SAE INTERNATIONAL

SURFACE VEHICLE RECOMMENDED PRACTICE

J3138™ OCT2022

Issued 2018-06
Revised 2022-10

Superseding J3138 JUN2018

(R) Diagnostic Link Connector Security

RATIONALE

The changes to this version of the document are for the addition of (non-standardized) CAN Diagnostics Channels including CAN FD and DoIP Channel(s).

FOREWORD

On Board Diagnostic regulations require passenger cars and light-, medium-, and heavy-duty trucks to provide a Diagnostic Connector, which conforms to the SAE J1962 and the SAE J1979 standards, to support communication of diagnostic information to off-board devices. Legislated diagnostic information is required to be communicated in a timely fashion to the off-board devices. Many vehicle manufacturers also provide access to enhanced diagnostic information and vehicle systems/subsystems via this connector.

TABLE OF CONTENTS

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

For more information on this standard, visit
https://www.sae.org/standards/content/J3138_202210/

1. SCOPE

This document describes a set of recommended actions to take to increase the likelihood of safe vehicle operation when a device (external test equipment, data collection device, etc.) whose normal operation has been compromised by a source external to the vehicle is connected to the vehicle's diagnostic system. The term "diagnostic system" is intended to be a generic way to reference all the different ways that diagnostic commands might be injected into the system.

The guidance in this document is intended to improve security without significantly impacting the ability for franchised dealer or independent aftermarket external test tools to perform legitimate diagnosis and maintenance functions.

The goal is that intrusive services are only allowed to be performed when the vehicle is in a Safe State such that even if the intrusive service were to be initiated with adversarial intent the consequences of such a service would still be acceptable.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J1930	Electrical/Electronic Systems Diagnostic Terms, Definitions, Abbreviations, and Acronyms - Equivalent to ISO/TR 15031-2
SAE J1962	Diagnostic Connector
SAE J1979	E/E Diagnostic Test Modes
SAE J1939-13	Off-Board Diagnostic Connector
SAE J3005	Permanently or Semi-Permanently Installed Diagnostic Communication Devices
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

2.1.2 ISO Publications

Unless otherwise indicated, the latest issue of ISO publications shall apply. Copies of these documents are available online at https://webstore.ansi.org/ or at https://www.iso.org/store.html

ISO 11898-1	Road vehicles - Controller area network (CAN), Part 1: Data link layer and physical signaling
ISO 11898-2	Road vehicles - Controller area network - Part 2: High-speed medium access unit
ISO 13400-2	Road vehicles - Diagnostic communication over Internet Protocol (DoIP) - Part 2: Transport protocol and network layer services
ISO 13400-3	Road vehicles - Diagnostic communication over Internet Protocol (DoIP) - Part 3: Wired vehicle interface based on IEEE 802.3
ISO 13400-4	Road vehicles - Diagnostic communication over Internet Protocol (DoIP) - Part 4: Ethernet-based high-speed data link connector
ISO 14229-1 Ed.3	Road vehicles - Unified diagnostic services (UDS) - Part 1: Application layer
ISO 14229-2	Road vehicles - Unified diagnostic services (UDS) - Part 2: Session layer services

ISO 14229-3	Road vehicles - Unified diagnostic services (UDS) - Part 3: Unified diagnostic services on CAN implementation (UDSonCAN)
ISO 14229-5	Road vehicles - Unified diagnostic services (UDS) - Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP)
ISO 15031-3	Road vehicles - Communication between vehicle and external equipment for emissions-related diagnostics - Part 3: Diagnostic connector and related electrical circuits, specification and use
ISO 15031-5	Road vehicles - Communication between vehicle and external equipment for emissions-related diagnostics - Part 5: Emission-related diagnostic services
ISO 15765-2	Road vehicles - Diagnostics on Controller Area Networks (DoCAN) - Part 2: Transport protocol and network layer services
ISO 15765-4	Road vehicles - Diagnostics on Controller Area Networks (DoCAN) - Part 4: Requirements for emission-related systems
ISO 27145 (all parts)	Road vehicles - Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

Klinedinst, Dan and King, Christopher, On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle, Carnegie Mellon University Software Engineering Institute, March 2016

3. TERMS AND DEFINITIONS

3.1 Definitions

3.1.1 CONTROLLER AREA NETWORK (CAN)

Communication protocol used on a vehicle as a means to provide generic legislated and proprietary enhanced data from in-vehicle ECUs to external test equipment. The protocol is also used to support intra-vehicle normal mode messaging that occurs between individual in-vehicle ECUs.

3.1.2 DIAGNOSTICS OVER IP (DoIP)

DoIP is specified in ISO 13400 and is short for Diagnostic communication over Internet Protocol.

It is part of the UDSonIP ISO 14229-5 diagnostic protocol stack. UDS (Unified Diagnostic Services) is a set of diagnostic services which is capable of supporting both legislated and enhanced diagnostics use cases.

The Diagnostics over IP protocol is used to transport diagnostic information over an Ethernet physical layer. UDS is specified on IP as well as on CAN and other physical layers.

For emissions related diagnostics, DoIP is currently referenced in ISO 27145 (WWH-OBD), which specifies a subset of UDS for diagnostic communication with the vehicle's OBD system.

3.1.3 DATA LINK CONNECTOR OR DIAGNOSTICS LINK CONNECTOR (DLC)

The SAE J1962, ISO 13400-4 or ISO 15031-3 or SAE J1939-13 connector.

3.1.4 ELECTRONIC CONTROL UNIT (ECU)

An on-board (in-vehicle network) computer for controlling vehicle functions.

3.1.5 GATEWAY

A physical or logical device on board the vehicle that controls communication into and out of a vehicle network.

3.1.6 KEY ON, ENGINE OFF (KOEO)

Refers to the vehicle operational mode when the key is in the “ON” position but the engine (or propulsion system) is “OFF.”

3.1.7 INTRUSIVE SERVICE

A diagnostic service that has the potential to alter the functionality of the vehicle.

3.1.8 NON-INTRUSIVE SERVICE

A diagnostic service that does not have the potential to alter the functionality of the vehicle.

3.1.9 ON BOARD DIAGNOSTICS (OBD)

A term referring to a vehicle's self-diagnostic and reporting capability. OBD systems give the vehicle owner or repair technician access to the status of the various vehicle sub-systems.

3.1.10 SAFE STATE

Vehicle operating mode based on conditions for performing intrusive service requests safely. A vehicle’s safe state can be different depending on the conditions required for specific intrusive service request.

3.1.11 SUBSERVICE

A subfunction of an ISO 14229-1 diagnostics service.

4. GENERAL RECOMMENDATIONS

Generally, the following forms of communication bus connection topologies are used in current vehicles:

a. Open access to communication buses

b. Communication buses isolated via a gateway

c. Hybrid combinations of a. and b.

4.1 Protocol Service Categorization

Ground based vehicles may use several types of serial communication protocols as defined by vehicle manufacturers or standards body organizations. Additionally regulating administrations have driven the development of functions inside protocol services. Working together over time and need, industry has created protocols defined by SAE J1979 (ISO 15031), SAE J1939, ISO 15765, ISO 14229, ISO 27145, ISO 13400-x, and more.

The following table(s) contain recommendations for categorizing standardized diagnostic services defined by the legislated protocol SAE J1979 and the enhanced protocol ISO 14229. These recommended categorizations of services as “intrusive” or “non-intrusive” are intended to be informative guidance for vehicle security experts, ECU developers, and other key industry partners. These tables apply to all mechanisms capable of transporting SAE J1979 and ISO 14229 services including, but not limited to, CAN, CAN-FD, and DoIP.

Table 1 - List of SAE J1979 services

Service	Description	Non-Intrusive	Intrusive
0x01	Request current powertrain diagnostic data	X	
0x02	Request powertrain freeze frame data	X	
0x03	Request emission-related diagnostic trouble codes	X	
0x04	Clear/reset emission-related diagnostic information	See 4.2	
0x06	Request on-board monitoring test results for specific monitored systems	X	
0x07	Request emission-related diagnostic trouble codes detected during current or last completed driving cycle	X	
0x08	Request control of on-board system, test, or component		X
0x09	Request vehicle information	X	
0x0A	Request emission-related diagnostic trouble codes with permanent status	X	

Table 2 - ISO 14229-1 services

Service	Description	Non-Intrusive	Intrusive
0x10	DiagnosticSessionControl, Subservice 0x01 (defaultSession) (reference ISO 14229-1 for Subservice definition)	X	
0x10	DiagnosticSessionControl, Subservice 0x02 (ProgrammingSession)		X
0x10	DiagnosticSessionControl , all other Subservices	See 4.2	
0x11	ECUReset		X
0x14	ClearDiagnosticInformation	See 4.2	
0x19	ReadDTCInformation	X	
0x22	ReadDataByIdentifier	X	
0x23	ReadMemoryByAddress	X	
0x24	ReadScalingDataByIdentifier	X	
0x27	SecurityAccess	See 4.2	
0x28	CommunicationControl		X
0x29	Authentication	See 4.2	
0x2A	ReadDataByPeriodicIdentifier	X	
0x2C	DynamicallyDefineDataIdentifier	X	
0x2E	WriteDataByIdentifier		X
0x2F	InputOutputControlByIdentifier		X
0x31	RoutineControl		X
0x34	RequestDownload		X
0x35	RequestUpload		X
0x36	TransferData		X
0x37	RequestTransferExit		X
0x38	RequestFileTransfer		X
0x3D	WriteMemoryByAddress		X
0x3E	TesterPresent	X	
0x83	AccessTimingParameters		X
0x84	SecuredDataTransmission	See 4.2	
0x85	ControlDTCSetting		X
0x86	ResponseOnEvent		X
0x87	LinkControl		X

4.2 Protocol Service Categorization Considerations

Services 0x04 and 0x14 are recommended to be non-intrusive. Performing services 0x04, 0x10, and 0x14 require that the ECU Server has knowledge that a vehicle has met the safe system conditions. Definition of safe system condition is presented in 4.8 (all sub-sections) in this document. There are circumstances where these services have an intrusive aspect (e.g., fail safe reactions which are temporarily disabled after clearing DTCs, checking presence of DTCs as precondition for remote engine start).

For Service 0x10, some Subservices are considered to be intrusive or have the potential to enable access to other intrusive services. As most of the Subservices are manufacturer specific, no generalized recommendation can be given here.

Services 0x27 and 0x29 have the potential to enable access to other intrusive services.

Service 0x84 has the potential to convey other services, some intrusive and some non-intrusive. In addition, depending on implementation, a gateway device may not be able to differentiate whether Service 0x84 is being used to covey intrusive or non-intrusive services, and may not be able to disallow some while allowing others. A vehicle manufacturer should carefully consider the security implications, but as a consequence of the above no generalized recommendation can be given here.

4.3 Legislated Diagnostic Protocols

The SAE J1979 command to Clear/Reset All Emission-Related Diagnostic Information (Service 0x04) may include clearing of fault information used for system protection. Current U.S. regulation requires Service 0x04 to be operational at KOEO, and it may be additionally operational during other conditions (e.g., engine running) at the manufacturer's option. If an OEM allows Service 0x04 beyond the KOEO condition, it shall provide safeguards to ensure system protection.

4.4 Network Communications and CAN Protocol Error Handling

Depending on the vehicle system design, either the Gateway or the individual ECU shall validate and respond to request messages based on standard CAN protocol and error-handling methodologies defined in ISO 15765 and ISO 14229 document sets. The vehicle system should reject messages appropriately.

It is recommended that a gateway that blocks a message that would normally be responded to (in a positive or negative manner) by the target ECU informs the external device that the message was blocked (for example, by issuing Negative Response Code such as "0x22 - conditionsNotCorrect"). However, there might also be reasons for the gateway not to respond (e.g., if the gateway detected a potential attack like denial of service for bus- or processor-load, continuous guessing of credentials by the client, replying to functional requests, …). Therefore, there is no requirement that a gateway that blocks the message need replicate any other response criteria that might normally be applied by the target ECU if the message had actually reached the device.

The following is a list of some of the nominal fields in Protocol Data Units (PDUs) from external devices that are candidates for filtering criteria. Any incorrectly formatted fields cause an appropriate error code to be returned to the external device. Clearly, as many of these fields as possible should be checked to provide the highest level of performance possible. Note that all of the listed items might not be possible to be implemented because of system resource restrictions.

- Network Address Information and format
- Network Target Address (correct ECU or OBD address allowed only, ECU shall reject incorrect/partial functional and physical addresses)
- Network Source Address (if applicable)
- Network Message length and format
- Network Message Payload (at least the service identifier)
- Network Message frequency/rate

NOTE: It is expected that a gateway that blocks a message that would normally be responded to (in a positive or negative manner) by the target ECU should inform external device that the message was blocked (for example, by issuing Negative Response Code such as "0x22 - conditionsNotCorrect"). There is no expectation that a gateway that blocks the message need replicate any other response criteria that might normally be applied by the target ECU if the message had actually reached the device.

While Negative Response Codes (NRCs) may provide information that could be used by malicious actors, they do not provide any ability to compromise the system.

A gateway and/or each individual ECU shall be responsible for the correct handling of error frames, whether properly generated or deliberately injected.

A gateway and/or each individual ECU shall be responsible for the correct handling of any “bus-off” condition, whether properly generated or deliberately injected.

4.5 Measurement and Calibration

Measurement and calibration protocols (e.g., xCP) accessible via the DLC should provide at least the same protection as recommended for the standardized diagnostic protocols (refer to SAE J1979 and ISO 14229). It is recommended to close serial communication interface access ports to production ECU hardware accessible via the DLC. This includes common industry and/or internal proprietary SCI type ports that allow for direct access to hardware functionality. In other words, the hardware processing units should not be able to be accessed in a manner consistent with calibration methods after the ECU is placed into a production vehicle.

4.6 Enhanced Diagnostic Protocols

Vehicle manufacturer enhanced diagnostic protocols shall provide at least the same of protection as recommended for the standardized diagnostic protocols (refer to SAE J1979 and ISO 14229). Enhanced diagnostic protocols are defined as those service identifiers which allow access to a greater number of parametric data plus device control, secure access, and service settings.

4.7 Service Requests to Gateway(s) or Individual ECUs

Gateways and/or each individual ECU shall reject invalid/unsupported service/subservice requests using the appropriate NRC (see 4.4 for details).

4.8 Vehicle Safe State

A vehicle Safe State is determined by the vehicle manufacturer.

Intrusive services should only be allowed when the vehicle is determined to be in a Safe State. However, it is possible that the parameters that are used to determine the Vehicle Safe State come from a faulty device which requires a diagnostic operation, and as a consequence that device is not correctly providing the information that is ultimately used to determine the Safe Vehicle State. In such a case, the gateway (or other component) may be unable to make the determination indicating a Vehicle Safe State. If the diagnostic operations required to rectify this situation require the use of an intrusive service, it is possible that the gateway (or other component) may actually block the operations that would ultimately allow the system to be repaired so that the gateway could once again properly determine a Safe Vehicle state.

Vehicle manufacturers shall provide a secure method to perform intrusive services for cases where the vehicle parameters used to determine safe state operation are absent (e.g., because of a fault in the component or signal needed to determine the safe state). This can be done, for example, by providing the possibility to bypass the evaluation of the safe state for those cases.

4.8.1 Determination of Vehicle Safe State

A gateway and/or each individual ECU which has received an intrusive service request from any source shall make a determination of the state of the vehicle at the time of the request by sampling one or more vehicle parameters. Vehicle parameters that might be used to make such a determination include, but are not limited to:

- Vehicle Speed
- Automatic Transmission Neutral/Drive Status or Manual Transmission Neutral Gear Status
- Any Door Switch Status and/or Hood Switch Status
- Driver’s Demand Engine Percent Torque