Current Trends and Solutions in Securing Automotive Software

Alexander Much, Rudolf Grave, Robert Leibinger, Martin Böhner, Elisabeth Waitz
Elektrobit Automotive GmbH
Erlangen, Germany
info.automotive@elektrobit.com

***Abstract*—this paper gives a short overview on the current trends and solutions in regarding security within automotive software.**

***Keywords*—security; automotive; software architecture;**

I. Introduction

The requirements regarding software development in the automotive industry are changing continuously, as the software alteration rate in a modern car is increasing together with the amount of functionality. Nowadays premium-segment vehicles contain more than 100 electronic control units (ECUs) which communicate with each other and the outside world. In parallel the complexity of the software increases and there are assumed to be more than 100 million lines of code per vehicle. High quality is the foundation of automotive software development and process models like Automotive SPICE are widely established.

II. Standardisation

Software architectures aim to resolve the functional and non-functional requirements and to control complexity. There is a standardized software architecture defined by AUTOSAR (Automotive Open System Architecture) which enables a common understanding and interchangeability between OEMs and their suppliers. AUTOSAR defines not only functional requirements to the software but also data formats for the description of applications, interfaces, etc. This common understanding enabled various cooperation models between OEMs and an ecosystem of suppliers. Improvements in collaboration have increased the reusability of software components and improved the overall software quality.

III. Autonomous Driving and Functional Safety

Another trend in the automotive industry, which already started years ago and is evolving more and more, is software functionality which takes action on vehicle dynamics: active interference on the brake systems (e.g. ABS, ESP) and steering (e.g. EPS) but also on safety functionalities like airbags and autonomous emergency breaking (e.g. AEB). Assisted driving functionalities like lane assist or Adaptive Cruise Control (ACC) are already established and evolving towards autonomous driving. Such systems are safety relevant, because a faulty activation or an outage of the system can have fatal impact.

With introduction of safety standards like ISO 26262, the automotive software industry aims to cover the aspects of functional safety in system development on process level as well as on method level. Aspects like functional safety have essential influence on software architectures and are partly resolved by standardization. Fundamental integrity mechanisms, like system monitoring, partitioning and time and process monitoring, or protected communication are available and implemented in production (see Fig. 1). But many aspects of functional safety are system or project specific and therefore need to be regarded and resolved individually.

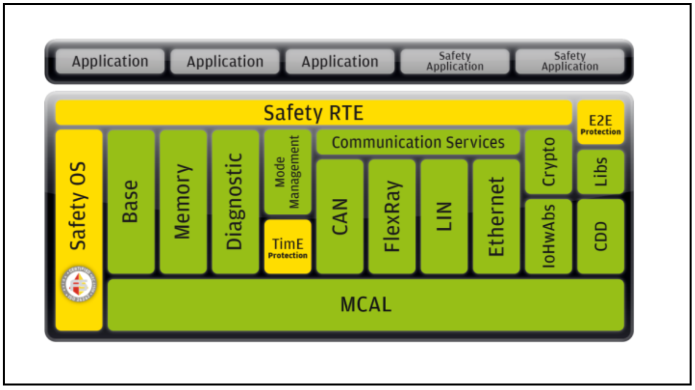

Fig. 1 AUTOSAR architecture extended by some standard components for functional safety

IV. Performance Controllers

Not only the amount of functionality, but also the processing intensity in the vehicle increases which requires a remarkable increase on computational power inside the car.

Analogues to common computer systems, this trend leads to a transformation from single processors to multicore systems. This influences the software architectures, because existing automotive systems are usually developed and optimized for single core processors and can hardly utilize additional computing power sufficiently. Furthermore, multicore systems enable a consolidation of the number of ECUs within a vehicle, which leads to an economy of energy and weight. These systems take over several functionalities of a domain, like e.g. chassis or interior, and are therefore called domain controllers. These controllers are usually safety relevant, because a single safety relevant function turns the overall system into safety relevance.

The most vehicle systems are traditionally fail-silent. The safe state is mostly the deactivation of the function.

Especially regarding driver assistance, the number of functionalities, for which a deactivation is classified as safety relevant, increases continuously. Although there is a gradual transition from the established driver assistance functions via partial automated driving to fully automated driving (refer to [3]), this trend requires the development of fail-operational systems: the safe state is not the (complete) deactivation of the system. This aspect of reliability of systems means new challenges for the system as well as for the software development and the resulting software architectures.

V. Connected Car and Cyber Security

Another important trend is the "connected car". Many OEMs provide online services to their customers, vehicle diagnostics can be performed "over the air", and traffic information or navigation maps are updated online. The vehicle cannot be assumed a closed system anymore. The connection and interaction with the cloud, enables new possibilities regarding performance and functionality, but also holds risks. Extremely expensive calculations which could not be realized inside the car due to limitations on performance and capacity can be outsourced from the vehicle to the cloud. Also a flexible mechanism is supposable, which allows the car to decide during runtime, whether a calculation can be performed inside the car's ECUs or due to a high processor load shall be executed by an online device. This outsourcing can support or even enable trends like autonomous driving.

Not only calculations can be outsourced, but foremost the collection and evaluation of data is increasing tremendously due to the connected car. Traffic data and environmental information can be evaluated to improve and ensure safety. But also personal data, e.g. related to the driving behavior, are of interest.

Independent of the use case, the basic rule holds that "whatever is connected is attacked by hackers". This increases importance of the system aspects "security" and "privacy". First successful attacks to vehicle systems via the internet are published and have caused a wide public attention to the topic. Cyber security aspects are not new to automotive software and systems like immobilizer, secure keys or secure odometer storage are state of the art.

VI. Development Process

In 2016, SAE published a guideline for development of security relevant systems (SAE J3061, „Cybersecurity Guidebook for Cyber-Physical Systems"). The guideline describes processes and methods and is derived from the life cycle of ISO 26262. The document is not a standard, like e.g. the ISO 26262, but it summarizes essential efforts like research programs or existing standards and publications. Therefore, it is a valuable contribution and can represent an entry point for the introduction of processes and methods.

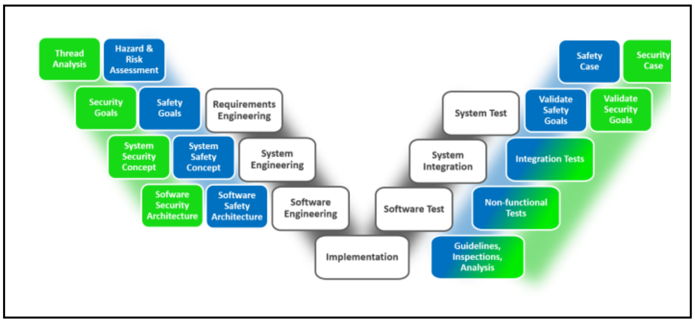

Fig. 2 Combined process model for system development

Functional safety and cyber security are mostly regarded independent from each other. Also the according organizational responsibilities are distributed inside of companies. But the todays systems need to realize both aspects and require the coordination of processes and development. From the point of "systems engineering" both aspects, functional safety and cyber security, are regarded as "specialty engineering". Other industries, like e.g. aircraft industry or railway technology, have already established this point of view.

The risk analysis can represent an example for the interaction of the two worlds. Functional safety defines a "hazard and risk analysis" (HARA) and the cyber security defines a "threat and risk analysis" (TARA). A threat from an attack can lead to a hazard regarding functional safety. This shows the relationship of security and safety. Therefore in general both analyses need to be performed early in the development process and the identified hazards and threats need to be aligned and regarded from the respectively other point of view as potential risk. There are already several publications to this topic and also the SAE document contains an entanglement of both processes.

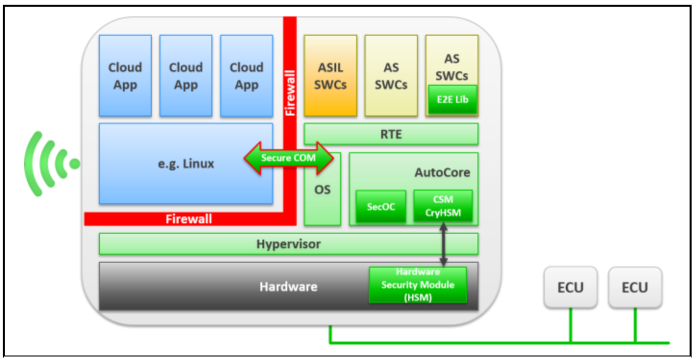

Fig. 3 "Smart Antenna"

Analogue to the functional safety, also for cyber security there will be efforts to standardize basic mechanisms. So e.g. AUTOSAR has defined basic libraries for cryptographic functions and interfaces as well as secured communication between ECUs. Dependent on the application these basic components can be realized completely in software for simple systems with minor security requirements or make use of dedicated hardware. In context of the EVITA (E-safety vehicle intrusion protected applications) project different scenarios and systems were provided. Systems with high security requirements can hereby utilize hardware components like e.g. the Hardware Security Module (HSM).

In future system architectures, the online access to the car is a critical element and needs to fulfill requirements regarding functional safety as well as regarding cyber security. The "smart antenna" is often consolidated with telematics functions and can additionally execute dynamic applications which need to be isolated from the basic functionalities (see Fig. 3).

The requirements towards today's ECU architectures are much more complex than in the past. By combining aspects like standard architectures, functional safety, cyber security, multicore systems and availability, the goal of weighting and combining single system aspects for developing "dependable systems" must be formulated. Fig. 4 shows possible approaches for different system aspects. Flexible solutions are necessary to solve the various scenarios by a combination of standard elements, which are assembled like in a modular constructions system to build up the "dependable" final system.

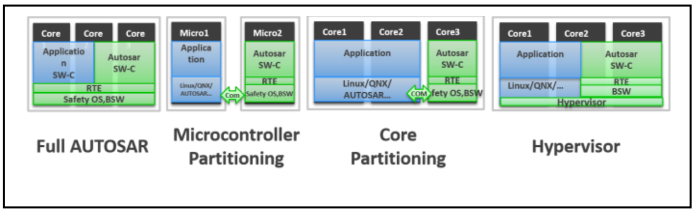

Fig. 4 Different solutions for multicore systems

References

[1] SAE International, J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"

[2] ISO 26262, "Road vehicles – Functional safety".

[3] SAE International, J3016 "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems"