



SURFACE VEHICLE RECOMMENDED PRACTICE

J3005™-2

MAR2020

Issued

2020-03

Permanently or Semi-Permanently Installed Diagnostic Communication Devices Security Guidelines

RATIONALE

SAE J3005-2 is being published as a new document as security and privacy recommended practice permanently or semi-permanently installed diagnostic communication devices.

The design of modern vehicle electrical architecture where the OBD diagnostic protocol is an open protocol, and the fact that vehicle manufacturers may have direct connection to the control bus of the vehicle in the connector, has been the enabler for various new use cases, but can also open up the car to hacking.

This document is a cyber-security recommended practice for manufacturers of permanently and semi-permanently installed diagnostic communication devices.

FOREWORD

The OBD connector has been developed as a standardized connector for use in passenger cars, light-duty, medium-duty and heavy-duty trucks, to access on-board diagnostic information by “generic” test equipment. The access was anticipated to be for short term use in a controlled environment to facilitate a maintenance procedure, e.g., the “generic” test equipment is installed in the vehicle in a workshop and is removed before the vehicle leaves the workshop. Vehicle manufacturers have added vehicle-specific diagnostic communication in the OBD connector; the connector has been seen as a standardized entry point to the complete vehicle for diagnostics.

Over time, other devices began making use of the standardized connector and data in a more or less permanent installation to collect and use standardized data for purposes other than a temporary maintenance procedure.

There are some areas where this can be a problem:

- Information security issue
- Privacy

The intention of SAE J3005-2 is to provide guidelines to device vendors in order to minimize the risk of these problems.

SAE Technical Standards Board Rules provide that: “This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user.”

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2020 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

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
http://www.sae.org

SAE WEB ADDRESS:

Full document details: [SAE J3005-2_202003](#)

For more information on this standard, visit
https://www.sae.org/standards/content/J3005-2_202003

Documents
Document Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Purpose	3
2.	REFERENCES.....	3
2.1	Applicable Documents	3
2.1.1	SAE Publications.....	3
2.1.2	ISO Publications.....	3
2.2	Related Publications	4
2.2.1	Other Publications.....	4
3.	TERMS AND DEFINITIONS	4
4.	TECHNICAL RECOMMENDATIONS FOR SECURITY	5
4.1	In-Vehicle Security Recommendations	5
4.2	Security Weaknesses in Diagnostic Protocols.....	7
4.3	System Design Principles	8
4.4	Separation of Duties in Security Critical Parameters.....	8
4.5	Use of Methodology	9
4.6	Wired/Over-the-Air Traffic Security	9
4.7	Firmware Update Process.....	9
4.8	Firmware Update Authentication and Integrity Check	9
4.9	Pseudo-Random Number Generation (PRNG)	9
4.10	Device Individualization.....	9
4.11	Roles Management.....	9
4.12	Hardware Code Read-Protection	9
4.13	Assume Your Code is Public	9
4.14	Testing or Auditing	9
5.	TECHNICAL REQUIREMENTS FOR PRIVACY	10
5.1	In-Vehicle Privacy Recommendations	10
5.2	Remote Privacy Recommendations.....	10
6.	NOTES	10
6.1	Revision Indicator.....	10
APPENDIX A	(INFORMATIVE) SECURITY SURVEY DONE BY CARNEGIE MELLON UNIVERSITY	11
APPENDIX B	(INFORMATIVE) TARA.....	12
Figure 1	Overview of standards	6
Figure 2	Permanently or semi-permanently installed diagnostic communication device firmware layout	6
Table 1		8

1. SCOPE

1.1 Purpose

The scope of the document is to define the cyber-security best practices to reduce interference with normal vehicle operation, or to minimize risk as to unauthorized access of the vehicle's control, diagnostic, or data storage system; access by equipment (i.e., permanently or semi-permanently installed diagnostic communication device, also known as dongle, etc.) which is either permanently or semi-permanently connected to the vehicle's OBD diagnostic connector, either SAE J1939-13, SAE J1962, or other future protocol; or hardwired directly to the in-vehicle network. This document only specifies requirements and guidance for those diagnostic communication devices and not for the vehicle. Refer to SAE J3138 for requirements for the vehicle side.

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 J1939-13	Off-Board Diagnostic Connector
SAE J1939-21	Data Link layer
SAE J1939-71	Vehicle Application Layer
SAE J1939-73	Application Layer - Diagnostics
SAE J1962	Diagnostic Connector
SAE J1979	E/E Diagnostic Test Modes
SAE J1979DA	Digital Annex
SAE J3005-1	Permanently or Semi-Permanently Installed Diagnostic Communication Devices
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
SAE J3138	Diagnostic Link Connector Security

2.1.2 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 14229-1	Road Vehicles - Unified Diagnostic Services (UDS) - Part 1: Specification and Requirements
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: Emissions-Related Diagnostic Services
ISO 15765-4	Road Vehicles - Diagnostic Communication Over Controller Area Network (DoCAN) - Part 4: Requirements for Emissions-Related Systems

2.2 Related Publications

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

2.2.1 Other Publications

Risks and Vulnerabilities of Aftermarket OBD II Devices, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA 15213.

NIST 800-57 Recommendation for Key Management

3. TERMS AND DEFINITIONS

3.1 ECU (ELECTRONIC CONTROL UNIT)

An ECU is an on-board (in-vehicle network) computer for vehicle functions.

3.2 HEAVENS (HEALING VULNERABILITIES TO ENHANCE SOFTWARE SECURITY AND SAFETY)

HEAVENS is a security model that provides a threat analysis and risk assessment methodology to facilitate the process of identifying security requirements and vulnerabilities of E/E (electrical/electronic) automotive systems, and to perform security evaluations of those systems. HEAVENS is developed as a European Council-founded project at Chalmers University of Technology in Sweden (<https://research.chalmers.se/en/project/5809>).

3.3 INFRASTRUCTURE

The term “infrastructure” is used by this document as the equipment used to receive the data sent by the devices connected to the OBD port, transport the information, and store it in a database used by regulatory. It is the term for handling the information off-board.

3.4 INTRUSIVE SERVICES

Intrusive services are any diagnostic services which may affect the normal functionality of the ECU.

3.5 ND (NOMADIC DEVICE)

A nomadic device is a portable/mobile communication device, e.g., a smartphone or tablet.

3.6 NV MEMORY (NON-VOLATILE MEMORY)

Non-volatile memory keeps its data when there is no supply voltage, e.g., flash memory.

3.7 PERMANENTLY INSTALLED DIAGNOSTIC COMMUNICATION DEVICE

Refers to a device which is hardwired into the in-vehicle wire harness (e.g., in taxi vehicles) for a long time; i.e., it is connected for days, not hours, and during normal vehicle operation. The permanently installed diagnostic communication device can often only be removed by a service technician.

3.8 PID (PARAMETER IDENTIFIER)

PID is an older term for DID, defined in SAE J1979DA.

3.9 REMOTE DEVICE

A remote device is a device which gathers data and sends it to a remote location utilizing wireless technology.

3.10 SEMI-PERMANENTLY INSTALLED DIAGNOSTIC COMMUNICATION DEVICE

Refers to a device which is plugged in into the SAE J1962 connector during normal vehicle operation. The difference between a permanently installed device and a semi-permanently installed diagnostic communication device is that the latter may be removed after some time by just disconnecting it from the OBD diagnostic connector.

3.11 STRIDE

STRIDE is a threat model defined by Microsoft in 2005:

Spoofing Identity, Tampering with Data, Repudiation, Non-Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege ([https://en.wikipedia.org/wiki/STRIDE_\(security\)](https://en.wikipedia.org/wiki/STRIDE_(security))).

3.12 TARA (THREAT ANALYZE RISK ASSESSMENT)

TARA is a method to analyze threats for a system and judge the risk. TARA is usually done together with STRIDE ([https://en.wikipedia.org/wiki/Threat_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))).

3.13 TELEMATICS

Telematics typically is any integrated use of telecommunications and informatics for sending, receiving, and storing information via telecommunication devices in conjunction with affecting control on remote objects, and, in this context, the integrated use of telecommunications and informatics, for application in vehicles and with control of vehicles on the move.

3.14 VIN (VEHICLE IDENTIFICATION NUMBER)

Number used to identify a vehicle according to ISO 3779.

3.15 VM (VEHICLE MANUFACTURER)

The company which owns the brand of the vehicle, or is the vehicle maker.

4. TECHNICAL RECOMMENDATIONS FOR SECURITY

4.1 In-Vehicle Security Recommendations

The interface shall not pass information from internet/nomadic devices directly to the in-vehicle networks. Middleware layers should separate the different data links (i.e., separate B from A).

NOTE: This document has been written for devices which are connected wirelessly to off-board systems/devices, but doesn't exclude standalone devices without wireless connection or devices connected via wired connection (e.g., USB).

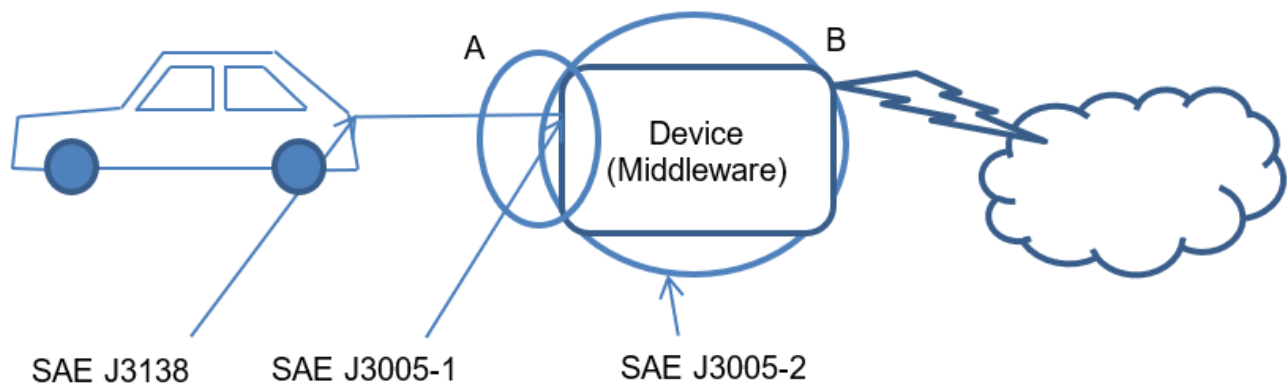


Figure 1 - Overview of standards

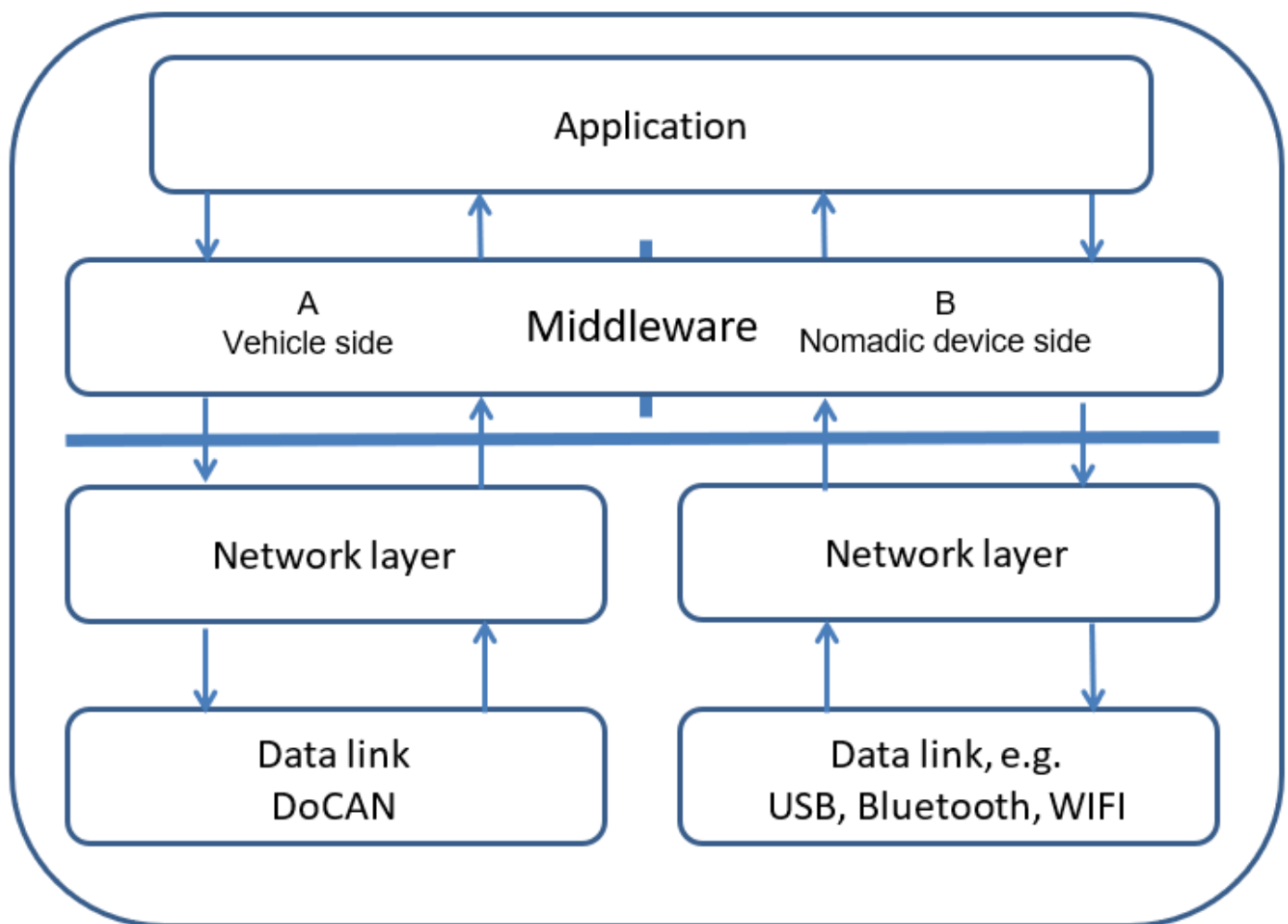


Figure 2 - Permanently or semi-permanently installed diagnostic communication device firmware layout