Cybersecurity Risk Analysis of an Automated Driving System*

Patrick Wagner[0000−0003−1133−6119], Nikolai Puch[0009−0000−6259−9846], and David Emeis[0009−0003−4960−944X]

Fraunhofer Institute AISEC {firstname}.{lastname}@aisec.fraunhofer.de

Abstract. New laws and technologies, but also persistent problems like truck driver shortage, have led to advances in the field of autonomous driving and consequently to new cyber risks. We present the results of our cybersecurity risk analysis for a Control Center-supervised Level-4 Automated Driving System (ADS), whose system model we created through expert interviews with a global truck manufacturer.
Example damage scenarios with high impact rating include *Disclosure of video data*, *Loss of ADS function in motion*, *Dangerous driving maneuvers*, and *Activation outside of Operational Design Domain*. We have identified over 200 threat scenarios, consisting of a combination of main attack steps that threaten specific parts of the item and preparation steps that determine how these parts are accessed and by which type of attacker. Without taking controls into account, the realization of these threat scenarios results in 65 significant risks.
We propose to treat the threat scenarios, on the one hand, by claims concerning implementation-relevant aspects and the attacker model, and on the other hand, by safety controls such as *Detection of system failure* and security controls such as *Authentic transmission of data*.
We conclude by detailing principles we have extracted from our analysis that can be applied to other cybersecurity risk analyses of automated driving systems.

Keywords: Cyber Security · Risk Analysis · Automated Driving · Truck · Logistics.

1 Introduction

Nowadays, a lot of research is being conducted on the use of Automated Driving Systems (ADSs) [14,10]. In the truck sector, in particular, the use of SAE J3016 Level-4 ADSs [22] seems inevitable, as there has been a sharp decline in truck drivers in recent years [13]. In Germany, a law was passed in 2021 that allows the operation of autonomous vehicles in approved areas of transport under specific conditions, such as technical supervision by a Control Center (CC) [9].

* The authors are grateful to the Federal Ministry for Economic Affairs and Climate Action of Germany for supporting this work by funding the project ATLAS-L4 within the research program *Neue Fahrzeug- und Systemtechnologien.*

The use of new technologies introduces new cyber risks. The UN Regulation No. 155 [25] and the international standard ISO/SAE 21434 [11] provide a fundamental framework to address these cyber risks in the automotive domain. However, there is a lack of concrete guidance on how Level-4 ADSs should be protected against cyber attacks, especially with regard to hub-to-hub transportation and connected and autonomous trucks. We aim to close this gap by presenting our results of a Cybersecurity Risk Analysis (CRA) conducted for a CC-supervised Level-4 ADS for trucks using the Modular Risk Assessment (MoRA) method [1].

To this end, we provide an introduction to the MoRA method in Section 3. We then present the results of our CRA in Section 4, starting with the item definition in Section 4.1. Damage scenarios that can be caused by cyber attacks on the item are specified in Section 4.2. Furthermore, claims regarding the scope and attacker model as well as controls and their effects are detailed in Section 4.3. Subsequently, in Section 4.4, we present threat scenarios with the highest risk values and show which controls should be implemented to reduce them to acceptable levels. Concluding, we summarize our findings and detail principles we have extracted from our CRA that can be applied to other CRAs of ADSs in Section 5.

2 Related Work

Currently, no uniform model for an ADS from the security perspective exists, but some common characteristics can be observed in the literature. A slim model consisting of perception, network, and ADS application/control is often used for risk analyses [2] and the exploration of security challenges for ADSs [8]. In more detailed models an ADS is described as a pipeline in which sensors like GPS, LiDAR, or Cameras detect environmental states, which may be fused with supplemental information. This data is then used for object detection/tracking and localization and then is used for assessment and behavior prediction, which in turn powers planning and finally the control module to operate the actuators. Those actions lead then to a new environmental state and thus start the control loop anew [28,7]. This model is often extended with Vehicle-to-Everything (V2X) communication, like map updates or communication for platooning [10,7].
Multiple authors analyzed the security of Connected and Autonomous Vehicles (CAVs) by looking at published attacks and defenses [10,8,14]. Their analysis can be grouped into the four domains of sensing, control, in-vehicle communication, and V2X communication. For sensing attacks, GNSS spoofing [18] or ultrasonic jamming [27] are common and increasingly publications focus on attacks against the machine learning models, which interpret LiDAR or camera data to detect obstacles, road users, or traffic signs [5,4,20]. For the control domain, there are several known attacks on Electronic Control Units (ECUs), focusing on telematics and infotainment systems due to their connected nature [24]. In-vehicle communication still uses protocols like CAN, LIN, and FlexRay, which were not designed with security in mind. Thus, the protocols are vulnerable to, e.g., eaves-

dropping, or Spoofing or manipulating (S/M) attacks [23,15]. V2X spans a broad range, starting with the communication between key fobs and locking systems, which are notoriously vulnerable [26]. The expansion to Vehicle-to-Vehicle or Vehicle-to-Infrastructure communication also opens the avenue for new attack possibilities, using sybil or impersonation attacks [16].
An often-referenced CRA method is RACE, which was proposed by Boudguiga et al. in 2015 [3]. They extend the EVITA Framework with an improved attack tree and attack techniques and limit the attack methods to five types. The risk is then calculated as the sum of controllability and the product of severity and attack likelihood. However, they do not conduct a detailed analysis of a CAV but instead did go into more detail in their follow-up paper [17]. Park et al. focus on simplifying the risk analysis process [19]. To calculate the risk, they sum up the four risk categories *probability*, *impact*, *exposure*, and *recovery*, which in turn are comprised of three risk factors. The factors are weighted and then evaluated to determine the score of a category. Their analysis focuses on the main functions of CAVs: Automotive over-the-air (OTA) functions and collision avoidance. The initial risk in their method is critical for OTA, which is lowered to a minor risk by checking for known vulnerability signatures, verifying software signatures, using Intrusion Detection and Prevention Systems (IDPSs), and encryption in transit. For the collision avoidance function the initial risk is minor and is transformed to negligible by the addition of IDPSs, secure flashing and boot, and secure OTA patching. Cui et al. were the first to consider the human control capability and the vehicle automation level with their Method VeRA which additionally focused on efficiency and ease of use [6]. VeRA describes the risk as the product of *attack probability* and *severity* and adds *human control*. To calculate *attack probability* necessary *equipment* and *knowledge* are evaluated and *severity* is evaluated in the categories *safety*, *privacy*, *finance*, and *operational*. For *human control*, the driver's experience and the vehicle's automation level are taken into account. Cui et al. conduct a case study to test VeRA and compare it against other methods. Three different automation levels and two features are evaluated: the first feature *cognitive driving intelligence system* consists of seven subfunctions and 116 detailed attacks are analyzed for it. The second feature *vehicle manipulation system* consists of three subfunctions, for which 264 detailed attacks are analyzed.

3 Method

We chose MoRA as our method because it is scientifically sound, compliant with ISO/SAE 21434, and already established in the automotive industry [1]. Figure 1 shows its main activities.

In *Item Definition*, the Target of Evaluation (TOE) is divided into its functions, data, components, and data flows. In addition, assumptions about the scope and attacker model are defined as claims. In *Asset Identification & Impact Rating*, damage scenarios in the impact categories *safety, financial, operational*, and *privacy* are identified. They are caused if an attacker violates the assets in

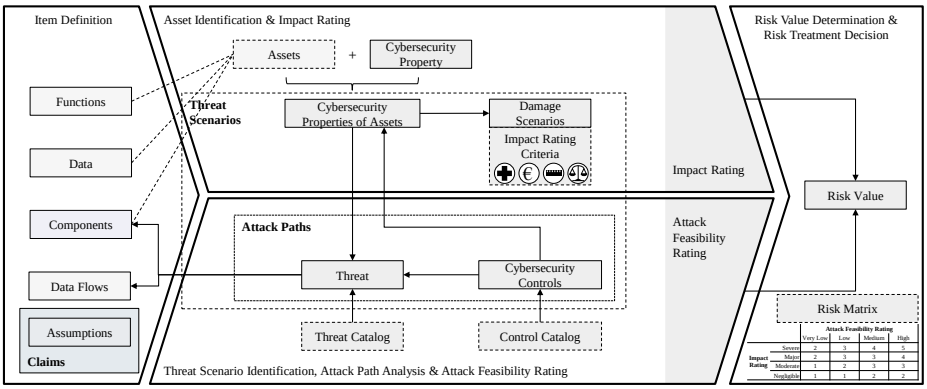

Fig. 1. Main MoRA activities, taken from [1] with adaptations to ISO/SAE 21434 terminology. The risk matrix for our CRA is shown in the bottom right corner.

terms of their security properties confidentiality, availability, or integrity. Each damage scenario is assigned an impact rating. For each Cybersecurity Property of an Asset (CSPA), the possible damage scenarios are specified. The next activity identifies threats to the CSPAs, attack paths to realize these threats, and controls that mitigate them. The attack feasibility rating of each threat and control is estimated using an attack potential-based approach [12]. Threat and control catalogs can be used to achieve comparable results across multiple CRAs. In the final activity, a risk value is determined for each threat by combining the impact ratings of all threatened CSPAs with the threat's attack feasibility rating according to a defined risk matrix.

4 Cybersecurity Risk Analysis of a Level-4 Automated Driving System

In the following subsections, an excerpt of the most relevant aspects of our CRA is presented.

4.1 Item Definition

We created the system model for the ADS based on expert interviews with employees of a global truck manufacturer. The ADS consists of six main components: *Perception*, *Prediction*, *Planning*, and *Control* form the control loop that enables environment awareness and autonomous driving within the Operational Design Domain (ODD). In addition, *System Management* monitors the health of ADS-relevant components and initiates Minimum Risk Maneuvers (MRMs) when necessary. Furthermore, *Mission Control* establishes communication with the external *CC*. Table 1 details the functions, data, and components of the item, and an architectural overview is shown in Figure 2.

Table 1: Functions, data, and components of the TOE, split by dashed lines. (Excerpt)

Name	**Description**
Collect Data	Sensors, CC, and Base Vehicle Monitoring transmit vehicle and environment data to Perception
Perform DDT	The ADS core components interact with each other in order to plan trajectories and send control commands to the actuators
Perform MRM	An MRM is triggered, e.g., by the CC or System Management, and subsequently performed by the vehicle
Virtual sensor data	CC sensor input to ADS, e.g., digital map data (incl. life traffic data), V2X communication (incl. traffic light status)
Base vehicle input	E.g., battery status, range, navigation information, egoself-awareness (e.g., wheel speed)
Raw video feed	Environment data captured via cameras
Sensor data	Vehicle and environment data, e.g., radar and LiDAR data, tire pressure, inertial measurement unit data
Fused sensor data	Raw video feed, sensor data, and virtual sensor data plausibility checked and fused
Planned trajectory	The truck's planned trajectory based on fused sensor data and object trajectories
Object trajectories	Predicted trajectories of objects
Dynamic adjustment	If the planned trajectory cannot be executed (e.g., because the tire pressure is not optimal or the battery cannot provide enough power), the planning is dynamically adjusted
Base vehicle output	Control commands of the automated driving function to the actuators, e.g., braking or steering
Initiate MRM	Trigger to perform an MRM
Truck	An ADS-equipped truck designed for driverless operation under routine/normal operating conditions during all trips within its given ODD [22]
Automated Driving System	The hardware and software that are collectively capable of performing the entire DDT on a sustained basis [22]; Level-4 driving automation system
Sensors	E.g., cameras, radars, LiDARs, tire pressure sensors, inertial measurement unit
Control Center	Provides an interface to remotely control and monitor driverless trucks
Perception	Collects information and extracts relevant knowledge from the environment. Tasks include locating obstacles, detecting road signs and markings, and determining the truck's position within the environment [21]
Prediction	Predicts future states of the driving environment, such as object trajectories [21]
Planning	Makes purposeful decisions in order to bring the vehicle from a start location to a target location while avoiding obstacles [21]
Control	Executes the planned actions by commanding the actuators [21]
Mission Control	Part of the ADS responsible for communication with the CC
System Management	Part of the ADS responsible for health monitoring and initiating MRMs
Actuators	E.g., brake or steering ECU
Base Vehicle Monitoring	ECUs that send inputs, such as egoself-awareness data, to Perception

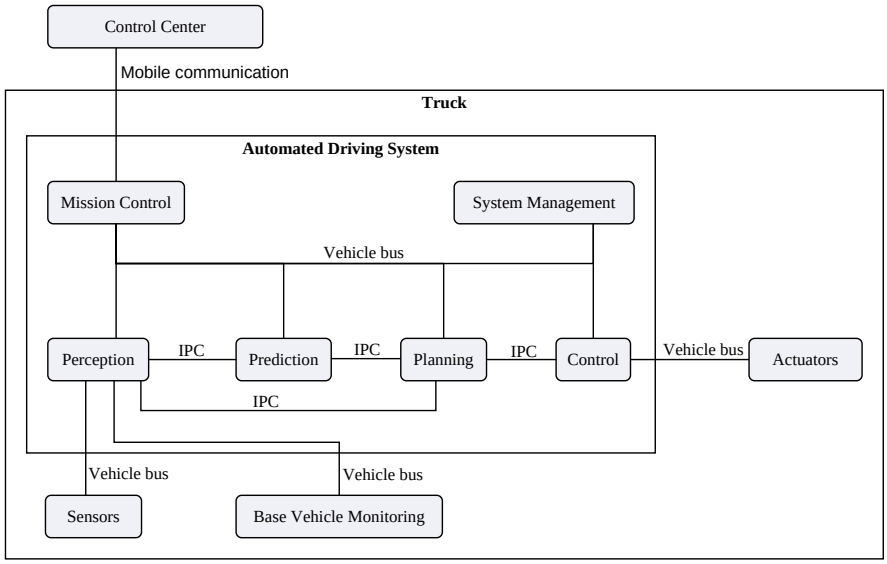

Fig. 2. ADS diagram showing the components and their connections; IPC stands for Inter-Process Communication.

In general, the communication flow to perform the Dynamic Driving Task (DDT) is as follows: *Sensors*, *Base Vehicle Monitoring*, and *CC* transmit information about the environment and the vehicle to the control loop. The control loop processes the information and sends control commands to *Actuators*. MRMs can be triggered by *System Management* or *CC*. The communication flow is visualized in Figure 3.

4.2 Damage Scenarios

If an attacker succeeds in violating the security properties confidentiality, integrity, or availability of parts of the TOE, a number of damage scenarios in the impact categories *safety, financial, operational*, and *privacy* can be caused, which are listed in Table 2.

Table 2: Damage scenarios for the TOE; Impact classes: S-Safety, F-Financial, O-Operational, P-Privacy; Impact rating: 0-Negligible, 1-Moderate, 2-Major, 3-Severe. (Excerpt)

Name	**Description and Rationale**
Disclosure of video data	P2: Multiple persons might be recognizable, General Data Protection Regulation violation
Loss of ADS function at rest	O2: Vehicle startup not possible

Continued on next page

Table 2: Damage scenarios for the TOE; Impact classes: S-Safety, F-Financial, O-Operational, P-Privacy; Impact rating: 0-Negligible, 1-Moderate, 2-Major, 3-Severe. (Excerpt) (Continued)

Loss of ADS function in motion	S3: Collisions possible, road users might suffer life-threatening injuries
Falsely triggering an MRM	O2: Vehicle stops on the hard shoulder
ADS function limited or loss of subcomponents	O1: Service required to restore full functionality
Dangerous driving maneuvers	S3: Manipulated ADS functionality could lead to collisions, road users might suffer life-threatening injuries
Activation outside of ODD	S3: Unsafe driving conditions on certain road sections where automated driving is not allowed could lead to life-threatening injuries F3: Violation of laws could lead to substantial financial damage for the fleet operator
Incorrect route planning for single vehicle	F0: Increased battery consumption
Temporary disturbance	O0: Temporary disturbance with no further impact

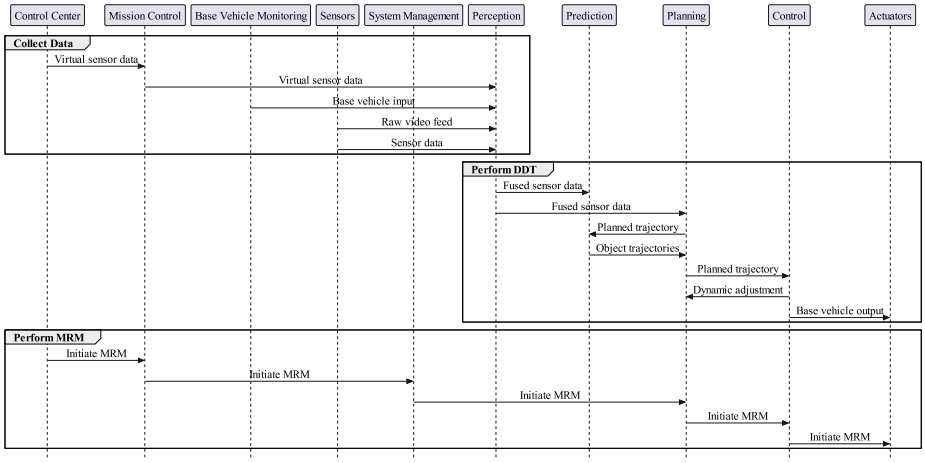

Fig. 3. Communication sequences showing the sender and receiver of each data flow, divided into the three functions.

4.3 Claims and Controls

The threat scenarios are treated by claims, which either mitigate or transform damage scenarios or have an effect on the attack feasibility ratings. Claims concern the scope of the analysis, e.g., *Attacks on the CC are not in scope*, or the attacker model, e.g., *Limited scope for tuning attacks*. Additionally, important implementation-relevant aspects that must be verified during the development of the TOE are specified in claims, e.g., *Remote attacks selectively considered* which specifies to which vehicle bus a remotely-accessible ECU is attached, or *MRM triggered by CC are not safety-critical*. They are listed in Table 3.

Table 3: Claims for the TOE; DS-Damage scenarios; AF-Attack feasibility rating; R-Risk value; > reads as "set to"; strikethrough reads as "removes"; {} means all contained values. (Excerpt)

Name	**Description**	**Effect on DS, AF or R**
Attacks on the CC are not in scope	The CC is assumed to be protected against internal and external attacks	R > 2
Limited scope for tuning attacks	A vehicle owner/tuner only causes damage scenarios that are in their interest	~~All damage scenarios~~ except Activation outside of ODD
Quality damages selectively considered	If the attacker has access to a truck bus or a component, then quality/operational damages caused by the TOE are not further relevant. If the truck is compromised by an attacker, a workshop visit should be made anyway, during which an integral state is restored	~~All operational damage scenarios~~
MRMs triggered by CC are not safety-critical	MRMs that are triggered by the CC are not safety-critical. In conclusion, no safety damages can occur if an attacker disrupts the transmission of this signal	~~Loss of ADS function in motion~~
Limited jamming of mobile radio	An attacker can only disrupt mobile radio connections temporarily and in proximity to the truck. Jamming attacks to trucks at rest can be recognized and further actions can be taken	{Loss of ADS function at rest, Falsely triggering an MRM, ADS function limited or loss of subcomponents} > Temporary disturbance
Remote attacks selectively considered	The truck's connections are split into online buses, which have at least one ECU with wireless interfaces (e.g., WiFi) attached, and offline buses. It is assumed that ECUs with wireless interfaces can be remotely compromised and attacks via the attached online buses are possible. It is further assumed that remote attacks on offline buses and their attached ECUs are infeasible. If it seems likely that an offline bus will be fitted with an after-market device with wireless interfaces, it will be treated as an online bus	AF > Very Low
Local attackers	Protecting against attacks from an external attacker that require physical access to ADS-relevant connections and components using security controls is not effective because the attacker has easier ways to cause life-threatening damage (e.g., disconnecting the brake lines)	~~Loss of ADS function in motion, Dangerous driving maneuvers, Activation outside of ODD~~
Confidential data is only processed in transit and not stored	Hardware attacks on components where this claim is applied cannot lead to Disclosure of video data, since this data is only processed in transit and not stored	~~Disclosure of video data~~
Risk independent of ADS	Risks where this claim is assigned exist independent of the ADS; in particular: manipulating control commands to actuators	R > 2

The threat scenarios are also treated by controls, which effect damage scenarios or attack feasibility ratings. Safety controls such as *Detection of system failure*, as well as security controls such as *Authentic and encrypted transmis-*

sion of data or *Denial of Service (DoS) protection for safety-critical components* are necessary to lower the risk values to an acceptable level. The most relevant controls are listed in Table 4.

Table 4: Controls proposed for the TOE; DS-Damage scenarios; AF-Attack feasibility rating; > reads as "set to"; strikethrough reads as "removes"; {} means all contained values. (Excerpt)

Name	**Description and Rationale**	**Effect on DS or AF**
Detection of system failure	Attacks on the availability of a safety-relevant signal do not endanger safety, but merely trigger an MRM The truck also performs an MRM when the connection to the CC is lost for a number of minutes	Loss of ADS function in motion > Falsely triggering an MRM
TLS between CC and Mission Control	The mobile connection between CC and Mission Control is secured using mutually authenticated Transport Layer Security in version 1.3 or higher. Secure, trustworthy certificate authorities are used. The certificates are validated. Trustworthy, restricted trust stores are used. Private keys are handled securely	AF > Very Low
Validation of sensor data through sensor fusion	Attacks on the integrity of data from a single sensor do not endanger safety, but merely trigger an MRM	{Loss of ADS function in motion, Dangerous driving maneuvers} > Falsely triggering an MRM
Redundancy against activation of ADS outside of ODD	Spoofing or manipulating a single input signal that is used to determine the ODD boundaries cannot lead to an activation of the ADS outside of the ODD The ODD boundaries are determined by the vehicle by *localization (GNSS etc.) *sensor data (lanes, signs etc.)	~~Activation outside of ODD~~
Authentic transmission of data	Authentic transmission of data. The data is signed by the sender and the signature is verified by the receiver	AF > Very Low
Encrypted transmission of confidential data	Encrypted transmission of confidential data to preserve privacy of road users	~~Disclosure of video data~~
DoS protection for safety-critical components	Attacks on ECUs where this control is applied cannot lead to the loss of availability of the functionality to perform MRMs; Simple flooding attacks are recognized and the communication to the sending ECUs is rate-limited or terminated	Loss of ADS function in motion > Falsely triggering an MRM
Hardening against remote attacks	Robust implementation of software, following secure coding guidelines, cybersecurity (penetration) testing, code reviews etc. to reduce the probability of software vulnerabilities	AF > Low (The probability of a software vulnerability exists, even when precautions are taken)
End-to-end signature of virtual sensor data	Virtual sensor data is signed by the CC and the signature is verified by Perception. This prevents that an attacker injects their own map data, possibly by compromising Mission Control, which could lead to dangerous driving maneuvers	~~Dangerous driving maneuvers, Activation outside of ODD~~

4.4 Threat Scenarios and Risks

The TOE 's security properties are threatened by a total of 216 threat scenarios, consisting of a combination of 84 main attack steps and 13 preparation steps. The main attack steps systematically threaten the confidentiality, availability,

and integrity of the data flows and components of the TOE, while the preparation steps determine how they are accessed (e.g., physical or remote) and by which kind of attacker (e.g., vehicle owner/tuner or external attacker). Table 5 shows an excerpt of some of the most critical threat scenarios for the ADS.

Table 5: Threat scenarios for the TOE; IR-Impact rating, S-Severe, Ma-Major; AF-Attack feasibility rating, H-High, M-Medium; R_b-Risk value before controls. (Excerpt)

Attack Path	**Claim**	**Damage Scenarios**	**IR**	**AF**	$\mathbf{R_b}$
Eavesdropping between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as an external attacker		Disclosure of video data	Ma	H	4
Disrupting Base vehicle input between Base Vehicle Monitoring and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU	Quality damages selectively considered	Loss of ADS function in motion	S	H	5
S/M Raw video feed between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner	Limited scope for tuning attacks	Activation outside of ODD	S	H	5
S/M Raw video feed between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner AND Attacking more than one connection to overcome sensor fusion or redundancies	Limited scope for tuning attacks	Activation outside of ODD	S	M	4
S/M Virtual sensor data between CC and Mission Control		Loss of ADS function at rest, Falsely triggering an MRM, ADS function limited or loss of subcomponents, Dangerous driving maneuvers, Activation outside of ODD, Incorrect route planning for single vehicle	S	H	5
S/M Virtual sensor data between CC and Mission Control, prep. by Attacking more than one connection to overcome sensor fusion or redundancies		Loss of ADS function at rest, Falsely triggering an MRM, ADS function limited or loss of subcomponents, Dangerous driving maneuvers, Activation outside of ODD, Incorrect route planning for single vehicle	S	M	4
S/M Virtual sensor data between Mission Control and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner AND Attacking more than one connection to overcome sensor fusion or redundancies	Limited scope for tuning attacks	Activation outside of ODD	S	M	4
S/M Virtual sensor data between Mission Control and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU AND Attacking more than one connection to overcome sensor fusion or redundancies	Quality damages selectively considered	Dangerous driving maneuvers, Activation outside of ODD, Incorrect route planning for single vehicle	S	M	4

Continued on next page

Table 5: Threat scenarios for the TOE; IR-Impact rating, S-Severe, Ma-Major; AF-Attack feasibility rating, H-High, M-Medium; R_b-Risk value before controls. (Excerpt) (Continued)

S/M Base vehicle input between Base Vehicle Monitoring and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU AND Attacking more than one connection to overcome sensor fusion or redundancies	Quality damages selectively considered	Loss of ADS function in motion, Dangerous driving maneuvers	S	M	4
S/M Fused sensor data, Object trajectories, or Planned trajectory between core ADS components, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner	Limited scope for tuning attacks	Activation outside of ODD	S	M	4
S/M Initiate MRM between CC and Mission Control	MRM triggered by CC are not safety-critical	Falsely triggering an MRM	Ma	H	4
DoS attack on core ADS components or System Management, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU	Quality damages selectively considered	Loss of ADS function in motion	S	H	5
Manipulating data, parameters or software of Mission Control, prep. by Attacking via remote interfaces		All Damage Scenarios possible, except Disclosure of video data	S	M	4

The application of the controls to the threat scenarios and their effects on damage scenarios, attack feasibility ratings, and risk values is shown in Table 6. Taking claims and controls into account, the realization of these threat scenarios results in only one significant risk. The remaining risk with value 3 concerns the exploitation of software vulnerabilities on *Mission Control*, which is the endpoint for external communication. In the context of this CRA, it is not ruled out that this remotely accessible component is compromised by a software vulnerability. However, to reduce the likelihood as much as possible, *Hardening against remote attacks* which includes robust implementation of software, following secure coding guidelines, cybersecurity (penetration) testing, and code reviews is proposed. In addition, safety impacts can be prevented by end-to-end signing the *Virtual sensor data* by the *CC* and verifying it in *Perception*.

Table 6: Controls applied to the threat scenarios of the TOE; IR-Impact rating, S-Severe, Ma-Major, N-Negligible; AF-Attack feasibility rating, H-High, L-Low, V-Very low; R_a-Risk value after controls; strikethrough reads as "removes". (Excerpt)

Attack Path	**Controls**	**Damage Scenarios**	**IR**	**AF**	$\mathbf{R_a}$
Eavesdropping between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as an external attacker	Encrypted transmission of confidential data	~~Disclosure of video data~~		H	1

Continued on next page

Table 6: Controls applied to the threat scenarios of the TOE; IR-Impact rating, S-Severe, Ma-Major, N-Negligible; AF-Attack feasibility rating, H-High, L-Low, V-Very low; R_a-Risk value after controls; strikethrough reads as "removes". (Excerpt) (Continued)

Disrupting Base vehicle input between Base Vehicle Monitoring and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU	Detection of system failure	~~Loss of ADS function in motion~~		H	1
S/M Raw video feed between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner	Validation of sensor data through sensor fusion, Redundancy against activation of ADS outside of ODD	~~Activation outside of ODD~~		H	1
S/M Raw video feed between Sensors and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner AND Attacking more than one connection to overcome sensor fusion or redundancies	Authentic transmission of data, End-to-end signature of virtual sensor data	~~Activation outside of ODD~~		V	1
S/M Virtual sensor data between CC and Mission Control	TLS between CC and Mission Control, Validation of sensor data through sensor fusion, Redundancy against activation of ADS outside of ODD, End-to-end signature of virtual sensor data	Loss of ADS function at rest, Falsely triggering an MRM, ADS function limited or loss of subcomponents, ~~Dangerous driving maneuvers~~, ~~Activation outside of ODD~~, Incorrect route planning for single vehicle	Ma	V	2
S/M Virtual sensor data between CC and Mission Control, prep. by Attacking more than one connection to overcome sensor fusion or redundancies	TLS between CC and Mission Control, End-to-end signature of virtual sensor data	Loss of ADS function at rest, Falsely triggering an MRM, ADS function limited or loss of subcomponents, ~~Dangerous driving maneuvers~~, ~~Activation outside of ODD~~, Incorrect route planning for single vehicle	Ma	V	2
S/M Virtual sensor data between Mission Control and Perception, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner AND Attacking more than one connection to overcome sensor fusion or redundancies	Authentic transmission of data, End-to-end signature of virtual sensor data	~~Activation outside of ODD~~		V	1
S/M Virtual sensor data between Mission Control and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU AND Attacking more than one connection to overcome sensor fusion or redundancies	Authentic transmission of data, End-to-end signature of virtual sensor data	~~Dangerous driving maneuvers~~, ~~Activation outside of ODD~~, Incorrect route planning for single vehicle	N	V	1

Continued on next page

Table 6: Controls applied to the threat scenarios of the TOE; IR-Impact rating, S-Severe, Ma-Major, N-Negligible; AF-Attack feasibility rating, H-High, L-Low, V-Very low; R_a-Risk value after controls; strikethrough reads as "removes". (Excerpt) (Continued)

S/M Base vehicle input between Base Vehicle Monitoring and Perception, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU AND Attacking more than one connection to overcome sensor fusion or redundancies	Authentic transmission of data, End-to-end signature of virtual sensor data	Loss of ADS function in motion, ~~Dangerous driving maneuvers~~	S	V	2
S/M Fused sensor data, Object trajectories, or Planned trajectory between core ADS components, prep. by Gaining physical access to vehicle electronics as vehicle owner/tuner	Authentic transmission of data	Activation outside of ODD	S	V	2
S/M Initiate MRM between CC and Mission Control	TLS between CC and Mission Control	Falsely triggering an MRM	Ma	V	2
DoS attack on core ADS components or System Management, prep. by Gaining access to an online vehicle bus via remote compromise of a connected ECU	DoS protection for safety-critical components	~~Loss of ADS function in motion~~		H	1
Manipulating data, parameters or software of Mission Control, prep. by Attacking via remote interfaces	End-to-end signature of virtual sensor data, Hardening against remote attacks	All Damage Scenarios possible, except Disclosure of video data and Damage Scenarios with safety impact	Ma	L	3

5 Conclusion

5.1 Principles for conducting Cybersecurity Risk Analyses on Automated Driving Systems

We have identified 18 damage scenarios, 216 threat scenarios, 11 claims, and 20 controls, and refined them in several discussions with a global truck manufacturer. We have extracted the following principles from our CRA to help future cybersecurity analysts to focus on the critical aspects of their CRAs on ADSs.

Threat scenarios that violate asset confidentiality must be adequately mitigated by controls if *Disclosure of video data* can be elicited by tapping *Raw video feed* on mobile connections, online buses, or vehicle buses that can be accessed by minor destruction from the vehicle exterior.

Threat scenarios that violate asset availability must be adequately mitigated by controls if *Loss of ADS function in motion* can be elicited by loss of data on online buses or DoS attacks via online buses on components to shut down their functionality. Controls are also necessary if *Loss of ADS function at rest* or *Falsely triggering an MRM* can be elicited by DoS attacks on components directly reachable via an external wireless interface (*Mission Control* in our example).

Threat scenarios that violate asset integrity must be adequately mitigated by controls for all data transmitted on mobile connections. This is also required

if *Activation outside of ODD* (tuning interest) can be elicited by spoofing or manipulating the input signals to the *Perception (Raw video feed, Virtual sensor data)* or signals in the ADS control loop *(Fused sensor data, Object trajectories, Planned trajectory)*. Controls are also necessary if *Dangerous driving maneuvers* or *Activation outside of ODD* can be elicited by spoofing or manipulating data on online buses *(Virtual sensor data, Base vehicle input)*, or by remote attacks where components could be compromised by exploiting software vulnerabilities. This is especially the case for components that are the endpoint of an external communication (*Mission Control* in our example). Here, safety damage scenarios can be prevented by end-to-end signing the *Virtual sensor data* by the *CC* and verifying it in *Perception*.

For all aspects, it must be taken into account that attackers may be able to attack more than one connection, so that controls such as *Validation of sensor data through sensor fusion* or *Redundancy against activation of ADS outside of ODD* may not be effective in this case.

5.2 Future Research Work

In order to achieve a holistic view of cyber risks, not only the ADS and its interfaces, but also other entities involved must be assessed. On the one hand, this concerns systems that are also used in vehicles at lower levels of autonomy but are now commanded by the ADS, such as the actuators. On the other hand, systems that are specifically intended for autonomous driving in Level-4, such as the *CC*, should be subjected to a detailed CRA.

References

1. Angermeier, D., Beilke, K., Hansch, G., Eichler, J.: Modeling security risk assessments. Embedded security in cars (escar Europe) **17th** (2019)
2. Bakhtina, M., Matulevicius, R.: Information security analysis in the passenger-autonomous vehicle interaction. International Conference on Availability, Reliability and Security (ARES) **16th** (2021)
3. Boudguiga, A., Boulanger, A., Chiron, P., Klaudel, W., Labiod, H., Seguy, J.C.: Race: Risk analysis for cooperative engines. International Conference on New Technologies, Mobility and Security (NTMS) **7th** (2015)
4. Cao, Y., Bhupathiraju, S.H., Naghavi, P., Sugawara, T., Mao, Z.M., Rampazzi, S.: You can't see me: Physical removal attacks on LiDAR-based autonomous vehicles driving frameworks. USENIX Security Symposium **32nd**, 2993–3010 (2023)
5. Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q.A., Fu, K., Mao, Z.M.: Adversarial sensor attack on lidar-based perception in autonomous driving. 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS) pp. 2267–2281 (2019)
6. Cui, J., Zhang, B.: Vera: A simplified security risk analysis method for autonomous vehicles. IEEE Transactions on Vehicular Technology **69th** (2020)
7. Dominic, D., Chhawri, S., Eustice, R.M., Ma, D., Weimerskirch, A.: Risk assessment for cooperative automated driving. ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) **2nd** (2016)

8. El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P.: Cybersecurity challenges in vehicular communications. Vehicular Communications **23th** (2020)
9. Federal Ministry for Digital and Transport: Germany will be the world leader in autonomous driving
10. Gao, C., Wang, G., Shi, W., Wang, Z., Chen, Y.: Autonomous driving security: State of the art and challenges. IEEE Internet of Things Journal **9th** (2022)
11. International Organization for Standardization: ISO/SAE 21434:2021 – Road Vehicles – Cybersecurity Engineering. (2021), standard.
12. International Organization for Standardization.: ISO/IEC 18045:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation. (2022), standard.
13. IRU Intelligence Briefing.: Driver shortage global report 2022.
14. Kim, K., Kim, J.S., Jeong, S., Park, J.H., Kim, H.K.: Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security **103th** (2021)
15. Liu, J., Zhang, S., Sun, W., Shi, Y.: In-vehicle network attacks and countermeasures: Challenges and future directions. IEEE Network **31th** (2017)
16. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on vanet security challenges and possible cryptographic solutions. Vehicular Communications **1st** (2014)
17. Monteuuis, J.P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., Urien, P.: Sara: Security automotive risk analysis method. ACM Asia Conference on Computer and Communications Security (ASIA CCS) (2018)
18. Narain, S., Ranganathan, A., Noubir, G.: Security of gps/ins based on-road location tracking systems. IEEE Symposium on Security and Privacy (2019)
19. Park, S., Park, H.: Pier: cyber-resilient risk assessment model for connected and autonomous vehicles. Wireless Networks (2022)
20. Pavlitska, S., Lambing, N., Zöllner, J.M.: Adversarial attacks on traffic sign recognition: A survey. ICECCME (2023)
21. Pendleton, S.D., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y.H., Rus, D., Ang Jr, M.H.: Perception, planning, control, and coordination for autonomous vehicles. Machines **5th** (2017)
22. SAE International: SAE J3016:2021 – Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. (2021), standard
23. Takahashi, J., Aragane, Y., Miyazawa, T., Fuji, H., Yamashita, H., Hayakawa, K., Ukai, S., Hayakawa, H.: Automotive attacks and countermeasures on lin-bus. Journal of Information Processing **25th** (2017)
24. Tencent Security Keen Lab: Experimental security assessment of mercedes-benz cars
25. United Nations Economic Commission for Europe: UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. (2021), e/ECE/TRANS/505/Rev.3/Add.154, Regulation.
26. Wouters, L., Gierlichs, B., Preneel, B.: My other car is your car: compromising the tesla model x keyless entry system. IACR Transactions on Cryptographic Hardware and Embedded Systems (2021)
27. Xu, W., Yan, C., Jia, W., Ji, X., Liu, J.: Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. IEEE Internet of Things Journal **5th** (2018)
28. Yurtsever, E., Lambert, J., Carballo, A., Takeda, K.: A survey of autonomous driving: Common practices and emerging technologies. IEEE Access **8th** (2020)