Safety and Security of IoT-based Solutions for Autonomous Driving: Architectural Perspective ⋆

Omar Veledar[1], Georg Macher[2], Violeta Damjanovic-Behrendt[3], Stefan Jaksic[4], Christos Thomos[5], Christoph Schmittner[4], Konrad Diwold[2,6], Leo Happ Botler[2], Eva Maria Holzer[1], Eric Armengaud[1], Kay Römer[2], and Mario Drobics[4][0000−0001−9194−6392]

[1] AVL List GmbH, Hans List Platz 1, 8020 Graz, Austria
omar.veledar@avl.com
[2] Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria
roemer@tugraz.at
[3] Salzburg Research Institute, Jakob-Haringer Strasse 5/3, 5020 Salzburg, Austria
violeta.damjanovic@salzburgresearch.at
[4] AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria
mario.drobics@ait.ac.at
[5] Infineon Technologies Austria AG, Siemensstrasse 2, 9500 Villach, Austria
Christos.Thomos@infineon.com
[6] Pro2Future GmbH, Inffeldgasse 25f, 8010 Graz, Austria
Konrad.Diwold@pro2future.at

Abstract. The ongoing business revolution, which is enabled by technological evolution of IoT, is affecting a wide range of industries. The effect of IoT on automotive sector is further enhanced by other trends, such as autonomous driving (AD). The user acceptance of AD depends on successful integration of IoT with Cyber-Physical Systems (CPS), which are crucial components for monitoring and control. Their reliance on data is strongly correlated to the dependability. This paper describes the architectural design for safe and secure IoT-based solutions aimed at AD, considering the design principles of the *IoT4CPS*, an Austrian national funded project. *IoT4CPS* seeks to create guidelines, methods and tools for safe and secure integration of IoT into AD and related smart production. It addresses secure localization in V2X communication networks and the tight integration of vertical stakeholders along the supply chain. A Digital Twin model is applied to evaluate safety and security solutions of a full life-cycle. We also propose design methods for ensuring dependability of IoT. The proposed holistic safety and security architecture of *IoT4CPS* considers the complete life cycle and value chain.

Keywords: IoT4CPS · IoT · CPS · Safety · Security · Dependability · Autonomous Driving

⋆ This research has been funded by the Austrian Research Promotion Agency (FFG) and the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), within the "ICT of the Future" project *IoT4CPS* (Trustworthy IoT for Cyber-Physical Systems) (December 2017 November 2020) and (FFG) (#6112792)

1 Introduction

In order to achieve the full potential of AD concept and to build a strong root of trust for IoT in a stable and cost-effective manner, operational and information technology interconnection and integration of security levels across all dimensions must ensure trusted interaction across devices, machines and networks, integrity, authenticity and confidentiality of information and sufficiently protected production data and intellectual property. This integration of appropriate security levels should also provide ease of deployment and not negatively impact performance or compromise on user experience. Tailored security functionality must be maintained to balance between performance and cost.

IoT is a key enabler of current automotive revolution. Its success is subjected not only to conceptual designs, but also to speed of transformation and depth of changes. The answers are emerging through pilot projects in the field of smart transportation, supply chains for manufacturing, logistics, connected infrastructures, smart cities and related urban mobility as a service etc. *IoT4CPS*' contribution is aimed at solutions for trusted IoT, which are applicable to Autonomous Driving (AD). Practical solutions that offer trusted interaction demand an architectural design for safe and secure IoT-based solutions. There is a need for extension of guidelines, methods and tools for safe and secure integration of IoT for autonomous driving and corresponding smart production.

The evolution of IoT and its application to AD is not the only supporter of revolution with automotive industry, which is one of the key European sectors [1]. The industry is also subjected to major societal challenges, such as: emission control [2], reduction of traffic fatalities [3], mobility for ageing population or congestion issues. The consumer habits are also evolving and are generating demands for mobility as a service, infotainment and connectivity, human-machine interaction and customisation. Four main trends that are influencing automotive industry are: electrification, assisted and autonomous driving, connected vehicles and diverse mobility [4]. Digitalisation (IoT inclusive) is a crucial supporter of these trends. The resulting real-time connectivity to cloud services is transforming vehicles from transportation means to integrated systems in a connected world of things. Simultaneously, mutual vehicle connectivity and interactions with infrastructure significantly contribute to road safety and user experience. Therefore, trends affecting connected vehicles (figure 1) raise research interest with potential to contribute to growth and creation of new business models.

2 IoT4CPS

The *IoT4CPS* is Austria's national flagship project, which aims to develop safe and secure IoT solutions for industrial applications. The overall goal of *IoT4CPS* is to provide methods and tools to support the development, production and maintenance of safe and secure IoT solutions in the field of AD and Smart Production, demonstrate their applicability in laboratory and industrial environments, and thus to increase innovation capacity in this area in Austria. The

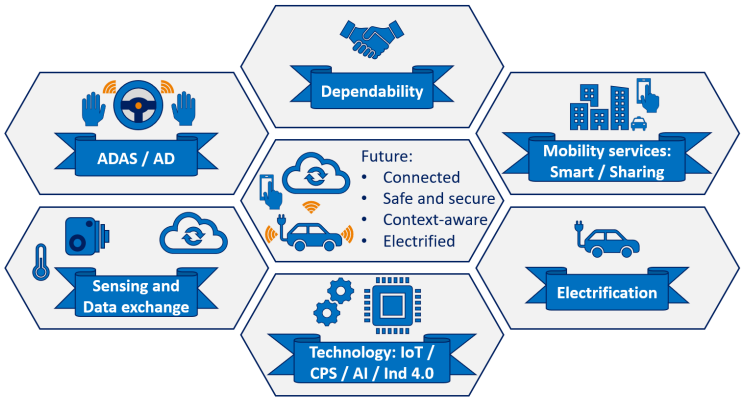

Fig. 1. Automotive domain trends

project involves 17 industrial and academic partners, enabling it to address security issues of CPS in a holistic approach both along the specific value chains and the product life cycles.

IoT4CPS aims to deploy innovative and trustworthy IoT components, solutions and environments, both for the product as well as its development and production environment, in order to (a) increase quality and range of functions for AD systems, and (b) accelerate the development, validation, instrumentation, production and in-field deployment of these solutions.

Through innovation in different technologies orientated towards two application fields, *IoT4CPS* supports full product life-cycle and aspects of designing, testing, producing, and operating of secure IoT elements and systems. The technological activities are grouped in three areas:

- **Design & Development of CPS:** Methods for the design of safe and secure industrial IoT applications. Provisioning of tools to support security by design or ease the integration of security mechanisms across partners.
- **Verification & Analysis:** Verification of system requirements to ensure system reliability and system monitoring to ensure system resilience.
- **Life-cycle Management:** Enable security throughout the system lifetime, including mechanisms to provide updates. Support integration of field learnings in production processes for next-generation solutions.

2.1 Use case: autonomous driving

As connected and automated driving are significantly benefiting from advances in secure, trusted IoT, the AD use case is exploited to demonstrate trustworthiness of developed assets, which are covering major parts of the AD value chain. The intricate technical solutions encompassed by AD are achieving marketable levels of maturity. The core is formed around CPS capable of hosting high-performance computing and connectivity. In contrast to historic addition of control units for each fresh functionality, the current trend bases control strategy on centralised

computing platform, increasing the CPS complexity. That is partially counterbalanced by edge computing, which reduces data traffic and enables decisions at reduced latency. The resulting distributed intelligence incorporates dependability, which is a critical factor in driving applications. The inevitable shift towards AD is uncovering an underlying conflict between the decision making around vast number of possible driving scenarios and the safety, which demands extensive testing of all possibilities. Therefore, the use case tackles security and safety aspect of technologies capable of meeting AD related challenges.

2.2 IoT Life-cycle management

One of *IoT4CPS*s overall project goals is digitalisation along the entire product life-cycle, leading to time-to-market acceleration for connected and autonomous vehicles. Simultaneously, the integrative solutions aim to improve overall quality through considerations of complete solutions while designing individual components. An inevitable drawback of added connectivity and digitalisation that shifts vehicle controls towards centralised control unit with distributed intelligence is the increased exposure of critical cyber-physical objects to outside world, which exposes additional dangers and leads to new safety and security related design requirements. As success of IoT solutions depends not only on conceptual designs, but also on testing, production and in-field operation and maintenance of systems, *IoT4CPS* takes a holistic view in terms of integration of operational aspects as well as the technology bricks. Hence, security levels are integrated across all dimensions aiming to ensure trusted interaction between components, to maintain data quality and to protect data. A significant side-effect of life-cycle integration is improved interaction possibilities for two process types: new security and existing safety processes. Positive consequences are expressed in reduced time-to-market and (technical and business) risk mitigation; both qualities are considerable contributors to sustainability of benefits.

3 Design and architecture

The concept of life-cycle management is further bolstered by development of components and their integration into an architecture that is designed with effective safety and security in mind. The architecture is an integral component of connectivity mechanisms to protect vehicles, which are becoming increasingly vulnerable to cyberthreats due to the rise of communication access points into vehicles. The concept of Digital Twins is used as a security and safety enhancing tool for communication and control components of the proposed architecture. Digital twins of complex systems aid addressing of potential attacks through virtualisation, which if applied at both, early development stages and at run-time operation, should help tackle risks early in the life-cycle of the control CPS. The run-time risks are further mitigated using novel dependability design methods. These are crucial for AD that is pushing towards integration of data-driven controllers with self-adaptable properties during own operating lifetime.

As such, they are prone to exhibiting behaviour that is not possible to predict at design stages. Such behaviour may result from vehicle detecting an unfamiliar environment. In such occasions, it is the secure localization that maps vehicles surroundings and provides information needed for decision making.

3.1 Architectural aspects of secure and reliable V2X communication

V2X connectivity aims to enhance safety of vehicles, passengers and pedestrians by extending the sensing capabilities of on-board sensors, as well as vehicles computing power through specialised ad-hoc edge and cloud application services. Through data exchange with the communication network and the surroundings (e.g., nearby vehicles, the road infrastructure, pedestrians), the on-board sensor data is exchanged and enhanced through communication with surrounding entities. V2X communication comprises four main sub-categories: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I road infrastructure), vehicle-to-network (V2N backend/internet), and vehicle-to-pedestrian (V2P) communications which can be extended by including a variety of other use-cases (figure 2). When fully empowered, it will be a key enabler and a vital component of AD.

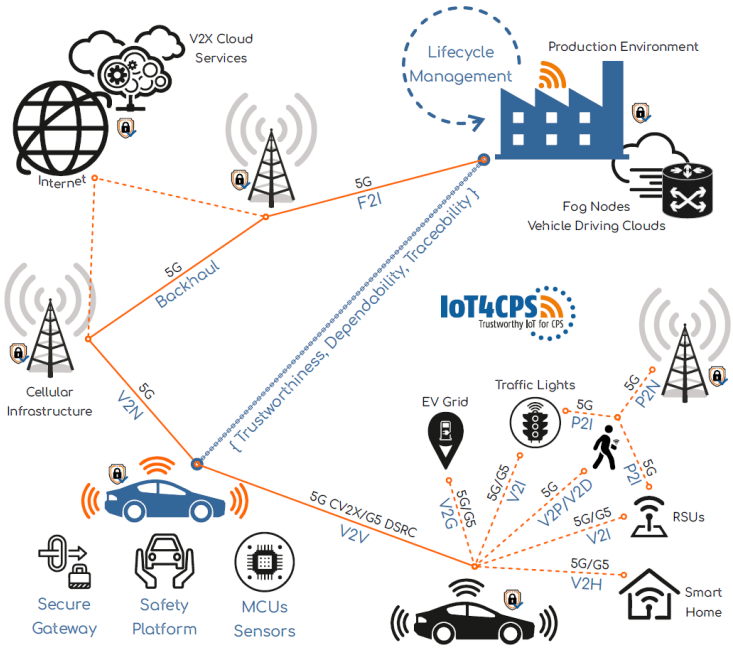

Fig. 2. V2X architectural aspects for secure and reliable communications

Current connectivity options applied to non-safety critical applications of SAE 0 and 1 level vehicles are in a basic form and are failing to to meet the

requirements of SAE Level 2-5 safety-critical applications. Higher levels of dependability, lower latency and higher capacity of wireless data communication are necessities. AD strongly depends upon integration of heterogeneous connectivity technologies (for in-vehicle and external radio access), with immense interoperability and cross-interference issues and a great difference in technology life-cycle between the vehicle and the communication modems. Wireless links must withstand extremely complex vehicular environment, in terms of mobility and dynamics, with highly diverse and contradictory demands with respect to the communication characteristics, as well as to other properties such as positioning accuracy, security, privacy and functional safety. Also, wireless connectivity introduces multiple security vulnerabilities into vehicle controls, infotainment, telematics and navigation systems or the supporting cloud infrastructure. Therefore, security-by-design is an imperative for sandboxing communication system drivers, embedding security along the entire V2X development phase and ensuring end-to-end encrypted communications and data privacy that safeguards autonomous vehicles at system level.

An initial evaluation of the quality of V2X technologies employs established metrics, such as end-to-end latency, communication coverage, position accuracy, data rate, link reliability and security features. The assessment of fundamental parameters determines capabilities of main V2X technology options, system architectures, constraints and hardware specifications that fulfill envisaged connectivity scenarios. The limitations must be resolved early in the design through simulations and large sets of field trials for as many V2X use-cases as possible. However, modelling, development, integration and testing in such an environment is an exceptional challenge. Also, as connected and autonomous vehicles become a common part of this complex ecosystem, requirements will become stricter and more demanding for unfolding the full potential of autonomous and cooperative driving. It is a common understanding that commitment from all V2X stakeholders is necessary to establish a complete connectivity framework able to fulfill ambition for evolution from SAE Level 2 to 5.

Main vehicle connectivity options are Dedicated Short Range Communications (DSRC) based on IEEE802.11p WLAN and 3GPP Cellular V2X based on cellular 4G (Rel. 14 and beyond) and upcoming 5G NR. Both options focus on lower layer definitions to offer long range, non-line-of sight abilities as an extension to vehicle sensors adding a redundancy factor towards enhanced safety and cooperative driving features. The upper layers are based on standardization activities such as IEEE (e.g., 1609), SAE, IETF, ETSI, ISO and CEN.

DSRC (EU: ITS-G5, US: WAVE) was developed for safety-critical V2V and V2I, by specifying ad-hoc networks (no communication infrastructure) in dedicated license spectrum bands (5.9GHz ITS band). It exchanges basic safety data with very low latency (¡50ms) in 2km radius, using public infrastructure and data security based on IEEE1609.2. The physical layer and lower MAC use the IEEE802.11p WLAN standard, which was finalised in 2010. Since then, IEEE802.11p [5] has passed broad and extensive validation tests and is very stable. It offers many mature products for deployment (e.g., C-ITS C2C-CC [6]).

Its Delegated Act [7] is awaiting EU approval. Hence, DSRC technology could become a regulatory requirement for intelligent transport system (ITS).

As no immediate advances are expected, DSRC applicability to V2X is limited. That opens the space to 3GPP Cellular V2X (C-V2X), which will leverage on 4G LTE evolution to 5G NR [8]. Cellular infrastructure is essential for data exploitation aimed to provide specialised cloud services, critical software and firmware over-the-air updates, life-cycle management, predictive maintenance, remote monitoring, as well as many alerts, warnings and notifications. The AD requirements are challenging for 4G LTE C-V2X and DSRC technologies, but 5G NR promises improvements in data rates, QoS support, ultra-low end-to-end latency, capacity and reliability, coverage and number of device connections, security, localization, energy efficiency, performance consistency and application support. These features aim to address ultra-reliable and low-latency connectivity for mission-critical services, device-to-device (V2V, V2I) communications, enhanced mobile broadband (V2P, V2N) and machine communication, as needed for a fully autonomous vehicle ecosystem. The upper layers of LTE C-V2X are making use of the same standards as the IEEE802.11p based technologies, as specified by automotive industry. However, independent implementation of two technologies and lack of interoperability mechanism renders them incompatible.

The resulting technology selection dilema is further complicated by the EC activities that could create a de facto mandate to integrate ITS traffic and safety-related communications. Considering the average 10-year vehicle lifespan, DSRC technology is likely to aid the upcoming vehicle generation in the 5.9 GHz ITS band. C-V2X is expected to enter markets in early 2020s, as a complement to V2V and V2I connectivity (safety critical ADAS and AD functions) and will enhance V2X connectivity with its unique V2N and V2P capabilities.

Uptake of C-V2X solutions and its differentiation from the outdated DSRC demands progress of wireless infrastructure. In this context, *IoT4CPS* is examining 5G PHY layer technologies for cellular access points, hardware architectures and behavioural models, transceiver modules capabilities and limitations, specifications for key building blocks that can address the requirements of secure C-V2X connectivity taking also into account the progress for the vehicle communication modules, sensors, actuators and computing hardware, as well as the solutions and tools for secure and safe AD platforms.

3.2 Secure localization

Localization enables a vehicle to map itself and its surrounding entities in a global coordinate system and precedes autonomous actions taken by the vehicle. In the light of AD, news headlines concerning accidents caused by drivers blindly trusting navigation systems (and, e.g., navigating their car into a river), corroborate the importance secure and trusted localization mechanisms.

A wide range of technologies have been brought forward and tested in the context of localization for AD, which likewise communication mechanisms, can rely on interactions with the infrastructure, other vehicles, people and the existing network, such as mapping, GNSS receivers, network interfaces, radars, LIDARs,

ultra-sound system, IMUs, Cameras, fingerprinting and Radar [9]. There is a trade-off between these technologies in terms of accuracy, cost, range and speed. The environment can also have a crucial impact on the robustness of the technology (e.g., GNSS functions poorly in tunnels), which leads to different levels of trust towards specific localization techniques in different application scenarios. In addition to non-malicious errors, the selective inference of localization techniques (e.g., via jamming) has to be taken into account, which opens yet another (less predictable) attack vector towards secure and trusted localization.

GNSS receivers are the main technology for vehicular self-localization, which can provide an inexpensive global positioning estimate, with GPS being the most prominent technology in this context. The main dependability issue of GNSS in the context of AD is the lack of availability of GPS systems in obstacle prone environments (e.g., urban environment, tunnels and bridges), as obstacles can block the incoming signals. From a security perspective GNSS systems can be subject to spoofing and jamming attacks [10].

The advent of deep-learning strategies gave rise to camera-based localization techniques [11]. Such approaches require adequate models, which counter and reduce the impact of lighting on the interpretation of a scene. A number of recent studies show how adversarial attacks [12] can impact camera-based systems. Such attacks must be foreseen during training to mitigate their potential effects. Redundancy, i.e., using multiple cameras, and adding optical filters are the two main solutions for this attack, but can still not prevent a more sophisticated (e.g., adversarial) attack, if the system is not trained to deal with it.

Signal spoofing and relaying can be used to attack a vehicles LIDAR-based localization system [13]. Spoofing and jamming also constitute a main attack vector in the context of ultra-sound systems. In addition, attackers can attempt to cancel ultra-sound based localization approaches [14].

WiFi-based localization systems are widely investigated in the literature. Due to hardware limitations, time-of-flight (ToF) techniques are usually not successful in providing decimeter level accuracy. Good accuracy can already be obtained with a AoA MIMO-based system, for instance, relying on a physically distributed infrastructure. Nonetheless, such a system is a typical target of jamming and spoofing attacks, which can make the system believe that the prover (unlocalized device) is in a completely different position. Also, in many scenarios, a dishonest prover can deceive such a system. Fingerprinting-based system were also investigated within WiFi [15], and in this case, the resistance against attacks and the ability to detect them were considered [16]. An attack can be detected and avoided, for instance, by selecting reliable signals that minimize the median of the distance.

AD localization can also be achieved via V2I communication [17]. In such a scenario, different ranging measurements between several entities can be obtained via round trip time (RTT) techniques using for example UWB technology. Besides UWB any localization approach based on RTT measurements can incorporate traditional distance bounding protocols in order to protect from many of the solved attacks, such as Mafia Fraud, Distance Reduction Fraud, Collusion

Fraud and impersonation [18]. This includes distance enlargement fraud (where an attacker convinces an entity that it is further away than it actually is). DEF can be covered, as far as the vehicle is within the region/triangle involved by at least three verifiers in the 2-D case, which is a limitation [19]. A drawback of V2I based localization is its cost. Besides, V2I ranging techniques can be used to obtain distance measurements between two vehicles (V2V) and construct a map of the environment (including other vehicles and objects) [20]. As outlined, each available localization technique is prone to attacks or environmental impacts. To counter these, cooperative localization techniques can be used. Here the sys-

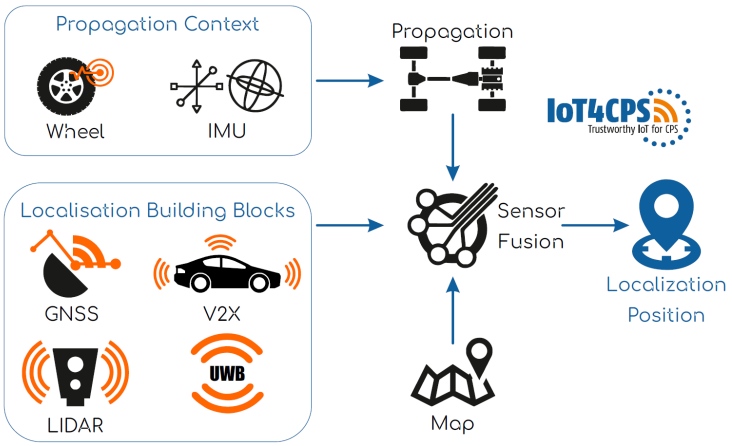

Fig. 3. Architecture of cooperative localization for autonomous driving

tem does not depend on a single source of localization, but uses a multitude of localization mechanisms. Results are cross-verified to a) increase the accuracy of the overall localization and b) detect and mend malicious and non-malicious malfunctioning. A resulting architecture for secure localization in autonomous vehicles is shown in 3, where the architecture incorporates redundancy in order to cancel out and mitigate the short comings of specific technologies. In order to get information on the vehicle's propagation, the inertial measurement unit (IMU) and sensors at the wheels can be used. For localization a combination of a number of technological building blocks are possible. The propagation information is fused with the outputs of the localization mechanisms and combined with map information to securely localize the vehicle. Given the redundancy in design, the shortcoming of a single localization building block (e.g., due to malicious attacks or environmental impact or even failure), can be identified in the process of data verification and fusion and balanced out by the system by relying on localization information obtained from other building blocks. In addition the process of fusing the results of different localization building blocks allows to mitigate noise in terms of position. Which building blocks should be used to comprise the final localization strategy depends on the use-case and

corresponding attack models. Combining different technologies, such as GNSS, LIDAR and Camera-based, all vulnerable to jamming, can increase the security level of the solution requiring an ultra sophisticated attacker to perform an attack. In this scenario, the attacker would have to simultaneously target all the sensors, which are spatially separated, with the corresponding technology. Also combining technologies that are sharing the same channel/physical principle can increase the security level by constraining gaps of one technology, such as UWB, which is still vulnerable to the DEF, but if combined with a WiFi fingerprinting approach manages to cover this attack. The table 1 summarizes the aspects of different localization strategies to enable a use-case dependant selection.

Technology	**Open Threats**	**Notes**	**References**
UWB	DEF	DEF can be overcomed within a triangle delimited by a trusted infrastructure	[18]
WiFi	Mafia Fraud (untrusted infrastructure)	> 3m accuracy without attack	[16]
Camera-based	Jamming/Blinding	No definitive countermeasure	[13]
LIDAR	Jamming/Saturating + Spoofing	Existing impractical solutions	[13], [14]
GNSS	Jamming + Spoofing	Many solutions to spoofing exist but are not yet necessarily implemented in a system level	[10]

Table 1. Localization technologies and attack models

3.3 Digital twin for autonomous driving

The AD trend includes CPSs and Digital Twins, thus expanding the digital representation of assets into executable models of manufacturing processes and workflows. Concurrent with the above trend, network-centric computing has evolved into cloud computing enabling large-scale data analytics and Machine Learning (ML), as prerequisite for desirable new solutions for autonomous decision making, adaptation and self-management of AD systems, predictive and intelligent forecasting capabilities. With the huge increase in connected devices and their business processes and workflows, comes a commensurate rise of cybersecurity risks and challenges. Traditional security solutions are inadequate when used in cloud environments. Therefore, strengthened cybersecurity for cloud services is a necessity, which requires novel design solutions with respect to the modelling of cybersecurity threats and countermeasures. *IoT4CPS* investigates the concept of a Digital Twin as a means of validating security and functional safety measures and their interplay with physical assets of AD settings. Our motivation is twofold: on one hand, it considers designing and implementing a demonstrator for the validation of novel methods, and on the other hand, we aim to augment current security and safety-critical AD functions by taking a data-centric approach to asset identification and monitoring, decision-making and virtualisation.

We designed the Digital Twin demonstrator architecture [21] with the following capabilities: Virtualization Management, Data Management, Model Management, Service Management, and Connectivity and Interoperability Component (figure 4). The Virtualization Management component identifies and monitors virtual assets in the cloud environment. It also involves data protection measures, access controls and responsibilities related to assets and it identifies and monitors processes and workflows that involve physical assets. The Data Management component implements data analytics services capable of consuming data coming from connected devices and their sensors. That data is also combined with, e.g., historic and maintenance data, customer feedback and complaints logs, product data and data from other business systems such as the ERP. The Model Management component addresses data models for capturing anomalous behaviour of assets. We consider threat models and data controls to identify dangerous data combinations. The Service Management component is designed to provide simulation and decision-making features for those cybersecurity services that need to be validated through the Digital Twin. Finally, the Connectivity and Interoperability component enables exchange of data between our Digital Twin and the MQTT broker.

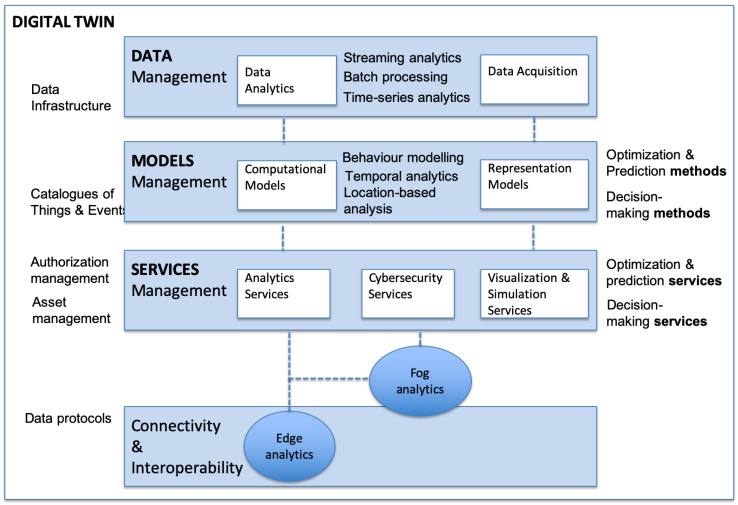

Fig. 4. Digital Twin Concept Architecture

In order to overcome the strong technology fragmentation, we compose our Digital Twin demonstrator from available open-source tools and services. At present, Digital Twin solutions are often built as closed systems, thus limiting the network potential of connected assets. Our current Digital Twin implementation includes a real-time monitoring system for virtual assets, e.g., for visual inspection and identification of assets. The current composition of open-source tools and services is shown in figure 5. After establishing the connection with the experimental environment, our next step is to (i) further explore cybersecurity

and safety properties of connected assets (e.g., access controls), (ii) continuously monitor processes and workflows involving those assets, (iii) compare asset measurement data with relevant metrics, and (iv) execute specific models to identify behavioural anomalies

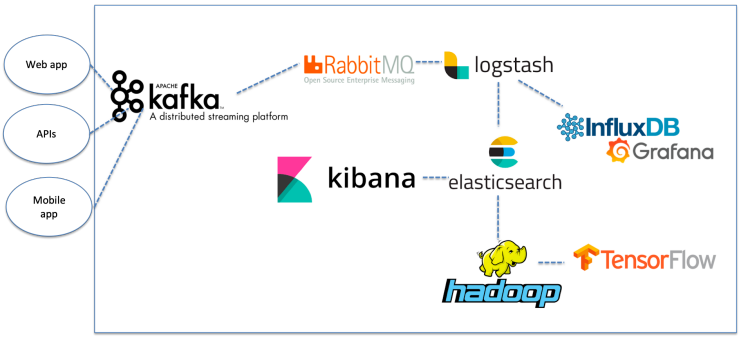

Fig. 5. A Composition of Open Source Tools and Services for a Digital Twin Demonstrator

3.4 Dependability design methods

In this section we propose how to ensure dependability attributes of IoT. Dependability by definition [22] consists of several attributes: availability, reliability, safety, confidentiality, integrity and maintainability. In the AD context, we focus on ensuring safety of a system during operation using real-time monitors based on Signal Temporal Logic (STL).

Latest AD advances, which primarily include application of machine learning, impose new verification challenges. Data-driven controllers are self-adaptable during lifetime [23], thus are able to learn new behavior patterns during operation. They may exhibit behavior which cannot be anticipated prior to their deployment in real conditions. As it is impossible to forecast all relevant scenarios, the design-time verification cannot provide firm safety guarantees. However, the safety requirements are fixed regardless of the device behavior. For this reason, we anticipate a natural shift of focus from exhaustive design-time verification to a specification-based verification method applied during execution (monitoring).

STL is a specification language for properties of analog and mixed-signal systems, based on widely-adopted Linear Temporal Logic [24]. The formal semantics of STL allows writing non-ambiguous high-level safety requirements [25] as well as generating real-time monitors. Several recent case studies [26,27,28,29] have shown the merits of using real-time monitors in industrial applications.

An STL hardware monitor is an instance of STL monitoring algorithm implemented on a hardware platform (i.e., FPGA). It is an autonomous unit which adopts a black-box approach and monitors a device in a non-intrusive fashion.

Hardware monitor size has proven to scale reasonably well in case of safety specifications. The monitors provide finite and predictable evaluation delay, which allow them to monitor systems in real-time. The architecture of the monitors does not impose any constraints w.r.t. their speed. The monitors operating frequency is bounded only by hardware limits, implying that monitors can receive inputs signals at the rate of hundreds of MHz. Thus, it is guaranteed that the events related to physical behaviors which occur at order of magnitude slower rate can be reliably monitored with this approach. Due to high operating speed, the monitor verdicts are produced within a very short time interval allowing for a timely reaction by a high-level component.

Three engineering levels are considered or AD dependability. We avoid or control failures in a basic system, e.g., transforming a control command like "steer left" or "speed up" in a concrete action. At this level, there are only minor differences between autonomous vehicles and traditional vehicles and the dependability engineering is addressed by functional safety standards like ISO 26262 and methods like FMEA / FTA. In traditional vehicles, control commands are given by the driver. AD control commands are given by a technical system, and we must correctly identify situations and provide correct control commands. For this we ensure that the system is able to handle all situations which are expected in the considered environments. We minimise uncertainties, e.g., the missing knowledge about situations, scenarios and risks. Hence, there is a need for methods which are either suited for complex systems or are able to document and address missing knowledge. The relevant standards are ISO PAS 21448. An additional layer of cybersecurity is taken into consideration for connected and autonomous vehicles. We ensure the use of only trustworthy information as basis for decision making. Therefore, methods such as SAHARA, FMVEA, Threat Modeling and standards like ISO/SAE 21434 are relevant.

4 Conclusion

In the sea of changes within automotive industry, IoT has emerged as one of the main bolstering tools for sustainable deployment of novel solutions. *IoT4CPS*' trusted IoT solutions contribute to full supply chain relevant for fail-operational AD functions. We are investigating crucial building blocks for secure V2X connectivity, also considering AD related components for secure and safe platforms. Secure localization plays a crucial role in the context of autonomous driving. While a variety of technologies exist, which can be utilized in this context, they differ in terms of the precision they can achieve and are susceptible to environmental factors and external attacks. The shortcomings of individual methods can be overcome via a cooperative localization approach (i.e., the combination of individual localization techniques). In addition, the ongoing developments and advances in the context of communication technologies are expected to supplement the existing variety of localization solutions overcoming security flaws that are still not solvable for individual technologies. Current Digital Twin platforms mainly address optimization aspects in manufacturing, while in *IoT4CPS* our

focus is to realize a demonstrator for validation of security and safety measures collected in the cloud. *IoT4CPS* is focusing on utilising Digital Twin demonstrator for validation of security and safety measures collected in the cloud and hence, for tackling the newly exposed security vulnerabilities. We also propose methods to ensure dependability attributes of IoT in general. These are huge topics and it is not possible to cover all of them into detail. However, in this paper, we are specifying certain aspects of the demonstration and focusing on points where security and safety can be provided. One of the primary goals of the application is vehicle safety and prevention of accidents.

References

1. European Automobile Manufacturers Association: The Automotive Pocket Guide 2018-2019, http://www.acea.be/publications/article/acea-pocket-guide.
2. EC, The Paris Protocol - A blueprint for tackling global climate change beyond 2020, https://ec.europa.eu/clima/sites/clima/files/international/paris_protocol/docs/com_2015_81_en.pdf.
3. EC, Road safety in the European Union: Trends, statistics and main challenges, https://ec.europa.eu/transport/sites/transport/files/road_safety/pdf/vademecum_2015.pdf.
4. Armengaud, E., Peischl, B., Priller, P., Veledar, O.: Automotive meets ICT enabling the shift of value creation supported by European R&D. In: 2018 International Congress: SIA CESA 5.0 Automotive Electronic Systems, Paris (2018). doi:10.1007/978-3-030-14156-1
5. IEEE 802.11p, https://standards.ieee.org/standard/802_11p-2010.html.
6. CAR 2 CAR Communications Consortium, https://www.car-2-car.org/.
7. EC, supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf.
8. 3GPP, Releases 14–17, https://www.3gpp.org/specifications/releases/.
9. Kuutti, S., Fallah, S., Katsaros, K., et al. A Survey of the State-of-the-Art Localization Techniques and Their Potentials for Autonomous Vehicle Applications. In IEEE Internet of Things Journal, vol. 5, no. 2, pp. 829-846, (2018).
10. Ioannides, R.T., Pany, T., Gibbons, G., Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. In Proceedings of the IEEE, vol. 104, no. 6, pp. 1174-1194, (June 2016).
11. Bertozzi M., Bombini L., Broggi A., Grisleri P., Porta P.P. (2009) Camera-Based Automotive Systems. In: Belbachir A. (eds) Smart Cameras. Springer, Boston, MA
12. Ilyas, A., Santurkar, S., Tsipras, D., Engstrom, L., Tran, B., and Madry, A. (2019). Adversarial Examples Are Not Bugs, They Are Features. arXiv preprint arXiv:1905.02175.
13. Petit, J., Stottelaar, B., Feiri, M., and Kargl, F.. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. Black Hat Europe, 11, (2015).
14. Yan, C., Xu, W., Liu, J. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. DEF CON 24 (2016).
15. Hernndez, N., Hussein, A., Cruzado, D., et al. Applying low cost WiFi-based localization to in-campus autonomous vehicles. 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), Yokohama, (2017) pp. 1-6.

16. Lai W.C., et al., A survey of secure fingerprinting localization in wireless local area networks, International Conference on Machine Learning and Cybernetics, Tianjin, (2013) pp. 1413-1417.
17. Deka, B. Secure Localization Topology and Methodology for a Dedicated Automated Highway System. (2013).
18. Avoine, G., et al. Security of Distance-Bounding: A Survey. ACM Comput. Surv. 51, 5, Article 94 (2018). DOI: https://doi.org/10.1145/3264628
19. Chiang, J.T., Haas, J.J., Hu, Y.C. Secure and precise location verification using distance bounding and simultaneous multilateration. In: Proceedings of the second ACM conference on Wireless network security. ACM, New York, NY, USA, 181-192.
20. Zheng X., Safavi-Naini R., Ahmadi H. (2015) Distance Lower Bounding. In: Hui L., Qing S., Shi E., Yiu S. (eds) Information and Communications Security. ICICS 2014. Lecture Notes in Computer Science, vol 8958. Springer, Cham
21. Damjanovic-Behrendt, V,: A Digital Twin Architecture for Security, Privacy and Safety. ERCIM News No. 115, Special Issue Digital Twins, (October 2018). https://bit.ly/2CCU0Il.
22. Avizienis, A., Laprie, J., Randell, B.: Fundamental concepts of dependability. University of Newcastle upon Tyne, Computing Science (2001)
23. Koopman, P., Wagner, M.: Autonomous vehicle safety: An interdisciplinary challenge. IEEE Intelligent Transportation Systems Magazine, 9(1):9096 (Spring 2017).
24. Pnueli, A., The temporal logic of programs. In: Proceedings of the 18th Annual Symposium on Foundations of Computer Science, pp. 46-57, IEEE Computer Society, Washington DC, (1977).
25. Maler O., Ničković D. (2004) Monitoring Temporal Properties of Continuous Signals. In: Lakhnech Y., Yovine S. (eds) Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems. FTRTFT 2004, FORMATS 2004. Lecture Notes in Computer Science, vol 3253. Springer, Berlin, Heidelberg
26. Nguyen T., Ničković D. (2014) Assertion-Based Monitoring in Practice Checking Correctness of an Automotive Sensor Interface. In: Lang F., Flammini F. (eds) Formal Methods for Industrial Critical Systems. FMICS 2014. Lecture Notes in Computer Science, vol 8718. Springer, Cham
27. Jones, K.D., Konrad, V., Ničković, D. (2010). Analog property checkers: a DDR2 case study. Formal Methods in System Design, 36, 114-130.
28. Fainekos, G.E., Sankaranarayanan, S., Ueda K., Yazarel, H. Verification of automotive control applications using S-TaLiRo, 2012 American Control Conference (ACC), Montreal, QC, 2012, pp. 3567-3572. doi:10.1109/ACC.2012.6315384
29. Selyunin, K., Nguyen, T., Bartocci, E., Grosu, R. (2016). Applying Runtime Monitoring for Automotive Electronic Development. 10012. 462-469. doi:10.1007/978-3-319-46982-9_30.
30. Tayeb, S., et al. Securing the positioning signals of autonomous vehicles. In: IEEE International Conference on Big Data, Boston (2017) pp. 4522-4528.
31. Capkun S., Hubaux, J. Secure positioning in wireless networks. In: IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 221-232 (2006).