# An Analysis of Automotive Security Based on a Reference Model for Automotive Cyber Systems

Jasmin Brückmann, Tobias Madl
Munich University of Applied Sciences
MuSe – Munich IT Security Research Group
Munich, Germany
email: madl@hm.edu, brueckma@hm.edu

Hans-Joachim Hof
Technical University of Ingolstadt
CARISSMA – Center of Automotive Research on Integrated Safety Systems and Measurement Area
Ingolstadt Research Group Applied IT Security
Ingolstadt, Germany
email: hof@thi.de

*Abstract*— **This paper presents an analysis of automotive security based on a reference model for Automotive Cyber Systems (ACS). In IT security, reference models are useful to conduct security analyses for either systems that do not exist yet, or for a number of existing systems that have similar properties. With Automotive Cyber Systems, both cases are present: some Original Equipment Manufacturers (OEMs) are already running Automotive Cyber Systems, whereas other OEMs only implemented partial Automotive Cyber Systems. The reference model presented in this paper is based on existing systems, as well as system architectures of research papers describing not yet existing applications of Automotive Cyber Systems. Hence, the reference model is of high relevance for future approaches on automotive security. The reference model was used to identify generic security requirements for automotive security in Automotive Cyber Systems. These security requirements are of high relevance for the design of upcoming Automotive Cyber Systems, as well as emerging applications like autonomous driving.**

***Keywords- Automotive Security; Automotive Cyber System; Cyber-Phyiscal System;***

## I. INTRODUCTION

Digitalization is currently a big driver of the automotive industry. Unique features of new vehicles often are based on software, communication between vehicles, and connected automotive services. Forbs expects 152 million connected vehicles worldwide in 2020 [1]. The interconnection of vehicles with infrastructure, other vehicles, as well as a whole ecosystem of services will result in a so-called Automotive Cyber System. Current systems are limited, as the Original Equipment Manufacturers (OEMs) usually try to keep systems closed, offering only a very small set of services to drivers, limiting the potential of the ecosystem. However, startups in the automotive domain nowadays implement their services by using On-Board Diagnostics (OBD) dongles. An OBD dongle connects to the OBD II interface of a vehicle, as well as to a smartphone that provides Internet connectivity. By doing so, startups can access internal communication of vehicles via the Internet. Due to this strategy, OEMs are likely to open their platforms for third-party services to avoid dangerous fiddling with the OBD interface. With the increasing connectivity of vehicles, in combination with the importance of mandatory safety requirements and some serious hacks, e.g., [10], IT security became a priority for Automotive Cyber System. SAE 3160 is the first automotive safety standard that also addresses IT security. It is to be expected that more automotive security standards will be published in the near future.

This paper presents a reference model for Automotive Cyber Systems. Nowadays, in the observation of the authors, the automotive industry tends to favor partial security solutions over a holistic approach to IT security. The reference model aims on promoting a holistic approach to IT security in Automotive Cyber systems. The second part of the paper describes a security analysis based on the reference model. It results in a set of generic security requirements for Automotive Cyber Systems. These generic security requirements can be specialized for future systems in the automotive domain, hence support holistic approaches to IT security in Automotive Cyber Systems.

The rest of this paper is structured as follows: Section II discusses related work on reference architectures for Automotive Cyber Systems. Section III presents the reference model for Automotive Cyber Systems. Section IV presents the security analysis. Section V concludes the paper.

## II. RELATED WORK

Most reference models in the automotive domain just model small parts of the whole systems. This is due to a very distinct “silo thinking” in the automotive industry in combination with the special structure of the automotive industry (many component suppliers that implement only small parts of the overall system). These reference models hinder a holistic approach to IT security. The reference architecture presented in this paper targets the whole Automotive Cyber System, including in-vehicle components, vehicle-to-vehicle communication, vehicle-to-infrastructure communication, as well as communication with an ecosystem of automotive services.

The works most similar to this paper are [2]-[4]. The models presented in these papers consider multiple parts of a full Automotive Cyber System. However, an analysis of these models showed that important components and data flows are missing. The reference architecture presented in this paper takes these components and data flows into consideration. Hence, it is more complete.

## III. Reference Model for Automotive Cyber Systems

The reference model for Automotive Cyber Systems was compiled from two sources: existing systems that implement parts of an Automotive Cyber System, and visions of future Automotive Cyber Systems collected from research papers and presentations on future products. Figure 1 gives an overview of the reference model.

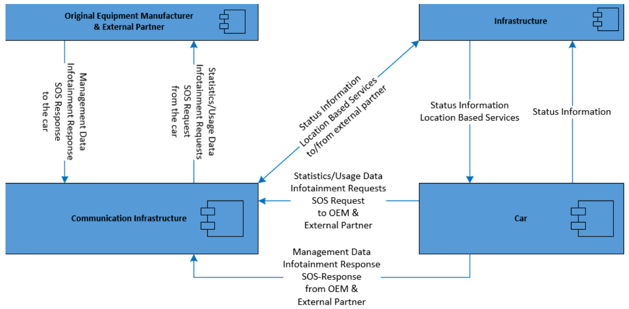
Original Equipment Manufacturer & External Partner
Infrastructure
Communication Infrastructure
Car
Management Data Infotainment Response SOS Response to the car
Statistics/Usage Data Infotainment Requests SOS Request from the car
Status Information Location Based Services to/from external partner
Status Information Location Based Services
Status Information
Statistics/Usage Data Infotainment Requests SOS Request to OEM & External Partner
Management Data Infotainment Response SOS-Response from OEM & External Partner

Figure 1. Overview of Automotive Cyber Systems (ACS) reference model.

The model consists of four components:

- OEM and external partners component
- Communication infrastructure component
- Infrastructure component
- Car component

The car communicates with nearby infrastructure and vehicles by Ad-hoc Long Term Evolution (Ad-hoc LTE) or WiFi. For long distance communication and access to other networks, the car component uses LTE or Universal Mobile Telecommunications System (UMTS). Both LTE and UMTS communication are represented by the communication infrastructure component in the reference model. The communication infrastructure component provides connectivity to the component OEM & external partners component. The OEM and other external partners offer automotive services. Components of the reference model are described in more detail in the following sections.

### *A.* OEM and External Partners component

Figure 2 and Figure 3 show sub components and data flows of the OEM & External Partners component.

Subcomponent Management Services provide essential services for maintaining functionality and security of the car. Managed services include software updates over the air (SOTA) and firmware updates over the air (FOTA). Vehicles in Automotive Cyber Systems communicate a lot with other systems (vehicles, infrastructure, services). Hence, any vulnerability in a connected component is a potential danger for the vehicle. A timely provisioning of patches for vulnerabilities is considered a key success factor for security in Automotive Cyber Systems.

Advanced services become possible with the availability of statistics of vehicle usage and other mobility data. The Data Analysis Platform subcomponent is responsible for data collection, privacy-preserving data transformation, and data storage.

The OEM Services component offers additional services of the OEM. For example, an OEM could offer personalized reminder for service attendance. It could also provide information or sponsored offers from external partners. The car's driving assistance system (FAS - Fahrzeugassistenssysteme) and high autonomous driving (HAF - Hochauomatisiertes Fahren) systems get their information from OEM services, because these services have a better overview of the overall traffic situation.

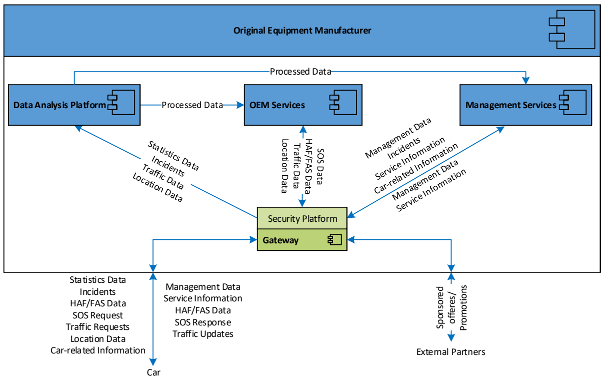
Original Equipment Manufacturer
Processed Data
Data Analysis Platform
Processed Data
OEM Services
Management Services
Statistics Data Incidents Traffic Data Location Data
SOS Data HAF/FAS Data Traffic Data Location Data
Management Data Incidents Service Information Car-related Information
Management Data Service Information
Security Platform
Gateway
Statistics Data Incidents HAF/FAS Data SOS Request Traffic Requests Location Data Car-related Information
Management Data Service Information HAF/FAS Data SOS Response Traffic Updates
Car
Sponsored offeres/ Promotions
External Partners

Figure 2. Subcomponents and their data flows at the OEM.

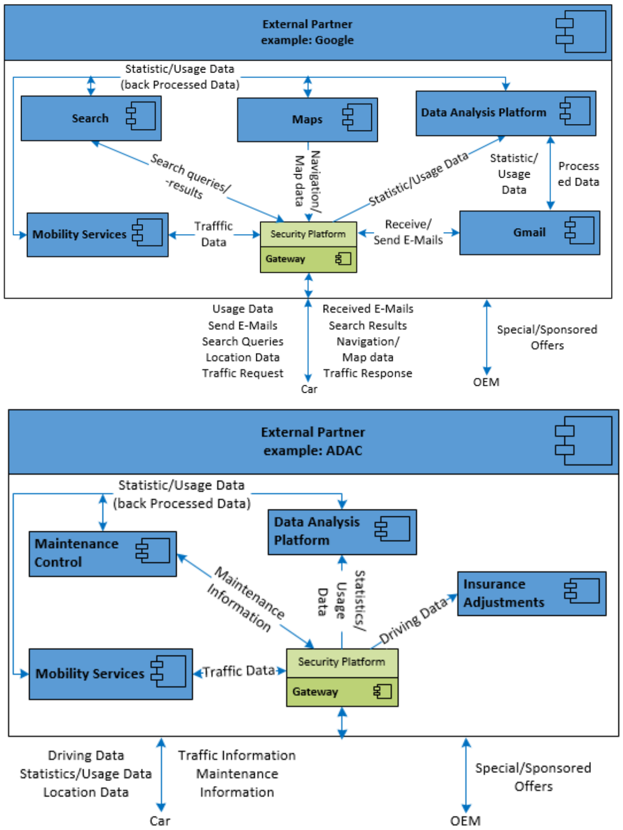

Figure 3. Subcomponent and data flows at two examples for external partners (Google and ADAC).

For the sake of this paper, Google and ADAC ("Allgemeiner Deutscher Automobil Club", association similar to the AAA in the US) were chosen as example of external partners. It is assumed that their subcomponents are prototypic for a wide range of other external partners. Subcomponents of external partners differ based on the services they are offering. Both institutions, ADAC and Google, offer mobility services, including information about the current traffic situation. Similar to the OEMs, external partners use a Data Analysis Platform component for data gathering, processing, and storage. The Security Platform component is similar to the Security Platform of the OEM. External partners may also offer some of their standard services adapted for automotive use. For example, Google may provide emails using their Gmail service, but emails are read to the user instead of a textual presentation. It should be noted that adaptations of standard IT services for automotive use might open new attack vectors for attackers.

ADAC offer extra subcomponents Maintenance Control and Insurance Adjustments. Among other things, the Maintenance Control subcomponent monitors the maintenance status of the car and informs the driver if the vehicle needs an inspection. The Insurance Adjustment subcomponent monitors the driving behavior and adjusts the insurance fee if the driver does not drive carefully (a so-called telematics tariff).

Figure 3 does not only show the subcomponents, but also the data flows of the OEM & external partners component. Most communication takes place between the OEM and the car. The data analysis platform receives statistics from the car, such as driving hours, hardware, or software incidents. Traffic and location data can be used for statistics, too. Once the collected data is processed, the OEM might improve its services and extends its product portfolio based on the data. The OEM Services receive traffic and emergency (SOS) requests and send the corresponding responses. For traffic requests and extended information they need the location data from the car. Additionally, they communicate with the HAF/FAS systems of the car, for example, to get advanced traffic information. This includes redirection because of current accidents or disruptions or automatic searching for a parking site. The Management Services component receives car related information to support the driver, for example, in case of incidents or hardware and software issues. Additionally, software and firmware updates are provided by the management services (called management data in Figure 3). Service information about the car and the OEM are also delivered by the management services.

Figure 3 also shows the data flows of external partners. The Google Search component receives search requests and answers with search results. For navigation purposes, maps and navigation instructions can be retrieved by the car from the Maps component. Gmail grants the passengers access to their mail accounts. The Mobility Services subcomponent is used to request a report on the current traffic situation. All components are sending statistics and usage data to the data analysis platform to be processed and used to improve offered services and to inspire new services. The Maintenance Control subcomponent monitors if the car should come to an inspection in the near future and informs the driver as needed. In order to analyze the driving behavior, the Insurance Adjustment subcomponent needs the driving data from the car. Both external partners are in contact with the OEM to share special or sponsored offers for the customers like bargains for.

### B. *Communication Infrastructure component (external component)*

The Communication Infrastructure component handles long distance communication and access to other networks. Vehicles typically use LTE or UMTS. The communication infrastructure component provides connectivity to the component OEM & external partners component. It should be noted that the communication infrastructure is an external component.

### C. *Infrastructure component*

The Infrastructure component includes the subcomponents Road-Side Units (RSUs) and Location Based Services (LBS) as can be seen in Figure 4.

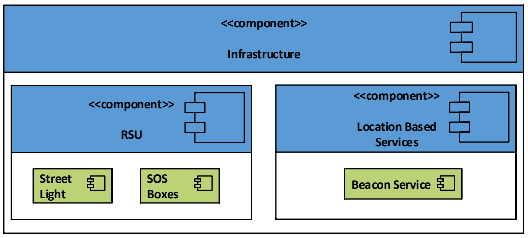

Figure 4. Subcomponents of Infrastructure component.

RSUs include traffic control devices like streetlights, road signs, or speed measurements.

LBS are services providing information that has been created, compiled, selected, or filtered taking into consideration the current locations of the users or those of other persons or mobile objects [11]. Local stores may provide LBS, for example, to promote current offers. An OEM may offer LBS to inform drivers about points of interest.

RSUs, as well as LBS communicate with the car using LTE, WiFi, or UMTS. Thereby, the RSU is directly talking with the cars Onboard Unit (OBU). The car and RSUs are exchanging status information, for example the current status of streetlights or the speed of the car. RSUs support emerging car applications like autonomous driving, as well as safety assistant systems. The Infrastructure component is communicating with the OEMs and external partners, too. It regularly sends status information about traffic or speed signs, receives commands to readjust the tempo limit, etc. Local stores or establishments provide LBS to the car. They may also send status information for big data analysis to the OEMs and external partners, or receive status information or additional offers.

### D. *Car component*

The car has five subcomponents. The Infotainment Unit subcomponent, the Processing Unit subcomponents, the Communication System subcomponents, and the Sensor and

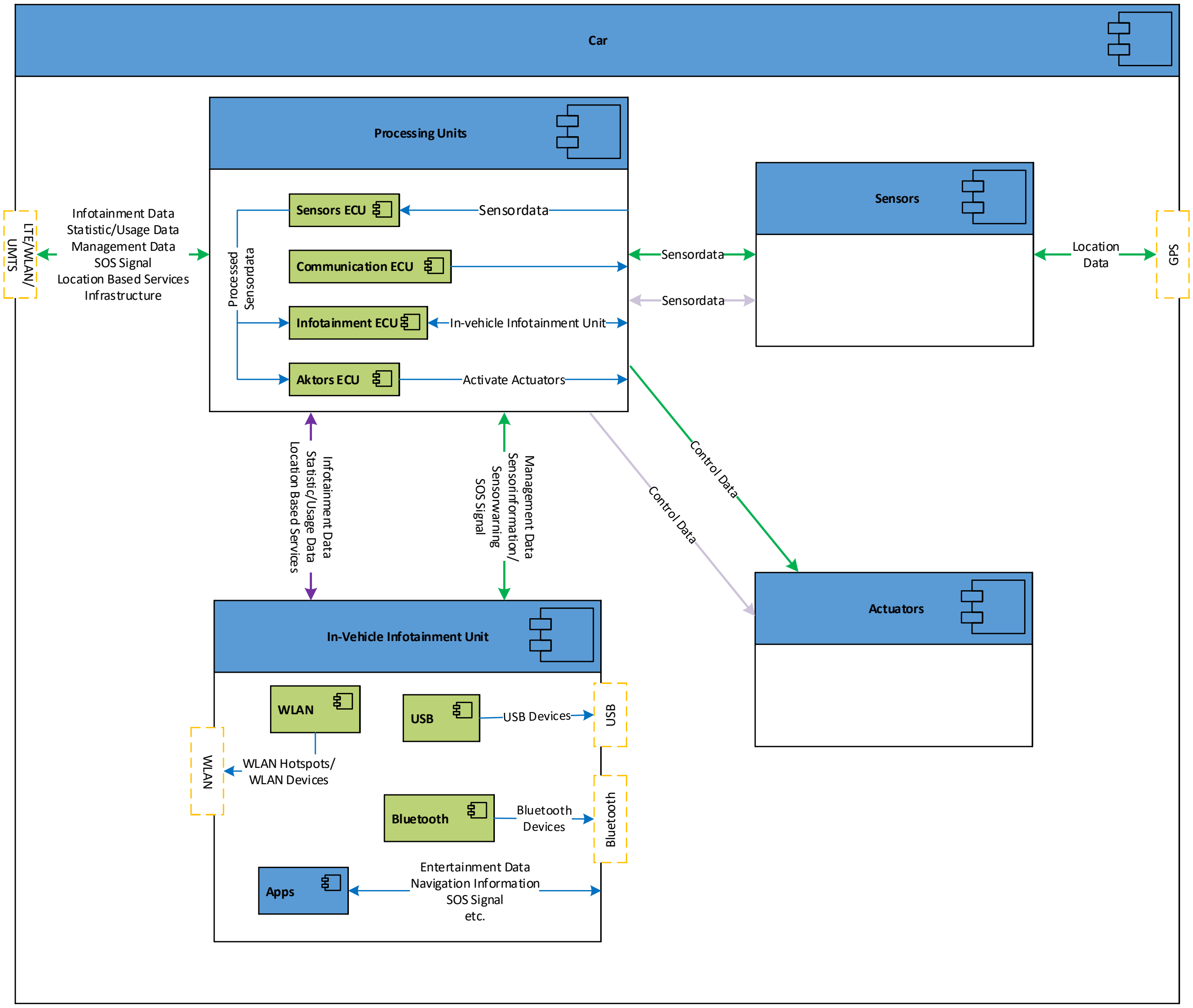

Figure 5. Subcomponent and data flows of the Car component.

Actor subcomponents. Figure 5 shows the subcomponents and the data flows between those subcomponents.

The Infotainment Unit subcomponent is the main interface for human interactions. It provides apps and services like telephone, mail, WWW, contacts, navigation, music, and emergency calls. It offers a wide range of short-range communication technologies that are suitable to connect to consumer devices. Supported communication standards typically include Bluetooth, WiFi, and USB.

Next, there are Processing Unit subcomponents. Normally, each subcomponent has at least one associated Electronic Control Unit (ECU) for processing incoming data and controlling resulting actions. These ECUs are distributed over the whole car and communicate with the respective unit to be controlled. An example would be a sensor ECU for receiving raw data from ultrasonic sensors and converting it to standardized data for further processing in the car. This data is then send to the central controlling ECU for processing.

The Communication System subcomponent supports various bus technologies for intra-vehicle communication. This system also provides interfaces for external communication (with OEM, external partners, or infrastructure). Inter-bus communication is possible via gateways. The Communication System also provides the well known OBD II interface that enables quick, easy and profound analysis of vehicles.

Other subcomponents include sensor and actuators. These are spread over the whole vehicle to provide various functionality. Sensors are used to gather data about the physical world (e.g., GPS position, open doors, park distance control, engine temperature, tire preassure, etc). Actuators are used to start actions, e.g., to start the windshield wipers.

## IV. Security Analysis and Security Requirements for Automotive Cyber Systes

The security analysis presented in this paper is based on CORAS [9]. CORAS is customizable on any system and component and offers an own risk-modeling notation that is inspired by UML. Its adaptability allowed for an application of CORAS on the presented reference model, and allows integrating previous work on application-specific attacker models [5-8]. CORAS is used to identify risks for assets. CORAS consists of 8 steps.

In the first step, the scope of the analysis is defined. The scope of the analysis presented in this paper is an analysis of an Automotive Cyber System implementing the reference model presented in Section IV.

The second step involves an adjustment of the scope of the analysis by the customer of the analysis. This step was omitted, as there is no customer for this analysis.

The third step involves refining the target description using asset diagrams. The following assets were identified: "personal data" (personal data of driver and passengers), "critical systems" (systems ensuring safety of the car or safety of other critical systems), "integrity of the car" (car does not get harmed), "integrity of human" (humans do not get harmed), and "public trust" (trust in products of OEM and external partners). In step 4, the importance of the assets is rated (1=very important, 5= minor importance). The most important assets are "integrity of humans" and "personal data", see Figure 6 for the complete ranking. Strict laws for safety of humans, as well as very strict privacy laws of the European Union motivate this rating.

| Asset | Importance | Type |
|---|---|---|
| Integrity of human | 1 | Indirect asset |
| Personal data | 1 | Direct asset |
| Critical data | 2 | Direct asset |
| Critical systems | 2 | Direct asset |
| Integrity of the car | 2 | Indirect asset |
| Public trust | 3 | Indirect asset |

Figure 6. Asset rating.

In this step, a likelihood scale (see Figure 7), as well as consequences scales for each asset (see Figure 8 for the consequence scale of the asset "critical system") are defined. The likelihood scale is motivated by statistics about German car incidents in 2016.

| Likelihood value | Description | Definition |
|---|---|---|
| Certain | more then twenty per year | $[200, \infty\rangle : 10y = [10, \infty\rangle : 1y$ |
| Likely | ten to twenty times per year | $[100, 200\rangle : 10y = [10, 20\rangle : 1y$ |
| Possible | five to nine times per year | $[50, 90\rangle : 10y = [5, 9\rangle : 1y$ |
| Unlikely | Two to four times per year | $[20, 40\rangle : 10y = [2, 4\rangle : 1y$ |
| Rare | Less than once per year | $[0, 10\rangle : 10y = [0, 1\rangle : 1y$ |

Figure 7. Likelihood scale.

| Consequence value | Description |
|---|---|
| Catastrophic | Safety critical systems |
| Major | Most valuable core systems |
| Moderate | Valuable systems |
| Minor | Standard systems |
| Insignificant | Additional feature systems |

Figure 8. Consequence scale for asset "critical systems".

In the next step, risks are identified using threat diagrams showing threat scenarios. The sixth step identifies consequences and likelihoods of the incidents that were identified in the prior step. In step seven, the risks are evaluated based on a risk matrix. The risk matrix uses likelihood and consequence of an incident to distinguish between acceptable risks and unacceptable risks. Figure 9 shows, as an example, the risks for the asset “personal data”, unacceptable risks are located in grey cells; acceptable risks are located in white cells. The risk matrix uses the shortcuts shown in Figure 10.

| | Insgnificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|
| Rare | | | | | ▨ |
| Unlikely | | | COI | CIU | COE, COI(1), COE(1) |
| Possible | | | ▨ | CCS, CCT, COC | COC(1) |
| Likely | | ▨ | LDI | LUT | LUT(1) |
| Certain | ▨ | ▨ | VUS(1) | ▨ | VUS |

Figure 9. Risk evaluation matrix for asset "personal data".

| Shortcut | Unwanted Incident |
|---|---|
| CIU | Compromised infotainment unit |
| CCS | Compromised communication system |
| UAC | Unauthorized access to car |
| SBS | Slow or broken system |
| VUS | Vulnerable system |
| CCT | Compromised confidentiality of transmitted data |
| COC | Compromised car |
| COE | Compromised oem or external partner |
| COI | Compromised infrastructure |
| LUT | Loss or unusability of transferred data |
| LDI | Loss of data/compromised integrity |
| UPB | Unpredictable behaviour |
| CSF | Complete service failure |

Figure 10. Shortcuts for risks

The last step identifies risk treatment for unacceptable risks. To avoid unacceptable risks, the following generic security requirements were identified based on the presented reference model for Automotive Cyber Systems. Security requirements also include requirements for processes of the organizations running an Automotive Cyber System or automotive services:

Technical requirements:

- Trustworthy software sources: Software should only be downloaded from trustworthy sources. Authenticity of data sources must be ensured, as well as integrity protection of software during transit.
- Security Warning during software installation: Drivers should have the ability to avoid software installation in improper situations.
- Appropriate access control for all components and subcomponents of the Automotive Cyber System.
- Restriction of functional access for components.
- Authentication of all connecting devices and all communication partners.
- Integrity checks of incoming traffic.
- Encryption of all communications.
- Strict control of incoming and outgoing connections and traffic.
- Redundancy of important systems.

ISBN: 978-1-61208-582-1

- Fail checks for important components.
- Fail safe states for important components.

Process requirements:

- Appropriate scope of training programs for employees.
- Use of secure software development life cycles throughout the development of all components of a Automotive Cyber System.
- Review of important changes and work.
- Careful selection for suppliers of software and hardware.

## V. Conclusion And Future Work

The contribution of this paper is twofold: first, the paper provides a reference model for Automotive Cyber System that is more complete than previous models and takes into consideration upcoming applications like autonomous driving. The reference model is of great help for engineering new applications for Automotive Cyber Systems. The second contribution is a security analysis of Automotive Cyber Systems using the reference model as a basis. Output of the security analysis is a set of generic security requirements for automotive security in Automotive Cyber Systems. The generic security requirements are considered to be highly useful for the design of upcoming Automotive Cyber Systems, as well as emerging applications like autonomous driving. The use of the reference model allowed for a holistic approach to automotive security.

## References

[1] N. McCarthy, “Connected Cars By The Numbers”, Forbes Business, January 2015, https://www.forbes.com/sites/niallmccarthy/2015/01/27/connected-cars-by-the-numbers-infographic [last access August 1st, 2017].

[2] L. Zhang, “Modeling automotive cyber physical systems,” in Distributed Computing and Applications to Business, Engineering & Sci- ence (DCABES), 2013 12th International Symposium on. IEEE, 2013, pp. 71–75.

[3] C. Ebert and I. N. Adler, “Automotive cyber-security” ATZextra, vol. 21, no. 2, 2016, pp.58–63.

[4] H. Abid, L. T. T. Phuong, J. Wang, S. Lee, and S. Qaisar, “V-cloud: vehicular cyber-physical systems and cloud computing,” in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. ACM, 2011, p. 165.

[5] C. Ponikwar, H.-J. Hof, and L. Wischhof, "Towards a High-Level Security Model for Decision Making in Autonomous Driving“, ACM Chapters Computer Science in Cars Symposium 2017 (CSCS 2017), Munich, Germany, July 2017, pp. 1-4.

[6] C. Ponikwar and H.-J. Hof, "Beyond the Dolev-Yao Model: Realistic Application-Specific Attacker Models for Applications Using Vehicular Communication“, The Tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), Nice, France, July 2016, pp. 4-9.

[7] M. Woerner and H.-J. Hof, "Realistic Attacker Model for Smart Cities“, Applied Research Conference 2016, Poster, Augsburg, Germany, 2016.

[8] C. Ponikwar, H.-J. Hof, and L. Wischhof, „Towards a High-Level Security Model for Decision Making in Autonomous Driving“, ACM Chapters Computer Science in Cars Symposium 2017 (CSCS 2017), Munich, Germany, July 2017, pp. 1-4.

[9] M. S. Lund, B. Solhaug, and K. Stølen, Model-driven risk analysis: the CORAS approach. Springer Science & Business Media, 2010.

[10] A. Greenback, „The jeep hackers are back to prove car hacking can get much worse“, Wired, 08-Jan-2016. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. [last access: August 1st 2017].

[11] K. Axel, “Location-based services: fundamentals and operation,” John Wiely & Sons, 2005.