



SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-76

NOV2025

Issued 2018-11
Revised 2025-11

Superseding J1939-76 APR2020

(R) SAE J1939 Functional Safety Communications Protocol

RATIONALE

The protocol has been updated to include a more robust implementation to address additional information that is relevant to implementing the standard. This resulted in an alternate implementation of the protocol that meets a stricter error probability and subsequent functional safety levels.

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 Functional Safety Communications Protocol document describes an optional application layer typically used when designing a high-integrity system that includes functional safety related features.

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, like an engine and transmissions, which 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: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: SAE J1939-76_202511

For more information on this standard, visit https://www.sae.org/standards/content/J1939-76_202511/

Documents

Standard, visit Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	4
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.1.2	IEC Publications.....	4
2.1.3	ISO Publications.....	4
2.2	Related Publications	4
2.2.1	Other Publications.....	4
3.	DEFINITIONS AND ABBREVIATIONS.....	5
3.1	Definitions	5
3.1.1	Terms Used in Document	5
3.1.2	Applicable IEC 61784-3:2024 Terms and Definitions	7
3.2	Abbreviations	8
4.	TECHNICAL REQUIREMENTS.....	9
4.1	Overview	9
4.2	Concept of Operation	9
4.2.1	Communication Error Coverage	11
4.2.2	Networks with Routers	13
4.3	Limitations	13
4.3.1	General Limitations	13
4.4	SAE J1939 PG Constraints.....	13
4.4.1	Applicable SAE J1939 Messages.....	13
4.4.2	Not Applicable SAE J1939 Message	13
5.	BEHAVIORAL REQUIREMENTS	14
5.1	General Requirements.....	14
5.1.1	Safety Data Group Operations.....	14
5.1.2	Safety Data Group and Safety Data Group Series	15
5.1.3	SDG Timing Requirements	16
5.1.4	Sequence Number	17
5.1.5	CRC.....	17
5.1.6	SHM and SDM Sequence within an SDG.....	18
5.2	Producer Requirements	18
5.2.1	General Requirements.....	21
5.2.2	Construct the SDM.....	21
5.2.3	Construct the SHM.....	21
5.2.4	Sequence Number	21
5.2.5	CRC.....	21
5.2.6	SDG Identifiers.....	22
5.2.7	SHM Priority and Destination Address.....	22
5.2.8	Transmit the SHM and SDM	23
5.3	Consumer Requirements	23
5.3.1	General Requirements.....	26
5.3.2	SHM Identification	26
5.3.3	SDM Identification	26
5.3.4	SHM and SDM Pairing	26
5.3.5	SDG Identifier Validation.....	27
5.3.6	SCT Validation	27
5.3.7	SRVT Validation.....	30
5.3.8	CRC Validation.....	31
5.3.9	Sequence Number Validation	32

6.	MESSAGE STRUCTURE AND REQUIREMENTS	33
6.1	Message Structure	33
6.2	Safety Header Message 2 (SHM2) Definition	33
6.3	Safety Header Message 2 Parameter Definitions	34
6.3.1	SHM2 Sequence Number (SPN 23604)	34
6.3.2	SDM Data Page (SPN 23605)	34
6.3.3	SDM Extended Data Page (SPN 23606)	34
6.3.4	SDM PS Value (SPN 23607)	34
6.3.5	SDM PF Value (SPN 23608)	35
6.3.6	SHM2 Enhanced CRC (SPN 23609)	35
6.4	Safety Header Message 1 (SHM1) Definition	37
6.5	Safety Header Message 1 (SHM1) Definition	37
6.6	Safety Header Message 1 (SHM1) Parameter Definitions	38
6.6.1	Inverted SDM Data Page (SPN 9387)	38
6.6.2	Inverted SDM Extended Data Page (SPN 9388)	38
6.6.3	Reserved Bit	38
6.6.4	SHM1 Sequence Number (SPN 9382)	38
6.6.5	Inverted SDM Source Address (SPN 9384)	38
6.6.6	Inverted SDM PS Value (SPN 9385)	39
6.6.7	Inverted SDM PF Value (SPN 9386)	39
6.6.8	SDM Data CRC (SPN 9383)	39
7.	SYSTEM DESIGN REQUIREMENTS	40
7.1	When to Use the SAE J1939-76 Functional Safety Communication Protocol	40
7.2	When Not to Use the SAE J1939-76 Functional Safety Communication Protocol	40
7.3	Configuration of the SAE J1939-76 Functional Safety Communication Protocol	40
7.4	Systems Constraints for Meeting Safety and Performance Levels	40
7.5	Guidance for Use in Systems	41
7.6	Error Reporting for SAE J1939-76	41
8.	NOTES	41
8.1	Revision Indicator	41
APPENDIX A	SAFETY MEASURES AND ANALYSIS USING SHM2	42
APPENDIX B	SAFETY MEASURES AND ANALYSIS USING SHM1	50
APPENDIX C	TÜV APPROVAL LETTER FOR SHM1 VERSION	57
Figure 1	Safety protocol overview	11
Figure 2	Concept of operation	15
Figure 3	Producer SDG2 behavioral model for SHM2	19
Figure 4	Producer SDG1 behavioral model for SHM1	20
Figure 5	Consumer SDG2 behavioral model for SHM2	24
Figure 6	Consumer SDG1 behavioral model for SHM1	25
Figure 7	Example of SCT violation, late SHM	28
Figure 8	Example of SCT violation, late SDM	29
Figure 9	Example of start-up timing	30
Figure 10	Example of SVRT violation	31
Figure 11	Sequence number validation examples for SHM1 message	32
Figure 12	SHM2 message structure	33
Figure 13	CRC computation illustration	35
Figure 14	Mapping of SHM1 SPs to CAN frame data field	37
Table 1	Communication error coverage	12
Table 2	Constraints for SAE J1939 PG applicable with SAE J1939 Functional Safety Communications Protocol	13
Table 3	Constraints for SAE J1939 PG not applicable with SAE J1939 Functional Safety Communications Protocol	13
Table 4	Maximum SCT requirement	16
Table 5	Maximum SRVT requirement	16

1. SCOPE

This document provides the technical requirements for implementing the SAE J1939 Functional Safety Communication Protocol in a manner determined suitable for meeting industry applicable functional safety standards.

2. REFERENCES

2.1 Applicable Documents

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

2.1.1 SAE Publications

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

SAE J1939 Serial Control and Communications Heavy-Duty Vehicle Network - Top-Level Document

SAE J1939-22 CAN FD Data Link Layer

SAE J1939-71 Vehicle Application Layer

SAE J1939-73 Application Layer – Diagnostics

SAE J1939-77 SAE J1939 CAN FD Functional Safety Assurance Data

2.1.2 IEC Publications

Available from IEC Secretariat, 3 rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 0211, www.iec.ch.

IEC 61508:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

IEC 61784-3:2024 Functional Safety Fieldbuses - General Rules and Profile Definitions

2.1.3 ISO Publications

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

ISO 13849-1:2015 Safety of Machinery - Safety-Related Parts of Control Systems - Part 1: General Principles for Design

ISO 25119-1:2010 Tractors and Machinery for Agriculture and Forestry - Safety-Related Parts of Control Systems - Part 1: General Principles for Design and Development

ISO 26262-2:2011 Road Vehicles - Functional Safety - Part 2: Management of Functional Safety

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

Best CRC Polynomials, Philip Koopman, Carnegie Mellon University, <https://users.ece.cmu.edu/~koopman/crc/>.

3. DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

3.1.1 Terms Used in Document

3.1.1.1 ADDRESS

The 8-bit field (or fields) used to identify the source (and destination when applicable) of a message (e.g., engine, transmission, etc.).

3.1.1.2 BLACK CHANNEL

A communication channel containing components that are not designed or validated to applicable functional safety standards.

3.1.1.3 COMMUNICATION CHANNEL

Logical connection between two end-points with a communication system.

3.1.1.4 CONSUMER

See “Consumer Safety Application.”

3.1.1.5 CONSUMER SAFETY APPLICATION

The ECU safety application that receives the Safety Header Message and the corresponding Safety Data Message and confirms SAE J1939 Functional Safety Communications Protocol protocol validations prior to using or applying the Safety Data Message data.

3.1.1.6 FIXED TRANSMISSION RATE PG

Classification of an SAE J1939 PG transmitted continually at a fixed periodic interval, according to its SAE J1939 Transmission Rate. A Fixed Transmission Rate PG is characterized as having an SAE J1939 Transmission Rate declared with only a single periodic interval, such as “100 ms.”

3.1.1.7 PRODUCER

See “Producer Safety Application.”

3.1.1.8 PRODUCER SAFETY APPLICATION

The ECU safety application that sends the Safety Header Message and the corresponding Safety Data Message.

3.1.1.9 SAFETY CYCLE TIME (SCT)

The period of time that transpires between successive SDM instances of the same Safety Data Group Series. The safety cycle time is typically the SAE-specified transmission rate.

3.1.1.10 SAFETY DATA GROUP (SDG)

A specific instance of a pair of SAE J1939 messages consisting of the SDM and its corresponding SHM. This series of messages has two forms: SDG1 and SDG2.

3.1.1.11 SAFETY DATA GROUP 1 (SDG1)

A safety data group consisting of an SDM and an SHM1 message.

3.1.1.12 SAFETY DATA GROUP 2 (SDG2)

A safety data group consisting of an SDM and an SHM2 message.

3.1.1.13 SAFETY DATA GROUP SERIES

The sequence of SDGs associated with a single data channel based upon a unique combination of PG, source address, and destination address.

3.1.1.14 SAFETY DATA MESSAGE (SDM)

The standard SAE J1939 message containing the operational data provided by the producing safety application and used by the consumer safety application as part of a safety-related system.

3.1.1.15 SAFETY HEADER MESSAGE (SHM)

The additional SAE J1939 message that is transmitted with each instance of a Safety Data Message as part of a Safety Data Group. The SHM provides CRC and sequencing data that enable the consumer safety application to detect data and communication errors. This message has two forms: SHM1 and SHM2.

3.1.1.16 SAFETY HEADER MESSAGE 1 (SHM1)

SHM1 is the original form of the SHM message that has a CRC that covers 8 bytes of data from the SDM. This message is deprecated.

3.1.1.17 SAFETY HEADER MESSAGE 2 (SHM2)

SHM2 is the newer form of the SHM message with enhanced CRC coverage. This new CRC covers 8 bytes of data from the SDM as well as the first 4 bytes of the SHM2 message and the source address of the producer (13 bytes total). See [6.3.2](#) for details. This message is the preferred one to use in all new applications.

3.1.1.18 SAFETY RELATED SYSTEM

Element or group of elements that independently implement a safety-related function of a system.

3.1.1.19 SAFETY-RELEVANT VALIDATION TIME (SRVT)

The period of time that transpires between the SHM and the SDM of the same SDG.

3.1.1.20 SDG IDENTIFIER

Refers to either or both SDG1 Identifier and SDG2 Identifier. See below.

3.1.1.21 SDG1 IDENTIFIER

The identifier of a pair of SHM1 and SDM messages that is used to identify the SDM message from the corresponding SHM1 message. The SDG1 Identifier is defined as the combination of the following SPs:

- Inverted SDM Data Page
- Inverted SDM Extended Data Page
- Inverted SDM Source Address
- Inverted SDM PS Value
- Inverted SDM PF Value

3.1.1.22 SDG2 IDENTIFIER

The identifier of a pair of SHM2 and SDM messages that is used to identify the SDM message from the corresponding SHM2 message. The SDG2 Identifier is defined as the combination of the following SPs:

- SHM2 SDM Data Page
- SHM2 SDM Extended Data Page
- SHM2 SDM PS Value
- SHM2 SDM PF Value

3.1.1.23 SEQUENCE OR SHM SEQUENCE

Refers to either or both the SHM1 sequence number and the SHM2 sequence number. This term is used when the behavior of the two SHM forms of the header message are the same.

3.1.1.24 SHM1 SEQUENCE NUMBER

The 5-bit number included in the SHM1 header message to identify sequential instances of the message.

3.1.1.25 SHM2 SEQUENCE NUMBER

The 14-bit number included in the SHM2 header message to identify sequential instances of the message.

3.1.1.26 VARIABLE TRANSMISSION RATE PG

Classification of an SAE J1939 PG transmitted continually but with the possibility of varying intervals between any two consecutive transmitted instances. A Variable Transmission Rate PG is characterized as having an SAE J1939 Transmission Rate describing on-event transmit behavior or a variable transmit period, such as “every 100 ms and on change but no faster than 20 ms” or “engine speed dependent.”

3.1.1.27 WHITE CHANNEL

Entire communication channel (including protocol, services, and network components) that complies with applicable functional safety standards.

3.1.2 Applicable IEC 61784-3:2024 Terms and Definitions

3.1.2.1 MESSAGE CORRUPTION

Messages can be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.

3.1.2.2 UNINTENDED REPETITION

Due to an error, fault, or interference, old not-updated messages are repeated at an incorrect point in time.

3.1.2.3 INCORRECT SEQUENCE

Due to an error, fault, or interference, the predefined sequence (for example, natural numbers, time references) associated with messages from a particular source is incorrect.

3.1.2.4 LOSS

Due to an error, fault, or interference, a message is not received or not acknowledged.

3.1.2.5 UNACCEPTABLE DELAY

Messages can be delayed beyond their permitted arrival time window, for example, due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (for example, FIFOs in switches, bridges, routers).

3.1.2.6 INSERTION

Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity.

3.1.2.7 MASQUERADE

Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a safety-related participant receives a non-safety-related message, which it treats as safety related.

3.1.2.8 ADDRESSING

Due to an error, fault, or interference, a message is mistakenly received between a sender and receiver that, in fact, is not the intended connection.

3.2 Abbreviations

ACK	Acknowledgment
BER	Bit Error Rate
CA	Controller Application
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
ECU	Electronic Control Unit
FSCP	Functional Safety Communication Protocol
PFH	Probability for Failure per Hour
PG	Parameter Group
PGN	Parameter Group Number
PL	Performance Level
SCT	Safety Cycle Time
SDG	Safety Data Group
SDG1	Safety Data Group 1
SDG2	Safety Data Group 2
SDM	Safety Data Message

SHM	Safety Header Message
SHM1	Safety Header Message 1
SHM2	Safety Header Message 2
SIL	Safety Integrity Level
SRVT	Safety-Relevant Validation Time

4. TECHNICAL REQUIREMENTS

4.1 Overview

This document describes the behaviors and messaging established to support industry-specific functional safety or performance levels when using an SAE J1939 communication network. Evaluation of this protocol according to IEC 61784-3:2024 has determined the protocol is capable of meeting IEC 61508:2010 SIL 2 or SIL 3. Implementations must strictly conform to the behavioral requirements described herein to attain these performance levels. See [Appendix A](#) and [Appendix B](#) for example analyses.

SAE J1939-76 is deemed capable of meeting IEC 61508:2010 SIL 3, which is a PFH less than 10^{-7} . The safety level capability according to other safety standards, such as ISO 26262, shall be based upon a PFH less than 10^{-7} . The contribution of the communication systems to the PFH must be less than 1% (or $<10^{-9}$ for SIL 3). Based upon a probability of failure per hour approach, this protocol can also achieve the functional safety levels for other standards, such as:

- ISO 26262-2:2011 (ASIL B, ASIL C)
- ISO 25119-1:2010 (AgPL_b, AgPL_c, or AgPL_d)
- ISO 13849-1:2015 (PL_c, PL_d, PL_e, Cat. 4)

Users of this protocol are responsible for any industry-specific safety performance compliance validation specific to their system and component implementations.

This document outlines a method to attain industry-specific safety performance levels of the SAE J1939 communication network. The overall system capability and resulting functional safety performance achieved is dependent upon the entire system design including, but not limited to, the communications subsystem.

4.2 Concept of Operation

The SAE J1939 Functional Safety Communication Protocol improves the reliable and safer delivery of critical data over an SAE J1939 network in a control system by pairing an additional message, known as a Safety Header Message (SHM), together with each transmitted instance of a critical data message, known as the Safety Data Message (SDM). In this manner, the paired messages along with a sequence number and repeated identifier in the specified cross-checking reduce the possibility of undetected message corruption and addressing errors and provide the ability to detect timeliness errors such as incorrect sequence, loss, unintended repetition, and unacceptable delay, as well as masquerade and insertion.

This version of the SAE J1939-76 standard introduces an enhanced CRC computation covering not only the data in the SDM but also 4 bytes of additional information from the SHM and 1 byte of source address information to reduce even further any undetected errors. The sequence number in this version has also been increased from 5 to 14 bits. To distinguish this new enhancement, a new SHM message called SHM2 is introduced. See [6.1](#). It is recommended that all new designs use this SHM2 message and enhanced CRC computation. The original SHM message is now referred to as SHM1.

When SHM is used in this document, it refers to either or both the SHM1 and SHM2 versions.

The introduction of the SHM2 version of the SHM message was because of updated communication standards like IEC 61784-3:2024 and newer methods of mathematically modeling the error probabilities. The informative analysis for the SHM2 version of the message is found in [Appendix A](#). The original SHM1 version of the SHM message is still a valid approach; however, the informative analysis shown in [Appendix B](#) is based on older mathematical models that have been replaced.

The SAE J1939 Functional Safety Communication Protocol deals with the reliable and safer delivery of critical data over an SAE J1939-based communication channel between the safety communication layer in the producer safety application (Producer) and the safety communication layer in the consumer safety application (Consumer). Destination-specific (PDU1) and broadcast (PDU2) PGs can be used as SDMs in this safety protocol since the behaviors of the producer and consumer are decoupled, i.e., no handshaking is required. The Safety Header Message is a general-purpose SAE J1939 PG designed to be used in conjunction with any SAE J1939 PG (SDM) that carries application or system operational data. The data field of each Safety Header Message instance contains parts of the CAN ID of the paired SDM, the CRC of the SDM data, and relative sequence of the paired SDM. The enhanced CRC in the SHM2 version of the message contains additional information from the SHM2 (see [6.3.6](#)). The SHM provides data that allows the paired SDM to be validated for correctness and consistency. Each Safety Header Message and Safety Data Message pair is known as a Safety Data Group.

The producer is responsible for constructing the SHM for each SDM and transmitting the SHM and SDM in correct order and within certain time constraints. The producer constructs the SHM data field with the PGN of the paired SDM, the CRC of the SDM data (and the SHM2 data in the case of the SHM2 version), and relative sequence of the paired SDM. The producer repeats this cycle each successive instance of the SDM.

The pair of SDM and SHM is known as a safety data group or SDG. The SDM and SHM1 pairing is called SDG1 and the pairing of SDM and SHM2 is called SDG2. When SDG is used alone, it refers to either or both SDG1 and SDG2.

The consumer is responsible for matching up the SHM and SDM pair forming an SDG and validating the timing and data integrity of the SDG prior to potentially providing the SDM for application use. The consumer verifies the SHM and SDM are received in correct order and within required timing constraint, uses the SHM data to validate the SDM data integrity, and validates SHM sequence number for duplicated or missed SDM. If a received SDG fails one or more of these validations, the consumer safety application cannot use the data from the SDM.

The basic aspects of the protocol are illustrated in the sequence diagram in [Figure 1](#). The associated pair of SHM and its SDM constitutes a single Safety Data Group (SDG) instance. The Safety-Relevant Validation Time (SRVT) identifies the timing between the SHM and SDM of a single SDG instance. The Safety Cycle Time (SCT) identifies the timing between consecutive SDM instances.

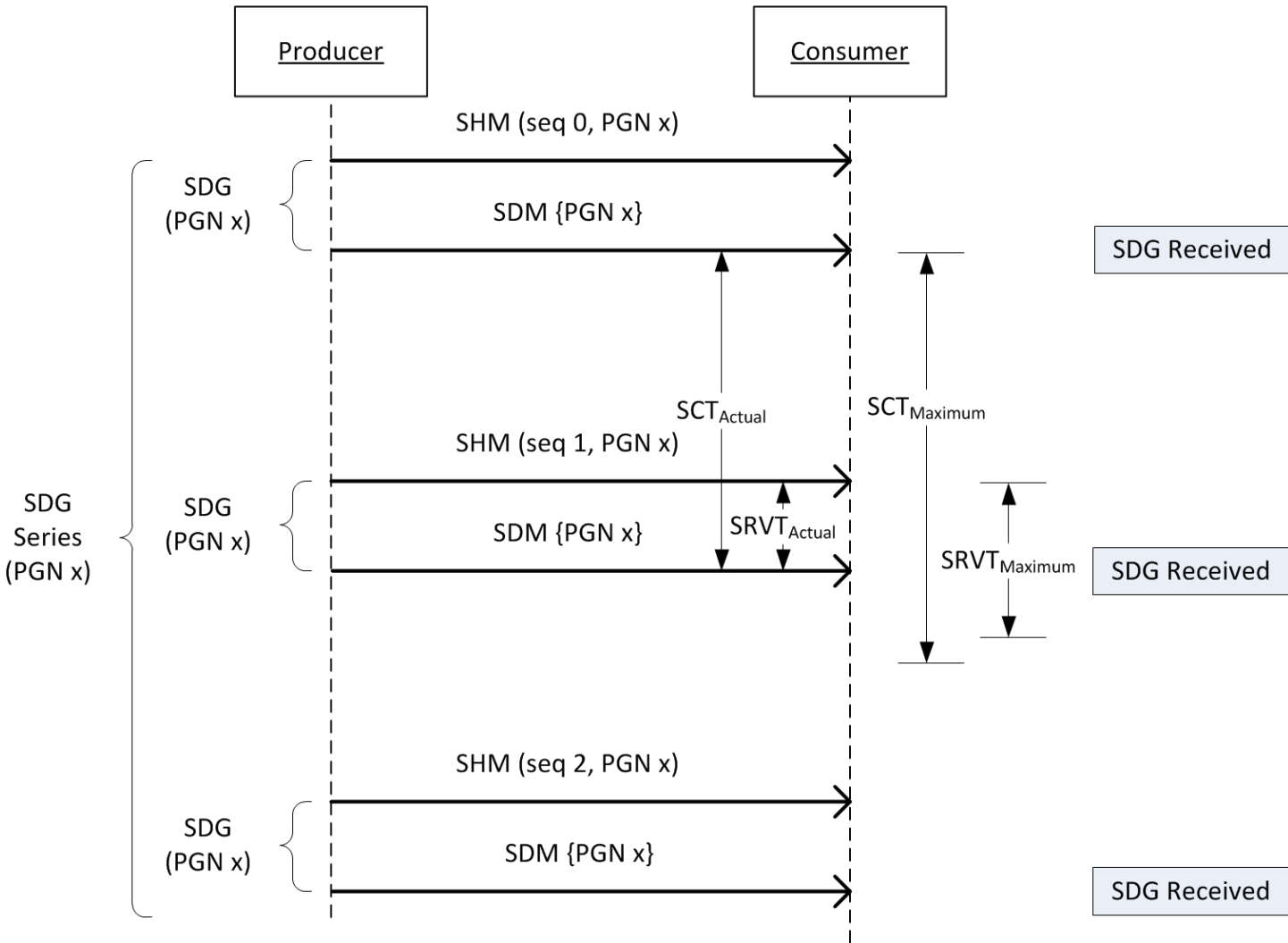


Figure 1 - Safety protocol overview

Multiple SDG instances may exist on the network simultaneously from the same or different producer. See 5.1.2 for details.

4.2.1 Communication Error Coverage

Table 1 specifies the diagnostic measures used in the SAE J1939 Functional Safety Communication Protocol for each of the IEC 61784 communication errors.

Table 1 - Communication error coverage

Communication Error	Measure for Detection
Addressing	Connection authentication is the measure for detecting addressing errors. The safety application layer uses the identifier information of the SDM and the CRC protected PGN and SA from the matched SHM of the same SDG to verify the SDM addressing matches the SHM, verify the source and destination address for both packets match, and verify this data was intended for this receiver address and came from the expected source address. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Corruption	Data integrity is the measure for detecting message corruption. The safety application layer uses the 32-bit SDM data CRC from the SHM to provide the data integrity assurance for the 64-bit data provided to the safety application via the SDM. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Incorrect Sequence	Sequence number is the measure for detecting incorrect sequence errors. The safety application layer uses the sequence number in every SHM to detect incorrect sequence of a message. Every SHM message contains a sequence number where the sequence number is expected to be incremented by one for each SDM update from a producer safety application. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Insertion	Sequence number and connection authentication are the measures for detecting insertion errors. The safety application layer uses the sequence number in every SHM to detect insertion errors. Authentication information is used by the consumer to detect if an unauthorized entity is attempting to insert messages. Every SHM message contains a sequence number where the sequence number is expected to be incremented by one for each SDM update from a producer safety application. The safety application layer cross-checks the identifier information of the SDM and the copy from the matched SHM2 (or the inverted copy from the matched SHM1) of the same SDG and cross-checks the 32-bit SDM data CRC from the SHM and the 64-bit data of the SDM to verify the SDG. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Loss	Sequence number is the measure for detecting loss errors. The safety application layer uses the sequence number in every SHM to detect loss of a message. Every SHM message contains a sequence number where the sequence number is expected to be incremented by one for each SDM update from a producer safety application. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Masquerade	Sequence number, connection authentication, data integrity, and redundancy with cross-checking are the measures for detecting masquerade errors. Sequence number requires an unauthorized entity to know in real time what the next sequence number is, and the consumer can receive two messages with the same sequence number, causing it to take protective measures. Authentication information is used by the consumer to detect if an unauthorized entity is attempting to insert messages. Portions of the producer's CAN ID are repeated in the SHM, and the safety application layer uses the 32-bit SDM data CRC from the SHM, which is not used elsewhere in the SAE J1939 standard or the CAN physical layer or data link layers, to determine when the SDM data can be used for safety related purposes.
Unacceptable Delay	Time expectation is the measure for detecting unacceptable delay errors. The safety application layer monitors the time from the last properly verified SDG to determine if too much time has transpired without reception of a new verified SDG. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.
Unintended Repetition	Sequence number is the measure for detecting unintended repetition errors. The safety application layer uses the sequence number in every SHM to detect old messages. Every SHM message contains a sequence number where the sequence number is expected to be incremented by one for each SDM update from a producer safety application. The safety application layer uses this as part of the validation process for the received safety related data to determine when the SDM data can be used for safety related purposes.

4.2.2 Networks with Routers

In the case of networks that employ routers between network segments, the possibility of excessively delayed messages or unintended transmission of stored messages from the router memory must be considered. The methods specified in [Table 1](#) for corruption, unintended repetition, incorrect sequence, and unacceptable delay are deemed to be effective for these errors.

4.3 Limitations

4.3.1 General Limitations

- This protocol does not address intrinsic safety, only functional safety.
- Security is not specifically addressed although some aspects of security are incidentally improved.

4.4 SAE J1939 PG Constraints

The SAE J1939 Functional Safety Protocol may be applied to SAE J1939 PGs (messages) with the following constraints.

4.4.1 Applicable SAE J1939 Messages

The SAE J1939 Functional Safety Protocol may be used with an SAE J1939 PG that meets both the data length and transmission rate constraints specified in [Table 2](#).

Table 2 - Constraints for SAE J1939 PG applicable with SAE J1939 Functional Safety Communications Protocol

Attribute	Constraint/Requirement
PG Data Length	• PG data length is defined as 8 bytes or less, i.e., PG never requires using SAE J1939 Transport Services.
PG Transmission Rate	• PG is defined with a fixed transmission rate, e.g., 100 ms, OR • PG is defined as an on-event transmit behavior or a variable transmission rate, e.g., “every 100 ms and on change but no faster than 20 ms.” See 5.1.3.3.

4.4.2 Not Applicable SAE J1939 Message

The SAE J1939 Functional Safety Protocol shall not be used with an SAE J1939 PG that meets any of the data length or transmission rate constraints specified in [Table 3](#).

Table 3 - Constraints for SAE J1939 PG not applicable with SAE J1939 Functional Safety Communications Protocol

Attribute	Constraint/Requirement
PG Data Length	• PG data length is defined as fixed or variable length that is able to exceed 8 bytes, i.e., PG can require or always requires using SAE J1939 Transport Services.
PG Transmission Rate	• PG is defined with an on-request transmission rate, such “on request,” “as needed,” “as required,” “as requested,” or “when needed.”

5. BEHAVIORAL REQUIREMENTS

The SAE J1939 Functional Safety Communication Protocol involves pairing an additional message, known as a Safety Header Message (SHM), together with each transmitted instance of a critical data message, known as the Safety Data Message (SDM). The producer periodically constructs each SDM and its SHM and then transmits the SHM and SDM within a certain time of one another and in a specific order relative to one another. The consumer verifies the SHM and SDM are received in order and within appropriate timing constraints, verifies the SDM instance using the SHM data, and checks for duplicated or missed SDM instances using the SHM sequence number. If a received SDG fails one or more of these validations, then a communication error for the SDG shall be reported to the consumer safety application. The consumer safety application is responsible for appropriate reaction to errors and the handling of restarting communication in a manner consistent with the safety or performance level of the application.

5.1 General Requirements

The requirements presented in this section apply to both the producer and the consumer. The requirements are described as they apply to a single Safety Data Group (SDG) within a single Safety Data Group Series. These requirements shall be performed independently for each Safety Data Group and Safety Data Group Series. Additional requirements for the complete system of network messages are discussed in [Section 7](#).

5.1.1 Safety Data Group Operations

Implementation of portions of the SAE J1939 Functional Safety Communications Protocol must be done in the safety application layers of the producer or consumer application as specified in [Figure 2](#). This requirement allows the communication link to be a black channel (see [A.1.2.1](#)), which is a communication channel containing components that are not designed or validated according to applicable functional safety standards. The black channel approach requires that all safety measures relied upon in the quantitative analysis must be part of the safety related application layer and that no credit shall be claimed for the CAN physical and data link layers.

- a. The construction of a Safety Data Group shall be performed within the Producing Safety Application. This is done to ensure the SHM and SDM contain valid and consistent information and that the safety application is functioning per design. The SHM CRC shall not be done at lower layers to avoid computing the SHM CRC for SDM data that has inadvertently changed when passed from the safety application to the lower layer.
- b. The validation of a Safety Data Group shall be performed within the consumer safety application. This is done since only the application knows how to validate the information contained within the messages. The Safety Data Group is not validated in the lower communication layers since this requires using information inside the messages.

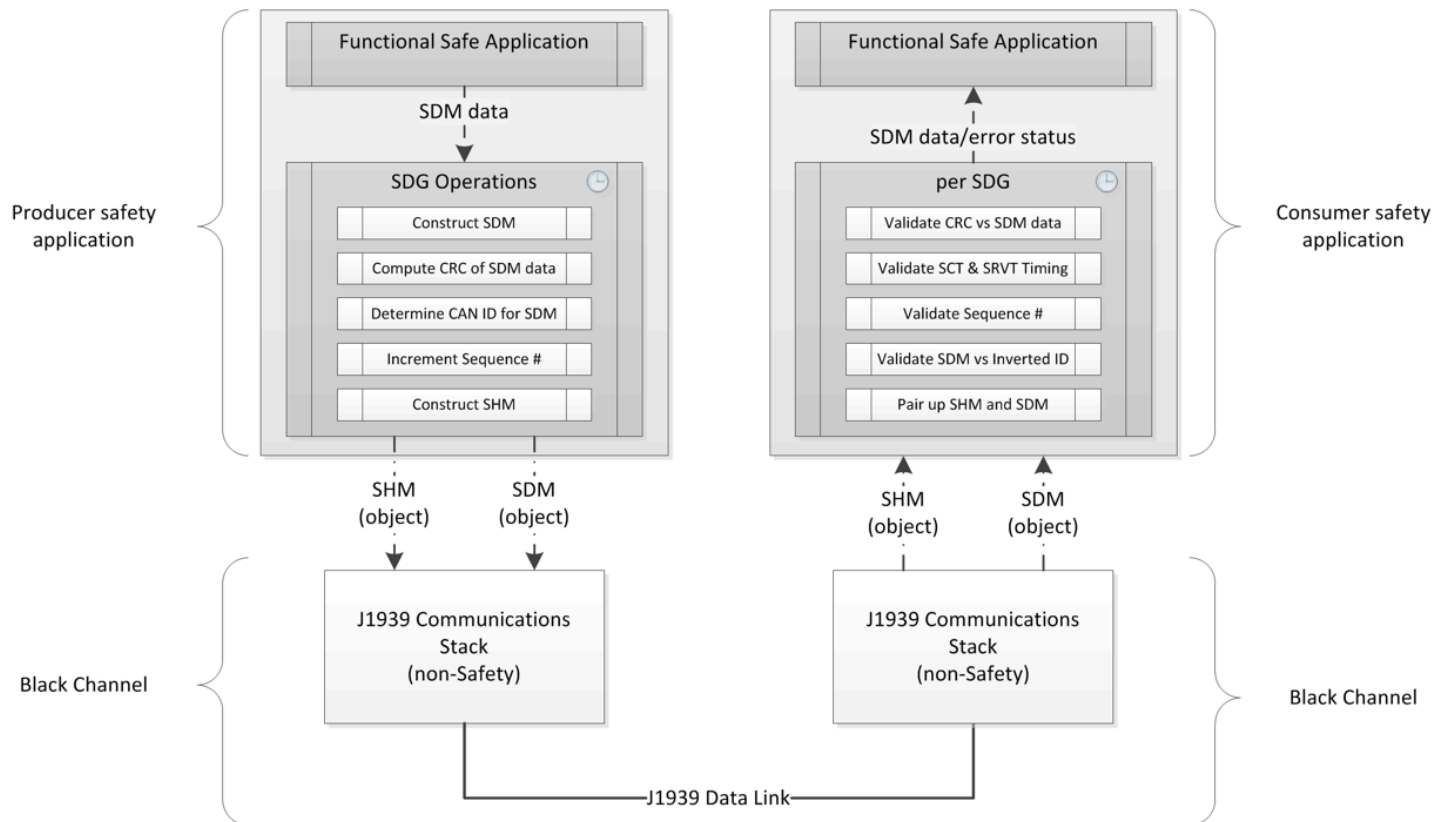


Figure 2 - Concept of operation

5.1.2 Safety Data Group and Safety Data Group Series

Safety Data Group (SDG) describes a specific SHM and SDM pair where the SDM is an SAE J1939 PG sent by a specific source address and, in the case of a PDU1 type PG, addressed to a certain destination address.

A Safety Data Group Series describes the sequence of periodic SDGs where every SDM consists of the same SAE J1939 PG sent by the same source address and, in the case of a PDU1 type PG, addressed to the same destination address.

Multiple Safety Data Group Series may exist on the network at the same time, for example:

- Multiple producers may send SDG Series to specific DAs or globally.
- One producer may transmit multiple SDG Series containing different PGs to specific DAs or globally.
- One producer, in the case of PDU1 type PG, may transmit the same PG to multiple DAs.

In each case, the combination of SA, DA, and embedded PG allows the consumer to properly match the paired messages for each SDG series.

5.1.3 SDG Timing Requirements

SAE J1939 Functional Safety Protocol uses time expectation as the measure for unacceptable delay communication errors. Timing measures are used with the timing between consecutive SDMs and with the timing between the SHM and SDM of an SDG instance.

5.1.3.1 Safety Cycle Time (SCT)

SCT is the period of time that transpires between reception of successive SDM instances of the same Safety Data Group Series. The actual SCT interval for the received SDM of an SDG shall be within the maximum SCT for that SDG. The maximum SCT defines the maximum time allowed to transpire between the reception of consecutive instances of SDMs of a valid SDG sequence. The failure to receive the subsequent instance of an SDM within the maximum SCT is basis for a communications incident for that SDG sequence. The maximum SCT requirement is shown in [Table 4](#). The maximum SCT for an SDG shall be based upon the timing basis (see [5.1.3.3](#)) for the SAE J1939 PG of the SDM.

Table 4 - Maximum SCT requirement

Timing Basis for SCT	Maximum SCT
Less than or equal to 200 ms	150% of the timing basis
Greater than 200 ms	Timing basis plus 100 ms

5.1.3.2 Safety-Relevant Validation Time (SRVT)

The SRVT is the time transpired between SHM reception and corresponding SDM reception of the same Safety Data Group instance. The time transpired between the received SHM and the received SDM shall be within the maximum SRVT for that SDG. The maximum SRVT specifies the maximum time allowed to transpire between the SHM reception and the SDM reception of a valid SDG instance. The failure to receive the SHM and the SDM within the maximum SRVT is basis for a communications incident for that SDG sequence. A maximum SRVT requirement example is shown in [Table 5](#). The maximum SRVT for an SDG is based upon the timing bases (see [5.1.3.3](#)) for the SAE J1939 PG of the SDM.

Table 5 - Maximum SRVT requirement

Timing Basis for SRVT	Maximum SRVT
Less than or equal to 200 ms	50% of the timing basis
Greater than 200 ms	100 ms

5.1.3.3 Timing Bases for SCT and SRVT

The timing bases for the SCT and SRVT intervals for an SDG are derived from the SAE J1939-defined Transmission Rate for the SAE J1939 PG of the SDM. This section describes how the timing bases and maximum SCT and SRVT values are determined for SAE J1939 PG. The bases for the maximum SCT and maximum SRVT depends upon the characterization of the SAE J1939 PG as a "Fixed Transmission Rate PG" or a "Variable Transmission Rate PG."

5.1.3.3.1 Fixed Transmission Rate PG Timing Basis

A fixed transmission rate PG is an SAE J1939 PG, which is periodically transmitted at a fixed interval, according to its SAE J1939 transmission rate. It is characterized as having an SAE J1939 transmission rate specified with a single periodic interval, for example, 100 ms

For a fixed transmission rate PG, the timing bases for both SCT and SRVT intervals shall be the period interval specified as the SAE J1939 transmission rate property of the SAE J1939 PG. For example, for a PG with an SAE J1939-defined transmission rate of "100 ms," the timing bases for both SCT and SRVT shall be "100 ms." Therefore, the maximum SCT is 150 ms and the maximum SRVT is 50 ms.

5.1.3.3.2 Variable Transmission Rate PG Timing Basis

A variable transmission rate PG is an SAE J1939 PG, which is periodically transmitted, but with the possibility of varying intervals between any two consecutive instances. It is characterized as having an SAE J1939 transmission rate with event-driven transmit behavior or a variable transmit period, such as “every 100 ms and on change but no faster than 20 ms.”

For a variable transmission rate PG, the timing bases for SCT and SRVT shall be the shortest period interval specified in the SAE J1939 transmission rate property. For example, for a PG with an SAE J1939-defined transmission rate of “every 100 ms and on change but no faster than 20 ms,” the timing basis for SCT would be 20 ms and the timing basis for SRVT would be 20 ms.

In applications where bus loading is a concern, the SCT and SRVT timing bases may be the longer period interval (i.e., 100 ms in the above example), but only if the system integrator confirms that no consumers of the protected message will trigger faults due to use of the longer SCT and SRVT timing bases.

5.1.3.3.3 Actual Update Rates

In either case of fixed or variable transmission rate PGs, the actual update rates of the deployed network shall be used by the consumer application software to detect timing violations. It is also applicable for the analysis of safety measures (see [Appendix A](#) and [Appendix B](#)).

5.1.4 Sequence Number

SAE J1939 Functional Safety Protocol uses sequence numbers as the measure for several communication errors, including repetition, incorrect sequence, loss, and insertion. Each SHM includes a sequence number that is managed independently for each Safety Data Group Series. It is the expectation of both producer and consumer that:

- a. The sequence number shall be maintained and incremented independently for each Safety Data Group Series.
- b. The sequence number shall increment by one for each new SDG instance.
- c. The sequence number shall roll over to zero on the next increment after 31 for 5-bit sequence number in SHM1 or after 16383 for 14-bit sequence number for the SHM2 version of the message.
- d. It is expected behavior that the sequence number shall not be incremented when the SHM CAN frame is being retransmitted as part of the CAN protocol, such as after a CAN error frame incident.

5.1.5 CRC

SAE J1939 Functional Safety Communication Protocol uses data integrity 32-bit CRC as the measure for message corruption communication errors. Each SHM1 and SHM2 includes a 32-bit CRC.

For SDGs using SHM1, the CRC is computed over the 8-byte data field of the SDM of the SDG. See [6.6.8](#).

For SHM2, the CRC uses a different polynomial and is computed over 13 bytes: the 8-byte data field of the SDM plus the first 4 bytes of the SHM2 of the SDG plus the 1-byte source address of the producer. See [6.3.6](#).

The CRC is transmitted in the SHM message and provides the means for a consumer to detect bit errors and incorrectly paired SHM and SDM within the Safety Data Group Series.

- a. The 32-bit CRC shall be computed using the algorithm specified in [6.3.6](#) for SHM2 and [6.6.8](#) for SHM1.
- b. The producer shall properly set all unused and undefined bits of the SDM data field to “not available” value prior to computing the CRC, as specified by SAE J1939-71.
- c. The SDM data field data shall be processed through the algorithm starting with byte 1 and continuing with each successive byte in the data field to the last data field byte. Byte 1 is the data field byte closest to the CAN Frame header. For SHM2, the additional 4 bytes of the SHM2 starting at byte 1 are included in the computation as well as the 1-byte source address of the producer.

5.1.6 SHM and SDM Sequence within an SDG

The sequential order of SHM and SDM reception in an SDG shall be enforced. The consumer shall require the SHM to be received before the SDM to which it will be paired. The maximum SRVT time constraint limits the duration between the SHM and the SDM that follows.

5.2 Producer Requirements

The requirements presented in this section apply specifically to the producer. The producer is responsible for constructing the SDM and SHM for each SDG instance and transmitting those SDM and SHM in the proper sequence and within the necessary timing constraints. The high-level behavioral model for the producer safety application for each required SDG is illustrated in the activity diagram in [Figure 4](#). The diagram is only a conceptual model for illustrating the operations and behaviors for producer safety application.