



SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-77

NOV2025

Issued

2025-11

SAE J1939 CAN FD Functional Safety Assurance Data

RATIONALE

SAE J1939-76 defines a protocol to provide safety assurance data for SAE J1939-21 messages, which are based on classic CAN data frames with 8-byte payloads. For SAE J1939-22 messages, which are based on CAN FD data frames with 64-byte payloads, the safety assurance data provided by SAE J1939-76 are no longer adequate for some PGs. Accordingly, this publication provides requirements for safety assurance data for A_PDUs carried inside either Multi-PG Protocol communications (as described by different Types of Service and Trailer Formats) or FD Transport Protocol communications (as described by different Assurance Data Types). In deference to those applications that wish to continue using SAE J1939-76 for functionally safe communications, this publication also provides requirements for using SAE J1939-76 for SAE J1939-22 communications.

FOREWORD

The definition of the SAE J1939 communications network consists of a collection of individual SAE J1939 documents based upon the layers of the Open System Interconnect (OSI) model for a computer communications architecture. The SAE J1939 CAN FD Functional Safety Assurance Data document describes parts of 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 a vehicle.

The SAE J1939 communications network is tailored for use in heavy-duty environments and is suitable for horizontally integrated vehicle industries. The SAE J1939 communications network is applicable for light-, medium-, 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 transmission, which are sourced from 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

SAE WEB ADDRESS: <http://www.sae.org>

Full document details: SAE J1939-77_202511

For more information on this standard, visit https://www.sae.org/standards/content/J1939-77_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	FAA Publications.....	4
2.1.3	IEC Publications.....	5
2.1.4	Other Publications.....	5
2.2	Related Publications	5
2.2.1	IEC Publications.....	5
2.2.2	ISO Publications.....	5
2.2.3	Other Publications.....	5
3.	DEFINITIONS	6
4.	ABBREVIATIONS	7
5.	BACKGROUND	9
6.	COMMUNICATION MODELS.....	9
6.1	Overview	9
6.2	FuSa Interface Model.....	9
6.2.1	Producer.....	10
6.2.2	Consumer.....	10
6.2.3	Router.....	11
6.2.4	SAE J1939-22 Protocol Stack.....	11
6.2.5	A_PDU Transmitter.....	13
6.2.6	A_PDU Receiver.....	13
6.3	FuSa Sequence Models.....	14
6.3.1	Communication Inside a LAN	14
6.3.2	Communication through a Router	15
6.4	Parameters.....	16
6.4.1	PGN.....	16
6.4.2	PG Data	16
6.4.3	DA	16
6.4.4	SA.....	16
6.4.5	Priority	16
6.4.6	FuSa Assurance.....	17
6.4.7	Cybersecurity Assurance	18
6.4.8	Safety Cycle Time (SCT and SCT _{max}).....	18
6.5	Communication Error Coverage	18
7.	TECHNICAL REQUIREMENTS.....	19
7.1	Timing.....	19
7.1.1	SCT	19
7.1.2	SCT _{max}	19
7.2	Producer.....	20
7.3	Consumer.....	22
7.3.1	Overview	22
7.3.2	Initialize	23
7.3.3	Wait.....	23
7.3.4	Verify Cybersecurity Assurance Information.....	23
7.3.5	Verify FuSa Assurance Parameters.....	23
7.3.6	Verify SN	24
7.3.7	Perform Bookkeeping.....	24
7.3.8	Process Communication Error	24
7.4	Router.....	24

7.5	FuSa Assurance Profiles.....	25
7.5.1	Overview	25
7.5.2	Functional Safety Profile Identifier (FSPI) (SPN 23890).....	26
7.5.3	FuSa Profile #1	26
7.5.4	FuSa Profile #2	31
7.5.5	FuSa Profile #3	34
8.	UTILIZING SAE J1939-76 IN SAE J1939-22 COMMUNICATIONS.....	38
8.1	Overview	38
8.2	Producer Requirements	39
8.3	Consumer Requirements	39
8.4	SAE J1939-22 Protocol Stack Recommendation	39
9.	NOTES.....	39
9.1	Revision Indicator.....	39
APPENDIX A	REFERENCE TABLES AND EQUATIONS	40
APPENDIX B	APPROXIMATIONS FOR RESIDUAL ERROR PROBABILITY FOR DATA INTEGRITY	44
APPENDIX C	SEQUENCE NUMBER USE CASES.....	49
APPENDIX D	JUSTIFICATION FOR CHOOSING A 32-BIT SIZE FOR THE SEQUENCE NUMBER.....	53
APPENDIX E	FuSa PROFILE EVALUATIONS.....	54
APPENDIX F	EXAMPLES OF CALCULATED INTEGRITY CHECK VALUES.....	57
Figure 1	UML class diagram of the FuSa interface model.....	9
Figure 2	UML sequence diagram for communicating safety-related A_PDUs inside a LAN.....	14
Figure 3	UML sequence diagram for communicating safety-related A_PDUs through a router.....	15
Figure 4	UML activity diagram for a producer	20
Figure 5	UML activity diagram for a consumer	22
Figure 6	Arrangement of data for calculating the ICV for FuSa Profile #1.....	29
Figure 7	Arrangement of the FuSa assurance data trailer for FuSa Profile #1.....	30
Figure 8	Arrangement of data for calculating the ICV for FuSa Profile #2.....	32
Figure 9	Arrangement of the FuSa assurance data trailer for FuSa Profile #2.....	33
Figure 10	Arrangement of data for calculating the ICV for FuSa Profile #3.....	36
Figure 11	Arrangement of the FuSa assurance data trailer for FuSa Profile #3.....	37
Table 1	Communication error coverage.....	18
Table 2	Maximum word lengths for given HDs for CRC-32K/9	27
Table 3	Maximum word lengths for given HDs for CRC-64-ECMA	35
Equation 1	Calculation of SCT_{max}	19

1. SCOPE

This document describes the functional safety (FuSa) assurance data to be included when communicating safety-related A_PDU's using either the Multi-PG service or the FD Transport service within an SAE J1939-22 protocol stack. It specifies the following:

- The parameters that make up the FuSa assurance information
- The behavioral requirements when producing and consuming FuSa assurance information
- The technical requirements for different FuSa profiles intended to meet different application requirements
- The trailer formats for the different FuSa profiles that can be incorporated into Multi-PG and FD Transport services

This document does not specify the assignment of a FuSa profile to any values of the TOS and TF fields when using the Multi-PG service, or to any value of the AD TYPE field when using the FD Transport service; instead, SAE J1939-22, or an OEM in the manufacturer-specific ranges of these fields, specifies the assignments for these fields.

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: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J1939-21 Data Link Layer

SAE J1939-22 CAN FD Data Link Layer

SAE J1939-31 Network Layer

SAE J1939-76 SAE J1939 Functional Safety Communications Protocol

SAE J1939-81 Network Management

SAE J1939DA J1939 Digital Annex

2.1.2 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

DOT/FAA/TC-14/49 Selection of Cyclic Redundancy Code and Checksum Algorithms to Ensure Critical Data Integrity, U.S. Department of Transportation, Federal Aviation Administration, https://www.faa.gov/sites/faa.gov/files/aircraft/air_cert/design_approvals/air_software/TC-14-49.pdf

2.1.3 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 61508-2	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions, ed. 3.0
IEC 61784-3:2024	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions, ed. 4.1

2.1.4 Other Publications

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

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 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, all parts

IEC 62280	Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems
-----------	--

2.2.2 ISO Publications

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

ISO 13849-1	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
ISO 19014-4	Earth-moving machinery - Functional safety - Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system
ISO 25119-1	Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 1: General principles for design and development

2.2.3 Other Publications

OMG, OMG Unified Modeling Language (OMG UML), version 2.5.1, <https://www.omg.org/spec/UML/>.

3. DEFINITIONS

3.1 BLACK CHANNEL

As defined in IEC 61508-2, a black channel is a communication channel where parts of the channel were not designed, implemented, and validated in accordance with functional safety specifications. Compare with *white channel*.

3.2 DATA FLOW

A data flow (sometimes referred to as a stream) represents related instances of the same parameterized information being communicated across a network in a system. The combination of the parameters being communicated, the sender of the parameter data, and the intended receiver(s) of the parameter data uniquely identifies a data flow within the context of the network.

3.3 FD TRANSPORT SERVICE

The FD Transport service is a service specified in SAE J1939-22 for transporting a message whose total length, including any trailer, exceeds the maximum payload size of a CAN FD data frame.

3.4 HAMMING DISTANCE (HD)

The Hamming distance between two strings of equal length is a count of the number of symbols that are different between the two strings.

3.5 HAMMING WEIGHT (HW)

The Hamming weight is a count of the number of symbols that are different between one string and a string of equal size that consists solely of zero-symbols. It is equal to the Hamming distance between the string and the all-zeros string.

3.6 LOCAL AREA NETWORK (LAN)

For the purpose of this document, a local area network is a network that is physically constrained in size and that shares the same address space among nodes connected to it. When compared to the definitions found in SAE J1939-31, a local area network is equivalent to a subnetwork that contains zero or more bridges across segments. A router can connect two or more LANs together.

3.7 MULTI-PG SERVICE

The Multi-PG service is a service specified in SAE J1939-22 for transporting one or more messages whose total length, including any trailers, is less than or equal to the maximum payload size of a CAN FD data frame.

3.8 OEM INTEGRATOR

An OEM integrator is the entity responsible for the final assembly and integration of various parts and networks into a cohesive vehicle system.

3.9 ROUTER

A router, as defined in SAE J1939-31, is a device for transferring messages between two or more network segments where the protocol is the same on both segments but where each network segment has a separate address space.

3.10 WHITE CHANNEL

As defined in IEC 61508-2, a white channel is a communication channel where the entire channel was designed, implemented, and validated in accordance with functional safety specifications. Compare with *black channel*.

4. ABBREVIATIONS

A_PDU	Application Protocol Data Unit
AD SIZE	Assurance Data Size
AD TYPE	Assurance Data Type
AppPI	Application Protocol Indicator
BAM	Broadcast Announce Message
C-PG	Contained Parameter Group
CA	Controller Application
CAN	Controller Area Network
CAN FD	Controller Area Network—Flexible Data Rate
CRC	cyclic redundancy check
CTS	Clear to Send
D_PDU	Data Link Protocol Data Unit
D_PDU1	Data Link Protocol Data Unit 1
D_PDU2	Data Link Protocol Data Unit 2
D_PDU3	Data Link Protocol Data Unit 3
DA	Destination Address
DataID	Data Identifier
DP	Data Page
ECU	electronic control unit
EDP	Extended Data Page
FIFO	first-in, first-out
FSCP	functional safety communication profile
FSPI	functional safety profile identifier
FuSa	functional safety
GE	Group Extension
HD	Hamming distance
HW	Hamming weight
ICV	integrity check value

LAN	local area network
LEN	length
OEM	original equipment manufacturer
PDU	Protocol Data Unit
PDU1	Protocol Data Unit 1
PDU2	Protocol Data Unit 2
PF	PDU Format
PG	Parameter Group
PGN	Parameter Group Number
PL	Payload Length
PS	PDU Specific
RTS	Request to Send
SA	Source Address
SCL	safety communication layer
SCT	safety cycle time
SCT _{max}	maximum 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
SN	sequence number
TF	Trailer Format
TOS	Type of Service
UML	Unified Modeling Language

5. BACKGROUND

The various standards under IEC 61508 provide the foundation of FuSa requirements for a number of other standards. The IEC 61508 standards define safety integrity levels (SILs), from SIL1 (lowest safety integrity level) through SIL4 (highest safety integrity level), as measures of performance for safety functions. The standard IEC 61784-3:2024, which is based on IEC 61508, defines several principles for communications related to functional safety and serves as another input to this document for implementation requirements.

Given that IEC 61508 and IEC 61784-3:2024 form the basis for several other FuSa standards for communications, the requirements provided in this document can fulfill the requirements of these other standards. However, to be clear, users of this document are responsible for the compliance, documentation, and validation of system and component implementations for any industry-specific safety performance requirements.

6. COMMUNICATION MODELS

6.1 Overview

The models presented in this section serve only to provide context for later technical requirements; they do not provide any requirements for hardware or software implementations.

6.2 FuSa Interface Model

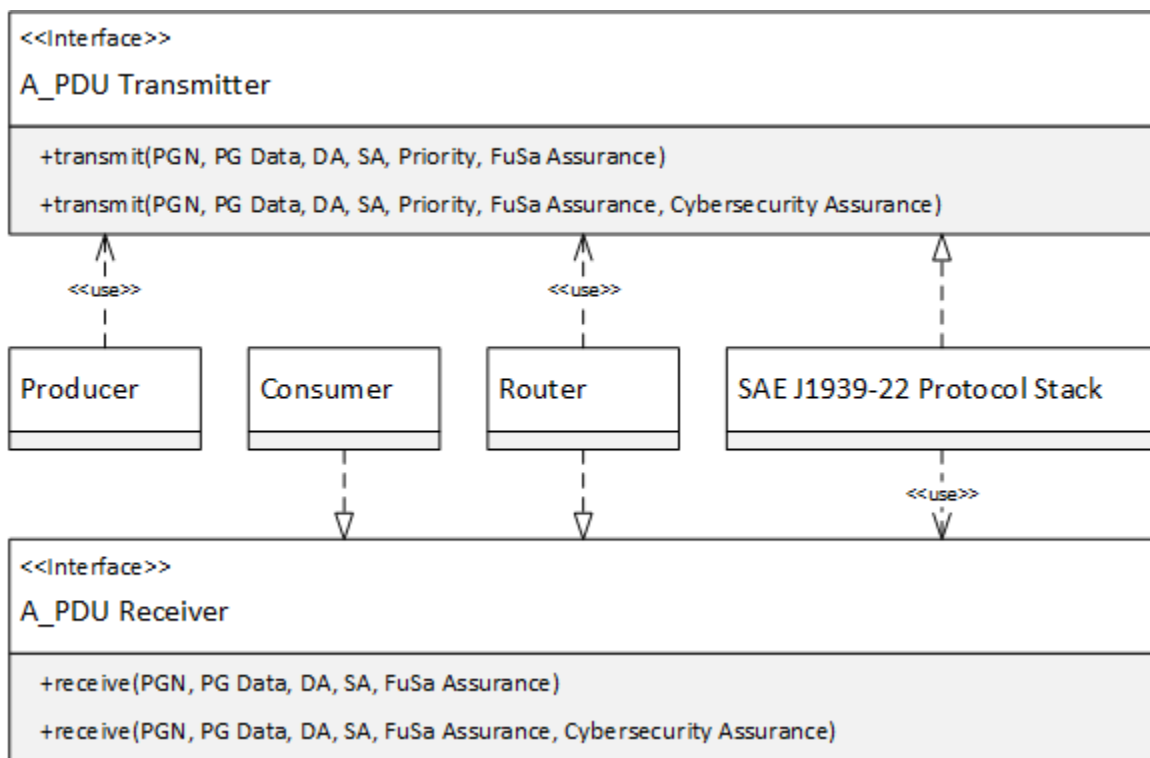


Figure 1 - UML class diagram of the FuSa interface model

Figure 1 is a definition of the interfaces used to model the interactions between producing and consuming safety applications and the underlying protocol stack that supports SAE J1939-22 communication. Although used by safety-related applications, the interfaces themselves are not safety related; instead, they provide access to a black channel communication. In addition, although SAE J1939-22 allows for communication of A_PDU without FuSa assurance information, this document only considers those A_PDU that require such information.

NOTE: The transmit and receive models provided in SAE J1939-22 influenced the design of this model, although some details differ.

6.2.1 Producer

The producer is a controller application that, as part of a safety function, transmits safety-related data to one or more consumers. As illustrated in Figure 1, a producer uses the A_PDU transmitter interface provided by the SAE J1939-22 protocol stack to communicate its safety data across a LAN.

The producer is responsible for the following—note the order provided below is not necessarily the order in which items are accomplished:

- Claiming, defending, and using an appropriate SA on its LAN
- Selecting the correct PGN associated with the PG data that it needs to communicate as part of the safety function
- Correctly updating and formatting the PG data in accordance with the PG's definition
- Selecting the appropriate DA on its LAN for either unicast or broadcast communication
- Selecting an appropriate priority for communicating the safety data over its LAN
- Correctly defining and calculating the FuSa assurance information to be communicated
- If necessary or desired, providing the appropriate cybersecurity assurance information to be communicated
- In accordance with the PG's definition, regularly submitting the above information to the SAE J1939-22 protocol stack to be communicated as an A_PDU to one or more consumers

6.2.2 Consumer

The consumer is a controller application that, as part of a safety function, receives safety-related data communications from a producer. As illustrated in Figure 1, a consumer implements the A_PDU receiver interface that is used by the SAE J1939-22 protocol stack to communicate safety data received from the LAN.

The consumer is responsible for the following—note the order provided below is not necessarily the order in which items are accomplished:

- Claiming, defending, and using an appropriate SA on its LAN—this serves as a DA when receiving A_PDUs
- In accordance with the PG's definition, monitoring for regular communication of the safety-related A_PDU from the producer and raising a communication error if it is not received within the expected timeframe
- Verifying either that the DA for the received A_PDU matches its SA or that the DA is the Global address
- If desired and if available, verifying the cybersecurity assurance information that was communicated
- Verifying the FuSa assurance information that was communicated
- Verifying the received PGN associated with the PG data that it needs as part of the safety function
- Correctly parsing and using the PG data in accordance with the PG's definition

6.2.3 Router

The router is a controller application that is not part of any safety-related application, but it receives safety-related communications from a producer and forwards said communications to one or more consumers as part of a black channel for communication across LANs. As illustrated in Figure 1, a router implements the A_PDU receiver interface that is used by the SAE J1939-22 protocol stack to communicate safety-related data received from the producer's LAN; it also uses the A_PDU transmitter interface provided by the SAE J1939-22 protocol stack to communicate this safety-related data across the consumer's LAN.

The router is responsible for the following—note the order provided below is not necessarily the order in which items are accomplished:

- Claiming, defending, and using an appropriate SA on each of the LANs to which it is connected—this serves as a DA when receiving A_PDUs on that LAN
- Verifying either that the DA for the A_PDU received on the producer's LAN matches its SA on that LAN or that the DA is the Global address
- Checking that the received PGN associated with the PG data is one that it can communicate from the producer's LAN to the consumer's LAN
- Selecting the appropriate DA to use for addressing in the consumer's LAN
- Selecting an appropriate priority for communicating the A_PDU over the consumer's LAN
- Correctly parsing the A_PDU's information received from the SAE J1939-22 protocol stack on the producer's LAN—namely, the PGN, PG data, FuSa assurance, and cybersecurity assurance if available
- Processing cybersecurity assurance information in one of two ways:
 - If the cybersecurity assurance information is to be processed on a per-hop basis, verifying the cybersecurity assurance information that was communicated for the A_PDU on the producer's LAN before providing appropriate and possibly different cybersecurity assurance information to be communicated for the A_PDU on the consumer's LAN
 - If the cybersecurity assurance information is to be processed on an end-to-end basis, communicating the cybersecurity assurance information provided by the producer, without alteration, for the A_PDU on the consumer's LAN
- Passing the PGN, PG data, FuSa assurance information, and (if necessary) cybersecurity assurance information to the SAE J1939-22 protocol stack on the consumer's LAN but using updated SA and DA values for that LAN

NOTE: Whether and how to process cybersecurity assurance information within the router depend entirely on the details of the cybersecurity system design and are beyond the scope of this document.

6.2.4 SAE J1939-22 Protocol Stack

The SAE J1939-22 protocol stack is a simple model for those lower protocol layers that form part of a black channel for communication of safety-related information between a producer and one or more consumers. As such, the SAE J1939-22 protocol stack is not part of any safety application and does not need to meet functional safety requirements.

When transmitting A_PDUs, the SAE J1939-22 protocol stack is responsible for the following—note the order provided below is not necessarily the order in which items are accomplished:

- Deciding whether to use the Multi-PG service or the FD Transport service to communicate the given A_PDU
- Arranging the contents of the given A_PDU into a format suitable for communication via Multi-PG or FD Transport
- Providing authentication and optionally encrypting the given A_PDU when cybersecurity assurance is present and if appropriate
- When using the Multi-PG service:
 - Correctly defining the TOS and TF fields based on the contents of the FuSa assurance information and cybersecurity assurance information
 - Deciding whether to use a D_PDU1 or D_PDU3 format to communicate the given A_PDU
 - Packing one or more individual C-PGs containing A_PDUs into the payload in the order that they were provided by the producer
- When using the FD Transport service:
 - Correctly defining the AD TYPE and AD SIZE fields based on the contents of the FuSa assurance information and cybersecurity assurance information
 - Deciding whether to use RTS/CTS or BAM to communicate the given A_PDU
 - Managing the FD Transport session as the originator

When receiving A_PDUs, the SAE J1939-22 protocol stack is responsible for the following—note the order provided below is not necessarily the order in which items are accomplished:

- Accepting received D_PDUs based on the DA, whether explicit (as in D_PDU1) or implied (as in D_PDU3)
- Accepting received D_PDUs based on the Multi-PG PGN or FD Transport PGNs (if a D_PDU1) or the Multi-PG AppPI (if a D_PDU3)
- Determining whether the Multi-PG service or the FD Transport service is being used
- When using the Multi-PG service, unpacking the individual C-PGs from the payload of the Multi-PG format and processing them in the order that they appeared in the payload
- When using the FD Transport service, managing the FD Transport session as the responder
- Decrypting and/or authenticating an A_PDU when cybersecurity assurance information is present and if appropriate
- Correctly parsing the relevant A_PDU information including the PGN, PG data, DA, SA, FuSa assurance information, and cybersecurity assurance information if available

NOTE 1: Since neither the Multi-PG service nor the FD Transport service uses the D_PDU2 format, this document does not consider use of D_PDU2 for communicating safety-related data via the SAE J1939-22 protocol stack.

NOTE 2: In some use cases, a router cannot alter encrypted or authenticated contents when passing them from one LAN to the other. This restriction can impact how the router's SAE J1939-22 protocol stacks operate.

6.2.5 A_PDU Transmitter

The A_PDU transmitter defines the boundary between the producer or router and the SAE J1939-22 protocol stack. The producer or router uses the operations defined in the A_PDU transmitter, and the SAE J1939-22 protocol stack provides implementations for them.

As shown in Figure 1, the A_PDU transmitter describes two transmit operations for sending a safety-related A_PDU across a LAN. These two operations have the same purpose and differ only in the presence of the cybersecurity assurance parameter. Below is a list of the parameters passed through the interface:

- PGN (see 6.4.1)
- PG data (see 6.4.2)
- DA (see 6.4.3)
- SA (see 6.4.4)
- Priority (see 6.4.5)
- FuSa assurance (see 6.4.6)
- Cybersecurity assurance (see 6.4.7)

6.2.6 A_PDU Receiver

The A_PDU receiver defines the boundary between the SAE J1939-22 protocol stack and the consumer or router. The SAE J1939-22 protocol stack uses the operations defined in the A_PDU receiver, and the consumer or router provides implementations for them.

As shown in Figure 1, the A_PDU receiver describes two receive operations for receiving a safety-related A_PDU from a LAN. These two operations have the same purpose and differ only in the presence of the cybersecurity assurance parameter. Below is a list of the parameters passed through the interface:

- PGN (see 6.4.1)
- PG data (see 6.4.2)
- DA (see 6.4.3)
- SA (see 6.4.4)
- FuSa assurance (see 6.4.6)
- Cybersecurity assurance (see 6.4.7)

6.3 FuSa Sequence Models

6.3.1 Communication Inside a LAN

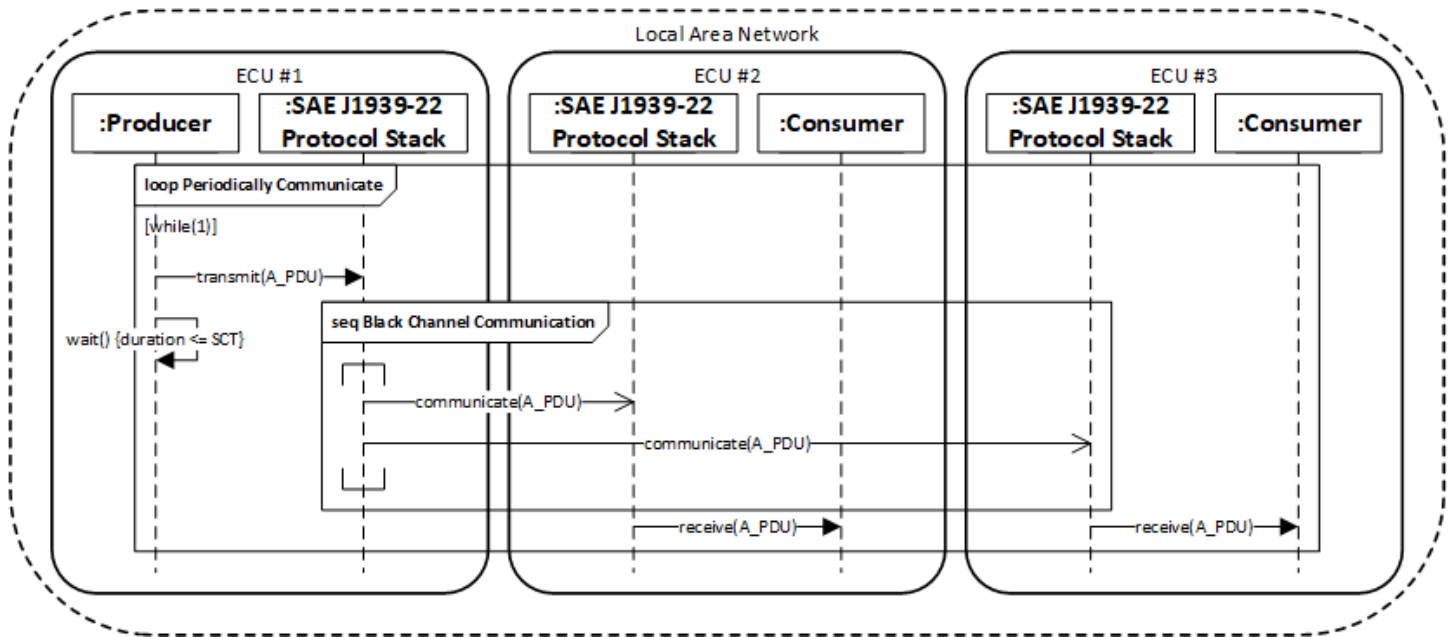


Figure 2 - UML sequence diagram for communicating safety-related A_PDUs inside a LAN

Figure 2 illustrates a model of communication between a producer and one or more consumers in the same LAN. The following steps describe the sequence:

1. The producer generates the A_PDU information as a part of its safety function and sends it to its SAE J1939-22 protocol stack for transmission. If this is to be a broadcast communication to a set of consumers, the producer uses the Global address as the DA; if this is to be a unicast communication to a specific consumer, the producer uses the consumer's address as the DA.
2. The producer's SAE J1939-22 protocol stack communicates the A_PDU across the LAN to the SAE J1939-22 protocol stacks of all consumers in the LAN if broadcast, or to the protocol stack of the specific consumer if unicast.
3. Each consumer's SAE J1939-22 protocol stack provides the A_PDU information to its consumer for reception as part of its safety function.
4. The producer repeats this sequence once the producer has waited up to the safety cycle time (SCT) (see 6.4.8) after it last generated A_PDU information.

NOTE: The coregion inside Figure 2 models a broadcast in that both communications occur in parallel. If the communication were unicast, there would be only one communication.

The "Black Channel Communication" fragment models message transmission across the LAN. The details within this fragment are deliberately vague to emphasize that the method of communication is largely immaterial to handling the safety-related A_PDU; for example, communication across the LAN could be via either a Multi-PG service or an FD Transport service. That being said, network delays cannot be so large as to cause a consumer to decide that A_PDUs were lost or that an unacceptable delay has occurred.

6.3.2 Communication through a Router

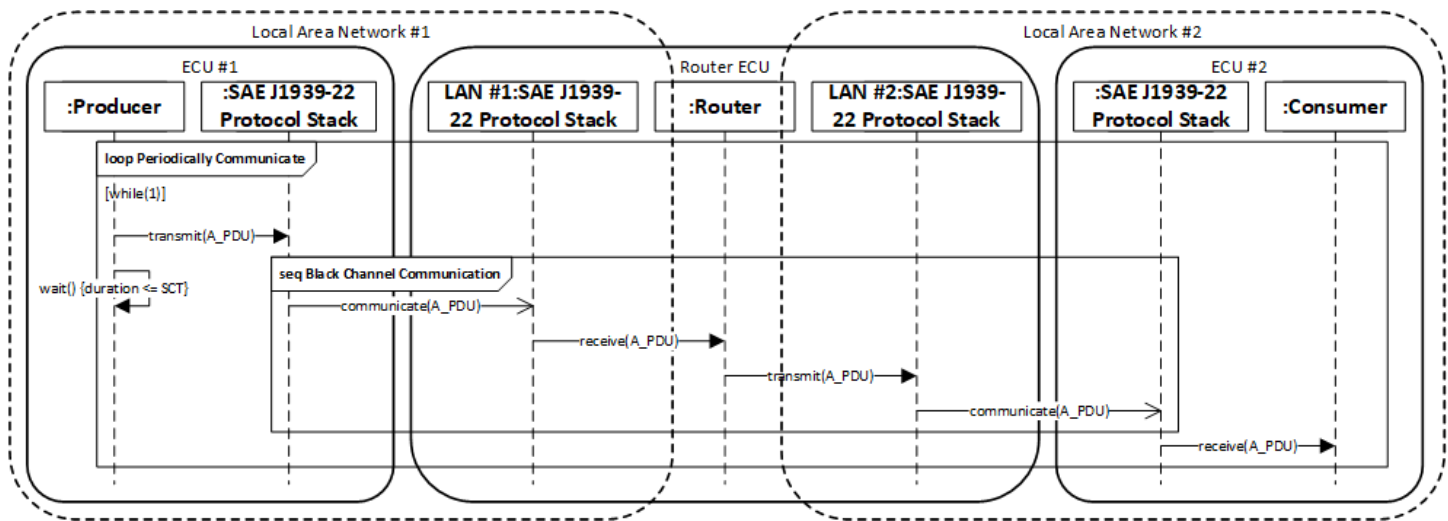


Figure 3 - UML sequence diagram for communicating safety-related A_PDUs through a router

Figure 3 illustrates a model of communication between a producer and a consumer in different LANs. The following steps describe the sequence:

1. The producer generates the A_PDU information as a part of its safety function and sends it to its SAE J1939-22 protocol stack for transmission, using the router's address in LAN #1 as the DA.
2. The producer's SAE J1939-22 Protocol Stack communicates the A_PDU across the LAN to the LAN #1:SAE J1939-22 protocol stack of the router.
3. The router takes the A_PDU information and sends it to its LAN #2:SAE J1939-22 protocol stack, using its address in LAN #2 as the SA and using the consumer's address as the DA.
4. The router's LAN #2:SAE J1939-22 protocol stack communicates the A_PDU across the LAN to the SAE J1929-22 protocol stack of the consumer.
5. The consumer's SAE J1939-22 protocol stack provides the A_PDU information to the consumer for reception as part of its safety function.
6. The producer repeats this sequence once the producer has waited up to the safety cycle time (SCT) (see 6.4.8) after it last generated A_PDU information.

The "Black Channel Communication" fragment models message transmission across the LANs. The details within this fragment are deliberately vague to emphasize that the method of communication is largely immaterial to handling the safety-related A_PDU; for example, communication across one or both LANs could be via either a Multi-PG service or an FD Transport service. That being said, network delays cannot be so large as to cause the consumer to decide that A_PDUs were lost or that an unacceptable delay has occurred.

NOTE: The model provided here illustrates communication through a single router, but it is possible for communication to continue through two or more routers in series.

In the process of routing an A_PDU from one LAN to another, a router and its associated SAE J1939-22 protocol stacks can perform one of the following transfers of the A_PDU's contents:

- They can transfer the contents from one Multi-PG message between the producer and the router to a different Multi-PG message between the router and the consumer. While doing so, the router and its associated SAE J1939-22 protocol stacks can combine the A_PDU with other A_PDUs, or with a different set of A_PDUs, in the new Multi-PG message.
- They can transfer the contents from one FD Transport message between the producer and the router to a different FD Transport message between the router and the consumer.
- They can transfer the contents from a Multi-PG message to an FD Transport message if the router needs to add cybersecurity assurance information such that the resulting message size exceeds the constraints of the Multi-PG service.
- They can transfer the contents from an FD Transport message to a Multi-PG message if all of the following conditions apply:
 - The producer provided cybersecurity assurance information for the router to consume.
 - The router does not need to add cybersecurity assurance information for the consumer to consume.
 - The resulting message size is within the constraints of the Multi-PG service.

6.4 Parameters

6.4.1 PGN

The PGN identifies the contents of the associated PG data including the position and format of parameters in the data. A PG definition always has a unique PGN.

NOTE: A PGN that is of type PDU1 defines the PS field as 00h.

6.4.2 PG Data

The PG data is an ordered sequence of bytes containing data for the parameters in the group identified by the PGN. A PG definition, provided in SAE J1939DA, specifies the format of the data.

6.4.3 DA

The DA is the SAE J1939 address, within a LAN, of the intended recipient(s)/responder(s) for the A_PDU.

NOTE: If the PGN is of type PDU2, then DA is effectively FFh (the Global address) regardless of the value provided in DA.

6.4.4 SA

The SA is the SAE J1939 address, within a LAN, of the sender/originator for the A_PDU.

6.4.5 Priority

The priority determines the importance of an A_PDU relative to other messages being communicated on the LAN, although it is irrelevant when communicating an A_PDU via D_PDU3. The priority value is one from a set of eight enumerated values, with 0 indicating highest priority and 7 indicating lowest. A PG definition specifies the default value to use for the priority, although an OEM integrator can adjust this value.

The priority facilitates timely black channel communication between a producer and any routers or consumers, but a consumer does not need knowledge of the priority for an A_PDU in order to use the A_PDU's information in its safety function; therefore, FuSa assurance information does not provide communication error coverage for priority.

6.4.6 FuSa Assurance

6.4.6.1 Overview

The FuSa assurance information is a collection of FuSa-related parameters that are generated by a producer and interpreted or verified by a consumer as part of the safety function. These parameters help to provide a necessary degree of assurance for the selected SIL.

NOTE: The sections provided here describe only those parameters necessary to meet FuSa requirements. An implementation can require additional parameters to be passed to and from the SAE J1939-22 protocol stack to ensure proper operation.

6.4.6.2 Functional Safety Profile Identifier (FSPI)

The FSPI provides identification of the FuSa profile employed by the producer when communicating its safety-related data. Using the FSPI, a consumer can verify that the FuSa assurance information it received aligns with the FuSa profile it expected.

Each FuSa profile specifies a different value for FSPI. See 7.5 for details.

NOTE: The use of FSPI serves as a check against the impact that a corrupted TOS, TF, or AD TYPE field can have on parsing and interpreting FuSa assurance information. (None of these three fields are part of the ICV calculation.) For example, without FSPI, there could be an unexpected reduction in error detection capability in the case where the producer calculates an ICV using one algorithm but, due to an incorrect value placed in the TOS, TF, or AD TYPE field, a consumer calculates the ICV using a different algorithm.

6.4.6.3 Data Identifier (DataID)

The DataID provides identification of the safety-related data being communicated within a system as a data flow. This identification is unique within the system and covers identification of the data, the producer sending the data, and the consumer(s) receiving the data. Using the DataID, a consumer can verify that the A_PDU is for the consumer, comes from the expected producer, and contains the expected parameter data.

Each FuSa profile specifies DataID in its own way and can make use of other parameters, for example, PGN, DA, and SA. See 7.5 for details.

6.4.6.4 Sequence Number (SN)

The SN describes the ordinal position of an A_PDU relative to other A_PDUs within the same data flow that are generated by a producer. Using the SN, a consumer can verify that the order of received A_PDUs is the same as the order in which the producer generated them and that an A_PDU has not been lost.

Each FuSa profile specifies SN in its own way. See 7.5 for details.

6.4.6.5 Length (LEN)

The LEN describes the length in bytes of the data over which the ICV is to be, or has been, calculated (see 6.4.6.6). Using the LEN, a consumer can verify that the length of the data being covered by the ICV is the same as the length provided by the producer.

Each FuSa profile specifies LEN in its own way. See 7.5 for details.

NOTE: The use of LEN together with requirements on trailer positioning serves as a check against the impact that a corrupted PL field or AD SIZE field can have on parsing FuSa assurance information. (Neither of these two fields are part of the ICV calculation.) Refer to DOT/FAA/TC-14/49, 5.1, for a discussion on how, for example, a corrupted length field can affect CRC error detection.

6.4.6.6 Integrity Check Value (ICV)

The ICV is a value calculated by the producer using the contents of FSPI, DataID, SN, PG data, and LEN to ensure data integrity. A consumer can verify that these parameters have not been altered since the producer generated them by comparing its calculated ICV to that generated by the producer.

Each FuSa profile specifies ICV in its own way. See 7.5 for details.

NOTE: ICV is a general term for an integrity check; use of this term emphasizes that checks other than CRCs can be employed as a part of FuSa assurance information.

6.4.7 Cybersecurity Assurance

The cybersecurity assurance information is a collection of security-related parameters that are generated by a producer and verified by a router and/or a consumer to ensure data integrity, authenticity, and, if necessary, confidentiality.

This document treats cybersecurity services as part of the black channel communication between a producer and any consumers; because of this, FuSa assurance information does not provide communication error coverage for cybersecurity assurance information.

6.4.8 Safety Cycle Time (SCT and SCT_{max})

The SCT describes the nominal period between successive transmissions by a producer of A_PDUs in a data flow, which is thus the expected nominal period between successive receptions of A_PDUs by a consumer. The related term SCT_{max} describes the maximum time that a consumer waits to receive a verified A_PDU in a data flow before determining that an unacceptable delay has occurred.

6.5 Communication Error Coverage

Table 1 provides various communication errors identified by IEC 61784-3:2024, the measures provided in IEC 61784-3:2024 and used in this document for detecting them, and the parameters described in 6.4 for achieving that detection.

Table 1 - Communication error coverage

Communication Error	Safety Measure(s)	Parameter(s) Used for Detection
Corruption	Data Integrity Assurance	FSPI, LEN, ICV
Unintended Repetition	Sequence Number	SN
Incorrect Sequence	Sequence Number	SN
Loss	Sequence Number	SN
Unacceptable Delay	Time Expectation	SCT _{max}
Insertion	Sequence Number, Connection Authentication	SN, DataID
Masquerade	Sequence Number, Connection Authentication, Data Integrity Assurance	SN, DataID, FSPI, LEN, ICV
Addressing	Connection Authentication	DataID