IoT4CPS
Trustworthy IoT for CPS

Trustworthy IoT Lifecycle Data Management for the Automotive Industry and Manufacturing

Date: September 2020
Editor: Violeta Damjanovic-Behrendt
Authors: WP5 team

Contents

1. SUMMARY

IoT Lifecycle Management is a part of the Trustworthy IoT for CPS (IoT4CPS) project and 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.

We report on the definition of extended data models and data analysis methods and the design of tools that follow recent initiatives, standards and recommendations in this sector. The work also provides the implementation of a Digital Twin prototype that is designed to identify security and safety measures of CAM applications and correlate these measures with multi-tenancy features of smart vehicles along the product lifecycle. Apart from the security and safety features, the report explores privacy, trust and ethics of CAM applications, within complex environments of smart cities and smart factories *(Figure 1)*.

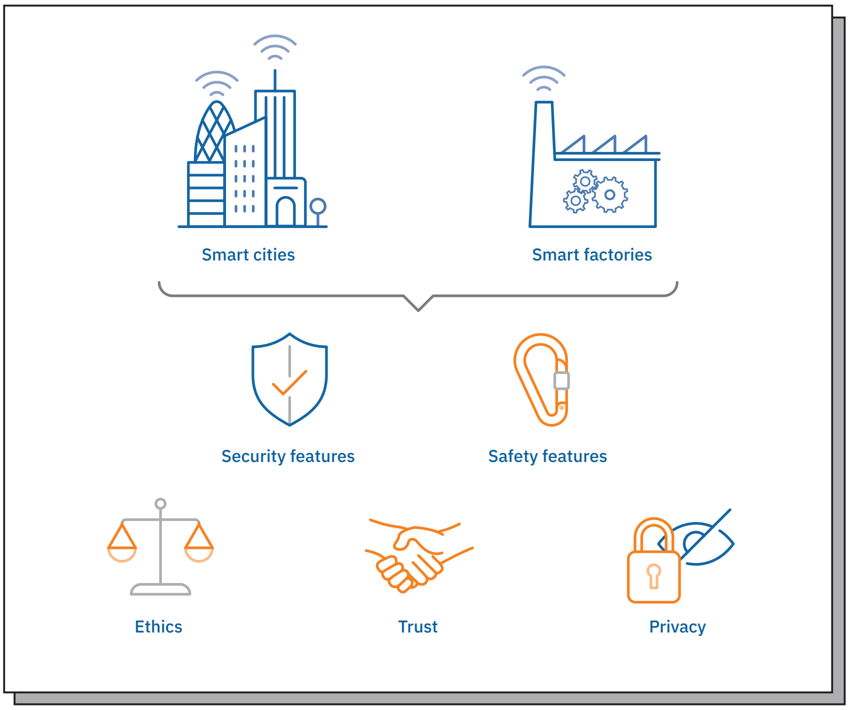

Figure 1: Areas of exploration of CAM applications within complex environments of smart cities and smart factories

2. CHALLENGE

The major challenge of IoT Lifecycle Management from the perspective of IoT4CPS is about synchronization, analysis and management of CAM services among multiple stakeholders in complex environments, such as smart cities and smart factories, designed to avoid harmful and fatal situations and to ensure secure and safe conditions, privacy controls and growth of trust as a key to the further adoption of mobility applications in Austria *(Figure 2)*.

New CAM technologies offer improved road safety, reduced congestion and CO2 emissions, increased accessibility to personal mobility, and more. To become commercially viable, CAM technologies need to open the door for new experiences, still solving challenges at various levels, e.g. technology and infrastructure development, businesses and governments, harmonization of communication standards for vehicle connectivity (e.g. 5G), faster and wider network connectivity, improved data sharing and data transparency, and ensuring continuous cybersecurity and safety conditions. The latter two challenges are at the core of several reports in WP5:
"Identity, Security and Safety in Product Lifecycle Data Management" (D5.4.1 and D5.4.2) and "Lifecycle Data Management Prototype" (D5.5.1, D5.5.2, and D5.5.3) explore the continuum of cybersecurity and safety procedures and conditions for CAM applications. The reports "Product Lifecycle Data Management (PLCDM) Stakeholder Perspectives" (D5.2) and "Cross-Platform Interoperation Model" (D5.3) are focused on data acquisition, data sharing and transparency with respect to various stakeholders and diversity of their roles in the CAM applications.

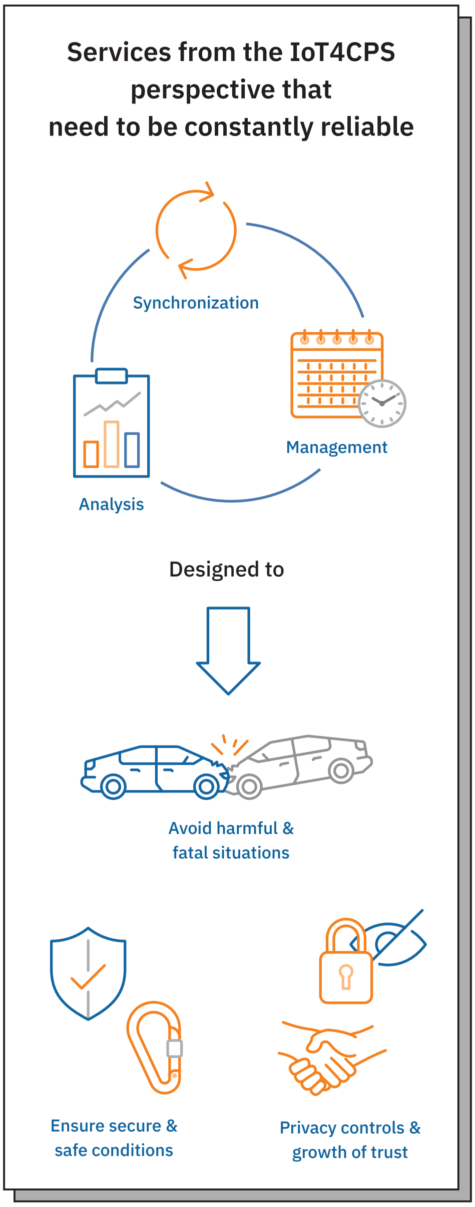
Services from the IoT4CPS perspective that need to be constantly reliable
Synchronization
Management
Analysis
Designed to
Avoid harmful & fatal situations
Ensure secure & safe conditions
Privacy controls & growth of trust

Figure 2: The major challenge of IoT Lifecycle Managment from the perspective of IoT4CPS

Apart from the technological growth, the CAM sector faces an additional set of challenges triggered by evolving regulations, recent initiatives, standards and frameworks in the sector, both at the national and international level. Starting from a set of measures to support the digitization of industry across multiple domains, as defined in the Digitising European Industry (DEI) programme created by the European Commission in 2016, the need for future digital platform infrastructures to interact with each other and be trustworthy is recognized as key, for attaining long term industrial development in Europe.

Additional international government bodies, regulations and initiatives that strongly influence the CAM sector are:

- The latest WP.29 UN cybersecurity regulation[1] from June 2020, which is the first international regulation that mandates cybersecurity in smart vehicles. This regulation outlines new processes and technology that manufacturers must adopt to achieve vehicle type approval with regards to cyber-security, safety, and environmental protection;
- The Directive on Security of Network and Information Systems (NIS)[2] sets cybersecurity regulations, incident response procedures, etc. affecting search engines, cloud providers and online marketplaces;
- The General Data Protection Regulation (GDPR)[3] sets requirements related to data protection in Europe;
- The European Telecommunications Standards Institute (ETSI) sets technical specifications, ETSI TS 102 940 to ETSI TS 102 943 Intelligent Transport System (ITS) security architecture[4] along with services specification to prevent unauthorized access to ITS services;
- IEEE 802.11p, is an International Standard for Wireless Access in Vehicular Environments [1].

In Austria, the latest roadmap "Austrian Action Programme on Automated Mobility", was issued by the Austrian Federal Ministry of Transport, Innovation and Technology (BMK[5]), outlines guiding principles for Automated Mobility, for the period 2019–2022. These principles include safety, technological bases and infrastructure to support future mobility, building trust throughout the entire product lifecycle, and impact assessment and access to data. With regard to BMK's principles, Lifecycle Data Management in IoT4CPS designs decision-making concepts and implements a Digital Twin-based prototype for security and safety validations for the CAM industry focused solutions.

The convolution of advanced technologies of smart vehicles and complex regulatory frameworks opened the scene for Digital Twins that can track products, merge, analyse and optimize the acquired data and ensure information exchange along PLCDM, virtualize manufacturing processes and provide advanced decision support. The CAM applications are designed to assist the owners of vehicles in a variety of ways and are beneficial to both the owners of smart vehicles and other stakeholders from the vehicle‘s ecosystem, e.g. passengers sharing the car, smart cities, smart roads infrastructure providers, car sharing dealers, etc. However, as CAM applications are based on cloud technologies, they are exposed to a vast attack surface in which every asset is a potential target that can compromise drivers', passengers' and by-standers' security, safety and privacy.

[1] UNECE WP.29 cybersecurity regulation: https://argus-sec.com/unece-wp29-approved/
[2] NIS Directive: https://www.enisa.europa.eu/topics/nis-directive
[3] GDPR: https://gdpr-info.eu/
[4] ETSI ITS; security standards series: https://argus-sec.com/etsi-intelligent-transport/
[5] BMK (Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie)

3. CURRENT STATUS

3.1 Digital Twins in the CAM Industry

The technology evolution shifted the concept of „twins“ from the aerospace industry to Industry 4.0. From 2011 onwards, the term Digital Twin has been used to represent “a set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level“ [2][3] (Figure 3). The literature review on the definitions and major capabilities of Digital Twins is quite broad, introducing Digital Twins as digital counterparts of physical products used to simulate these products in a virtual world in order to predict their future states or behaviour of a system [4] [5] [6]. A study defines the Digital Twin as a comprehensive digital representation of an individual product, its properties, condition and behaviour [7]. Its key functionalities include support for the design tasks, operational processes and validations of system properties through multi-domain and multi-level simulations along lifecycle phases [8].

Digital Twins are also built to increase the manufacturing flexibility and competitiveness, improve the product design performance through behaviour forecasting over the lifetime (e.g. Predix[6] by GE), improve efficiency and quality in manufacturing (i.e. Simcenter 3D[7] by Siemens) or enable synchronous data transmission between the product and the factory (e.g. Tesla [9]). In the CAM industry, the Digital Twin is seen as lifecycle management and certification paradigm that incorporates models and simulations consisting of vehicle states and historical data [10]. Some automotive studies refer to the Digital Twin as a simulation that integrates an on-board health management system, maintenance history, and recorded vehicle and fleet data [11].

In WP5 of IoT4CPS, the process of simulating and measuring of the relevant design and engineering parameters, operational behaviour and performances of smart vehicles, and their disposal and environmental impacts, is enabled using the concept of Digital Twins. This covers the modelling of major automotive components, such as the vehicle’s assets, stakeholders, security and safety metrics, and the definition of data analytics and decision support methods such as predictive modelling, pattern detection, correlations of dynamic sensor data to Key Performance Indicators (KPIs) and historical data in order to improve procedures that affect the user’s driving experience, security and safety.

[6] PREDIX: https://www.predix-ui.com/#/home
[7] Simcenter 3D: https://blogs.sw.siemens.com/simcenter/simcenter-3d-2020-1-whats-new/

3.2 Digital Twins in the Security Industry

Smart vehicles and their sub-systems such as infotainments (navigation, cameras, entertainment services), body controls (seat belts, seat heating), chassis and power train controls (speed control), communication controls, etc. are designed to augment user experience through information exchange amongst various stakeholders. This can open many privacy, security and safety issues leading to reputational damage for the users, car manufacturers, suppliers, network service providers, software and application providers, garages, and other stakeholders. The data collected by smart vehicles can contain privacy data and when processed by advanced cloud services that intelligently combine, correlate and link privacy data, the privacy of stakeholders can also be affected in unintended ways *(Figure 3)*.

The advanced data-centric methods of Digital Twins can be designed to monitor and mirror the entire product lifecycle with the aim of providing significant gains in security, safety, privacy and reliability of smart vehicles. The services of Digital Twins can be designed to support GDPR policies, enable privacy anomalies detection, security and safety issue detection, incidence response and mitigation mechanisms. The literature review on Digital Twins for Information Security applications refers to several current approaches, e.g. a method based on the comparison of configuration data of physical devices to their virtual replicas, in order to detect deviations that may refer to compromised CPSs [12], or a method for virtual penetration testing of a system in order to capture and fix vulnerabilities early, instead of relying on real system parameters [13] [14]. The concept of designing Digital Twins for privacy assessments and protection for CAM applications is presented in [15]. An overview of current open source Digital Twins implementing security paradigms yields the following:

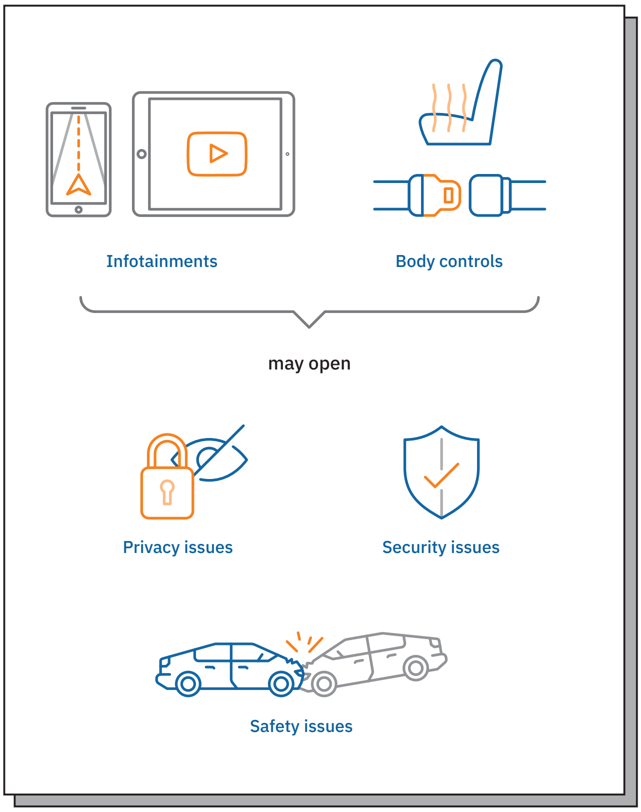

Figure 3: Smart vehicles & their sub-systems

- MiniCPS is a toolkit for security research on CPS networks that explores different attack scenarios and evaluate countermeasures [16], and
- CPS Twinning is a prototype [12] that contains security modules for network analysis and can be used to check certain security and safety rules in a simulation model.

3.3 Shifting Security and Privacy to IoT Lifecycle Management

User and device identity management is an integral part of IoT-based product lifecycle data management that provides a source of trust for cloud-based services that require authentication and authorization procedures. For example, the device identity managers use specific authentication mechanisms to identify the user who is linked to the specific device via the device manager.

Smart vehicles and their CAM applications consist of numerous IoT-, CPS- and cloud-based assets (sensors, devices, things) which are characterized by their increased connectivity and number of interfaces. While on the one hand, smart vehicles and their applications are designed to improve information sharing amongst stakeholders, on the other hand, they can enable implicit sharing of privacy data (e.g. personal data, personal information, Personally Identifiable Information (PII), or Sensitive Personal Information (SPI)) enabling massive surveillance and exposing users to a vast attack surface. Security, safety and privacy features of smart vehicles can also be overridden by hackers exploiting vulnerable security flows, algorithms and relevant technologies designed to improve safety for e.g. collision prevention and mitigation (pedestrian detection, Anti-lock Braking System (ABS), obstacle detection, etc.), braking, hill drive assistance, terrain and wheel information sensors (temperature warning, tire pressure monitoring system, etc.), and more. Hence, user and device identity management, access controls and data governance mechanisms need to be designed to mutually control information sharing and need to be defined at an early stage. The user identity and privacy settings are continually transmitted through the entire product lifecycle, every time the user information is exposed through diverse business and identity access systems. Finally, the user identities of terminated accounts related to the end-of-life phase of the smart vehicle, need to be removed from the vehicle and the cloud data centres, or anonymized and protected to prevent possible data manipulations in the future.

In certain situations, the identity of users and devices could be established correctly, even if they do not operate at their intended location. This may be caused by malicious conduct or mechanical collisions on devices. The promising solution in such cases is to deploy wireless localization systems for user and assets along lifecycle phases. An example of a wireless localization system is presented in D5.4.2 “Identity, Security and Safety in Product Lifecycle Data Management” [17].

Apart from the identity management and access controls, the next level of security controls includes continuous security and safety monitoring and assessments based on anticipated risks for both the users and devices. The objective of such assessments is to examine all assets involved in corporate processes, gather detailed information about them and find associated vulnerabilities. For example, it makes sense to start with security and safety assessment of those assets with highest vulnerability (e.g. devices with a high network exposure) or largest potential risk (e.g. breaking and driving controls). The identified vulnerabilities need to be mitigated in order to protect the system. This includes configuring and updating each asset to strengthen its security and comply with security standards and regulations and corporate governance rules.

Once the proper security measures are established, the system needs to be monitored for changes to identify any potential vulnerabilities caused by newly installed applications or missing security patches, and to ensure that the integrity of the system is maintained even when it is used by the authorized users.

Understanding risks related to trust, ethics and legal issues is seen as a key to ensure greater safety. Although trust and ethics are not at the core of IoT4CPS, both are considered as additional concerns for major stakeholders, such as authorities, governance bodies, manufacturers and the public alike. There is currently a large body of trust algorithms proposed for sensor networks and distributed applications used to calculate trust of IoT systems, as well as trust management protocols for IoT systems and CPS applications. Ethics can be seen as a trust enabler for smart vehicles, and in no case should the ethical algorithms be put in practice as non-transparent black boxes. The need for optimization strategies for safety-critical decisions of smart vehicles should become an integral part of smart vehicles and their controlling algorithms. This is also reflected in recent trends towards assisting intelligence that places “humans in the loop” for the final decisions while not requiring constant human input and intervention [18].

4. RESULTS

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. The vehicles communicate with a range of systems, from traffic management, weather monitoring, pollution control, emergency response, to fuel supply, operational powertrain and chassis controls. In order to provide smooth communication, information exchange and interactions among smart vehicles and their environment, it is necessary to ensure interoperability at various levels. For example, the interoperability at the data level enables information gathered from vehicles (e.g. in-vehicle operations, planned journeys, environment measures) to be used to make the journey more efficient, reduce the costs, improve safety and protect the privacy of stakeholders *(Figure 4)*. The role of standards and best practices can be seen as increasingly important in ensuring data interoperability and enabling the transmission of operational and environmental information in the CAM sector. Another set of recommendations includes the reference architectures that guide the integration of IoT devices at various functional layers, e.g. the Platform Industry 4.0 (RAMI 4.0 (Reference Architecture Model for Industry 4.0), IIC (Industrial Internet Consortium) (IIRA 2.0 (Industrial Internet Reference Architectures) and the cloud communication standard OPC-UA (OPC Unified Architecture).

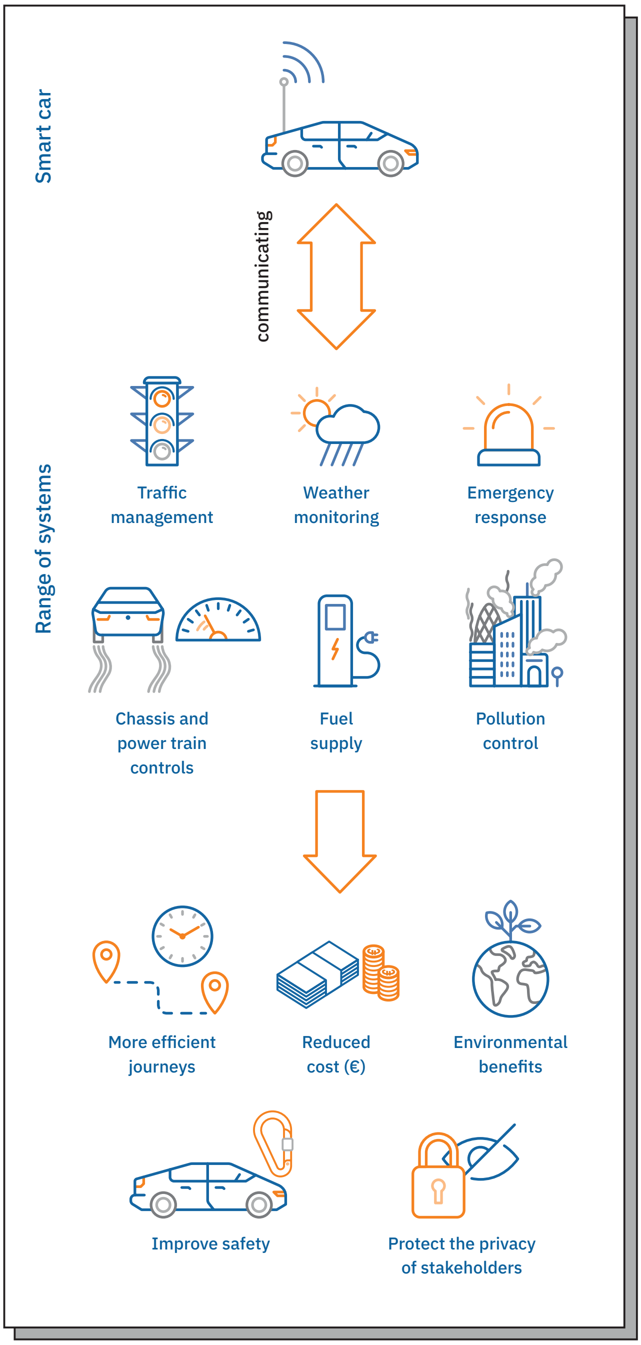

Figure 4: Example of range of systems communicating with a smart car and the results of ensuring interoperability at various levels

An extensive overview of relevant standards and recommendations for CAM applications is provided in the report D5.1 “Data Models for the IIoT and Industry 4.0, and in the Automotive Sector” [19]. The CAM sector typically does not publicize data. Hence, to bridge the existing gap between data engineering and IoT lifecycle data acquisition and management, the report D5.2 “Data Model for Multi Stakeholder Lifecycle Data Management” [20] presents the IoT4CPS data methodology that includes the following steps:

- Searching for relevant public datasets that include automotive lifecycle data and automotive security, safety and privacy data,
- Designing methods to assimilate the diverse datasets to support decision-making processes,
- Developing security, safety and privacy models and risk-based metrics to help security and safety analysts decide on relevant hypotheses,
- Developing techniques to address emerging threats in cloud security, at the software layer (against ransomware, phishing) and the infrastructure layer,
- Assessing the expected improvement and the increase in the value that is added to the overall security and safety of the system through the Digital Twin prototype.

The report D5.2 “Data Model for Multi Stakeholder Lifecycle Data Management” also presents an underlying multi-tenancy data model that includes data sources for stakeholders from both Automotive Driving and Automotive Manufacturing. In the report D5.4.1 “Identity, Security and Safety in Product Lifecycle Data Management”, the same data model is extended to address identity, security and safety features, along the previously identified multi-tenancy aspects in the CAM industry [21]. In the report D5.4.2 “Identity, Security and Safety in Product Lifecycle Data Management”, the data model is further extended to include privacy, ethics and trust features for CAM applications [17]. The presented approach in IoT4CPS contributes to the design of cross-interaction and interoperation among the smart vehicle’s systems and their stakeholders in the cloud, while providing security, safety and privacy validations along the vehicle’s lifecycle. This is discussed in the report D5.3 “Cross-Platform Interoperation Model” [22]. In order to widen the re-usability of publicly shared automotive data, the D5.3 report also compares the proposed models with the existing cross-platform interoperation models, such as those suggested by knowledge-base and data technologists and models developed through Austrian and European data management initiatives, e.g. International Data Spaces (IDS)[8], Data Market Austria (DMA)[9], the Common European Data Spaces for the Manufacturing Sector[10], etc.).

As the majority of current CAM solutions are of a commercial nature, IoT4CPS designs a basis for an open source technology for security and safety validations of the automotive applications. Such technology utilizes the concepts of Digital Twins to effectively combine measurable data sources (sensors) with desired values (metrics), and enhance connected asset and stakeholder data with derivative data obtained from analytics tools. This data can be further correlated to detect operational abnormalities and generate alerts. These results are presented in a series of three reports, D5.5.1 „Lifecycle Data Management Prototype I“, D5.5.2 „Lifecycle Data Management Prototype II“ and D5.5.3 „Lifecycle Data Management Prototype III“ [23,24,25].

[8] International Data Spaces: https://www.internationaldataspaces.org/
[9] Data Market Austria: https://datamarket.at/
[10] https://ec.europa.eu/digital-single-market/en/news/common-european-data-spaces-smart-manufacturing-0

5. POSSIBLE EXPLOITATION

The current lack of standardized and regulated approaches to security, safety, privacy and trust is seen as the greatest obstacle to further growth of IoT and CPS systems, slowing down the evolution of smart vehicles and future CAM applications. The current security mechanisms in smart vehicles perform continuous tracking of vehicles for road safety purposes, thus requiring privacy and security features to be adequately addressed, e.g. through pseudonymization of messages for long and short term (authorization ticket) certificates, and more. Hence, transparency laws and guidelines on the use of advanced technologies are necessary and emerging. Some approaches to protecting privacy follow Privacy by Design (PbD), GDPR, Privacy Impact Assessment (PIA), or design “notice and choice” systems that 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. Today, many automotive companies, including vehicle renting services, offer privacy checklists when selling or renting smart vehicles to customers. These lists strongly suggest removing private and sensitive data, e.g. phone and address book, navigational data to favourite locations, home, friend’s home, work, mobile applications with the data exchanged during the drive, garage door programming, dongles that may share data with third parties, etc.

The results of the analysis provided in the reports D5.4.1 and D5.4.2 serve as a basis for the design and implementation of the Digital Twin prototype in IoT4CPS. For example, to enable safe navigation, both smart vehicles and smart roads need to transmit information about traffic, weather and road works to the cloud. The prototype implemented in IoT4CPS was tested in two scenarios, as described in more detail in the report D5.5.3:

- The first scenario targets the safety features of the smart vehicle through safety warnings on bad weather conditions, such as the presence of ice or other slippery conditions on the road, and
- The second scenario is about identifying security vulnerabilities of production systems. These vulnerabilities could affect orders with delivery dates that cannot be reached due to unplanned machine breakdowns.

The further design of the Digital Twin prototype for the automotive industry and manufacturing requires not only an effective data strategy and methods to be put in place; it also requires balancing regulatory issues at national and international levels and building a strong data governance framework that can provide traceability of events along the entire lifecycle and supply chain.

REFERENCES

[1] D. Jiang and L. Delgrossi, (2008). „IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," VTC Spring 2008 – IEEE Vehicular Technology Conference, Singapore, pp. 2036–2040.

[2] M. Grieves. Digital Twin: Manufacturing Excellence through Virtual Factory Replication, 2014.

[3] Grieves, M., Vickers, J. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. in Kahlen F-J. Flumerfelt, S., Alves, A., (Eds.) Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches, Springer International Publishing, pp. 85–113. (2017)

[4] Rios, J., Hernandez, J.C., Oliva, M., and Masb, F. Product Avatar as Digital Counterpart of a Physical Individual Product: Literature Review and Implications in an Aircraft System. In: ISPE CE: pp. 657–666. (2015).

[5] Negri, E., Fumagalli, L., Macchi, M. A Review of the Roles of Digital Twin in CPS-based Production Systems. In Proceedings of the 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27–30 June 2017, Modena, Italy. Procedia Manuf 2017; 11:939–48. 2017.

[6] Gabor, T., Belzner, L., Kiermeier, M. A Simulation-Based Architecture for Smart Cyber-Physical Systems. IEEE International Conference on Autonomic Computing (ICAC) 2016:374–379. (2016)

[7] Haag, S. and Anderl, R. Digital Twin – Proof of Concept. Manufacturing Letters, (2018)
Online: https://doi.org/10.1016/j.mfglet.2018.02.00

[8] Boschert S, Rosen R (2016) Digital Twin – The Simulation Aspect. in Hehenberger P, Bradley D, (Eds.) Mechatronic Futures: Challenges and Solutions for Mechatronic Systems and their Designers, Springer International Publishing 2016, pp. 59–74

[9] Schleich, B., Anwer, N., Mathieu, L., Wartzack, S. Shaping the Digital Twin for Design and Production Engineering. In CIRP Annals – Manufacturing Technology. Pp. 141–144. (2017)

[10] Hochhalter, J., Leser, W.P., Newman, J.A. Coupling Damage-Sensing Particles to the Digital Twin Concept. NASA Center for AeroSpace Information. (2014)

[11] Reifsnider, K., Majumdar, P., Multiphysics Stimulated Simulation Digital Twin Methods for Fleet Management. 54th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 1578. (2013)

[12] M. Eckhart, and A. Ekelhart, "Towards security-aware virtual environments for digital twins," in Proceedings of the 4th ACM Workshop on Cyber-Physical System Security (CPSS '18). 2018, ACM, New York, NY, USA, 61–72.

[13] Bécue et al., "CyberFactory#1 – Securing the industry 4.0 with cyber-ranges and digital twins," in 14th IEEE International Workshop on Factory Communication Systems, Imperia, 2018, pp. 1–4.

[14] R. Bitton et al. "Deriving a cost-effective digital twin of an ics to facilitate security evaluation," in I Javier Lopez, Jianying Zhou, and Miguel Soriano (eds.), Computer Security, pp. 533–554, Cham, 2018. Springer International Publishing.

[15] V. Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry," in Proceedings of the 9th International Conference on Intelligent Systems: Theory, Research and Innovation in Applications. 2018, Portugal.

[16] D. Antonioli, and N.O. Tippenhauer, “MiniCPS: A Toolkit for Security Research on CPS Networks,” in Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and PrivaCy (CPS-SPC’15). 2015. ACM, 91–100.
[17] D5.4.2 „Identity, Security and Safety in Product Lifecycle Data Management“. 2020. Online available: https://iot4cps.at/deliverables-and-publications/
[18] Russel Stuart, (2020). “How Not to Destroy the World with AI”. ECAI 2020 keynote: https://digital.ecai2020.eu/keynote-speakers/
[19] D5.1 „Lifecycle Data Models for Smart Automotive and Smart Manufacturing“. 2018. Online available: https://iot4cps.at/deliverables-and-publications/
[20] „Product Lifecycle Data Management (PLCDM) Stakeholder Perspectives“. 2019. Online available: https://iot4cps.at/deliverables-and-publications/
[21] D5.4.1 „Identity, Security and Safety in Product Lifecycle Data Management“. 2019. Online available: https://iot4cps.at/deliverables-and-publications/
[22] D5.3 „Cross-Platform Interoperation Model“. 2019. Online available: https://iot4cps.at/deliverables-and-publications/
[23] D5.5.1 „Lifecycle Data Management Prototype I“. 2019. Online available: https://iot4cps.at/deliverables-and-publications/
[24] D5.5.2 „Lifecycle Data Management Prototype II“. 2020. Online available: https://iot4cps.at/deliverables-and-publications/
[25] D5.5.3 „Lifecycle Data Management Prototype III“. 2020. Online available: https://iot4cps.at/deliverables-and-publications/

ABBREVIATIONS

ABS	Anti-lock Braking System
BMK	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
CAM	Connected and Automated Mobility
CPS	Cyber Physical System
DEI	Digitising European Industry
DMA	Data Market Austria
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
IDS	International Data Spaces
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architectures
IoT	Internet of Things
IoT4CPS	Trustworthy IoT for CPS
ITS	Intelligent Transport System
KPIs	Key Performance Indicators
NIS	Network and Information Systems
OPC-UA	OPC Unified Architecture
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLCDM	Product Lifecycle Data Management
RAMI	Reference Architecture Model for Industry 4.0
SPI	Sensitive Personal Information
UNECE	United Nations Economic Commission for Europe

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

Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Layout & Grafik

Nora Novak, goldmaedchen Grafikdesign

Legal Notices

The information in this document is subject to change without notice.

The Members of the IoT4CPS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IoT4CPS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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