IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D9.4
Final Report on Published Work, Workshops and Non-Scientific Events

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: Initial Dissemination & Website
Type: Public
Editor(s): Mario Drobics (AIT), Andreas Martin (AIT)
E-mail: jpammer@sba-research.org
Author(s): Julia Pammer
Doc ID: D9.4

Amendment History

Version	Date	Author	Description/Comments
V 0.9	18.12.2020	J. Pammer	Initial Version
V 1.0	31.12.2020	J. Pammer	Updates, Final Version

Legal Notices

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.

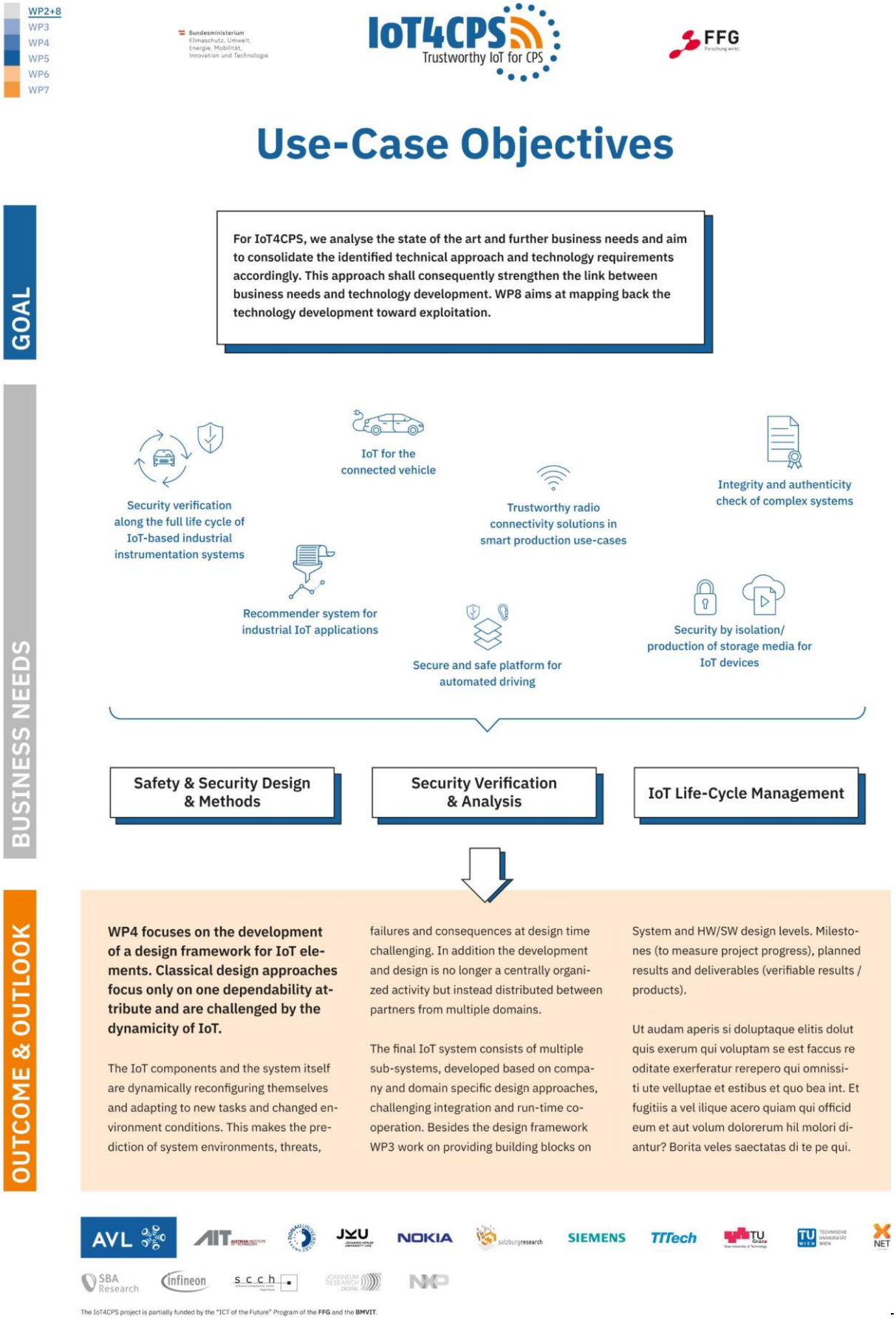
1. Inhaltsverzeichnis

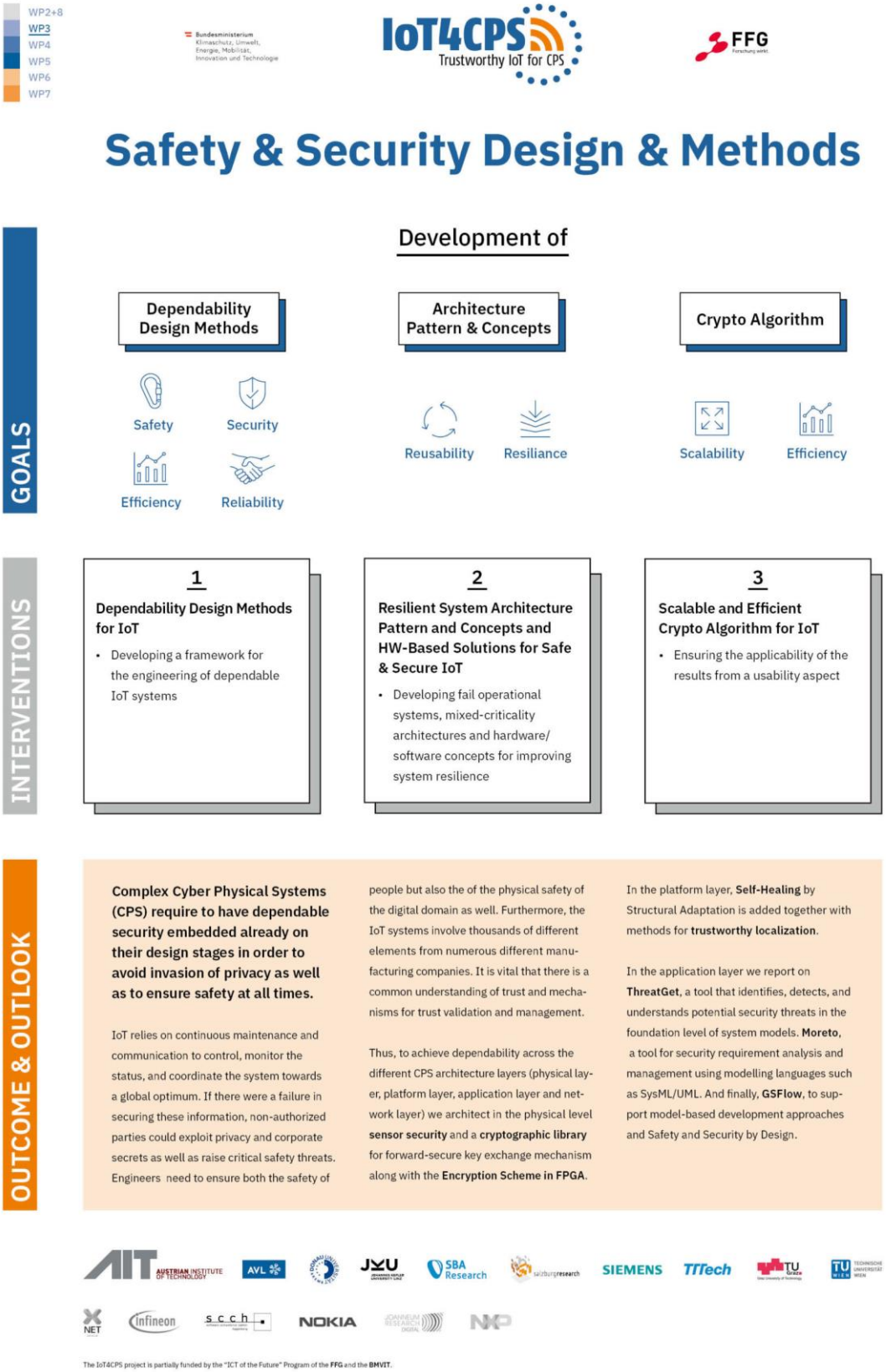
1. Published Work

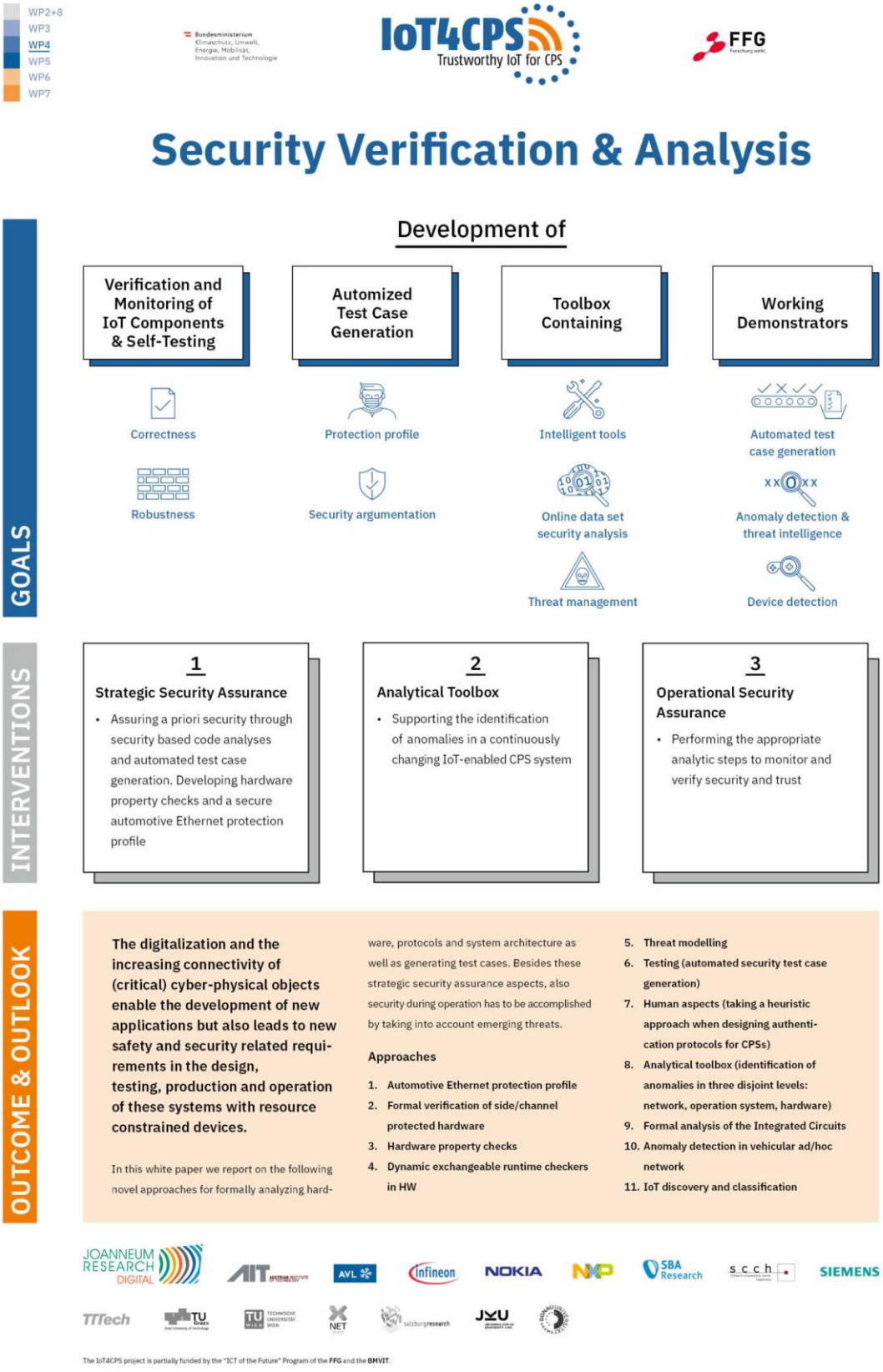
Over the last three years, the IoT4CPS project has addressed the challenges arising from the use of information and communication technologies (ICT) in real industrial environments. The extensive project results are now available to the Austrian economy for an accelerated time-to-market of real industry 4.0 applications as well as developments in the field of autonomous driving. The fruitful partnership between 16 consortium partners from industry and science should now clear the way for targeted follow-up projects. This way, theoretical knowledge gains in IoT Security will lead to concrete IoT implementations. A press release issued in December 2020 comprises achievements of the three year journey and emphasizes on their potential to establish a strong connectivity at a European level. Click here to read to full press release.

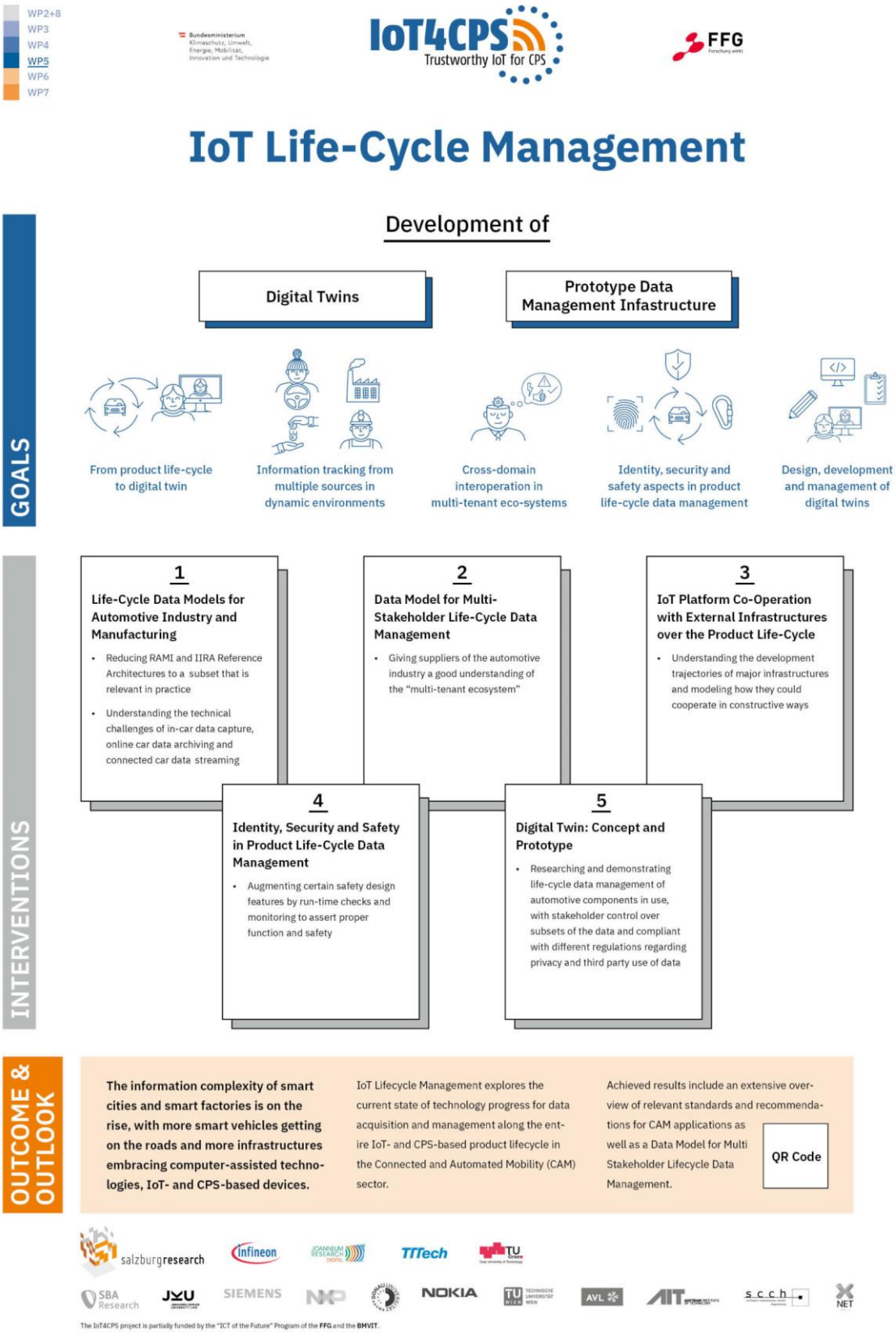
1.1 Posters

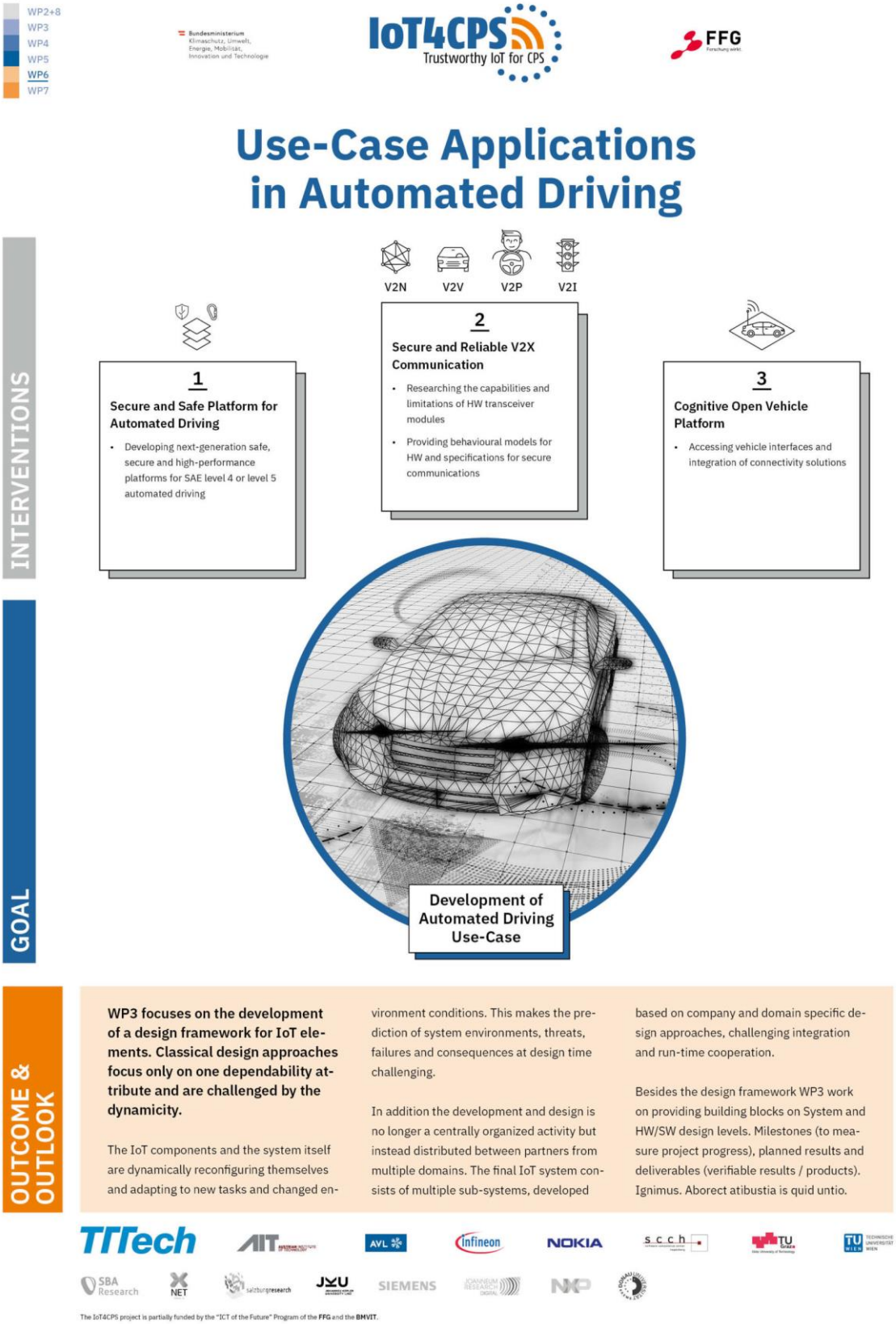
The intentions and processes of all work packages were illustrated in the form of posters. The overall aim of this rather simplified illustration is to present our results to the Austrian society in a comprehensible way. The posters provide a basis for the compact description of all contents summarized in the white papers. All posters can be viewed in detail in the upcoming section.


WP2+8
WP3
WP4
WP5
WP6
WP7
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
IoT4CPS Trustworthy IoT for CPS
FFG
Use-Case Objectives
GOAL
For IoT4CPS, we analyse the state of the art and further business needs and aim to consolidate the identified technical approach and technology requirements accordingly. This approach shall consequently strengthen the link between business needs and technology development. WP8 aims at mapping back the technology development toward exploitation.
BUSINESS NEEDS
Security verification along the full life cycle of IoT-based industrial instrumentation systems
IoT for the connected vehicle
Trustworthy radio connectivity solutions in smart production use-cases
Integrity and authenticity check of complex systems
Recommender system for industrial IoT applications
Secure and safe platform for automated driving
Security by isolation/ production of storage media for IoT devices
Safety & Security Design & Methods
Security Verification & Analysis
IoT Life-Cycle Management
OUTCOME & OUTLOOK
WP4 focuses on the development of a design framework for IoT elements. Classical design approaches focus only on one dependability attribute and are challenged by the dynamicity of IoT.
The IoT components and the system itself are dynamically reconfiguring themselves and adapting to new tasks and changed environment conditions. This makes the prediction of system environments, threats, failures and consequences at design time challenging. In addition the development and design is no longer a centrally organized activity but instead distributed between partners from multiple domains.
The final IoT system consists of multiple sub-systems, developed based on company and domain specific design approaches, challenging integration and run-time cooperation. Besides the design framework WP3 work on providing building blocks on System and HW/SW design levels. Milestones (to measure project progress), planned results and deliverables (verifiable results / products).
Ut audam aperis si doluptaque elitis dolut quis exerum qui voluptam se est faccus re oditate exerferatur rerepero qui omnissi-ti ute velluptae et estibus et quo bea int. Et fugitiis a vel ilique acero quiam qui officid eum et aut volum dolorerum hil molori di-antur? Borita veles saectatas di te pe qui.
AVL
AIT
JKU
NOKIA
salzburgresearch
SIEMENS
TTTech
TU Graz
TU Wien
SBA Research
Infineon
scch
NXP
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.


WP2+8
WP3
WP4
WP5
WP6
WP7
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
IoT4CPS Trustworthy IoT for CPS
FFG
Safety & Security Design & Methods
GOALS
Development of
Dependability Design Methods
Safety
Security
Efficiency
Reliability
Architecture Pattern & Concepts
Reusability
Resiliance
Crypto Algorithm
Scalability
Efficiency
INTERVENTIONS
1
Dependability Design Methods for IoT
• Developing a framework for the engineering of dependable IoT systems
2
Resilient System Architecture Pattern and Concepts and HW-Based Solutions for Safe & Secure IoT
• Developing fail operational systems, mixed-criticality architectures and hardware/ software concepts for improving system resilience
3
Scalable and Efficient Crypto Algorithm for IoT
• Ensuring the applicability of the results from a usability aspect
OUTCOME & OUTLOOK
Complex Cyber Physical Systems (CPS) require to have dependable security embedded already on their design stages in order to avoid invasion of privacy as well as to ensure safety at all times.
IoT relies on continuous maintenance and communication to control, monitor the status, and coordinate the system towards a global optimum. If there were a failure in securing these information, non-authorized parties could exploit privacy and corporate secrets as well as raise critical safety threats. Engineers need to ensure both the safety of people but also the of the physical safety of the digital domain as well. Furthermore, the IoT systems involve thousands of different elements from numerous different manufacturing companies. It is vital that there is a common understanding of trust and mechanisms for trust validation and management.
Thus, to achieve dependability across the different CPS architecture layers (physical layer, platform layer, application layer and network layer) we architect in the physical level sensor security and a cryptographic library for forward-secure key exchange mechanism along with the Encryption Scheme in FPGA.
In the platform layer, Self-Healing by Structural Adaptation is added together with methods for trustworthy localization.
In the application layer we report on ThreatGet, a tool that identifies, detects, and understands potential security threats in the foundation level of system models. Moreto, a tool for security requirement analysis and management using modelling languages such as SysML/UML. And finally, GSFlow, to support model-based development approaches and Safety and Security by Design.
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
AVL
JKU
SBA Research
salzburgresearch
SIEMENS
TTTech
TU Graz
TU WIEN
NET
Infineon
scch
NOKIA
NXP
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.


WP2+8
WP3
WP4
WP5
WP6
WP7
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
IoT4CPS Trustworthy IoT for CPS
FFG
Security Verification & Analysis
GOALS
Development of
Verification and Monitoring of IoT Components & Self-Testing
Automized Test Case Generation
Toolbox Containing
Working Demonstrators
Correctness
Protection profile
Intelligent tools
Automated test case generation
Robustness
Security argumentation
Online data set security analysis
Anomaly detection & threat intelligence
Threat management
Device detection
INTERVENTIONS
1
Strategic Security Assurance
• Assuring a priori security through security based code analyses and automated test case generation. Developing hardware property checks and a secure automotive Ethernet protection profile
2
Analytical Toolbox
• Supporting the identification of anomalies in a continuously changing IoT-enabled CPS system
3
Operational Security Assurance
• Performing the appropriate analytic steps to monitor and verify security and trust
OUTCOME & OUTLOOK
The digitalization and the increasing connectivity of (critical) cyber-physical objects enable the development of new applications but also leads to new safety and security related requirements in the design, testing, production and operation of these systems with resource constrained devices.
In this white paper we report on the following novel approaches for formally analyzing hardware, protocols and system architecture as well as generating test cases. Besides these strategic security assurance aspects, also security during operation has to be accomplished by taking into account emerging threats.
Approaches
1. Automotive Ethernet protection profile
2. Formal verification of side/channel protected hardware
3. Hardware property checks
4. Dynamic exchangeable runtime checkers in HW
5. Threat modelling
6. Testing (automated security test case generation)
7. Human aspects (taking a heuristic approach when designing authentication protocols for CPSs)
8. Analytical toolbox (identification of anomalies in three disjoint levels: network, operation system, hardware)
9. Formal analysis of the Integrated Circuits
10. Anomaly detection in vehicular ad/hoc network
11. IoT discovery and classification
JOANNEUM RESEARCH DIGITAL
AIT
AVL
Infineon
NOKIA
NXP
SBA Research
scch
SIEMENS
TTTech
TU Graz
TU Wien
NET
salzburgresearch
JKU
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.


WP2+8
WP3
WP4
WP5
WP6
WP7
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
IoT4CPS Trustworthy IoT for CPS
FFG
IoT Life-Cycle Management
GOALS
Development of
Digital Twins
Prototype Data Management Infastructure
From product life-cycle to digital twin
Information tracking from multiple sources in dynamic environments
Cross-domain interoperation in multi-tenant eco-systems
Identity, security and safety aspects in product life-cycle data management
Design, development and management of digital twins
INTERVENTIONS
1
Life-Cycle Data Models for Automotive Industry and Manufacturing
Reducing RAMI and IIRA Reference Architectures to a subset that is relevant in practice
Understanding the technical challenges of in-car data capture, online car data archiving and connected car data streaming
2
Data Model for Multi-Stakeholder Life-Cycle Data Management
Giving suppliers of the automotive industry a good understanding of the "multi-tenant ecosystem"
3
IoT Platform Co-Operation with External Infrastructures over the Product Life-Cycle
Understanding the development trajectories of major infrastructures and modeling how they could cooperate in constructive ways
4
Identity, Security and Safety in Product Life-Cycle Data Management
Augmenting certain safety design features by run-time checks and monitoring to assert proper function and safety
5
Digital Twin: Concept and Prototype
Researching and demonstrating life-cycle data management of automotive components in use, with stakeholder control over subsets of the data and compliant with different regulations regarding privacy and third party use of data
OUTCOME & OUTLOOK
The information complexity of smart cities and smart factories is on the rise, with more smart vehicles getting on the roads and more infrastructures embracing computer-assisted technologies, IoT- and CPS-based devices.
IoT Lifecycle Management explores the current state of technology progress for data acquisition and management along the entire IoT- and CPS-based product lifecycle in the Connected and Automated Mobility (CAM) sector.
Achieved results include an extensive overview of relevant standards and recommendations for CAM applications as well as a Data Model for Multi Stakeholder Lifecycle Data Management.
QR Code
salzburgresearch
Infineon
TTTech
SBA Research
JKU
SIEMENS
NXP
NOKIA
AVL
AIT
s c c h
NET
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.


WP2+8
WP3
WP4
WP5
WP6
WP7
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
IoT4CPS Trustworthy IoT for CPS
FFG
Use-Case Applications in Automated Driving
INTERVENTIONS
V2N
V2V
V2P
V2I
1
Secure and Safe Platform for Automated Driving
Developing next-generation safe, secure and high-performance platforms for SAE level 4 or level 5 automated driving
2
Secure and Reliable V2X Communication
Researching the capabilities and limitations of HW transceiver modules
Providing behavioural models for HW and specifications for secure communications
3
Cognitive Open Vehicle Platform
Accessing vehicle interfaces and integration of connectivity solutions
GOAL
Development of Automated Driving Use-Case
OUTCOME & OUTLOOK
WP3 focuses on the development of a design framework for IoT elements. Classical design approaches focus only on one dependability attribute and are challenged by the dynamicity.
The IoT components and the system itself are dynamically reconfiguring themselves and adapting to new tasks and changed environment conditions. This makes the prediction of system environments, threats, failures and consequences at design time challenging.
In addition the development and design is no longer a centrally organized activity but instead distributed between partners from multiple domains. The final IoT system consists of multiple sub-systems, developed based on company and domain specific design approaches, challenging integration and run-time cooperation.
Besides the design framework WP3 work on providing building blocks on System and HW/SW design levels. Milestones (to measure project progress), planned results and deliverables (verifiable results / products). Ignimus. Aborect atibustia is quid untio.
TTTech
AIT
AVL
Infineon
NOKIA
scch
TU Graz
TU Wien
SBA Research
NET
salzburgresearch
JKU
SIEMENS
NXP
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

WP2+8
WP3
WP4
WP5
WP6
WP7

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

IoT4CPS Trustworthy IoT for CPS

FFG Forschung wirkt.

Use-Case Applications in Industry 4.0

INTERVENTIONS

1

Trustworthy Radio Connectivity Solutions for I4.0 Environments

- Examining the application of holistic secure connectivity concepts
- Evaluating novel technologies that address unanswered connectivity requirements

2

Traceability of Components and Systems throughout Life-Cycle

- Examining the application of holistic secure traceability concepts
- Evaluating the required set of wireless technologies
- Investigating the aspects of authenticity, potentially privacy and secure cryptography implementation and verification concepts

3

Security by Isolation

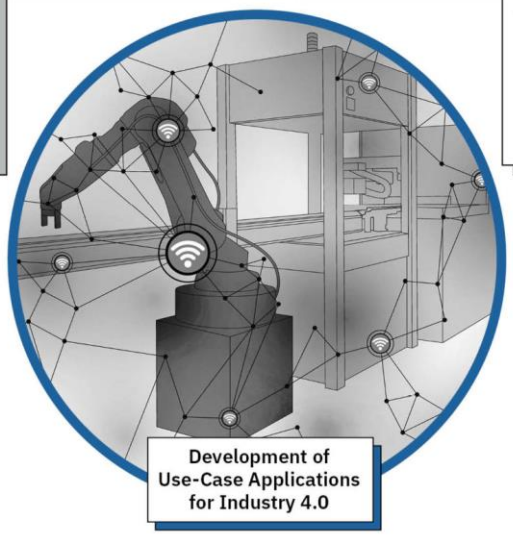
- Implementing test beds and developing guidelines for securing IoT products and for secure set-up of production environments

4

Cognitive Open Vehicle Platform

- Accessing vehicle interfaces and integration of connectivity solutions

GOAL



Development of Use-Case Applications for Industry 4.0

OUTCOME & OUTLOOK

Smart production is characterized by increased dynamicity in configuration, system context, system environments and even tasks.

For that reason, potential risks should be considered and analyzed not only during the design time but also during the complete system lifecycle. To provide solutions for the main demand drivers and support the digitalization over the entire lifecycle of complex industrial products, IoT4CPS has developed an extensive design framework for highly dependable Industrial IoT elements towards the vision of safe and secure Industry 4.0.

The outcomes of this project address the aspects security, safety, reliability and resilience of IoT-based CPS systems for largely heterogeneous, distributed and dynamic environments holistically through a high degree of integration along the value chain and product lifecycle, leading to a significant time-to-market acceleration for complex products.

A relevant set of the developed technologies and components are integrated into demonstrators encompassing aspects of real industrial settings for smart production use-cases. These are being set up in a way that considers the heterogeneity of the industrial IoT environment and at the same time focuses on a high degree of reusability.

Infineon AIT AVL NXP s c c h SIEMENS TTTech TU Graz NET SBA Research salzburgresearch NOKIA JKU TU Wien

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

1.2 White Papers

While the technical deliverables provide in depth insights for those familiar with the covered subject, the white papers will make the project´s content accessible to potentially interested individuals on a large scale.

White Paper Work Package 3: Safety & Security Design & Methods

Complex Cyber Physical Systems (CPS) require to have dependable security embedded already at their design stages in order to avoid invasion of privacy as well as to ensure safety at all times.

View here

White Paper Work Package 4: Security Verification & Analysis

The digitalization and the increasing connectivity of (critical) cyber-physical objects enable the development of new applications but also lead to new safety and security related requirements in the design, testing, production and operation of these systems with resource constrained devices.

View here

White Paper Work Package 5: IoT Life-Cycle Management

The information complexity of smart cities and smart factories is on the rise, with more smart vehicles getting on the roads and more infrastructures embracing computer-assisted technologies, IoT- and CPS-based devices.

View here

White Paper Work Package 6: Use-Case Applications in Automated Driving

The present automotive megatrend of driving automation [Schramm, 2013] is a substantial contributor to the Grand Societal Challenges.

View here

White Paper Work Package 7: Use-Case Applications in Industry 4.0

Smart production is characterized by increased dynamicity in configuration, system context, system environments and even tasks.

View here

White Paper Work Packages 2 & 8: Use-Case Objectives

Analyzation of the state of the art business needs as well as consolidation of respective technology needs will consequently improve the applicability and benefits of technological

developments
View here

1.3 Public Deliverables

Over the duration of the project, more than 40 deliverables were created. 34 of them have been made available to the public on the project website. The detailed reports, most of which are technical, are intended to form the basis for clarifying specific questions and for possible further research.

View all public documents here

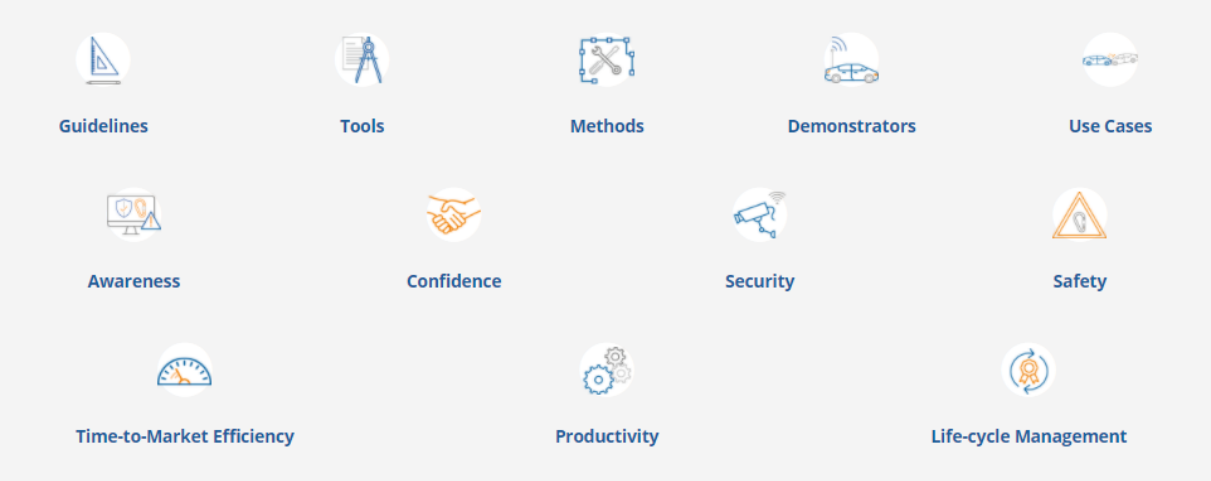
1.4 Publications

Over the course of the past three years, the IoT4CPS consortium has achieved numerous accepted papers at well-known and high-ranked scientific conferences. Dissemination of project findings took place at venues in Europe, the US and Asia. A complete list of all publications can be found on the projcet website.

View all publications here

1.5 Technical Results – Repository

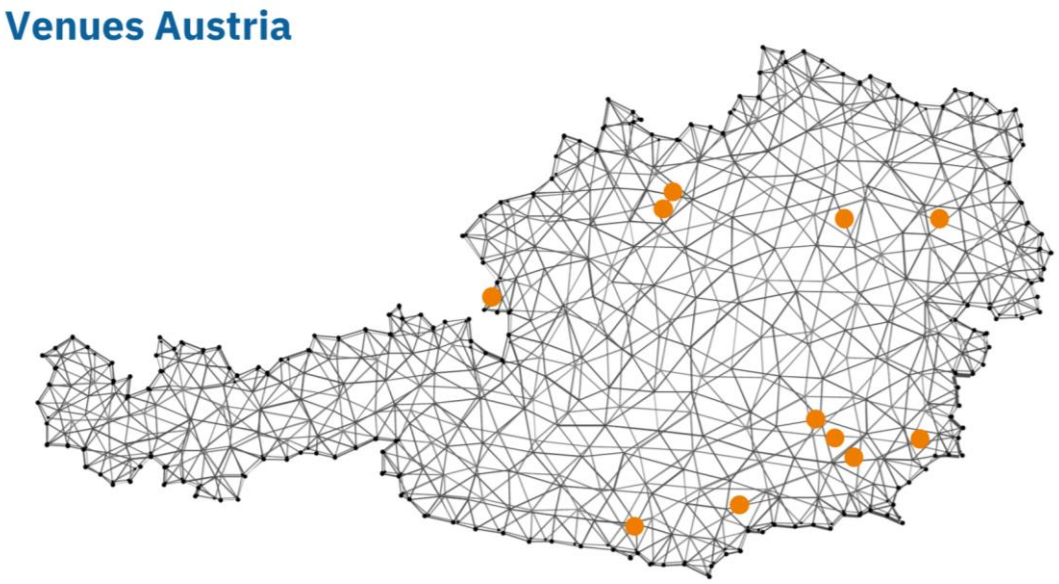
The IoT4CPS project has created a framework consisting of guidelines, tools & methods and demonstrators for coping with the cyber-security challenges in autonomous vehicles and smart production. The IoT4CPS repository lists all relevant sources of documents consolidated in one database. These documents intend to support digitalization along the entire product lifecycle and accelerating the time-to-market in the development of connected and autonomous vehicles. The achievement compiled in the repository comprise the following items.



Click here to download the full repository.

2. Workshop Organisation & Non Scientific Dissemination

The IoT4CPS consortium executed numerous community outreach activities over the past year. Various approaches (e.g., lightning talks, networking sessions, panel discussions) enabled us to target most diverse peers. Over the past three years, the IoT4CPS project was introduced at numerous national and international venues. National plaforms were particularily used for community outreach and networking activities. International venues helped distribute scientific findings and establish contacts in the international scientific field. The overall number of appearances at non scientific events can be quantified with almost 100.


Venues Austria


Venues International

2.1 Workshop Organisation and Non-Scientific Dissemination

The following section shall provide insights into workshops and events with the highest reach and impact creation in the second half of the project. On the European level the lighthouse character of the project was reflected by the representation of AIT at the second stakeholder workshop on industrial IoT (16.05.2019, Brussels). Another example where stakeholders were brought together is the digitization workshop where results from IoT4CPS among others were discussed with a special focus on the topic trust (19.08.2019, Vienna). An important milestone to the project´s sustainability concept was the execution of the second edition of the WISI workshop (Workshop on Industrial Security and IoT) at the virtual ARES & CD-MAKE 2020 (25.-28.08.2020, originally planned at UCD Dublin). The objective of the workshop was to support knowledge exchange and networking between researchers in the field of Industrial IoT Security, with the specific focus on the flagship project IoT4CPS. The participants in the workshop included the authors of the accepted papers which are coming from Austrian research institutions and industrial partners, as well as the general ARES audience which joined the workshop. Another successful break out session on "Trust in complex cyber-physical environments" was conducted at IDSF 2020 (03.12.2020).
The project partners from IoT4CPS agree that a holistically considered IoT security in cyber-physical systems will be a "living" scientific-industrial focus topic also in the following years. The extensive project results are now available to the Austrian economy for an accelerated time-to-market of real Industry 4.0- applications, developments in the field of "autonomous driving" and for many other scenarios, in order to strengthen Austria's position as a technology location in the long term. In order to create the highest possible impact on a national level, the official project closing was thus conducted as a break out session at the 2020 Summit Industrie 4.0 (10.12.2020). This enabled the consortium to make results and achievements as well as potential future challenges visible to almost 100 participants from industry and research.

2.1.1 Second WISI Workshop at ARES & CD-MAKE Conference 2020

The 2020 edition of the ARES & CD-MAKE conference was conducted as a remote event with over 300 participants from 43 nations. The event focuses on bringing together researchers in order to exchange ideas and present their current work. Unfortunately, due to well-known situation with the coronavirus, the event was held online. Similar to the 2019 edition, the Program Committee was strongly supported by the IoT4CPS scientific and industrial community. The 2020 WISI workshop accepted 5 submissions, with a focus on cybersecurity for IoT, mobile devices and industrial devices, as well as network intrusion detection and testing for security. Apart from that the workshop helped further deepen the collaboration between IoT4CPS consortium partners.

2.1.2 Trust in Complex Cyber-Physical Environments – IoT4CPS @ IDSF 2020

Under the motto "Security in times of pandemics and major global events", the IDSF 2020 was organized as a virtual conference from 02.12.-03.12.2020 by the AIT Austrian Institute for Technology and the Austrian Chamber of Commerce (Wirtschaftskammer Österreich – WKO). The IoT4CPS consortium hosted a break out session on "Trust in Complex Cyber-Physical Environments" on December 03.The session was joined by more than 30 participants from research and industry. A wide field of professional backgrounds provided a fruitful baseline for in-depht discussion on future challenges and legal aspects in the fields of autonomous vehicles and industry 4.0.

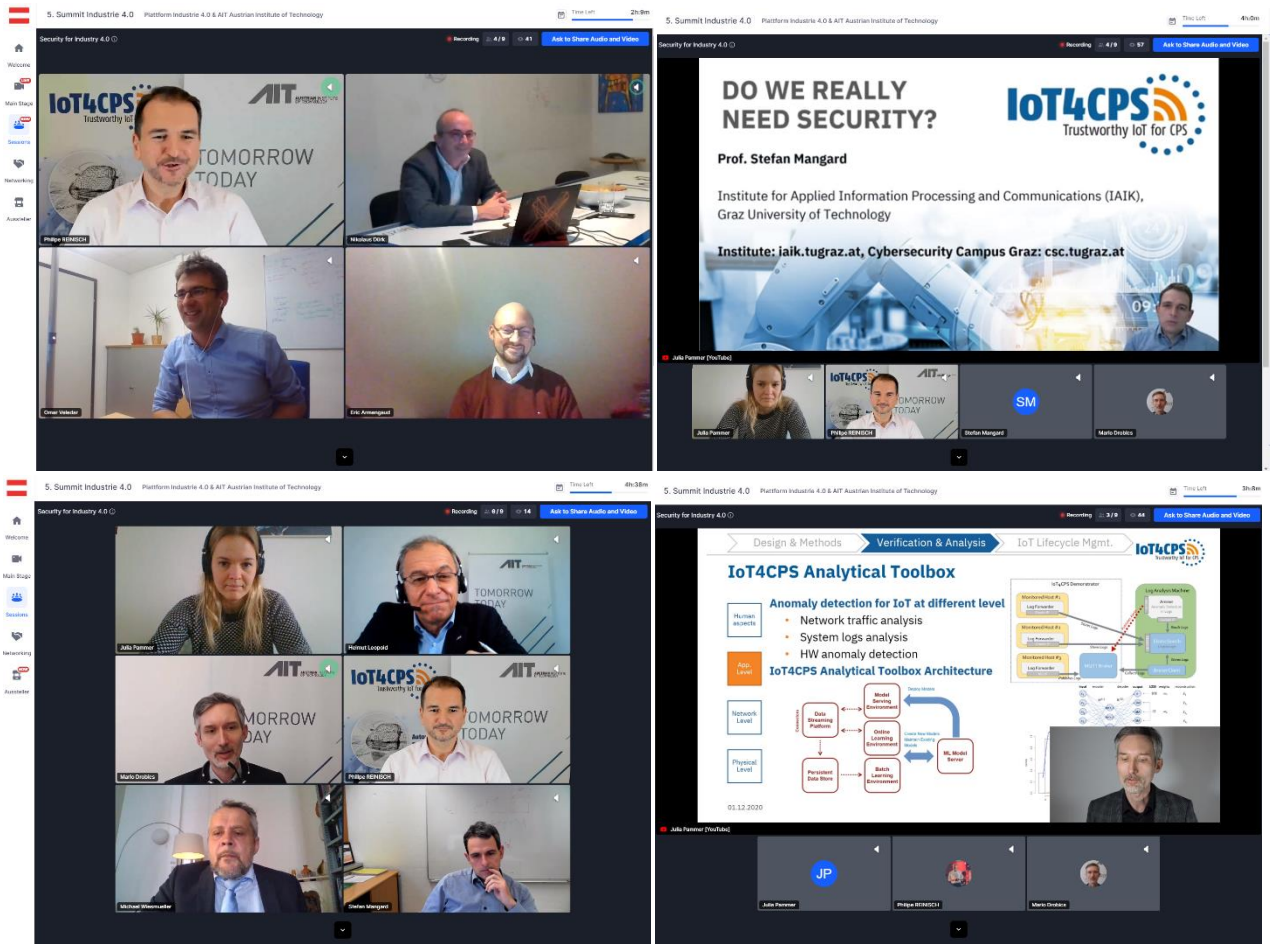
Rewatch the full session "Trust in Complex Cyber-Physical Enviroments" here. View all details about IDSF 2020 here.

2.1.3 Security in Industry 4.0 – IoT4CPS Project Closing @ Summit Industrie 4.0

The IoT4CPS consortium hosted a keynote session and parallel session in the course of this year´s virtual Summit Industrie 4.0 organized by Plattform Industrie 4.0. The session was kicked off with welcome notes from Michael Wiesmüller (Ministry for Climate Action,

Environment, Energy, Mobility, Innovation and Technology) and Helmut Leopld, AIT Austrian Institute of Technology GmbH. After a talk from Stefan Mangard, TU Graz, on "Why is more security research necessary?", IoT4CPS project leader Mario Drobics, AIT Austrian Insitute of Technology GmbH, introduced findings and achivements of the project and explained "How to establish trust in complex cyber-physical environments like autonomous vehicles and connected factories". In the consequent session "From research to application: How companies are using IoT4CPS" Nikolaus Dürk (X-Net Services GmbH) and Eric Armengaud (AVL List GmbH) provided insights into the application of project findings. The session concluded with future prospects. Peter Kerschl (FFG), Violeta Damjanovic-Behrendt (Salzburg Research), Konstantinos Georgoulias (EIT Manufacturing East) and Günther Goach (President Carinithian Chamber of Labor) discussed future projects and potential collaborations.

2.1.4 Impressions



3. Results & Outlook

The IoT4CPS project has provided all involved partners with extensive scientific groundwork with a high degree of practical relevance. The goal is to bring the topic of security in the context of IIOT to a wider European research audience as part of the new European research program "Horizon Europe". The project results very clearly reflect the combined technological competence of Austria´s leading industrial companies and research partners.