An Overview of Automotive Security Standards

Obaid Ur-Rehman and Nataša Živić, Christoph Ruland
University of Siegen
Chair for Data Communications Systems
D-57068 Siegen, Germany
{obaid.ur-rehman, natasa.zivic, christoph.ruland}@uni-siegen.de

***Abstract*—Traditional vehicle standards, such as ISO 26262-1:2011, were focused mainly on reliability and functional safety aspects. Due to the demand for increased connectivity and the emergence of autonomous driving systems, security of vehicles is becoming ever more relevant and important. Modern vehicles are a part of the cyber physical world and can be attacked from the Internet. These security needs can be addressed at many levels such as secure design and development of the software running on the Electronic Control Units, secure bus networks as well as secure connectivity to the outside world, e.g., the Internet. Unfortunately, until now there are no global standards dedicated to vehicular security. The good news is that recently some standardization activities have started to support the security aspects of the vehicles. This includes addressing the security on many levels, such as secure programming guidelines (e.g., MISRA), threat analysis and risk assessment (e.g., SAE J3061), cyber security engineering of road vehicles, (e.g., ISO/SAE 21434) and connectivity to the backend (e.g., ISO 20078). In this paper an overview of these security standards is given.**

Keywords—Automotive Security; Standards; Risk Analysis; Secure Software Development

I. INTRODUCTION

Today's automotive systems consist of a large number of Electronic Control Units (ECUs) connected together using various different networking protocols and standards. A modern vehicle consists of more than 100 ECUs and this number is ever increasing with the addition of new functionalities such as driver assistance systems and automated driving. These functionalities are pushing towards the usage of more software-based components as well as higher demands on computational power. Additionally, there is also a high demand for connectivity to the external world through various forms of wireless communications technologies such as Cellular / mobile networks, WiFi, Bluetooth and GPS. On the down side, the addition of these new features and connectivity is making the vehicle open to cybersecurity threats through a huge number of the available attack vectors and attack surfaces.

This transition of a vehicle from a completely closed system to a system that is a component of the Internet of Things (IoT), is already resulting in a tremendous increase in the complexity of the vehicular software as well as the hardware. This is evident from the use of embedded operating systems on the ECUs and with the development of Advanced Driver Assistant Systems (ADAS) and autonomous driving which will further be supported by (Adaptive) AUTOSAR. At the same time, with the addition of new functionalities and external as well as internal communication interfaces, the security threats to modern vehicles are also increasing considerably. Considering that a modern vehicle is part of the cyber physical system, with the possibility of being attacked and hacked from the cyber space, there is a need for establishing sound security practices in the automotive domain. This can be achieved by following standard risk analysis techniques to assess and prioritize the risks. Additionally, there is a need to follow standardized approaches for software design, development and testing of automotive software.

These security threats and risks are better addressed by following the standard software development guidelines and methodologies and verifying this using standardized software testing practices. Moreover, the security is also enhanced by the use of standardized networking protocols. Some standards have been developed, and some are still under development, to address and enforce security in the automotive engineering process. These include the standards specifically designed for the automotive domain such as SAE J3061, ISO/SAE 21434 and ISO 20078, aside from various other recommendations, best practices and guidelines. There is a need to understand the various security standards and study their applicability to the automotive domain.

Additionally, as the use of software is ever increasing in the automotive domain, it is necessary that the automotive software should be developed with security in mind, in addition to safety which is already highly valued in the automotive industry. The development of software must follow standardized approaches, best practices and guidelines. This will allow the software to be testable so that the quality of software can be measured and it can be assessed that the software is reliable also from the security perspective.

In this paper, the existing and upcoming major security standards and guidelines, for road vehicles, are identified and discussed. At the time of this writing, a survey or comparison of the standards is missing in the literature. This paper aims to give the reader an introduction to the important and interesting topic of security in road vehicles.

The paper is organized as follows. In Section II, ISO/SAE 21434 is discussed, which is an upcoming standard for cybersecurity engineering of road vehicles. In Section III, SAE J3061 is discussed, which is a cybersecurity guidebook for cyber-physical vehicle systems. Section IV discusses ISO 20078, which is a standard for extended vehicle, including the

vehicle and the backend. Finally, the paper is concluded in Section V.

II. ISO/SAE CD 21434: Road Vehicles - Cybersecurity Engineering

The most awaited ISO and SAE standard, ISO/SAE 21434 [1], focuses on the cyber security engineering aspects of a modern road vehicle. The standard is still under development and is planned to be released in May 2020. It is a joint effort between ISO and SAE, which have previously developed standards for safety of road vehicles. The standardization committee also includes representatives of major automotive manufacturers and Tier 1 suppliers.

The intention behind the standard is to focus on the specification of requirements for cybersecurity risk management for road vehicles, their components and interfaces. The standard aims at the complete cybersecurity engineering (i.e., concept, design and development phases), but also on the production, operation, maintenance, and decommissioning phases. The intention of the standard is also to define a framework that will include requirements for cybersecurity process and the development of a common language for communicating and managing cybersecurity risks among the automotive stakeholders. ISO/SAE 21434 will be applicable to modern road vehicles that include electrical and electronic systems. It will focus on their interfaces and communications but it will remain independent of any specific technology or solutions related to cybersecurity. A good summary of ISO/SAE 21434 and the progress has been reported in [5].

The activities of the standardization are split into four parts, i.e., risk management, product development, operation and maintenance, and process overview and interdependencies.

A. Risk management

Risk management is the basic and most important activity of any cybersecurity engineering process. The goal is to identify the risks, rate them with the aim to prioritize the most serious ones and to ensure that they are addressed and brought under control and acceptability level. The risks may come from many inside or outside factors such as external interfaces of the vehicle to the user, external communication to other vehicles, infrastructure or the backend and the ability to perform a software update.

ISO/SAE 21434 will interact with ISO 26262 and borrow from ISO 15408 for the risk assessment and may also adapt ISO 27000 to the automotive domain.

B. Product development

The product development is based on the V-model, which is also used in general in the IT industry, but more specifically in the safety systems. It has been discussed well for the safety engineering process in ISO 26262, which has also been adopted recently to the automotive domain (i.e., ISO 26262-1:2018).

A cybersecurity aware v-model starts with the system concept, where the threat analysis and risk assessment method (e.g., as in SAE J3061) is performed. This information is then used for system specification for software and hardware. The hardware and software development is performed and the system is verified for residual risks, which if possible, may be mitigated further. This is finally followed by validation of the system. Testing might include automated testing as well as pen-testing.

C. Production, operation and maintenance

During the vehicle production, the standard tackles the cybersecurity topics such as who access the software and hardware of the vehicle. After the vehicle has been produced, there are chances that vulnerabilities are introduced during the operation and maintenance. The topics handled by the standard include the whole supply chain such as the supplier, vehicle manufacturer, as well as the customer. While the vehicle is in operation, there might be new vulnerabilities introduced or uncovered and exploited. The manufacturer or the supplier should be able to develop patches for the software to address the vulnerabilities.

D. Process overview and interdependencies

This section includes the topics which might not fall under a concrete cybersecurity activity. They are however necessary for the achievement of cybersecurity such as development of a cybersecurity culture and cybersecurity management across the organization. A parallel to this is the safety culture and safety management of the ISO 26262.

III. SAE J3061: Cybersecurity Giudebook for Cyber-Physical Vehicle Systems

This cybersecurity guidebook [2] recommended practice defines a set of high-level guiding principles for cybersecurity in automotive cyber-physical systems which are to be used in series production. It defines a framework for inclusion of cybersecurity into the lifecycle of automotive cyber-physical systems. Furthermore the guidebook provides information on tools and methods for designing and validation of cyber-physical automotive systems. It provides basic guiding principles on cybersecurity in automotive systems and finally, it provides the base for further standards development activities for automotive cybersecurity.

SAE J3061 recommends application of a cybersecurity process for all automotive systems responsible for functions that are Automotive Safety Integrity Level (ASIL) rated per ISO 26262 [3], or that are responsible for functions associated with propulsion, braking, steering, security and safety, as well as automotive systems that handle Personally Identifiable Information (PII).

A. Safety critical vs. Security critical systems

A safety-critical system is usually defined as a system that may cause harm to life, property, or the environment if the system does not behave as intended or desired. On the other

hand, a security-critical system is a system that may lead to financial, operational, privacy, or safety losses if it is compromised through a vulnerability of the system. Some systems are both, safety and security critical, i.e. steering assist system. Some systems are only security, but not safety critical, such as the entertainment system. An autonomous vehicle can be both safety as well as security critical, e.g., rogue cars on the road, controlled by hackers are a big safety hazard for other traffic participant and road users.

Safety handles potential hazards by introduction of safety mechanisms into the design of automotive systems. Safety often utilizes the detailed hazard analysis technique called Fault Tree Analysis (FTA) [3] to identify potential causes of the top hazard events and look for single-point and multipoint random hardware failures.

System cybersecurity considers potential threats from a malicious attacker (intentionally induced failures) aiming to cause harm or gain financial benefits. Cybersecurity, in parallel to safety, utilizes detailed threat analysis technique called Attack Tree Analysis (ATA). ATA determines potential paths that an attacker could take through the system to lead to the top-level threat. Despite differences, similarities can be found between the approaches of safety and security.

B. Guiding principles

Guiding principles can be expressed in a following way:

- Know your system's cybersecurity risks
- Understand the key cybersecurity principles
- Consider vehicle owners' use of system
- Focus on cybersecurity in the concept and design phases
- Implement cybersecurity in the development, verification and validation phases
- Consider cybersecurity in incident response such as establishing an internal response team but also communicating security incidents to Auto-ISAC
- Cybersecurity considerations at the end of vehicle's life

C. Cybersecurity process overview

Management of cybersecurity consists of two aspects: the overall management of cybersecurity and management of cybersecurity activities within specific stages of the development life cycle.

The concept phase is the initiation of the cybersecurity lifecycle includes the development of a cybersecurity program plan. This describes the activities to be carried out as part of the cybersecurity lifecycle. Thereby, the Threat Analysis and Risk Assessment (TARA) activity is used to assess the potential threats to the system and to determine the risk associated with each of the threats.

Product development considers systems level, hardware level and software level.

A System Context (system level) defines interfaces between the system's hardware and software, the crucial data flows, as well as storage and processing within the system. Using the System Context, the system-level technical cybersecurity requirements are then allocated to hardware and software or to both.

Hardware security requirements are specified from the cybersecurity requirements of the hardware during the system level development. Following hardware design, a vulnerability analysis can be performed to help identify potential vulnerabilities in the design and to address the potential vulnerabilities.

Software security requirements can be specified from the cybersecurity requirements of the software during the system level development. Following software architectural design, a vulnerability analysis can be performed to help identify potential vulnerabilities in the software architectural design and to address the potential vulnerabilities.

The operation phase includes: operation and service consisting of normal maintenance activities and repair maintenance and repair activities.

Service that could affect cybersecurity includes re-flashing ECU's, connecting to the on-board diagnostics port, telematics system updates, update of the battery management system of fully electric or hybrid vehicles, vehicle to cloud computing interfaces, etc.

Supporting processes include configuration management, documentation management, change management, management of cybersecurity requirements and requirements for dealing with distributed development.

The gate reviews aim to ensure that appropriate activities have been performed and completed correctly and consistently before the next step of development begins. They may be conducted by a small team of technical experts that should be independent of the feature development.

D. Overall management of cybersecurity

The guideline provides detailed recommendation on following concepts:

- Creating, fostering, and sustaining a cybersecurity culture
- Establishing methods to help ensure compliance to an adopted cybersecurity engineering process
- Identifying and establishing needed communication channels with respect to cybersecurity, both internally and externally
- Development and implementation of training and mentoring to achieve a competence in cybersecurity for cyber-physical vehicle systems

- Incorporating a field monitoring process that includes monitoring hacker chatter, media articles, reporting unsuccessful attacks, etc.
- Incorporating an incident response process that includes an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

E. Process Implementation

Process implementation consists of three types of implementations: applying a cybersecurity process separately with integrated communication points to a safety process, applying a cybersecurity process in conjunction with a safety process tailored according to ISO 26262 and some cybersecurity processes and steps are shared with safety and some that are unique to cybersecurity only.

IV. ISO 20078: ROAD VEHICLES - EXTENDED VEHICLE

ISO 20078 [4] is the extended vehicle (ExVe) standardization project. The project considers additional benefits of diagnostic data and telematics, such as emergency Call (eCall), roadside assistance, pay how you drive, remote door lock / unlock, diagnostic help desk, early field warning, preventive diagnostics, remote diagnostics, remote software or firmware update (Over-the-Air), diagnostics at the reception, digital service booklet, maintenance, service Call (sCall) and breakdown Call (bCall).

The standard helps in solving the following problems:

- Customer's access: the customer has right and a software tool for controlling his vehicle and personal data
- Security of the data connection: End-to-End security has to exist
- Access to the vehicle: technology used in different cases
- Definition of the vehicle data structures: data available by the vehicle electronics and processed for the customer.

Three different optional solutions concerning vehicle access have been discussed so far:

- In-Vehicle Interface: a customer reads and writes data into and from the vehicle
- Application Platform: a customer and an OEM, 3rd party or neutral server read and write data into and from the vehicle
- Extended Vehicle: a customer and a 3rd party server use a standard interface (ExVe) to read and write data to and from vehicle's telematic units, which are OEM specific.

ExVe defines:

- ExVe content: the data content in a human readable data format
- ExVe access: defines the mechanism to read and alter data
- ExVe security: defines an end-to-end security mechanism
- ExVe control: defining the customer portal; protection of data privacy and OEM's

ExVe is implemented to enable the 3rd party stakeholder to access customers, independent operators and vehicle manufacturers. Server-to-Server intercommunication allows for any connected 3rd party stake-holder to handle data in his own manner, e.g., through apps, web services, or other analysis methods.

V. CONCLUSION

In this work, the currently available major automotive security standards as well as those currently under development are briefly discussed. This is followed by a brief overview of their objectives and their domain of applicability. The major domains covered by these standards include threat analysis, cybersecurity engineering, software development, internal and external network communications and connectivity to the backend servers.

Security has not been given a higher importance in the automotive industry as compared to other industries such as IT and manufacturing. Currently there is no study available to compare the present and future security guidelines and standards in the automotive domain. Such a detailed comparison including in-depth analysis of security in the automotive world is planned for future.

REFERENCES

[1] ISO/SAE 21434: Road Vehicles -- Cybersecurity engineering, Technical Committee: ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

[2] SAE J3061: "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", January 2016

[3] ISO 26262: "Road vehicles – Functional safety", International Organization for Standardization (ISO) in 2011

[4] ISO 20078: Road vehicles -- Extended vehicle (ExVe) 'web services'

[5] Christoph Schmittner, Zhendong Ma, "Status of the Development of ISO/SAE 21434", 25th European Conference, EuroSPI 2018, Bilbao, Spain, September 5-7, 2018