendor
- SW & configuration distribution and update mechanisms
- Commissioning
- Operation
- Transfer of trust, e.g. in the context of part exchange, part update, fixing parts, sale/used parts
- Maintenance

Based on a concise description of the UC and the life cycle including a detailed analysis of all assets, the partners (AVL, NXP, TUG) need to perform a multi-stage joint risk and threat analysis. The different stages assume different levels of protection which must be employed. The risk and threat analysis will identify parts, where the available protection mechanisms are not withstanding certain attacks

based on the attack model. In such cases necessary protection requirements to achieve a desired level will be formulated.

“Strategic Security Assurance” will address the topic of HPC (hardware property checks) for side-channel attacks like the verification of masking solutions in close cooperation with TU Graz/ IAIK. Masked implementations of cryptographic protocols are central protection mechanisms to secure critical infrastructures against local physical attack scenarios, so called side-channel attacks. This is especially important if the ecosystem is not under full control and not all parties have the same level of trust.

This countermeasure to secure the implementation of cryptographic operations can either be achieved in HW or SW. HPC (hardware property checks) shall identify side-channel based anomalies. Additionally, other aspects like security-based code analyses and automated test case generation can directly be linked to the risk and threat analysis outlined in section 3.5.4 and substantially support the overall goal of a holistic and structured security approach. This may as well be used to identify functional, and communication anomalies in communication protocols.
IN addition we see potential input from the following tasks / work-packages to our Use Case, and therefore strongly suggest to stay closely aligned and continue to monitor the outputs from these tasks.

- WP3 – T3.1 (T1.a): Dependability design methods for IoT
  Requirements for installation and commissioning in life-cycle, improved measures for trust provisioning might prove to be an important input to be combined with the outcome of the risk and threat analysis in UC2.b.

- WP4 – T4.2 (T2.b): Analytical toolbox
  As mentioned already above, analytic tools based on novel methods from machine learning and other classification techniques might serve as a useful addition to any risk and threat analysis.

- WP4 -- T4.3 (T2.c): Operational Security Assurance
  Scanning network topologies and network data classification again is a meaningful way, which can be employed in the analysis of the UC2.b.

- WP5 -- T5.4 (T3.d): Identity, Security and Safety in Product Life Cycle Data Management
  Outcomes of this task might be used to increase the security in the configuration and commissioning phase of the life-cycle management of industrial IoT use-cases.

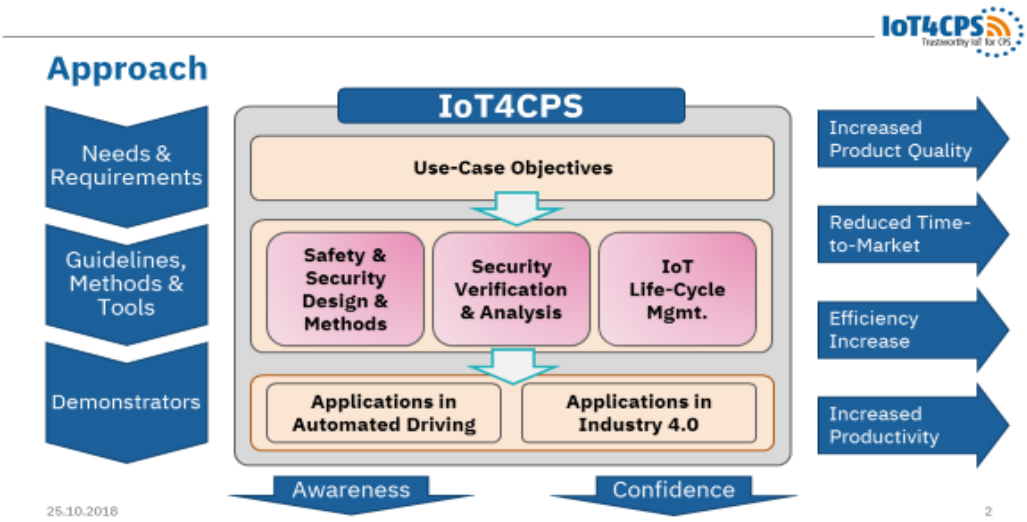

Figure 7: Scope c) for technological needs – Other tasks in WP3-5

3.5.5 Related Standardization

Obviously various RFID related standards are relevant in succeeding implementation steps; however, this is not the scope of the work in IoT4CPS, which focuses on the security layer.

3.5.6 Mapping along the Reference Architecture

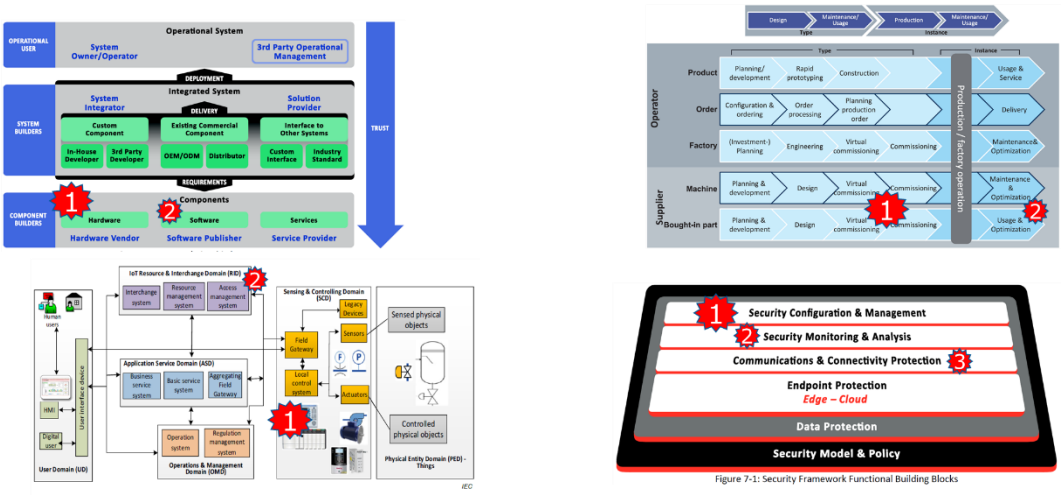

Figure 8: Mapping[3] of NXP's Scenario towards [1]

3.6 Siemens: Recommender System for industrial IOT applications

3.6.1 Context

In the past, IOT systems were typically used for consumer applications. In recent times, industrial IOT applications such as factory automation, building automation or grid automation get more and more important. In contrast to classical automation and communication systems, IOT systems are more flexible and typically cause fewer capital expenditures.

However, in different automation domains, there are demands of increased dependability. Depending on the use case different dependability features need to be considered. Especially for use cases in critical systems or for the automation of critical infrastructure (e.g. power grid) there are special requirements for a communication system.

In almost every industrial use case the lifecycle plays an important role. Systems in factory or grid automation typically have long life-cycles and require a continuous operation.

In contrast to that requirements, IOT systems and technologies hardly consider any dependability demands. While security gets more and more important for IOT systems, aspects regarding safety, reliability or availability are hardly considered. Also features such as determinism and bounded latency are typically not addressed by IOT technologies. Independent of that, the world of IOT systems is changing fast. According to different trends technologies become popular and a few years after they are hardly supported by vendors or manufacturers.

3.6.2 Business Motivation and Reasoning

To allow the application of IOT systems to critical systems or applications, the previously mentioned issues must be addressed. For example, if an IOT technology of a complex automation system should be replaced by another one, there shouldn't be too much re-engineering effort required. Instead, the system should dynamically be reconfigured automatically with a minimum of effort. The behavior of the overall system should not change in terms of global requirements. If a certification according to a

[3] number in marks indicates priority, 1 being most prior

certain standard exists (e.g. IEC 61598), it is desired that the certification process should require to be completely initiated; instead, the process of reconfiguration should prove the compliance.
As many technologies do not provide enough support for dependability even not for security in particular, there is also a need for using according mechanisms on top of common technologies. For example, if protocols do not satisfy demands regarding reliable data transfer, additional mechanisms must be applied to address this. If there are security requirements such as end-to-end encryption in a system using multiple protocols, additional measures must be applied.

Having a dynamic system or a dynamic configuration tool that is capable of dealing with the demands of the application and the system configuration as well as with the properties of the used or available technologies, would allow to apply IOT technologies even to systems with a long lifecycle. If measures can be applied on top of the systems independent of the underlying technologies, IOT technologies can replace even special communication and automation systems (especially in case of relaxed real-time demands). Since dedicated automation systems could then be replaced by IOT systems, the capital expenditures will decrease. Due to the flexible nature of IOT technologies also the operational expenditures can be decreased.

3.6.3 Alignment to Industry and Research Roadmaps

Bringing IOT technologies to automation is a general goal of Siemens. The needs are aligned with different internal roadmaps of the operating companies of Siemens.

3.6.4 Concrete technological needs

According to the requirements and expectations, mainly the task “T1a) Dependability Design methods for IoT” should provide the necessary technological basis. In the first step, a recommender system will be necessary that is capable of storing attributes of desired technologies in a machine-readable way. Furthermore, it should be possible to define the requirements of the desired system according to the use case. Based on these properties, it should be possible to derive a valid system configuration.

3.6.5 Related Standardization

As the needs do not target a specific use case in a specific domain, related standards can hardly be stated. In the different automation domains (e.g. factory automation, grid automation), there are several standards that must be fulfilled. For example, a very general standard in many domains is IEC 61508.

3.6.6 Mapping along the Reference Architecture

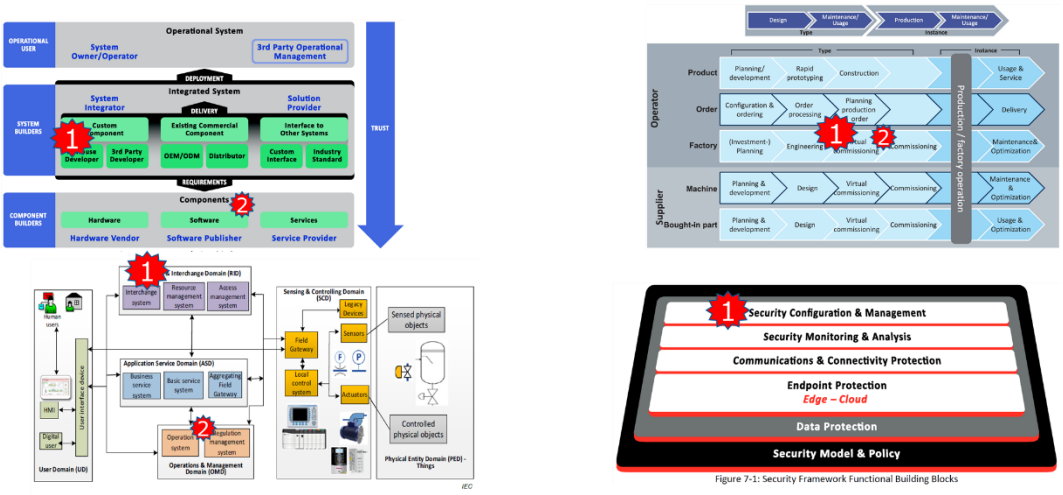

Figure 9: Mapping[4] of SIEMENS' Scenario towards [1]

3.7 TTTech: Secure and Safe Platform for Automated Driving

Vision: Provide an automotive platform for safe and secure execution of software functions for automated driving.

3.7.1 Context

Automated Driving (and ADAS systems) include complex functions for raw sensor data processing, sensor fusion, path planning, motion control, etc. The system integrator must develop, integrate and test such functions during the product development and ensure system safety and security. *Along the value chain*, TTTech positions itself as a hardware developer (typically without production), software provider as well as system integrator. In addition, it typically develops and delivers the system safety architecture. Although only remotely related, IIRA Business Viewpoint is *B2B*. The *Usage Viewpoint* would imply, for example, roles *function developer*, *system integrator, system tester,* etc (and associated Activities). The *Systems* are *Electronic Control Unit* (as the runtime hardware platform), *software middleware*, as well as development tools. In the Functional Viewpoint, *Entity Abstraction* and *Communication* are the most related and the *control domain.* In the Implementation, *Gateway-Mediated Edge Connectivity and Management* pattern is related to the focus topic.

For the trust requirements, the most relevant is safety. The automated driving platform must ensure ASIL-D capabilities. From the hardware point of view, current high-performance CPUs cannot fulfil such safety requirements and they must be combined with safety-related CPUs (e.g., Infineon Aurix) to enable overall high safety. Only with a sophisticated software middleware which enables hard real-time software execution and communication, overall system safety can be guaranteed.

3.7.2 Business Motivation and Reasoning

Every new generation of vehicles contain more and more functions in different domains (ADAS, infotainment, connectivity, etc.). While before every function was accompanied by a new electronic control unit, in the future this will not be possible. There is a trend towards consolidation and reduction of the number of ECUs and integration of several more-or-less related functions on a single,

[4] number in marks indicates priority, 1 being most prior

more powerful ECU. Parallel to this change, there is also a shift in the modes of collaboration between different automotive players. In the past, it was common that one supplier (typically a Tier-1) develops and produces a complete system containing software functions, software framework and ECU hardware. Today and in the future, OEMs are more flexible and chose the best (also fastest) independent suppliers of hardware and software and integrate the systems on their own or with the help of specialized system integrators. Such systems integrators can provide added value if they have frameworks to speed up and ease the system and software integration in such new technical and business environments.

3.7.3 Alignment to Industry and Research Roadmaps

The focus topic *Secure and Safe Platform for Automated Driving* is related to the Ecsel Roadmap "Multi Annual Strategic Research and Innovation Agenda for ECSEL Joint Undertaking" [12], most prominently to the objective 6 "Secure and strengthen a commanding position in design and systems engineering including embedded technologies." And the objective 7 "Provide access for all stakeholders to a world-class infrastructure for the design, integration and manufacture of electronic components and embedded/cyber-physical and smart systems.". The results of the research in the topic will be applied to the Smart Mobility application from this roadmap by developing the *capabilities* for Cyber Physical Systems as well as Safety and Security.

The focus topic is also aligned with the Austrian Research, Development & Innovation Roadmap for Automated Vehicles [9].It addresses the relevant automated driving, midterm and long-term scenarios for Level 3 and Level 4 automated driving (mostly for Automotive Domain Automated Vehicles but also for Off-Highway Domain Automated Vehicles). From the task fields of activities, it addresses *TF_1 System Architecture.*

3.7.4 Concrete technological needs

Concrete technological needs are to be developed are related to *T1.b) Resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT.* The developed patterns and architectures have to provide abstraction of underlying hardware and such the possibility for the customer to design scalable system architectures with high degree of application SW re-use. For the safety, it should implement different safety mechanisms, e.g, memory partitioning, timing supervision, protection of communication between applications, HW diagnostics and supervision. The fulfilment of the needs should be shown in UC1) Secure and Safe IoT for Automated Driving

3.7.5 Related Standardization

- Adaptive AUTOSAR
- SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"
- ISO 26262

3.7.6 Mapping along the Reference Architecture

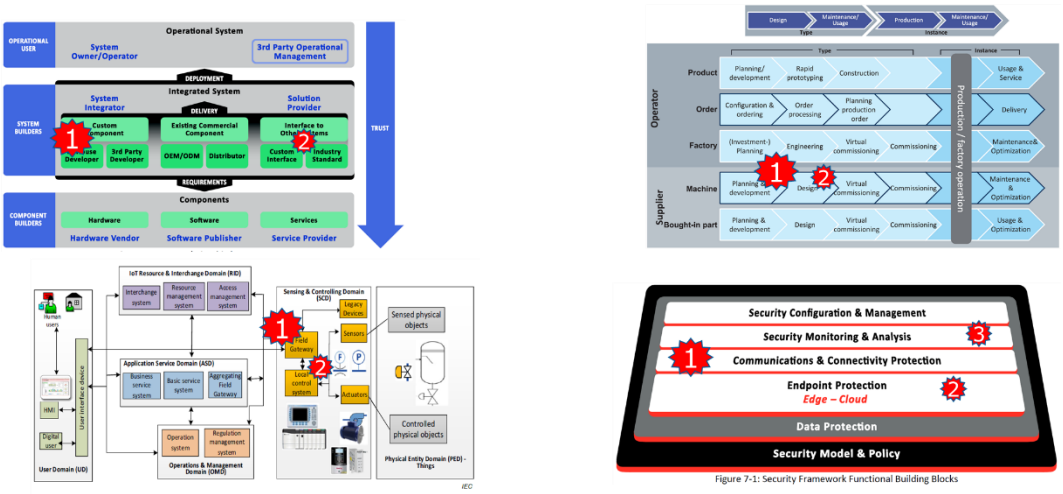

Figure 7-1: Security Framework Functional Building Blocks

Figure 10: Mapping[5] of TTTech's Scenario towards [1]

[5] number in marks indicates priority, 1 being most prior

3.8 X-Net: Security by Isolation / Production of Storage Media for IoT devices

Vision: Security by Isolation / Production of IoT devices

3.8.1 Context

Mainly belongs to the use-case Industry 4.0 but is also relevant in Automated Driving.

Context system builders:
The topic applies to system integrators and solution provider:

- System integrators need a product to automatically produce copy protected and encrypted storage media for their IoT device themselves. Custom Components require unique and customized data. The production itself must be flexible and secure enough to support individual recording processes. The configuration of the storage medium must consider different (security) strategies and allow updates to meet future needs. Therefore, a solution to produce storage media for IoT devices must take secure data transfer, secure production processes and security measures over the life cycle of a product into account.
- Solution provider need industry standards for encryption and data protection. Data that is generated during the operation has to be processed, demands decisions or are passed on to other systems (e.g. for data analysis, anomaly detection, remote support). Security measures are necessary to ensure e.g. authorized access to a device, secure data transfer, remote monitoring, identification and updates.

Both positions of the value chain need secure communication. Software publisher are interested in protecting their software, even if it is integrated in the products of third parties.

Context component builders:
Storage media that are secure and copy protected as well as secure communication is relevant for hardware vendor and software publisher similarly. Encryption technology of storage devices and techniques for secured communication between devices, machines and other means are relevant for single components.

3.8.2 Business Motivation and Reasoning

The production and integration of storage media for IoT devices has to consider multiple requirements and at the same time meet future needs. The more devices are connected to the Internet and processes and transfers data that has been collected during operation, the more important security issues get. Leaks and faults (e.g. caused through manipulation or error) can have fatal results. Though solutions respect state-of-the-art security measures, these can be outdated soon. Products, e.g. vehicles, have a life time of more than 10 years, but security standards and IT are continuously improved. Storage media that are integrated in these products must be upgraded to fulfill the necessary security standards even at the end of the life time of a product. Updates, monitoring and configurations must be handled remote. Unique identification and authentication mechanism are necessary to ensure access and correspondence.

3.8.3 Alignment to Industry and Research Roadmaps

Virtualization:
Recording and processing of data (e.g. of production systems, production processes, environment, relationships) need security strategies that consider the systems themselves, their networks, necessary service activities, data transfer processes and of course the security of personal user data. This is especially important, when data is generated over the whole life cycle of a product and considers the whole value added chain. In every point that storage devices are necessary for data transfer or data processing, individual and unique security strategies must be integrated.

Software Engineering:
Smart applications and services must be adapted to future requirements – during run-time and preferably without interruption. Update cycles and adaptations must be possible under consideration of customization and available resources.

Expertise and key technology:
Standards in the production, use and configuration of storage media and IoT device communication can be set and internationally bring benefits.

Agile Value Networks:
Lot-size one and distributed manufacturing
Automated production of unique storage media in lot-size 1 must be supported to provide highest possible security (e.g. unique keys) and to fulfill the requirements of customized production. Automation of production requires processes that consider agile environments and flexibly react on any production order. Digital twins are very close to reality and require communication that reliably deliver data.
Storage media integrated in IoT products and IoT device communication need to consider data security, cybersecurity services, secure networks and ICT and must interact with trusted routers and secure and trusted networks. The use of open source software has to be forced.

3.8.4 Concrete technological needs

Security by Isolation strategies and the production of IoT devices need

- chip controller for encrypted media that enable security configurations and data protection as well as a software to assure secure booting and decryption of the controller (T1.b)
- secure encryption strategies that handle encryption methodology, key exchange and secure data transfer (T1.c).
- software and hardware that automatically record storage media under considering of data transfer, data initialization and distribution. The whole communication chain from data source to the (outsourced) place of production and to the encrypted media need to be secured and assure data protection. Dependable Design methods for IoT (T1.a) are required.
- remote update and IoT communication requires secure communication chains that are highly available and flexible for future requirements. Connectivity has to be protected and security management to be provided (T3).

- standards. Individual and customized solutions are developed, but do not generate any standard. Guidelines are needed to settle valid standards (T1.c). Security management will be realized (T2.a).
- security monitoring and analysis that ensure e.g. the functionality of the secure network or identify attacks (T2.c).

These technological needs are developed in UC2.c and lead to the demonstration of a hardware and software element including technology like e.g. raspberry pi, special controllers and other means. They represent secure communication measures as well copy protected and encrypted systems.

3.8.5 Mapping along the Reference Architecture

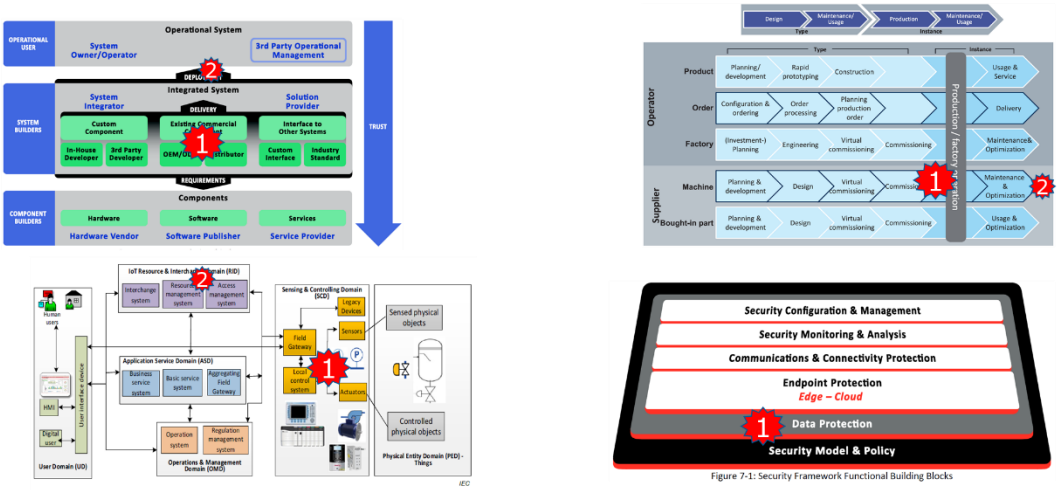

Figure 11: Mapping[6] of X-net's Scenario towards [1]

[6] number in marks indicates priority, 1 being most prior

4. Discussion of Results

4.1 Assets

In total the following items were captured (as of [15.8.2018]), referring to the structure in Figure 2

Item	Number of captured items in SharePoint
Use Cases	14
Requirements	18
Threats	84
Data Sources	2
Implementation Contexts	6
Technological Building Blocks	13
Demonstrators	5

Table 3: Summary of captured assets

A more detailed analysis of the achieved objectives towards the business model canvas and in the respective steps will be done in WP8, especially T8.2 and T8.3 (IoT4CPS value proposition update and recommendations) in deliverable D8.2.

4.2 Accumulated Mapping of described scenarios

By aggregating the architectural mappings of each scenario into one unified diagram, distribution and coverage of IOT4CPS can be depicted in Figure 12.
The top-left pane (trust relationship between actors) indicates full coverage of all roles. While a bit weak on the system operator side, many use cases focus on the components and system integration level.
The top-right diagram (lifecycle viewpoint) again indicates good coverage of basically all phases for supply side and factory operation. Aspects of order processing and (end-customer) products are not in scope of this consortium.
The aggregated mapping to the IoT Reference Architecture can be seen in the bottom-left diagram, covering most aspects from the IoT device to the cloud. While there are no direct references to the HMI layer, usability aspects (“usable security”) are addressed in this project (however not visible in this diagram).
Finally, the bottom-right diagram (security framework functional building blocks) displays the complete and overlapping coverage of all security aspects, providing a rich set of requirements for WP 3 to WP 5.

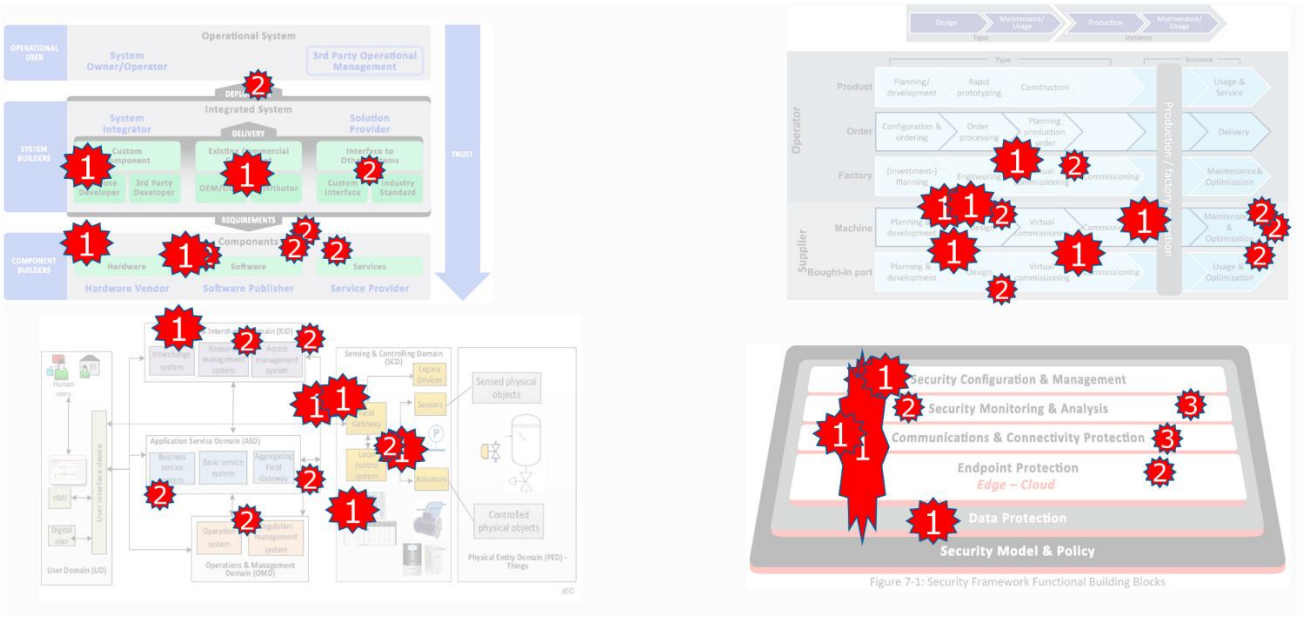

Figure 12: Combined Mappings[7] of all described scenario towards [1]

4.3 Conclusion

Methods and infrastructure to capture information on business needs for use cases in the two focus areas of the IOT4CPS project (I4.0 and AD). were developed and established. Input from analysis and requirement engineering efforts by the use case providers resulted in information structured as use cases, threats, and contexts (and summarized as “assets”). In a second step, each use case’s business needs, market requirements, and applicable industry roadmaps as well as standardization activities were analyzed. These two views combined shall allow to define and develop solutions for a safe and secure (I)IoT with the expected impact in IIoT.

WP2 results are available to all partners, being managed using a SharePoint repository.[8] Assets were reviewed by the WP2 consortium and shall be used as base for the R&D activities in WP3, 4 and 5. Assets will be re-visited by WP8, to validate project results against the formulated business needs.

To improve interoperability, and allow development of versatile components, a set of reference architecture documents was defined and documented in [1]. In order to provide a more abstract view, use case owners map the individual use cases and domain-specifics to these standard architectures.

[7] number in and size of marks indicates priority, 1 being most prior

[8] More complex items like application data or, program source will be managed by an github repository, not part of WP2

References

[1] M. Drobics, "IoT4CPS Common Reference Architecture," IOT4CPS Consortium, 2008.

[2] IOT4CPS Consortium, *Project description for proposals: Trustworthy IoT for CPS,* 2017.

[3] IOT4CPS Consortium, "IOT4CPS Assets," [Online]. Available: https://portal.ait.ac.at/sites/AHIT/IoT-LP/_layouts/15/start.aspx#/Wiki/Asset%20Management.aspx. [Accessed 30 8 2018].

[4] Verein Industrie 4.0 Österreich, "Ergebnispapier "Forschung, Entwicklung & Innovation in der Industrie 4.0"," 2018.

[5] European Commission, "European Commission C-ITS Platform phase I final report of January 2016".

[6] European Commission, "European Commission C-ITS Platform phase II final report of September 2017," 2017.

[7] ECSEL JU, "Multi-Annual Strategic Plan (“MASP”) 2018, ECSEL JU".

[8] ERTRAC, "Strategic Research Agenda: Input to 9th EU Framework Programme".

[9] Josef Affenzeller et al., "Austrian Research, Development & Innovation Roadmap for Automated Vehicles (BMVIT)".

[10] AIOTI Consortium, "AIOTI WG11 – Smart manufacturing," 2015.

[11] ECSO Consortium, "ECSO European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP)," 2016.

[12] ECSEL Consortium, "ECSEL 2017 Multi Annual Strategic Research and Innovation Agenda for ECSEL Joint Undertaking," 2017.

[13] Siemens, "Charter of Trust".

Abbreviations

Abbreviation	Description
AD	Automated Driving
ADAS	Advanced Driver Assistance System
I4.0	Industry 4.0
UC	Use Case
WP	Work Package
V&V	verification and validation
WP	Work Package

Appendix A: Initiatives and Activities related to Trustworthy radio connectivity solutions in smart production use-cases

Industrial Internet Consortium (IIC) aims to deliver a trustworthy IIoT framework for devices and systems. IIC security working group developed Industrial Security Framework that defines and provides comprehensive guidance of Industrial IoT security. Industrial Reference Architecture. It has also created the IIRA architecture model, based on ISO/IEC/IEEE 42010:2011 standard. IIC collaborates tightly with the Industrie 4.0 platform to enhance the interoperability of systems from the different domains.

Alliance for Internet of Things Innovation (AIOTI) aims to create and master sustainable innovative European IoT ecosystems and address the challenges of IoT technology and applications deployment, including standardization, interoperability, and policy issues. WG3 has published a deliverable for High Level architecture that provides information on identification, security, management of devices, gateways, infrastructure etc.

IoT Security Foundation (ISF) aims to share knowledge, best practices, and advice on security within the IoT. It has several working groups with objectives to promote quality and ensure the pervasiveness of security.

Cloud Security Alliance (CSA) focuses on defining and raising awareness of best practices to help ensure a secure cloud computing environment. The group has published research, guidelines, and best practices for IoT security.

European Union agency for Network and Information Security (ENISA) is a lead agency for cybersecurity in Europe, dedicated to network security and information security aiming to the implementation of union-wide and national cybersecurity strategies, policy and regulation, education, training, and various other activities.

Cloud Standards Customer Council (CSCC) aims to the acceleration of the cloud's successful adoption. Its main work is focusing on standards, security, and interoperability issues for the transition to the cloud.

GSMA also tackles the issue of IoT security and published specifications for embedded SIM/UICC and remote provisioning and guidelines that promote best practices for the secure design, development and deployment of IoT services. It also provides a mechanism to evaluate security measures.

PRPL is an open-source foundation works on improving security and faster deployment of embedded devices in IoT and it has a security working group to research security for next generation device-to-data center connectivity.

Online Trust Alliance (OTA) is an industry working group that established the IoT Trustworthy Working Group to guide developers, device manufacturers and service providers to enhance privacy, security and lifecycle of IoT products.

OWASP IoT project provides information on several areas such as: IoT Attack Surface Areas, IoT Vulnerabilities, Firmware Analysis, ICS/SCADA Software Weaknesses, Community Information, IoT Testing Guides, IoT Security Guidance, Principles of IoT Security, IoT Framework Assessment, Developer, Consumer and Manufacturer Guidance, and Design Principles.

The Eclipse IoT Working Group works towards the implementation of standards and protocols for constrained devices, gateways, and cloud platforms.

International Roadmap for Devices and Systems (IRDS) is an initiative to help the alignment and consensus across a range of stakeholders to identify trends and develop a roadmap of electronic industry from devices to systems and from systems to devices including all related technologies in the computer industry

3GPP Release 16 is defining standards for 5G communications corresponding to NR Phase 2aims to the definition of a full system for next generation new services and markets. There is increasing support of vertical industries such as non-terrestrial networks (NTN), vehicle to everything (V2X), public safety, and Industrial Internet of Things (IoT). 3GPP Release 15 specification also outlines the 5G standard includes a low-latency variant that cellular operators and several industrial OEMs are considering for use in manufacturing environments.

5GPPP aims to deliver solutions, architectures, technologies and standards for the ubiquitous next generation communication infrastructures of the coming decade.

The 5G Alliance for Connected Industries and Automation (5G-ACIA) is a central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain.

Productive 4.0 is a European co-funded innovation and lighthouse program that tackles theoretical and conceptual approaches in the field of Industry 4.0. Specific technological and conceptual approaches will be provided in fields like service-oriented architecture (SOA), IOT components & infrastructures, process virtualization or standardization.

Semi 4.0 is an ECSEL project for power semiconductors and electronics manufacturing 4.0. It focuses on five objectives: Balancing of system security and production flexibility, Increased information transparency between fields and enterprise resource planning (ERP), Management of critical knowledge decision making and for maintenance, Fab digitalization and virtualization incl. simulation platform, Automation systems for flexible distributed production.

Appendix B: Standardization activities related to Trustworthy radio connectivity solutions in smart production use-cases

Standards like the ISO/IEC 27000 series remain relevant and useful for broader IoT cross-platform implementations. Existing standards are also evolving towards industrial IoT use cases and new specifications are emerging. For hardware specifications one should look to EMVCo, TPM, Trusted Execution Environment (TEE), SIM, eUICC. For transport specifications the relevant technologies are Cellular, NFC, Bluetooth, RFID, and ZigBee. For infrastructure, there is the Datagram Transport Layer Security (DTLS), 6LoWPAN and IoT6. For lightweight cryptography, ISO/IEC 29192, SHA, AES, ECC, HIP-DEX, IKEv2, are mostly relevant. For critical and functional safety, IEC 61010, IEC 61508, ISO 26262, ISO 13849. For authentication OAuth, OTrP. For firmware and software, UEFI and HCE. For semantic, JSON, RESTful, SENML. For data protocols, Constrained Application Protocol (CoAP), MQTT, AMQP, DDS, Lightweight M2M (LWM2M). For device management, OMA-DM and TR-069. For multi-layer frameworks there is Thread, IEEE P2413, AllJoyn, and IoTivity.

IETF has various working groups on DTLS (Datagram Transport Layer Security) In Constrained Environments (DICE), Constrained RESTful Environments (CORE), CBOR Encoded Message Syntax (COSE), Authentication and Authorization for Constrained Environments (ACE), and 6lo, and currently has published RFCs on CoAP and DTLS. IETF also has authored a number of guidance documents challenges, considerations, and best practices for IoT security. IETF working groups also collaborate with outside organizations, such as IEEE, the W3C, the Internet Architecture Board (IAB), the Information-Centric Networking group (ICNRG), and the Crypto Forum (CFRG). Due to the open and free nature of its work IETF is one of the more prominent bodies driving efforts in IoT and security.

The ISO and the IEC have a joint subcommittee on IT security techniques (ISO/IEC JTC1/SC27) regarding IoT security standardization. OPC-UA standardized by IEC, is a vendor-independent protocol that allows diverse pieces of control equipment to communicate with each other, effectively enabling a hyper-connected network across multiple industrial ecosystems.

ITU has its ITU-T Study Group 20 and Study Group 17currently working on security issues for IoT use cases.

ETSI has the Technical Committee CYBER Industry Specification Group on cross-sector Context Information Management (ISG CIM), focusing on IoT security, low-power supplies, radio spectrum requirements, and embedded communication modules. ETSI IoT activities were transferred into the oneM2M partnership under which, security is the focus of one of the six dedicated WGs. ETSI has also the ETSI TC CYBER committee cooperating to the oneM2M security WG to specify a secure component platform named ETSI TC SCP. oneM2M is an initiative to ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the IoT. TS0001 defines functional architecture based on RESTful resource-based architecture and TS0003 contains Security Solutions specifications for authentication and securing communications between adjacent M2M nodes under Security Association Establishment Framework (SAEF), for authorization using Access Control Lists and for access managements using the Privacy Policy Manager.

AvNu Alliance working group is driving development of the Time-Sensitive Networking standard, a low-latency industrial communications protocol that can interface and deliver data over standard IEEE 802 IT networks, and that aims to augment and replace fieldbus protocols.

Industrial Society of Automation has ISA99 standard (security) committee with a strong collaborative relationship to IEC Technical Committee 65 WG 10, for the development of the ISA/IEC 62443 series on Industrial Automation and Control System Security (IACS). Details can be found on ISA TR100.15.01.

Consumer Technology Association aims to extend the internet connectivity beyond traditional boundaries and has a dedicated IoT working group that has issued a Cybersecurity Assessment Tool and CTA smart home Security Checklist that may also apply to industrial environments.

IEEE standards association is also related to many different IoT standards and security is addressed by the IoT Technical Community with efforts in the P2413 standard for an Architectural Framework for the IoT
3GPP SA WG3 is responsible for security and privacy in 3GPP systems. TR33.860 and TR33.863 studies are very relevant for security enhancements in cellular IoT and for very low throughput machine type communication devices. Also, TR22.804 study for communication for automation in vertical domains discusses in detail the applications for production in industrial automation, energy automation, but also transportations.

U.S. NIST Cybersecurity Framework for IoT supports the development and application of standards, guidelines and tools to improve the cybersecurity of connected devices and their environments. NIST CPS Public Working Group (PWG) developed a framework on how to achieve trustworthiness and implement appropriate cybersecurity and privacy mechanisms in smart system. NIST also provides specification for technologies where IoT plays a significant role (e.g. RFID, Bluetooth, encryption, networks, and cloud).

GlobalPlatform is a nonprofit industry association focusing on developing specifications for trusting and securely enabling digital services and devices throughout their life cycle. The association standardizes and certifies a security hardware/firmware combination, known as a secure component, which acts as an on-device trust anchor. Several task forces run various aspects of research and development of specifications. Of interest are the Security, Industrial IoT, and Consumer IoT groups.

The Bluetooth Special Interest Group is developing Bluetooth mesh that will enable robust wireless communications for industrial sensor networks.

Open Connectivity Foundation is an industry group for the development of standards for IoT, offering AllJoyn (an open source IoT framework that enables devices and apps to discover and communicate with each other, regardless of transport layer, manufacturer, or the need for Internet access) and IoTivity (open-source software framework enabling seamless device-to-device connectivity to address the emerging needs of the IoT) which are now both sponsored by the Linux Foundation. OCF published the OCF Security Specification that covers a wide range of security

instructions providing a common security framework that allows reliable interoperability among devices from different manufacturers.

Object Management Group (OMG) is active in IIoT standardization offering DDS protocol for the IoT which enables network interoperability for connected machines, enterprise systems, and mobile devices. Also, it works with the Industrial Internet Consortium for integration of DDS specification. OMG work also includes Dependability Assurance Framework for Safety-Sensitive Consumer Devices, Threat Modeling, Structured Assurance Case Metamodel, Unified Component Model for Distributed, Real-Time and Embedded Systems, Automated Quality Characteristic Measures, and Interaction Flow Modeling Language (IFML), for the Industrial IoT space.

Open Mobile Alliance (OMA), through the Device Management Working Group (DMWG) specifies protocols and mechanisms to achieve the management of mobile devices, services access, and software on connected devices for mobile networks and the IoT. It is also behind the OMA LWM2M protocol designed for remote management of M2M devices and related service enablement.

Trusted Computing Group (TCG) develops and promotes open, vendor-independent global industry standards and specifications, such as TPM (Trusted Platform Module) and TPM 2.0 for hardware modules with cryptographic capabilities. TCG has also been focusing on researching a standards-based approach to securing embedded and IoT systems at their foundation, securing hardware and on ensuring network security. TCG ICS Specification for Network Segmentation is based on ISA TR100.15.01 architecture and ISA99 security models.