



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

1.	SCOPE.....	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
3.	TERMS AND DEFINITIONS	4
3.1	Definitions	4
4.	GENERAL RECOMMENDATIONS	5
4.1	Protocol Service Categorization.....	5
4.2	Protocol Service Categorization Considerations	6
4.3	Legislated Diagnostic Protocols.....	7
4.4	Network Communications and CAN Protocol Error Handling.....	7
4.5	Measurement and Calibration	8
4.6	Enhanced Diagnostic Protocols	8
4.7	Service Requests to Gateway(s) or Individual ECUs	8
4.8	Vehicle Safe State.....	8
4.8.1	Determination of Vehicle Safe State	8
4.8.2	Intrusive Message Block	9
4.8.3	Rejecting Messages.....	9
4.8.4	Conditional Change of Vehicle Safe State.....	9
4.8.5	Performing Tasks Defined in Service Information	9
4.8.6	Protocol Services Supporting Repair Procedures	9
4.8.7	Lifecycle Service Availability	9

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 © 2022 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 J3138_202210

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

Documents

Document Sharing Hub

5.	TECHNICAL RECOMMENDATIONS FOR VEHICLE NETWORKS WITH NO GATEWAY	10
6.	TECHNICAL RECOMMENDATIONS FOR VEHICLE NETWORKS WITH PARTIAL FUNCTION GATEWAY	10
7.	TECHNICAL RECOMMENDATIONS FOR VEHICLE NETWORKS WITH FULL GATEWAY OR MULTIPLE GATEWAY CONFIGURATION(S)	10
8.	NOTES	10
8.1	Revision Indicator.....	10

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