Challenges and current solutions for safe and secure connected vehicles

Dr. Simone Böttger, Dr. Alexander Mattausch, Simon Dürr
Elektrobit Automotive GmbH
Erlangen, Germany

July 12, 2018

Digitalization reshaped our everyday life in the past twenty years and the automotive industry is also part of this change. Today's vehicles are increasingly *smart* and connected providing additional safety and convenience features (autonomous emergency braking, adaptive cruise control). Next generation vehicles will be highly automated and autonomous up to level 5 (driverless), which will fundamentally change the meaning of driving. At the same time, all these benefits require more powerful control units and a greater flexibility in electronic control unit (ECU) software, which inevitably calls for a redesign of the E/E architecture inside the vehicle.

While safety was always considered as a critical engineering concern in the automotive industry, security became a significant challenge when vehicles began turning into rolling computers. Due to the fatal nature of vehicles, autonomously driving and connected vehicles need to be highly reliable in safety and security to gain full acceptance, much more than other devices in the Internet of Things. Consequently, safety and security are key concepts in the system architecture of future vehicles.

This paper will give an overview of the current challenges and solutions regarding safety and security within the vehicle's E/E architecture.

1 Introduction

There are two major technologies emerging, which will fundamentally change what driving means: autonomous driving and connectivity.

Autonomous driving is aiming to reduce the input from human operators to the point of no driver but travelers only. New features of automated driving and advanced driver assistance systems that are already in use (adaptive cruise control, intelligent parking assistant, lane warning systems, autonomous emergency braking etc.) are paving the way for autonomously driving vehicles. These features make use of connectivity to gain the required external information from the infrastructure. In the future, vehicle-to-everything (V2X) technologies will include much more elements of the near and remote environment (road signs, traffic lights, other vehicles, cloud etc.) to wirelessly establish the necessary exchange of information. More vehicles will leverage V2X to ease congestion, avoid accidents, or reduce emissions.

Connectivity also enables OEMs to efficiently manage the software during the whole life cycle of the vehicle. As the complexity of software architectures and the variety of applications increase, feature upgrades, urgent bug-fixes, or security patches will become necessary on a frequency that cannot be realized by recalling vehicles to the dealer's shop when needed. For this reason, over the air (OTA) update technologies are essential for the next step toward high-level autonomous driving.

Along with the transformation of the vehicle toward a computerized system on wheels with connections to the internet and other external networks, the driving experience of the end-user will change. Passengers already have the option to connect devices like smartphone or tablet to the vehicle and use apps that are running on them via the In-Vehicle-Infotainment system. New business concepts like pay-by-use models will appear, where the customer pays for certain features on demand (air conditioning, seat heating, navigation, 3D bass). Same with the whole vehicle, people do not need to own a car but can make use of car sharing models and choose the equipment of the vehicle as desired for the current purpose.

2 E/E architecture

The current E/E architecture is based on trusted functional domain controllers for e.g. chassis, body, or powertrain. To master the upcoming E/E system complexity and the demand for more computational power and a fast data transmission channel, there shall be a small number of high-performance controllers interconnected via automotive Ethernet. These central computing platforms run on multi-core processors that monitor and control a number of less intelligent, yet highly specialized ECUs. The future architecture of a vehicle infrastructure is envi-

sioned as a service-oriented architecture with multi-layer services. The current numerous ECUs will be split into low-performance I/O controllers and high-performance domain controllers, which are dynamic systems that provide update capabilities as well as safety and security features.

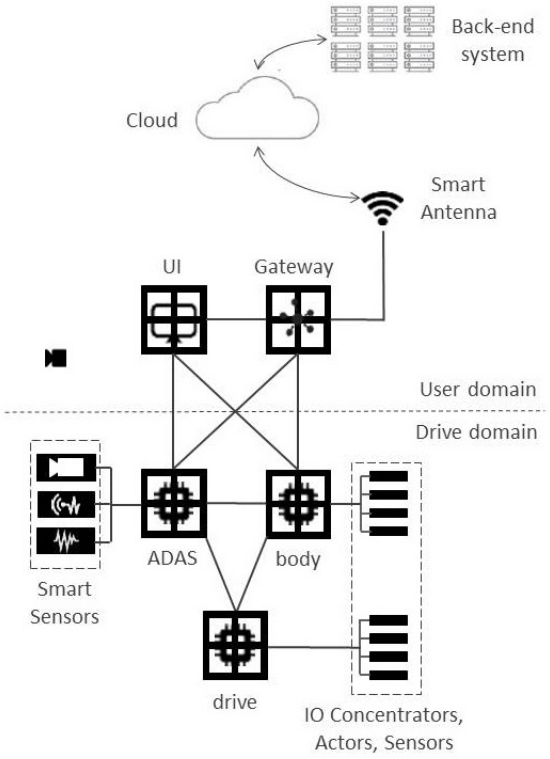

Figure 1: Centralized architecture

This influences the software architecture because the centralized performance ECUs require a consolidated platform that hosts the heterogeneous functionalities of automotive control and infotainment.

In response, the AUTOSAR consortium currently develops a new software platform, the adaptive platform (AP), which complements the widely-used classical platform (CP). The combination of both platforms shall guarantee the requirements on performance as well as safety and security of the E/E architecture of next generation technologies. For instance, one of the main features of the AP is the ability to update individual functions on the ECU retroactively and during run-time.

The AP is based on the POSIX operating system, which can run on a multi-core processor or on a hypervisor to realize virtualization. While a multi-core controller provides a safe and secure separation of performance partitions, virtualization provides a safe and secure separation of software partitions (Figure **??**).

3 Functional safety

These trends initiated a paradigm shift in automotive safety concepts. In case of a detected failure, the standard approach in many safety relevant systems is fail-silent; that is, the safe state is usually the deactivation of the function. For autonomous driving and the electrification of main vehicle functions, x-by-wire technologies are introduced, replacing mechanical or hydraulic backup systems. These technologies require fail-operational behavior, which means that the function is (partially) maintained for a certain period of time after failure and then deactivated or resumed without service interruption. Developing a fail-operational architecture for each x-by-wire system is essential to facilitate reliability and safety. Multiple redundancy, as in avionic systems, cannot simply be adopted to automotive platforms because of the resulting higher hardware costs, weight and energy consumption. A slightly different approach, which provides fail-operational behavior between ECUs with manageable costs, is the so-called 1-out-of-2 diagnostic (1oo2D) system architecture (e.g. [8]). In case of a fault, the function is dynamically reallocated to another ECU, which temporarily continues the function until the vehicle can be safely halted. For this, both ECUs need to be equipped with strong diagnostic capabilities and additional monitoring elements.

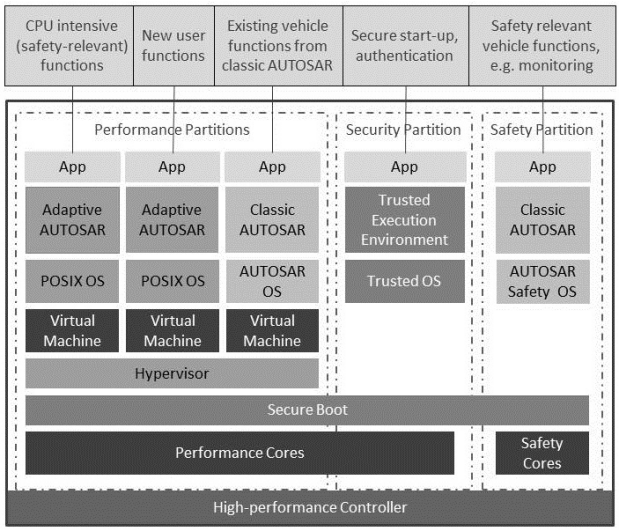

Figure 2: Software architecture of a high-performance controller

4 Connectivity and security

With all the unprecedented possibilities and opportunities that come with digitalization and connectivity, new challenges concerning security issues arise. As the number of advanced functionalities, electronic components, processing intensity, and connection points of a vehicle increase, the amount of assets gets larger, extending the attack surface to a new dimension. A vehicle compromised through vulnerability in the system may lead to operational, privacy, financial, or safety loss.

In the past, the vehicle was a closed system and threats that require (prior) physical access to the in-

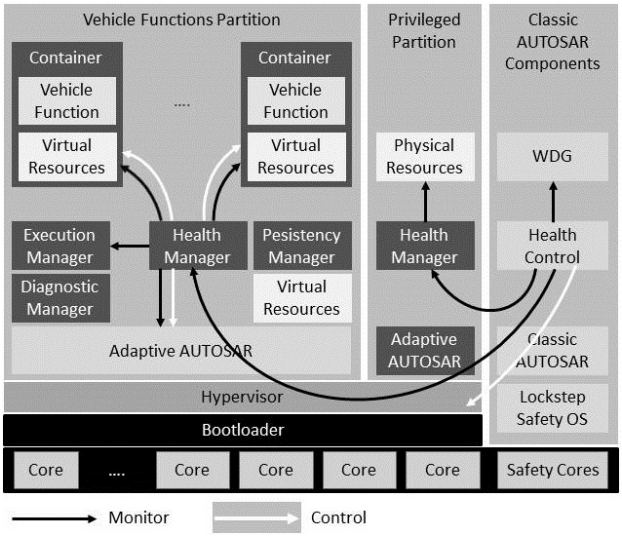

Figure 3: AUTOSAR's distributed health management

vehicle network had been excluded from the security concept. Since wireless connections expose the vehicle to external attacks, the automotive industry is facing unconsidered threat models. In case of the attack on the Chevrolet Impala of General Motors in 2010, it took years to fix the vulnerabilities and implement countermeasures ([9]). Since then, many successful attacks have shown that, like every device connected to the Internet, a vehicle with wireless connections is vulnerable to remote attacks ([1], [2], [6]).

The most prominent attack that finally raised everyone's attention to the importance of security in the automotive industry, was the attack on the Jeep Cherokee in 2015 ([5]). Two security researchers remotely gained access to the Jeep via the diagnostic bus port of the entertainment system and took control over vehicle functions including steering and brakes. Less significant threats to personal safety may cause financial problems or reputational damage to the OEMs, when the whole fleet of a popular model is affected via OTA mechanisms.

How to avoid such attacks? First of all, one has to accept that there is no such thing as a 100% secure system. Instead, one has to check the system for vulnerabilities on a continuous basis, try to think like an attacker, learn about new threat models, and adjust the system's security as needed. The latter makes OTA software updates a must-have technology for connected vehicles.

Hidden vulnerabilities are unavoidable and might be found by a black-hat hacker first. In this case, the goal is slowing down or stopping the attacker on the path to the most critical assets. For this, many challenging obstacles need to be implemented by means of security mechanisms in every layer (Figure 4). This is a well-established strategy in military, known as defense in depth. By causing delays for the attacker, additional intrusion or anomaly detection mechanisms enable applying several defense modes, e.g. reconfiguration (request change of session key), and enhance the chances of stopping the attacker before doing any serious damage.

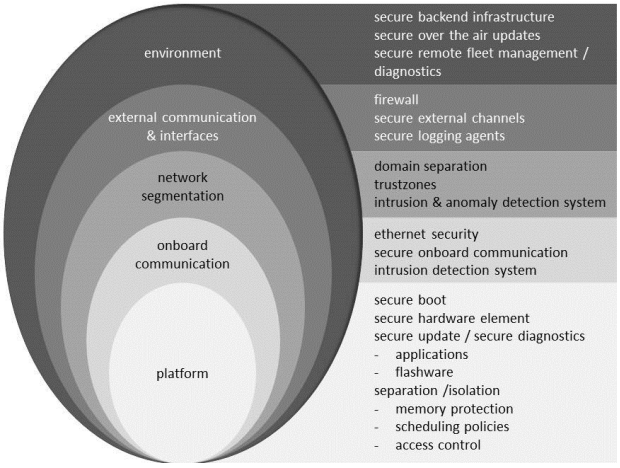

Figure 4: Layered security

In fact, in almost every example where attackers took control of vehicle functions, they were only able to do so because they found not a single vulnerability but a chain of vulnerabilities on their way to these critical functions.

5 Standardized development process

As shown in the last section, security issues have an impact on safety, when security mechanisms fail to ensure the integrity of safety functions. On the other hand, safety mechanisms like consistent monitoring and reporting is a key requirement for good, layered security. Functional safety and security are not independent from each other and need to be synchronized in processes and development like in other domains.

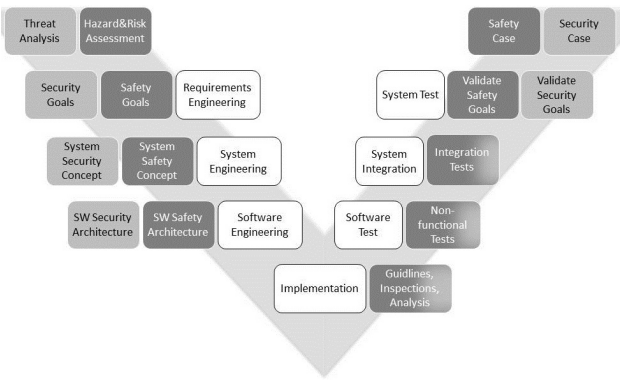

Figure 5: Combined safety and security process model for systems engineering

The ISO 26262 standard ([3]) covers the aspects of functional safety in system development on process level as well as on method level. An equivalent security standard does not exist yet. The guidebook for the development of security relevant systems SAE J3061 ([7]) describes processes and methods similar to the life cycle of ISO 26262 but is not a standard. In 2019, this gap shall be filled by the standard ISO/SAE 21434. It shall specify the requirements for cyber security risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design, development), production, operation, maintenance, and decommissioning.

Acknowledgment

This work was supported by the Federal Ministry for Economic Affairs and Energy (BMWi) under Grant 01MD16002G.

References

[1] c't magazine for computer techniques: Beemer, Open Thyself! Security vulnerabilities in BMW's ConnectedDrive, http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html, 2015.

[2] Troy Hunt: *Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs*, https://www.troyhunt.com/controlling-vehicle-features-of-nissan/, 2016.

[3] ISO 26262: *Road vehicles - Functional safety.*

[4] ISO/SAE 21434: *Road vehicles - Cybersecurity engineering.*

[5] Charlie Miller, Chris Valasek: *Remote exploitation of an unaltered passenger vehicle*, http://illmatics.com/Remote\%20Car\%20Hacking.pdf, 2015.

[6] Sen Nie, Ling Lu, Yuefeng Du: *Free-fall: hacking Tesla from wireless to CAN bus*, https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf,

[7] SAE J3061: *Cybersecurity guidebook for cyber-physical vehicle systems*, 2016.

[8] Philipp Schleiss, Christian Drabek, Gereon Weiss, Bernahrd Bauer: *Generic Management of Availability in Fail-Operational Automotive Systems*, SAFECOMP 2017: Computer Safety, Reliability, and Security, 2017

[9] WIRED magazine: *GM took 5 years to fix a full-takeover hack in millions of onstar cars*, https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/, 2016