IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D8.1
IoT4CPS value proposition and positioning in national and European ecosystem

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

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: IoT4CPS value proposition and positioning in national and European ecosystem
Type: Public (this is a shortened version of the full confidential deliverable)
Editor(s): Omar Veledar
E-mail: omar.veledar@avl.com
Author(s): Omar Veledar (AVL), Julia Pammer (SBA), Eric Armengaud (AVL), Michael Jarne (NXP), Peter Priller (AVL), Mario Drobics (AIT), Stefan Jaksic (AIT), Christoph Striecks (AIT), Heribert Vallant (JR), Violeta Damjanovic-Behrendt (SRFG), Edin Arnautovic (TTTech), Christos Thomos (IFAT), Julia Pammer (SBA), Ezio Bartocci (TUW), Andreas Martin (AIT), Patrick Traxler (SCCH), Irene Karitnig (IFAT), Christos Thomos (IFAT)
Doc ID: 8.1

Amendment History

Version	Date	Author	Description/Comments
V0.01	05.04.2019	Omar Veledar and Eric Armengaud	Initial version prepared
V0.02	06.05.2019	Omar Veledar and Julia Pammer	Core content (prior to project's 4th plenary meeting)
V0.03	13.05.2019	O Veledar, P Priller, M Drobics, S Jaksic, C Striecks, H Vallant, C Schranz, F Strohmeier, V Damjanovic-Behrendt, E Arnautovic, C Thomos, J Pammer, E Bartocci	Post project's 4th plenary session
V0.04	15.05.2019	O Veledar, E Armengaud, P Priller	Content analysis and detailed exchange with WP2
V0.05	27.05.2019	O Veledar and Eric Armengaud	Rework
V0.06	29.05.2019	O Veledar, Michael Jarne, H Vallant, V Damjanovic-Behrendt, I Karitnig, C Thomos	Consolidation of further partner contributions into version for internal review
V0.07	06.06.2019	Andras Martin (AIT)	Document reviewed
V0.08	13.06.2019	Omar Veledar (AVL)	Final updates for submission
V1.00	13.06.2019	Andreas Martin and Mario Drobics (AIT)	Final version

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

Abbreviations

AD	Autonomous Driving
ADAS	Advanced Driver Assistance System
CAN	Controller Area Network
CPS	Cyber-Physical System
Dx.y	Deliverable (x = WP number, y = deliverable identifier within that WP)
EFFRA	European Factories of the Future Research Association
MFVEA	Failure Mode, Vulnerabilities and Effects Analysis
Ind4.0	Industry 4.0
IoT	Internet of Things
STAMP	System-Theoretic Accident Models & Processes
UC	Use Case
V2X	Vehicle to Everything
WP	Work Package

Executive Summary

This deliverable is a product of cooperation between IoT4CPS partners, as organised within WP8 and WP9. It defines the purpose of the consortium and the project and it focuses onto impact creation that is resulting from active collaboration within the projects. The document describes technical advances in terms of safety and security design methods, security and verification analysis and lifecycle management. The new building blocks are contributing towards creation of trusted IoT technologies. The project is using two main use cases (as well as few smaller derivatives of the main use cases) to determine the suitability of the developed technological advances in the field of Autonomous Driving and Industry 4.0. The project is also relying on wide core business competencies and diverse set of partners to provide cross-fertilisation across the industrial domains. The main form of impact creation is envisaged through increase of usage of results and effective maximisation of project benefits. These are also complemented with national and international exposure of the project.

The business development opportunities are yet to be fully exploited and there is a chance that potential improvements will further open up during the second half of the project. The current technological advances are performed on the level of technology bricks. It is their integration that is likely to increase a number of potential improvements and eventual exploitation of the same for business purposes. However, the project is on a stable course to fulfil the initial exploitation plans in terms of business development.

1. Introduction

This IoT4CPS project deliverable is created through partner cooperation in the work package for impact creation (WP8). The work is also tightly correlated to WP9 (Dissemination & Communication Measures). The goal is to report on impact created in the first phases of the project and consequent value proposition and project positioning in national and European ecosystem.

1.1 Cooperative impact creation through project as a temporary organisation

Impact analysis answers a very basic question of what the purpose of the consortium is and why the project is performed. It is difficult to justify the time, the cost and the effort invested into any activity if provisions of results and deliverables are not then transferred into usage. Hence, rather than delivering unique output as a response to the set of project goals, which is normally done through technical project deliverables, this document considers impact creation as a result of cooperation between the project partners and their interactions within consortium and with the external stakeholders. The impact creation is less focused on results and is more orientated towards actual and potential imprint on communities that is created through implementation of the technical solutions. It is used to not only contribute to turning ideas into reality in terms of assets, but also as a part of transformational process for the project partners and the neighbouring communities in a quest to shine the light on the future of integrated Internet of Things (IoT) and Cyber-Physical Systems (CPS).

The impact created through the temporary project organisation should also be aligned to the organisations' strategies. As the consortium is formed by a set of diverse partners with different interests, it would be impractical to satisfy boundary conditions determined by all participating organisations. Hence, the impact creation is to be aligned to project's overall sustainability related goals in combination with the strategy of the funding bodies and the participating organisations. The lighthouse nature of IoT4CPS in its essence highlights the need for a sustainability drive, as one of the major aspects of the project that is necessary for value maximisation and delivery of solutions and benefits to overall stakeholders. The strategic approach to sustainability increases the chances of achieving the desired benefits.

1.2 Document aims and structure

This document aims to provide an interim review of expected project impact on wider communities within industrial and academic domains and across geographies. In combination with further planned activities within the project, such a consolidated review closes the feedback loop by providing steering recommendations for the remainder of the project.

The rest of this document is structured in following form. Section 2 describes the high-level planning process in terms of impact creation, which integrates consequent technical developments in its subsection 2.1, as well as their aiming towards usage increase through demonstrations described in subsection 2.2. The specific (achieved and expected) benefits resulting from project deliverables are presented in section 3. The promotion channels of project deliverables on national and international level are presented in section 4. This section also identifies national and European projects with high correlation and shared exploitation potential. Such a formulation helps position the project within the relevant ecosystem. Section 5 provides an intermediate business update resulting from the current technological developments. Section document is rounded with section 6 which identifies intermediate recommendations for the project partners.

2. IoT4CPS advances

As depicted in **Figure 1**, IoT4CPS and especially its technical WPs focus on delivery of results through deliverables and their demonstrations within the boundaries of the use cases. The impact can only be created through maximisation of the usage and the resulting active interaction with the external stakeholders. Such activities are expected to widen the project benefits.

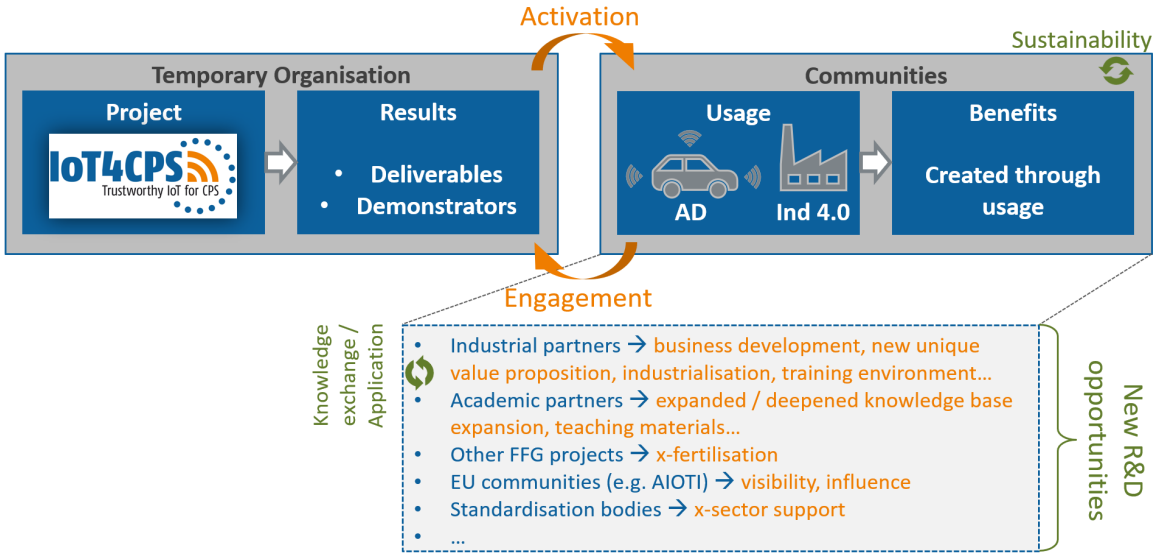

Figure 1 Focus on usage of developed technology bricks

In line with the concept portrayed in **Figure 1**, the IoT4CPS planning of the initial phase was performed from right to left i.e. usage is placed into a primary focus. The identified exemplary use cases are based around Autonomous Driving and Industry 4.0. Consequently, standard requirement engineering procedures are applied in WP2, which resulted with specifications for technological building blocks and demonstrators within the boundaries of the identified use cases, as described in IoT4CPS deliverable 2.2 (Consolidated business needs). A major challenge of such consolidation of needs and their formalisation into technical requirements for WP3 (Safety & Security Design Methods), WP4 (Security Verification & Analysis) and WP5 (IoT Life-Cycle Management), is the need to respond to heterogeneous business needs that are covering a wide range of interests, technologies and approaches.

Contrary to the planning, the sustainable implementation within and beyond IoT4CPS is performed from left to right (**Figure 1**). As originally proposed, IoT4CPS partners are through collaboration putting an effort into creation of deliverables. However, these, as simply the means to an end, are directed towards accomplishing specific outcomes, aimed at providing sustainable benefits. Hence, the WPs 3-5 are focusing on results with the usage in mind (through implementation of requirements and specifications of WP2), as it is the usage, rather than the deliverables themselves, that is yielding long-lasting benefits. It is the usage of these results that is expected to create impact on communities and eventually generate benefits for the involved stakeholders. In line with the planning, at this half-way stage of the project, the technical WPs are showcasing their progress in terms of laboratory prototypes of intended technology bricks. They are also reporting development of their security concepts as envisaged within IoT4CPS. As the demonstrators are becoming available, it is up to the project partners to test their usability and possible level of integration into two identified domains (AD and Ind 4.0). Successes in that direction have a potential to reach the full range of stakeholders and hence address their enthusiasm for, as well the potential resistance to the offered technological advancements.

2.1 Trusted IoT technologies

The main technical developments of IoT4CPS are performed in WPs 3-5. This is where the project is aiming for delivery of technology bricks needed for trusted IoT solutions. The developments are grouped in three

categories: safety and security design methods, security verification and analysis as well as lifecycle management.

2.1.1 Safety and security design methods

The primary target of the safety and security design methods currently being developed is to establish guidelines, methods and tools required for safe and secure IoT for CPS. The currently developed solutions include, but are not limited to:

- Dependability design methods, such as:
  - STAMP-based method for planning and concept phase for CPS road networks
  - Security tools and methods: FMVEA, MoReTo, GSFlow
  - Recommender System for dependable IoT applications
  - Self-Healing by Structural Adaptation
- Trustworthy localisation methods
- Resilient system architecture pattern and concepts and hardware (HW) - based solutions for safe & secure IoT
- Scalable and efficient crypto algorithm for IIoT

The technical design and concepts are described in IoT4CPS D3.1 (Design & Methods Concept), while the guidelines and recommendations at the mid-term of the project are reported in D3.3 (Guidelines and recommendations for resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT) and D3.5 (Guidelines and recommendations for the use of cryptography to build trustworthy IoT applications). These guidelines provide specific recommendations in terms of resilient architectures and integration of cryptographic components into crucial IoT solutions of the project. They also offer directives for the related work outside of the scope of this project, hence widening outreach possibilities and extending the impact. The recommendations do not only refer to the integration within IoT4CPS during the second half of the project but are also relevant for the external stakeholders (now, as well as in the future), especially for developers and hardware and software architects. The intent of IoT4CPS partners is to integrate these design methods within the boundaries of the recommendations and hence to tempt to improve usage. The usage increase is then the basis for impact creation and maximisation of benefits of IoT4CPS.

In terms of specific outputs, IoT4CPS is tapping into research and application of self-healing techniques with and without redundancies. Such solutions are aiming to improve safety of autonomous driving (through substitution of failing sensors and redundancy of control components). The added benefits are expected to leave a positive mark on acceptance from both public and industrial stakeholders.

IoT4CPS is also developing scalable, efficient low-latency cryptography algorithms for IoT solutions, which are exploitable in industrial environment.

In terms of immediate impact that is not limited to industrialisation, we strongly believe that the publicly available roadmap that was developed with support of IoT4CPS: “A Roadmap Towards Resilient IoT for CPS”[1], is an excellent exploitation resource by a range of stakeholders when considering their future ambitions within the field, as it provides our view on consolidated the current and expected challenges facing integration of IoT and CPS. More importantly, it summarises our suggestions for potential sustainable solutions for building a resilient IoT for CPS. The offered solutions are undergoing the process of optimisation and benchmarking, hence influencing the complete ecosystem through provision of recommendations and identification of potential paths of future development. That is especially the case in the sphere of detection and recovery, as well as the future work on distributed approaches. As some of those activities are performed in collaboration within the consortium, additional consortium cohesion is being achieved, be it through strengthening of internal links or through knowledge exchange.

[1] arXiv:1810.06870v2

2.1.2 Security verification and analysis

The security aspects of the future applications are considered in both terms, project specific and general. The common criteria, as identified in WP2 and WP4, are used for development of initial Protection Profile, which focuses on security characteristics of automotive Ethernet technology. The Protection Profile covers threats, security objectives, and formal security functional requirements for automotive Ethernet. Furthermore, the protection profile maintains traceability between threats, objectives and requirements, which is a valuable factor that contributes to dependability of fail operation safety features.

The internal cooperation is strengthened through knowledge exchange between the scientific and industrial partners and intended application of provided security solution in industrial products. In particular, this is seen in collaborations through threat modelling, results of which is being integrated into some partners' industrial product.

The project has also already contributed to an improvements of certain security verification practices at the level of commercially available products. The resulting security improvements are contributing towards lowering resistance towards the new technology.

These technical developments are also incorporating human aspects within the systems. Thereby, the security protocols focus on integration of human factors. This is relevant for impact creation, as majority of the CPS rely on human interactions. That is also the case in both of IoT4CPS application domains, AD and Ind 4.0. Future solution must integrate forms of human-to -machine interactions that could be based on speech, haptics, gestures, vision and human perception. Although, there is an evident drive towards minimization of human interactions and increase of automation, human interventions are still necessary.

Further technological impact is determined in terms of generation of automated test cases. Industrialisation of such a concept, which increases coverage of broker implementation, is expected to be favourable due to the rapid increases in data generation and management. The laboratory demonstrations will soon have to seek a way towards industrial releases. The impact creation is also expected through increased collaboration of consortium partners through data sharing models.

2.1.3 Lifecycle management

Lifecycle data models and methods for data capturing and data management in Smart Manufacturing and Smart Automotive sectors are of crucial importance in terms of impact creation of IoT4CPS. The existing standards and data models offer an opportunity for potential enhancements in these two sectors. The generated Digital Twin demonstrator considers the existing standards and provides a set of guidelines for further improvements. These are to be tested and implemented in cooperation between scientific and industrial partners within the project. The impact carrying guidelines are to be brought to the market and also offered as a set of recommendations to other stakeholders in the fields of Smart Manufacturing and Smart Automotive sectors.

The main impact is expected to arise from utilisation of lifecycle data models that support new digital manufacturing initiatives across Europe and are relying on Industry 4.0 technologies, e.g. Internet of Things (IoT), Cyber Physical Systems (CPSs), Smart CPSs, Smart Data and Smart Factory. The various elements of the digital models that are already developed within IoT4CPS are being moved from the current broad view towards specific expectations of autonomous driving. The intent is to demonstrate the usefulness of the current concepts and to increase their usage in industrial environment.

In addition to the base applications derived through implementation of digital twins, they are also targeting further improvements of available gateway honeypots. The resulting learnings are mutually beneficial, as they also provide feedback loop for further improvements of the digital twins' security methods.

The European Commission's Digitising European Industry (DEI) initiative places an emphasis on future digitalised platform infrastructures to interact with each in a trustworthy manner. This work is heading towards satisfaction of such needs at a high degree of trade-offs between safety, security and availability, as well as monitoring and supervision capabilities in run-time.

2.2 Industrial application

Current trends within automotive industry signify high levels of uncertainty for the sector. Possibly strongest trends are AD and Ind 4.0. Their influences have also dictated the choice of industrial applications that are interwoven throughout IoT4CPS. The demonstrations are primarily pointing at overcoming resistance through technological reassurances. They are also contributing towards impact creation through a range of means of providing positive change[2]:

- Increased visibility and promotion of developed technology solutions
- Provision of own perspective and determination of potential direction through offering lessons learned and technological guidelines
- Promotion of the higher vision, as it fits to a project of a lighthouse status, so to encourage follow-up cooperation and to provide guidance
- Integration of technologies and skills of several partners aimed at improving performance through building on each other's strengths
- Flexible approach in terms of components used and their specifications, yet fixed goals in mind
- Encouragement

It must be noted that reasonable project limitations (scope, time and budget) prevent all technological solutions to be demonstrated. Hence, smaller strategic samples are chosen to demonstrate progress of highest potential impact.

2.2.1 Architecture for safe and secure automated driving platform

A demonstration platform for autonomous driving encompasses a range of technical capabilities. Its core is a CPS capable of hosting high-performance computing and connectivity solutions. Simultaneously, the inevitable shift towards autonomous driving does not fit well with safety-critical tasks due to an underlying conflict between the vast number of possible situations that could be encountered by an autonomous vehicle and the safety domain's perspective, which demands extensive testing. The demonstrated architecture combines the expected sensors (with their strengths and weaknesses) with the analytical and decision-making processes that must satisfy safety standards through decision making at minimum acceptable time frames. The non-trivial data management considers the gradual transfer of decision-making processes from humans to the machines in potentially hazardous traffic circumstances. The demonstrator utilises developed technologies to deliver a safe, secure, efficient and reliable chain. The fail-operational aspect of the platform and the trusted and secured computing base are of the highest importance in terms of impact on autonomous driving, as such characteristics offer several possibilities to help resolve current challenges presented by the autonomous driving. Its computational power enables monitoring, control and collection of vehicle data close to the physical world. The analytics performed near the source, at the edge of IoT network, help ensure component operational integrity and supports data security. These technological advances are actively spearheading the trend of autonomous driving.

The architectural aspect of V2X communication that is utilised for accurate, reliable and timely information exchange is also demonstrated. Once again, the crucial factor of data management is road safety and prevention of accidents. The communication impacts autonomous driving by being the key enabler that ensures road safety, enhances human perception and driving comfort and provides novel infotainment capabilities.

2.2.2 Use-Case Applications in Industry 4.0

The demonstrator is offering a generic architectural solution that is reusable by the industry in the future. A compromise solution must be implemented, as it is not possible to demonstrate securing of a complete factory. Hence, the technical concepts are broken down to smaller sections and evaluated individually. It is determined

[2] Rosabeth Moss Kanter, TED talk, 2016

that this chain of solutions that could eventually be integrated into a complete picture must form a chain of trust. The chain may not be complex, as it should lend itself to simple installation and maintenance with no need for complex specialist training. However, it should still exhume usability and capability to detect and deal with a range of specific threats. The simplicity of installation and maintenance combined with the ability to cover threats is what lends the concept to creation of impact in terms of Ind 4.0 applications. The impact creation is to be further maximised by generalisation of the concept as much as possible, so that easy usage also contributes to sustainability of the solutions in post-project phase.
Specific technology solutions that are being developed and that will contribute to the demonstrator include, but are not limited to:

- Improvements in basic communication technology capabilities and limitations at semiconductor level and consequently support to secure and reliable connectivity requirements set by Ind 4.0 edge gateways, which contributes to trustworthy radio connectivity for Ind 4.0
- Traceability of components and systems focusing on threats, as they occur throughout life-cycle
- Security by isolation

3. Impact through benefit realisation

Through new contributions to fundamental knowledge on development and operation of trustworthy CPS, IoT4CPS is providing a fertile ground for benefit creation aimed primarily at two distinct categories: AD and Industry 4.0. However, the benefits in terms of security and trustworthiness of IoT are not limited to those two domains only. The main benefits are seen in increase of security and trustworthiness and resulting impact on ecosystem, but also in terms of economic impact, as originally envisaged in the Business Model Canvas.
As described in section 2 and depicted in **Figure 1**, it is the usage of the project outcomes that creates benefits. The impact creation is equally possible through increase of usage, but also through benefit maximisation and their outward orientation and communication. As it is the project outcomes that are a starting point for impact creation their broad overview is listed in Table 1, which shows actual and expected results being derived from completed deliverables, as well as of the deliverables that are currently in preparation. At the intermediate stage of the project, maximisation of benefits is relatively limited due to a lack of maturity. It is expected that a more precise benefit realisation map is to be generated for the updated final version of this deliverable towards the end of the project.

Table 1. Impact creation through maximisation of benefits

	D	Deliverable description	Changes	(Potential) Usage	Benefits
Completed Deliverables	D9.1	Initial Dissemination Plan and project website	Enabled digital presence, enhanced project awareness, increased visibility, improved sustainability, simplified and enabled communication	Technical cross-correlation, exploitation of technical results, creation of new consortia, implementation of new guidelines	National and international presence within a range of communities, added cross-fertilisation with other projects and domains, improved internal and external communication, sustainability drive, stakeholder engagement
	D1.1	Initial Data Management Plan	Data definition, defined data structure, provided legal framework, established framework to support research data	Data collection, analysis and exploitation of results	Better usage of time and resources, improved data safety, improved internal cooperation, satisfied regulatory requirements, enhanced communication between internal stakeholders
	D5.1	Data Models for the IIoT and Industry 4.0 and in the automotive sector	Contributions to technical roadmap, defining technical exploitation, clarified state-of-the-art, envisaged	Following pre-defined technical roadmap, exploitation of data within a pre-defined framework, Digital	Consolidated specific requirements, improved self-adaptivity and self-optimisation potential,

			potential technology boosts	Twin as a safety and security component	determined direction for technical advances
	D2.1	Consolidated state-of-the art report	Research aligned to community standards, clarified state-of-the-art	Integration of specific methodologies for trustworthy IoT into industrial products	Consolidated technology approach, streamlined technical improvements
	D2.2	Consolidated business needs	Defined market requirements, integration into clearly defined industrial use cases	Implementation of technology bricks into use cases (AD and Ind 4.0)	Improved exploitation potential through working within use cases with clear marketable opportunities
	D3.1	Design & Methods Concept	Development aligned to results of risk identification and analysis, compliance with standards and best practice guidelines, optimised risk treatment decisions	Offering security by design in the final marketable products	Improved safety and security of IoT solutions during the design process
	D6.1.1	Architecture for safe and secure automated driving platform demonstrator	Determined methods of incorporating V2X communication into two use domains, defined cooperation for platform integration into use cases	Application of improved safety and integrated security in the AD functions, integrated security for Ind 4.0 applications, implemented V2X communication for AD	Improved safety and security of go-to-market solutions
	D9.2.1	Annual updates on the dissemination plan, incl. reporting	Created dissemination plan, definition of measurable criteria for dissemination related activities, communication strategy clarified, identified marketing opportunities	Creation of new opportunities through project marketing, alignment with other communities	Increased project visibility, enhanced stakeholder engagement, created basis for future collaboration(s), project marketing (internal and external)
	D1.2	Year 1 Project Report	Demonstrated transparency, clarified and documented achievements and shortcomings	Continued collaboration	Satisfied regulatory requirements, improved motivation, improved understanding of

					current position and needed progress
	D4.1	Automotive Ethernet protection profile	Definition of security characteristics of automotive Ethernet technology	Replacement or complementing of the CAN bus communication with the automotive Ethernet	Serve as a draft Protection Profile to get an understanding if the Common Criteria are suitable for application to automotive in-vehicle networks and, potentially, to automotive information technology in general
Current deliverables	D3.3	Guidelines and recommendations for resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT	Established guidelines	Implementation in AD and Ind 4.0 use cases	Improved system resilience, impacting wider community, potential standardisation activities
	D3.5	Guidelines and recommendations for the use of cryptography to build trustworthy IoT applications	Created guidance for API design for cryptographic libraries, created guidelines for implementing cryptographic algorithms in hardware	Exploitation of cryptographic methods in use cases, build-up of consumer trust	Improved security of use cases, potential standardisation activities
	D4.3.1	Analytical Toolbox first release	Implemented verification and analysis methods in design and product release stages	Secure verification and analysis for product releases, secure products, network traffic protection	Improved security of products through anomaly detection of OS and HW, minimised effects of cyber-attacks
	D4.4.1	Laboratory demonstrator of automated testing first release	Integrated technology bricks, demonstrated improvements	Industrialised automated testing	Improved security (and safety)
	D5.2	PLCDM Stakeholder Perspectives	Defined research direction of the hardware-enabled identity management	Eased adjustment of digital twin concept within industrial standards	Implementation of the newly defined multi-tenancy aspects of data models required for digital twins in industrial environment

	D5.4.1	Identity management, security and safety aspects of IIoT PLCDM	Security features and safety issues represented as data points over the product life cycle, added semantic enhancements to the component tracing	Life-cycle management and standardised digital twin of industrial systems	Improved security life-cycle management, standardised way of evolving the "digital twin" concepts through both, security and product lifecycle data management
	D5.5.1	Life cycle data management prototypes	Ensured life-cycle data management compliance with different regulations	Enhancing privacy and third-party data usage, automotive components life cycle data management	Security validations through Digital Twins; improved privacy and safety aspects
	D8.1	IoT4CPS value proposition and positioning in national and European ecosystem	Enhanced internal collaboration, clarified standardisation aspect, identified future impact creation potential	Product standardisation, project marketing	Increased awareness of achievements and shortcomings, improved motivation and collaboration potential, enhanced sustainability

In summary, through communication and cooperation, as well as resulting cross-fertilisation with other projects, initiatives and communities, IoT4CPS is improving its presence and influence. The resulting stakeholder engagement is at the heart of impact creation.
On a technical level, improvements in efficiency, data security and driving safety, as well as recommendations for the regulatory and standardisation requirements are helping IoT4CPS to leave the stamp within its ecosystem. In general terms, positive impact on dependability of the proposed solutions is steadily influencing the stakeholder engagement practices. The improvements in terms of life-cycle management and data management are positively influencing the fledging area of European data economy.
The technological applicability to the demonstrations is also positively correlated to an increase of the exploitation potential and are helping envisage clear marketable opportunities.
Possibly the most influential undercover signs of impact creation on the surroundings is seen in a slow but steady decimation of the resistance to the IoT technology. IoT4CPS is contributing to such activities through demonstrations and communication of its achievements towards the full range of stakeholders.
The sustainability drive of IoT4CPS is significantly impacted and is also impacting the relevant ecosystem through continual networking and promotion. These activities are already resulting with new practical ideas and initiatives in terms of future projects.

4. Relevant national and European ecosystems

In line with the flagship charter, IoT4CPS is also targeting increase in the visibility of Austrian technologies, products, procedures and services for trustworthy IoT at a national and international level by the creation of a dedicated Austrian Industrial IoT cluster and participation of IoT4CPS members in the different Austrian and European expert groups as well as standardization activities as listed in Table 2 of the project proposal. Table 1 is an updated version of the same table pointing at planned national networking activities.

Table 2. Updated overview of national networking activities

Name	Who	Target Group	IoT4CPS Relation
IoT-Austria https://www.iot-austria.at/	AIT, DUK	Groups of individuals and organisations with knowledge, experiences and interest in IoT in Austria and wider.	An association that supports digital transformation across Europe. It enables IoT4CPS partners to discuss IIoT related security aspects with interested stakeholders.
OVE, TK MR 65 https://www.ove.at/	AIT, DUK, IFAT	Austrian enterprises and institutions as well as experts and interested parties from the entire field of electrical engineering.	Contributions to national certification and standardization activities, increasing project visibility by informing stakeholders of project results, cooperating regarding safety & security for the industrial domain on the national level.
Austrian Standards https://www.austrian-standards.at/	AIT, SBA	Parties with interests into standards for Austrian, European and global markets.	Contributions to national certification and standardization activities, cooperation on the national level regarding safety and security for the automotive domain.
Verein Industrie 4.0 Österreich https://plattformindustrie40.at/	AVL, AIT, IFAT, JR, SBA, TUW	Stakeholders interested into technological developments and innovations in the context of Industry 4.0.	Participating in consolidation process and disseminating results to platform members.
Platform Industrie 4.0 Oberösterreich https://plattformindustrie40.at/	SCCH, X-Net	Industry and research partners related to I4.0	Collaboration regarding usage of IoT in industrial domain.
AC Styria https://www.acstyria.com/	AVL, JR, NXP	A network of approximately 300 Styrian companies operating in automotive and aerospace industries and rail system.	Collaboration regarding usage of IoT in the automotive domain.
Alp.Lab https://www.alp-lab.at/	AIT, AVL, JR, TTTech, SAGÖ	Strategic Austrian partners in the field of components and systems of automated driving.	Contributions to the development of security and privacy standards related to the automated driving

			domain. Joint activities on security testing.
Austrian Traffic Telematics Cluster (ATTC) https://www.attc.at/	JR, AIT	Leading Austrian research, commercial and industrial companies with interest into furthering the development and practical application of new technologies in the field of telematics systems for traffic infrastructure.	Awareness about IoT Security related to Car2X.
Gesellschaft für Mess-, Automatisierungs- und Robotertechnik (GMAR) http://www.gmar.at/	DUK	Austrian companies, research and educational institutions operating in the fields of measurement, automation and robot technology.	Increase awareness and impact among industry and academia in the field of instrumentation, automation, robotics and measurements.
ECSEL Austria https://www.ecsel-austria.net/	AVL, TTTech, NXP, SBA, IFAT, SAGÖ	Primarily industrial, but also scientific organisation representing the technology areas of micro and nanoelectronics, embedded systems and systems integration.	Synchronisation with ECSEL Austria community to increase the impact and visibility of the IoT4CPS project.

In addition to the national activities, IoT4CPS partners are also actively promoting project outcomes within European communities, the main sample of which are presented in Table 3.

Table 3. Overview of European networking activities

Name	Who	Target Group	IoT4CPS Relation
AIOTI https://aioti.eu/	AIT, AVL, NXP	Alliance for Internet of Things Innovation.	Dialogue and interaction in terms of IoT developments and their trends and applications. Influencing through white-paper creation. AVL is co-chairing a Work Group on Smart Mobility
BDVA http://www.bdva.eu/	AIT, JR, TUW	Big Data Value Association.	Cooperation in terms of Data Management, Data Analytics, Data Protection, Data Visualisation.
ECSEL-JU https://www.ecsel.eu/	AIT, AVL, IFAT, ITI, NXP, TTTech, TTTechA, SAGÖ	Public-Private Partnership for Electronic Components and Systems.	Promoting the project results and increasing impact among industry and academia in the area of electronic components and systems, as well as the applications.
EFFRA https://www.effra.eu/	SRFG	European Factories of the Future Research Association	Promoting the project innovative results to the European network with an interest in the Factories of the Future Public-Private Partnership.

Horizon 2020 https://ec.europa.eu/programmes/horizon2020/en	ALL partners	EU framework programme for research, technological development and innovation.	Creating visibility for the project results extending dialogue in terms of IoT and its uses.

At the national and EU project level, it is possible to identify certain cross-correlations in terms of benefit realisation and enhanced impact creation as a result of organisations' activities in multiple projects. Such a sample of European projects is shown in Table 4 and at the national level in Table 5.

Table 4. Other national projects with some correlation and possible shared exploitation

Project Name	Who	Project focus	IoT4CPS correlation
CPS/IoT Ecosystem (HRSM + FFG)	AIT, TTTech, TUW	Bringing closer together CPS and IoT into a single ecosystem by evaluating intersection points in theory and in practice.	Development of new smart applications.
Dependable Things	TUG	Dependability of IoT solutions that are resilient against failures and attacks.	Dependability of IoT devices
DMA – Data Market Austria	AIT, DUK, JR, SAGÖ	Data management and exploitation within the newly created data economy.	Technological innovations in terms of data management, as well as controlled access to distributed cloud services.
DGT – Dynamic Ground Truth	TUG, TTTech, AVL	Improving ADAS and ADF development processes to the maturity levels demanded by the markets.	The correlation is evident in use case representing AD, but is also seen in reliable capturing of vehicle environment data.
REALISM - Real-time simulation of multiple connected Autonomous	AIT, AVL	Real-time simulation of multiple connected Autonomous vehicles with the crossover in terms of V2X communication and related simulation tools.	V2X communication and fleet monitoring applications.
SALSA	TTTech	Living safety and security cases for cyber-physical systems certification.	CPS and related security and safety of AD.

Table 5. EU funded projects with certain level of correlation and possible cross-fertilisation

Project Name	Who	Project focus	IoT4CPS correlation
AQUAS (ECSEL-JU)	AIT, SAGÖ	Bringing novel Safety-Security-Performance co-engineering methods into mainstream industrial practice.	Security and Safety Engineering Methods, Dependability design methods.
Car2Tera (H2020)	IFAT	In-cabin radar and onboard, high speed data communications.	IoT and 5G connectivity for sensor data communication.

CPSwarm (H2020)	TTTech	Tool chain for autonomous CPSs.	Safety critical applications using CPS.
Cybersec4europe (H2020)	AIT	Cyber-security through test and demonstration of potential governance structures for the network of competence centres.	Cyber-security.
DEIS (H2020)	AVL	Assuring dependability of CPS.	Safety and security for AD and integrated full life-cycle dependability.
M3TERA (H2020)	IFAT	Wide-spread use of low-cost THz technology in society, enabled by the proposed micromachined heterogeneous integration platform.	Connectivity of the future and impact on society.
Prystine (ECSEL-JU)	AVL, TTTech	Fail-operational Urban Surround perceptION (FUSION) which is based on robust Radar and LiDAR sensor fusion and control functions.	Safety and security of AD. Security of connectivity solutions.
SEMI40 (H2020)	IFAT	Smart Production and Cyber-Physical Production Systems.	Cyber-security for CPS and industrial digitalisation.
SERUMS - Securing Medical Data in Smart Patient-Centric Healthcare Systems (H2020)	SCCH	Security and privacy of future-generation healthcare systems, putting patients at the centre of future healthcare provision, enhancing their personal care and maximising the quality of treatment they receive.	Security and privacy-preserving algorithmic techniques such as storing data that cannot be linked to individuals or (cyber-physical) systems.
SPARTA - Strategic Programs for Advanced Research and Technology in Europe (H2020)	JR	SPARTA is a Cybersecurity Competence Network, with the objective to develop and implement top-tier research and innovation cooperative actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap,	Within SPARTA the following four research and innovation programs are addressed • Full Spectrum Situational Awareness • Continuous Assessment in Polymorphous Environments • High-Assurance Intelligent Infrastructure Toolkit • Secure and Fair AI Systems for Citizen Some of the challenges addressed in these programs have a relation to IoT4CPS topics.

One of the direct results that 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. A graphical representation of IoT4CPS' fit into the ecosystem is shown in figure

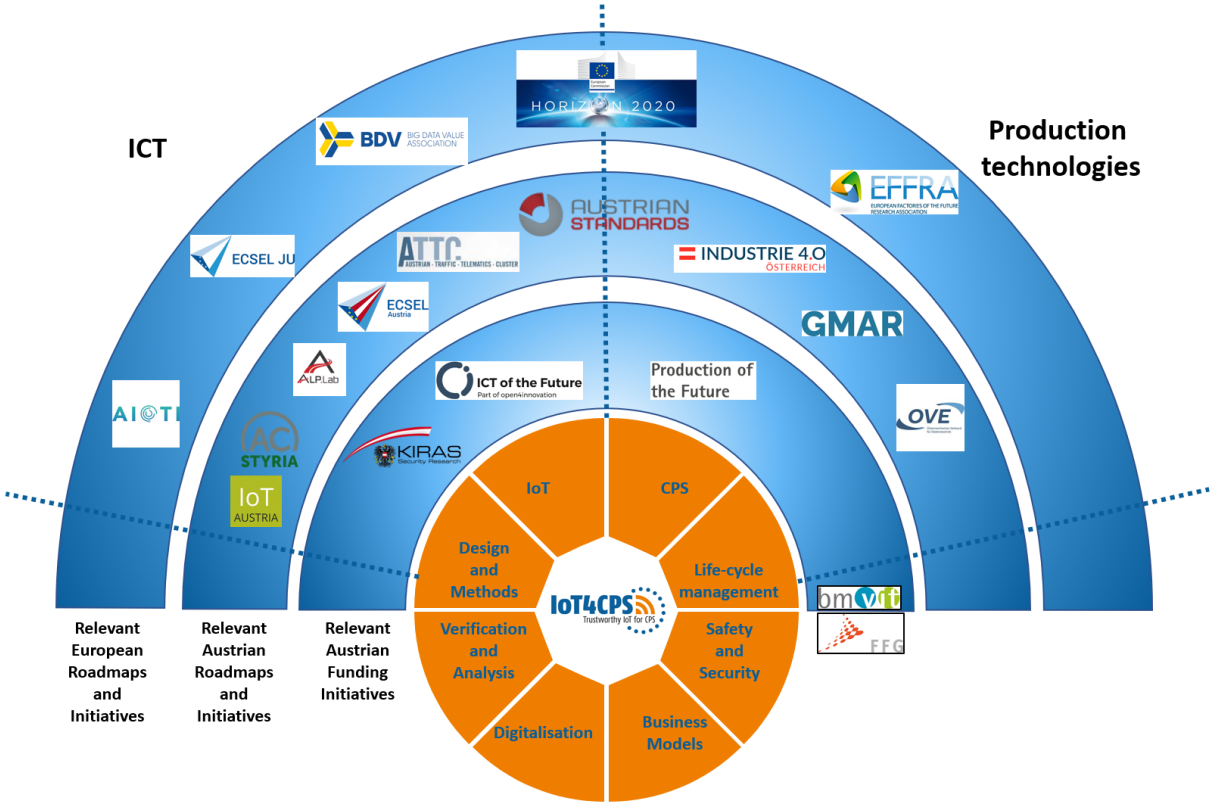

Figure 2. IoT4CPS within European and Austrian ecosystems

A crucial aspect of the impact creation are the dissemination activities, which are covered in project's WP9. It is implementation of the original communication strategy, as well as its adaptation throughout the project duration that is a major contributor to impact creation. As the communication strategy is also resulting from the stakeholder analysis, it helps identify the most appropriate methods for maximisation of usage and benefits, as well as for the consequent impact creation. It is the activities of WP9, such as organisation of publications, public engagement activities and social media interactions that help promote the assets and achievements of IoT4CPS, which in turn ease the meaningful penetration towards the full range of stakeholders. The measurable criteria of WP9 also helps gage some of the effects of the impact creation activities of IoT4CPS.

In summary, the most relevant direct measure resulting from the activities that are targeting increase of IoT4CPS' visibility is seen in effective stakeholder engagement. The above classified networking activities all boil down to a single crucial point and that is sustainability of project benefits through increased awareness of the project outcomes and improved usage. Hence through increased awareness of IoT4CPS and its assets, the consortium is already impacting the relevant ecosystem beyond the post-project phase.

5. Business updates

In terms of go-to market strategy, considerable updates are expected to emerge through increased usability of developed assets. Hence, specific business recommendations are expected to emerge thought the second half of the project. This section is hence presenting considerations at the intermediate stage of the project.

5.1 Marketability of technical developments

As the first half of the project is focusing onto development of elementary technology elements that are then to be integrated into complex systems during the second half of the project, there are limited updates in term of business development form individual partners. These are expected to emerge during integration stages of the project, when it is more likely to become evident if certain new business development opportunities arise as a result of either increased partner cooperation or due to the technical developments. Hence, there are currently no noteworthy updates performed on the business model canvas (proposal Figure 10).

5.2 Networking

In terms of industrial impact creation, the project partners are driving dissemination activities in industrial and scientific publications, despite initially heavy reliance on preliminary project results. The usage of social media (LinkedIn and Twitter) is aimed not only at maintaining the visibility of the project, but also to manage the business contacts and potential stakeholders.
The public kick-off and the active participation at the ICT 2018: Imagine Digital - Connect Europe have provided an opportunity to interact with other communities, such as “Data Markets Austria”. Similar effect was achieved at several smaller events, such as the Vienna Cyber Security Week and the at the Graz Security Days for Industry 2018. Future activities of a similar nature will include leading a Symposium Workshops at the 14th ARES & CD-MAKE Conference at the University of Kent, Canterbury from August 26-29, 2019.

5.3 Sustainability

The aforementioned networking activities are a significant contributing factor towards the project sustainability, which is also supported through education, by engaging with new interns and postgraduate students. The student engagement activities are also expanded through collaborative work between industrial and academic partners e.g. some recent teaching activities at TU Graz were result of a cooperation between AVL and ITI, or recent security training materials at NXP reaching approximately 800 participants annually.
In principle IoT4CPS is considering its sustainability in terms of:

- Business opportunities and growth through marketable assets in the later stages of the project and beyond the project closedown
- Societal participation and empowerment that is likely to result from the increased usage of IoT devices as a result of improvements of security solutions and lowering of the resistance towards the new technology and crucially through improved safety of AD
- Contributions to environmental sustainability that will be aided through improvements in transport solutions and introduction of new mobility services that rely on IoT and CPS developments.

5.4 Expected business updates

The current focus of the WP8 is based around activities that are contributing towards mid-term value proposition update and recommendations and the activities are on track with expectations. The main expected benefits will result from a review of technical WPs and the consolidated feedback to WP2 as a recommendation for the second half of the project. The real business impact is expected to occur in the remaining stage of the project and through extended life of the project benefits in the post-project phase. In order to maximise the business benefits for the project partners, WP8 is to be used to monitor and manage marketable opportunities that are resulting from IoT4CPS. The final outcomes will be presented in an updated business model canvas in deliverable 8.2 (Report on opportunities and recommendations for trusted IoT).

6. Recommendations

The following is a list of recommendations at the intermediate stage of the project as a result of activities within WP8 and in combination with the dissemination activities of WP9. The recommendations an organ of a living body of knowledge. Hence, they are not set in stone and are prone to continual updates till the project closedown.

No.	Recommendation
1	As the maturity of the currently developed solutions is increasing and the possibilities for their integration into existing projects are becoming more evident, it is recommended to analyse generated and expected benefits through a benefit realisation map. The map should be used as an overview and a plan for increased impact creation in the post-project phase. The map is a living document that is used as a guardrail for the project partners. Its final version will be publicly presented in the updated version of this deliverable (D8.2).
2	A tight collaboration should continue between WP8 (Impact Creation) and WP9 (Dissemination and Communication Measures) in order to promote the outcomes of the cooperation within the consortium partners. The partners are enticed to continue their cooperation and to prologue creating impact through dissemination activities on their own accord.
3	The cross-fertilisation between IoT4CPS and other projects and communities must be continued. It is recommended to deepen the 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 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. The partners are also encouraged to combine the diverse expertise for generation of training materials.
5	It is recommended to the industrial partners to actively seek the paths of provision of new unique value proposition, as a result of IoT4CPS developments.
6	Stakeholder engagement is a crucial factor of impact creation. As such, it is recommended to perform an update of stakeholder analysis and act accordingly.
7	The great diversity that is brought into IoT4CPS by the wide range of partners in terms of their core businesses, also represents an opportunity to seek domain cross-fertilisation and new customer segments for results of IoT4CPS. That is especially the case when considering implementation of elementary technology bricks into other use cases.
8	Where possible, it is recommended to attempt to implement verification techniques, which are generated within IoT4CPS into industrialised environment, so to guarantee product quality (e.g. Device.Connect) at the point of instrument exit from the manufacturing facilities.
9	As the IoT ecosystem is still in its pre-mature stages of development and technical standards are lagging the technical progress, it is advisable to continue exploiting project findings for generation of standardisation recommendations. The project findings may also be used for contribution to domains that have already established technology-independent standards.
10	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.