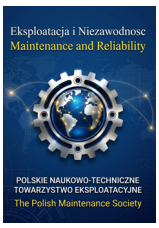

Eksploatacja i Niezawodnosc - Maintenance and Reliability

Volume 29 (2027), Issue 2

https://ein.org.pl

The Polish Maintenance Society

Vehicle ECU On-board diagnostic system threat analysis and risk assessment

Piotr Pełechaty[1,*], Łukasz Jan Konieczny[1]

[1] Faculty of Transport and Aviation Engineering, Silesian University of Technology, Poland
* Corresponding Author: piotr.pelechaty@polsl.pl

Received: 12 January 2026
Revised: 28 September 2026
Accepted: 2 October 2026
Online: 23 October 2026

This is an open access article under the CC BY 4.0 license

Abstract

This article presents a security assessment of the on-board diagnostic (OBD) system integrated into a vehicle's electronic control unit (ECU), specifically targeting the Unified Diagnostic Services (UDS) protocol. The research focuses on a representative Battery Management System (BMS) ECU for electric vehicles within its operational context. The study aims to evaluate security vulnerabilities across all OBD functionalities and propose risk mitigation strategies for software implementation. A Threat Analysis and Risk Assessment (TARA) was conducted following the ISO/SAE 21434 standard for road vehicle cybersecurity engineering. The authors identified seven primary assets requiring protection and defined 11 damage scenarios. Furthermore, feasibility ratings were calculated for 18 attack paths involving both physical and wireless OBD interfaces. Based on the assessment, the authors recommend specific software enhancements to mitigate the identified cybersecurity threats.

Keywords: *OBD, TARA, vehicle, security, risk*

Article citation:
Pełechaty P, Konieczny Ł J, Vehicle ECU On-board diagnostic system threat analysis and risk assessment, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2027: 29(2) http://doi.org/10.17531/ein/241316

Highlights

- Conducting security Threat Analysis and Risk Assessment of ECU OBD functionality.
- Damage scenarios impacting safety caused by diagnostic functions.
- Feasibility rating of local OBD attacks is higher than wireless.
- Risk mitigation for OBD software implementation is possible.

1. Introduction

Individual ECUs in modern vehicles control various electronic systems, affecting functionality and safety. Each of these ECUs provides a self-diagnostic function accessed via the traditional 16-pin On-Board Diagnostic (OBD) data link connector (DLC) port inside the vehicle or over a cellular interface in newer models [1]. Currently, the diagnostic interface offers extensive functionality beyond standard DTC and PID readouts, such as software flashing, calibration and test routines implementing the UDS protocol [2–4]. The diagnostic interface's wide range of functions significantly raises security concerns and expands the potential attack surface.

Unauthorized access to specific diagnostic procedures can pose significant security threats leading to safety, operational, and financial damage [5,6]. The diagnostic interface may be misused to perform unauthorized vehicle modifications (e.g., chip tuning) or post-crash repairs that do not comply with required specifications (e.g., the reuse of second-hand safety components). The ECU firmware can be manipulated by attacks utilizing diagnostic interfaces [7]. As pointed by the ENISA agency, users or insufficiently trained staff may also unintentionally disrupt vehicle systems through the diagnostic interface by misconfiguration or uncertified diagnostic tools [8].

The obligatory regulation UNECE R155 (approval of vehicles with regard to cybersecurity and cybersecurity management systems) lists the OBD port and diagnostic functionality as one of the potential threats to the vehicle and requires security controls to be applied [9]. Thus, it is essential to develop access control for ECU diagnostic functions through user and test-tool authentication. On the other hand, EU

Regulation 2018/858 ensures the “right to repair” by mandating the availability of standardized diagnostics beyond traditional OBD on the CAN bus for all vehicle systems in the European market [10,11].

Establishing an optimal balance between the open availability of standard diagnostic procedures (which are essential for independent repair workshops) and the cybersecurity of specialized enhanced diagnostic functions remains a critical challenge, particularly when constrained by cost-effectiveness. Throughout the software development process and the formulation of the security concept, engineers must rigorously classify diagnostic functionalities. This classification dictates whether specific routines should remain unrestricted, require strict user authentication, or should be permanently disabled in production vehicles.

A key part of the system design is choosing the right cryptographic protection and deciding between symmetric and asymmetric cryptography, which offers stronger security but incurs higher costs and operational overhead. This choice directly affects the selection of UDS protocol access control mechanisms: either the UDS Security Access service (SID 0x27) using symmetric challenge-response methods, or the UDS Authentication service (SID 0x29) based on an asymmetric Public Key Infrastructure (PKI). Finally, ensuring the integrity, authenticity, and confidentiality of data accessed or flashed via diagnostic interfaces requires the implementation of mechanisms ranging from basic integrity checks (e.g., CRC) to advanced Secure Boot and Authenticated Boot solutions.

To systematically navigate these complex design choices and ensure compliance with mandatory vehicle type-approval regulations such as UNECE R155, conducting a Threat Analysis and Risk Assessment (TARA) is needed [12]. The structured process of conducting this risk analysis and making design decisions is defined by the ISO/SAE 21434 standard and its conceptual predecessor, the HEAVENS methodology. Both the HEAVENS framework and the ISO/SAE 21434 standard provide a comprehensive approach for identifying attack vectors, evaluating threat feasibility, and determining the specific risk profile of each diagnostic service [12,13].

Applying this risk-driven approach enables engineers to implement proportionate countermeasures, preventing both the under-protection of critical functions and the costly over-engineering of low-risk operations. Ultimately, a rigorous TARA (Threat Analysis and Risk Assessment) grounded in the HEAVENS methodology and aligned with ISO/SAE 21434 serves as the critical step for designing an optimized, regulatory-compliant security architecture that effectively safeguards vehicle diagnostic interfaces across all lifecycle phases [12,14].

2. Motivation

High-level cybersecurity frameworks (e.g., HEAVENS and EVITA), along with the UNECE R155 regulation and the ISO/SAE 21434 standard, frequently use the generic term "OBD" (On-Board Diagnostics) to categorize diagnostic-related attack vectors. However, this broad classification can be misleading, as it encompasses multiple distinct protocols and routines. This study aims to demystify the general "OBD" umbrella by explicitly focusing on the Unified Diagnostic Services (UDS) protocol, performing an in-depth analysis of attack trees to identify the concrete UDS services that can be exploited by malicious actors. While existing literature often treats OBD as a generalized attack surface [15], our research explicitly decomposes UDS services into 18 distinct attack paths and assigns them quantitative feasibility ratings

Furthermore, conducting a rigorous Threat Analysis and Risk Assessment (TARA) requires a granular understanding of the target system. By utilizing a representative Battery Management System (BMS) ECU model, this study facilitates the differentiation of attack scenarios based on the specific memory domains targeted—namely RAM, Flash Firmware, and Flash Calibration data. This hardware-aware approach, combined with a detailed examination of the underlying AUTOSAR software architecture and the Diagnostic Communication Manager (DCM) module, significantly enhances the precision of the analysis and directly influences the final risk assessment outcomes.

This study is designed to serve as a practical example for adapting legacy ECUs to meet contemporary cybersecurity requirements. Ultimately, these findings directly contribute to the development of knowledge demonstrating how theoretical security concepts can be translated into actionable engineering practices, providing cost-effective risk treatment solutions.

3. BMS OBD risk assessment

This chapter delineates the TARA methodology according to the ISO/SAE 21434 (Road vehicles—Cybersecurity engineering) standard, using a BMS ECU as an example for cybersecurity risk determination. The considerations are limited to the on-board diagnostic functionalities of the ECU; other attack paths were omitted, as the goal of the research is to improve the security and robustness of OBD software implementations.

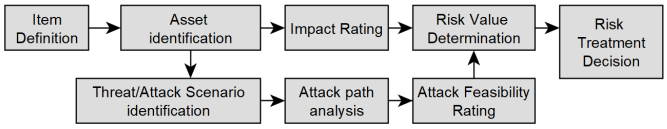

Figure 1. The ISO 21434 TARA process diagram.

3.1. BMS ECU item definition

For the TARA, a representative Battery Management System (BMS) ECU was selected. It is responsible for managing high-voltage battery operations, including HV contactor control, battery status monitoring, charge process management, and State of Charge (SoC) estimation. The BMS ECU is an embedded system architected around a specialized microcontroller running dedicated firmware. Every TARA process shall start with a detailed item definition and boundaries definition of the assessed system (Figure 2.)

- The main high-voltage switch is connected to the ECU over the DIO ports. The switch status depends on the actual driving situation of the vehicle, and it is the main safety feature when disconnecting the high-voltage battery from the electric motor.
- The BMS ECU communicates over SPI_1 and SPI_2 with the HV battery and the integrated battery temperature sensor. The SPI_1 is used for battery cell monitoring and balancing.
- The BMS system is equipped with an external high-voltage and current sensor connected to the CAN_Private Bus. The sensors are cyclically providing measurements to the BMS ECU.
- Inside the BMS flash memory calibration values are stored, including threshold values for maximum current, etc. The calibration values are initially written in the production process for individual ECUs but can be updated in the dealership by the on-board diagnostic functionality compliant with the UDS protocol.
- The integrated bootloader can update the ECU's firmware over the CAN_1 bus. The bootloader mode can be entered over on-board diagnostic functions provided by the UDS protocol [3]. The bootloader erases the firmware before downloading and decrypting the new firmware from CAN_1. To protect the manufacturer's intellectual property and ensure data confidentiality during transit, the firmware payload is transmitted in an encrypted format using a symmetric cipher (AES-128). The new firmware will be set as valid and executed only if the CRC (for safety check) and RSA 2048 signature (security authenticity check) are verified successfully. The X.509 certificate, including the public key, is stored in BMS ECU flash memory. When invalid firmware is downloaded or the download procedure is interrupted, the BMS ECU will stay in bootloader mode, waiting for the next firmware update.
- The BMS ECU microcontroller is equipped with a Hardware Security Module (HSM), which serves as a dedicated security core. At every startup, the HSM verifies the integrity of the ECU firmware through a Secure Boot process, utilizing a symmetric AES-128 CMAC calculation. The cryptographic keys are stored securely within the HSM and are inaccessible to the application core. If the Secure Boot verification fails, the ECU remains in bootloader mode, awaiting a valid firmware update.
- ECU firmware includes the Diagnostic Communication Manager (DCM) component responsible for implementing diagnostic protocol, ensuring compliance with the AUTOSAR architecture [16]. The DCM supports both legislated OBD protocols (ISO 15031 / SAE J1979) and Unified Diagnostic Services (UDS, ISO 14229). To protect safety- and security-critical functionalities, the UDS protocol implements authentication process via service 0x27 (“Security Access”) or service 0x29 (“Authentication”) [3]. This process employs a unidirectional challenge-response mechanism using either symmetric cryptography (AES-128) or asymmetric cryptography (RSA-2048 or similar) without a session key exchange. Upon successful

authentication, the diagnostic tool is authorized to execute specific subsets of diagnostic functions, governed by Role-Based Access Control (RBAC) defined in the tool's certificate. The private key for authentication is managed securely by a PKI server, while the corresponding public key, contained within an X.509 certificate, is stored in the BMS ECU's non-volatile memory (Flash).

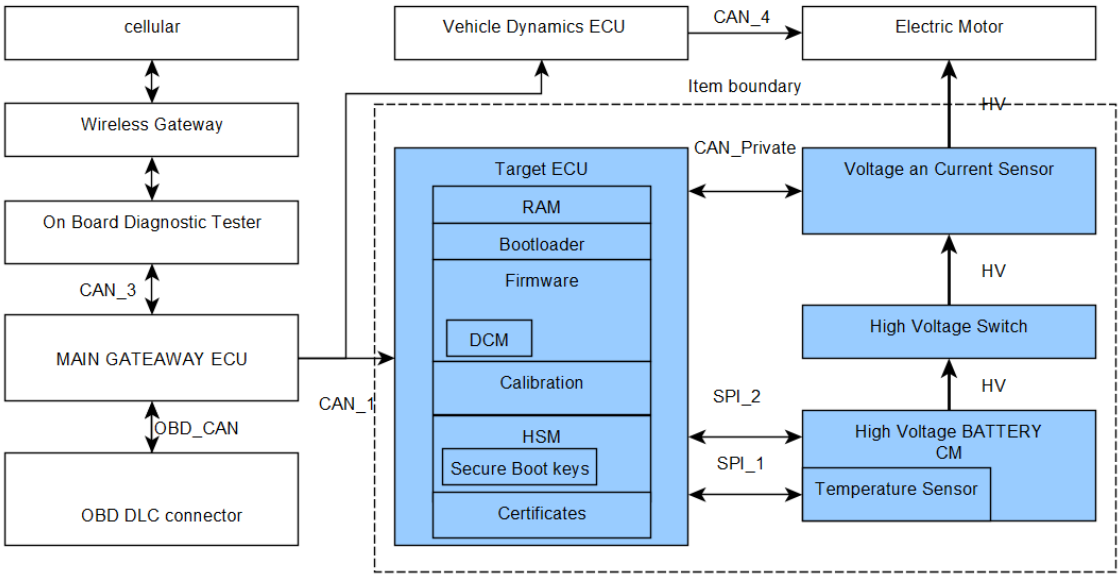

Figure 2. Item definition schematic of the Battery Management ECU and its operational environment within the electric vehicle.

The direct operational environment of the BMS ECU consists of:

- CAN_1 bus connecting the BMS to other ECUs inside the vehicle and main gateway. This bus is used for safety data exchange.
- The Vehicle Dynamics ECU (VD ECU) controls the electric motor torque and ESP braking functions. It communicates with the BMS ECU on CAN_1, providing driving situation signals and receiving the HV battery status information.
- On-board diagnostic connector OBD DLC connected to a dedicated OBD_CAN bus which is interfaced with the CAN_1 network via the main gateway.
- The main gateway is acting as a firewall for the CAN_1 bus, filtering the incoming bus traffic before forwarding it to CAN_1. It allows only specific diagnostic messages to be sent from the OBD DLC port to CAN_1.
- A cellular (LTE) connection to the OEM backend enables remote access to the BMS ECU's on-board diagnostic functionality. It is assumed that this cellular interface is secured via TLS connections, accessible exclusively by the vehicle OEM. All cellular communication is filtered by a wireless communication gateway and deserialized by an on-board diagnostic module before being forwarded to the main gateway ECU via the CAN_3 bus.
- Electric motor supplied by high-voltage (HV) and controlled by the main high-voltage switch and measured by the voltage and current switch.

3.2. Asset definition and damage scenario identification

This section identifies the assets requiring protection within the representative BMS ECU, along with their cybersecurity properties: Confidentiality (C), Integrity (I), and Availability (A). These assets are subsequently mapped to potential damage scenarios (DS.X). The impact rating for each scenario is evaluated across four categories: Safety, Financial, Operational, and Privacy (SFOP). The assessment criteria conform to Appendix F of the ISO/SAE 21434 standard and are grounded in the system item definition [12]. Finally, the list of damage scenarios has been aggregated to present only those with the highest impact rating in each category (Table 1).

In total 7 main assets were identified:

- CAN_1 bus communication,
- CAN_Private bus communication,
- firmware,

- calibration data,
- RAM data,
- crypto material,
- SPI/DIO.

As presented in Table 1, compromising system assets can lead to serious safety risks for passengers, result in vehicle immobilization, and cause significant financial losses for the manufacturer (OEM). While these findings highlight critical vulnerabilities, a full assessment depends on analyzing how feasible specific attacks are. This step is essential to accurately determine the overall cybersecurity risk [12].

Table 1. Asset list and their properties assigned to the highest-rated damage scenario.

	Asset	Property C / I / A	Damage scenario	Impact Rating Category (SFOP)	Rating (factor)
DS.1	CAN_1 Bus Communication	A	CAN_1 Bus communication not available. The main HV switch cannot be closed. Vehicle cannot be driven.	O	Severe (2,0)
DS.2	CAN_1 Bus Communication	I	CAN_1 Bus data overwritten. BMS status frames affected. Change in vehicle dynamics or unintended vehicle stop.	S	Major (1,5)
DS.3	CAN_Private Bus Communication	I / A	CAN_Private Bus data modified or not available. Modification of private current sensor parameters- impact on vehicle dynamics and engine torque.	S	Major (1,5)
DS.4	ECU Firmware	A	ECU Firmware erased. Vehicle cannot be driven.	O	Severe (2,0)
DS.5	ECU Firmware	I	ECU Firmware modified by 3rd Party. HV Battery management affected - overheating and fire while driving.	S	Severe (2,0)
DS.6	ECU Firmware	C	ECU Firmware read out. Loss of intellectual property ECU of supplier.	F	Major (1,5)
DS.7	ECU Calibration	A	ECU Calibration erased or invalid. Vehicle cannot be driven.	O	Severe (2,0)
DS.8	ECU Calibration	I	ECU Calibration modified by 3rd Party. HV Battery management affected - overheating and fire while driving.	S	Severe (2,0)
DS.9	ECU RAM Memory	I	Modification of ECU RAM Memory. HV Battery management affected - Battery overheating and fire while driving.	S	Severe (2,0)
DS.10	Private Crypto Material	C / I /A	Private crypto material (keys) not available or modified or disclosed. No Secure diagnostic (UDS). No firmware update - security concept not valid.	O	Severe (2,0)
DS.11	SPI_1 and DIO Communication	I / A	Battery Actuators and BMS communication not possible HV Battery management affected - Vehicle cannot be driven.	O	Severe (2,0)

3.3. Threat scenario identification and feasibility rating

Based on the identified system assets and damage scenarios (Table 1.), specific **attack scenarios** were delineated that impact these assets and induce malfunctions. For the purposes of this study, the focus was narrowed to attack scenarios concerning on-board diagnostic functions, which in the analyzed system are accessible via the physical OBD Data Link Connector (DLC) and wireless 5G/WiFi interfaces (Figure 2.). To define these attack scenarios, the Microsoft STRIDE methodology was employed, enabling the classification of system cyber-threats based on **S**poofing, **T**ampering, (Non) **R**epudiation, **I**nformation Disclosure, **D**enial of service, **E**levation of Privileges [17].

The analysis involves identifying and detailing all potential threat paths, referred to as **Attack Paths**. To maintain the conciseness of this chapter while providing a more comprehensive overview of various trajectories, the author has opted for a descriptive presentation of these attack paths rather than employing expanded system diagrams.

The final stage of this analytical phase is the **feasibility assessment** of the attack paths. To evaluate feasibility, specific parameter values were calculated to represent the attack potential, in accordance with the IT security evaluation methodology defined in the **ISO/IEC 18045:2022** standard [18]. The parameters influencing the feasibility of an attack path include **ET** (Elapsed Time), **SE** (Specialist Expertise), **Ko** (Knowledge of the item), **Wo** (Window of Opportunity), and **Eq** (Equipment). Numerical values were assigned to these parameters to represent the degree of difficulty in executing the attack (Table 2.). Feasibility rating V_a is expressed as the sum of all parameter values, where a lower V_a value signifies higher attack feasibility. The feasibility value is calculated using the following formula:

$$Va = ET + SE + Ko + Wo + Eq \quad (1)$$

where:

Table 2. Attack potential values used for feasibility rating.

Elapsed Time (**ET**)		Specialist expertise (**SE**)		Knowledge of the item (**Ko**)		Window of Opportunity (**Wo**)		Equipment (**Eq**)	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤ 1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤ 1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤ 1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤ 6 months	17	Multiple experts	8	Strictly confidential	11	Difficult / none	10	Multiple bespoke	9

A comprehensive list of these attack scenarios, along with their assigned attack paths, is provided below. Attack paths were labeled according to template **AP.*X.Y.Z*** where:

X is the related damage scenario ID (DS.X from Table 1.),

Y is attack scenario ID value {1;13}, (13 different attack scenarios were identified),

Z is attack path ID value.

Attack scenario 1

Applies for CAN_1 availability related to damage scenario 1 (DS.1).

A denial of Service on the CAN_1 bus can be caused by signal jamming or by flooding the bus with too many CAN frames when additional security measures not applied [19,20]. This saturates the system and prevents frame transmission. CAN_1 bus is partly protected by the main gateway ECU, which filters communication from diagnostic interfaces.

- **Attack Path AP.1.1.1 - CAN_1 flooding by OBD DLC**:
  a) Compromising the main gateway ECU to forward all OBD_CAN messages to the CAN_1 bus (high priority non diag. CAN IDs) at high frequencies.
  b) A jamming device connected to the OBD DLC port injects invalid, high-priority CAN messages at a high frequency. These messages are forwarded directly to the CAN_1 bus by the gateway ECU, resulting in bus saturation.

Feasibility assessment parameter values for AP.1.1.1:

$ET = 1$; $SE = 6$; $Ko = 7$; $Wo = 4$; $Eq = 4$; $\boldsymbol{Va = 22\ (low)}$ (2)

- **Attack Path AP.1.1.2 - CAN_1 flooding by wireless OBD**:
  a) Gaining unauthorized access to the 5G/WiFi wireless diagnostic protocol. This involves obtaining the access password and extracting vehicle data.
  b) Gaining unauthorized access to the wireless communication gateway. Manipulating or obtaining security keys to control the gateway.
  c) Manipulating the on-board diagnostic tester ECU to send jamming frames. The goal is to force the ECU to transmit interference that disrupts system communication.
  d) Compromising the main gateway ECU to forward all OBD_CAN messages to the CAN_1 bus (high priority non diag. CAN IDs) at high frequencies.

Feasibility assessment parameter values for AP.1.1.2

$ET = 1$; $SE = 6$; $Ko = 11$; $Wo = 0$; $Eq = 7$; $\boldsymbol{Va = 25\ (low)}$ (3)

Attack scenario 2

Applies for integrity of CAN_1 bus communication related to damage scenario 2 (DS.2).

Reverse engineering and tampering CAN_1 bus is possible by overwriting or injecting frames [19, 21]. Original frames can be overwritten, or additional frames can be injected. This is due to the CAN bus specification, which only provides functional safety mechanisms, such as end-to-end (E2E) protection, but lacks built-in cryptographic security [20]. Still CAN_1 bus is protected by the main gateway ECU, which filters communication from diagnostic interfaces.

- **Attack Path AP.2.2.1 - tampering CAN_1 by OBD DLC**:

This attack path is very similar to above AP.1.1.1 (sending crafted CAN frames instead of jamming).

- **Attack Path AP.2.2.2 - tampering CAN_1 over wireless OBD**:

This attack path is very similar to above AP.1.1.2 (sending crafted CAN frames instead of jamming).

Attack scenario 3

Applies to CAN-Private Bus integrity and availability (DS.3).

The CAN-Private bus is an isolated network connecting the BMS ECU and its sensors. Diagnostic traffic from the OBD-CAN and CAN-3 buses can only interfere with the CAN-Private bus if the BMS ECU itself is completely compromised. Out of

scope.

Attack scenario 4

Applies for firmware availability (DS.4).

The BMS ECU firmware is vulnerable to erasure through unauthorized update session spoofing. The update mechanism typically erases the application memory prior to receiving and verifying new data via the bootloader. If a spoofed update is initiated and subsequently aborted, the controller is left without valid software restricted to bootloader mode. The firmware update is conducted via the UDS protocol and secured by the "Security Access" authentication process.

- **Attack Path AP.4.4.1– firmware erasing by OBD spoofing**:
  a) Physical connection of a basic UDS diagnostic tool to the OBD DLC.
  b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) to gain enhanced diagnostic access [22,23].
  c) Initiating a software update ("Start Programming Session") that remains incomplete or invalid.

Feasibility assessment parameter values for AP.4.4.1

$ET = 1$; $SE = 3$; $Ko = 7$; $Wo = 4$; $Eq = 0$; $\boldsymbol{Va = 15}$ **(medium)** (4)

Attack scenario 5

Applies for firmware availability (DS.4).

The availability of the BMS ECU firmware can be compromised by a Denial of Service (DoS) targeting the software update process. It may become impossible to remotely install safety-critical updates by a device that interferes with UDS diagnostic communication used for the update procedure.

- **Attack Path AP.4.5.1- denial of Service of firmware update process:**
  a) Physical connection of a custom-built tool to the OBD DLC.
  b) Manipulating the Gateway ECU to accept simultaneous diagnostic communication from both the CAN-OBD and CAN-3 buses by precisely timing the transmission of frames.
  c) Monitoring and waiting for the remote software update process (originating from wireless and CAN-3 connections).
  d) Issuing the UDS 0x37 ("Request Transfer Exit") command at the appropriate moment to interrupt the data transfer process.

Feasibility assessment parameter values for AP.4.5.1

$ET = 1$; $SE = 6$; $Ko = 3$; $Wo = 10$; $Eq = 7$; $\boldsymbol{Va = 27}$ **(very low)** (5)

Attack scenario 6

Applies for firmware integrity (DS.5).

Tampering with the BMS ECU firmware is possible through modifications of the flash memory or by uploading unauthorized software to the controller. The diagnostic UDS protocol supports special services for memory write operations which are protected by "Security Access". The firmware integrity is protected by HSM secure boot. Firmware signature is verified when downloaded.

- **Attack Path AP.5.6.1– tampering of firmware over OBD DLC**:
  a) Connection of a specialized bespoke UDS diagnostic tool to the OBD DLC.
  b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) [22,23].
  c) Initiating UDS services for writing to the Flash memory 0x3D ("Write Memory by Address").
  d) Bypassing or compromising the software integrity verification mechanisms (Secure Boot).

Feasibility assessment parameter values for AP.5.6.1

$ET = 1$; $SE = 6$; $Ko = 7$; $Wo = 4$; $Eq = 4$; $\boldsymbol{Va = 22}$ **(low)** (6)

- **Attack Path AP.5.6.2- flashing a modified software image over OBD DLC**:
  a) Preparing custom firmware image and digital signature, which requires an RSA private key.
  b) Physical connection of a basic UDS diagnostic tool to the OBD DLC.
  c) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) to gain enhanced diagnostic access [22,23].
  d) Flash the custom firmware.

Feasibility assessment parameter values for AP.5.6.2

$ET = 1$; $SE = 6$; $Ko = 11$; $Wo = 4$; $Eq = 0$; $\boldsymbol{Va = 22}$ **(low)** (7)

- **Attack Path AP.5.6.3 - flashing a modified software image over wireless OBD:**
  a) Preparing custom firmware image and digital signature, which requires an RSA private key.
  b) Gaining unauthorized access to the 5G/WiFi wireless

diagnostic protocol. This involves obtaining the access password and extracting vehicle data.

c) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) to gain enhanced diagnostic access [22, 23].

d) Flash the custom firmware.

Feasibility assessment parameter values for AP.5.6.3

$ET = 1$; $SE = 8$; $Ko = 11$; $Wo = 0$; $Eq = 7$; $\boldsymbol{Va = 27}$ **(very low)** (8)

Attack scenario 7

Confidentiality of firmware (DS.6).

The BMS ECU firmware may be accessed by unauthorized parties, leading to information disclosure. Extracting the software from the controller's flash memory and its subsequent decompilation can result in the loss of intellectual property and pose significant cybersecurity threats.

- **Attack Path AP.6.7.1 – firmware readout over OBD**:
  a) Physical connection of a basic UDS diagnostic tool to the OBD DLC.
  b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) to gain enhanced diagnostic access [22,23].
  c) Issuing the UDS service 0x23 ("Read Memory by Address") to read the firmware from flash memory.

Feasibility assessment parameter values for AP.6.7.1

$ET = 1$; $SE = 3$; $Ko = 7$; $Wo = 4$; $Eq = 0$; $\boldsymbol{Va = 15}$ **(medium)** (9)

- **Attack Path AP.6.7.2 - sniffing the firmware update communication:**
  a) Connecting a specialized CAN bus data logger directly to the CAN_1 bus.
  b) Awaiting the UDS protocol software update process and recording the transmitted data.
  c) Decompressing and decrypting the firmware, which requires secret AES keys.

Feasibility assessment parameter values for AP.6.7.2

$ET = 4$; $SE = 3$; $Ko = 7$; $Wo = 10$; $Eq = 4$; $\boldsymbol{Va = 28}$ **(very low)** (10)

Attack scenario 8

Applies for calibration data availability (DS.7).

A Denial of Service affecting the BMS ECU calibration can be achieved through the erasure of its non-volatile flash memory. Removal of calibration data is possible via diagnostic services; however, this function is restricted to production environments and authorized workshops, requiring prior "Security Access" authentication.

- **Attack Path AP.7.8.1 – calibration data erasing over OBD DLC:**
  a) Physical connection of a basic UDS diagnostic tool to the OBD DLC.
  b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) [22,23].
  c) Issuing the UDS dedicated routine 0x31 clearing all calibration data.

Feasibility assessment parameter values for AP.7.8.1

$ET = 1$; $SE = 3$; $Ko = 7$; $Wo = 4$; $Eq = 0$; $\boldsymbol{Va = 15}$ **(medium)** (11)

Attack scenario 9

Applies for calibration data tampering (DS.8).

Overwriting the calibration values in the memory using the diagnostic write commands is possible. Manipulated or invalid calibration data may influence the BMS system's behavior. Writing calibration data is possible via diagnostic services; however, this function is restricted to production environments and authorized workshops, requiring prior Security Access authentication.

- **Attack Path AP.8.9.1 - Overwrite calibration data over OBD DLC:**
  a) Physical connection of a basic UDS diagnostic tool to the OBD DLC.
  b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) [22,23].
  c) Overwriting calibration memory values via UDS diagnostic services 0x3D ("Write Memory by Address").

Feasibility assessment parameter values for AP.8.9.1

$ET = 1$; $SE = 3$; $Ko = 7$; $Wo = 4$; $Eq = 0$; $\boldsymbol{Va = 15}$ **(medium)** (12)

- **Attack Path AP.8.9.2 - Overwrite calibration data over wireless OBD:**
  a) Gaining unauthorized access to the 5G/WiFi wireless diagnostic protocol. This involves obtaining the access password and extracting vehicle data.
  b) Gaining unauthorized access to the wireless communication gateway. Manipulating or obtaining security keys to control the gateway.
  c) Bypassing the security of the on-board tester

diagnostic authentication process.

d) Compromising the UDS protocol diagnostic authentication process (Security Access" Service) [22,23].

e) Overwriting calibration memory values via UDS diagnostic services 0x3D ("Write Memory by Address").

Feasibility assessment parameter values for AP.8.9.2

$ET = 1$; $SE = 8$; $Ko = 11$; $Wo = 0$; $Eq = 7$; $\boldsymbol{Va}$ **= 27 (very low)** (13)

Attack scenario 10

Applies for RAM data tampering (DS.9).

RAM memory tampering can be achieved in similar way as non-volatile calibration memory tampering. Direct write operation to ram variables is utilized in development phase or in forensic cases.

- **Attack Path AP.9.10.1 - overwrite RAM data over OBD DLC**

This attack path is very similar to above AP.8.9.1 (only difference in physical memory address).

- **Attack Path AP.9.10.2 - overwrite RAM data over wireless OBD**

This attack path is very similar to above AP.8.9.2 (only difference in memory address).

Attack scenario 11

Applies for private cryptographic material (DS.10).

As the private cryptographic material is stored in secure HSM memory and cannot be overwritten by any diagnostic command, no attack path related to onboard diagnostic functionality was found. Out of scope.

Attack scenario 12

Applies for availability of the SPI and DIO functionality (DS.11).

Disrupting the microcontroller can lead to a Denial of Service of its peripheral hardware. In the event of a shutdown or reset, the BMS ECU cannot actuate the high-voltage contactor to vehicle operation.

- **Attack Path AP.11.12.1 - disabling SPI and DIO functionality:**

a) Connecting an attacking device to the OBD Data Link Connector (DLC).

b) Transmitting specially crafted diagnostic requests to the controller that cause a system halt or reset due to errors in the DCM (Diagnostic Communication Manager) module, utilizing fuzzing or buffer overflow techniques.

Feasibility assessment parameter values for AP.11.12.1

$ET = 4$; $SE = 3$; $Ko = 0$; $Wo = 4$; $Eq = 4$; $\boldsymbol{Va}$ **= 15 (medium)** (14)

Attack scenario 13

Applies for integrity of the SPI and DIO communication (DS.11).

Tampering with the functionality of peripheral interfaces is possible via diagnostic functions. Services controlling SPI and DIO are implemented for manufacturing and maintenance testing; they are strictly restricted to specific diagnostic modes and require prior UDS "Security Access" authentication.

- **Attack Path AP.11.13.1 - tampering SPI and DIO communication over OBD DLC:**

a) Physical connection of a basic UDS diagnostic tool to the OBD DLC.

b) Compromising the UDS protocol diagnostic authentication process ("Security Access" Service) [22,23].

c) Enter production or repair mode and execute UDS diagnostic routines controlling the SPI and DIO peripheral interfaces.

Feasibility assessment parameter values for AP.11.13.1

$ET = 1$; $SE = 6$; $Ko = 7$; $Wo = 4$; $Eq = 4$; $\boldsymbol{Va}$ **= 22 (low)** (15)

3.4. Feasibility rating argumentation

To explain the reasoning behind the attack potential parameter values given above, two examples will be decomposed and explained in detail (see the parameter values in Table 2).

The first example examines the attack path **AP.8.9.1** - the feasibility rating of tampering with the BMS ECU calibration data stored in flash memory.

- **Elapsed Time (ET)** is set to 1. The attack can be conducted in a timeframe shorter than one week but longer than one day. This time is consumed by trial-and-error attempts to modify the calibration values, as reverse engineering is required.
- **Specialist Expertise (SE)** is set to 3 (Proficient). The attacker needs expertise in the UDS protocol and must understand the calibration data layout of the specific BMS ECU (requiring reverse engineering) [22,24].

- **Knowledge of the Item (Ko)** is set to a high value of 7 (representing confidential knowledge). This is because the attacker needs access to confidential information regarding the UDS authentication process for the specific BMS ECU. Specifically, the private key for the challenge-response mechanism is required (UDS Service 0x27 “Security Access” or 0x29 “Authentication”). Access to the diagnostic authentication keys for writing calibration data is restricted strictly to production lines and authorized workshops [22,24].
- **Window of Opportunity (Wo)** is set to 4 (Moderate). The feasibility of accessing the UDS interface depends to a high degree on the assumed attacker profile. In the evaluation of attack paths requiring physical OBD access, a Window of Opportunity value of 4 (Moderate) was assigned, in accordance with ISO/SAE 21434 guidelines. This value reflects the general constraints of physical attacks, which require presence inside the vehicle.
- **Equipment (Eq)** is set to 0 (Standard). A standard OBD dongle or interface that supports UDS services (e.g., 0x3D – "Write Memory By Address") is sufficient. Such devices are widely accessible on the market.

Summing these parameter values, the total feasibility rating (Va) is 15, which indicates a medium attack feasibility.

It should be noted that alternative paths for the same attack exist. For instance, an attacker could utilize specialized equipment, such as the OEM's proprietary diagnostic testers. In this case, the Eq parameter would increase to a maximum value of 9, while the Knowledge of the item (Ko) parameter would decrease to 3. However, regarding the final score, this attack variant would ultimately be less feasible (Va = 20).

Next, let's examine the attack path **AP.5.6.3**—the feasibility rating of tampering with the firmware over the wireless OBD interface.

- **Elapsed Time (ET)** is set to 1. The attack can be conducted in a few days. This accounts for the time required to gather all necessary information and execute the complex attack.
- **Specialist Expertise (SE)** is set to 8 (Multiple Experts). The attack requires deep, multidisciplinary expertise in vehicle cellular networks, the UDS protocol, and the reverse engineering of the firmware signing process [25].
- **Knowledge of the Item (Ko)** is set to a high value of 11 (representing strictly confidential knowledge). The attackers need unauthorized access to a highly protected cellular connection to the vehicle (involving TLS protection certificates), which is exclusively granted to the vehicle manufacturer. Furthermore, since the firmware downloaded to the BMS ECU is digitally signed, the attacker must acquire the private asymmetric RSA key. Only the official firmware signing authority possesses this key [25].
- **Window of Opportunity (Wo)** is set to 0 (Unlimited). Cellular access is ubiquitous, allowing the attack to be executed remotely from any distance.
- **Equipment (Eq)** is set to 7 (Bespoke). Specialized, custom-built equipment is required to perform the attack. Diagnostic devices capable of establishing remote cellular connections to specific vehicle models are not standardized; they are developed and used exclusively by OEMs.

Summing up these parameter values, the total feasibility rating (Va) is 27, which indicates a very low attack feasibility.

3.5. Risk value determination

The final risk value is determined by integrating impact and feasibility metrics. To achieve this, a custom calculation methodology was developed that complies with ISO/SAE 21434 requirements while circumventing the intermediate translation of feasibility ratings into descriptive categories. By reducing the number of analytical steps, this approach yields a more streamlined and efficient Threat Analysis and Risk Assessment (TARA). The proposed formula consolidates the standard two-step remapping process into a single continuous function, consequently increasing the resolution of the resulting risk values.

The proposed risk calculation formula:

$$R = \begin{cases} I * (\frac{30-Va}{5}), Va < 30 \\ 0 \qquad\qquad\quad , Va \geq 30 \end{cases} \tag{16}$$

R: Value representing relative risk.

I: Damage scenario impact rating (Table 1.).

Va: Attack path feasibility rating related to corresponding damage scenario.

The outcomes of the risk calculations are summarized in Table 3. For comparative purposes, standard risk values (Rs),

derived in accordance with ISO/SAE 21434 Appendix H, are also included. This comparison demonstrates that the proposed methodology accurately preserves the relative distribution of high and low risk levels. It should be noted that the absolute risk values are of secondary importance; rather, their relative magnitudes across all evaluated attack paths are essential for identifying and prioritizing the most critical threats.

4. Risk treatment

High risk value (6,00) was identified for 5 attack paths:

- AP.4.4.1 - firmware erasing by OBD DLC spoofing,
- AP.7.8.1 - calibration data erasing over OBD DLC,
- AP.8.9.1 - tampering calibration data over OBD DLC,
- AP.9.10.1 - tampering RAM data over OBD DLC.
- AP.11.12.1 – disabling SPI and DIO functionality.

Table 3. Risk value calculation for all threat scenarios based on impact and feasibility rating.

Damage Scenario		**Attack Path**		**RISK (R)**	**RISK (Rs)**
ID	Impact **(I)**	ID	Feasibility **(Va)**		
DS.1	Operational, Severe (2)	AP.1.1.1	22	3,20	3
		AP.1.1.2	25	2,00	2
DS.2	Safety, Major (1,5)	AP.2.2.1	22	2,40	2
		AP.2.2.2	25	2,00	1
DS.4	Operational, Severe (2)	AP.4.4.1	15	6,00	**4**
		AP.4.5.1	27	1,20	2
DS.5	Safety, Severe (2)	AP.5.6.1	22	3,20	3
		AP.5.6.2	22	3,20	3
		AP.5.6.3	27	1,20	2
DS.6	Financial, Major (1,5)	AP.6.7.1	15	4,50	3
		AP.6.7.2	28	0,60	1
DS.7	Operational, Severe (2)	AP.7.8.1	15	6,00	**4**
DS.8	Safety, Severe (2)	AP.8.9.1	15	6,00	**4**
		AP.8.9.2	27	1,20	2
DS.9	Safety, Severe (2)	AP.9.10.1	15	6,00	**4**
		AP.9.10.2	27	1,20	2
DS.11	Operational, Severe (2)	AP.11.12.1	15	6,00	**4**
		AP.11.13.1	22	3,20	3

A common characteristic of the identified high-risk attack paths is the reliance on a single security mechanism, which significantly elevates the attack feasibility. In these scenarios, the only barrier is the diagnostic UDS protocol's challenge-response routine (Service 0x27 "Security Access" or Service 0x29 "Authentication") (exception is AP.11.12.1). As evidenced by recent research [22-26], this mechanism can be bypassed, or credentials can be inadvertently granted to a malicious OBD tester. Were a vulnerability in the UDS authentication process to be exploited—such as through brute-force attacks, key disclosure, or Man-in-the-Middle, the attack feasibility would increase drastically [23,27]. Once an attacker gains a privileged role, they can easily manipulate memory content using services such as UDS 0x3D ("Write Memory By Address"). While the implementation of Service 0x27 ("Security Access") or Service 0x29 ("Authentication") crucial, it must not be the sole line of defense. Additionally, the risk for those attack paths shall be mitigated by additional security measures in the BMS ECU, and the authors suggest following software improvements:

- To mitigate attack path AP.8.9.1 (tampering with calibration via the OBD DLC), a Secure Boot function for calibration data must be implemented within the BMS ECU. The Hardware Security Module (HSM) would ensure the integrity and authenticity of the calibration parameters. If an integrity violation is detected, the ECU should remain in bootloader mode until a valid calibration is provided, or alternatively, revert to a safe default configuration. Unlike uniform firmware, calibration is unique to each ECU. This implementation will impact production cycle times and costs, as the bootloader must perform the flashing, verification, and Secure Boot metadata updates, rather

than allowing direct memory writes.

- The attack path AP.7.8.1 (removal of calibration data) can be avoided when combined with Secure Boot in conjunction with a default calibration fallback (see above for AP.8.9.1). The size of calibration data is relatively small (2 kB), and inside the memory a default copy will fit.
- To mitigate Attack Path AP.9.10.1 (unauthorized RAM access via UDS), the most effective solution is to disable diagnostic access to internal RAM. While direct RAM read/write capabilities are facilitated by the UDS and XCP protocols for engineering and production purposes, these must be deactivated by implementing a secure ECU lifecycle management. Access should be restricted to specific states, such as Engineering or Forensic modes, and remain permanently disabled in the Delivery/Field state.
- For attack path AP.4.4.1 (erasing the firmware, Denial of Service of the ECU, Bricking Attack), the primary issue is that the new firmware, which is downloaded to the ECU, can be verified (RSA signature verification) after the existing application has been erased and the new data is completely downloaded to the flash memory. When the firmware update procedure is aborted, or the signature verification fails, the BMS ECU will start the bootloader mode and wait for new firmware. For an attacker (after successful authentication to UDS), it is relatively easy to clear the firmware (denial of service) just by flashing any firmware without a valid signature. A robust countermeasure is the implementation of A/B memory partitioning (dual-bank flash). This approach allows the ECU to roll back to the previous functional firmware version if the update fails. However, this requires doubling the flash memory capacity, resulting in increased hardware overhead and costs.
- The risk associated with Attack Path AP.11.12.1 (unauthorized disabling of SPI and DIO functionality) can be mitigated through a robust and secure implementation of the Diagnostic Communication Manager (DCM) module and the CAN communication stack. To ensure resilience against malformed requests, the implementation must undergo rigorous fuzz testing to identify and resolve potential software vulnerabilities.

5. Conclusion

The conducted Threat Analysis and Risk Assessment, based on the ISO/SAE 21434 methodology, demonstrated that the OBD diagnostic interface cannot be treated as a generic, homogeneous attack surface. The engineering-perspective analysis of the BMS ECU proved that the focus must be directed toward specific vulnerabilities at the level of individual UDS protocol services applied on specific system assets. Five attack paths were assigned the relative high risk value (6.00). These include attacks involving firmware erasure via OBD DLC spoofing, erasing and tampering with calibration data, unauthorized manipulation of RAM data, and the intentional disabling of SPI and DIO functionalities. The vast majority of high-risk attack vectors rely on compromising a single security mechanism—the UDS protocol's challenge-response authentication routine (Service 0x27 “Security Access” or Service 0x29 “Authentication”). Once this weak point is breached, the attacker gains unobstructed access to manipulate memory using services such as 0x3D (“Write Memory By Address”). This implies that while UDS authentication remains a fundamental requirement, it absolutely must not constitute the single protective barrier within the system architecture.

A notable finding of this assessment is that the risk of a wireless cellular attack is lower than the direct connection to the OBD DLC port. This is caused by the much lower feasibility of the wireless attack. While the window of opportunity for a cellular attack is significantly larger, it also requires specialized expertise and tools. Even when cellular connection to the vehicle by unauthorized parties would be granted, the attacker needs to compromise other ECUs inside the vehicle (the cellular gateway has to be compromised, the on-board diagnostic tester authentication is needed, and finally authentication or manipulation of the main gateway ECU is needed) before reaching the BMS over CAN_1 bus [15,25]. In a modern, centralized E/E architecture designed according to industry’s best practices, such multi-stage wireless attack scenarios remain highly improbable.

The opposite situation takes place on the standard OBD DLC port, where most of diagnostic commands from the tester are forwarded directly to the BMS ECU. Standard OBD

communication needs to be passed to the ECU, this bypasses the need for authentication at the main gateway, a design choice often driven by the necessity to support standardized diagnostic tools for independent operators [26,28–30]. Only one level authentication to the BMS ECU is needed in case specialized functionalities are requested (single-point-of-failure). While the general requirement for physical access to the cabin theoretically reduces the "Window of Opportunity" compared to remote attacks, this assessment depends heavily on the assumed attacker profile. If the threat model considers a malicious vehicle owner (e.g., performing unauthorized chip-tuning) or a rogue mechanic at an independent repair shop, their window of opportunity expands significantly, as their physical access to the OBD port is unrestricted. In such scenarios, the local attack becomes exceptionally dangerous and highly feasible, requiring the attacker only to bypass the UDS "Security Access" routine to execute critical tasks like firmware manipulation.

In conclusion, effective risk mitigation requires shifting security measures further down the architecture directly into the ECU software, preventing unauthorized and permanent modifications even if a diagnostic session is compromised. Implementing mechanisms such as hardware-backed Secure Boot for calibration processes, robust fallback mechanisms for update failures (A/B memory partitioning), and strictly disabling internal RAM access in production controllers (Delivery/Field state) is critical for safeguarding vehicle stability and passenger safety.

References

1. International Organization for Standardization. ISO 15031-3:2023 Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 3: Diagnostic connector and related electrical circuits: Specification and use. Geneva: International Organization for Standardization; 2023.
2. International Organization for Standardization. ISO 15031-5:2015 Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 5: Emissions-related diagnostic services. Geneva: International Organization for Standardization; 2015.
3. International Organization for Standardization. ISO 14229-1:2020 Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer. Geneva: International Organization for Standardization; 2020.
4. Huang J, Nan J, Chai Z, Lin C. Analysis of UDS diagnostic service applied on vehicle ecu. *Applied Mechanics and Materials* 2013; 437: 779-782. https://doi.org/10.4028/www.scientific.net/AMM.437.779.
5. Zhang Y, Ge B, Li X, Shi B, Li B. Controlling a car through OBD injection. In: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE; 2016. p. 26-29. https://doi.org/10.1109/CSCloud.2016.42.
6. Kang TU, Song HM, Jeong S, Kim HK. Automated reverse engineering and attack for CAN using OBD-II. In: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall); Chicago, IL. IEEE; 2018. p. 1-7. https://doi.org/10.1109/VTCFall.2018.8690781.
7. EVITA Consortium. Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. E-Safety Vehicle Intrusion Protected Applications (EVITA); 2009. http://www.evita-project.org/ [accessed 1 May 2026].
8. European Union Agency for Cybersecurity (ENISA). ENISA good practices for security of smart cars. European Union Agency for Cybersecurity; 2019. https://www.enisa.europa.eu/publications/smart-cars [accessed 1 May 2026].
9. United Nations Economic Commission for Europe (UNECE). UN Regulation No. 155 — Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Geneva: United Nations; 2021.
10. European Union. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. *Official Journal of the European Union* 2018; L 151: 1-218.
11. International Organization for Standardization. ISO 15765-4:2021 Road vehicles — Diagnostic communication over Controller Area Network (DoCAN) — Part 4: Requirements for emissions-related systems. Geneva: International Organization for Standardization; 2021.
12. International Organization for Standardization. ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering. Geneva: International Organization for Standardization; 2021.
13. HEAVENS Consortium. Deliverable D2: Security models. HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS).

Autosec; 2016. https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf [accessed 1 May 2026].
14. Lautenbach A, Almgren M, Olovsson T. Proposing HEAVENS 2.0 – an automotive risk assessment model. In: Proceedings of the 5th ACM Computer Science in Cars Symposium (CSCS '21). New York, NY: Association for Computing Machinery; 2021. p. 1-12. https://doi.org/10.1145/3488904.3493378.
15. Rathore RS, Hewage C, Kaiwartya O, Lloret J. In-vehicle communication cyber security: challenges and solutions. *Sensors* 2022; 22(17): 6679. https://doi.org/10.3390/s22176679.
16. AUTOSAR GbR. Specification of diagnostic communication manager (AUTOSAR CP R19-11). Munich: AUTOSAR GbR; 2019. https://www.autosar.org/fileadmin/standards/classic/1911/AUTOSAR_SWS_DiagnosticCommunicationManager.pdf [accessed 22 April 2026].
17. Kruk T. Practical modelling of threats to ICT systems using the STRIDE model. *Pomiary Automatyka Robotyka* 2024; 28(2): 93-99. https://doi.org/10.14313/PAR_242/93.
18. International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation. 3rd ed. Geneva: International Organization for Standardization; 2022.
19. Pandey S, Grover J, Rai R. Decoding in-vehicle communications: analyzing CAN bus data for enhanced security. *SN Computer Science* 2025; 6: 889. https://doi.org/10.1007/s42979-025-04423-1.
20. Marchetti M, Stabili D. Anomaly detection of CAN bus messages through analysis of ID sequences. In: Proceedings of the 2017 IEEE Intelligent Vehicles Symposium (IV). IEEE; 2017. p. 1577-1583.
21. Kumar R, Sahu H, Penta A, Bhatt P. Reverse engineering of CAN (Controller Area Network) of an electric vehicle. In: Proceedings of the Symposium on International Automotive Technology (SIAT); Pune, India. SAE International; 2026. https://doi.org/10.4271/2026-26-0150.
22. Pełechaty P, Konieczny Ł. Analysis of security vulnerabilities in vehicle on-board diagnostic systems. *Diagnostyka* 2024; 25(3): 192162. https://doi.org/10.29354/diag/192162.
23. Lauser T, Munoz Molto G, Krauß C. (Un)authenticated diagnostic services: a practical evaluation of vulnerabilities in the UDS authentication service. In: Proceedings of the 2024 Cyber Security in CarS Workshop; 2024.
24. Pareja R, Córdoba S. Fault injection on automotive diagnostic protocols: bypassing the security of protected UDS implementations (Report 3124-1747.EN). USA: Keysight Technologies; 2024.
25. Matsubayashi M, Koyama T, Okano Y, Tanaka M, Miyajima A, Oshima Y, Ukai S, Wakatsuki T, Sugashima T, Nakamura T. Attacks against UDS on DoIP by exploiting diagnostic communications and their countermeasures. In: 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring). IEEE; 2021. p. 1-6. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448963.
26. Green C, Chatterjee R, Daily J. Exploiting diagnostic protocol vulnerabilities on embedded networks in commercial vehicles. In: Proceedings of the Symposium on Vehicle Security and Privacy (VehicleSec); San Diego, CA. San Diego: Internet Society; 2024. https://doi.org/10.14722/vehiclesec.2024.23046.
27. Lauser T, Krauß C. Formal security analysis of vehicle diagnostic protocols. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023). New York, NY: Association for Computing Machinery; 2023. p. 1-10. https://doi.org/10.1145/3600160.3600184.
28. Rohith M, Sreelakshmi K. Design and integration of gateway electronic control unit (ECU) for automotive electronics applications. In: 2021 Asian Conference on Innovation in Technology (ASIANCON); Pune, India. IEEE; 2021. p. 1-4. https://doi.org/10.1109/ASIANCON51346.2021.9545049.
29. Robert Bosch GmbH. The E/E architecture of the future (Whitepaper). Bosch Mobility; 2023. https://www.bosch-mobility.com/en/mobility-topics/ee-architecture/download-ee-architecture/ [accessed 18 May 2026].
30. Vector Informatik GmbH. OBDonUDS - SAE J1979-2. Vector Informatik GmbH; 2023. https://www.vector.com/int/en/products/solutions/diagnostic-standards/obdonuds/ [accessed 18 April 2026].

List of Symbols/Acronyms

BMS	Battery Management System
CAN	Controller Area Network Bus
CMAC	Cipher-based Message Authentication Code

DIO	Digital Input Output
ECU	Electronic Control Unit
HSM	Hardware security Module
HV	High voltage
OBD	On-Board Diagnostic
OBD DLC	On Board Diagnostic Data Link Connector
PKI	Public Key Infrastructure
SPI	Serial Peripheral Interface
SoC	State of Charge in battery
TARA	Threat Analysis and Risk Assessment
TLS	Transport Layer Security
UDS	Unified Diagnostic Services
VD ECU	Vehicle Dynamic Electronic Control unit.
VOBD ECU	Inside vehicle on-board diagnostic ECU
XCP	Universal Measurement and Calibration Protocol