

Measures to Prevent Unauthorized Access to the In-Vehicle E/E System, Due to the Security Vulnerability of a Remote Diagnostic Tester

Peter Subke

Softing Automotive Electronics GmbH

Muzafar Moshref

Softing North America Inc.

Andreas Vach and Markus Steffebauer

Softing Automotive Electronics GmbH

ABSTRACT (SUMMARY)

Remote diagnostic systems support diagnostic communication by having the capability of sending diagnostic request services to a vehicle and receiving diagnostic response services from a vehicle. These diagnostic services are specified in diagnostic protocols, such as SAE J1979, SAE J1939 or ISO 14229 (UDS).

For the purpose of diagnostic communication, the tester needs access to the electronic control units as communication partners. Physically, the diagnostic tester gets access to the entire vehicle's E/E system, which consists of connectors, wiring, the in-vehicle network (e.g. CAN), the electronic control units, sensors, and actuators.

Any connection of external test equipment and the E/E system of a vehicle poses a security vulnerability. The combination can be used for malicious intrusion and manipulation. Any unauthorized access to the E/E system of a vehicle can severely harm the functional safety and finally cause damage to the vehicle or - even worse - to life and health of people.

This paper describes the architecture of a system for remote diagnostics, its security vulnerability and measures to increase the security.

CITATION: Subke, P., Moshref, M., Vach, A., and Steffebauer, M., "Measures to Prevent Unauthorized Access to the In-Vehicle E/E System, Due to the Security Vulnerability of a Remote Diagnostic Tester," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 10(2):2017, doi:10.4271/2017-01-1689.

INTRODUCTION

Figure 1 illustrates a diagnostic system that is commonly used in aftermarket service workshops. For the purpose of diagnostic services, external test equipment, in this context also referred to as diagnostic tester (TST), is connected to the data link connector (DLC) of a vehicle via a vehicle communication interface (VCI). Today, the TST-to-VCI connection is USB, Bluetooth or Wifi, whereas the VCI-to-DLC connection is CAN - or Ethernet on some newer passenger cars, such as the MY 2016 AUDI or the current Mercedes-Benz S-class.

In the context of this paper, a "remote diagnostic system" is characterized in that the diagnostic tester and the vehicle are physically separated (Figure 2) by an internetwork (e.g. the internet), meaning that the distance does not matter, and the connection can be wired, wireless or a mixture.

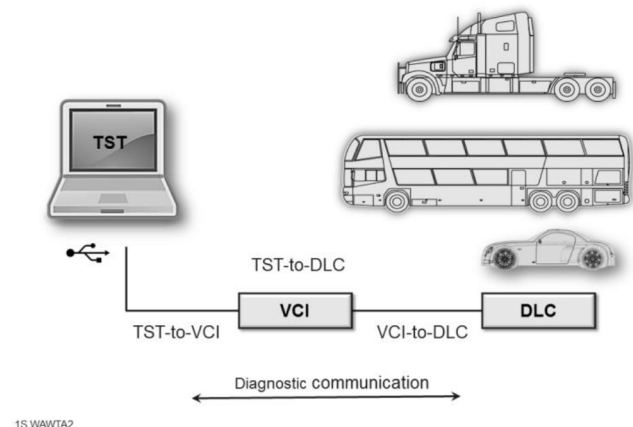


Figure 1. Diagnostic system with TST, VCI and DLC

In general, a remote diagnostic system provides the same functionality as a diagnostic tester on-site in the aftermarket workshop, e.g. reading of diagnostic data, starting diagnostic functions, or updating ECU firmware. In addition, a remote diagnostic system can get access to more than one vehicle at the same time, providing the ability to collect fleet data and use the information e.g. for predictive maintenance services.

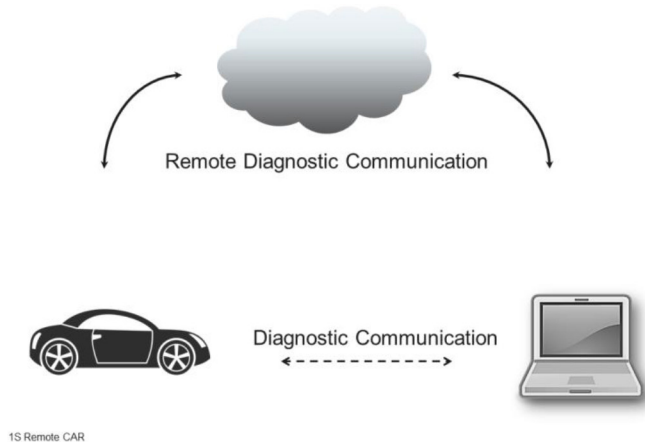


Figure 2. Remote diagnostic system: Tester and vehicle are physically separated

DIAGNOSTIC COMMUNICATION

Both on-site and remote diagnostic systems support diagnostic communication by having the capability of sending diagnostic service requests to a vehicle and receiving diagnostic service responses from the vehicle.

As illustrated in Figure 3, in-vehicle communication and diagnostic communication are sub-functions of data communication.

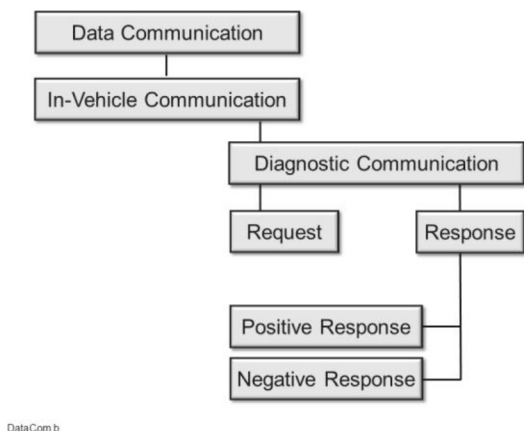


Figure 3. In-Vehicle communication and diagnostic communication

In-vehicle communication is characterized in that the electronic control units (ECUs) on-board a vehicle are connected to each other by bus systems (e.g. CAN), forming an in-vehicle network, and in that they send and receive messages that contain information. They virtually talk to each other.

Diagnostic communication is characterized in that an external diagnostic tester talks to an ECU or a group of ECUs. For that purpose, the diagnostic tester needs an up and running in-vehicle network. Diagnostic communication between the diagnostic tester and a vehicle requires a diagnostic communication protocol. Since the implementation of standardized protocols increasingly replaces the implementation of proprietary ones, the diagnostic protocols specified in SAE J1979 (OBD II), SAE J1939 (HD OBD), ISO 27145 (WWH OBD) and ISO 14229 (UDS) can be considered as customary.

If CAN is used as VCI-to-DLC connection, the DLC is the OBD II connector according to SAE J1962 A (for vehicles with 12 VDC supply voltage) or B (for vehicles with 24 VDC supply voltage), or SAE J1939-13 for heavy-duty commercial vehicles.

On some newer vehicles, Ethernet is used in addition to CAN. In that case, previously unused pins of the SAE J1962 OBD II connector are assigned to the four Ethernet wires and the Ethernet activation signal.

Note: Even if Ethernet is used for the service-related diagnostic communication, CAN is a must to meet legislated OBD requirements.

Figure 4 illustrates the pin assignment of the J1962 OBD II connector with additional Ethernet pins.

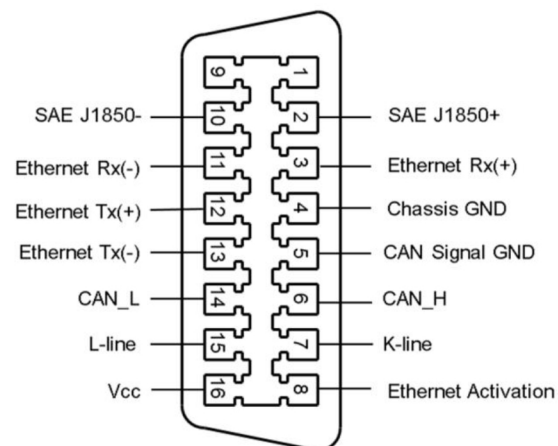


Figure 4. Pin assignment of the SAE J1962 (OBD II) connector

The pin assignment is derived from ISO 13400-4 (2016) - Diagnostic communication over Internet Protocol (DoIP) - Part 4: Ethernet-based high-speed data link connector

Figure 5 illustrates a diagnostic system that is based on a DLC with Ethernet, whereas the in-vehicle network is still based on CAN.

The gateway separates CAN and Ethernet, and the Ethernet-to-WLAN Converter finally converts the diagnostic communication on the OSI model physical and data link layer. With such a converter, the VCI-to-DLC connection is wired Ethernet, and the TST-to-VCI connection is wireless. The tester can be a PC with Windows, a smart device with Android or iOS, or any other module with LINUX as operating system.

The tester may or may not be connected to the internet, but if it is connected to the internet, there is a connection between the internet and the in-vehicle network with remote access to e.g. the ECM (Engine Control Module) and the TCM (Transmission Control Module).

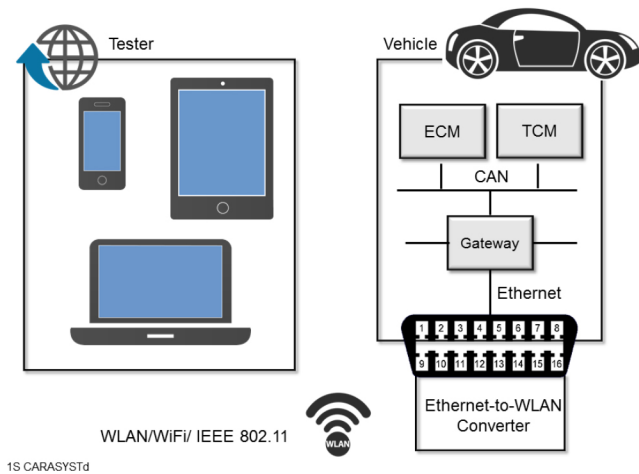


Figure 5. Ethernet-based diagnostic system with WiFi TST-to-VCI connection (ECM = Engine Control Module, TCM = Transmission Control Module)

The gateway in Figure 5 converts UDS on Ethernet to UDS on CAN (ISO 14229-3), which has to be implemented in the ECUs that are connected to the CAN (in this example, ECM and TCM).

UDS ON ETHERNET

For diagnostic communication, the diagnostic tester sends a diagnostic service request and expects either a positive or a negative diagnostic service response from at least one ECU. Diagnostic services are specified in diagnostic protocols. In the following, ISO 14229 (see Table 1) is used as an example.

Table 1. The content of ISO 14229: Road Vehicles - Unified Diagnostic Services (UDS)

ISO 14229	Road vehicles – Unified Diagnostic Services (UDS)
Part 1 (2013)	Specification and requirements
Part 2 (2013)	Session layer services
Part 3 (2013)	UDS on CAN implementation (UDSonCAN)
Part 4 (2012)	UDS on FlexRay implementation (UDSonFR)
Part 5 (2013)	UDS on Internet Protocol implementation (UDSonIP)
Part 6 (2013)	UDS on K-Line implementation (UDSonK-Line)
Part 7 (2015)	UDS on LIN implementation (UDSonLIN)

The OSI model application layer of UDS consists of the specification of 26 parametrizable service requests (Table 2).

Note: Not all services are supported by all ECUs. There is always a manufacturer specific subset of supported services.

Table 2. Unified Diagnostic Services and Service Identifier (SID)

0x10	Diagnostic Session Control	0x2A	Read Data By Periodic Identifier
0x11	ECU Reset	0x2C	Dynamically Define Data Identifier
0x27	Security Access	0x2E	Write Data By Identifier
0x28	Communication Control	0x2D	Write Memory By Address
0x3E	Tester Present	0x14	Clear Diagnostic Information
0x83	Access Timing Parameter	0x19	Read DTC Information
0x84	Secured Data Transmission	0x2F	Input Output Control By Identifier
0x85	Control DTS Setting	0x31	Routine Control
0x86	Response On Event	0x34	Request Download
0x87	Link Control	0x35	Request Upload
0x22	Read Data By Identifier	0x36	Transfer Data
0x23	Read Memory By Address	0x37	Request Transfer Exit
0x24	Read Scaling Data By Identifier	0x38	Request File Transfer

1S UDSRQ

Part 5 of ISO 14229 contains the UDS on Internet Protocol (UDSonIP) specification on the Application layer of the OSI model. Figure 6 illustrates the OSI model layers that form the entire protocol stack of UDS on Ethernet.

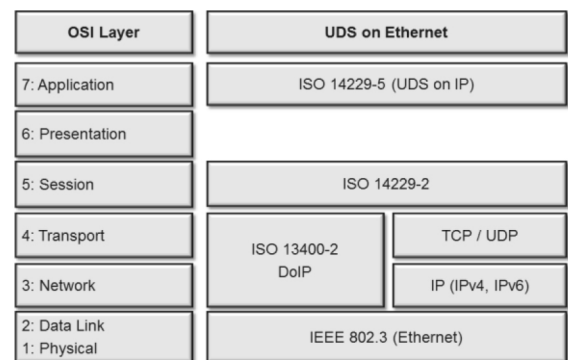


Figure 6. The OSI model protocol stack of UDS on Ethernet

For diagnostic communication on Ethernet, the entire protocol stack as depicted in Figure 6 has to be implemented in both the tester and the ECUs.

The Transport Layer (TCP and UDP) and the Network Layer (IPv4 and IPv6) are grouped as DoIP (Diagnostics over Internet Protocol) and specified in ISO 13400 (Table 3).

Table 3. The content of ISO 13400: Road vehicles - Diagnostic communication over Internet Protocol (DoIP)

ISO 13400	Road Vehicles – Diagnostic communication over Internet Protocol (DoIP)
Part 1 (2011)	General information and use case definition
Part 2 (2012)	Transport protocol and network layer services
Part 3 (2016)	Wired vehicle interface based on IEEE 802.3
Part 4 (2016)	Ethernet diagnostic connector