



IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future

Project No. 863129

Deliverable D8.2

Report on opportunities and recommendations for trusted IoT

The 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 & TTTech Auto 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

For more information on this document or the IoT4CPS project, please contact:

Mario Drobits, AIT Austrian Institute of Technology, mario.drobits@ait.ac.at

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

 Federal Ministry
Republic of Austria
Climate Action, Environment,
Energy, Mobility,
Innovation and Technology



Document Control

Title: Report on opportunities and recommendations for trusted IoT
Type: Public
Editor(s): Omar Veledar
E-mail: omar.veledar@avl.com
Author(s): Andreas Martin (AIT), Christian Derler (JR), Christian Lettner (SCCH), Christina Tiefnig (IFAT), Eric Armengaud (AVL), Heinz Weiskirchner (Nokia), Heribert Vallant (JR), Kay Römer (ITI), Leo Happ Botler (ITI), Martin Matschnig, Lukas Krammer (SAGOE), Mario Drobics (AIT), Martin Matschnig (SAGOE), Omar Veledar (AVL), Sebastian Ramacher (AIT), Stefan Marksteiner (AVL)
Doc ID: IoT4CPS-D8.2

Amendment History

Version	Date	Author	Description/Comments
V0.1	22.01.2020	Omar Veledar, Mario Drobics	Initial version
V0.2	16.07.2020	All authors	Integrated initial partner content
V0.3	15.01.2021	Omar Veledar	Version for initial review
V0.4	22.01.2021	Eric Armengaud	Reviewed Version
V0.5	06.04.2021	Omar Veledar	Ready for delivery
V1.0	07.04.2021	Andreas Martin	Final version

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.

Content

Abbreviations	5
Executive Summary	6
1. Introduction	7
1.1 The IoT as an inevitable enabler and a driver of exploitation	7
1.2 Vehicles in command of own performance.....	8
1.3 Trustworthy communication as a key aspect of user acceptance.....	8
2. Exploitable results	9
2.1 Methods	9
2.2 Tools	10
2.3 Technology building blocks.....	11
2.4 Conceptual guidelines	12
2.5 Reusable architecture patterns	12
2.6 Exploitable solutions.....	13
3. Value proposition	14
4. Business Model update	15
5. Sustainable future of project assets and relationships	16
5.1 Opportunities for trusted IoT solutions.....	17
5.2 New Business Opportunities	18
5.3 New Research Opportunities.....	18
5.4 Evident exploitation risks	20
5.5 Recommendations.....	20
6. Conclusion	22
7. References.....	22

Abbreviations

AD	Autonomous Driving
ADAS	Advanced Driver Assistance System
CPS	Cyber-Physical System
Dx.y	Deliverable (x = WP number, y = deliverable identifier within that WP)
IoT	Internet of Things
IIoT	Industrial Internet of Things
UC	Use Case
VR	Virtual Reality
WP	Work Package

Executive Summary

This document delivers a high-level overview of IoT4CPS technical results on their path towards impactful exploitation. The widespread focus is a replication of the diversity of partners in the project. Their common link is seen in the drive towards increased quality, accelerated development and validation, and deployment in an industrial environment. The basis for these results is active collaboration between the project partners on a mission to provide improvements in the dependability of modern systems. That is demonstrated in two industrial domains, driving automation and Industry 4.0. Each domain provides one practical demonstration, which is where the suitability of the developed technological advances is examined.

The document also considers realistic benefits and value creation, which are yielding from the usability and applicability of the project outcomes. At a partner level, the potential for future collaborations and research direction also come into play. These are considered within the realm of the national and international ecosystem. The technical development and relationship building at the wide stakeholder level are supplemented by the business development opportunities. These activities are contributing towards the sustainable future of the project results, hence prolonging the impact of the project beyond the project closure phase. It is the integrative solutions across the partners that are likely to increase potential improvements and eventual exploitation of the same for business purposes.

1. Introduction

As a crucial creator of benefits that form an improved overall depiction of future mobility, autonomous driving (AD) is contributing to solving the challenges posed by climate change, road safety and improved utilisation of transport infrastructure. While AD is unable to provide holistic solutions to solve the posed questions on its own, it is a key component of the integrated picture of mobility.

Similarly, the ongoing pressure posed by modern society on manufacturing and industry is being answered by the development and deployment of novel smart technologies for the modernisation of traditional industrial practices. In this domain, automation is largely contributing to efficiency and productivity improvements. It is also an enabler of more flexible operations, data and knowledge sharing and collaborative actions.

This document provides an insight into how IoT4CPS paves a path towards exploitation of its results in the fields of AD and Industry 4.0. It also presents the opportunities and recommendations that are collected throughout the project from its initial phase to the closing stages. These recommendations are resulting from cooperation between project partners and their interactions within the project, as well as with the external stakeholders. Simultaneously, these activities are aligned with the strategies of individual organisations.

1.1 The IoT as an inevitable enabler and a driver of exploitation

A frequent issue that concerns Internet of Things (IoT) within the automotive industry is the lack of overview and integration across the board. The huge number of activities often fail to interlink with each other. Some of the elementary questions that arise are related to new business models, value generation and sustainable exploitation of results or maximisation of benefits. Hence, the basic question is related to the measures that could contribute to the sustainable exploitation of IoT in the world of mobility and production.

Connectivity as a component of digitalisation is one of the top automotive trends [1]. The realisation of benefits promised by the introduction of connectivity is only possible if there are progressive technical developments. These developments often call for a reorientation of strategy. The positive aspect of connectivity is that it no longer is a radical idea – the maturing technology is lowering the uncertainty levels. The exploitation of these solutions depends on positioning within the ecosystem. An integrator becomes highly dependent on technology providers and can offer a limited unique proposition. On the other hand, a creator of own solutions opens new opportunities for existing business models and exploitation. In either case, research suggests the expectations are to implement business model innovation as a driver for the success of IoT [2]. The IoT4CPS works in that direction by following its own objective 3 in support of the digitalisation along the entire product lifecycle leading to a time-to-market acceleration. The project also underpins the path to exploitation through activities that are aligned with the overall objective 4, which is concerned with delivering demonstrators to showcase the integration of security concepts along the product life-cycle and across the value chain. Such demonstrations are sure supporters of change and increased acceptance of the new technology.

Just as IoT is a key technological enabler of digitalisation and a mean to drive new business models, it is also a key technical component for the demonstration of the two IoT4CPS' use cases. The autonomous driving (AD) demonstration is considering the enhancement of an open vehicle demonstrator by the integration of smart IoT as an enabler for smart instrumentation. The details of the demonstration are described in D6.3b. In broad terms, it considers the integration of connectivity solutions with the aim of provisioning interfaces to the vehicle and the existing vehicle functions. The Industry 4.0 demonstration is integrating trustworthy connectivity solutions into the production environment, as described in D7.5. The key component, in that case, is traceability through the life-cycle of the systems and their components.

The key characteristic of the demonstrations is moved away from the simple technical demonstration. It also integrates an investigation of inspiring business possibilities. Hence, the outcomes are reported here as opportunities and recommendations for trusted IoT. As already reported in D8.1, those opportunities and related benefits are not created through project deliverables, but through the usage of created assets (Figure 1), which is the primary concern of WP8.

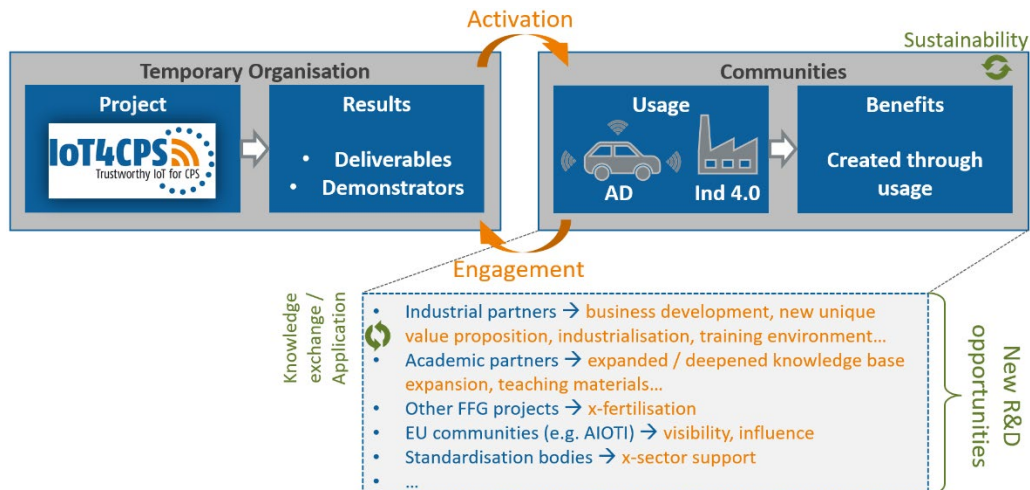


Figure 1 Usage of developed technology bricks

1.2 Vehicles in command of own performance

To increase benefits through the usage of IoT, one must consider the current automotive trends. The digital transformation in this domain is supporting the trends of electrification, connected vehicles, assisted and automated driving, and diversity in mobility services [1]. The convergence of these trends is often pivoted around a single technology and that is IoT. Hence, the proposed applications in this field are seeking to deliver new products and services, which are heavily reliant on IoT. Combining that finding with the fact that the AD is edging towards practical realisation, IoT4CPS puts forward its trustworthy connectivity solutions as an integral component of AD. Although the predominant aspect is that of security, safety and privacy are playing an important role in those solutions. All three of those components are key factors for lowering user resistance to new technology. By continuing to work in that direction, the sustainability of the offered solutions is guaranteed. The level of automation will continue to progress (Figure 2) as per their definition [2]. Each one of those levels contains own set of dependability requirements and IoT4CPS is contributing to their fulfilment through the technical offer, as described in section 5.

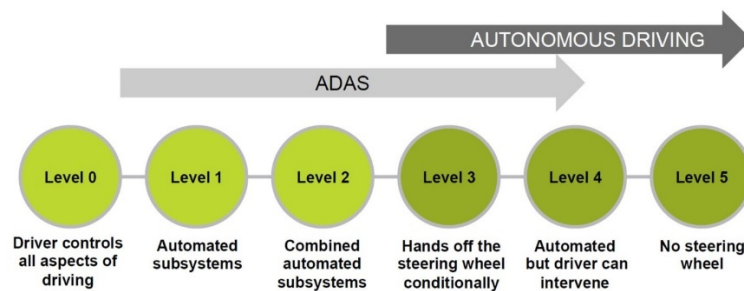


Figure 2 From ADAS to autonomous driving; SAE J3016 defines 6 levels of automation

1.3 Trustworthy communication as a key aspect of user acceptance

The vehicles of the future are no longer seen as products in a classic sense but as service hubs, the majority of which imposes the need for connectivity. That directly infers the need for secure and trustworthy measures to protect vehicles against unauthorised access. As driving is a safety-critical activity, dependability is crucial for vehicle communication, to guarantee safe driving operation. In addition to safety, user acceptance is heavily conditioned by the successful integration of IoT and Cyber-Physical Systems (CPS).

Despite the technical development in the promising domain, there is a lack of established methodology for systematically building homogenous end-to-end solutions [3]. Hence, dependable, trustworthy solutions are inevitable for the quality of future applications and user acceptance. The integration of appropriate security levels should lend itself to easy deployment, with no negative impact on either system performance or user

experience. These should be aligned with the emerging standards, such as “ISO/SAE DIS 21434 Road Vehicles - Cybersecurity Engineering” [3], which achieves a common understanding of security by design in product development and along the entire supply chain [4]. Hence, the success of the project results and direction of future research and development activities must comply with the notion of trustworthiness throughout the life-cycle of assets.

2. Exploitable results

Considering the described aspects: IoT as a technology enabler (section 1.1), progressing driving automation (section 1.2) and the need for trustworthy solutions (section 1.3) IoT4CPS’ results are targeting these three aspects. To that extent, a high-level list of major project outcomes is provided in this section.

Besides the exploitable results of the project, IoT4CPS enables the generation of benefits through improved collaboration, technology access and new insights. It enables partners to either broaden and/or strengthen their portfolios and enter new markets. Some of the key activities and aspects that are contributing to the maximisation of benefits are:

- Improved understanding of core skills and competencies of the project partners as a form of introduction for collaboration either in this project, in future collaborations or business context
- Trust gained and relationships strengthened through collaboration
- Mutually created and/or shared insights in Industrial IoT (IIoT) infrastructures
- An introduction to the robotics community
- Shared insights into the needs for secure communication in the IoT setting
- Provided an industrial environment to test and evaluate the cryptographic schemes for the research partners
- Enhanced understanding of the factory and the mobility of the future
- Ability to cooperate on industry-driven use cases which allow the design, adaption and test of algorithms/methods given specific requirements
- Collaboration with a wide range of industry partners and universities
- Development of strategic partnerships
- Marrying multiple concepts for increasing system reliability
- Higher visibility in the Austrian research community
- Quality improvements (security) for existing products

2.1 Methods

The following methods are being delivered by the project.

- Self-Healing by Structural Adaptation
- Security risk assessment methods (FMVEA)
- Trusted orientation and localisation
- Method for collaborative single-anchor localization
- Concept to protect against cyber-attacks to distance estimation
- Security test case generation approach based on attacks
- Anomaly detection algorithms
- Threat Modelling for Device.Connect™

These methods are intended for the optimisation of indoor and mobile (vehicle) environment. The benefits yielding from their usage are resulting from their contributions to:

- Increased quality through improving:
 - the resilience of the systems to runtime failures (systems are assessed for the risk of failure, and possible impact), as well as to localisation-based attacks
 - quality of position estimations (through collaborative localisation)

-
- security of localisation
 - system resilience to localisation-based attacks
 - overall system security
 - Expanded range of functions, such as:
 - prevention of Cyber-attacks
 - trustworthiness of localisation (indoor and mobile)
 - wireless connectivity in a smart production environment including:
 - autonomous and collaborative cyber-physical production systems
 - AI-based automation and real-time monitoring for optimisation of industrial processes
 - remote predictive maintenance of industrial assets
 - industrial wearables
 - Augmented Reality (AR)
 - automated test case generation by extending security testing for IOT based applications by incorporating attack pattern knowledge
 - online anomaly detection on diverse datasets and data streams (analytical toolbox) through the usage of a framework that allows training, evaluating and deploying anomaly detectors

2.2 Tools

A range of tools, which were either developed or supported by activities of IoT4CPS can be divided into three categories, subject to the stages of their development:

- design, implementation, testing:
 - MoReTo, ThreatGet [4], GSFlow
 - wireless Sensor Network Implementation for testing Industrial Wireless Connectivity in a realistic scenario based on LoRaWan technology
 - taxonomy of state-of-the-art technologies enabling direction estimation.
 - threat modelling (template) Pentesting
 - recommender system for dependable IoT applications
 - automated software test case generation and execution
- roll-out, run-time analysis/monitoring:
 - AMiner (Log Based Anomaly Detection)
 - Sensor Security with Watermarking
 - IoT Discovery
- lifecycle:
 - IoT Discovery

Either achieved or anticipated benefits provided by these tools contribute to the following:

- Quality improvements by:
 - enabling designers to choose the most suitable angle of arrival technology achieving pre-established requirements
 - decreasing system vulnerability
 - delivering security-relevant requirements at the design stage using threat modelling i.e. the specified pentest catalogue addresses each identified threat with respective mitigation to help software developers, software testers as well as system architects to improve the modelled architecture concerning cybersecurity during development
 - increasing system quality by implementing a systematic design recommender system for dependable IoT
 - increased system security
 - detecting potential attacks on IoT or misuse of services

- ensuring data authenticity through the usage of a lightweight method
- Range and reach of functions by:
 - empowering system developers to apply direction-finding features of existing transceivers in new applications
 - enabling penetration of existing functions into more complex systems
- Accelerating development by:
 - identifying security threats and risks in the design phase
 - automatically and systematically handling identified security threats and risks
 - eliminating the need to re-evaluate the covered technologies in specific environment or conditions
 - increasing threat awareness and communication during the development and testing processes
- Accelerating validation by:
 - accelerating security testing
 - enabling automatic system validation based on technology and system properties
 - increased automation in software testing
- Contributing to instrumentation by:
 - Supporting the audit process
- Production and in-field deployment by:
 - securing IoT devices and related services

2.3 Technology building blocks

The following are the key technology bricks that are contributed to by IoT4CPS in a considerable measure:

- Hardware
 - Autonomous Driving Platform
 - HW-Checker Apps
 - DriCon™ (a compact driver control tool)
- Software/firmware
 - IoT Recommender System
 - Crypto Library
 - A library implementing Bloom Filter Encryption and integration as 0-RTT forward-secure key exchange in OpenSSL
 - Simulator enabling the comparison of different single-anchor positioning systems.
 - MQTT test adapter
 - The online anomaly detection platform
 - Remote control of a real vehicle using DriCon™ and an android device

These building blocks are directly impacting the following:

- quality improvements by:
 - increasing security of FPGA based SoCs through the usage of Checker Apps
 - allowing the design of complex IoT systems in a systematic way, which also eases device integration
 - selecting the most suitable methods to improves the quality of position estimations
- range of functions by:
 - improving the versatility of the autonomous driving platform that integrates safety features with high-performance computing units
 - providing strong security guarantees at reduced latency for resource constraint clients
 - enabling assessment of the impact of the parameters
 - developing a software platform for online anomaly detection
- development acceleration by:
 - enabling detection of performance issues without the need for implementation in hardware

- validation acceleration by:
 - facilitating benchmarking of new related methods to the implemented ones and selecting the most viable option for any given case
 - applying the new approach for generating security test cases (i.e., combining random exploration of input sequences to construct valid sequences in conformance to protocol specifications in combination with invalid interaction sequences including invalid, unexpected, or random data as inputs, which are derived from attack patterns that target vulnerabilities in the system under test)
 - improvements in regression and conformance testing (e.g. for detecting incompatibilities between MQTT broker implementations)
 - improving testing of robustness against attacks known for having a high chance of bringing the system into an undesired/insecure state

2.4 Conceptual guidelines

A set of conceptual guidelines was developed through IoT4CPS. The key findings specifications, recommendations and guidelines support:

- wide-area communication issues
- development of usable cryptographic APIs
- secure and reliable V2X communications
- integration of safety measures to avoid cyber-attacks against localisation systems
- experiment design to compare direction-finding technologies
- using localisation as a mean to ensure correct provisioning
- implementing cryptographic algorithms in resource-constrained hardware
- Dynamic Partial Reconfiguration (DPR) Framework

The targeted benefits are related to the following topics:

- Security of 5G connectivity that supports reliable and secure V2X connectivity
- avoiding cryptographic API non-intentional misuses
- improvements in terms of the quality of the assessment of new technologies
- improvements in design structure
- 5G new radio access networking
- wireless infrastructure HW models
- verification of mispositioned components
- avoidance of serious production faults due to mispositioned components
- flexibility in FPGA based IoT devices
- in-field updates of programmable logic

2.5 Reusable architecture patterns

The findings in terms of architectural development are concerned with:

- dependable vehicle architecture that lends itself to the integration of AI algorithms into control loops
- wide area of communication issues
- verification and validation patterns
- recommendations for architectural building blocks
- framework for automated generation of security test cases for regression testing
- machine learning-based anomaly detection pipeline using autoencoders

These patterns are contributing towards improvements in terms of:

- quality and functionality by:
 - considering 5G security and reliability functions

- examining and developing machine learning model management and online learning patterns
- accelerating development by:
 - setting the concrete steps for practitioners to achieve dependable systems
- accelerating validation by:
 - automating the security analysis, validation and verification

2.6 Exploitable solutions

Based on the exploitable project outcomes from section 2, the created solutions are primarily focusing on two specific use cases, which are mentioned in section 1.1 and described in detail in D6.3b and D7.5. Although the maturity level of the offered solutions varies across the board and is also partner dependant, these are creating a base for improved usage and sustainable future of the project outcomes (as described in 1.1 and depicted in Figure 1). It must be noted that not all the outcomes are showcased in the final project demonstrations. The key solutions, split per domain:

- AD:
 - trustworthy communication channels
 - autonomous driving platform
 - open vehicle demonstrator targeting driving automation based on the autonomous driving platform
 - ThreatGet-based analysis of security risks in the automotive CPS
 - specifications and guidelines for 5G cellular infrastructure that enables reliable and secure V2X connectivity for connected and autonomous driving functions
- Industry 4.0:
 - trustworthy communication channels
 - log-based anomaly detection mechanism for IIoT devices
 - trusted localisation methods
 - recommender system for building complex dependable IoT systems
 - trustworthy radio connectivity solutions for Industry 4.0 environments
 - improvements for PHY layer wireless communication
 - an efficient solution for single-anchor indoor localization scenarios (E-SALDAT)
 - threat model-driven Penstesting approach
 - discovery and classification of IoT devices (IPv6, Bluetooth, LoRa)

These solutions have the potential for further improvements and application in other fields. The additional domains are expected to contribute to cross-fertilisation as an additional factor for maintaining the sustainability of the project outcomes. Through increased usage of the presented solutions, the following drivers of benefits and benefits are anticipated in the post-closure phase of IoT4CPS:

- improved trustworthiness of wide-area fixed and mobile communication for both use cases, AD and Ind4.0.
- lower latency for client-initiated secure communication
- address safety and security challenges for enabling autonomous driving functions for vehicle producers
- trustworthy usage of localisation systems, which are relying on direction estimation, based on efficient, accurate and secure collaborative localisation
- cost savings through reduced usage of resources for security testing
- improved innovation ecosystem within the realm of Austrian industry (enhanced competitiveness)
- increasing product quality
- shortened time-to-market
- increased production efficiency

3. Value proposition

To provide a sustainable future for the project assets and to determine which aspects the project partners ought to focus on delivering the anticipated value, the Value Proposition Canvas is developed for IoT4CPS (Figure 3). The canvas ensures that the IoT4CPS outcomes are well-positioned concerning the customer expectations, values and requirements.

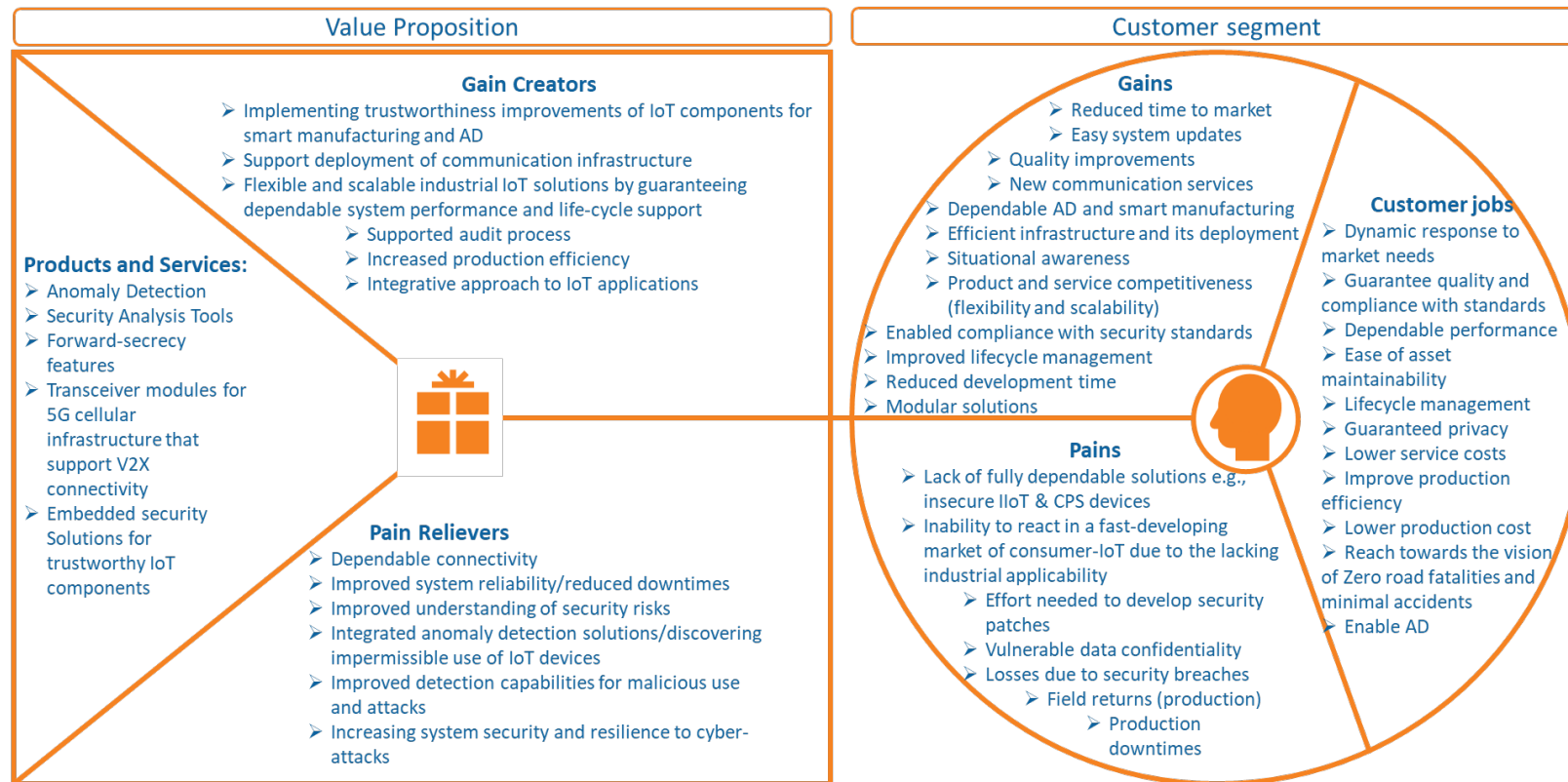


Figure 3 IoT4CPS Value Proposition Canvas

4. Business Model update


Key partners	Key activities	IoT4CPS value proposition	Customer relationships	Customer segments
 <p>IoT4CPS consortium bringing together full range of Austrian research partners in the security domain as well as main Austrian industry players in Industry 4.0 and Autonomous Driving</p>	<ul style="list-style-type: none"> ➤ Development of trustworthy IoT components ➤ Development of key components and functions for autonomous driving ➤ Development of key components for smart production ➤ Development and enhancement of tools and solutions for autonomous driving along the entire product lifecycle ➤ Practical demonstrations ➤ Dissemination activities 	<ul style="list-style-type: none"> ➤ <u>Obj1</u>: Framework library for trustworthy IoT tools and solutions ➤ <u>Obj2</u>: Innovative components targeting efficiency increase by 10% for the deployment of connected vehicles and level 3 and 4 autonomous driving functions ➤ <u>Obj3</u>: Digitalisation along the entire product lifecycle leading to a time-to-market acceleration of 10% ➤ <u>Obj4</u>: Industrial demonstrators ➤ <u>Obj5</u>: Involve and support of Austrian IIoT/AD/Ind4.0 communities 	<ul style="list-style-type: none"> ➤ Dedicated personal assistance and co-creation of assets/value (Obj1-4) through direct interaction to support integration of technology solutions for customer assets ➤ Community creation (Obj5) and interaction with full range of stakeholders aimed at enabling direct interaction and exchange with the relevant national and European ecosystem ➤ Strategic partnership (Obj5) development and open exchange between industry and academia 	<ul style="list-style-type: none"> ➤ Seg1 (Obj1-4) Vehicle manufacturers, Tier 1 suppliers needing smart and connected components, engineering services and tools for efficient development, integration, validation and instrumentation of innovative AD functions and components. ➤ Seg1 (Obj1,3,4) Manufacturing plant owners requiring trustworthy connectivity solutions to improve their competitiveness in terms of production efficiency. ➤ Seg3 (Obj5) National or European agencies seeking for aligned expertise for trustworthy IoT
Cost structure <ul style="list-style-type: none"> ➤ Fixed costs such as personal (expertise), marketing, lab and material parts 		Revenue streams <ul style="list-style-type: none"> ➤ Software and tool licences (Obj1,3,4): selling licences to use the respective tools and solutions ➤ Components and platforms (Obj2,4): selling ownership rights to the customers ➤ Engineering services (Obj1,2,3,4): selling respective engineering services 		

Figure 4 IoT4CPS Business Model Canvas

To define the economic and other benefits and the target market, a business model overview for the IoT4CPS project is updated (**Fehler! Verweisquelle konnte nicht gefunden werden.**) following the originally planned activities and their updates throughout the project.

5. Sustainable future of project assets and relationships

Knowledge creation, sharing and exploitation are central to a successful innovation [5]. Through meaningful cooperation within IoT4CPS, the project partners have identified and exchanged knowledge across the organisations. The aim is to secure a sustainable future for the project results through a cooperative approach to the exploitation of the gained knowledge. The IoT challenges (especially the ones within the automotive domain) are too big to be solved on one's own. Open research and collaborations are highly recommended and should be treated not as outsourcing, but as capacity development [2].

In terms of a direct continuation of cooperation between IoT4CPS partners, the following are current specific activities:

- 5G collaboration in the field of Ind4.0 following from the two use-cases (Nokia)
- The potential extension of research results for anomaly detection towards predictive maintenance
- Collaboration in terms of enhancing smart production activities aimed at serving vehicle manufacturers and electronic industry with advanced semiconductor solutions (IFAT)
- Hardware-based security with innovative technologies for safe, secure and reliable M2M connectivity (IFAT)
- Cooperation in upcoming ECSEL Project VALU3S (AIT)
- HW crypto implementation (TUG- IAIK)
- Self-healing systems (TUW)
- Combining thread modelling approaches used in practice with automated test case generation (research institutions – industry)
- Combined anomaly detection and test case generation (across research institutions)
- Semantic-based anomaly detection and causality discovery (e.g. using knowledge graphs) (research institutions – industry)
- Expanding test case generation methodologies
- Integration of safety-relevant autonomous driving platform into real vehicles (AVL-TTTech)

The key anticipated short-term benefits of future collaborations are expected to follow from the development of new services (e.g., 5G) and the creation of in-depth insights into IoT/CPS installations. From the hardware perspective, the expectation is to further deepen and extend the concepts, methods and tools developed in IoT4CPS. The key aspect that is to be considered for future development is that the partners need to face future complex changes and requirements in the Industry 4.0 manufacturing era to meet future expectations and trends in an ideal way.

One of the direct results that already arose from the European activities is that the project consortium has received multiple invitations for possible contributions to the H2020 calls ICT-01-2019 / ICT-15-2019 at the ICT 2018: Imagine Digital, Connect Europe. Equally, the bilateral cooperation between project partners will be extended in the Horizon Europe program, especially in the field of security and IoT in general. A graphical representation of IoT4CPS' fit into the ecosystem is shown in Figure 4.

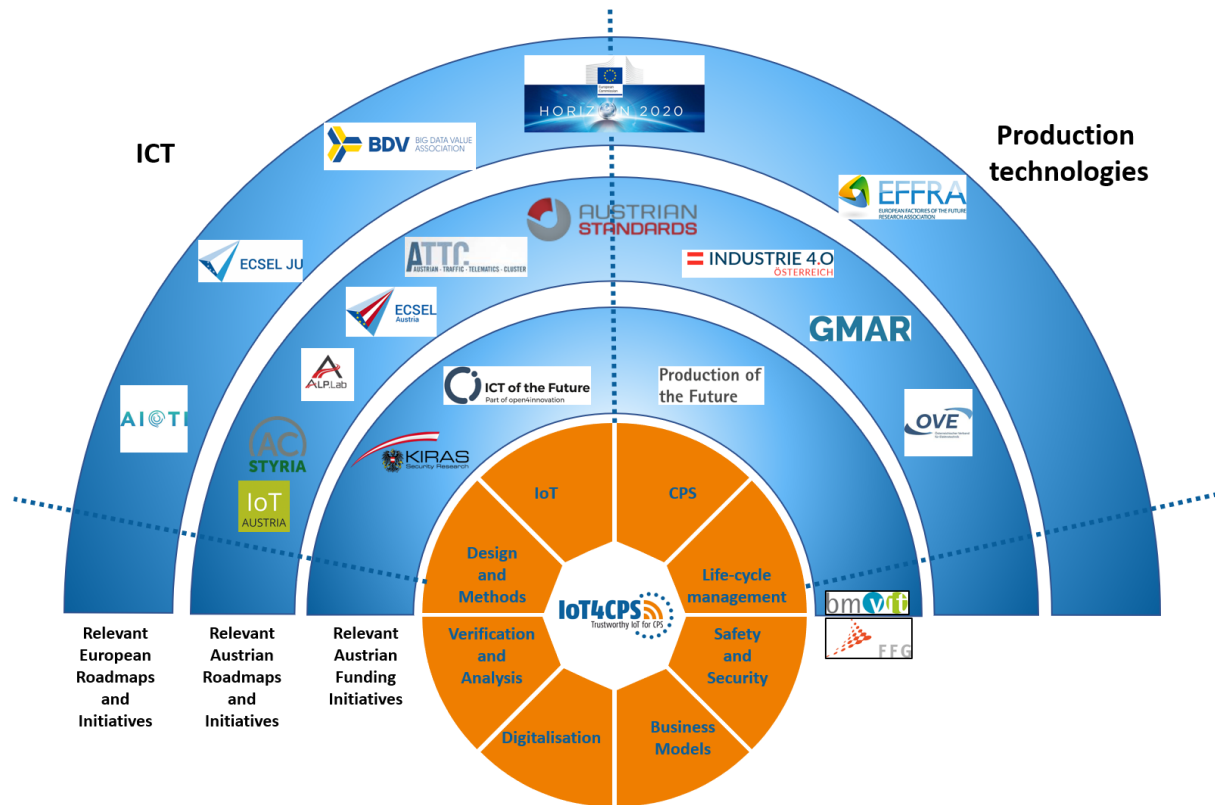


Figure 4 IoT4CPS within European and Austrian ecosystems

5.1 Opportunities for trusted IoT solutions

Automated cars on the roads and robots in factories are both highly mobile and need to collaborate in dynamic neighbourhoods [6]. One supporting ICT infrastructure for such a highly dynamic and trustworthy operation relies on a dependable and adaptive safety platform. The AD platform of the HW component in section 2.3 has gone through hardware and interface improvements through the IoT4CPS project and internal collaboration. The resulting performance and the compatibility of the offered solution to vehicle control algorithms make the platform an optimal choice for further exploration and exploitation. As it is clear that AD is no longer a distant vision, but a reality, there is a need to further enhance the available functions to allow progression towards higher levels of automation [7]. That is where this platform offers a perfect fit. It is its capabilities for integration into a real vehicle and the related security features that are the driving factors for the drive to continue using the safety platform in future R&D and business activities.

ThreatGet [4], which is listed in sections 2.2 and 2.6, has got an immense potential as a threat model tool for IoT-based smart factory and autonomous driving vehicles. Its key weapon is the capability to increase overall system security. It enables the creation of reusable and extendable threat models that can be implemented in several generations of a product as well as in different lifecycle stages, as described in detail in D3.2. The power of the tool is that it is applicable in any application domain which requires security analysis. Hence, its exploitation potential crosses the boundaries of IoT4CPS and is a good candidate for sustainable exploitation. The lessons learned in this project have contributed to the evolution of the tool with enhanced features. The current commercial version is offered by LieberLieber GmbH and AIT Austrian Institute of Technology and is aimed at checking vehicle cybersecurity aspect. Its success proves the conversion of the exploitation potential into industrial usage. The tool is complemented with other tools i.e. MORETO and GSFlow, which enhance the management of the whole product development concerning the safety standards (complete life-cycle).

The exploitation of the Self-Healing by Structural Adaptation algorithms (D6.1) is focusing on a mixed-criticality platform, which is a common platform for developing automotive features. The activities within IoT4CPS have proved the integration potential of the algorithms, hence offering improved system resilience. This added value is the key exploitation driver of the algorithm.

A comprehensive set of approaches, which were developed in WP4, assure security by both formal and empiric methods to detect anomalies and uncover vulnerabilities at different system levels. Considering the increasing complexity of the modern CPS and their inherent need for dependable operation, the demonstrated security improvements emerging from the anomaly detection algorithms offer a sustainable outlook for these approaches. That is further enhanced by the portability of the approaches to other industrial domains. In certain cases, it is only minor or medium adaptations that are needed for the adaptations.

The developed privacy and security features, which follow Privacy by Design (PbD), GDPR, Privacy Impact Assessment (PIA), or design “notice and choice” systems can guide users through privacy settings wizards, or send warnings to the users as a flashing light or flashing icons to show different levels of risk, or offer other automated ways for the users to check their privacy data status. These approaches offer exploitation opportunities within the automotive domain, especially amongst vehicle renting services where they offer privacy checklists when selling or renting smart vehicles to customers. These lists strongly suggest removing private and sensitive data. The basis of these approaches is presented in D5.4.1 and D5.4.2, which involves the implementation of the Digital Twin prototype in IoT4CPS. The importance and a generic approach to digital twins in the automotive world are highlighted in [7]. Further enhancements and industrialisation of the offered Digital Twin approaches will depend on an effective data strategy and methods to be put in place, as well as balancing regulatory issues at national and international levels.

5.2 New Business Opportunities

In terms of realistic business opportunities that are directly resulting drawn from IoT4CPS assets, the following are of key importance:

- Elaboration of new 5G based services (Nokia) in cooperation with the existing partners
- Integration of anomaly detection into IIoT/CPS devices
- Improvement of the existing security tools aiming at assuring security for complex solutions that need to comply with the latest cybersecurity standards
- Development of secure communications solutions, which are intrinsically transparent for easier integration so that upgrading from non-secure communication to secure one does not require a rewrite of the networking stack
- Building automation and construction site monitoring

5.3 New Research Opportunities

The key aspects that are of interest for future research in the field from the perspective of the project partners, aside from the obvious AD and Industry 4.0 applications are:

- 5G/IoT security and reliability
- Predictive Maintenance
- Aggregation of (log) data from IIoT networks to reflect complex situations in manageable numbers of alerts
- A broad scope of approaches to ensure the dependability of IoT systems (such as the ones identified in WP3) and interconnections and intersections between these approaches to ensure better usability and added value
- The synergy between different dependability approaches, many of which are complementary to each other

-
- Reducing the overheads for secure end-to-end communication with strong security guarantees even further
 - Providing future-proof security guarantees by employing post-quantum secure schemes
 - Tools and solutions among the entire product lifecycle for AD
 - All topics covering Communications Sector, Industrial Automation Sector and Security for IoT Sector from the perspective of semiconductor devices - especially components for cellular base stations, RF transceivers, secure and energy-efficient solutions for wireless connectivity
 - Joint positioning and pose estimation
 - Security issues on direction finding systems
 - Integration of direction finding with distance estimation leading to a full single-anchor localization system
 - Collaborative localisation using multiple antenna nodes.
 - Formalisation of the semi-formal thread modelling to a formal verification approach
 - Security Testing
 - Big Data and Stream Analytics
 - Knowledge Graphs
 - Model Lifecycle Management

The key identified success factors, which are identified as the main supporters of the oncoming research activities are:

- Successful validation concerning different use cases and industries
- The adoption of dependability methods by industrial partners i.e. knowledge transfer between research organisations and industrial partners
- Deployment of research prototypes in real-scale industrial challenges i.e. scaling up
- Significant improvements in runtime or bandwidth overheads
- Significant improvement in the achieved security properties
- Addressing the challenges of ultra-reliable, low-latency, secure connectivity for autonomous driving and Industrial IoT functions
- Identification of suitable IoT use cases and their technology requirements i.e. an appropriate definition of the problem to be solved
- Collaboration with partners with complementary interests/expertise to allow a holistic coverage of dependability
- Improved efficiency and effectivity of methods for secure system development
- Currently, IoT systems lack system-wide security at a very low level (hardware) and technology-independent system design and management at a very high level, both of which are the key factors for a successful IoT system

The following are some of the recommended future R&D topics in the context of trusted IoT and their industrial applications:

- Possible attacks on the IoT trustworthiness
- Validation and Verification in the context of cyber-security
- Virtualized demonstration platforms to be able to build and test new software libraries on the platform without needing access to the hardware
- 5G-enabled Industrial IoT and V2X services
- Lightweight Security Protocols enabling low-power fog computing
- AI-enabled Networking and application services ensuring safety for the Internet of Vehicles
- Ambient Intelligence for Industrial CPS and processes
- Joint positioning and pose estimation
- Security issues on direction finding systems

- Integration of direction finding with distance estimation leading to a full single-anchor localization system
- Collaborative localisation using multiple antenna nodes
- Risk-based approaches in security testing where risks can be derived from threat modelling and/or common vulnerability enumerations

5.4 Evident exploitation risks

IoT4CPS has provided an opportunity to identify technology gaps between prototypes and industrial solutions. The line of investigation that has supported bridging this gap so far follows the guidelines provided by the established standards and protocols, such as OpenSSL in the case of the crypto library.

While mass adoption of low-power and low-cost secure wireless connectivity technologies in the industrial space is on track, the investigated solutions must ensure trustworthiness, ease of use and effective integration with existing environments. This requires a long-term transformation until it is fully integrated into real-life industrial use cases to enable the promises and benefits of smart factories in the Industry 4.0 domain.

5.5 Recommendations

Table 1 is a collection of recommendations at the project's closing stages.

Table 1 IoT4CPS sustainability recommendations

No.	Recommendation
1	As the complexity of CPS is increasing, together with its reliance on IoT, it is evident that it is unlikely for single players in the field to cover the full vertical solutions. The limited mapping of technical solutions and business interests of a single source to the full vertical needs is likely to cause issues. Hence, it is highly recommended to pursue extensive cooperation in terms of exploration and to combine business offers to deliver one-stop-shop solutions for the end-users. This is evident in IoT4CPS where a diverse set of partners complement each other in terms of technical know-how and terms of potential exploitation.
2	As it is expected for many industrial domains to rely on the same IoT solutions, a certain level of tailoring (and sometimes customisation) is inevitable. However, as the basis for many applications is the same, it is recommended to work on common solutions with tailoring to specific domains coming on a top layer. The inevitable cross-fertilisation across domains is likely to deliver improved solutions for all. IoT4CPS has shown this through cooperation between driving automation and Industry 4.0.
3	An unsurprising finding of IoT4CPS is that cooperation with other projects and communities inevitably creates positive benefits for all parties involved. It is recommended for lighthouse initiatives, in general, to nurture deep cooperation where possible and hence perform both: promotion of project results and extension of consortium influence, which in turn should help direct the future activities in the area (e.g. through the definition of road-maps, participation in white-paper creation etc.).
4	It is recommended to deepen the collaboration between the industrial and academic partners in the fields of knowledge transfer and industrialisation of generated technology bricks as well as in the form of provision of the industrial needs and use cases.
5	Where possible, it is recommended to attempt to implement verification techniques, which are generated within IoT4CPS into an industrialised environment, to guarantee product quality at the point of instrument exit from the manufacturing facilities.
6	As the IoT ecosystem is still in its premature stages of development and technical standards are lagging the technical progress, it is advisable to continue exploiting project findings for the generation of standardisation recommendations. The project findings may also be used for contribution to domains that have already established technology-independent standards.

7	The partners are encouraged to continue their monitoring and contribution activities related to potential creation of a common European data space in industrial value ecosystems by defining tested and verified rules and practicalities for scalable data sharing, taking into account technical, legal, ethic and business aspects.
8	As the dependable IoT solutions are improved with holistic concepts, they are complemented with an appropriate toolchain. Despite each toolchain focusing on own scope, the tools should aim to complement each other, hence, capturing the complete spectrum of challenges. Their advantage is a flexible methodology, which is independent of the application domain. There is an expanding range of such domains, which require solutions, hence offering a chance for increased exploitation.
9	It is recommended to develop (modular) portable tools with the ability to be applied to different domains. Should successful exploitation occur, portability is also a highly recommended aspect for any development within the IoT world. The dependability methods and tools ought to be developed in a generic and domain agnostic manner. They should come into consideration at the design stage, as adding dependability methods in post-design stages is a cumbersome and complex process with the potential to expose opportunities for cyber-attacks due to a non-holistic solution to the challenge.
10	Designing a complex IoT ecosystem in a reliable and functional manner could benefit from the usage of a computational recommender system, which relies upon analysis of specific requirements and high-level architecture patterns.
11	Trustworthy localisation is a necessity in many IoT applications. This goes beyond security and reaches deep into the safety aspect of the many domains and their applications. One must pay attention to the evolution of the available techniques not to be left behind in terms of development. This kind of evolution is also followed by the evolving data encryption methods, which are crucial for secure data transmission and avoidance of security incidents.
12	A crucial aspect of all proposed design techniques, methods and tools is intuitive usability. An increasingly promising method of ensuring system resilience is seen in self-healing techniques. These offer a proper adaptation to failures and attacks.
13	Vehicle communication must offer a high degree of dependability and as such, must be supported by a trustworthy connection to: <ul style="list-style-type: none"> ➤ Aid improvement of acceptance rate ➤ Ease operational activities e.g. opening an opportunity to remotely perform vehicle maintenance
14	Due to an increased sensitivity of industrial applications to cyber-threats, secure communication must guarantee seamless operation with the elimination of attacks to maintain minimal down-times i.e. beyond minimising the failures. The benefit is secured through the usage of different tools and methods, such as authentication, encryption, access control, remote access, validation and matching processes. Future activities must also consider the protection of operations from intruders to guarantee data privacy.
15	The following characteristics should be considered in future development and applications: <ul style="list-style-type: none"> ➤ Fast and uncomplicated integration ➤ Easy maintenance and update of the system ➤ Global decentralised commissioning ➤ Central logging and monitoring ➤ Redundant system ➤ Individual single encryption, also for virtual machines and data containers ➤ Comprehensive logging and encrypted recording of remote access ➤ Full-automated exchange of systems in the event of failure by hardware suppliers ➤ Bypass internet connections through 3G–5G

16	Continual penetration testing is recommended in support of guideline specification and the creation of recommendations for future technical development.
17	An extensive benchmark of solutions is endorsed across domains to seek common solutions across a broad range of industrial settings.
18	It is recommended to shift away from solutions that focus on specific technologies, some of which are prone to changes. Instead, the focus could be placed on flexible and secure hardware concepts in combination with a future-proof system design.
19	Continued intensive actions within the ecosystem are highly appreciated (see Figure 4).

6. Conclusion

By offering an overview of IoT4CPS' exploitable results, this document report on opportunities and recommendation for trusted IoT based on the lessons learnt from IoT4CPS. The generated assets are providing enhancements to two industrial domains (AD and Industry 4.0), which is also evaluated in project demonstrations. The value offered by the generated assets provides a possibility to maintain a sustainable path for the project outcomes. A set of realistic recommendations is provided on several levels i.e. project itself, continued collaboration between project partners and continual collaboration within the ecosystem. The key finding is that in the world of ever so more complex CPS and the tasks that they perform, there is an explicit need to cooperate and cross-fertilise across institutions and the domains.

7. References

- [1] E. Armengaud, B. Peischl, P. Priller and O. Veledar, "Automotive Meets ICT—Enabling the Shift of Value Creation Supported by European R&D," in *Langheim J. (eds) Electronic Components and Systems for Automotive Applications. Lecture Notes in Mobility.*, Cham, 2019.
- [2] O. Veledar, New business models to realise benefits of the IoT technology within the automotive industry, Vienna: WU ExecutiveAcademy, 2019.
- [3] G. Macher, C. Schmittner, O. Veledar and E. Brenner, "ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell," in *Casimiro A., Ortmeier F., Schoitsch E., Bitsch F., Ferreira P. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2020*, 2020.
- [4] A. M. Shaaban and C. Schmittner, "Threat-get: New approach towards automotive security-by-design," in *28th Interdisciplinary Information Management Talks*, 2020.
- [5] J. Bessant and J. Tidd, *Innovation and Entrepreneurship*, 3rd ed., Chichester: John Wiley & Sons Ltd, 2015.
- [6] G. Macher, K. Diwold, O. Veledar, E. Armengaud and K. Römer, "The Quest for Infrastructures and Engineering Methods Enabling Highly Dynamic Autonomous Systems," in *Walker A., O'Connor R., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science, vol 1060*, Springer, Cham, 2019.
- [7] O. Veledar, V. Damjanovic-Behrendt and G. Macher, "Digital Twins for Dependability Improvement of Autonomous Driving," in *Systems, Software and Services Process Improvement. EuroSPI 2019. . Communications in Computer and Information Science, vol 1060.*, Springer, Cham, 2019.