Hacking Trucks – Cybersecurity Risks and Effective Cybersecurity Protection for Heavy-Duty Vehicles

Marko Wolf[1] and Robert Lambert[2]

Abstract: Similar to passenger cars, heavy-duty vehicles, such as commercial trucks and buses, are becoming increasingly software-driven, interconnected and semi-automated, and hence are also becoming increasingly susceptible to cybersecurity attacks. This article will identify and evaluate these cybersecurity threats and risks affecting the monetary business operation, reliability, and safety of heavy-duty vehicles, comparing them with similar cybersecurity risks for typical passenger vehicles. Based on this overall cybersecurity threat and risk analysis, the article will then present and explain our holistic and multi-layer protection approach to reduce such cybersecurity risks for heavy-duty vehicles.

Keywords: Cyber security, automotive, heavy-duty, security risk, threat, protection

1 Introduction and Motivation

Most automotive industry players agree [McK16] that three central technology trends – namely connectivity, electro-mobility, and autonomous driving – will determine the development of the automotive domain for next 10-15 years. According to Werner Bernhard [Ber16], Head of Daimler Trucks & Buses, significant change will affect commercial vehicles in particular which "will experience more changes within the next 10 years as we have seen in the last 50 years". As shown in Figure 1, the rise of these three game-changing technologies will accelerate the deployment of electronic control systems, greatly increase the amount of vehicular software, and compound the number of digital interfaces, all of which will in turn increase the degree of networking and the system complexity in general.

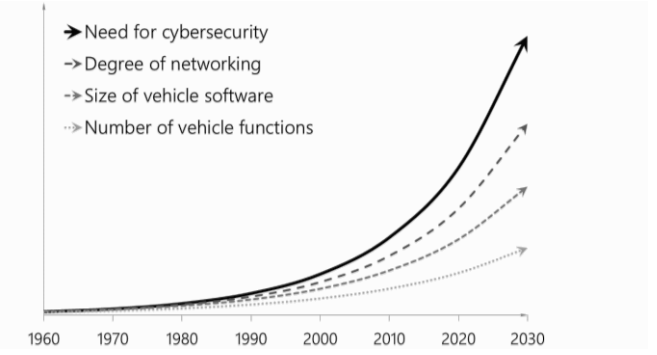

Figure 1: In order to improve fuel efficiency, fleet management, and safety, heavy-duty vehicles

[1]ESCRYPT GmbH, Munich, Germany (marko.wolf@escrypt.com
[2]ETAS Canada Inc., Kitchener, Canada (robert.lambert@etas.com)

will utilize – similarly to passenger vehicles - more electronic control systems, an increasing degree of networking, and a larger amount of software [Cha09]; this clearly also increases the need for proper cybersecurity protections.

However, since "complexity is the worst enemy of security" [Sch12] we will experience also more related cybersecurity risks & threats and hence we will also need more cybersecurity protection. In fact, compared with standard passenger vehicles, heavy-duty vehicles will be even more susceptible to cybersecurity threats since these vehicles:

- will use more complex and software-driven functionality (e.g., for platooning),
- will create, process, store and exchange more data internally and also externally via powerful, long-distance wireless communication channels (e.g., LTE interfaces for fleet management),
- will be more standardized, homogenous, and interoperable (e.g., use interchangeable engines, and employ the SAE J1939 in-vehicle network protocol),
- must often support multiple attachments (e.g., tractor implements) which, if they communicate with the vehicle, present a risk for virus and worm infection (especially since attachments will often be produced by multiple distinct manufacturers, so any weaknesses in communication protocols will take much coordination effort, and even more time, to fix satisfactorily),
- have greater value (typically > 100.000 €) and often carry valuable or dangerous loads (e.g., goods worth 1 million € per truck or hazardous chemicals),
- promise more gains from each attack and have larger potential attack benefits (e.g., systematic toll fraud, large-scale counterfeiting), and last but not least,
- are in motion up to 20 hours a day, with 3x the distance travelled, up to 5x the size and up to 30x the weight of a typical passenger car.

Considering these features together, we perceive how urgent the need for cybersecurity is. Cybersecurity considerations are just as critical as the usual safety considerations for heavy-duty vehicles, and in fact, security considerations are necessary to provide safety.

1.1 Our Contribution

This article will identify and evaluate potential cybersecurity threats and risks affecting the reliability, safety, and monetary business operation of heavy-duty vehicles in comparison with similar cybersecurity risks for typical passenger vehicles. Based on this overall threat and risk analysis, the article will then present and explain our holistic and multi-layer protection approach to reduce such cybersecurity risks for heavy-duty vehicles.

1.2 Related Work

While passenger vehicle security is already well covered in security engineering, security research, and the media (for instance by the notable publication [CMK11]), heavy-duty vehicle security, has up until now, been investigated or tackled only rarely. Some recent publications have begun to raise awareness of the problem, for example [OBr16] and [PSA16]. The currently most prominent publication regarding heavy-duty vehicle security, [BHM16], demonstrates several practical attacks on vehicle safety owing to the openness and easy (physical) access to a standardized in-vehicle network (via SAE J1939 protocol) used across all trucks and other heavy-duty vehicles in the USA. However, to the authors' knowledge there are virtually no publications providing detailed investigations into potential attackers, attack motivations, attack paths, damage potentials, or even potentially effective security protection for heavy-duty vehicles.

2 Cybersecurity Threats on Heavy-Duty Vehicles

While trucks and buses differ from standard passenger vehicles in size, weight, value, typical use, and, attraction to hackers (cf. Section 1), their internal E/E architecture is quite similar to passenger cars. As depicted in Figure 2, they also consist of about 50 distributed electronic control units (ECUs) that communicate with each other over standardized automotive bus networks such as CAN. They further provide various standardized communication interfaces to the outside world such as the physical on-board diagnosis interface (e.g., OBD port), short-range wireless communication interface (e.g., Wi-Fi), and long-distance mobile broadband communication (e.g., LTE). Hence, trucks and buses can also be susceptible to similar cybersecurity threats and risks as passenger cars.

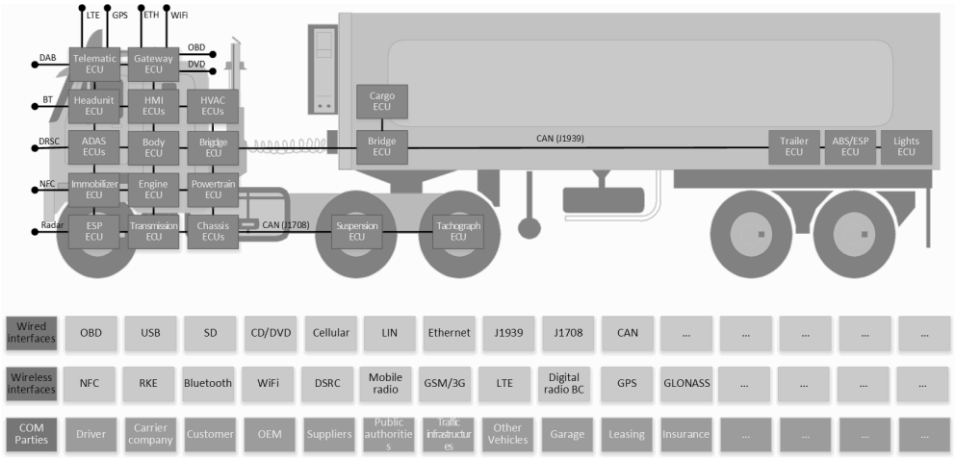

Figure 2: Typical heavy-duty vehicle E/E architecture with its various wired and wireless

interfaces

The next subsections will identify and evaluate current and future cybersecurity threats and risks affecting the monetary business operation, reliability, and safety of heavy-duty vehicles as compared with similar cybersecurity risks for typical passenger vehicles (where similar security threats exist). To this end, we provide exemplary (real-world) attacks; identify typical attackers and evaluate their individual attack potential. We further identify exemplary damaged parties; evaluate the damage potential of the attack; and calculate the resulting cybersecurity risk, which is then compared with similar cybersecurity threats for passenger vehicles (where similar security threats exist). For evaluation of the attack and damage potentials and the calculation of the resulting cybersecurity risk, we use a simplified version of the well-established security risk evaluation method as described in [SW12] and shown in Table 1.

Attack success probability ↓	**Security risk assessment**			
Certain	Medium	High	High	High
Possible	Small	Medium	High	High
Unlikely	Negligible	Small	Medium	High
Very rare	Negligible	Negligible	Small	Medium
Damage potential →	Insignificant	Significant	Critical	Catastrophic

Table 1: Simplified 4x4 automotive cybersecurity risk matrix according to [SW12]

The following sections analyze four important vehicular cybersecurity attack categories, which are physical theft, electronic manipulation, data theft, and safety attacks.

2.1 Physical Theft of Complete Vehicles or Valuable Vehicle Components

Physical theft of complete vehicles or valuable vehicle components is probably the oldest and most prominent vehicle security attack. Compared with passenger vehicles, heavy-duty vehicles are subject to a higher security risk because of the much higher attack gain of up to 1 million € for a truck with a valuable load.

	Passenger vehicle	**Heavy-duty vehicle**
Exemplary attacks	Theft of airbags, navigation systems, whole car	Theft of navigation system, tractor, load, or both
Typical attacker	Organized crime	Organized crime
Attack probability	Possible	Possible
Damaged party	Owner	Owner, operator, customer
Damage potential	Significant	Critical
Resulting cybersecurity risk	**Medium**	**High**

Table 2: Systematic derivation and comparison of cybersecurity risks for passenger vehicles and heavy-duty vehicles regarding vehicle theft or theft of valuable vehicle components

Truck vehicle thieves can abuse the known security vulnerabilities of many remote keyless entry (RKE) and immobilizer implementations, which are similar to those installed in today's passenger cars [GOD16]. Therefore, thieves can attack RKE by:

- simple jamming of the remote "lock" signal,
- calculating and sending the "unlock" signal based on a wiretapped "lock" signal,
- injecting the "unlock" signal into the unprotected onboard network via physically connecting to it through exposed and easily accessible physical bus interfaces (e.g., trailer hitch, external user interface)

If separation between internal and external networks is weak, even wireless interfaces like Wi-Fi or Bluetooth might be abused to inject "unlock" messages. Quick thefts of locked trucks raise suspicions that such thefts based on weak cybersecurity are still prevalent[1]. Truck component thieves in turn can abuse inherently limited physical protection (often put in place in order to enable easy interoperability and exchange of parts) and weak component authentication mechanisms (often not implemented at all) which could prevent the installation or the proper operation of vehicle components from unknown sources.

2.2 Manipulation Attacks on Electronic Vehicle Functionality and Vehicle Data

Together with physical thefts, unauthorized manipulations of in-vehicle data and functionality are probably the most common vehicle cybersecurity attacks. They are usually insider-attacks executed by the legitimate owner or driver of the truck, very often with professional support from specialized companies[2], which makes it particularly hard to defend against, especially since the truck manufacturers are seldom the damaged parties.

In fact, most manipulation attacks try to circumvent legal restrictions that protect the environment (e.g., disable exhaust gas treatment [Bo17]), driving safety (e.g., disable emergency brake system [Sta16]), traffic safety and fair competition (e.g., manipulated speedometers[3]) or try to betray the used-vehicle buyer (e.g., odometer manipulation). Damages to OEMs emerge mainly by warranty fraud due to out-of-specification usage (e.g., chip tuning) or manipulated lifetime counters (e.g., manipulated motor running time). However, with the continuously growing pay-on-demand economy (e.g., truck leasing, truck renting, or very costly special vehicles used only for a short time period such as agriculture vehicles), attacking such digital pay-on-demand (third-party) business models (e.g., pay-as-you-drive insurances) becomes a critical manipulation attack target as well [Law08].

[1] https://www.usatoday.com/story/news/crime/2016/07/05/clarkstown-cops-180k-truck-stolen-lot/86728206/
[2] http://www.allcartuning.com/chiptuning-lkw.html
[3] http://www.c-a-i.net/products.php?category=speedo

	Passenger vehicle	Heavy-duty vehicle
Exemplary attacks	Chip tuning, odometer manipulation, Pay-per-use bypassing, EDR manipulation	Chip tuning, tachograph manipulation, bypassing legal or safety limitations, Pay-per-use bypassing, manipulate vehicle/load monitoring
Typical attacker	Owner	Owner, driver, operator
Attack probability	Unlikely	Possible
Damaged party	OEM, third party, society	OEM, third party, society
Damage potential	Significant	Significant (at least)
Resulting cybersecurity risk	**Small**	**Medium**

Table 3: Systematic derivation and comparison of cybersecurity risks for passenger vehicles and heavy-duty vehicles regarding manipulation attacks on electronic vehicle functionality and data

With modern vehicle E/E architectures, virtually all manipulation attacks can be executed by electronic means alone, with only minimal or even no physical manipulation. The insider attacker will mainly use the easily accessible onboard diagnosis interface (OBD) which allows deep access to virtually all onboard ECUs. In order to manipulate certain data or functionality (usually via some variable control parameters stored in a table in ECU flash memory), the attacker needs to re-engineer some "hidden commands" or - for trucks even more simply – can make "use" of the standardized SAE J1939 protocol used in virtually all modern trucks [BHM16].

Even though most manipulations will cause "only" financial damages, deep software manipulation of today's complex E/E architectures, which control several critical driving functionalities, performed with home-brewed tools of dubious origin and quality, can clearly affect vehicle-driving safety as well, even though that might not have been intended. And here we see an elevated damage potential for heavy-duty compared to passenger vehicles. The attack potential for heavy-duty vehicles is rated higher than for normal passenger vehicles owning to many factors: the standardized, easy accessible J1939 interface and the increased number of promising attack targets that could work to the benefit of an owner, driver, or operator. This elevates the "medium" cybersecurity risk for trucks and buses.

2.3 Data Theft Attacks or Misuse of Digital Vehicle Data

Data theft or data misuse attacks might be expected to be rare events at a first consideration, but are already a multibillion-dollar real-world problem.

The most prominent data theft attacks are IP thefts employed to reduce engineering costs for competing products or to make counterfeit parts. According to the U.S. Federal Trade Commission, "counterfeiting represents a $12 billion per year problem for the entire automotive industry". However, it is not only a financial problem, but is very often also a safety problem. This is because counterfeit parts may not perform as well as legitimate

OEM aftermarket components, may be manufactured with less precision, or may use inferior materials. Truck braking systems are one of the components most likely to be counterfeited, and these fake braking parts result in a large number of deadly accidents [Cla14]. Other IP theft targets are costly to developed engine control software or exhaust-cleaning programs. Vehicular IP thefts and software piracy attacks are mainly insider attacks (i.e., attacks having complete physical control of the target vehicle) executed by dedicated experts that, for instance, simply dump ECU software binaries using an OBD command, re-enable fused debug interfaces, up to more sophisticated physical attacks that, for instance, de-package a chip and read-out memories with powerful microscopes [Sko01].

Like with passenger cars, other data theft attacks are privacy infringements that involve secretly collecting, storing, and transferring, for instance, vehicle location, vehicle operation, or driver's communications[4]. This data could then be used to monitor individual driving behavior (e.g., to defend warranty claims), enable individual marketing (e.g., location-based services), resell collected data to third parties[5] (e.g., Google maps), or – in the worst case – this secretly stored data used against the driver in case of an accident[6]. However, for commercial trucks, in addition to potential privacy infringements, economic espionage is much more likely, and the attack path is similar. In contrast to passenger cars, modern trucks often enable OEMs, logistic operators, carriers, and sometimes even customers to have considerable remote access to truck internal data, even in some cases allowing direct access to the CAN bus to monitor and control vehicle position, or to get information on how the vehicle has been loaded, or even how it is being driven. Competitors can try to hack into these remote interfaces to monitor (or disturb) their competition or might try to steal or purchase such data from third party application providers (e.g., digital toll applications) that collect, store, aggregate, and sell such data without the explicit knowledge and permission of the driver or operator.

While the attack probability for heavy-duty vehicles is already somewhat larger due to the broader deployment of remote access applications, the damage potential for trucks regarding espionage and safety is considerably larger, resulting in a high cybersecurity risk.

	Passenger vehicle	**Heavy-duty vehicle**
Exemplary attacks	IP theft, privacy invasions, counterfeit parts	IP or business secrets theft, privacy invasions, counterfeits parts, vehicle tracking, load control or navigation manipulation, operator/driver extortion
Typical attacker	Plagiarist, competitor, third parties (e.g., insurances), OEM	Plagiarist, competitor, third parties (e.g., insurance companies), OEM, government, organized crime
Attack probability	Possible	Possible

[4] https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/
[5] http://www.usatoday.com/story/money/cars/2013/03/24/car-spying-edr-data-privacy/1991751/
[6] https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht/

Damaged party	Driver, owner, OEM	Driver, operator, customer, OEM, society
Damage potential	Significant	Critical
Resulting cybersecurity risk	**Medium**	**High**

Table 4: Systematic derivation and comparison of cybersecurity risks for passenger vehicles and heavy-duty vehicles regarding data theft attacks or misuse of digital vehicle data

2.4 Attacks on Vehicle Reliability and Vehicle Safety

Finally, yet importantly, truck reliability and safety are at least as endangered as it has been recently demonstrated with real-world passenger cars, where hackers where able to remotely hijack a Jeep over the Internet and have successfully attacked the Jeep's steering, acceleration, and braking systems[7]. In fact, due to the standardized J1939 protocol used in virtually all modern trucks, the (most) costly attack preparation step, the reverse engineering of the susceptible internal commands, would not be necessary, making such safety attacks against trucks and buses much easier. Researchers from Michigan University have already demonstrated such attacks in practice on a class-8 semi-tractor and a 2001 school bus [BHM16]. Even though they have not executed their attacks remotely, it is easy to imagine that hackers will find many similar remote entry points as have already been very successfully found into passenger cars [CMK11].

In real life, such safety attacks have not happened yet against cars nor against trucks, since these attacks are still quite costly to prepare and provide virtually no direct financial benefit, or would cause enormous search pressure if abused for extortion or even terrorism. Thus, we rate the attack probability for trucks "unlikely" in the first instance, while we inherently rate the potential damage of a 40-ton vehicle driving around at 60 mph without brakes "catastrophic", which results again in high cybersecurity risks for trucks compared with "medium" for passenger vehicles.

	Passenger vehicle	**Heavy-duty vehicle**
Exemplary attacks	Delete critical data, lock critical functions, hijack driving functionality	Delete critical data, lock critical functions, hijack driving functions
Typical attacker	Extortionist, terrorist, nation-state	Extortionist, terrorist, nation-state
Attack probability	Very rare	Unlikely
Damaged party	Driver, society	Driver, operator, customer, society
Damage potential	Catastrophic	Catastrophic
Resulting cybersecurity risk	**Medium**	**High**

Table 5: Systematic derivation and comparison of cybersecurity risks for passenger vehicles and heavy-duty vehicles regarding attacks on vehicle reliability and vehicle safety

[7] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

3 Cybersecurity Protection for Heavy-Duty Vehicles

The following section will provide our holistic, systematic and multi-layer protection approach in order to reduce the cybersecurity risks for heavy-duty vehicles to a minimum. Our holistic approach assures vehicular security by applying the following three security principles:

(1) *Security for the entire heavy-duty vehicle system* (i.e., from individual ECU to connected cloud backend)
(2) *Security for the entire heavy-duty vehicle lifecycle* (i.e., from first requirements analysis to vehicle phase-out)
(3) *Security for the entire heavy-duty vehicle organization* (i.e., from security processes to security governance)

The next three subsections explain the realization of these three security principles in more detail. We do not have to start from scratch, but can benefit and reuse much of the already existing experience and security solutions from the passenger vehicle domain. In fact, most of the security approaches for passenger vehicles can be directly transferred to the heavy-duty vehicle domain.

3.1 Security for the Entire Heavy-Duty Vehicle System

For sustainable vehicular security, it is necessary to always consider the whole vehicle system starting from the individual ECU up to the connected services in the backend, since a smart attacker would also check the whole vehicle system for the weakest link at which to execute an attack most easily. Thus, for instance, even a perfectly secure encryption algorithm would lose all security if we use a global secret key for every truck, if that one key can be obtained from any ECU which uses the secure algorithm.

For sustainable vehicular security, we also need multiple lines of defense since – especially within the rather slow and costly to adapt vehicular security domain - we always have to assume that one of our protection measures might become weakened or even fail. Long term, real-world security experience forbids the typical “single point of failure” protection approaches which might have, for instance, only a single firewall gateway isolating a secure internal vehicle network from an insecure external one, and where a single vulnerability would compromise all vehicles of that type in the world completely and at once.

Unfortunately, until now exists no standardized vehicle security approach yet, but Figure 3 shows how a sustainable vehicular security approach might look from the technical perspective, where the vehicle system employs multiple lines of defense. Each line or layer uses different security mechanisms, assuming that not all security mechanisms would fail at once. Based on a secure trust anchor, usually realized with an automotive-capable hardware security module [WW12], we can assure the integrity (and confidentiality) of the ECU firmware which uses, for instance, secure boot or trusted

boot protection [WG11]. The protected ECU firmware in turn provides higher-level software-based security functions to enable secure onboard communication protocols such as the AUTOSAR-based "Secure Onboard Communication (SecOC)" protocol [AS15]. A secure in-vehicle E/E architecture further separates connected ECUs into three to ten mutually isolated sub-networks of different security and safety classes, which can communicate across subnets only via secure gateway processors enforcing strict firewalling rules [JSV13]. Vehicle-external communication is further protected by a central gateway (CGW) equipped with vehicular intrusion detection (IDS) and response (IRS) systems, which implement external communication security protocols for securing V2V (e.g., IEEE 1609) and V2I (e.g., Embedded TLS) communications [WSA15]. Finally, yet importantly, all relevant backend and infrastructure services such as key management and cloud services, but also connected IoT and cellular devices, need strong classical network security and mobile security solutions.

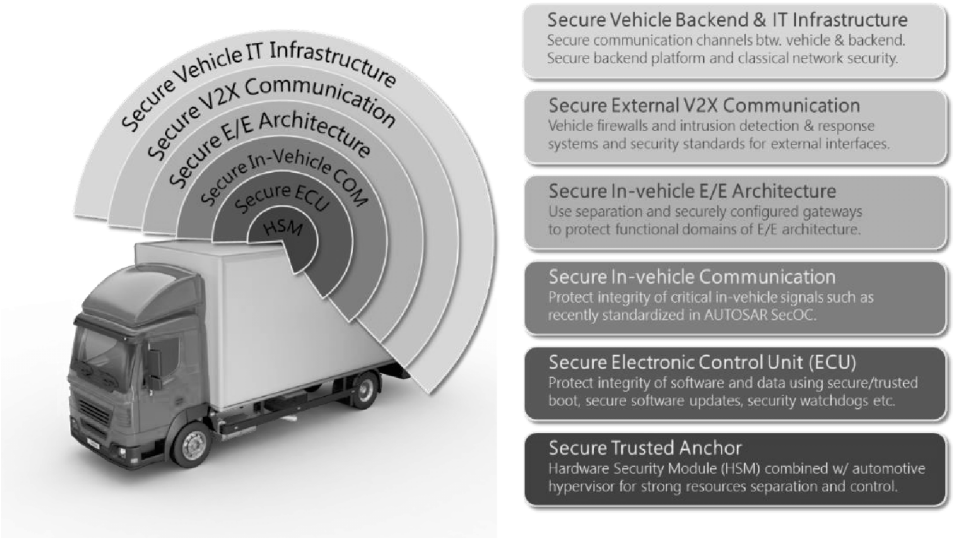

Figure 3: Multiple lines of defense protecting the entire heavy-duty vehicle system.

3.2 Security for the Entire Heavy-Duty Vehicle Lifecycle

In contrast to classical engineering, where the operational environment is mainly defined by natural laws and reliable statistics and where engineering processes usually end with the start of production, security engineering does not end until product phase-out. This is because the security environment is continuously changing, particularly in early production, or when newly identified attack paths, new vulnerabilities, or new security research are discovered.

Thus, security engineering uses a continuous vehicle security lifecycle [SAE16] that

provides security procedures for the whole vehicle lifecycle from requirements engineering until phase-out, as shown in Figure 4 (including some exemplary security procedures executed during each lifecycle phase).

Such a continuous lifecycle also has some additional technical and organizational implications, since for instance all development hardware, all tool chains, and at least some of the experts involved have to remain available until final phase-out, which means for heavy-duty vehicles: for up to 20 years.

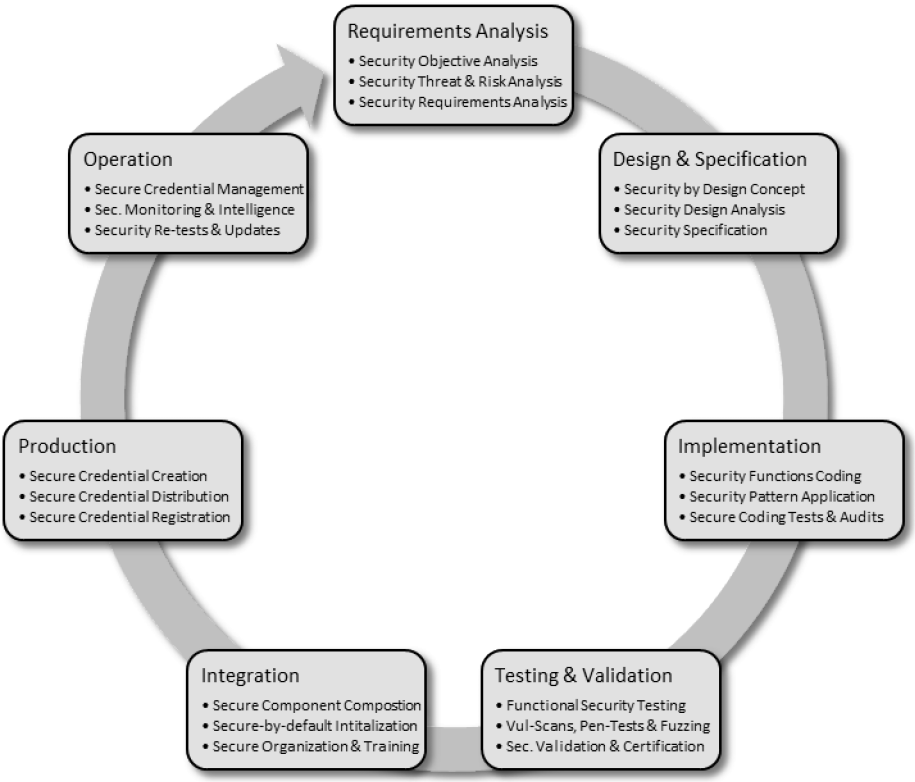

Figure 4: Continuous vehicle security lifecycle with exemplary security operations per lifecycle phase, which are executed continuously until product phase-out, to be able to react to the continuously changing security environment.

3.3 Security for the Entire Heavy-Duty Vehicle Organization

Vehicle security is indeed much more that “just another technical vehicle feature” developed by “just another company division”. In fact, sustainable vehicle security requires deep cross-divisional integration and strong commitment from the whole

organization. This is especially difficult since security, at first glance, creates neither new features nor new revenues, but only additional documentation, processes, and complexity without any immediately apparent benefits.

Without engaging the whole organization, the efforts for security can become quickly ineffective and bogged down by compatibility issues, insufficient resources, hard-wired dummy values, "secret" (debug) circumventions, or organizational process vulnerabilities such as insufficient access and usage control for important cryptographic secrets.

On the other hand, a well-engaged security organization helps a lot for instance to avoid inefficiency by several mutually incompatible isolated solutions (also known as "Insellösungen"). It also clearly reduces security risks by reducing complexity ("which is the worst enemy of security"), provides always a good system overview and ensures proper management of all security-critical functions and corresponding credentials. Moreover, well-organized vehicle security management can in fact increase security without extra costs, for instance, if small separate security mechanisms can together share a powerful high-security hardware crypto module.

Figure 5 gives a first overview on how a vehicle manufacturer or vehicle supplier could setup his vehicle security organizational structure, which is an independent and additional structure to the classical IT security organizational structure. Thus the vehicle security organizational structure shown in Figure 5 clearly focusses on the cybersecurity protection of the company's products, but does not replace classical organizational IT security, such as securing company networks or controlling access to the company's facilities.

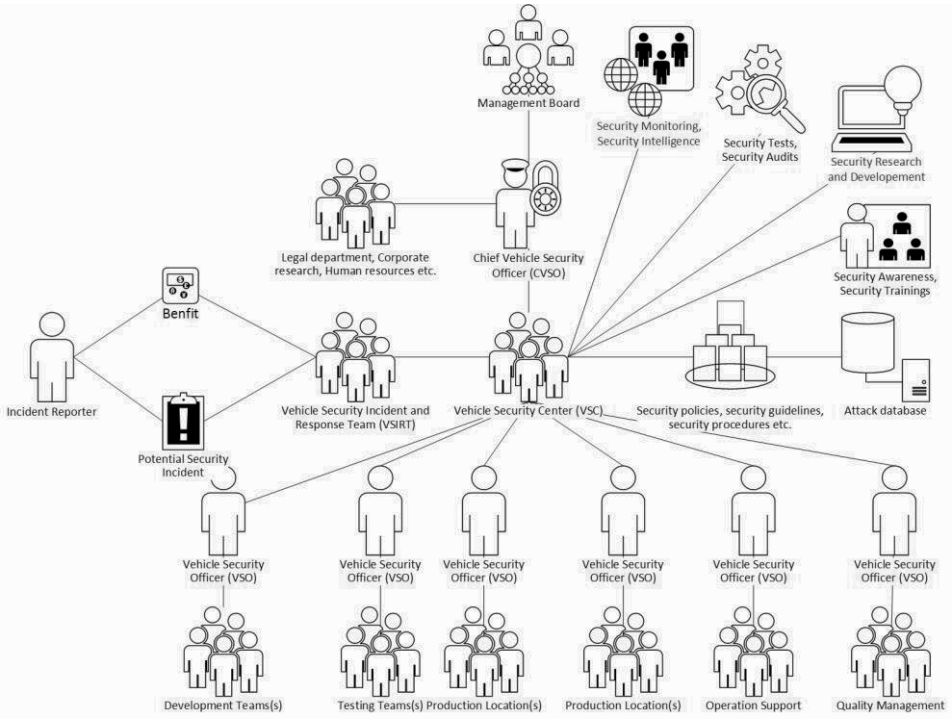

Figure 5: Roles and relations for implementing vehicle security within the organization.

In the following, a very short description of the different security roles and their responsibilities shown in Figure 5 is given.

Vehicle Security Officer (VSO) is an (additional) role of a team member in who is involved in virtually all organizational units participating in the vehicle product lifecycle, such as development, testing, production, and operation, but also in cross-divisional departments such as quality management. The VSO ensures, for instance, that his team members get sufficient cybersecurity training, comply with all relevant security rules and processes, apply up-to-date cybersecurity protection mechanisms, and report new cybersecurity risks and threats (if any), new security requirements, or potential improvements for vehicle cybersecurity protection. VSOs are steered by and report to the Vehicle Security Center.

Vehicle Security Center (VSC) is a team of dedicated vehicle security experts which develop and maintain the relevant cybersecurity procedures (e.g., security engineering process), guidelines (e.g., secure coding guideline), and policies (e.g., access control policy for software signing key) for ensuring sufficient cybersecurity protection of all company vehicle products through their entire lifecycle. The VSC works closely with the Vehicle Security Incident and Response Team (VSIRT) to evaluate (new) security risks

and threats and, if needed, coordinates the development and rollout of effective response measures such as security patches. The VSC further works closely with many other company departments, for instance with legal departments to keep their cybersecurity requirements up-to-date (e.g., new privacy protection laws), with cooperate IT for hosting security services (e.g., security credential management system), or with cooperate research to improve their knowledge about new security threats and effective protections. The VSC is further responsible for in-house security training and awareness, internal security tests and audits security monitoring and intelligence, and development of new cybersecurity protection measures. The VSC in turn is managed the Chief Vehicle Security Officer (CVSO) who will directly (and exclusively) report to the management board.

Vehicle Security Incident and Response Team (VSIRT) is a team of vehicle security experts focused on new cybersecurity risks and threats around the company's products and cybersecurity forensics. The VSIRT monitors press & media, attends relevant security conferences, boards, and committees, talks to customers, employees, and even competitors to learn about new security risks and threats. Sometimes they even provide "bug bounty" programs, which pay for security vulnerabilities detected and reported by so-called "white hackers". The VSIRT is also responsible for executing (e.g., revoking a certificate) or requesting (e.g., development of a security patch) effective response measures in case of a critical product security risk. The VSIRT is steered by the VSC.

Chief Vehicle Security Officer (CVSO) is a senior executive heading all vehicle security activities of a company. The CVSO decides about the vehicle security strategy, manages relevant cybersecurity risks, ensures cybersecurity governance, and makes decisions on all critical incident response measures (e.g., service shutdowns). Since cybersecurity is a cross-divisional function, the CVSO reports only directly to the management board and can thus push necessary cybersecurity protection requirements and measures through all other company departments.

4 Summary and Outlook

In this article, we have identified and evaluated potential cybersecurity threats and risks affecting the reliability, safety, and monetary business operation of heavy-duty vehicles in comparison with similar cybersecurity risks for typical passenger vehicles. Based on this analysis, we then presented and explained our holistic protection approach to reduce such cybersecurity risks for heavy-duty vehicles.

The analysis has shown that the cybersecurity risks for heavy-duty vehicles are often of higher risk when compared to typical passenger vehicles, since the corresponding attacks on heavy-duty vehicles could be executed easier or would have a larger damage potential. The analysis further shows that most of these cybersecurity threats are already realistic, in fact already executed, today and will become even more critical in the future.

But the article showed also that many effective cybersecurity protection measures already existing in the passenger vehicle domain, can very often be easily transferred to the heavy-duty vehicles. The next version of this article will further investigate the costs and efforts needed for implementing proper cybersecurity protections for heavy-duty vehicles and will show that the return on investment will be achieved even earlier and more easily when compared with the implementation and return expected in standard passenger vehicles.

5 References

[AS15] AUTOSAR, "Specification of the Secure Onboard Communication", In *AUTOSAR Release 4.2.2*, July 2015.

[Ber16] Wolfgang Bernhard, "Daimlers Lkw-Chef will autonome Trucks bis 2020", In *Manager Magazin*, June 2016.

[BHM16] Yelizaveta Burakova et al., "Truck Hacking: An Experimental Analysis of the SAE J1939 Standard", In *USENIX Workshop on Offensive Technologies*, August 2016.

[Bo17] Christian Bock, "Die Lüge vom sauberen LKW", In *ZDF Zoom*, January 2017.

[Cha09] Robert Charette, "This car runs on code" In *IEEE Spectrum 46.3*, 2009.

[Cla14] Jane Clark, "Are Your Aftermarket Truck Parts the Real Deal?", In *Truckinginfo.com*, March 2014.

[CMK11] Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces", In *USENIX Security*, August 2011.

[GOD16] Flavio Garcia et al., "Lock It and Still Lose It–On the (In) Security of Automotive Remote Keyless Entry Systems", In *USENIX Security*. August 2016.

[JSV13] James Joy et al., "Gateway Architecture for Secured Connectivity and in Vehicle Communication", In *VDI Wissensforum*, October 2013.

[Law08] Nate Lawson, "Highway to Hell: Hacking Toll Systems", In *Blackhat*, August 2008.

[McK16] McKinsey, "Automotive Revolution Perspective Towards 2030", In *Advanced Industries*, January 2016.

[OBr16] Chris O'Brien, "Long-Haul Trucking Connectivity Brings Hacking Risks", In *Trucks.com Trucking Technology*, May 2016.

[PSA16] FBI & NTHSA, "Motor Vehicles Increasingly Vulnerable to Remote Exploits", In *Public Service Announcements* I-031716-PSA, March 2016.

[SAE16] SAE J3061 Vehicle Cybersecurity Systems Engineering Committee, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", In *SAE International*, January 2016.

[Sch12] Bruce Schneier, „Complexity the Worst Enemy of Security", In *Schneier Security Blog*, December 2012.

[Sko01] Sergei P. Skorobogatov, "Copy Protection in Modern Microcontrollers", In http://www.cl.cam.ac.uk/~sps32/mcu_lock.html, November 2001.

[Sta16] Kristina Staab, "Wenn der Lkw die Notbremse zieht", In *SWR Aktuell Hintergrund*, August 2016.

[SW12] Michael Scheibel et al., "A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems", In *Automotive Safety & Security*, November 2012.

[WG11] Marko Wolf et al., "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module", In *International Conference on Information Security and Cryptology*, November 2011.

[WSA15] Yaron Wolfsthal et al., "Solution for Detecting Cyber Intrusions to Connected Vehicles", In *IBM Security Intelligence*, September 2015.

[WW12] André Weimerskirch et al., “Hardware Security Modules for Protecting Embedded Systems”, In *ESCRYPT Security Whitepapers*, May 2012.