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
Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe

Automotive Security + Technical Inspections

Concept Validation Production Operation Decommissioning
Development
European road safety measures 1 3 Technical Inspections
Automotive Security 2 4 Automotive Security Inspections
Vision Zero – European road safety measures


Goal: reduce road deaths to zero by 2050

„Safe System“ approach including:

– Infrastructure
– Safe road use
– Safe vehicles
– Emergency response

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
Features and Functions [2]

- Electronic fuel injection
- Antilock brakes

1975

1985

1995

2005

2015

2025

- Gearbox control
- Traction control
- CAN
- Electronic fuel injection
- Antilock brakes

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

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

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

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

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
Development of Intelligent Vehicles

SAE Level 0
- Automatic Emergency Braking
- Blind Spot Warning
- Lane Departure Warning
- Moving-Off Information System [5]

SAE Level 1/2
- Lane Centering
- Adaptive Cruise Control
- Intelligent Speed Assistance [6]

SAE Level 3
- Traffic Jam Chauffeur
- “Driver Pilot” [3]

SAE Level 4
- Local Driverless Taxi [4]
- Automated Valet Parking

SAE Level 5

Features

Driver support features
Automated driving features
Planned features

Complexity
Planned are the following safety features [6]:

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

Gradual introduction of technologies (A-D):

<table>
<thead>
<tr>
<th>Time stage</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>All new vehicle types</td>
<td>-</td>
<td>6 July 22</td>
<td>7 July 24</td>
<td>7 January 26</td>
</tr>
<tr>
<td>All vehicles registered for the first time</td>
<td>6 July 22</td>
<td>7 July 24</td>
<td>7 July 26</td>
<td>7 January 29</td>
</tr>
</tbody>
</table>
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 safety measures

1

Automotive Security

2

Technical Inspections

3

Automotive Security Inspections

4
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


### Attack Taxonomy

Classification scheme to describe known automotive security attacks

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Unauthorized flashing of malicious code on the engine ECU by using the diagnostic reprogramming routine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>Adventures in Automotive Networks and Control Units (C. Valasek et al.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Class</td>
<td>Tampering</td>
<td>Firmware Modification</td>
<td>None</td>
</tr>
<tr>
<td>Attack Base</td>
<td>Diagnostic Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Type</td>
<td>Real Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Violated Security</td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affected Asset</td>
<td>Information Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>CWE-693: Protection Mechanism Failure</td>
<td>CWE-287: Improper Authentication</td>
<td>Unauthorized reprogramming possible</td>
</tr>
<tr>
<td>Interface</td>
<td>OBD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Flashing of malicious code on ECU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Clause 9</th>
<th>Clause 10, 11</th>
<th>Clause 12</th>
<th>Clause 13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Development &amp; Validation</td>
<td>Production</td>
<td>Operation &amp; Maintenance</td>
</tr>
</tbody>
</table>

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, Verification & Validation
8. Cybersecurity Validation
9. Monitor, incident response, update, report

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
UN R155 in the Type Approval Framework

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

**Key Points:****

ISO/SAE 21434 → Determining ISO/SAE 21434

Interpretation Document → Ensuring correct interpretation of standards

EU Type Approval 2018/858/EU → European Union's approval framework

GSR 2019/2144/EU → General Safety Regulations

UN R155 Cybersecurity → International standard for cybersecurity in vehicles

Organizational Requirements:
- Cybersecurity Management System (CSMS)
- Risk assessment, protection of critical elements, implementation of appropriate measures

**Flowchart:****

1. ISO/SAE 21434
2. Interpretation Document
3. EU Type Approval 2018/858/EU
4. GSR 2019/2144/EU
5. UN R155 Cybersecurity
   - CSMS Certificate (max. 3 years)
   - Type Approval Certificate
   - Technical Service
     - CSMS Report
     - Documentation
   - Inspection Report
   - Type Approval Authority

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
European road safety measures

Automotive Security

Technical Inspections

Automotive Security Inspections
Security Lifecycle ISO/SAE 21434

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

- Concept
- Development
- Validation
- Production
- Operation
- Decommissioning

Type Approval

ca. 3 years

∅ 9,8 years*

Continuous CSMS Reports, Periodic Technical Inspections (PTI)

*Statistics of [12] for 2021

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
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)

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

27 % of defects in lighting equipment and other parts of the electronic system

10 % of defects in chassis, frame, body, parts attached to it

17 % of defects with an environmental Impact

16 % of defects in Axels, Wheels, Tires, Suspension

18 % of defects in the Braking System


Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
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.
### European road safety measures

1. **Automotive Security**
   - Keywords: Attack collection, taxonomy, ISO/SAE 21434, UN R155 process

2. **Technical Inspections**
   - Keywords: Roadworthiness assessment, 2014/45/EU Directive, inspection of equipment, condition, function, and performance

### Automotive Security Inspections

- Trust is Good, but Control is Better

- Mona Gierl, University of Applied Sciences Karlsruhe
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

Ø 9.8 years in Germany

Operating time

Automotive Security Inspections – Trust is Good, but Control is Better
Mona Gierl, University of Applied Sciences Karlsruhe
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:

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


Sources


[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