



SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-91A

MAR2025

Issued

2025-03

Security Recommendations for Interfaces to On-Vehicle Networks

RATIONALE

This document provides guidelines for securing communications with vehicles utilizing the on-vehicle to off-vehicle interface.

FOREWORD

The SAE J1939 communications network is defined using a collection of individual SAE J1939 documents based upon the layers of the Open System Interconnect (OSI) model for computer communications architecture.

The SAE J1939 communications network is a high-speed ISO 11898-1 CAN based communications network that supports real-time closed loop control functions, simple information exchanges, and diagnostic data exchanges between Electronic Control Units (ECUs) physically distributed throughout the vehicle.

The SAE J1939 communications network is developed for use in heavy-duty environments and suitable for horizontally integrated vehicle industries. The SAE J1939 communications network is applicable for light-duty, medium-duty, and heavy-duty vehicles used on-road or off-road, and for appropriate stationary applications which use vehicle-derived components (e.g., generator sets). Vehicles of interest include, but are not limited to, on-highway and off-highway trucks and their trailers, construction equipment, and agricultural equipment and implements. The physical layer aspects of SAE J1939 reflect its design goal for use in heavy-duty environments. Horizontally integrated vehicles involve the integration of different combinations of loose package components, such as engines and transmissions that are sourced from many different component suppliers. The SAE J1939 common communication architecture strives to offer an open interconnect system that allows the ECUs associated with different component manufacturers to communicate with each other.

SAE Executive Standards Committee 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 © 2025 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, 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 J193991A_202503

For more information on this standard, visit https://www.sae.org/standards/content/J193991A_202503/

Documents

Document Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	3
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.1.2	ISO and SAE Publications	4
2.1.3	ISO Publications.....	4
2.2	Related Publications	4
2.2.1	SAE Publications.....	5
2.2.2	ANSI Accredited and IEEE Publications	5
2.2.3	ISO Publications.....	5
2.2.4	NHTSA Publications.....	5
3.	DEFINITIONS AND DESCRIPTION OF TERMS	5
4.	ABBREVIATIONS	10
5.	INTRODUCTION AND OVERVIEW	10
5.1	Cybersecurity Analysis and Risk.....	10
5.2	Use Cases for Securing the Off-Vehicle to On-Vehicle Communication Network Interfaces.....	11
5.3	SAE J1939 Layered Network Security Model.....	11
5.4	SAE J1939 Layered Network Security Model Documents.....	12
6.	TECHNICAL RECOMMENDATIONS	13
6.1	General Security Recommendations	13
6.2	Secure ECUs (Hardware)	14
6.3	Secure Architecture.....	14
6.3.1	Domain Separation	14
6.3.2	Vehicle Message Matrix (VMM)	15
6.3.3	Gateway and Firewall Functions	15
6.4	Secure Connectivity	16
6.4.1	Authentication and Authorization	16
6.4.2	SAE J1939 Network On-Board Diagnostics Interface	17
6.4.3	Diagnostic Services and Diagnostic Firewall	17
6.5	Imposter Detection and Reporting	21
7.	NOTES.....	21
7.1	Revision Indicator.....	21
Figure 1	Layered security model.....	12
Figure 2	Layers of network security	13
Figure 3	Network security separation.....	15
Table 1	Intrusiveness categorization of SAE J1939 diagnostic services.....	19

1. SCOPE

This document provides recommendations to vehicle manufacturers, ECU developers, and other device suppliers in securing the SAE J1939 network from cybersecurity risks. This document focuses on security measures related to on-vehicle network architecture and security measures for communication interfaces between devices, ECUs, or networks. The focus is on security related to network communications on the vehicle side of off-vehicle interfaces, such as the SAE J1939-13 connector.

The recommendations in this document aim to address cybersecurity risks presented by communication between the vehicle and the rest of the supporting ecosystem via the vehicle networks. The risk focus is on safety and operational risks, although other risks are possible. This document should be used as a reference to current best practices for addressing off-vehicle communication security.

This document focuses on recommendations related to the Secure Architecture and Secure Connectivity aspects of vehicle security; it is the first in a family of security-related documents. Recommendations for secure on-board communications between ECUs and any other on-vehicle device will be defined in another document. While Secure ECU is out of scope for this document, this document does include some Secure ECU recommendations only to the extent needed to support the recommendations of topics that are in scope.

Some of the described guidelines and measures described in this document include:

- Overview of the SAE J1939 layered security model
- Secure Architecture
 - Domain Separation
 - Vehicle Messaging Matrix (VMM) to document all network messaging
 - Multi-level security (MLS) policy, based on VMM, to control message flow between domains
- Secure Connectivity
 - Gateways and firewalls to isolate on-vehicle networks from off-vehicle networks and control message flow of incoming messages from off-vehicle
 - Firewall-based diagnostic services control
 - ECU-based diagnostic services control
- An alert service for reporting detected imposter messaging activity

It is recognized that not every application of SAE J1939 networks requires the same level of cybersecurity measures. Techniques to determine the level of cybersecurity measures required are out of scope for this document. Generally, higher-risk applications require higher levels of cybersecurity measures.

Generally, there are three forms of communication methodologies used in current vehicles:

1. Open access to communication buses – security included inside each networked ECU
2. Communication buses isolated via a gateway – central security interconnect ECU
3. Combinations of (1) and (2)

This document provides guidelines for securing communications with any off-board device for vehicles utilizing any of these methodologies.

2. REFERENCES

2.1 Applicable Documents

General information regarding this series of documents is found in SAE J1939.

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 Serial Control and Communications Heavy-Duty Vehicle Network - Top-Level Document

SAE J1939-13 Off-Board Diagnostic Connector

SAE J1939-21 Data Link Layer

SAE J1939-22 CAN FD Data Link Layer

SAE J1939-73 Application Layer - Diagnostics

SAE J1939DA J1939 Digital Annex

SAE J2728 Heavy Vehicle Event Data Recorder (HVEDR)

SAE J3101 Hardware Protected Security for Ground Vehicles

2.1.2 ISO and SAE Publications

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

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.

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

2.1.3 ISO Publications

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

ISO 11898-1 Road vehicles - Controller area network (CAN) - Part 1: Data link layer and physical coding sublayer

ISO 14229-1 Road vehicles - Unified diagnostic services (UDS) - Part 1: Specification and requirements

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 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 J1939-01 On-Highway Equipment Control and Communication Network

SAE J1939-02 Agricultural and Forestry Off-Road Machinery Control and Communication Network

SAE J1939-31 Network Layer

SAE J1939-71 Vehicle Application Layer

SAE J1939-81 Network Management

SAE J3138 Diagnostic Link Connector Security

2.2.2 ANSI Accredited and IEEE Publications

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

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

ANSI/IEEE STD.802-1D Local Area Networks: Media Access Control (MAC) Bridges

2.2.3 ISO Publications

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

ISO 11783 Tractors and machinery for agriculture and forestry - Serial control and communications data network

ISO 11992 Road vehicles - Interchange of digital information on electrical connections between towing and towed vehicles

ISO 15765 Road vehicles - Diagnostics on controller area network (CAN)

2.2.4 NHTSA Publications

Available from National Highway Traffic Safety Administration, 1200 New Jersey Avenue, SE, Washington, DC 20590, Tel: 1-888-327-4236, <https://www.nhtsa.gov/>.

Cybersecurity Best Practices for the Safety of Modern Vehicles

3. DEFINITIONS AND DESCRIPTION OF TERMS

Refer to SAE J1939 for definitions that are not defined in this document.

3.1 ASSET

A cybersecurity asset is any item of value to the stakeholders. That value is determined by the stakeholders in consideration of the loss concerns across the entire system life cycle. Assets may be tangible or intangible and must be protected based on the security risk to the assets. Examples of assets include, but are not limited to, any data, service, or device of the vehicle system that is used to support information-related activities. A formal, structured process to determine assets and their security risk level should be used.

3.2 ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are large numbers that are paired but not identical (asymmetric). The keys are used as an input to cryptography algorithms that convert plain text to ciphertext. Here, text can be any type of data that requires protection; it is not necessary for the data to be a human language text. With asymmetric cryptography, one key can encrypt the text, but that key cannot decrypt the ciphertext. Only the second key of the key pair can convert the ciphertext back to plain text.

This asymmetric encryption property means that one key can be shared with everyone and is called the public key. The other key in the pair is kept secret and is called the private key. The sender uses the recipient's public key to encrypt the text; the recipient uses the private key to decrypt the text. The sender trusts only the recipient can decrypt the text, as only the recipient knows the required private key.

The reverse is also true. The sender can encrypt a bit of text with their private key. Any recipient can use the sender's public key to verify the identity of the sender. The recipient trusts the sender sent the message, as only the sender knows the required private key. It is important to note that in this case, the public key allows for decryption, and the text is not confidential.

For a bidirectional chain of trust, the methods are combined. The sender encrypts the data to be transmitted with the receiver's public key, ensuring confidentiality of the text. Some additional data, known as a signature, is encrypted with the sender's private key, ensuring integrity of the text. The sender trusts only the receiver can decrypt the main text, and the receiver trusts only the sender sent the message. For asymmetric cryptography to be secure, the private key of the key pair must always be protected. If the private keys are compromised, then the chain of trust is broken, and security is not possible.

Common examples of asymmetric cryptographic algorithms are RSA encryption algorithm, Elliptic-curve cryptography, and Diffie-Hellman key exchange protocol.

3.3 ATTACK SURFACE

An attack surface describes all the points of entry of a system available to an attacker.

3.4 AUTHENTICITY

Authenticity is the ability for the receiver of the data to be able to verify the data originated by a known source. Authenticity can be achieved by applying a signature to all or part of the data (hash value).

3.5 AUTHORIZATION

Authorization is the ability of the receiver of data to verify the privileges of the sender. These privileges can include the ability to invoke certain diagnostic services, e.g., read or write defined data. Authorization can be achieved by the use of credentials. Credentials can be the use of digital signatures with or without the addition of certificates.

3.6 BELL-LAPADULA MODEL

A security policy that focuses on data confidentiality. The sender and receivers of data are grouped into levels based on security requirements. Bell-LaPadula model defines a set of security rules:

1. An item at a given security level may not read data from an item at a higher security level – *no read up*
2. An item at a given security level may not write to an item at a lower security level – *no write down*

Summary: *No read up, no write down*

3.7 BIBA INTEGRITY MODEL

A security policy of access control is designed to ensure data integrity. The sender and receivers of data are grouped into levels based on integrity requirements. Biba model defines a set of integrity rules:

1. An item at a given integrity level must not read data at a lower integrity level – *no read down*
2. An item at a given integrity level must not write data to a higher integrity level – *no write up*

Summary: *No write up, no read down*

3.8 CONFIDENTIALITY

Confidentiality aims to ensure that an unauthorized party cannot interpret the content of the transmitted or stored data. This can be achieved by encrypting the data. Encryption could be done either prior to transmission and/or during storage.

3.9 COPY PROTECTION

Copy protection guarantees that the data can only be used on the intended device or by the intended user. Copy protection can be achieved by encrypting the data using a specific key to bind the data to a specific device or user.

3.10 CRYPTOGRAPHIC HASH FUNCTION

A cryptographic hash is a hash function that provides an ability to evaluate the integrity of the data and makes it difficult to reconstruct the data by knowing the hash value. Not all hash functions provide this ability. In general, cryptographic hash functions are provided by standards organizations. The National Institute of Standards and Technology (NIST) provides the SHA1, SHA2, and SHA-3 standards.

3.11 CRYPTOSYSTEM

A cryptosystem is a suite of cryptographic algorithms required to implement a given requirement or service. This typically includes algorithms for key generation, encryption, and (if necessary) decryption.

3.12 DIAGNOSTIC SERVICE

A diagnostic service is a message used to request diagnostic information from a device or modify a device's behavior for diagnostic purposes. A diagnostic service is initiated by a client, typically an off-board device such as a service tool, and the diagnostic service is performed by a server, typically an on-vehicle device. The SAE J1939 diagnostic services are defined in SAE J1939-73; refer to ISO 14229-1 UDS for information on other possible vehicle diagnostics services available on a SAE J1939 data link.

3.13 DOMAIN

A domain is a collection of objects. These objects can be anything. Within the cybersecurity context, these objects are most commonly items such as data, software, microcontrollers, ECUs, communication networks, sensors, and actuators.

Domains are very useful to group objects that share common characteristics. In the context of this document, domains refer to physical communication networks.

3.14 ECU

An ECU is an embedded software Electronic Control Unit. It is a computer based electronic assembly that can send or receive SAE J1939 messages.