Hochschule Karlsruhe
University of
Applied Sciences

Institut für
Energieeffiziente Mobilität

Automotive Security Inspections – Trust is good, but control is better!

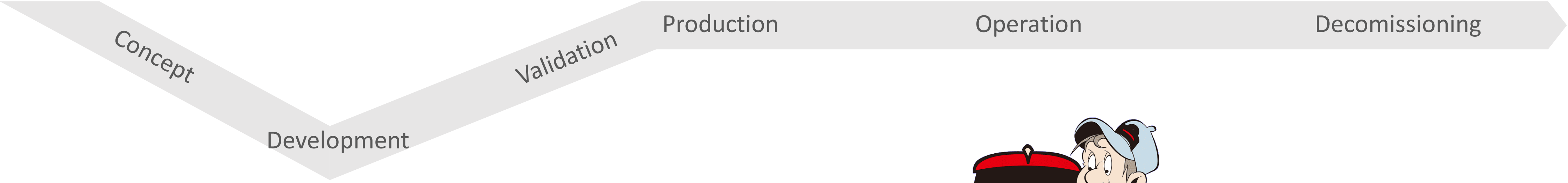
Vehicular 2022

presented by Mona Gierl, M.Sc.
University of Applied Sciences Karlsruhe, Germany
mona.gierl@h-ka.de

IARIA KIT Karlsruher Institut für Technologie GTÜ

Automotive Security Inspections?

Automotive Security + Technical Inspections



1 European road safety measures

2 Automotive Security

3 Technical Inspections

4 Automotive Security Inspections

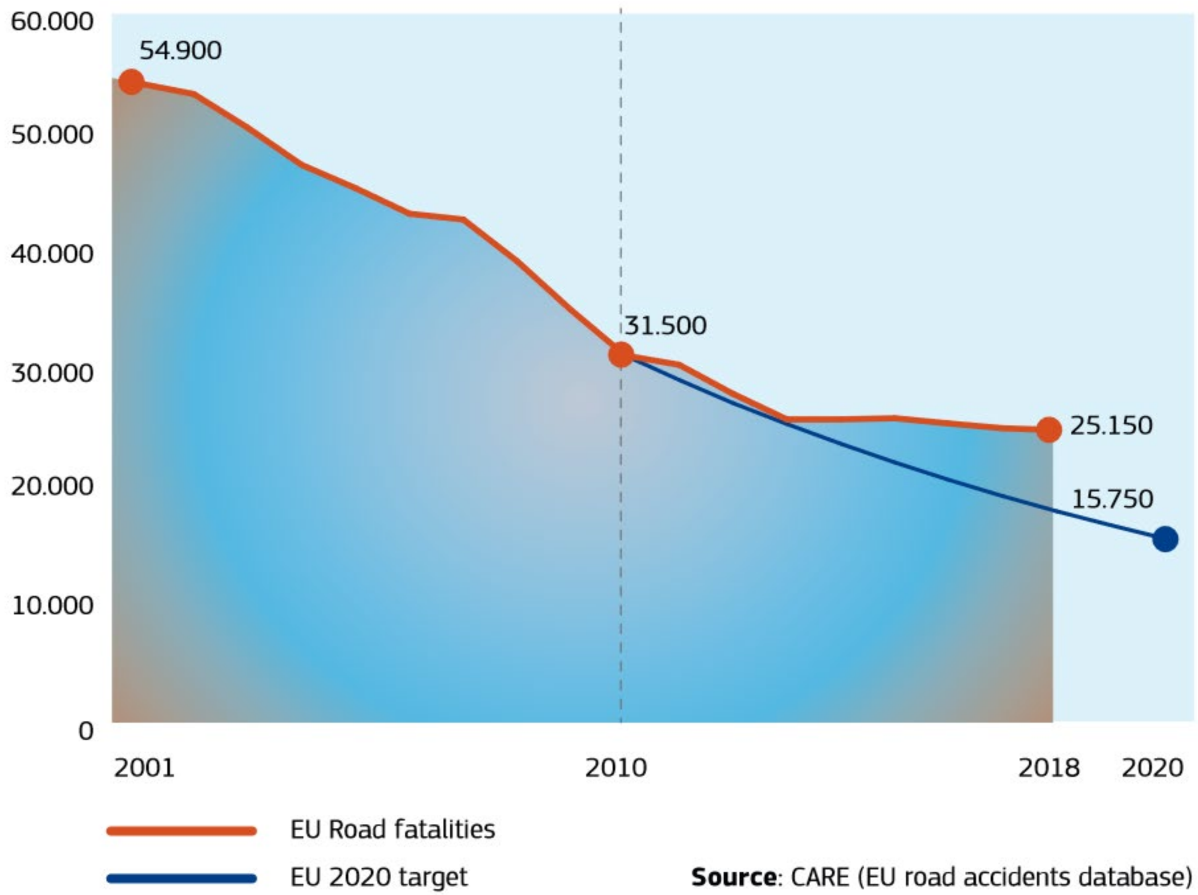
Vision Zero – European road safety measures

Road Safety Policy Framework 2021 – 2030 [1]

Goal: reduce road deaths to zero by 2050

„Safe System“ approach including:

- Infrastructure
- Safe road use
- Safe vehicles
- Emergency response



Features and Functions [2]

1975

Electronic fuel injection
Antilock brakes

1985

Gearbox control
Traction control
CAN
Electronic fuel injection
Antilock brakes

1995

Hybrid powertrain
Electronic stability control
Active body control
Emergency calling
Electric power steering
Flexray
Gearbox control
…

2005

Electric powertrain
Adaptive cruise control
Lane assistant
Automatic start and stop
Emergency brake assistance
Head-up display
Electronic brake control
Remote diagnostics
Online software updates
AUTOSAR
Hybrid powertrain
…

2015

Mobility services
Driver assistance systems
Brake-by-wire
Steer-by-wire
Connectivity, V2X
5G mobile communication
Full-cell technology
Laser-sourced lighting
3D displays
Gesture HMI
Ethernet/IP backbone
Electric powertrain
Adaptive cruise control
…

2025

Development of Intelligent Vehicles

Complexity →

Features ↓

SAE Level 0	SAE Level 1/2	SAE Level 3	SAE Level 4	SAE Level 5
Automatic Emergency Braking	Lane Centering	Traffic Jam Chauffeur	Local Driverless Taxi [4]	
Blind Spot Warning	Adaptive Cruise Control	"Driver Pilot" [3]	Automated Valet Parking	
Lane Departure Warning	Intelligent Speed Assistance [6]		Automated Hub-to-Hub Traffic [7]	
Moving-Off Infor-mation System [5]				

Driver support features — Automated driving features — Planned features

General Safety Requirements (GSR) – 2019/2144/EU

Planned are the following safety features [6]:

- Intelligent speed assistance[B]
- Alcohol Interlock Installation Facilitation (breathalyser)[B]
- Driver drowsiness and attention warning systems[B]
- Blind Spot Information System[B]
- Emergency stop signal[B]
- Reversing detection systems[B]
- Event data recorders[B,D]
- Accurate tyre pressure monitoring[A,B], etc.

Gradual introduction of technologies (A-D):

Time stage	**A**	**B**	**C**	**D**
All new vehicle types	-	6 July 22	7 July 24	7 January 26
All vehicles registered for the first time	6 July 22	7 July 24	7 July 26	7 January 29

Further Type Approval Requirements

UNECE 1958 Agreement

2018/858/EU Regulation
2019/2144/EU GSR

National law references EU Regulations

UN R0 –
UN R163

64 Contracting Parties including EU

extends and references
UN Regulations

UN R155 Cybersecurity Regulation:

„In the European Union, the new cybersecurity regulation (UNECE WP.29/R155) will be mandatory for all new vehicle types as of July 2022 and will be mandatory for all new vehicles produced as of July 2024"

European road safey measures	1	3	Technical Inspections
Automotive Security	2	4	Automotive Security Inspections

Motivation Automotive Security

Attacks on the vehicle – Survey at IEEM [8]

In total: 343

222 Single Stage, 121 Multi Stage Attacks

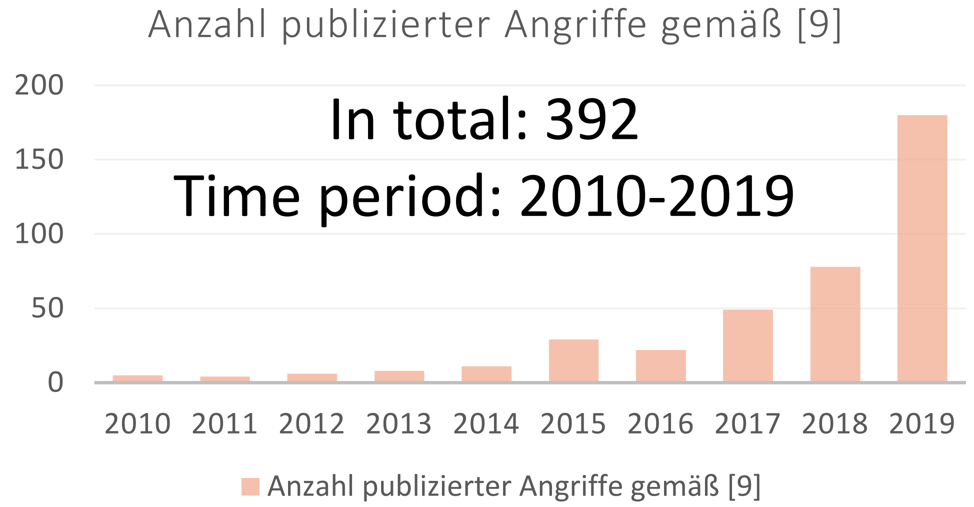
Time period: 2002-2019

public resources, research papers, etc.

Survey Upstream Security [9]

In total: 392

Time period: 2010-2019



[8] Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. *Information* **2019**, *10*, 148.

[9] Upstream Security, Upstream Security Global Automotive Cybersecurity Report 2020, online: https://www.upstream.auto/

Attack Taxonomy

Classification scheme to describe known automotive security attacks

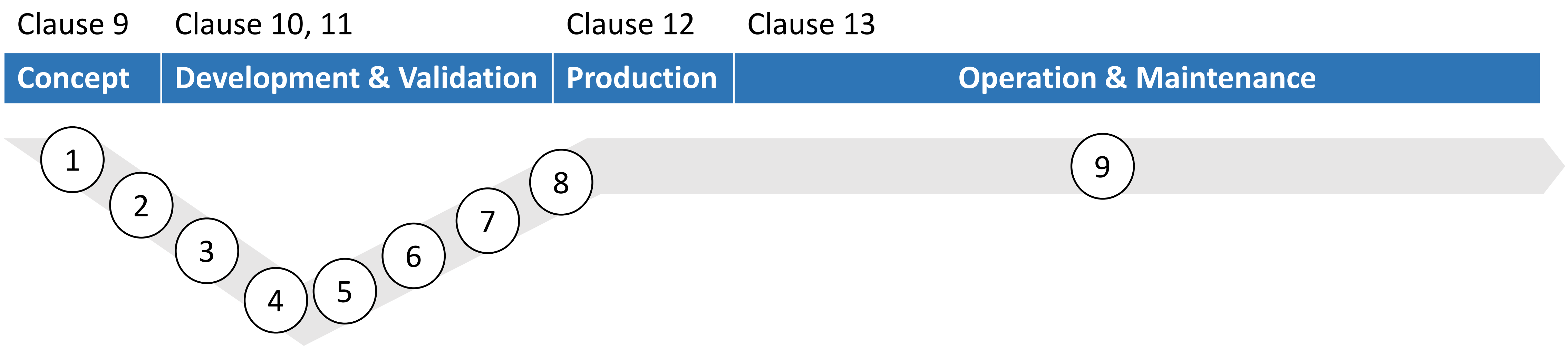
Goal: uniform description of automotive attacks + reuse attack steps in security engineering

Category	Level 1	Level 2	Level 3
Description	Unauthorized flashing of malicious code on the engine ECU by using the diagnostic reprogramming routine		
Reference	Adventures in Automotive Networks and Control Units (C. Valasek et al.)		
Year	2013		
Attack Class	Tampering	Firmware Modification	None
Attack Base	Diagnostic Attack		
Attack Type	Real Attack		
Violated Security Property	Integrity		
Affected Asset	Information Security		
Vulnerability	CWE-693: Protection Mechanism Failure	CWE-287: Improper Authentication	Unauthorized reprogramming possible
Interface	OBD		
Consequence	Flashing of malicious code on ECU		
Attack Path	Downloading a new calibration update for ECU from manufacturer and Reverse Engineering of the Toyota Update Calibration Wizard (CUW). Monitoring the update process. Reverse Engineering update algorithm for calibration updates. Modification of calibration update. Reflashing of malicious update.		

Further entries:
- Requirements (e.g. access)
- Restrictions
- Attack Level
- Acquired Privileges
- Vehicle Model
- Component
- Tool
- Attack Motivation
- CVSS Rating

Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. Information 2019, 10, 148.

ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering



1 – Item Definition, Cybersecurity Goals

2 – Cybersecurity Concept

3 – Cybersecurity Requirements, Architectural Design

4 – Software Requirements, Architectural Design

5 – Software Integration, Verification

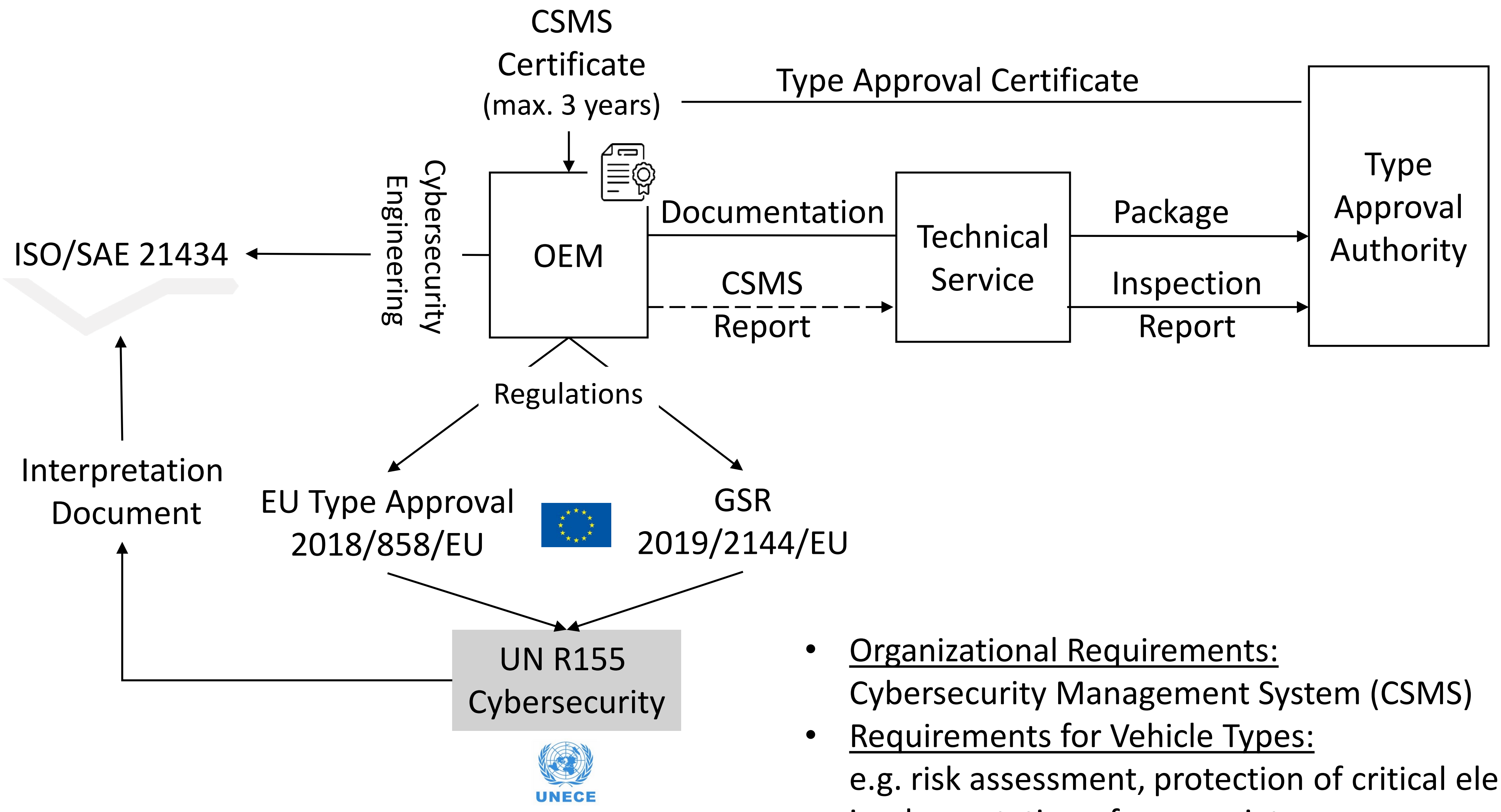
6 – System Integration, Verification

7 – Item Integration, Verifcation & Validation

8 – Cybersecurity Validation

9 – Monitor, incident response, update, report

UN R155 in the Type Approval Framework



- <u>Organizational Requirements:</u>
  Cybersecurity Management System (CSMS)
- <u>Requirements for Vehicle Types:</u>
  e.g. risk assessment, protection of critical elements, implementation of appropriate measures

European road safey measures 1

Automotive Security 2

3 Technical Inspections

4 Automotive Security Inspections

Security Lifecycle ISO/SAE 21434

Phases of the Security Lifecycles according to ISO/SAE 21434 [10]

ca. 3 years

Type Approval

UNECE

∅ 9,8 years*

Conzept | Development | Validation | Production | Operation | Decommissioning

Continuous CSMS Reports, Periodic Technical Inspections (PTI)

*Statistics of [12] for 2021

Periodic Technical Inspections

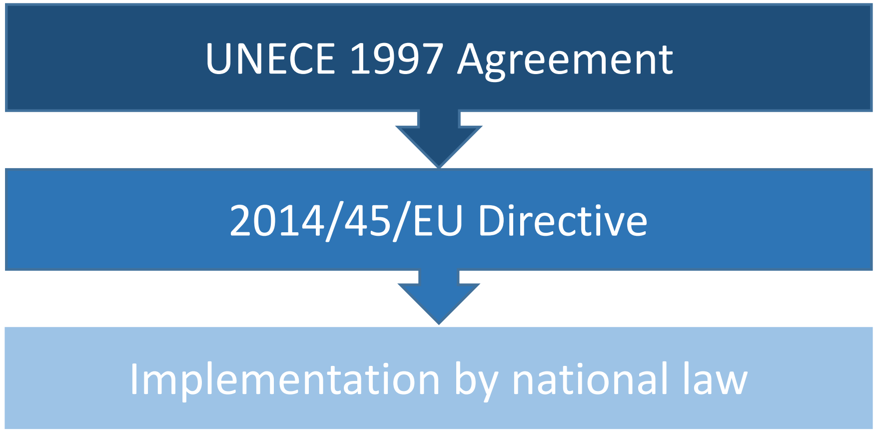
“A properly maintained and fully functioning vehicle meeting all safety requirements is less likely to be involved in a road accident.” [11]

EU Roadworthiness Package:

– 2014/45/EU Periodic Roadworthiness Inspections

– 2014/47/EU Roadside Inspections

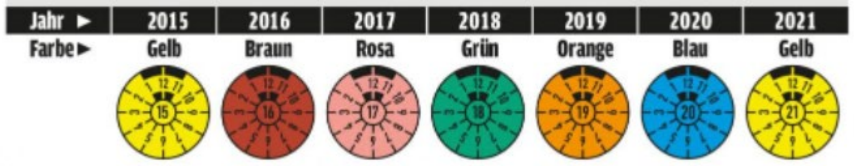
– 2014/46/EU Vehicle Registration Documents



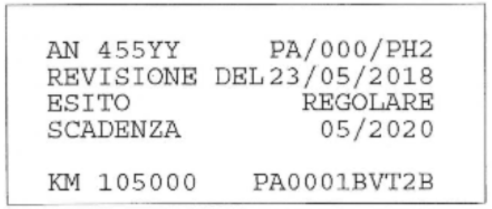
Overview of rules, testing frequency, issued documents, etc.:

[Roadworthiness Certificate and the Proof of Test (europa.eu)](#) (RWC and the POT)

German RWC POT



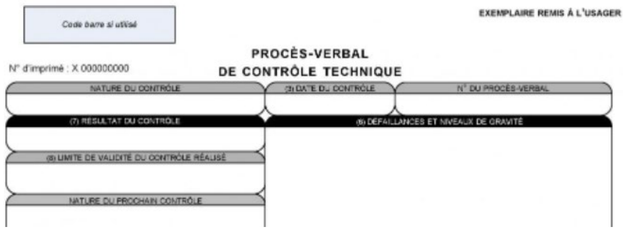
Italian RWC POT



AN 455YY PA/000/PH2
REVISIONE DEL 23/05/2018
ESITO REGOLARE
SCADENZA 05/2020

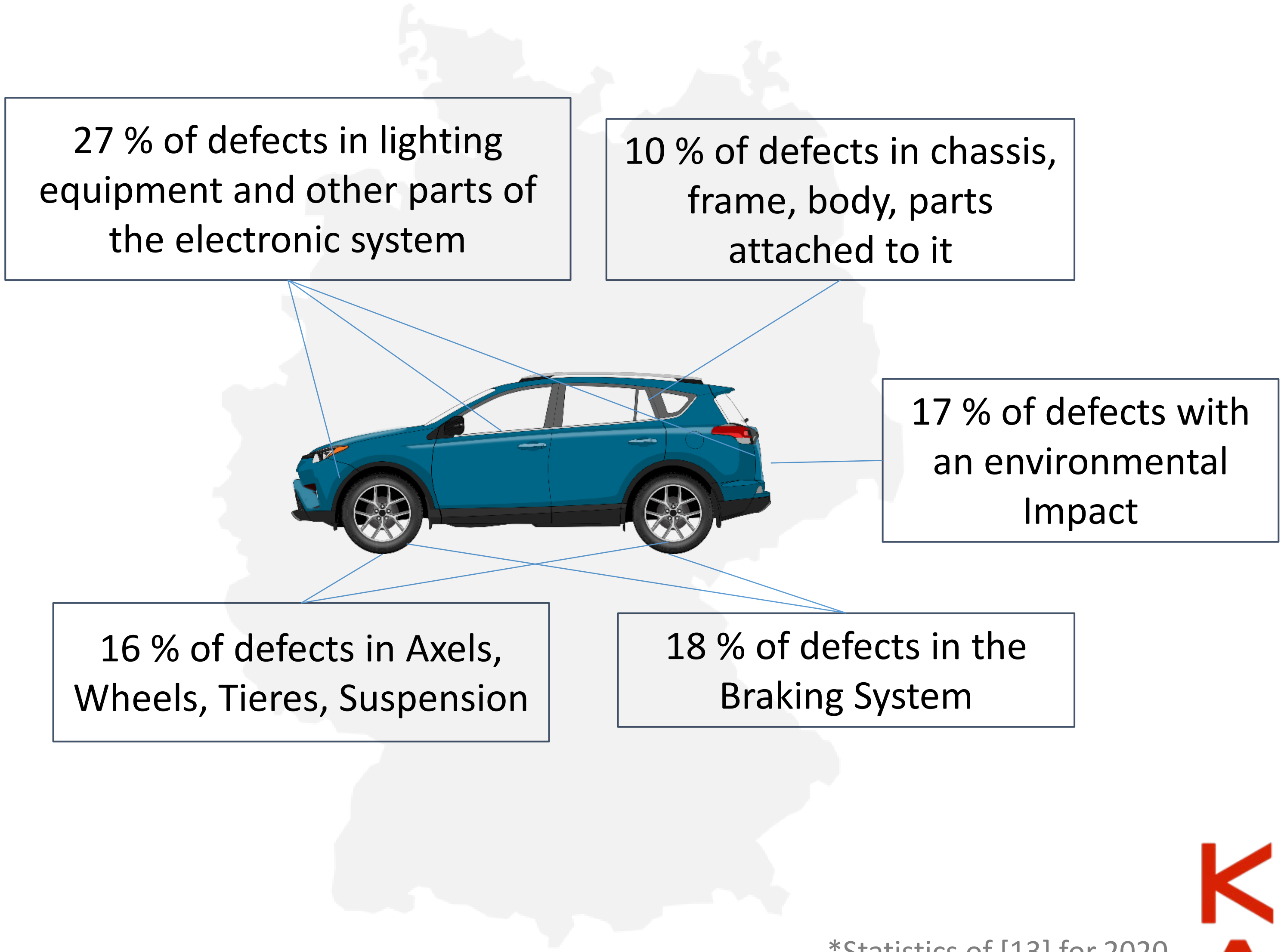
KM 105000 PA0001BVT2B

French RWC POT



Periodic Technical Inspections (PTI) in Germany

- 12.5 Mio. vehicles (26%) in Germany are 5-9 years old (2021) [12]
- PTI is mandatory every 2-3 years for german passenger cars
- Visual, functional, and electronic inspection without disassembly



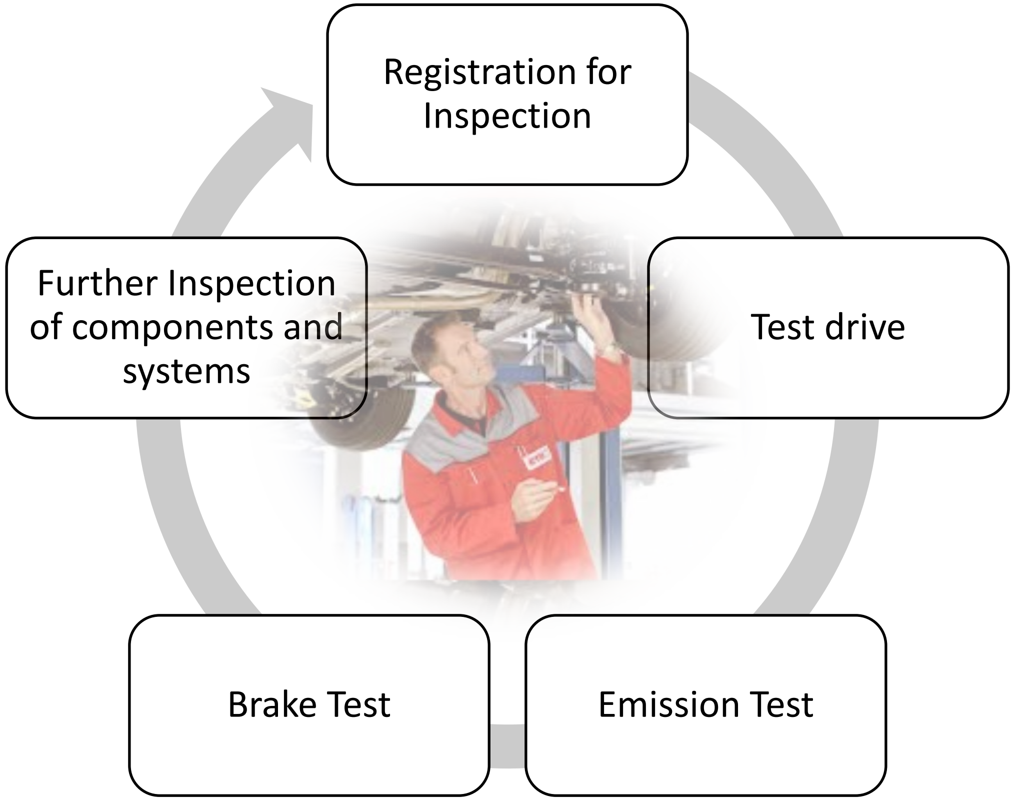
*Statistics of [13] for 2020

Periodic Technical Inspections (PTI) in Germany

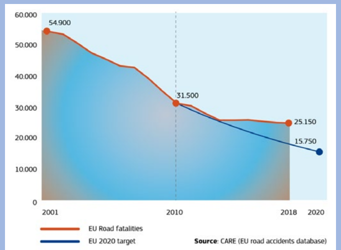
EU Directive 2014/45/EU demands the examination of:

- Identification and classification of the vehicle
- Braking equipment, Steering, Visibility
- Photometric equipment and other parts of the electric installation
- Axles, wheels, tires, suspension
- Chassis, frame, platform, attached parts
- Environmental impact

➡ Inspection of equipment, condition, function, and performance.

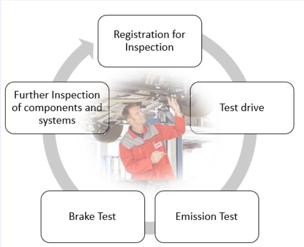


Keywords:
Vision Zero, Safe Vehicle, General Safety Regulation, further Type Approval requirements



European road safey measures

1



Keywords:
Roadworthiness assessment, 2014/45/EU Directive, inspection of equipment, condition, function, and performance

3

Technical Inspections

Automotive Security

2

4

Automotive Security Inspections

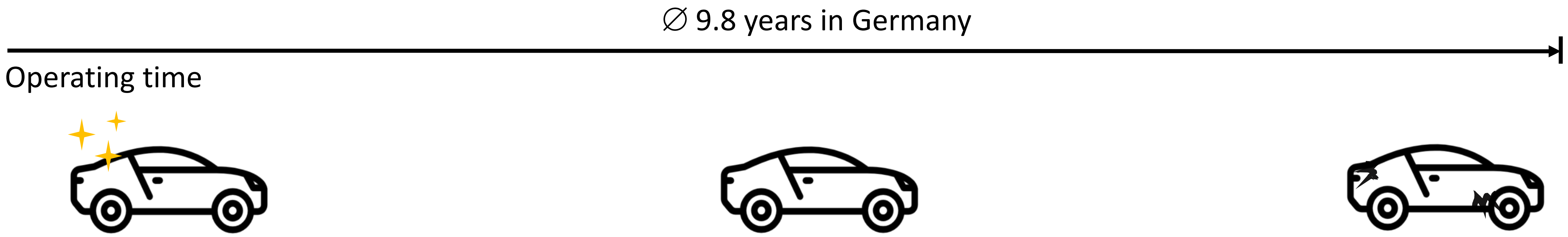
Keywords:
Attack collection, taxonomy, ISO/SAE 21434, UN R155 process

Attacks on the vehicle –
Survey at IEEM [8]

In total: 343
222 Single Stage, 121 Multi Stage Attacks
Time period: 2002-2019
public resources, research papers, etc.

Operational Security Challenges

I. Security is dynamic
II. Security measures may age
III. Security is „not visible“ during normal operation
IV. Unallowed manipulations due to self interest (Tuning)
V. Changes to the overall system due to Over-the-Air Updates



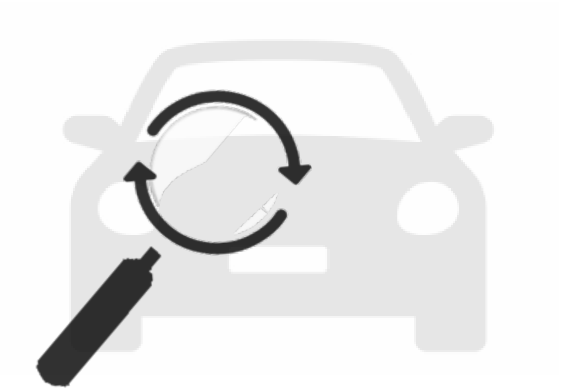
Conclusion and further steps

Requirements for Automotive Security Inspections

I. Continuous, efficient vehicle testing over the entire life cycle

II. Connected vehicles require dynamic security test methods

III. Adaptation of current inspection methods in the field necessary



Prerequisites:

- Definition of suitable evaluation methods for validation of automated and connected vehicles
- Further research and standardization work for test methods in the field and their data access

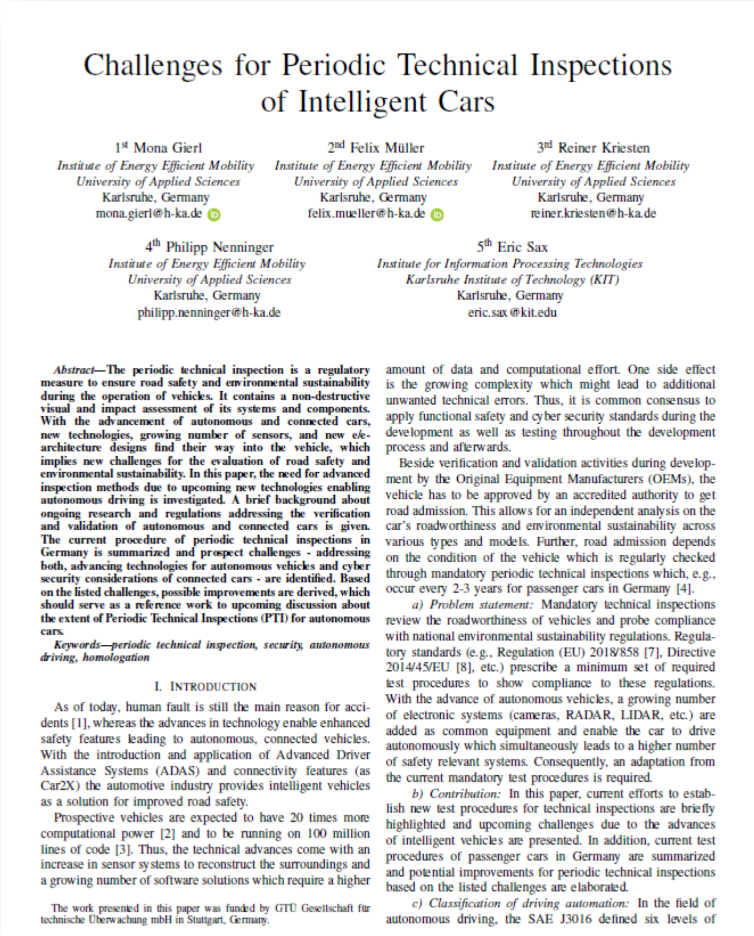
Research Project to investigate diagnosis of autonomous driving functions and the cyber security assessment of safety-relevant vehicle systems for the periodic technical inspection

Challenges and Improvements for PTI

Tuesday, 18:30 - 20:15 Session #5 [VEHICULAR, INTERNET]

Further information on our research project:

Webiste: https://www.h-ka.de/en/ieem/projects/next-level-main-inspection



Challenges for Periodic Technical Inspections of Intelligent Cars

1st Mona Gierl
Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
mona.gierl@h-ka.de

2nd Felix Müller
Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
felix.mueller@h-ka.de

3rd Reiner Kriesten
Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
reiner.kriesten@h-ka.de

4th Philipp Nenninger
Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
philipp.nenninger@h-ka.de

5th Eric Sax
Institute for Information Processing Technologies
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
eric.sax@kit.edu

***Abstract*—The periodic technical inspection is a regulatory measure to ensure road safety and environmental sustainability during the operation of vehicles. It contains a non-destructive visual and impact assessment of its systems and components. With the advancement of autonomous and connected cars, new technologies, growing number of sensors, and new e/e-architecture designs find their way into the vehicle, which implies new challenges for the evaluation of road safety and environmental sustainability. In this paper, the need for advanced inspection methods due to upcoming new technologies enabling autonomous driving is investigated. A brief background about ongoing research and regulations addressing the verification and validation of autonomous and connected cars is given. The current procedure of periodic technical inspections in Germany is summarized and prospect challenges - addressing both, advancing technologies for autonomous vehicles and cyber security considerations of connected cars - are identified. Based on the listed challenges, possible improvements are derived, which should serve as a reference work to upcoming discussion about the extent of Periodic Technical Inspections (PTI) for autonomous cars.**

***Keywords*—periodic technical inspection, security, autonomous driving, homologation**

I. Introduction

As of today, human fault is still the main reason for accidents [1], whereas the advances in technology enable enhanced safety features leading to autonomous, connected vehicles. With the introduction and application of Advanced Driver Assistance Systems (ADAS) and connectivity features (as Car2X) the automotive industry provides intelligent vehicles as a solution for improved road safety.

Prospective vehicles are expected to have 20 times more computational power [2] and to be running on 100 million lines of code [3]. Thus, the technical advances come with an increase in sensor systems to reconstruct the surroundings and a growing number of software solutions which require a higher amount of data and computational effort. One side effect is the growing complexity which might lead to additional unwanted technical errors. Thus, it is common consensus to apply functional safety and cyber security standards during the development as well as testing throughout the development process and afterwards.

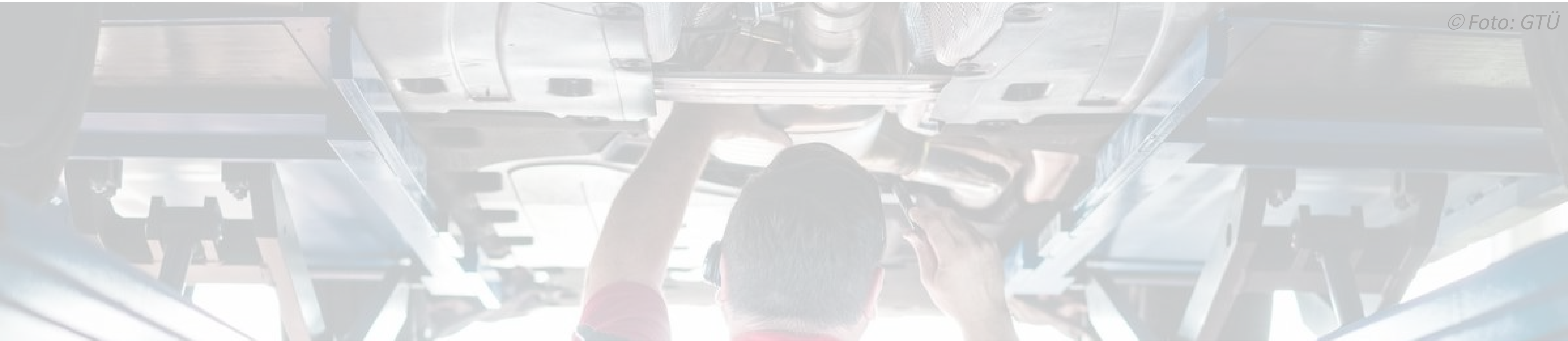
Beside verification and validation activities during development by the Original Equipment Manufacturers (OEMs), the vehicle has to be approved by an accredited authority to get road admission. This allows for an independent analysis on the car's roadworthiness and environmental sustainability across various types and models. Further, road admission depends on the condition of the vehicle which is regularly checked through mandatory periodic technical inspections which, e.g., occur every 2-3 years for passenger cars in Germany [4].

a) Problem statement: Mandatory technical inspections review the roadworthiness of vehicles and probe compliance with national environmental sustainability regulations. Regulatory standards (e.g., Regulation (EU) 2018/858 [7], Directive 2014/45/EU [8], etc.) prescribe a minimum set of required test procedures to show compliance to these regulations. With the advance of autonomous vehicles, a growing number of electronic systems (cameras, RADAR, LIDAR, etc.) are added as common equipment and enable the car to drive autonomously which simultaneously leads to a higher number of safety relevant systems. Consequently, an adaptation from the current mandatory test procedures is required.

b) Contribution: In this paper, current efforts to establish new test procedures for technical inspections are briefly highlighted and upcoming challenges due to the advances of intelligent vehicles are presented. In addition, current test procedures of passenger cars in Germany are summarized and potential improvements for periodic technical inspections based on the listed challenges are elaborated.

c) Classification of driving automation: In the field of autonomous driving, the SAE J3016 defined six levels of

The work presented in this paper was funded by GTÜ Gesellschaft für technische Überwachung mbH in Stuttgart, Germany.



Thank you for your attention!

Contact:

Mona Gierl, M.Sc.

University of Applied Sciences Karlsruhe

E-Mail: mona.gierl@h-ka.de
Web: www.h-ka.de/en/ieem/profile

IARIA

Hochschule Karlsruhe
University of
Applied Sciences
HKA

KIT
Karlsruher Institut für Technologie

GTÜ

Sources

[1] EU Commission, "EU road safety policy framework2021 – 2030: Next steps towards 'Vision Zero'", 2020, Mobility and Transport, doi:10.2832/391271

[2] M. Staron, "Automotive Software Architectures", 2017, Springer International Publishing, doi: 10.1007/978-3-319-58610-6

[3] Mercedes-Benz Group, "The front runner in automated driving and safety technologies", 2022, online: https://group.mercedes-benz.com/innovation/case/autonomous/drive-pilot-2.html, accessed: May 2022

[4] R. Bellan, "Germany gives greenlight to driverless vehicles on public roads", 2021, online: https://techcrunch.com/2021/05/24/germany-gives-greenlight-to-driverless-vehicles-on-public-roads/, accessed: May 2022

[5] United Nations, "UN R159 - Uniform provisions concerning the approval of motor vehicles with regard to the Moving Off Information System for the Detection of Pedestrians and Cyclists", 2021

[6] EU Parliament and Council, "Regulation (EU) 2019/2144 Type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users", 2019, online: https://eur-lex.europa.eu/eli/reg/2019/2144/oj, accessed: April 2022

[7] MAN Truck and Bus, "ATLAS-L4 funding project: self-driving from hub to hub", 2022, https://press.mantruckandbus.com/corporate/atlas-l4-funding-project-self-driving-from-hub-to-huben/, accessed: April 2022

[8] Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. Information 2019, 10, 148.

[9] Upstream Security, Upstream Security Global Automotive Cybersecurity Report 2020, online: https://www.upstream.auto/

Sources

[10] ISO, SAE, “ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering”, 2021

[11] EU , “Vehicle Inspection”, online: https://ec.europa.eu/transport/road_safety/eu-road-safety-policy/priorities/safe-vehicles/vehicle-inspection_en, accessed: May 2022

[12] German federal motor transport authority (Kraftfahrt-Bundesamt, kba), “Bestand an Kraftfahrzeugen und Kraftfahrzeuganhängern nach Fahrzeugalter” (Number of motor vehicles and trailers by vehicle age), 2021, FZ 15

[13] German federal motor transport authority (Kraftfahrt-Bundesamt, kba), “Jeder dritte Personenkraftwagen wies Mängel auf” (Every third passenger car had defects), 2020