



**QUEEN'S  
UNIVERSITY  
BELFAST**

## **Bird's-eye view on the automotive cybersecurity landscape and challenges in adopting AI/ML**

Siddiqui, F., Khan, R., & Sezer, S. (2022). Bird's-eye view on the automotive cybersecurity landscape and challenges in adopting AI/ML. In N. Abdennadher, E. Benkhelifa, J. M. Lloret, & Y. Jararweh (Eds.), *2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC 2021)* (pp. 1-6). (2021 6th International Conference on Fog and Mobile Edge Computing, FMEC 2021). Institute of Electrical and Electronics Engineers Inc.. <https://doi.org/10.1109/FMEC54266.2021.9732568>

**Published in:**

2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC 2021)

**Document Version:**

Peer reviewed version

**Queen's University Belfast - Research Portal:**

[Link to publication record in Queen's University Belfast Research Portal](#)

**Publisher rights**

© 2021 IEEE.

This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

**General rights**

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

**Take down policy**

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact [openaccess@qub.ac.uk](mailto:openaccess@qub.ac.uk).

**Open Access**

This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: <http://go.qub.ac.uk/oa-feedback>

# Bird's-eye view on the Automotive Cybersecurity Landscape & Challenges in adopting AI/ML

Fahad Siddiqui, Rafiullah Khan, Sakir Sezer

*The Centre for Secure Information Technologies (CSIT), Queen's University Belfast*

Belfast, United Kingdom

f.siddiqui, rafiullah.khan, s.sezer@qub.ac.uk

**Abstract**—The integration of intelligent functionalities in connected and autonomous automotive system has great potential to deliver personalised user experience and improve traffic management. It can benefit the society by improving highway capacity and safety of road users. The adoption of data-driven Artificial Intelligence and Machine Learning models in the automotive sector is opening venues to new services and business models such as autonomous fleet management, self-driving trucks, robo-taxi etc. However, where the sharing of mix-critical data brings opportunities, it simultaneously presents serious cybersecurity and functional safety risks. In recent years, the cyber attacks have impacted every segment of automotive system including electronic control unit, infotainment, communications, firmware, mobile apps etc. This adoption of AI and ML as enabling technology for next-generation autonomous transportation systems is going to significantly widen the automotive attack surface. This trend has increasing tendency of exposing both vehicle and road-side infrastructure to a wide range of sophisticated cyber attacks. This paper aims to review and build a body of knowledge on the topic of automotive cybersecurity, by bridging a domain-specific knowledge gap among automotive system designers, engineers and system security architects. For this purpose, it discuss the autonomous driving system data processing pipeline and threat analysis and risk assessment process of automotive cybersecurity standard ISO/SAE 21434 to harness and harden automotive cybersecurity. It highlights automotive system architectural and ecosystem challenges in adopting AI and ML driven decision making.

**Index Terms**—Autonomous Systems, Cybersecurity Engineering, AUTOSAR Classic, AUTOSAR Adaptive, Threat Analysis and Risk Assessment (TARA), ISO/SAE 21433, Functional Safety

## I. INTRODUCTION

The introduction of *Smart Mobility* offer a great potential to provide enhanced reliability and safety of road users, while simultaneously shorting journey times and increasing highway capacity [1], [2]. It is estimated that by 2030, the number of connected vehicles will reach 700 million, while the number of autonomous vehicles will reach 90 million worldwide [3]. The UK department of transport predicts that the connected and autonomous vehicles business would worth £41.7 billion by 2035 [4]. By design, an autonomous (self-driving) system shall operate in a partially unknown and dynamic environment. An environment composed of static (vehicles parked at the road-side, buildings, trees etc.) and dynamic objects (pedestrians, road markings, lane markings, traffic lights and street signs). Therefore it is essential for autonomous vehicle to build a map of its environment to perceive its surroundings and localise

itself within this dynamic environment. For this purpose, the autonomous driving system use multiple sensors (Cameras, LIDAR, RADAR and road-side infrastructure etc.) to sense the surrounding environment. The collected sensed data is then processed by leveraging data-driven *Artificial Intelligence* (AI) and *Machine Learning* (ML) models to build the scene representation, enabling capability to autonomously plan and take appropriate decisions by adjusting vehicle's physical controls (steering, acceleration and braking) as illustrated in Fig. 1. However, these scene understanding, planning and decision making processes are heavily dependent on the sensor data coming from multiple sources (Cameras, LIDAR, RADAR, road infrastructure V2X etc.). This data can be adversely manipulated or modified while propagating within the autonomous driving system data processing pipeline as illustrated in Fig. 1, which can lead to compromise and hazardous situations. Therefore, where each stage of the data processing pipeline bring benefits, it also widens the attack surface and likelihood of vehicles being exposed to cyber attacks [5], [6]. According to a report published in 2021, the remote attacks have consistently outnumbered physical attacks since 2010, accounting for 79% of all attacks between 2010 and 2020 and 77.8% of all attacks in 2020 alone [3]. The reported cyber attacks have impacted every segment of a connected vehicle and now rapidly extending towards autonomous vehicles. According to a report, the existing (known) automotive system vulnerabilities can manipulate alarming 23% of car control and safety-critical systems [3]. These cybersecurity risks have a direct impact on the safety of passengers and pedestrians as well as critical road infrastructure.

This paper aims to review and build a body of knowledge on the pressing topic of automotive cybersecurity by bridging a domain-specific knowledge gap among automotive system designers, engineers and cybersecurity architects. This fundamental knowledge of automotive system engineering and cybersecurity concepts which are critical for establishing a holistic automotive cybersecurity engineering processes by design rather than on ad-hoc basis, making automotive systems cyber resilient. Section II presents an overview of automotive cyber attack landscape and their impact on the future of the autonomous driving industry. The *Automotive Open System Architecture* (AUTOSAR) and its cybersecurity-related features are presented in Section III. *Threat Analysis and Risk Assessment* (TARA) process introduced by ISO-21434 automotive

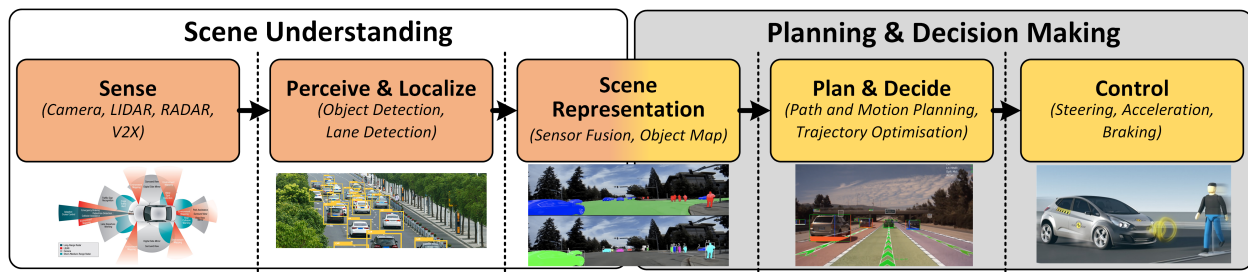


Fig. 1. An autonomous driving system data processing pipeline is composed of scene understanding, planning and decision making tasks [7].

cybersecurity standard to harness and harden cybersecurity is discussed in Section IV. Section V highlights the architectural challenges and impact of AI and ML driven decision making on the future of autonomous driving.

## II. AUTOMOTIVE CYBER ATTACKS

For a long time, vehicles have always been an appealing target for adversaries in the form of theft. Though such type of attacks require physical access to the vehicle, therefore the early vehicle security technologies were mainly confined to physical security i.e. door locks, ignition, immobiliser, radio and alarm systems. During the last decade, mass integration of complex hardware/software technologies and on-board connectivity has open the door to a wide range of new threats and attack vectors, which in-turns have enabled new opportunities for the adversaries to remotely carry out sophisticated cyber attacks. *Attack vector* is defined as a way a hacker triggers system's latent vulnerabilities to gain access to the system and its resources. According to the Global Cybersecurity report [3], the most common cyber attack vectors used against vehicles by hackers between 2010 and 2020 are:

- Servers - 32%
- Keyless Entry/Key Fob - 26%
- Mobile Application - 9%
- On-board Diagnostics Port - 8%
- Infotainment - 7%
- Electronic Control Unit (ECU) - 4%
- In-vehicle Network - 3%

The presented cyber attack vector distribution shows that server-based attacks have been the most effective method used by hackers. As they can be launched remotely with minimal infrastructure and effort, therefore they are harder to detect and stop. Fig. 2 shows a timeline of headline grabbing cyber attacks launched between 2015 and 2020.

The first public evidence of such remote cyber attack was reported in July 2015, when two hackers have managed to penetrate the Jeep Cherokee entertainment system and remotely control the vehicle dynamics and braking system [8]. Fiat Chrysler had recalled 1.4 million vehicles to fix this vulnerability by upgrading the firmware [9]. A group of German researchers have eavesdrop the keyless fob radio communication and demonstrated a replay attack gaining access to the vehicle in March 2016. This attack vector has affected 24 different vehicle manufacturing brands including Audi, BMW,

Ford and Toyota [10]. In 2017, researchers from Keen Security Lab were successful to install malware and remotely control Tesla Model S braking, side mirrors and locking system [11]. Besides, a team of ethical hackers conducted an in-depth hardware/software analysis of in-vehicle infotainment, telematics control unit and central gateway module of multiple BMW vehicles, and found 14 vulnerabilities with local and remote access vectors [12].

The transition from a connected to an autonomous vehicle has expanded the automotive system attack surface by targeting data-driven AI and ML methods. Tesla's autopilot uses a camera to detect lane markings to position the vehicle in the middle of the road and to automatically change lanes when required. In April 2019, Keen Security Labs researchers managed to trick the ML-based autopilot system of the Tesla Model S and made vehicle change lanes [13]. The hackers were managed to adversely manipulate the active cruise control system by subtly altering the speed limit sign. In response, the vehicle accelerated up to 50 mph in a 30 mph zone [14].

It is evident that reported cyber attacks have impacted every segment of a connected vehicle and rapidly extending towards autonomous vehicle. There is a crucial need for cybersecurity hardening of automotive system design and engineering processes making them cyber resilient. Since automotive software plays a crucial role integrating value-added services from different automotive vendors, Section III discusses AUTOSAR and its cybersecurity related features.

## III. AUTOMOTIVE OPEN SYSTEM ARCHITECTURE (AUTOSAR) & CYBERSECURITY

AUTOSAR is an initiative [15] that standardise software architecture of automotive ECUs by increasing reuse and ex-changeability of software modules between vehicle manufacturers and suppliers. The concept is to separate the hardware-independent application software from the hardware-dependent software (memory drivers, crypto drivers, communication drivers etc.) by employing a run time software abstraction [16]. It avoids compatibility issues and re-development of similar automotive software components. The following are two standard AUTOSAR architectures as shown in Fig 3.

### A. AUTOSAR Classic

The AUTOSAR Classic architecture is designed for deterministic, hard real-time, safety-critical vehicle services such as



Fig. 2. Timeline of major threats discovered and attacks launched between 2015 and 2020. These threats and attacks have severely impacted the automotive industry and developed an appetite for automotive cybersecurity.

airbags, braking, steering, acceleration etc. which are generally implemented on an embedded micro-controller and real time processor architectures (e.g. Arm Cortex-M and Cortex-R). In AUTOSAR Classic, the run time software abstraction layer is known as *AUTOSAR Run time Environment (RTE)* [17] as shown in Fig. 3. However, to ensure the stringent timing requirements of safety-critical services, the automotive applications have to be statically defined, configured for each ECU and integrated into the automotive system. This well-defined static configuration of services has become a major limitation for vehicle manufacturers to effectively manage the life cycle of the vehicle [16]. Fiat Chrysler recalled 1.4 million vehicles to fix the cybersecurity vulnerability that exploited to kill the Jeep on the highway [9]. Volkswagen recalled more than 150,000 Audi cars due to passenger side airbag activation concerns [18]. Daimler recalled 2.6 million Mercedes vehicle in China for software communication failure [19]. Therefore, the static configuration and lack of life cycle management approach to automotive systems have caused serious threats to the cybersecurity and functional safety of the vehicle and brought severely financial damage to vehicle manufacturers. Nonetheless, the distributed E/E automotive architecture composed of hundreds of ECUs executing static software severely limits the system life cycle management opportunities. The application requirements promised by autonomous vehicles demand a high performance, centralised and adaptable automotive software architecture to harden cybersecurity.

### B. AUTOSAR Adaptive

For adaptable and high performance automotive system architecture, a service-oriented *AUTOSAR Adaptive* architecture [20] was introduced in 2017. This architecture is designed to meet the diverse computation and mix-critical cybersecurity and functional safety requirements of connected

and autonomous vehicles as illustrated in Fig. 3. It has a support for compute-intensive AI and ML inference task and to deliver soft real-time automotive services (over-the-air firmware update, smart services, customised infotainment, remote feature and life cycle management etc.) running on heterogeneous multi core processor architectures e.g (Arm Cortex-A, GPU, FPGA etc.). This software architecture supports dynamic communication, high-speed data processing and adaptable system cybersecurity and functional safety capabilities. Due to technological evolution, there is a major shift in automotive system architectures moving from distributed application-specific ECUs to a few centralised high-performance domain controllers that can provide bundled services [16]. It provides optimal foundations for autonomous driving systems, as they require data-intensive computing, flexible communication, handling of mix-critical data services and on-demand update and infotainment services. The adoption of hypervisor technology in the automotive software architecture, enable system-level capability to isolate and partition mix-critical system services which can be leveraged to enhance

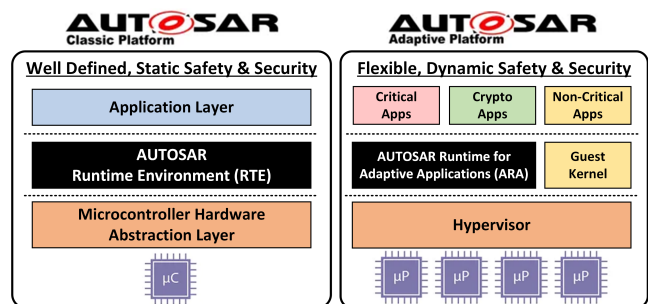


Fig. 3. Run time software abstractions supported by AUTOSAR Classic and Adaptive Platform [17], [20]

TABLE I  
 AVAILABILITY OF SECURITY MODULES SUPPORTED BY AUTOSAR CLASSIC AND ADAPTIVE [21]

AUTOSAR	Crypto Stack	SecOC	TLS	IPSec	Secure Diagnostics	Identity & Access Management
Classic (v4.4)	✓	✓	✓	✗	✓	✗
Adaptive (R19-03)	✓	✗	✓	✓	✗	✓

cybersecurity and functional safety of the system as shown in Fig. 3. Furthermore, hypervisor technology enables independent development of automotive services by different vendors which can be configured at run time.

### C. Security modules supported by AUTOSAR

AUTOSAR Classic and AUTOSAR Adaptive standards supports security modules based on the the principle of *confidentiality*, *integrity* and *authentication*. These security modules ensure that the information is transmitted from the source to the destination node unchanged, and only authorised receiving nodes have access to this information [16]. It includes:

- **Crypto Stack** - allows access to cryptographic primitives such as keys/certificates required to provide confidentiality. The access to these cryptographic primitives is only through the provided interfaces which are independent of their respective crypto implementations making them portable to different ECUs.
- **Secure communication** - ensures the security of data in motion both inside and outside of the vehicle. AUTOSAR supports several secure communication protocols including Secure CAN communication SecOC, TLS, IPSec as automotive Ethernet is becoming increasingly important.
- **Identity & Access Management** - ensures that only authorised applications can access certain automotive system resources. These access rights can be dynamically configured and updated remotely.
- **Secure Diagnostics** - allows to record critical events (unauthorised access, error etc.) occurred in the vehicle network and ensure authorised access to this data. This valuable information allows to investigate, evaluate and diagnose the causes of events (failure/malfunction etc.)

Table I lists the availability of these security modules in both standards which is directly dependent on their architectural differences, computing resources and the underlying computing technologies. However, the availability of these security modules is one part of the automotive cybersecurity puzzle. Another critical part is the adaptation and deployment of security modules to architect system defences [22]. This requires a holistic risk-oriented automotive *cybersecurity engineering* which is discussed in Section IV [5], [21].

## IV. AUTOMOTIVE CYBERSECURITY STANDARD

Historically the purpose of a vehicle is to provide mobility, therefore the main focus of vehicle manufacturers was limited to the functional safety of the vehicle, its passengers and pedestrians. But with the introduction of autonomous driving, the consolidation of mix-critical data and connected services has widened the attack surface as well as the likelihood

of vehicles being exposed to cyber attacks [5], [6], [7]. The field of automotive cybersecurity is new to automotive system designers and engineers, as it is continuously evolving with the discovery of new attack vectors and vulnerabilities as discussed in Section II. Therefore, the well established automotive functional safety standard (ISO 26262) alone is insufficient to provide guidance and enclose cybersecurity related challenges. Initially, vehicle manufacturers and suppliers had adopted an individual bolt-on approach to tackle these cybersecurity challenges. But soon, they realised the efficacy of joint effort and urgent need for establishing guidelines and standard due to the increasing growth of cyber attacks, prevalence and their level of sophistication [24].

In 2016, the Society of Automotive Engineers (SAE) came together and released SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems). This guidebook establishes a set of high-level overview and guiding principles for cybersecurity of cyber-physical vehicle systems. Later the evolved version of this guidebook has been translated into the first draft of ISO/SAE 21434 (Road vehicle - Cybersecurity Engineering) standard in 2020 [25]. In contrast to SAE J3061, ISO/SAE 21434 provide actionable steps/requirements to manage cybersecurity processes and comply with these requirements. The following are the key objectives:

- Establish standardised cyber-related terminologies that shall be used across the automotive industry. As they are fundamental in understanding and evaluating cyber-risks.
- Create an effective automotive cybersecurity framework to manage each stage of the vehicle life cycle which can be tailored for vehicle manufacturers and suppliers etc.
- Define assurance levels that provide guidance outlining the automotive cybersecurity requirements. These requirements shall be met to maintain cyber resilience of the vehicle during the whole life cycle.

ISO/SAE 21434 standard provides a cybersecurity baseline for vehicle manufacturers and suppliers to effectively manage cybersecurity risks. It specifies the cybersecurity requirements for road vehicle E/E systems, including their components and interfaces during the entire vehicle life-cycle from concept, development, production, operation, maintenance, and decommissioning [24]. Chapter 15 of ISO/SAE 21434 standard proposes a *Threat Analysis and Risk Assessment* (TARA) process as a holistic automotive cybersecurity engineering approach to harness and harden cybersecurity of the vehicle as shown in Fig. 4. This allows system security architect to determine and quantify the risks and their potential damage tailored for each automotive application use case. This process involves identification of the system's assets, threat and damage scenarios, feasibility to launch attacks by exploiting each

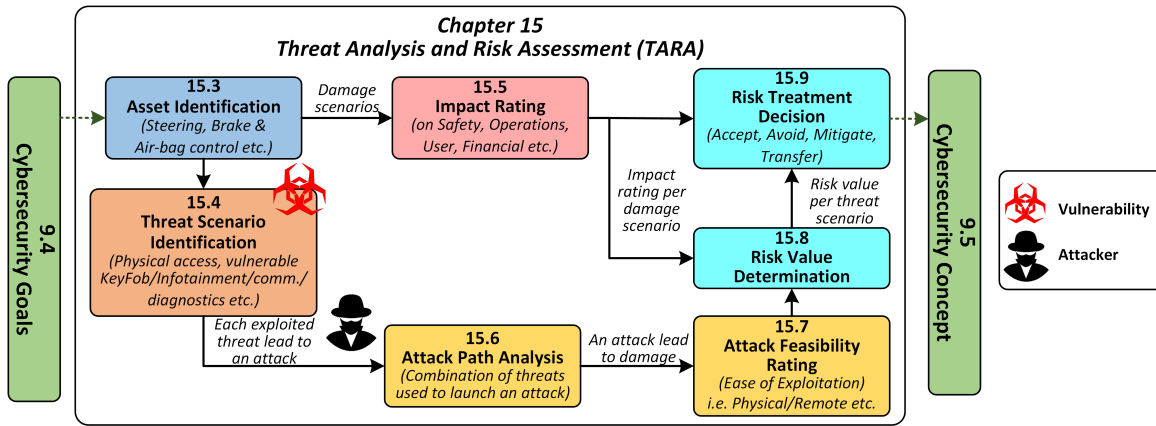


Fig. 4. Block diagram of Threat and Risk Assessment (TARA) process defined in ISO/SAE 21434 (Chapter 15) [23].

threat scenario and impact rating of each damage scenario as shown in Fig. 4. The outcome of this process is the risk value per threat scenario which allow security architects to evaluate and determine an appropriate risk treatment decision whether to accept, avoid, mitigate or transfer each risk.

ISO/SAE 21434 defines *Cybersecurity Assurance Level* (CAL) as an attribute associated with a system, a component, or a specific cybersecurity goal [26]. There are four levels, where CAL4 being most demanding and CAL1 being least stringent. These levels enable security architects to tailor baseline cybersecurity activities to target assurance level and utilise them to define justifiable cybersecurity goals that are measurable against technical merit. However, the standard or these levels do not provide any technical cybersecurity requirement or specification. In the context of autonomous vehicles, there is no functional safety without cybersecurity. Therefore the CAL levels defined in ISO/SAE 21434 complements the *Automotive Safety Integrity Level* (ASIL) of ISO 26262 (*Road Vehicles - Functional Safety*) standard.

## V. AUTOMOTIVE CYBERSECURITY CHALLENGES

The development of autonomous system is a complex process that brings together multiple technologies including sensing, computer vision, machine learning and control systems. Since AI/ML being the enabling technology, it is essential to focus on its cybersecurity challenges [7] and highlight the shortcomings in the existing automotive ecosystem to better understand the future research directions.

### A. Challenges in adopting AI and ML computing

Current AI and ML systems are achieving tremendous performances in a wide range of conditions. But their capacity to generalise is limited due to the complexity and diversity of the world. One major unsolved challenge for ML systems is the right handling of corner cases, where an unknown situation encountered outside of the training data set. It is challenging to guarantee that an ML system will output the right results in unusual conditions, leading to hazardous situations. For instance, ignoring a stop sign partially covered by snow, or

stopping in front of a bush slightly over-hanging the side of the road. Such cases has been exploited by the Keen Security Lab on Tesla Model S autopilot [13] and MobileEye EyeQ3 [14].

Generally AI and ML vulnerabilities are classified as *intentional* and *unintentional* adversarial threats. Intentional threats are the malevolent exploitation of the limitations and vulnerabilities present in AI and ML methods to cause intended offence and harm. The *Data Evasion* and *Data Poisoning* are the most prominent type of adversarial ML attacks [27]. Unintentional threats are the side effects of benevolent usages, due to open issues inherent in the trustworthiness, robustness, limitations and functional safety of current AI and ML methods. The following are some of the major adversarial threats relevant for autonomous driving system [2], [5]:

- Sensors are the primary source of information for the AI/ML based system. An attacker can exploit sensor jamming, spoofing, blinding/saturation sensors to manipulate the AI/ML model by feeding malicious data or intentionally providing scarce data.
- Communication interfaces between system components of autonomous driving pipeline are critical. Disrupting such communication interfaces by launching a DoS/DDOS can impact availability of critical operations.
- Adversarial manipulation of vehicle communications, road infrastructure and transmitted sensor data (man-in-middle) can force the processing stage to falsely interpret the scene, incorrectly plan and take malicious decisions.

Nonetheless, AI/ML models are supposed to learn and change their behaviour over a period of time. Therefore, the cybersecurity risk assessment shall be systematically monitored and maintained during the life-cycle of the AI model.

### B. Shortcomings in existing Automotive Ecosystem

- Mass integration of legacy off-the-shelf system components and protocols into modern vehicles without assessing their cybersecurity and functional safety risks.
- A lack of cybersecurity ownership, where third-party components are used among vehicle manufacturers, original equipment manufacturers and service providers.

- Scarcity of cybersecurity-aware automotive design practises and absence of baseline cybersecurity requirements.
- The large scale integration of third-party software components not designed for safety-critical systems. They open doors to diverse latent vulnerabilities that manifest within different layers of software and hardware stack.
- A lack of centralised system-level visibility and defences in automotive architectures, essential for building a holistic run time system context and monitoring controls.
- Absence of secure-by-design approach and proactive system-level defences that can protect, detect, respond and recover automotive systems against cyber attacks.

## VI. CONCLUSION & FUTURE DIRECTION

The benefits of autonomous vehicle technologies are promising as they can help reduce risky and dangerous driver behaviours, reduce the number of crashes on our roads and reduce traffic congestion. However, on the other side of the spectrum, weaponizing this autonomous driving technology could have catastrophic consequences to safety and security of the society. There is an urgent need for defining a holistic risk-based automotive cybersecurity engineering processes which shall be inline with the core cybersecurity principles of standards, frameworks and best practices, while leveraging the domain-specific expertise of cybersecurity experts. These well-defined cybersecurity engineering processes then shall be integrated/mapped onto the existing model-based embedded software development processes, enabling means to guarantee both functional and non-functional properties by construction. These process will also provide necessary foundations to systematically architect a multi-layered system cybersecurity architecture, by deploying various defences, making it resilient against latent vulnerabilities and cyber attacks. However, mitigating sophisticated attacks is a challenging undertaking and analogous to shooting bulls-eye on a multidimensional fast-moving target. There is no single silver bullet to mitigate or address these diverse automotive cybersecurity challenges. The aim of this paper is to provide meaningful insights for system designers and security architects to better understand the risks in designing automotive cybersecurity solutions.

## ACKNOWLEDGEMENT

This research work was funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant 957210 (XANDAR).

## REFERENCES

- [1] R. Coppola and M. Morisio, "Connected Car: Technologies, Issues, Future Trends," *ACM Comput. Surv.*, no. 3, pp. 46:1–46:36, 2016.
- [2] A. Koesdwiady and R. Soua and F. Karray, "Improving Traffic Flow Prediction With Weather Information in Connected Cars: A Deep Learning Approach," *IEEE Trans. Veh. Technol.*, no. 12, pp. 9508–9517, 2016.
- [3] (2021) Upstream Security's 2021 Global Automotive Cybersecurity Report. [Online]. Available: <https://upstream.auto/2021report/>
- [4] (2021) UK on the cusp of a transport revolution, as self-driving vehicles set to be worth nearly £42 billion by 2035. [Online]. Available: <https://www.gov.uk/government/news/uk-on-the-cusp-of-a-transport-revolution-as-self-driving-vehicles-set-to-be-worth-nearly-42-billion-by-2035>
- [5] K. Kim *et al.*, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, p. 102150, 2021.
- [6] Z. El-Rewini *et al.*, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
- [7] Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A. and Sanchez Martin. (2021) Cybersecurity challenges in the uptake of Artificial Intelligence in Autonomous Driving.
- [8] (2015) Hackers remotely kill a Jeep on the Highway - with me in it. [Online]. Available: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- [9] (2015) After Jeep Hack, Chrysler Recalls 1.4M Vehicle for Bug Fix. [Online]. Available: <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>
- [10] (2016) Hackers Are Stealing Keyless Entry Cars with a \$200 Device. [Online]. Available: <https://www.techlicious.com/blog/hackers-keyless-entry-car-radio-tools/>
- [11] (2017) Keen Lab hackers managed to take control of Tesla vehicles again. [Online]. Available: <https://electrek.co/2017/07/28/tesla-hack-keen-lab/>
- [12] (2018) New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars . [Online]. Available: <https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/>
- [13] (2019) Tesla's autopilot tricked into driving on the wrong side of the road. [Online]. Available: <https://www.newscientist.com/article/2198325-teslas-autopilot-tricked-into-driving-on-the-wrong-side-of-the-road/>
- [14] (2020) Hackers can trick a Tesla into accelerating by 50 miles per hour. [Online]. Available: <https://www.technologyreview.com/2020/02/19/868188/hackers-can-trick-a-tesla-into-accelerating-by-50-miles-per-hour/>
- [15] AUTOSAR Enabling Continuous Innovation. [Online]. Available: <https://www.autosar.org/>
- [16] V. Bandur *et al.*, "Making the Case for Centralized Automotive E/E Architectures," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1230–1245, 2021.
- [17] AUTOSAR Classic Platform. [Online]. Available: <https://www.autosar.org/standards/classic-platform/>
- [18] (2021) Volkswagen recalls Audi A3s on passenger air bag concerns. [Online]. Available: <https://eu.usatoday.com/story/money/2021/03/27/vehicle-recall-check-volkswagen-recalls-audi-a-3-s-air-bag-concerns/7028190002/>
- [19] (2021) Daimler will recall 2.6M Mercedes cars in China. [Online]. Available: <https://europe.autonews.com/automakers/daimler-will-recall-26m-mercedes-cars-china>
- [20] AUTOSAR Adaptive Platform. [Online]. Available: <https://www.autosar.org/standards/adaptive-platform/>
- [21] (2020) AUTOSAR Security: Adaptive platform must focus on holistic vehicle protection. [Online]. Available: [https://www.etas.com/download-center/files/DLC\\_realtimes/RT\\_2019\\_2020\\_en\\_54\\_rgb\\_ESCRYPT.pdf](https://www.etas.com/download-center/files/DLC_realtimes/RT_2019_2020_en_54_rgb_ESCRYPT.pdf)
- [22] M. Hagan, F. Siddiqui, and S. Sezer, "Enhancing Security and Privacy of Next-Generation Edge Computing Technologies," in *Proc. 17th International Conference on Privacy, Security and Trust (PST)*, Canada, 2019, pp. 1–5.
- [23] (2020) ISO/SAE FDIS 21434 Road vehicles — Cybersecurity engineering. [Online]. Available: <https://www.iso.org/standard/70918.html>
- [24] Christoph Schmittner and Georg Macher, "Automotive Cybersecurity Standards - Relation and Overview," in *Computer Safety, Reliability, and Security - SAFECOMP 2019 Workshops, Proceedings*, Italy, 2019, pp. 153–165.
- [25] (2020) ISO/SAE 21434: Setting the Standard for Automotive Cybersecurity. [Online]. Available: <https://upstream.auto/blog/setting-the-standard-for-automotive-cybersecurity/>
- [26] Macher, Georg and Schmittner, Christoph and Veledar, Omar and Brenner, Eugen, "ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell," in *Computer Safety, Reliability, and Security. SAFECOMP Workshops*, Germany, 2020, pp. 123–135.
- [27] M. Goldblum *et al.*, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," *CoRR*, vol. abs/2012.10544, 2020. [Online]. Available: <https://arxiv.org/abs/2012.10544>