2022-01-0114 Published 29 Mar 2022

The Future of OBD: Enhanced On-Board Diagnostic System with Remote Access

Peter Subke and Julian Mayer Softing Automotive Electronics GmbH

Citation: Subke, P. and Mayer, J., "The Future of OBD: Enhanced On-Board Diagnostic System with Remote Access," SAE Technical Paper 2022-01-0114, 2022, doi:10.4271/2022-01-0114.

Received: 25 Jan 2022 Revised: 25 Jan 2022 Accepted: 13 Jan 2022

Abstract

Vehicle manufacturers and their suppliers are legally mandated to develop low-emission engine technologies. Type approval for road-vehicles or non-road mobile machines is only granted when the limits for carbon monoxide (CO), nitrogen oxides (NOx), hydrocarbons (HC), and particulate matters (PM) are observed. In addition to complying with emission standards, road-vehicles must be equipped with a supervising system (OBD) that monitors emission-related components and detects and indicate divergences from admissible pollutant limits. As of today, emission control systems are required for non-road mobile machinery, but not their monitoring by an OBD system.

This paper starts with a short introduction to the classical OBD system. For more than three decades, OBD serves as an essential part of the environmental protection.

The use of electrical powertrains is increasing and the deployment of combustion engines is nearing its end, not only in passenger cars but also in heavy-duty commercial vehicles and mobile machinery. Although electrically powered vehicles do not need the monitoring of exhaust gas relevant components, the OBD system will not disappear. On the contrary, the OBD system is being expanded and given new tasks. Especially in autonomous road-vehicles and automated mobile machines, an enhanced on-board diagnostic system is indispensable to ensure availability, safety, and security.

Vehicles are connected to the cloud, meaning that there is a wireless connection of the vehicle on the road to a cloud-based system that acquires, analyses and stores data. From this perspective, the question arises as to whether we really still need the insecure, wired OBD Port.

This paper describes components and features of an enhanced on-board diagnostic system that monitors both the emission-related and safety-related functions of autonomous vehicles and automated machines. It comes with a radio data link that replaces the traditional wired OBD Port.

1. Introduction

Figure 1 illustrates the classical setup for diagnostic communication between an external test equipment (TST) and a Device Under Test (DUT). TST and DUT are connected to each other via a Vehicle Communication Interface (VCI). In the context of this paper, the DUT is physically that part of the vehicle´s E/E system that performs emission control, namely the OBD system. The E/E system consists of several Electronic Control Units (ECU), sensors, actuators, in-vehicle networks, wiring and connectors. Diagnostic communication consists of service requests, sent by the TST to the OBD system and service responses, sent by the ECUs. At a specific point in time, diagnostic communication is a 1:1 (peer-to-peer) connection between the TST and one specifically addressed ECU.

A very popular in-vehicle network is the Controller Area Network (CAN). CAN allows that all connected ECUs receive all messages, in this case the diagnostic service request sent by the TST. But there is only one ECU that processes the service request and answers with a positive or negative response. That is also true if the request is addressed to "all ECUs of the OBD system", meaning functionally addressed.

Diagnostic communication takes place between the TST and a single ECU that is addressed by an assigned CAN-ID. It consists of a TST-to-ECU request and an ECU-to-TST response.

Figure 3 supports a detailed description of the components, their names, and abbreviations: Emission-related Electronic Control Units (ECUs), such as the Engine Control Module (ECM) and the Transmission Control Module (TCM) are part of the OBD system. The ECM and the TCM are connected to each other and to a Gateway Control Module (GTM) via the Controller Area Network (CAN). The GTM serves as a gateway between the Diagnostic Link Connector (DLC) and the CAN. A Vehicle Communication Interface (VCI) is used to connect the Tester (TST) to the DLC. Today, the most common TST-to-VCI connections are USB and WLAN, and the VCI-to-DLC connection is either CAN or Ethernet.

The communication between the TST and an ECU requires a diagnostic protocol that specifies communication parameters such as the physical data link (e. g. Unshielded Twisted Pair of Wires, or UTP), the signal levels, timing, frame formats, etc. Today´s diagnostic protocol specifications meet

- Supports UDS on IP
- acquires diagnostic and in-vehicle data
- acquires safety-related data such as the current position, acceleration, deceleration, and the angular velocity of the vehicle.

One advantage of this architecture is that the control over the system and its safety as well as the access to data (information) are given back to the vehicle manufacturer.

Other than in a service workshop setup as it is shown in Figure 1, when the vehicle is immobilized and connected to a stationary TST only for a few minutes, the xTCU can periodically acquire diagnostic data from the in-vehicle network over time and under real driving conditions, feeding a vehicle condition monitoring system in the cloud. For that purpose, the xTCU is connected to the DoIP Gateway, acquires signals, diagnostic data and inertia data under real driving conditions and sends the compressed and encrypted data packages as MQTT messages to the NoSQL data processing system in the cloud. The architecture (Figure 10) has been described in [2].

In addition to the results of the enhanced OBD system, the acquisition of preconfigured data over time and a smart analysis supports vehicle-specific condition monitoring (CM). CM allows the identification of deviations and thus the prediction of a failure before it occurs.

Another advantage of the system shown in Figure 9 is that there is only one data link to the vehicle, based on a well-established technology.

Enhanced Security

It is no surprise that "Security by Design" is a much better approach than to plug security holes in a 35-years old technology like CAN.

In January 2021, the UNECE World Forum for Harmonization of Vehicle Regulations introduced Regulation WP.29 UN R155 that mandates the establishment of a Cyber Security Management System (CSMS) and measures to secure the development, production, operation, maintenance and decommissioning of automotive items.

In the European Union, these regulations will be made mandatory for all new vehicle types from July 2022.

In August 2021, SAE and ISO published a joint standard: ISO/SAE 21434 (2021): Road vehicles – Cybersecurity engineering.

Automotive cybersecurity is no longer a playground for nerds, white hat hackers or security researchers. One of the most important tasks of the system designers is the proactive detection of potential security gaps/vulnerabilities and the implementation of powerful measures before it become a zero-day exploit.

With the 5G access to the vehicle the tedious attempts to lock the OBD-II port are a matter of the past. The 5G network security is based on well-proven 4G security measures, but also includes some enhancements. A detailed description of the powerful measures can be found at [6, 7].

One of many security measures is to securely authenticate the xTCU and the MQTT server [9]. The method comprises establishing the connection using a pre-shared server key, establishing the identity of the xTCU using a pre-shared client key (stored on the eSIM of the xTCU), and cryptographically generating a session key for authentication of the xTCU. The method is specified in and protected by US Patent US 2021/0067353 A1.

5. Conclusion/Summary

The most effective method to solve the OBD-II port security problem is to get rid of the wired connector. This paper describes a 4-step approach to replace the OBD-II port by wireless 5G data link.

STEP 1: Combine the classical OBD-II system and the enhanced diagnostic system to an enhanced On-Board Diagnostic System (eOBD). The eOBD system shall monitor environmental and safety-related functions and detect cyber-attacks that affect the safety.

STEP 2: The in-vehicle communication shall be based on SAE J1939, the diagnostic protocol is UDS on IP.

STEP 3: Replace the VCI by an Ethernet cable.

STEP 4: Replace the Ethernet cable by a 5G modem (xTCU). As the connection of the vehicle to the cloud (V2C) becomes customary, the wireless data link can be used for remote diagnostics.

References

1. Subke, P., "Diagnostic Communication with Road-Vehicles and Non-Road Mobile Machinery," *SAE Book*, Product Code R-474, ISBN 978-0-7680-9367-4.
2. Subke, P. and Moshref, M., "Right First Time: Cloud-Based Cyber-Physical System for Data Acquisition and Remote Diagnostics to Optimize the Service Quality," SAE Technical Paper 2021-01-0158 (2021), doi:10.4271/2021-01-0158.
3. Subke, P., Moshref, M., and Erber, J., "In-Vehicle Diagnostic System for Prognostics and OTA Updates of Automated / Autonomous Vehicles," *SAE Int. J.Advances & Curr. Prac. in Mobility* 2(5):2963-2968,2020 doi:10.4271/2020-01-1373 Technical Paper 2020-01-1373.
4. Subke, P., "Improvement of the Resilience of a Cyber-Physical Remote Diagnostic Communication System Against Cyber Attacks," SAE Technical Paper 2019-01-0112 (2019), doi:10.4271/2019-01-0112.
5. Walter, R. and Walter, E., "Data Acquisition from Light-Duty Vehicles Using OBD and CAN," SAE Handbook, Order Number R-458, doi; 10.4271/R-458.
6. Liyanage, M., "A Comprehensive Guide to 5G Security," ISBN 1119293049, 2018.
7. Jayakody, D., Srinivasan, K., and Sharma, V., *5G Enabled Secure Wireless Networks* (ISBN: Springer-Verlag, 2019), ISBN:13-9783030035075
8. Klinedinst, D. and King, C., "On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle," Carnegie Mellon University, March 2016, WhitePaper/2016_019_001_453877.pdf

9. Rannow, H. and Schober, G., Authentication between a telematic control unit and a core server system, United States Patent Application Publication US 2021/0067353 A1.
10. Markham, T. and Chernoguzov, A., "A Balanced Approach for Securing the OBD-II Port," *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* 10, no. 2 (2017): 390-399. https://doi.org/10.4271/2017-01-1662.
11. SAE International Surface Vehicle Recommended Practice, "Guidance for Remote OBD Task Force," SAE Standard J3005.
12. SAE International Surface Vehicle Recommended Practice, "Diagnostic Link Connector Security," SAE Standard J3138_201806.
13. ISO/SAE 21434 (2021): "Road Vehicles - Cybersecurity Engineering."
14. Zhu, D., Kumar, V., Ravi, V. et al., "Detection Method for Cyber Security Attack on Connected Vehicles," SAE Technical Paper 2021-01-1249 (2021), doi:10.4271/2021-01-1249.
15. Jentz, R., Lenzen, T., and Meissner, H., "Diagnostic Evaluation of Exhaust Gas Recirculation (EGR) System on Gasoline Electric Hybrid Vehicle," SAE Technical Paper 2020-01-0902 (2020). https://doi.org/10.4271/2020-01-0902.
16. Van Nieuwstadt, M., Lehmen, A., Ravi, V. et al., "A Unique Application of Gasoline Particulate Filter Pressure Sensing Diagnostics," *SAE Int. J. Passeng. Cars - Mech. Syst.* 14, no. 2 (2021). https://doi.org/10.4271/06-14-02-0007.

Contact Information

Dipl.-Ing. Peter P. Subke c/o
Softing Automotive Electronics GmbH, Germany
+49 175 5826 579
sub@softing.com

Julian Mayer (MBA and Eng.) c/o
Softing Automotive Electronics GmbH, Germany
+49 89 45656
erj@softing.com

Definitions/Abbreviations

CAN - Controller Area Network (ISO 11898)

DLC - Diagnostic link connector (SAE J1962, ISO 13400)

DoCAN - Diagnostic communication over Controller Area Network

DoIP - Diagnostic communication over Internet Protocol

GTM - Gateway Control Module

ECM - Engine Control Module

OBD - On-Board Diagnostics

OBD on UDS - SAE J1979-2

TCM - Transmission Control Module

TST - (external) test equipment, diagnostic tester, service/workshop tester

UDS - Unified Diagnostic Services (ISO 14229)

VCI - Vehicle Communication Interface

WWH OBD - Worldwide Harmonized On-Board Diagnostics (ISO 27145)

ISSN 0148-7191