Establishing an Automotive Cyber Defense Center

Falk Langer[1][0000-0001-8780-0868] and Fabian Schüppel[2][0000-0003-4218-6459] and Lukas Stahlbock[3][0000-0002-4426-103X]

[1,2,3,4] IAV GmbH, Berlin, Germany

Abstract. As vehicles turn into human-transporting computers, more specific attention to the issue of long-term secure operation is needed. In order to prevent cyber-attacks on the fleet, monitoring the internal state of the individual vehicles' IT-infrastructure is required.
In this paper we provide a suggestion on how vehicles could be managed over the course of their lifetime. Establishment of an Automotive Cyber Defense Center is a key factor of ensuring the secure operation of the vehicle fleet by an OEM. Within this paper we demonstrate why establishing such a center is necessary, what kind of security operations it needs to perform and what stakeholders are involved in ensuring secure operation of public road transport.

Since Cyber Defense Centers and the required technology are well-established in classical IT-infrastructure, we propose an architecture for the automotive domain which uses these technologies, highlighting the gaps in transitioning from operating a network to operation of a vehicle fleet.

The most important difference being the distributed, inhomogeneous and nomadic nature of a vehicle fleet. In order to overcome this gap we provide an exemplary implementation, which aims to make security relevant information available for usage within a Cyber Defense Center, using IoT-technology.

Keywords: Cyber Defense Center, Secure Operation, Security Management, Security Monitoring.

1 Motivation

Today's vehicles have different online connections for instance for passenger entertainment systems, navigation with real time traffic, smartphone connections or software updates. In addition to these consuming services that are already on the market, vehicles will connect to each other and vehicles interact with public infrastructure (Vehicle-2-X/V2X) to realize future autonomous driving use cases. Consequently, there will be a distributed system with many different stakeholders, different services and different eco-systems with a huge attack surfaces that control public transportation. Due to this, a detailed consideration of (cyber) security in the vehicle is necessary.
At least since the online remote attack and wireless control of a Jeep in 2015 [1], security is also intensively investigated by the car manufacturers (OEMs). It becomes clear that with a hacked vehicle in addition to the economic damage personal injury can be

caused. Due to this, a cyber-security system known from typical IT systems is required to ensure the security of vehicles and subsequently transportation.
The case that the United Nations (UN) is taking this topic in focus indicates it is not only important for product quality from OEMs, but rather for well-being of humans. The "UN Task Force on Cyber security and OTA issues (CS / OTA)" defines the necessary parts of a cyber-security system. These include a cyber-security management and monitoring system with incident response.

2 State of the Art Cyber Defense Center

We observe that many different approaches, descriptions and definitions around cyber security management are used. To classify the context of this paper, in the following sections a short overview of definitions used within this context is provided and some exemplary announcements and publication with focus on the automotive domain are listed.

2.1 Terminology

The European Union has founded its European Union Agency for Network and Information Security in 2004, a new Cybersecurity Act was agreed upon in 2018. [8]

According to UNECE WP.29 ITS/AD from "UN Task Force on Cyber security and OTA issues (CS / OTA)" [2], a cyber-security management system (CSMS) is required to be established to support the security of vehicles throughout their lifetime. This complements the secure development techniques of vulnerability handling during development by reactive monitoring of cars even after production aligned to the security processes described in the upcoming ISO/SAE 21434 [3]. ·

This approach is already well known in several other businesses that protect their critical information infrastructure by an information security operation center (ISOC / SOC) and react to incidents in their systems or products through a computer or product security incident response team (CSIRT, PSIRT).

A well-established technique is the usage of a security information and event management (SIEM) system, which contains rules to match specific logging information on events to detect circumstances to react on suspicious behavior.

We intend to create such a security operation center (SOC) for the automotive business, with a dedicated opportunity to analyze and react to field incidents within vehicles, between vehicles and for the communication of data with backend systems of OEMs. That means that a Cyber Defense Center (CDC) is a composition of most of the above introduced elements for protecting a running IT system against attacks in the meaning to ensure a secure operation of this system.

2.2 Defining the role and task of an Automotive Cyber Defense Center

In the previous section a short introduction to different assets or roles for ensuring a secure operation of an IT system are shown. It can be stated out that the tasks of a Cyber Defense System are currently not clearly defined.
Some major players in the IT and automotive industry published their plans or concepts for similar Automotive Cyber Defense Center (ACDC). These ideas are driven from the concepts in the previous chapters mentioned and are extended by Automotive typical topics. Automotive typical topics are mostly the kind of information to deal with, the transport of this information to an SOC and the production and provisioning of updates (Update over The Air - OTA) to the vehicles.

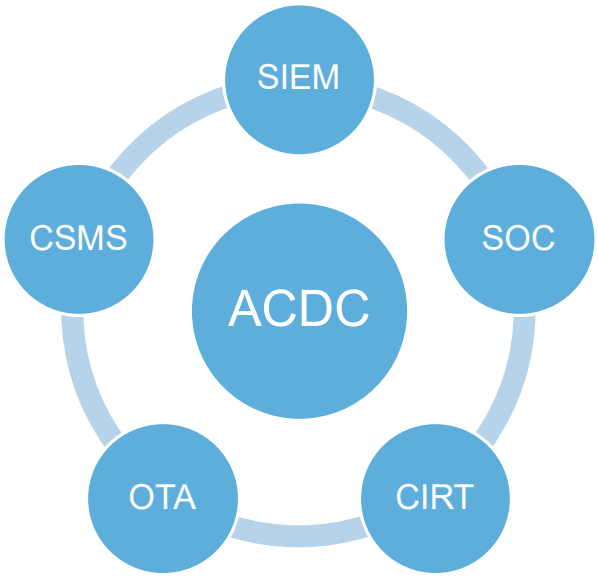

Fig. 1. ACDC is the agglomeration of different elements for ensuring secure operation of a system

In the following examples of automotive and non-automotive cyber defense systems are listed: Deutsche Telekom uses a cyber-defense system to protect their systems and customers systems [4] and are developing an automotive Cyber Defense Center [5]. In a research project at the Warwick University the vehicle security system restrictions for runtime and processing power is scrutinized [6]. The British Standards Institute is developing an automotive security standard motivated by autonomous driving [7], In a SAE survey 84% of automotive professionals have concerns that their organizational cybersecurity practices are not keeping pace with evolving technologies [9]. Bosch is introducing an integral approach for Automotive Security including Manufacturing IT-Security, Embedded IT-Security and Enterprise IT-Security [10]. Vector is mentioning the elements of a cyber defense center without combining them [11].

It can be stated out that all of this proposals are dealing with the basic elements provided in the previous chapter (compare **Fig. 1.**). The examples show that Automotive Cyber Defense Systems or Centers are in development. Today there is no commercial or un-commercial CDC for the automotive domain available for productive use. Especially no holistic solution, which fit to the boundaries of a vehicle.

3 Requirements from ISO and UNECE

There are two major sources of requirements regarding an ACDC. One the one hand there is the UNECE that announces in WP.29 ITS/AD a Cyber Security Management System for transportation systems. On the other hand there is the ISO/SAE 21434 „Road vehicles - Cybersecurity engineering“. To get an overview we summarize the major aspects from the UNECE WP.29 ITS/AD in [**Fig. 2**] and from the ISO/SAE 21434 in [**Fig. 3**] within this chapter.

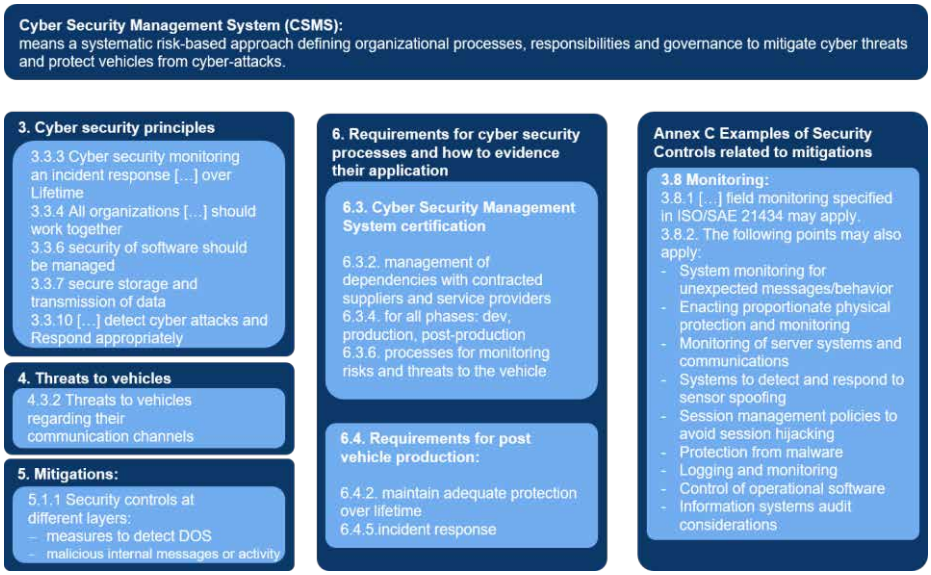

Fig. 2. Requirements from UNECE WP.29 ITS/AD: Cyber Security [2]

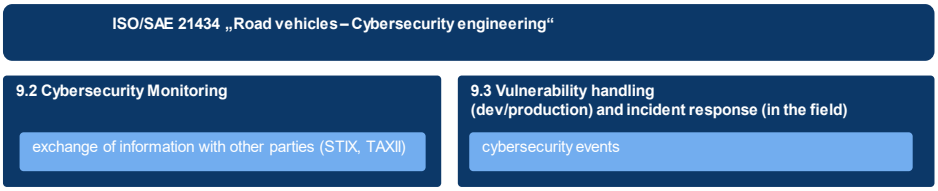

Fig. 3. Requirements from ISO/SAE 21434 “Road vehicles – Cybersecurity engineering” [3]

4 Introduction of an Automotive CDC

An Automotive CDC is a CDC adapted to the automotive environment.

4.1 Focus of protection by an ACDC

In contrast to a classical CDC an ACDC protects not only a single network or IT infrastructure, it has to observe and protect vehicles and services around transportation of human beings or goods within a public road infrastructure. In principle, there is the question of the system border of the system to protect. In case of an ACDC this is an important difference in contrast to a CDC.
In a simple view, one can assume that an ACDC has to observe the behavior of a single vehicle to protect the safety of the user of this vehicle. However, this perspective seems to be too restrictive. There are many scenarios where attacks of public infrastructure with the usage of infected cars are thought to be possible. Additionally, we talk about a distributed (IoT) system. It is well known that the proof of correct behavior in distributed system is difficult[1].
The overall goal is to protect the public transportation and all entities that can be damaged in case of security hazards. Therefore, the overall focus needs to be much more than the secure operation of single vehicle. It need to be the secure operation of services around transportation that control the behavior of vehicles in some way. This can be obviously attacks to cars itself, but also attacks to traffic information systems or V2X systems and many others.

4.2 Control Observing Layers

To get an idea of the different perspectives and system levels an ACDC need to care for, we suggest the following protection layers for transportation systems on public roads (compare **Fig. 4**).

1. Secure operation of public mobility (all vehicles in a public area)
2. Secure operation of OEM controlled Mobility Services
3. Secure operation of Vehicle Fleet
4. Secure operation of a single vehicle

[1] Lamport, Leslie "A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable." Email message sent to a DEC SRC bulletin board at 12:23:29 PDT on 28 May 87.

The elements that are operated are the vehicles themselves. Whereby the vehicle can be abstracted as a set of networks and nodes (ECUs). The vehicle operator runs these entities. We distinguish in

5. Protection of the network within the vehicle
6. Protection of a single entity (e.g. ECU) within the vehicle

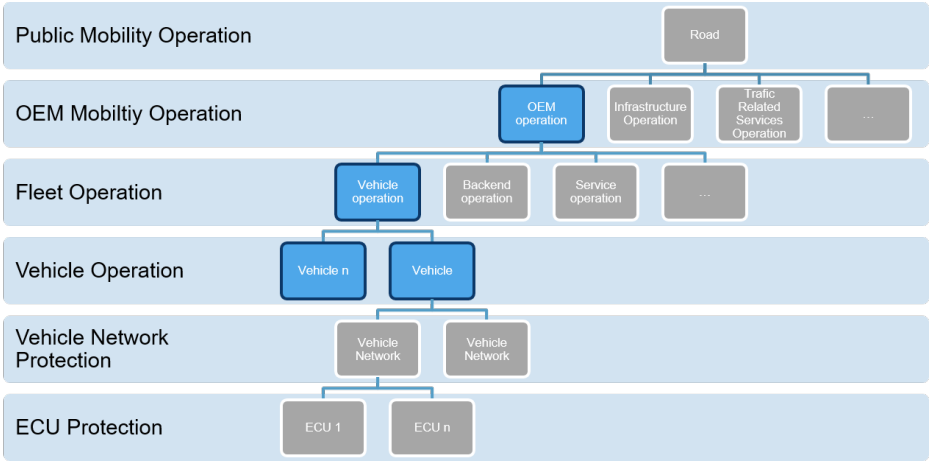

Fig. 4. Overview Operation Layer

The two lower layers Car-Network and ECUs provide the functionality for observing the status of the vehicle and are the acting entities in case of defense activities within the vehicle.

These different perspectives can be translated into different stakeholders and different level of

- Reaction time
- Criticality
- Autonomy
- Data aggregation
- Control-Flow

The relation between these different levels is shown in **Fig. 5**

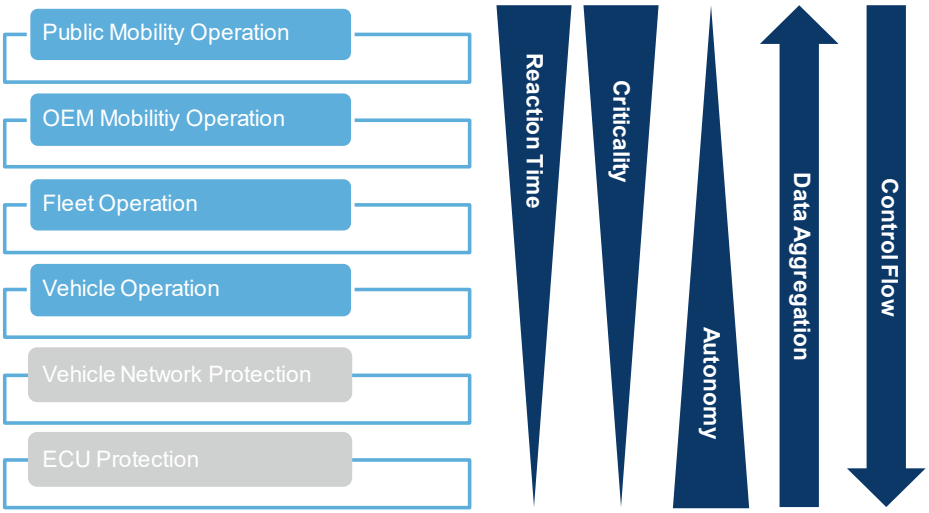

Fig. 5. Different perspectives and operation layers of an ACDC

5 Suggested Architecture of an ACDC

Based on reference architectures from other domains we define requirements for an ACDC and propose an architecture containing its essential elements. Furthermore, we show how our proposed architecture may be adapted for implementation.

5.1 Observing and Controlling Hierarchy

In order to monitor and control the secure operation of all layers different CDCs have to work together. The core elements of an ACDC are the Fleet Operation and Vehicle Operation layer because these are the link between embedded vehicle security mechanisms and typical IT SOCs. Therefore, we focus on designing a monitor and control architecture for these layers and define the following high-level requirements for it:

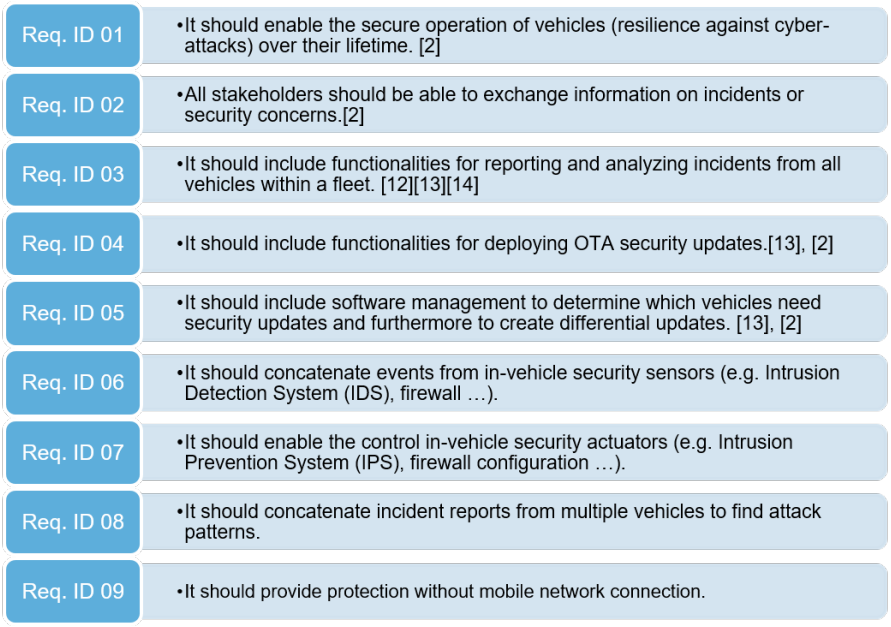

Fig. 6. Requirements for an ACDC architecture

To create a framework that fulfills these requirements we cannot completely follow an automotive standard since the ISO/SAE 21434 is not published yet but we will align our approach to the current draft version [3]. Furthermore, this standard will be created with respect to existing standards from other business sectors [15]. The connected vehicle can be seen as a thing in the IoT, which also leads to some similarities to industrial control systems (ICS). Therefore, we are adapting reference architectures from connected vehicles, IoT and ICS with respect to cyber security that show similarities to ACDC requirements and further are compliant with the IEC 62443 to create an ACDC framework.

A security architecture for ICS follows an adaption of the Purdue Enterprise Reference Architecture. It is based on defining security zones, which are a grouping of logical or physical assets that share common security requirements and conduit definition that are a path for the flow of information between two zones [16]. As proposed in [17] the security zones can be separated in Information Technology (IT) and Operational Technology (OT) which can be adapted to the layers in a way that the Public Mobility and OEM Mobility layer can be controlled with of-the-shelf IT SOCs; whereas the lower layers need OT SOCs with special automotive knowledge.

In [17] the cybersecurity reference architecture proposes three levels within the OT security zones that will be adapted to our framework:

1. I/O and devices
2. Control
3. Supervisory

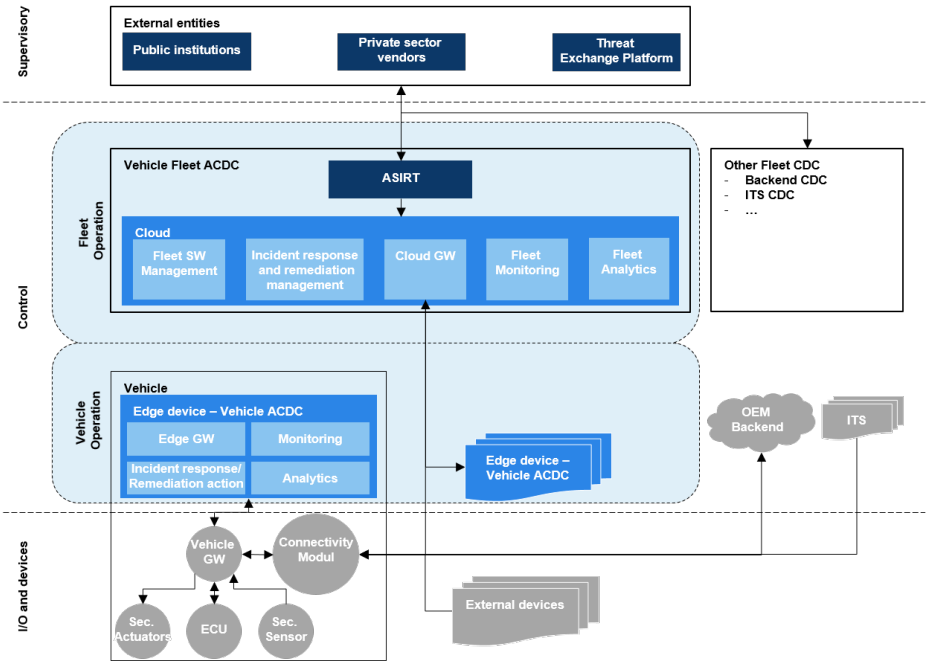

Fig. 7. ACDC architecture for Vehicle Operation layer and Fleet Operation layer

The suggested framework uses edge computing and is based on security design principles from [2] as well as reference architectures from similar domains. In [12] an intelligent SOC architecture is presented that shows a general framework but lacks an abstraction layer in order to use it for connected cars. In contrast to that, a framework for managing security incidents and response to attacks for connected cars is shown in [13]. An SOC is postulated that collects logs from the vehicle and is coordinated from an incident response team. Furthermore, an edge computing solution is provided in order to reduce mobile network traffic. This concept is heading in right direction but lacks a decomposition in multiple independent layers. Furthermore, using IDS more intelligence can be brought inside the vehicle by appending the scope of the cyber defense system. A multi-layer cybersecurity reference architecture as in [14] recommends an operations layer as well as an intelligence layer. The operations layer is responsible for security monitoring and incident response and is adapted as the vehicle operation layer. Similarly, the intelligence layer where detailed threat analysis is done is adapted as the fleet operation layer. The initial choice for using edge computing is because it experiences growing usage for connected vehicles [19], [20]. From a more technical point of view it can be stated that edge computing platforms deliver a variety of built-in functions for software deployment and log analysis [**Fig. 6**, Req. ID 04], [**Fig. 6**, Req. ID08]. Furthermore, compared to proprietary solutions using a 3rd party edge computing platform reduces time, development costs, infrastructure costs (serverless computing),

guarantees state of the art security mechanisms for the control level and facilitate co-operations between different OEMs.

The ECU and Vehicle Network Protection layers are abstracted as security sensors and security actuators because they are using embedded hardware or software security mechanisms that are not the focus of this framework. Within the Fleet Operation and the Vehicle Operation layer, a monitoring and analytics module will be implemented in order to detect incidents and analyze attack patterns [13], [14]. An incident response module will be responsible for reacting on certain incidents. Thereby, the modules on the edge device and on the cloud differ in terms of autonomy, reaction time and availability.

As part of the Vehicle Operation layer, the Vehicle ACDC acts as a comprehensive IDS and IPS that can autonomously initiate simple prevention actions like adapting firewall rules or displaying a warning to the driver. The functionality of the Vehicle ACDC does not depend on a cloud connection because the edge modules are always available within the vehicle [**Fig. 6**, Req. ID 09]. Every incident will also be forwarded by the Vehicle ACDC to the Fleet Operation layer for further investigation. Therefore, the Vehicle ACDC needs to persist incident information if no mobile network connection can be established. Further general data processing tasks within the Vehicle Operation layer that are not explicitly shown in [**Fig. 7**] will be adapted from [18]. Data is categorized to decide if higher level processing is needed (evaluation). For such higher level processing the data shall be in a consistent format (formatting). Furthermore, cryptic data is handled with additional information (expanding/decoding). Since vehicles and especially a vehicle fleet generate a lot of data it is summarized in order to reduce data and traffic on the vehicle network, mobile network and higher level processing systems (distillation/reduction). Data is processed to determine whether it represents a threshold or an alert (assessment).

The core element of the Fleet Operation layer is the ASIRT (Automotive SIRT) that is a collaboration of OEM specific security experts and external hunting teams from different domains (e.g. IT). The ASIRT will investigate incidents from single vehicles in a fleet and concatenate information from all vehicles to find anomalies within the fleet. In order to investigate incidents the ASIRT exchanges information with external entities like public institutions (e.g. researcher), private sector vendors (e.g. tier1, service provider) and threat exchange platforms (e.g. Open Threat Exchange). The ASIRT will initiate counter measures, which will be triggered by reported incidents from vehicle ACDCs, detected incidents from the fleet ACDC or reported threats from external entities. Counter measures can be security updates that will be deployed for the vehicle fleet, which leads to the necessity of a fleet software management module to identify all vehicles that need a certain update.

5.2 Exemplary Implementation

As a proof of concept we implement the architecture from [Fig. 7] using Microsoft's edge computing solution Azure IoT Edge due to the leading position on cloud and edge computing usages from automotive OEMs [19][21].
Each device must have at least an Edge Hub, an Edge Agent, a Container engine and a Security Daemon. The Edge Hub acts as a proxy for the IoT Hub (Cloud GW) and enables the inter module communication on each device. The Edge Agent instantiates modules and monitors their states. All modules in the cloud or on edge devices are executed within containers. Therefore, a container engine is required that is compatible with the open container initiative (e.g. Docker). The Security Daemon manages certificates and establishes secure in-device communication as well as device to cloud communication. Azure IoT Edge uses a HTTPS connection based on TLS1.2 with X.509 certificates for the device to cloud communication which is state of the art for secure communication above the transportation layer of the OSI model [22], [23].

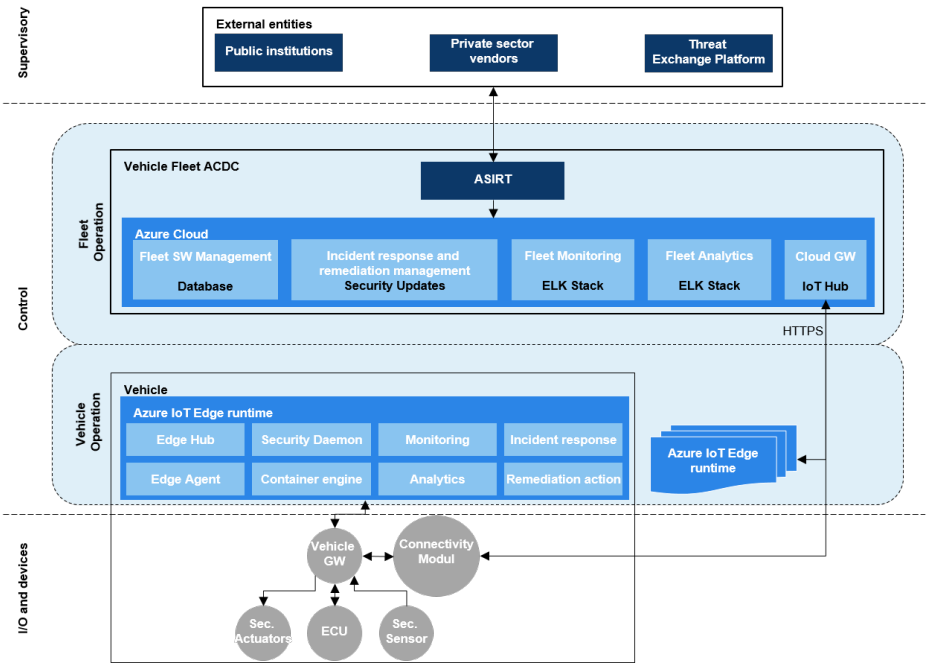

Fig. 8. ACDC architecture for exemplary implementation

The IoT Hub cares for the device provisioning and the routing of messages between all endpoints. The Fleet Monitoring and Fleet Analysis is realized by using the ELK stack (Elasticsearch, Logstash, Kibana); an open source project that can process and transform data from multiple sources simultaneously. The search engine is JSON-based for which reason logs and incident reports are forwarded in JSON-format. The ELK stack also provides a visualization tool that helps the ASIRT to investigate incidents [24].

The Fleet SW Management can be realized as a database that stores meta data from each vehicle. During the device provisioning an entry in the Fleet Software Management database is created that will further be updated whenever the software of a vehicle was changed. As remediation management actions security updates can be provided that contain update packages for ECUs. The vehicles remediation module will initiate an update process at a suitable time; that may be after the driver parked the vehicle at home and agreed to start the update process.

Considering the Vehicle Operation layer and Fleet Operation layer inter and intra layer communication require at least four interfaces in order to report incidents or deploy security updates:

1. interface to forward logs and security sensor events to the edge device.
2. interface to control security actuators.
3. interface to forward logs and vehicle meta data (e.g. position) to the cloud.
4. interface to initiate remediation actions and forward security updates.

6 Discussion and Outlook

As we have shown, the rising use of cyber security mechanisms due to potential threats in connected vehicles and their environments require multiple systems that manage the secure operation on different layers. In order to achieve secure transportation the secure operation of each layer as well as their interactions have to be established. Therefore, OEMs must instantiate a Security Operation Center and better Cyber Defense Center. Most of the technology is available. The most important new topic is transportation of information from vehicles to the operation center and provisioning of security actions like software or configuration updates to vehicles. For this, we recommend the use of IoT methods because they have been successfully integrated in other domains.

To ensure the secure operation of public road traffic the operation center of different OEMs and infrastructure must interact for exchanging information about possible attacks and vulnerabilities. OEMs need to think about architecture and interfaces for a Cyber Defense Center due to the need to build in support within their vehicles. It is very likely that OEMs will not operate Cyber Defense Centers by themselves.

In order to achieve this, we proposed an architecture that adapts architecture elements from other domains (e.g. ICS) and additionally considers requirements from UNECE WP.29 ITS/AD and ISO/SAE 21434.

6.1 Discussion

It can be stated out that the transport of data from the vehicle to the OEM's backend, the processing of the huge amount of result data, the requirements for privacy and last but not least the modalities an ACDC can operate a single vehicle are the critical topics that need be investigated in future. For transporting, storing and processing of data there are lot of mechanism that can be reused from other industries. But especially the topic of privacy needs to be discussed if one uses data from vehicles. If the observation of vehicles is required the legislator has to define boundaries how to use these information.

Furthermore for controlling the vehicle itself by an operator from an ACDC need automotive specific solutions, to ensure the safety and stability of the vehicle.

6.2 Outlook and future work

An evaluation for the proof of concept implementation provided within this paper needs to be done, to figure out its performance, limitations and scalability within this new use case for edge computing mechanism.

Additionally the manner of how an ACDC can operate a vehicle at runtime needs to be investigated. One of the already established mechanism is the online update functionality of vehicles. But updates are not feasible to react on threats in real-time. A possible solution may be preconfigured fallback scenarios within the vehicle which can be controlled by an operator. This or other solutions need to be investigated to find out there limitations and their capability to ensure the safety goals at vehicles control system.

Acknowledgement

This work is funded by the German Federal Ministry of Education and Research (BMBF) within the SecVI project.

References

1. Greenberg, A.: Hackers Remotely Kill a Jeep on the Highway - With Me in It, wired.com 21.7.2015, [https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, last accessed 2019/06/13
2. UN Task Force on Cyber security and OTA issues (CS/OTA) https://wiki.unece.org/download/attachments/81888965/TFCS-TPahCS2-04%20Draft%20Recommendation%20on%20Cyber%20Security%20-%20capturing%20suggested%20amendments%20from%20test%20phase%20participants.docx?api=v2, last accessed 2019/06/12
3. ISO/SAE CD 21434. International Organization for Standardization, “Road Vehicles -- Cybersecurity engineering”
4. Cyber Defense Center https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/details/im-zentrum-der-abwehr-348664 , last accessed 2019/06/12
5. Cybersecurity for Connected Cars (2018) https://www.t-systems.com/blob/842040/f76b6beae62a2a1523274cccca00a281/DL_WP_Cyberabwehr_vernetzte_Autos.pdf last accessed 2019/06/12
6. Mundhenk, P.: Security for Automotive Electrical/Electronic (E/E) Architectures. Cuvillier Verlag, Göttingen 2017 https://warwick.ac.uk/fac/sci/eng/staff/saf/publications/mundhenk-phdthesis2017.pdf
7. Burgess, R.: New cyber security standard to help prevent car hacking. Autocar 19 December 2018. https://www.autocar.co.uk/car-news/industry/new-cyber-security-standard-help-prevent-car-hacking , last accessed 2019/06/12

8. Krempl, S. : EU-Gremien einig: Sicherheit vernetzter Geräte soll zertifiziert werden. Heise online 11.12.2018 https://www.heise.de/newsticker/meldung/EU-Gremien-einig-Sicherheit-vernetzter-Geraete-soll-zertifiziert-werden-4247937.html. last accessed 2019/06/12
9. De Reno, M.: Special Report: Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices. SAE Mobilus 21.3.2019 https://saemobilus.sae.org/cybersecurity/feature/2019/03/special-report-securing-the-modern-vehicle-a-study-of-automotive-industry-cybersecurity-practices. last accessed 2019/06/12
10. Bits und Bytes in Berlin: Wie Bosch Auto, Herd und Fertigung vernetzt. Bosch Pressemeldung 6.5.2019 https://www.bosch-presse.de/pressportal/de/de/diese-highlights-zeigt-bosch-auf-der-bosch-connectedworld-2019-in-berlin-188608.html. last accessed 2019/06/12
11. Ebert, C., Metzker, E.: Cyber Security for the Automotive Industry- Practical experiences on the application of Cyber Security, vector informatik 9/2016 https://assets.vector.com/cms/content/know-how/_technical-articles/Security_Cyber_ElektronikAutomotive_201609_PressArticle_EN.pdf, last accessed 2019/06/13
12. ArcSight ESM flyer, https://www.microfocus.com/media/flyer/the_new_arcsight_enterprise_security_manager_is_here_introducing_esm_flyer.pdf, last accessed 2019/06/12
13. Sakurai, K., Kataoka, M., Kodaka, H., Kato, A., Teraoka, H., Kiyama, N.: Connected Car Solutions Based on IoT. In Hitachi Review vol. 67, No. 1, pp. 72-78
14. DXC Cyber Reference Architecture – White Paper, https://assets1.dxc.technology/security/downloads/DXC-Security-Cyber_Reference_Architecture.pdf, last accessed 2019/06/12
15. Schmittmer, C., Griessnig, G., Ma, Z.: Status of the Development of ISO/SAE 21434. In: Larrucea, X. et al. EuroSPI 2018, CCIS 896, pp. 504-513,2018
16. Whitepaper Industrial Security based on IEC 62443, https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf, last accessed 2019/06/12
17. Trend Micro Cybersecurity Reference Architecture for Operational Technology – White Paper, http://iiot-world.com/wp-content/uploads/2017/12/Trend-Micro-Cybersecurity-Reference-Architecture-for-Operational-Technology.pdf, last accessed 2019/06/12
18. The Internet of Things Reference Model – White Paper, http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf, last accessed 2019/06/12
19. Volkswagen Automotive Cloud, https://news.microsoft.com/de-de/volkswagen-und-microsoft-treiben-zusammenarbeit-bei-automotive-cloud-voran/, last accessed 2019/06/12
20. Ford Selects Wind River Over-the-Air Update Technology, https://www.windriver.com/news/press/pr.html?ID=21606, last accessed 2019/06/12
21. BMW continues to bet on the (Azure) cloud, https://techcrunch.com/2019/02/26/bmw-continues-to-bet-on-the-azure-cloud/?renderMode=ie11, last accessed 2019/06/12
22. Microsoft Azure IoT Edge dokumentation, https://docs.microsoft.com/de-de/azure/iot-edge/, last accessed 2019/06/12
23. Microsoft Azure IoT dokumentation, https://docs.microsoft.com/de-de/azure/iot-fundamentals/iot-security-deployment, last accessed 2019/06/12
24. ELK stack homepage, https://www.elastic.co/de/elk-stack, last accessed 2019/06/13