SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-76	NOV2018
Issued 2018-11	

SAE J1939 Functional Safety Communications Protocol

RATIONALE

This is the first publication of this application layer protocol for SAE J1939. It addresses the need for high-reliability communications over an SAE J1939 network for vehicle features considered to be functional safety-related.

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 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.

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

SAE values your input. To provide feedback on this Technical Report, please visit
http://standards.sae.org/J1939-76/201811

TABLE OF CONTENTS

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 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 J1939-21 Data Link Layer

2.1.2 IEC Publications

Available from IEC Central Office, 3 rue de Varembe, P.O. Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 02 11, www.iec.ch.

IEC 61508-2:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

IEC 61784-3:2016 Functional Safety Fieldbuses - General Rules and Profile Definitions

IEC 62280 Railway Applications - Communications, Signalling and Processing Systems - Safety-Related Communication in Transmission 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 ISO Publications

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

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

ISO 25119-1 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

2.2.2 Miscellaneous

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 CONSUMING SAFETY APPLICATION

The ECU safety application end-point that receives the standard SAE J1939 PGN message (Safety Data Message) and the corresponding Safety Header Message, and confirms functional safety protocol validations prior to using or applying the Safety Data Message data.

3.1.1.3 CONSUMER

See "Consuming Safety Application."

3.1.1.4 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.”

3.1.1.5 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.”

3.1.1.6 PRODUCING SAFETY APPLICATION

The ECU safety application end-point that sends the standard SAE J1939 PGN and the corresponding Safety Header Message.

3.1.1.7 PRODUCER

See "Producing Safety Application."

3.1.1.8 RECEIVER

See "Consuming Safety Application."

3.1.1.9 TRANSMITTER

See "Producing Safety Application."

3.1.1.10 SAFETY-RELATED SYSTEM

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

3.1.1.11 COMMUNICATION CHANNEL

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

3.1.1.12 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 consuming safety application to detect data and communication errors.

3.1.1.13 SAFETY DATA MESSAGE (SDM)

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

3.1.1.14 SAFETY DATA GROUP (SDG)

A specific instance of a pair of SAE J1939 messages consisting of the SDM and its corresponding SHM.

3.1.1.15 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.

3.1.1.16 SAFETY-RELEVANT VALIDATION TIME (SRVT)

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

3.1.1.17 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 transmit rate.

3.1.1.18 BLACK CHANNEL

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

3.1.1.19 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 Terms and Definitions

3.1.2.1 MESSAGE CORRUPTION

Messages may 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 may 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
PFH	Probability for Failure per Hour
PG	Parameter Group
PGN	Parameter Group Number
PL	Performance Level
SCT	Safety Cycle Time
SDG	Safety Data Group
SDM	Safety Data Message
SHM	Safety Header Message
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 safety or performance levels when using an SAE J1939 communication network. Independent evaluation[1] 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 for analysis.

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}. Based upon a probability of failure per hour approach, this protocol may 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 the specified cross checking reduces the possibility of undetected message corruption and addressing errors and provides the ability to detect insertion, loss, unintended repetition, unacceptable delay, masquerade, and incorrect sequence.

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 the CAN ID of the paired SDM, the CRC of the SDM data, and relative sequence of the paired SDM. 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 CAN ID of the paired SDM, the CRC of the SDM data, and relative sequence of the paired SDM. The Producer repeats this cycle each successive instance of the SDM.

The Consumer is responsible for pairing up the SHM and SDM 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, then a communication error for the SDG shall be reported to the Consumer safety application.

---

[1] Refer to TÜV letter “Evaluation of SAE J1939 Functional Safety Communication Protocol” dated 2 August 2018.

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.

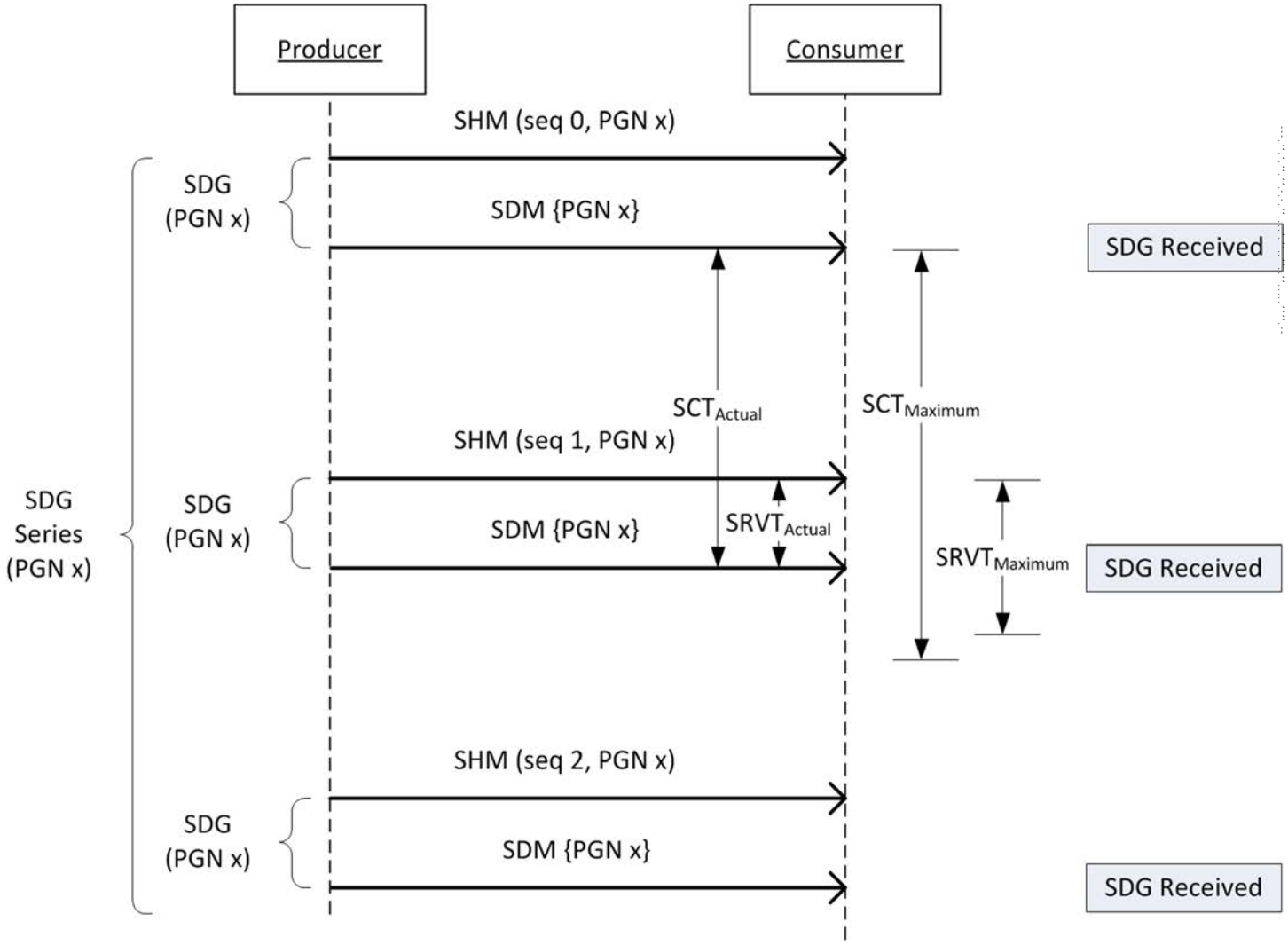


Figure 1 - Safety protocol overview

4.2.1 Communication Error Coverage

Table 1 describes 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	Diagnostic Measure for Detection
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 critical data to determine when the SDM data may be used for safety critical 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 critical data to determine when the SDM data may be used for safety critical 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 critical data to determine when the SDM data may be used for safety critical 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 critical data to determine when the SDM data may be used for safety critical 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 critical data to determine when the SDM data may be used for safety critical purposes.
Insertion	**Sequence number** and **redundancy with cross check** are the measures for detecting insertion errors. The safety application layer uses the sequence number in every SHM to detect insertion errors. 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 29-bit identifier of the SDG and the inverted copy from the matched SHM 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 critical data to determine when the SDM data may be used for safety critical purposes.
Masquerade	**Different data integrity assurance** is the measure for detecting masquerade errors. 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 may be used for safety critical purposes.
Addressing	**Connection authentication** is the measure for detecting addressing errors. The safety application layer uses the 29-bit identifier of the SDM and the inverted copy from the matched SHM of the same SDG to verify the SDM addressing matches the SHM and to 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 critical data to determine when the SDM data may be used for safety critical 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 described 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 is not applicable for use with every SAE J1939 PG (message). The constraints and requirements for use of this protocol for an SAE J1939 PG are presented.

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 described in Table 2.

Table 2 - Constraints for SAE J1939 PG applicable with functional safety 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 periodic transmit period, e.g., 100 ms. **OR** • PG is defined with an on-event transmit behavior or a variable transmit period, e.g., "every 100 ms and on change but no faster than 20 ms." The shortest defined period, e.g., 20 ms, is used as the fixed periodic rate for that PG with the Functional Safety Protocol.

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 described in Table 3.

Table 3 - Constraints for SAE J1939 PG not applicable with functional safety 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 may 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 consuming 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 Functional Safety Protocol must be done in the safety application layers of the producer or consumer application as shown in Figure 2. This requirement allows the communication link to be a black channel (see 0), 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 critical 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 Consuming 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.

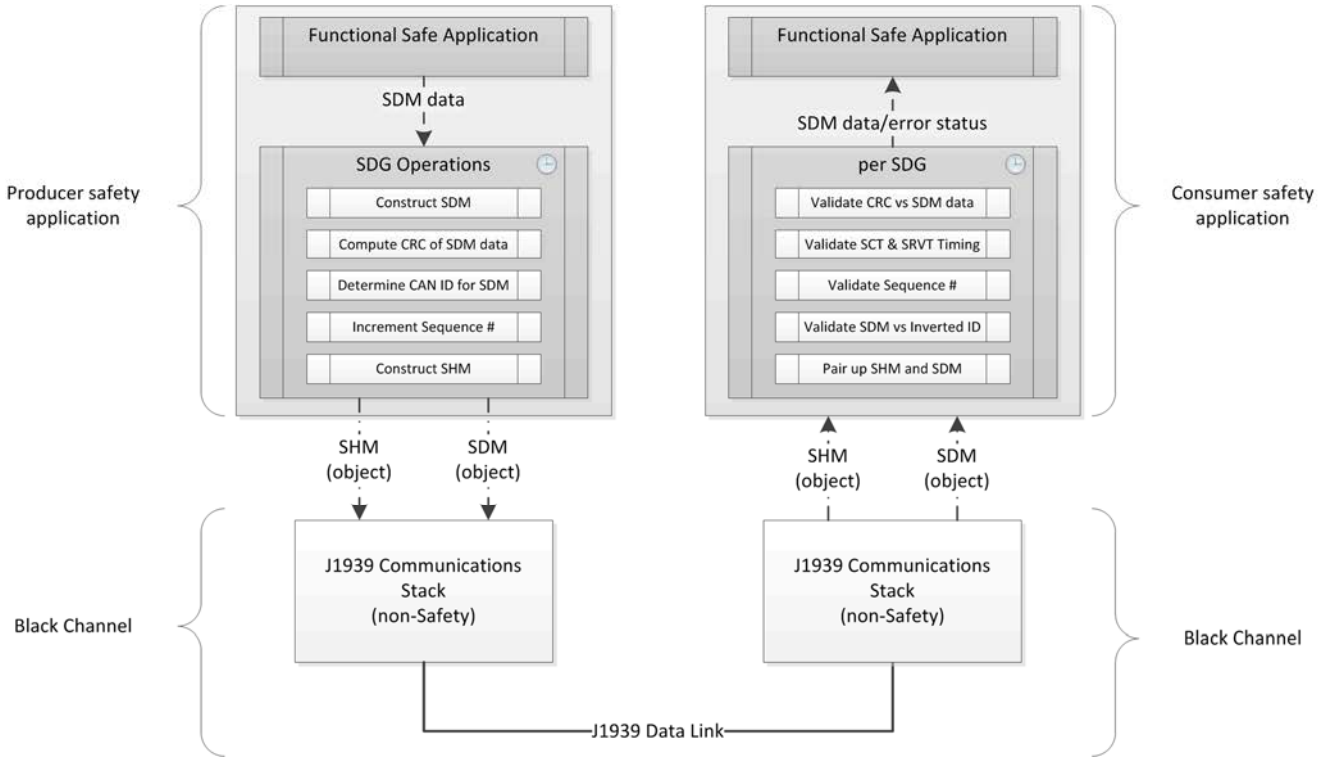


Figure 2 - Concept of operation

5.1.2 Safety Data Group and Safety Data Group Series

Safety Data Group (SDG) describes a specific SHM and SDM where the SDM is specific 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.

5.1.3 SDG Timing Requirements

SAE J1939 Functional Safety uses “time expectation” as the measure for unacceptable delay communication errors. Timing measures are used with the timing between consecutive SDMs (SCT interval) and with the timing between the SHM and SDM (SRVT interval) of an SDG instance. The timing basis 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 basis and maximum SCT and SRVT values are determined for SAE J1939 PG. The basis 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."

5.1.3.1 SDG Timing Basis

The SDG Timing Basis describes the time interval used as the basis for the SCT and SRVT for an SDG. The SDG Timing Basis is derived from the SAE J1939-defined Transmission Rate for the SAE J1939 PG of the SDM.

5.1.3.1.1 Fixed Transmission Rate PG Timing Basis

Fixed Transmission Rate PG describes 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.”

For Fixed Transmission Rate PG, the SDG Timing Basis shall be the period interval specified as the SAE J1939 Transmission Rate property of the PG. For example, the SDG Timing Basis would be “100 ms” for a PG with an SAE J1939-defined Transmission Rate of “100 ms.”

5.1.3.1.2 Variable Transmission Rate PG Timing Basis

Variable Transmission Rate PG describes an SAE J1939 PG transmitted continually, but with the possibility of varying intervals between any two consecutive 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.”

For Variable Transmission Rate PG, the SDG Timing Basis shall be the shortest period interval specified in the SAE J1939 Transmission Rate property of the PG. For example, the SDG Timing Basis would be “20 ms” for a PG with an SAE J1939-defined Transmission Rate of “Every 100 ms and on change but no faster than 20 ms.”

5.1.3.1.3 Actual Update Rates

In either case of fixed or variable messages involved in the functional safety communication, the actual update rates of the deployed network shall be used in both the analysis and the detection of timing violations.

5.1.3.2 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 a valid 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 SDG Timing Basis (see 5.1.3.1) for the SAE J1939 PG of the SDM.

Table 4 - Maximum SCT requirement

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

5.1.3.3 Safety-Relevant Validation Time (SRVT)

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 defines 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 SDM within the maximum SRVT is basis for a communications incident for that SDG sequence. The maximum SRVT requirement is shown in Table 5. The maximum SRVT for an SDG shall be based upon the SDG Timing Basis (see 5.1.3.1) for the SAE J1939 PG of the SDM.

Table 5 - Maximum SRVT requirement

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

5.1.4 Sequence Number

SAE J1939 Functional Safety 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.

a. Sequence Number shall be maintained and incremented independently for each Safety Data Group series.

b. Sequence Number shall increment by one for each new SDG instance.

c. Sequence Number shall roll over to zero on the next increment after 31.

NOTE: 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 SDM Data CRC

SAE J1939 Functional Safety uses “data integrity (CRC)” as the measure for message corruption communication errors. Each SHM includes a CRC of the data field of the SDM of the SDG. The CRC 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 on the SDM data field using the algorithm specified in 6.2.2.

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.

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 (Transmitter) 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 3. The diagram is only a conceptual model for illustrating the operations and behaviors for Producer safety application.

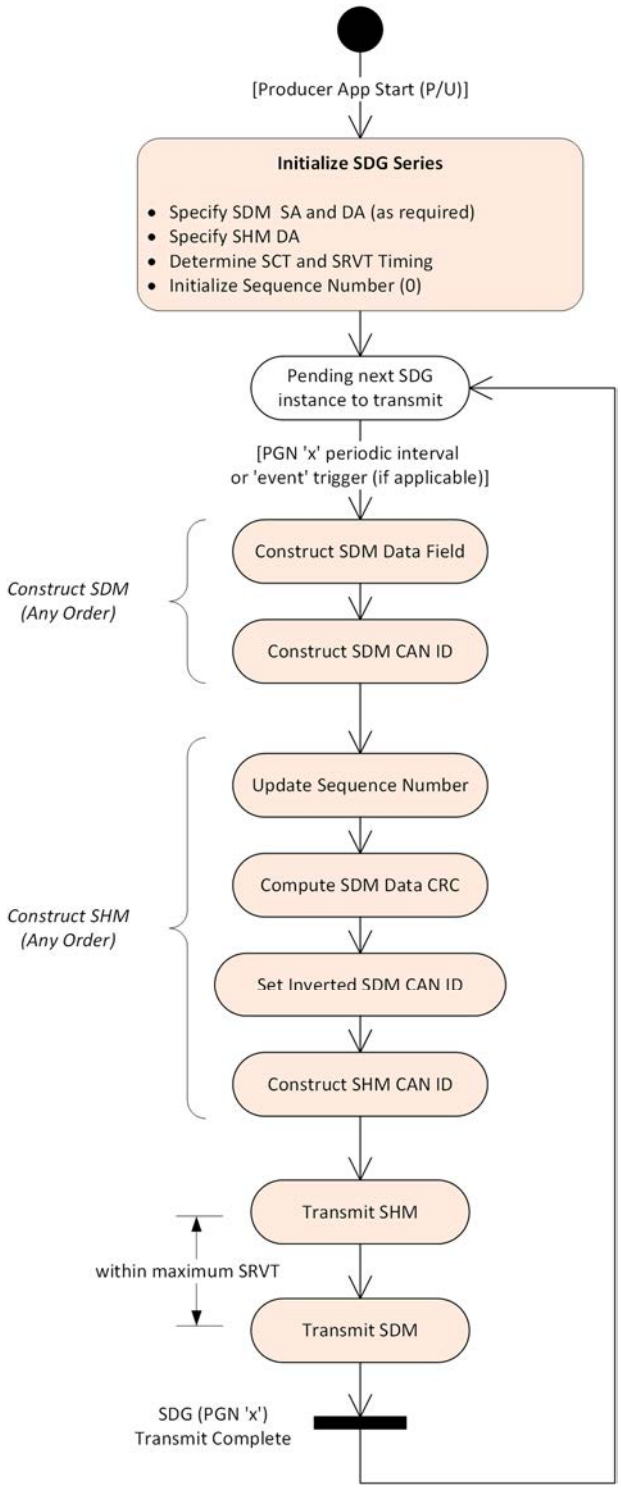


Figure 3 - Producer SDG behavioral model

5.2.1 General Requirements

a. The SDM data field for an SDG instance shall be fully constructed within the Producer Safety Application.

b. The SHM data field for an SDG instance shall be fully constructed within the Producer Safety Application.

c. Producer shall periodically transmit an SDG within the maximum SCT for the SDM, as specified in 5.1.3.2.

5.2.2 Construct the SDM

The Producing Safety Application must fully construct the SDM data field and SDM CAN ID in order to construct the corresponding SHM. The SDM data field must be constructed in order to compute the SDM Data CRC value reported in the SHM. The SAE J1939 PG, Source Address and, conditionally, the Destination Address values of the SDM CAN ID must be fully specified to generate the Inverted CAN ID value reported in the SHM.

5.2.2.1 SDM Priority

The Priority value in the SAE J1939 message header for the SDM and SHM can affect the Producer's ability to send the SHM and SDM within the timing requirements and maintain the required transmit order of the SHM and SDM within an SDG instance.

The Producer shall consider the following SDM Priority value recommendations for overall performance:

- The SAE J1939 Default Priority defined for the PG shall be used as the SDM Priority unless the message priority value has been intentionally adjusted, such as to tune for network performance.

- A Priority value of 001b or 000b is recommended for Variable Transmission Rate PGs if the SDG timing basis is less than 50 ms. See 5.1.3.1.2.

5.2.3 Construct the SHM

The Producing Safety Application must fully construct the SHM data field for the corresponding SDM. The SHM data field contains the Sequence Number, SDM Data CRC, and the inverted 29-bit identifier of the SDM excluding the three Priority bits. The SHM data field structure and field bit positions are specified in 6.1. The contents for each of the SHM data fields shall be set according to the requirements specified in 5.2.4, 5.2.5, and 5.2.6.

5.2.4 Sequence Number

The “Sequence Number” for the SHM shall be set according to the requirements in 5.1.4 and the requirements specified below.

a. Each Safety Data Group series shall have its own sequence associated with it.

b. Upon startup, the Sequence Number shall be 0000b for the SHM of the first SDG of each combination.

5.2.5 SDM Data CRC

The CRC shall be computed for the SDM data field as specified in 5.1.5.

5.2.6 Inverted 29-bit Identifier

The Producer shall construct the “Inverted 29-bit Identifier” data for the SHM data field by performing a bitwise inversion (i.e., 0 to 1, or 1 to 0) of the 29-bit CAN ID of the SDM, excluding the three Priority bits. The Producer Safety Application must know the SAE J1939 PG, Source Address, and, conditionally, the Destination Address values to be used for the 29-bit CAN Id of the SDM.

5.2.7 SHM Priority and Destination Address

5.2.7.1 SHM Priority

The Priority value in the SAE J1939 message header for the SDM and SHM can affect the Producer's ability to send the SHM and SDM within the timing requirements and maintain the required transmit order of the SHM and SDM within an SDG instance.

The Producer shall set the Priority of the SHM according to the following requirements.

a. Priority shall be a value with the same or higher priority as the SDM Priority (see 5.2.2). A higher priority value has a lower numerical value.

5.2.7.2 SHM Destination Address

The Destination Address in the SAE J1939 message header of the SHM shall be set according to the following requirements.

a. If the SDM is a PDU1 PG (destination specific), then the SHM Destination Address shall be the same address used as the SDM Destination Address.

b. If the SDM is a PDU2 PG (broadcast), then the SHM Destination Address shall be SAE J1939 Global Address.

5.2.8 Transmit the SHM and SDM

This section specifies the transmit requirements that shall be directly controlled by the Producer safety application. The actual transmission of the SHM and SDM messages onto the data link is not required to be performed within the Producer safety application. The Producer does have behavior requirements for its role in the transmission of the SHM and SDM messages. Failure to transmit them according to these requirements will result in detected communication errors by Consumers.

a. The SHM shall be transmitted before the SDM, as specified in 5.1.6.

b. The SDM shall be transmitted no later than the maximum SRVT after transmitting the SHM.

c. There is no minimum time requirement between the SHM and SDM messages.

d. The transmission of the SHM and SDM of an SDG shall commence only after transmission of the SHM and SDM of the previous SDG has been completed. The Producer shall not transmit any part of a subsequent SDG in between the SHM and SDM of the previous SDG.

5.3 Consumer (Receiver) Requirements

This section defines the behavioral requirements of the Consumer safety application to validate the SHM and SDM of an SDG and either provide the validated SDM data for safety application use or withhold the SDM data from the safety application together with an indication of a detected communication incident.

The high-level behavioral model for the Consumer 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 Consumer safety application. The Consumer processing requires identifying and pairing the SHM and SDM into SDGs, validating the CAN ID between the SHM and SDM, validating the SCT and SRVT timing, validating the SDM data to the CRC, and validating the SHM sequencing. 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 resulting Consumer safety application response and system response to each communications incident is application design-specific and cannot be specified as part of this standard.

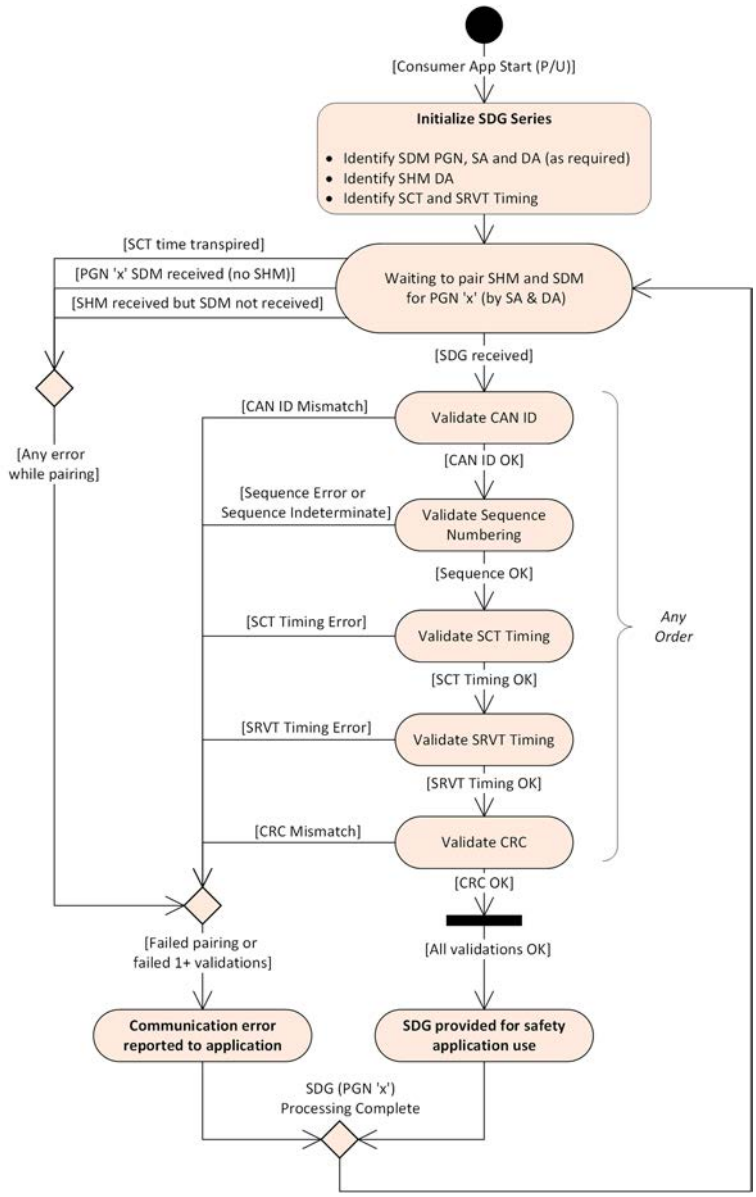


Figure 4 - Consumer SDG behavioral model

5.3.1 General Requirements

a. A received SDG shall only be provided to the safety application for use if the SDG is positively validated for CAN ID, SCT Timing, SRVT timing, CRC, and Sequence Numbering.

b. 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.

c. These requirements apply to each individual safety data group (SDG). An individual SDG is defined as being a specific SHM and SDM pair from a specific Producer (source address).

d. If the Consumer is designed to receive the same SDM from multiple different Producers, then these requirements are applied separately and independently to each SDG from each Producer.

e. The Consumer must have the ability to determine the timing and sequence of reception of the SHM and SDM of the SDG. It may be necessary to timestamp each received SHM and SDM to validate SCT interval, SRVT interval, and the receive order of the SHM and SDM of an SDG.

5.3.2 SHM Identification

The following requirements shall be used to identify an SHM for the SDG series. If an SHM fails one or more of these requirements, then the SHM shall not be regarded as an SHM for the SDG series.

a. The SHM “Inverted 29-bit Identifier” data (excluding Priority bits) shall identify the PG, Source Address and, optionally, Destination Address values required for the SDM of this SDG series.

b. The SHM Source Address of the SHM shall be the Source Address of the Producer associated with this SDG series.

c. The SHM Destination Address of the SHM shall be the appropriate Destination Address for this SDG, as specified in 5.2.7.2.

5.3.3 SDM Identification

The following requirements shall be used to identify an SDM for the SDG series:

a. The SDM for each SDG shall be the same PG message sent by the same Source Address and, in the case of a PDU1 type PG, addressed to the same Destination Address.

b. If the PG of the SDM is a PDU1 type PG, then any instance of PG sent by the same Source Address but addressed to a different Destination Address shall not be regarded as an SDM for the SDG series.

5.3.4 SHM and SDM Pairing

The SHM and SDM for an SDG are paired according to the following requirements:

a. The paired SHM shall be the most recent received SHM for this SDG, per 5.3.2.

b. The paired SDM shall be the first SDM (see 5.3.3) that is received after the SHM and received within the Functional Safety maximum timing interval constraints.

c. If an SDM is received and there is no received SHM pending to be paired, then a communications error (due to invalid SHM and SDM order) for the SDG shall be reported to the Consumer safety application.

5.3.5 CAN ID Validation

CAN ID Validation shall be performed on the paired SHM and SDM of the SDG, per 5.3.4. SAE J1939 Functional Safety Communications Protocol uses the CAN ID of the SDM and the “Inverted 29-bit Identifier” data in the SHM to validate the pairing of SHM and SDM of the SDG. The three Priority bits of the CAN ID are excluded.

a. The CAN ID of the SDM shall exactly match the CAN ID specified by the “Inverted 29-bit Identifier” in the SHM.

b. If the CAN ID of the SDM does not exactly match the CAN ID specified by the “Inverted 29-bit Identifier,” then a communication error for the SDG shall be reported to the Consumer safety application.

5.3.6 SCT Validation

The Consumer shall validate an SDM is periodically received within the maximum SCT constraint, as specified in 5.1.3.2. If an SCT violation is detected, then a communication error for the SDG shall be reported to the Consumer safety application.

a. If the time transpired between the SCT timing reference and the SDM is less than or equal to the maximum SCT, then the SDG shall be declared as validated with regards to SCT timing.

b. If the time transpired between the SCT timing reference and the SDM is greater than the maximum SCT, then an SCT timing violation shall be declared for the SDG and a communication error for the SDG shall be reported to the Consumer safety application.

c. A received SDM shall be used as the SCT timing reference for the next SDM.

d. Upon startup, the initial SCT timing reference shall begin at the time when the Consumer application is able to receive SAE J1939 messages.

e. If an SHM or an SDM is not received within an SCT interval, then the SCT timing reference for the next SDM shall begin at the time the maximum SCT interval transpired for the missed SDM.

5.3.7 SRVT Validation

The Consumer shall validate the time between the received SHM and SDM are within the maximum SRVT constraint, as specified in 5.1.3.3. If an SRVT violation is detected, then a communication error for the SDG shall be reported to the Consumer safety application.

a. If the time transpired between receiving the SHM and receiving the SDM is less than or equal to the maximum SRVT, then the SDG shall be declared as validated with regards to SRVT timing.

b. If the time transpired between receiving the SHM and receiving the SDM is greater than the maximum SRVT, then an SRVT timing violation shall be declared for the SDG and a communication error for the SDG shall be reported to the Consumer safety application.

c. If the time transpired between receiving the SHM and receiving the SDM indicates the SDM was received before the SHM, then an SRVT timing violation shall be declared for the SDG and a communication error for the SDG shall be reported to the Consumer safety application.

5.3.8 CRC Validation

The Consumer shall validate the SDM Data CRC to the data field of the SDM of the SDG according to the following requirements.

a. The CRC shall be computed for the data field of the paired SDM as specified in 5.1.5.

b. If the computed CRC exactly matches the “SDM Data CRC” value reported in the SHM, then the SDG shall be declared as validated with regards to CRC.

c. If the computed CRC does not exactly match the “SDM Data CRC” value reported in the SHM, then a CRC violation shall be declared for the SDG and a communication error for the SDG shall be reported to the Consumer safety application.

5.3.9 Sequence Number Validation

The Consumer shall validate the Sequence Number of the SHM in the SDG series according to the following requirements. Sequence Number validation is used to confirm SDGs are received in the correct order and to detect unacceptable sequence issues, such as skipped SDGs, repeated SDGs, multiple skips, and repeats. Sequence Number validation is illustrated in Figure 5. See 5.1.4 for requirements on incrementing the Sequence Number.

a. Sequence Number validation shall only be performed on an SHM that is paired with an SDM.

b. The SDG Sequence Number shall be declared not valid if the Consumer has not received at least two SDGs.

c. Sequence Number shall be declared valid if the current Sequence Number equals the last received Sequence Number incremented by one.

d. The last received Sequence Number shall be the Sequence Number of the most recently received SDG, regardless if the Sequence Number of that SDG was declared valid or not valid.

Normal (start up)

Last Sequence Number	unknown	0	1	2	3	4	5	6	7	8	9
Last Sequence Number + 1	unknown	1	2	3	4	5	6	7	8	9	10
Received Sequence Number	0	1	2	3	4	5	6	7	8	9	10
Sequence Number Match?	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Sequence Number Validation	Not Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid

Normal (roll-over)

Last Sequence Number	29	30	31	0	1	2	3	4	5	6	7
Last Sequence Number + 1	30	31	0	1	2	3	4	5	6	7	8
Received Sequence Number	30	31	0	1	2	3	4	5	6	7	8
Sequence Number Match?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Sequence Number Validation	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid

SDG Missed

Last Sequence Number	14	15	16	16	18	19	20	20	20	23	24
Last Sequence Number + 1	15	16	17	17	19	20	21	21	21	24	25
Received Sequence Number	15	16	not rcvd	18	19	20	not rcvd	not rcvd	23	24	25
Sequence Number Match?	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
Sequence Number Validation	Valid	Valid	Not Valid	Not Valid	Valid	Valid	Not Valid	Not Valid	Not Valid	Valid	Valid

SDG Duplicate

Last Sequence Number	14	15	16	17	17	18	19	20	21	22	23
Last Sequence Number + 1	15	16	17	18	18	19	20	21	22	23	24
Received Sequence Number	15	16	17	17	18	19	20	21	22	23	24
Sequence Number Match?	TRUE	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Sequence Number Validation	Valid	Valid	Valid	Not Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid

SDG Out of Order

Last Sequence Number	14	15	16	18	17	19	20	21	22	23	24
Last Sequence Number + 1	15	16	17	19	18	20	21	22	23	24	25
Received Sequence Number	15	16	18	17	19	20	21	22	23	24	25
Sequence Number Match?	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Sequence Number Validation	Valid	Valid	Not Valid	Not Valid	Not Valid	Valid	Valid	Valid	Valid	Valid	Valid

Figure 5 - Sequence number validation examples

6. MESSAGE STRUCTURE AND REQUIREMENTS

This section presents the technical requirements on the structure of the SHM data field and the requirements for each of the data field parameters. The basic SHM structure is illustrated in Figure 6. The SHM data field structure and field bit positions are specified in 6.1.

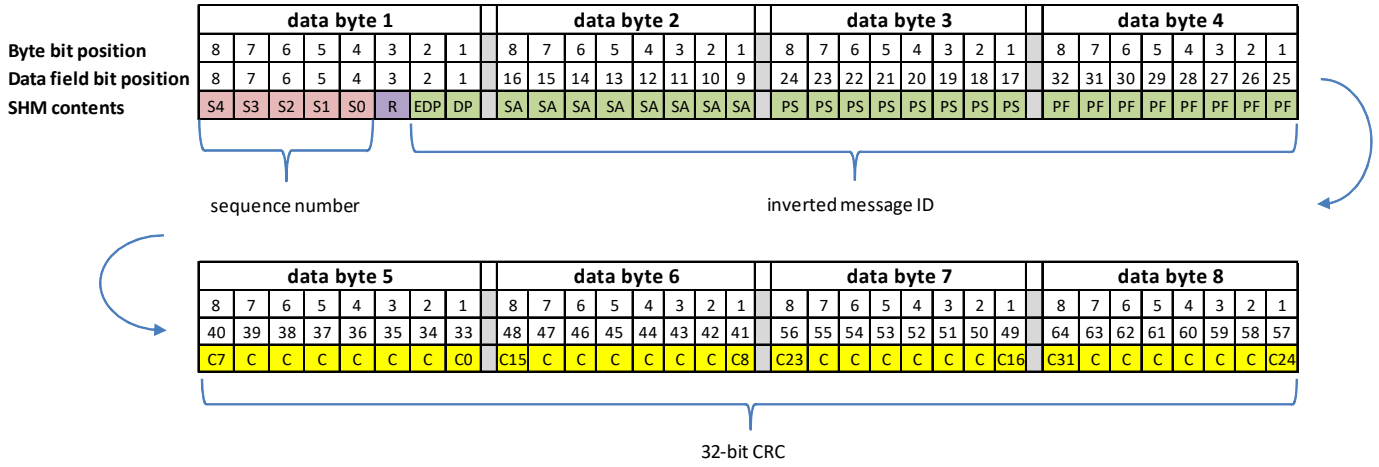


Figure 6 - SHM message structure

where:

Sx = SDG sequence number

R = reserved

EDP, DP, PS, PF = inverted SDM ID without priority

Cx = 32-bit CRC

6.1 Safety Header Message Definition

PGN 3584 Safety Header Message - SHM

Transmission Repetition Rate: As required
Data Length: 8 bytes
Extended Data Page: 0
Data Page: 0
PDU Format: 14
PDU Specific: DA Destination Address PGN Supporting Information:
Default Priority: See SHM Priority (5.2.7.1)
Parameter Group Number: 3584 (000E00h)

Start Position	*Length*	*Parameter Name*	
1.1	1 bit	Inverted SDM Data Page	See 6.2.6
1.2	1 bit	Inverted SDM Extended Data Page	See 6.2.7
1.3	1 bit	Reserved – set to 1	See 6.2.8
1.4	5 bits	SDG Sequence Number	See 6.2.1
2	1 byte	Inverted SDM Source Address	See 6.2.3
3	1 byte	Inverted SDM PS Value	See 6.2.4
4	1 byte	Inverted SDM PF Value	See 6.2.5
5-8	4 bytes	SDM Data CRC	See 6.2.2

6.2 Safety Header Message Parameter Definitions

6.2.1 Sequence Number (SPN 9382)

The Sequence Number is a 5-bit parameter (0 to 31). The sequence numbering shall be maintained separately for each Safety Data Group Series. The sequence number shall be incremented by one for each successive instance of that SDG, rolling over from the value 31 to the value 0. 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.

Data Length: 5 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 31 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.2 SDM Data CRC (SPN 9383)

The SDM Data CRC is the 32-bit CRC of the data field of the corresponding SDM. The CRC is defined as follows:

- Length: 32 bits
- Polynomial hex representation of divisor: 6938392Dh.
- This is most significant bit first representation of a hexadecimal number with 32 bits. The most significant bit represents the coefficient of x^{31} and the least significant bit represents the coefficient of x^0. The coefficient of x^{32} is omitted and understood to be one.
- Polynomial representation: $x^{32}+ x^{30}+ x^{29}+ x^{27}+ x^{24}+ x^{21}+ x^{20}+ x^{19}+ x^{13}+ x^{12}+ x^{11}+ x^8+ x^5+ x^3+ x^2+ x^0$
- Hamming distance: HD=10, up to 100 bits
- Initial value = FFFFFFFFh
- Final XOR value = 0
- Inputs not reflected
- Results not reflected

Data Length: 32 bits
Resolution: 1/bit, 0 offset
Data Range: 0 to 4294967295 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.2.1 CRC CALCULATION EXAMPLES

EXAMPLE A
CAN frame payload 8 bytes:
00h 01h 02h 03h 04h 05h 06h 07h
Calculated CRC = C550537Dh

EXAMPLE B
CAN frame payload 8 bytes:
12h 34h 56h 78h 9Ah BCh DEh F0h
Calculated CRC = D7713A27h

EXAMPLE C
CAN frame payload 8 bytes:
00h 00h 00h 00h 00h 00h 00h 00h
Calculated CRC = 76AC1AB7h

EXAMPLE D
CAN frame payload 8 bytes:
FFh FFh FFh FFh FFh FFh FFh FFh
Calculated CRC = FFD18D4Dh

6.2.3 Inverted SDM Source Address (SPN 9384)

This element represents the bit inversion (i.e., 0 to 1, or 1 to 0) of the Source Address (SA) of the SDM identifier associated with the current SHM. This element provides the ability to pair the SHM to the corresponding SDM.

Data Length: 8 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 255 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.4 Inverted SDM PS Value (SPN 9385)

This element represents the bit inversion (i.e., 0 to 1, or 1 to 0) of the PDU Specific (PS) of the SDM identifier associated with the current SHM. This element provides the ability to pair the SHM to the corresponding SDM.

Data Length: 8 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 255 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.5 Inverted SDM PF Value (SPN 9386)

This element represents the bit inversion (i.e., 0 to 1, or 1 to 0) of the PDU format (PF) of the SDM identifier associated with the current SHM. This element provides the ability to pair the SHM to the corresponding SDM.

Data Length: 8 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 255 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.6 Inverted SDM Data Page (SPN 9387)

This element represents the bit inversion (i.e., 0 to 1, or 1 to 0) of the Data Page (DP) of the SDM identifier associated with the current SHM. This element provides the ability to pair the SHM to the corresponding SDM.

Data Length: 1 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 1 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.7 Inverted SDM Extended Data Page (SPN 9388)

This element represents the bit inversion (i.e., 0 to 1, or 1 to 0) of the Extended Data Page (EDP) of the SDM identifier associated with the current SHM. This element provides the ability to pair the SHM to the corresponding SDM.

Data Length: 1 bit
Resolution: 1/bit, 0 offset
Data Range: 0 to 1 Operational Range: Same as data range
Type: Status
Supporting Information:
PGN reference: 3584

6.2.8 Reserved Bit

There is 1 bit in the data field that currently has no assigned meaning or value. A logical “1” shall transmitted for this bit.

7. SYSTEM DESIGN REQUIREMENTS

7.1 When to Use the SAE J1939-76 Functional Safety Communication Protocol

The method described in this document shall be applied to any SAE J1939 PG that is used as part of a functional safety channel in a system as determined by the system and safety design process. It shall be used when additional protection against undetected message errors is required by the system design.

7.2 When Not to Use the SAE J1939-76 Functional Safety Communication Protocol

- The Safety Header Message shall be used only when required for specific data messages. Overuse of this method will lead to increased network load.

7.3 Configuration of the SAE J1939-76 Functional Safety Communication Protocol

- This protocol does not include any services for telling a Controller Application, at run time, to enable or disable the transmission of Safety Header Messages.

- The System Designer is responsible for ensuring the Transmitter Controller Application for a particular Safety Data Message is properly configured to transmit the Safety Header Message and that any Receiver Controller Applications are configured to make use of this information.

7.4 Systems Constraints for Meeting Safety and Performance Levels

There is a limit to the number of safety relevant message pairs or SDGs per hour of network operation in order to meet the constraints of the mathematical analysis. The probability for failure per hour (PFH) must be calculated for each complete system design to insure it meets the limits for the SIL or PL that the system requires. Examples of this calculation are given in Appendix A.

8. NOTES

8.1 Revision Indicator

A change bar (l) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY THE SAE TRUCK AND BUS CONTROL AND COMMUNICATIONS COMMITTEE
OF THE SAE TRUCK AND BUS ELECTRICAL/ELECTRONICS STEERING COMMITTEE

APPENDIX A - SAFETY MEASURES AND ANALYSIS

A.1 MEASURES FOR COMPLIANCE

There are two methods for ensuring the required safety measures are in place. These methods are qualitative and quantitative. These methods are intended to address both random and systematic faults in the system.

A.1.1 Qualitative Analysis

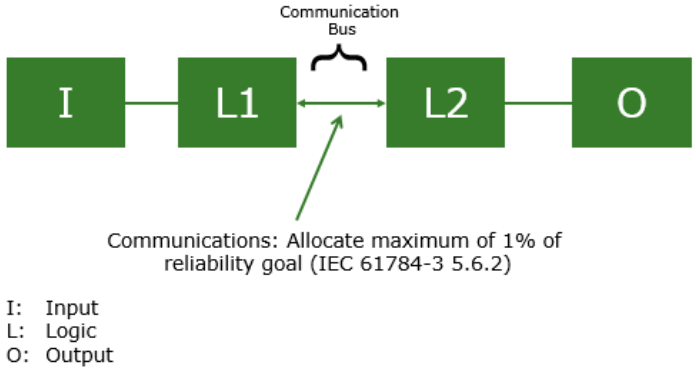
The motivation for the data link layer publication is to address functional safety standards. The functional safety standards principally reference IEC 61784-3 Functional Safety Fieldbus standards. This standard calls out qualitative and quantitative requirements that are intended to protect the communication bus from bit disturbances.

Table A1 contains the qualitative measures used to detect communication errors and the coverage provided by each measure used in a manner similar to IEC 61784-3 Table 1.

Table A1 - Qualitative errors and measures

IEC 61784-3 Communication Errors	**Safety Measures Used in SAE J1939 Functional Safety Protocol**							
	Sequence number	**Time stamp**	**Time expectation**	**Connection authentication**	**Feedback message**	**Data integrity**	**Redundancy with cross check**	**Different data integrity assurance**
	5.1.4, 5.3.9		5.1.3, 5.3.6, 5.3.7	5.3.2, 5.3.3, 5.3.4		5.1.5, 5.3.8	5.3.5, 5.3.8	5.1.5, 5.3.8
Message Corruption						X		
Unintended Repetition	X							
Incorrect Sequence	X							
Loss	X							
Unacceptable Delay			X					
Insertion	X						X	
Masquerade								X
Addressing				X				

A.1.2 Quantitative Measures



The quantitative measures analyze the reliability of the proposal to ensure the desired safety integrity level may be attained. The proposal shall not exceed 1% of the target reliability level per IEC 61784-3:2016. The resulting targets for an IEC 61508 communications bus are as follows:

Table A2 is derived from IEC 61508 and calls out the probability of failure per hour allowed in order to attain a safety integrity level. The probability of failure per hour is utilized in high-demand systems such as the communication bus sending periodic messages.

Table A2

IEC 61508 safety integrity level	Probability of failure per hour maximum allowed	Communication bus probability of failure per hour
SIL 4	$<10^{-8}$	$<10^{-10}$
SIL 3	$<10^{-7}$	$<10^{-9}$
SIL 2	$<10^{-6}$	$<10^{-8}$
SIL 1	$<10^{-5}$	$<10^{-7}$

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}.

A.1.2.1 Black Channel and White Channel

In addition to the qualitative analysis and quantitative analysis, the type of channel is also a consideration. White channel communications involve the analysis of the specific solution. Black channel analysis considers only the communication bus and is independent of the specific solution. The use of black channel analysis allows the use of modules that may not have been analyzed per IEC 61508 or similar standards. This proposal shall focus on a black channel solution. Any white channel analysis will be left to the system designer.

The black channel proposal is also intended to enable backward compatibility with existing modules by achieving SIL 2 and SIL 3 capable safety channels as part of a safety-related system.

The black channel option assumes a bit error rate (BER) equal to or less than 10^{-2}. The BER is as defined in IEC 61784-3:2016.

This option allocates 1% of the probability of failure per hour (PFH) for the safety function. For SIL 2 IEC 61508 requires the PFH of the safety function to be $<10^{-6}$. The resulting PFH for the communication bus is therefore $<10^{-8}$.

A.1.2.2 Calculation of PFH for a Given System Design

The following calculations must be performed for any complete system to assess its ability to meet SIL or PL levels. It can be shown that for many if not most practical systems SIL 2 and SIL 3 are achievable.

PFH for a known system is computed by:

$$PFH = R_{total}(PE) * v * m \quad \text{(Eq. A1)}$$

where:

v = safety-related messages per hour of network operation

m = number of receiving nodes for each safety message

R_{total} = total residual error rate

The total residual error rate is made up of multiple errors:

$$R_{total} = RR_T + RR_A + RR_I + RR_M \quad \text{(Eq. A2)}$$

where:

RR_T = residual error rate per hour for timeliness

RR_A = residual error rate per hour for authenticity

RR_I = residual error rate per hour for data integrity

RR_M = residual error rate per hour for masquerade

A.1.2.2.1 Data Integrity Errors

The data integrity error rate is computed from the probability of the CRC failure which is:

$$RR_I = R_{CRC}Pe \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times P_e^k \times (1 - P_e)^{n-k} \quad \text{(Eq. A3)}$$

$$\binom{n}{k} = \frac{n!}{k! \times (n-k)!} \quad \text{(Eq. A4)}$$

where:

r = size of CRC in bits

P_e = bit error rate for an unshielded cable = 1E-02

k = Hamming distance of the CRC polynomial selected. In this case, the polynomial 6938392Dh yields a hamming distance value = 10.

n = block length of the data plus the size of the CRC

$$n = block\ length = Essential\ data\ to\ protect + size\ of\ CRC = 64 + 32 = 96 \quad \text{(Eq. A5)}$$

Substituting for these variables we get:

$$R_{CRC}Pe \approx 2^{-r} \times \sum_{k=d_{min}}^{n} \binom{n}{k} \times P_e^k \times (1 - P_e)^{n-k} \approx 2^{-32} \times \frac{96!}{10! \times (96-10)!} \times 1E\text{-}02^{10} \times (1 - 1E\text{-}02)^{96-10} \quad \text{(Eq. A6)}$$

$$RR_I = R_{CRC}Pe \approx 1.10656E\text{-}17 \quad \text{(Eq. A7)}$$

A.1.2.2.2 Timeliness Errors

The residual error rate for timeliness is computed thus:

$$RR_T = RP_I * 2^{-LT} * R_A * RP_{FSCP} \quad \text{(Eq. A8)}$$

where:

LT = bit length of the sequence number = 5

w = Range of values of accepted time stamps or sequence number for receiving safety PDUs. Assumed to be one.

R_T = Rate of occurrence of incorrect sequence safety PDUs. Assumed to be the same as worst case for corrupted messages = 1.10656E-17.

RP_{FSCP} = Residual error probability for other measures unique to the FSCP. Assumed to be 10^{-3}.

so:

RR_T = 3.458E-22

A.1.2.2.3 Authenticity Errors

The residual error rate for authenticity errors is

$$RR_A = RP_I * 2^{-LA} * R_A * RP_{FSCP} \quad \text{(Eq. A9)}$$

where:

RP_I = Residual error probability for data integrity. As computed above with 32-bit CRC, protection is 1.10656E-17.

LA = bit length of the connection authentication, 26 bits of the CAN ID

R_A = Rate of occurrence for misdirected safety PDUs. Assumed to be 10^{-3}.

RP_{FSCP} = Residual error probability for other measures unique to the FSCP. Assumed to be 10^{-3}.

so:

RR_A = 1.6489E-31

A.1.2.3 Total Residual Error Rate from Eq. A2 Becomes

$$R_{total} = 3.458\text{E-}22 + 1.6489\text{E-}31 + 1.10656\text{E-}17 = 1.10659\text{E-}17 \quad \text{(Eq. A10)}$$

Using the above value and your system specifications for *v* and *m* in Equation A1, you can compute the PFH. Examples for various values of *v* and *m* are shown in Table A3.

$$PFH = 1.10659\text{E-}17 * v * m \quad \text{(Eq. A11)}$$

Table A3 - PFH examples

Case	Number of Safety-Relevant Message Pairs/Second	% of Bus Load at 500 kbps	Mess/Hour V	Number Receivers m	PFH	SIL 2 <1E-8	SIL 3 <1E-9
1	100	5%	720000	1	7.9674E-12	YES	YES
2	100	5%	720000	100	7.9674E-10	YES	YES
3	200	10%	1440000	1	1.5935E-11	YES	YES
4	200	10%	1440000	50	7.9674E-10	YES	YES
5	500	25%	3600000	1	3.9837E-11	YES	YES
6	2000	100%	14400000	6	9.5609E-10	YES	YES
7	2000	100%	14400000	15	2.3902E-09	YES	NO
Worst	2000	100%	14400000	253	4.0315E-08	NO	NO

Observations:

1. Case 1: For a practical system using 100 SDGs per second, both SIL 2 and SIL 3 can be achieved. This is one transmitter sending an SDG to one receiver every 10 ms, or this is two transmitters sending one SDG each to one receiver each every 20 ms, and so on.

2. Case 2: Likewise, one transmitter can send one SDG to 100 receivers that all use the information in safety-related functions and still meet SIL 3. Increasing the number of receivers to 126, however, meets SIL 2, but not SIL 3.

3. Cases 3, 4, and 5: Similarly, an increased bus load to 25% can achieve safety or performance levels if the message update rate and number of receivers meet the constraints of Equation A11.

4. Since these safety protocol messages come in pairs, then on a 500 kbps CAN network a maximum of 2000 pairs can exist.

5. The worst-case analysis of 2000 SDGs (100% bus load at 500 Kbps) between a single transmitter and 253 receivers does not meet SIL 2 or SIL 3.

6. However, a network fully loaded with safety relevant messages with fewer receivers can achieve SIL 2 (Case 7) or even SIL 3 (Case 6).

Conclusion:

As shown above, a detailed analysis can and must be performed on any complete system including the CAN communication network. Doing so may result in confidence that the given system will meet required performance levels.

It shall be the responsibility of the end user to verify the safety or performance level for their application as well as the impact of the network portion of the system.

A.1.3 Application Limitations

A.1.3.1 Assumptions

- The sequence number as defined in the SAE J1939 Functional Safety Protocol is 5 bits long, resulting in 32 messages. The maximum number of skipped messages allowed shall be less than 40% of the sequence number range in order for the sequence number to be a valid qualitative protective measure. This will allow for 12 skipped messages.

- It must also ensure that the number of skipped messages allowed falls within the diagnostic detection time of the safety-related system process safety time. Process safety time is the maximum permitted time between the occurrence of a failure that has potential to give rise to a hazardous event, and the time by which the system must complete action to prevent the hazardous event from occurring. The diagnostic detection time is the maximum time permitted within the process safety time for detecting the fault while still allowing sufficient time for performing the necessary system response.

- It is necessary that the PFH calculations for the deployed system be performed for the worst case expected for the system.

APPENDIX B - TÜV APPROVAL LETTER

TÜV SÜD Rail GmbH Barthstr. 16 D-80339 München Germany

SAE INTERNATIONAL
400 Commonwealth Drive
Warrendale, PA 15096
The USA

Your reference/letter of	Our reference/name	Phone extension/e-mail	Fax extension	Date	Page
	PS Dr. P. Supavatanakul	+49 (89) 5791-3524 peerasan.supavatanakul@tuev-sued.de	-2933	2nd August 2018	1 of 1

Re: Evaluation of SAE J1939-76 Functional Safety Communication Protocol

To whom it may concern:

we would like to inform you that the related review of the following documents

[A1]	Surface vehicle recommended practice J1939 Functional Safety Communication Protocol (J1939-76)	PropDft	9th July 2018
[A2]	Properness of 32 Bit CRC Polynomial used in SAE_J1939 (Email)	-	13th Apr 2018
[A3]	Calculation of CRC Properness 6938392h (Email)	-	2nd Jun 2018

has shown that the safety specification for **SAE J1939-76 Functional Safety Communication Protocol** is able to meet the requirements according to the functional safety standards IEC 61508-2:2010 (upto SIL 3), and the industrial safety communication standard IEC 61784-3:2016.

The review of detailed design and the planning of V&V activities are necessary to demonstrate that implementation of SAE J1939-76 fulfils the aforementioned standards.

Yours sincerely,

Digital unterschrieben von Peter Weiß
Datum: 2018.08.02 15:40:16 +02'00'

Peter Weiß
Technical Certifier

Digital unterschrieben von Peerasan Supavatanakul
Datum: 2018.08.02 14:36:48 +02'00'

Dr. Peerasan Supavatanakul
Project management

Headquarters: Munich
Trade Register Munich HRB 154539
USt-IdNr.: DE 814 205 994
Information pursuant to Section 2(1)
DL-InfoV (Germany) at
www.tuev-sued.com/imprint

Managing Director:
Dipl.-Ing. Klaus-Michael Bosch
Dipl.-Wirtsch.-Ing. Jan Rösler
Hypovereinsbank Munich
Acc. No. 667566061
Bank sort code 700 202 70
IBAN: DE 067 002027 00667 566061
SWIFT: HYVEDEMM

Phone:+49 89 5791-1473
Fax: +49 89 5791-2933
www.tuev-sued.de/rail
TÜV®

TÜV SÜD Rail GmbH

Barthstraße 16
80339 München
Germany