SAE INTERNATIONAL

SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-22 SEP2022

Issued 2021-03
Revised 2022-09

Superseding J1939-22 JUL2021

CAN FD Data Link Layer

RATIONALE

This revision provides a method for a FD.TP.CM_Abort to declare whether the Originator or the Responder session is to be aborted. The minimum data size of FD.TP transfers is corrected. The Figure 27 example is corrected. Other minor editorial changes are made throughout.

FOREWORD

This series of SAE Recommended Practices have been developed by the Truck and Bus Control and Communications Network Committee of the Truck and Bus Electrical and Electronics Steering Committee. The objectives of the committee are to develop information reports, recommended practices, and standards concerned with the requirements, design, and usage of devices that transmit electronic signals and control information among vehicle components. The usage of these recommended practices is not limited to truck and bus applications; other applications may be accommodated with immediate support being provided for construction and agricultural equipment, and stationary power systems.

These SAE Recommended Practices are intended as a guide toward standard practice and are subject to change so as to keep pace with experience and technical advances.

This data link layer is used for all SAE J1939 applications on an SAE J1939-17 physical layer.

TABLE OF CONTENTS

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**

For more information on this standard, visit
https://www.sae.org/standards/content/J1939-22_202209/

1. SCOPE

The SAE J1939 documents are intended for light-, medium-, and heavy-duty vehicles used on or off road, as well as appropriate stationary applications which use vehicle derived components (e.g., generator sets). Vehicles of interest include, but are not limited to, on- and off-highway trucks and their trailers, construction equipment, and agricultural equipment and implements.

The purpose of these documents is to provide an open interconnect system for electronic systems. It is the intention of these documents to allow electronic control units to communicate with each other by providing a standard architecture.

This particular document, SAE J1939-22, describes the data link layer using the flexible data rate as defined in ISO 11898-1, December 2015. The flexible data rate capability in CAN (commonly called CAN FD) is implemented as a transport layer in order to allow for functional safety, cybersecurity, extended transport capability, and backward compatibility with SAE J1939DA.

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	Recommended Practice for a Serial Control and Communications Heavy Duty Vehicle Network
SAE J1939-17	CAN FD Physical Layer
SAE J1939-21	Data Link Layer
SAE J1939-31	Network Layer
SAE J1939-71	Vehicle Application Layer
SAE J1939-81	Network Management
SAE J1939DA	Digital Annex

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 11898-1:2015 Road Vehicles - Controller Area Network (CAN) - Part 1: Data Link Layer and Physical Signalling

2.2.2 AUTOSAR Publications

Copies of these documents are available online at https://www.autosar.org/.

Specification of I-PDU Multiplexer AUTOSAR Classic Release R20-11

Specification of CAN Network Management AUTOSAR Classic Release R20-11

3. DEFINITIONS

Many terms and definitions are defined in SAE J1939 documents and are not repeated here. Only the additional new terms are listed here.

3.1 APPLICATION LAYER PROTOCOL DATA UNIT (A_PDU)

This SAE J1939 application layer protocol data unit contains the Parameter Group data and supporting metadata necessary for use in a D_PDU.

3.2 ASSURANCE DATA

The results of calculation for cybersecurity and/or functional safety coverage of the A_PDU (e.g., CRC).

3.3 CAN DATA FRAME

The ISO 11898-1 MAC sub-layer comprises the protocol data unit (PDU) containing the ID field (11 bit or 29 bit) and the data field (up to 64 bytes).

3.4 CLASSICAL BASE FRAME FORMAT (CBFF)

An ISO 11898-1 CAN data frame with an 11-bit identifier, a single bit rate, and a maximum data field length of 8 bytes.

3.5 CLASSICAL EXTENDED FRAME FORMAT (CEFF)

An ISO 11898-1 CAN data frame with a 29-bit identifier, a single bit rate, and a maximum data field length of 8 bytes.

3.6 C-PG PAYLOAD LENGTH

Length of the PG data including assurance data from functional safety and/or cybersecurity coverage.

3.7 DATALINK LAYER PROTOCOL DATA UNIT (D_PDU)

This SAE J1939 datalink layer protocol data unit contains one or more A_PDUs formatted for transmission by the CAN controller.

3.8 FD BASE FRAME FORMAT (FBFF)

An ISO 11898-1 CAN data frame with an 11-bit identifier, a flexible bit rate, and a maximum data field length of 64 bytes.

3.9 FD EXTENDED FRAME FORMAT (FEFF)

An ISO 11898-1 CAN data frame with a 29-bit identifier, a flexible bit rate, and a maximum data field length of 64 bytes.

3.10 LARGE MESSAGE

A large message is considered to be a PG with more than 60 data bytes or an A_PDU that doesn’t fit in a Multi-PG C-PG due to large data size and large assurance data together.

3.11 NAME

An 8-byte value as specified in SAE J1939-81 which uniquely identifies the primary function of a CA and its instance in a vehicle network.

3.12 SEGMENT

One of multiple CAN data frames used when a PG is defined with more data to be transmitted than fits in a single CAN FD frame.

4. ABBREVIATIONS

ACK	Acknowledgment[1]
ACKM	Acknowledgement PG
A_PDU	Application Layer Protocol Data Unit
AppPI	Application Protocol Indicator
BAM	Broadcast Announce Message
BRS	Bit Rate Switch (refer to ISO 11898-1:2015)
CA	Controller Application (refer to SAE J1939-81)
CAN	Controller Area Network (refer to ISO 11898-1)
CAN FD	Controller Area Network - Flexible Data Rate
CAN ID	Controller Area Network Identifier
CBFF	Classical Base Frame Format (refer to ISO 11898-1:2015)
CEFF	Classical Extended Frame Format (refer to ISO 11898-1:2015)
CM	Connection Management
C-PG	Contained Parameter Group
CPGN	Contained Parameter Group Number
CRC	Cyclic Redundancy Check
CS	Cybersecurity
CTS	Clear to Send
DA	Destination Address
DLC	Data Length Code
DP	Data Page
D_PDU	Datalink Layer Protocol Data Unit
DT	Data Transfer
EDP	Extended Data Page
EOF	End of Frame (refer to ISO 11898-1:2015)

[1] In this document, ACK refers to the Acknowledgement PG with the control byte set to a value indicating positive acknowledgement.

EOMS	End of Message Status
FBFF	Flexible Data Rate Base Frame Format (refer to ISO 11898-1:2015)
FD	Flexible Data Rate
FDF	FD Format Indicator Bit (refer to ISO 11898-1:2015)
FEFF	Flexible Data Rate Extended Frame Format (refer to ISO 11898-1:2015)
FS	Functional Safety
GE	Group Extension
ID	Identifier
IDE	Identifier Extension Bit (refer to ISO 11898-1:2015)
LSB	Least Significant Byte or Least Significant Bit
MF	Manufacturer
MSB	Most Significant Byte or Most Significant Bit
NA	Not Allowed
NACK	Negative Acknowledgment[2]
P	Priority
PDU	Protocol Data Unit
PF	PDU Format
PG	Parameter Group
PGN	Parameter Group Number
PS	PDU Specific
RTR	Remote Transmission Request
RTS	Request to Send
SA	Source Address
SOF	Start of Frame bit (refer to ISO 11898-1:2015)
SPN	Suspect Parameter Number
SRR	Substitute Remote Request
TP	Transport Protocol

[2] In this document, NACK refers to the Acknowledgement PG with the control byte set to a value indicating negative acknowledgement.

T_PDU Transport Layer Protocol Data Unit

T_h Hold Time

T_r Response Time

5. OPERATING PRINCIPLES/OVERVIEW

This document endeavors to maintain compatibility with all Parameter Groups in SAE J1939. However, the manner by which Parameter Groups are transmitted differs from SAE J1939-21. SAE J1939-22 is specified to maximize the use of the CAN FD network bandwidth, provide integral support for functional safety and cybersecurity measures, and provide improved large data transport services. Consequently, some SAE J1939-21 messaging services are not permitted on SAE J1939-22 networks and some SAE J1939-21 messaging services have limited use on SAE J1939-22 networks.

5.1 Maximize Use of CAN FD Network Bandwidth

- All SAE J1939-22 messages shall use FBFF or FEFF data frames with ISO 11898-1 BRS set so that the frame bit rate switching is used.

- CEFF data frames, per SAE J1939-21, shall not be transmitted on an SAE J1939-22 network, except for the following two exceptions. The first exception allows the Address Claimed PG to be sent as a single CEFF data frame, per SAE J1939-21. The second exception allows a device to transmit CEFF data frames (per SAE J1939-21) only to determine if the network is an SAE J1939-22 network; CEFF frames shall be ceased once a device determines it is connected to an SAE J1939-22 network.

- CBFF data frames, per SAE J1939-21, shall not be transmitted on an SAE J1939-22 network. The FBFF CAN ID structure for SAE J1939-22 is incompatible with CBFF CAN ID structure for SAE J1939-21.

- The FEFF data frames match the SAE J1939-21 method for addressing.

- SAE J1939 PGs shall not be sent using a single FEFF data frame, in a manner similar to a single CEFF data frame in SAE J1939-21. This is disallowed because not all PGs have a fixed data length; thus it is impossible to identify the end of valid data and the start of padding bytes for some PGs.

- SAE J1939 PGs shall be sent using the Multi-PG transport mechanism and the FD Transport Protocol.

- The Address Claimed PG shall not be sent using the Multi-PG transport mechanism; it shall be sent as either a single FEFF data frame (per J1939-22) or a single CEFF data frame (per SAE J1939-21).

- Non-SAE J1939 defined Transport Protocols shall use FBFF data frames (D_PDU3) with the applicable AppPI. Non-SAE J1939 defined Transport Protocols may also use the Multi-PG transport mechanism or FD Transport Protocol with any SAE J1939 assigned PGs for those non-SAE J1939 protocols, such as PGNs 512 and 52480. The ISO15765 defined Transport Protocol may use either FBFF data frames with AppPI defined in Table 6 or FEFF data frames with the ISO15765 assigned PGNs in SAE J1939DA without using the Multi-PG or FD Transport Protocol defined in this document. This exception is made because the ISO FD-capable transport method was published prior to the methods defined in this document.

- Multi-PG transport mechanism provides a method to combine multiple PGs into a single FEFF data frame thus optimizing bandwidth. This method is analogous to an AUTOSAR Container-PDU. These requirements apply to all PG Data Pages. The FEFF Multi-PG transport mechanism allows Multi-PG data frames to be sent destination specific or globally. The FBFF Multi-PG transport mechanism only allows Multi-PG data frames to be sent globally.

- When sending a Destination Specific FEFF Multi-PG data frame, all the included PGs must be Destination Specific (PDU1) PGs directed to the same Destination Address specified in the CAN identifier field. Globally broadcast (PDU2) PGs shall not be included in a Destination Specific FEFF Multi-PG data frame.

- The PS field in the CPGN for an A_PDU1 C-PG shall not include a Destination Address; instead, the PS field shall be set to 0. This is for AUTOSAR compatibility since AUTOSAR message routing (i.e., PG identification) is controlled by the contents of the CAN Header only. The Destination Address for the A_PDU1 C-PG shall be derived from the Multi-PG message address. See 6.5.3.6.2 for details.

- PGs shall be ordered within the Multi-PG message from oldest to newest where the first PG is the oldest and the last is more recent. Extracting the PGs should also be done in chronological order. See 6.5 for details.

5.2 Integral Support for Functional Safety and Cybersecurity

- The Multi-PG transport mechanism allows for functional safety and/or cybersecurity content for each PG contained in the data frame.

- The FD Transport Protocol allows for functional safety and/or cybersecurity content for the transmitted PG.

5.3 Improved Large Data Transport Services

- The FD Transport Protocol is capable of significantly larger data transmission sizes and provides for up to eight concurrent destination specific transfers and up to four concurrent broadcast transfers.

- The SAE J1939-21 Transport Protocol shall not be used on an SAE J1939-22 network; specifically, the Transport Protocol - Data Transfer PG (TP.DT) (PGN 60160) and the Transport Protocol - Connection Mgmt PG (TP.CM) (PGN 60416) shall not be sent by any CAN controller on an SAE J1939-22 network segment.

- The FD Transport Protocol shall only be used when the data size of the transported PG, including any assurance data, is too large for the maximum size of a C-PG in a Multi-PG data frame.

5.4 AUTOSAR Compatibility

This document intends to achieve compatibility with AUTOSAR at the time of publication. The CAN wake feature of AUTOSAR NM may use FBFF with the BRS disabled for hardware compatibility reasons.

6. TECHNICAL REQUIREMENTS

This document provides guidelines for the reliable transfer of data across the SAE J1939-17 physical layer. This document provides methods to package multiple SAE J1939 messages, transport large data sets, and has provisions to protect content for functional safety and cybersecurity.

Hardware that does not conform to SAE J1939-17 shall not be used on an SAE J1939-22 network to avoid disruption of network operation.

This document is organized in layers by means of protocols and services as shown in Figures 1 and 2. These figures show a flow of data through the layers and are not a design specification for implementation but rather a conceptual model to understand this document's organization. This document covers the content within the blue dashed outlines.

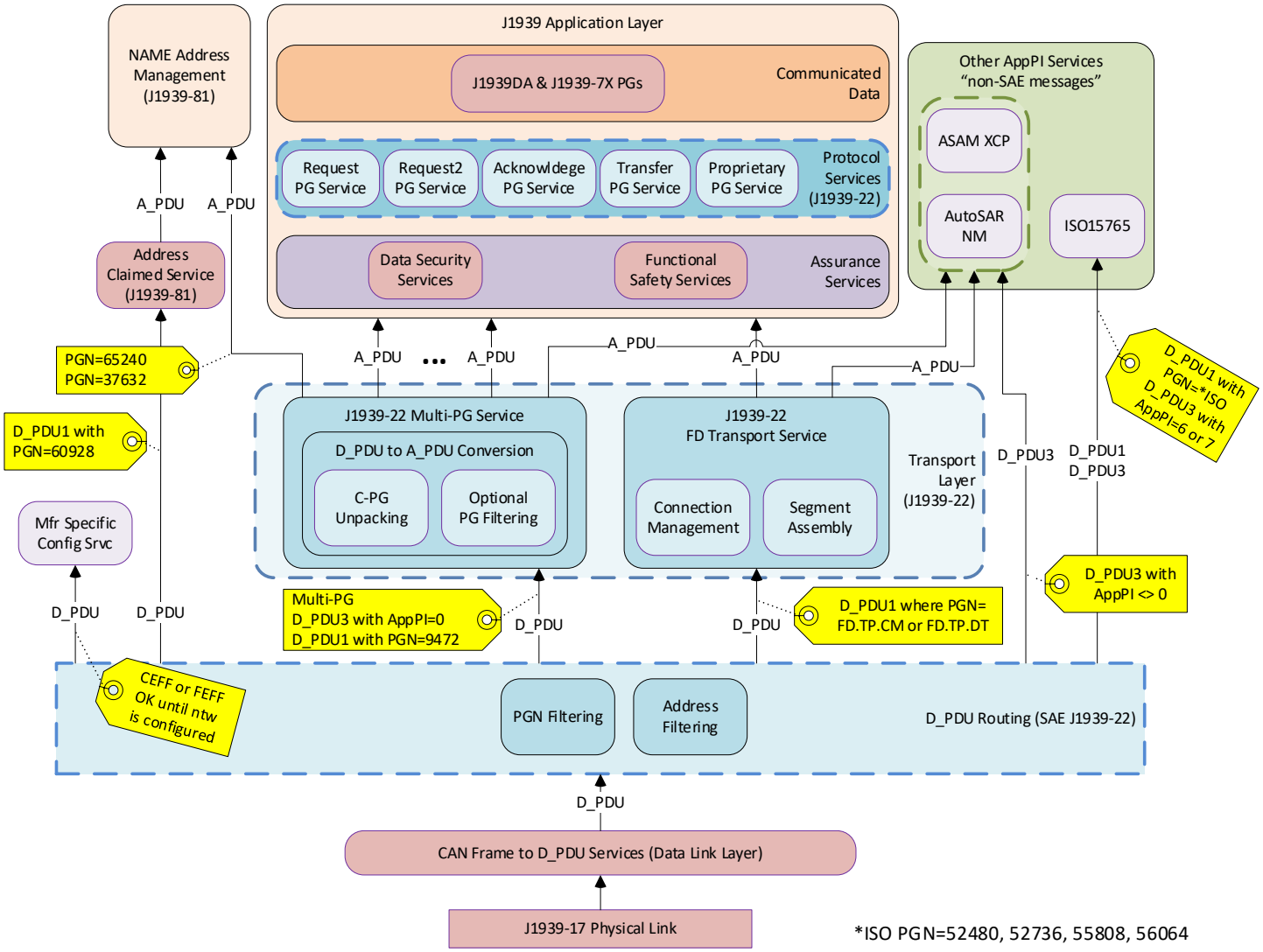


Figure 1 - Receive model

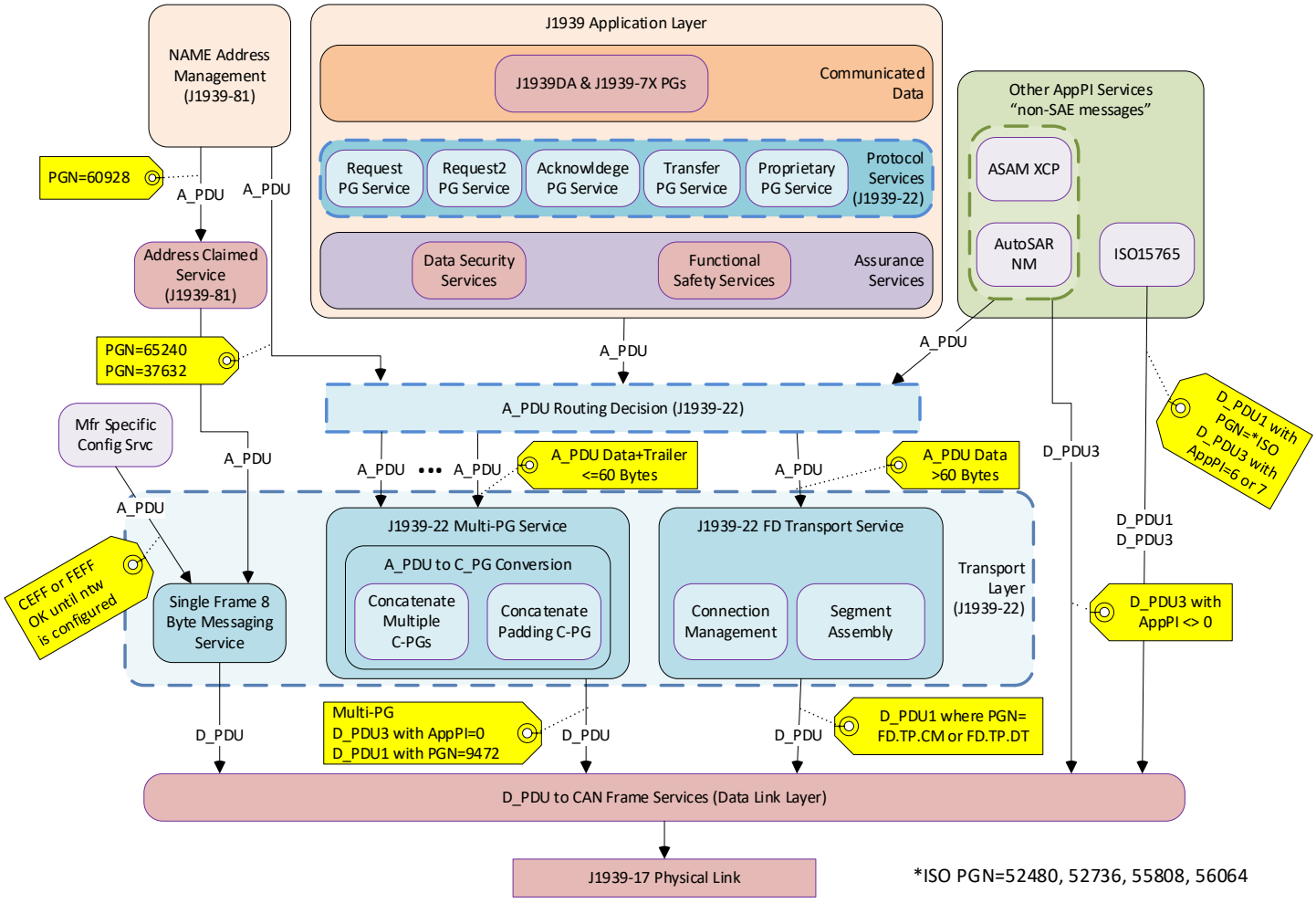


Figure 2 - Transmit model

References to sections related to terms in the figures:

- A_PDU is explained in 6.1
- D_PDU is explained in 6.2
- Multi-PG is explained in 6.5
- FD Transport Service is explained in 6.6
- Request Service is explained in 6.10.1
- Request2 Service is explained in 6.10.2
- Acknowledge Service is explained in 6.10.3
- Transfer Service is explained in 6.10.5

6.1 Application Protocol Data Unit (A_PDU)

In SAE J1939-21, there is only one Application PDU (A_PDU) per CAN data frame. In SAE J1939-22, multiple A_PDUs may be combined within a single Multi-PG facilitated by the larger payload capability of CAN FD. Additionally, some Parameter Group (PG) definitions require more space than is supported by a single CAN FD data frame to send the corresponding data. Flexible Data Transport Protocol (FDTP) messages are used to transport PGs with more data than fits in a single CAN FD data frame.

The attributes of Application Protocol Data Unit (A_PDU) data include application data and can also include identification data, functional safety data, and/or cybersecurity data. Table 1 shows some common data attributes in no particular order. Individual implementations may include additional data, as needed.

Table 1 - Application protocol data attributes

Attribute	Transmit	Receive	Reference
PGN value	Include	Include	6.1.3
PG data and PG size	Include	Include	6.5.3.2
Functional safety assurance data and FS size (if applicable)	Include	Include	6.5.3.6.1
Cybersecurity assurance data and CS size (if applicable)	Include	Include	6.5.3.6.1
Destination Address (if A_PDU1)	Include	See Note 1	6.3.1.5.1
Source Address (if applicable)	See Note 2	Include	6.3.3.1
Priority	Include	See Note 3	6.3.1.1
Transmit latency constraints	Include	N/A	6.5.4

Notes:
1. For example, a gateway would need this passed up to the application or perhaps an ECU which contains more than one Controller Application (multiple source addresses).
2. Necessary for an ECU which contains more than one Controller Application (multiple source addresses).
3. Priority shall not be used as a filter and thus has no reason to be passed on to the application.

6.1.1 A_PDU1 Format

The A_PDU1 Format is used for destination specific Parameter Groups.

6.1.2 A_PDU2 Format

The A_PDU2 Format is used for global Parameter Groups.

6.1.3 Parameter Group Number (PGN)

The Parameter Group Number is a unique numeric value assigned to each SAE J1939 Parameter Group that is used to identify an SAE J1939 PG. The numeric value is derived from four individual component values: Extended Data Page (EDP), Data Page (DP), PDU Format (PF), and PDU Specific (PS). The PGN is expressed as a 24-bit value in SAE J1939 documentation and when identifying a Parameter Group Number (PGN) in the data field of a CAN data frame. Figure 3 illustrates the constituent component bit fields, placement, and transmission order.

The procedure for converting the identifier fields to a 24-bit value is shown in the “placement” illustration in Figure 3:

- The six most significant bits are set to zero.
- EDP, DP, and PF are copied into the next 10 bits.
- Lastly, if the PF value is less than 240 ($F0_h$), then the least significant byte of the PGN is set to zero. Otherwise, it is set to the PS value.

When identifying a Parameter Group Number (PGN) in the data field of a CAN data frame, the 24-bit value is sent LSB first, middle byte second, and MSB third, as illustrated by the “Transmission Order” illustration in Figure 3.

See Table 2 to correlate the constituent components to the PGN ranges and types. Note that not all 2^{17} (or 131072) combinations are available for assignment using the conventions specified in this document. The conventions specified yield 8672 PGNs (calculated as: 2 pages * [240 + (16*256)] = 8672 PGs). Refer to SAE J1939DA for the complete list of assigned PGNs. See 6.3.1 for further description of the identifier fields.

Data Definition

EDP	DP	PF								PS							
b17	b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
MSb																	LSb

Placement

MSb							LSb	MSb							LSb	MSb							LSb
Byte 3								Byte 2								Byte 1							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
0	0	0	0	0	0	b17	b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0

Transmission Order

MSb							LSb	MSb							LSb	MSb							LSb
Byte 1								Byte 2								Byte 3							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
b7	b6	b5	b4	b3	b2	b1	b0	b15	b14	b13	b12	b11	b10	b9	b8	0	0	0	0	0	0	b17	b16

Figure 3 - Parameter group number transmission order

Table 2 - Parameter group number examples

EDP	DP	PF	PS	PGN	PGN	Number of Assignable PGNs	Cumulative Number of PGNs	SAE or Manufacturer Assigned
Bit 2	Bit 1	Bits 8 to 1	Bits 8 to 1	Dec	Hex			
0	0	0 - 238	0	0 - 60928	000000_h - $00EE00_h$	239	239	SAE
0	0	239	0	61184	$00EF00_h$	1	240	MF
0	0	240 - 254	0 - 255	61440 - 65279	$00F000_h$ - $00FEFF_h$	3840	4080	SAE
0	0	255	0 - 255	65280 - 65535	$00FF00_h$ - $00FFFF_h$	256	4336	MF
0	1	0 - 238	0	65536 - 126464	010000_h - $01EE00_h$	239	4575	SAE
0	1	239	0	126720	$01EF00_h$	1	4576	MF
0	1	240 - 254	0 - 255	126976 - 130815	$01F000_h$ - $01FEFF_h$	3840	8416	SAE
0	1	255	0 - 255	130816 - 131071	$01FF00_h$ - $01FFFF_h$	256	8672	MF

Parameter group assignments do not have fixed boundaries between fast and slow types but they do have fixed boundaries between PDU1 and PDU2 types. These boundaries are shown in Table 3. Boundary X indicates the separation between PDU1 Fast and PDU1 Slow for Data Page 0. PGN assignments are made upon Request where the fast PGN assignments increase in numerical value and the slow PGN assignments decrease in numerical value. Eventually the two will meet at Boundary X. Likewise, Boundary Y denotes the separation between PDU2 Fast and PDU2 Slow for Data Page 0. Boundary X1 and Y1 represent the same concept for Data Page 1 but the slow/fast boundaries are unlikely to be the same. See 6.2.1 and 6.2.2 for details about PDU Formats and assignment strategy.

Table 3 - SAE J1939 parameter group number template

EDP	DP	PF	PS	Parameter Group Definition	TP Segmented	PGN
0	0	0	DA	PDU1 Fast Format - 100 ms or less	Not Allowed	0
0	0	1	DA		Not Allowed	256
Boundary X				↓		
				↑		
0	0	238	DA	PDU1 Slow Format - greater than 100 ms	Allowed	60928
0	0	239	DA	PDU1 Format - Proprietary A	Allowed	61184
0	0	240	0	PDU2 Fast Format - 100 ms or less	Not Allowed	61440
0	0	240	1		Not Allowed	61441
Boundary Y				↓		
				↑		
0	0	254	254		Not Allowed	65278
0	0	254	255	PDU2 Slow Format - greater than 100 ms	Allowed	65279
0	0	255	0 - 255	PDU2 Format - Proprietary B	Allowed	65280 - 65535
0	1	0	DA	PDU1 Fast Format - 100 ms or less	Not Allowed	65536
0	1	1	DA		Not Allowed	65792
Boundary X1				↓		
				↑		
0	1	238	DA	PDU1 Slow Format - greater than 100 ms	Allowed	126464
0	1	239	DA	PDU1 Format - Proprietary A2	Allowed	126720
0	1	240	0	PDU2 Fast Format - 100 ms or less	Not Allowed	126976
0	1	240	1		Not Allowed	126977
Boundary Y1				↓		
				↑		
0	1	254	254		Not Allowed	130814
0	1	254	255	PDU2 Slow Format - greater than 100 ms	Allowed	130815
0	1	254	0 - 255	PDU2 Format - Proprietary B	Allowed	130816 - 131071

LEGEND:
EDP: Extended Data Page
PF: PDU Format
DA: Destination Address
DP: Data Page
PS: PDU Specific
PGN: Parameter Group Number
TP Segmented: Transport Protocol for large messages

6.1.4 Services for A_PDU Routing

The services are based on the PG size + FS size + CS size specified for the A_PDU. The decision flow is depicted in Figure 4. If the additive size is less than or equal to 60 bytes then a Multi-PG service shall be used. See 6.5 for Multi-PG functional details. If the additive size is greater than 60 data bytes, the FD Transport Protocol (FD.TP) is used. See 6.6 for FD Transport Protocol functional details. The FD Transport Protocol is used to transmit the A_PDU data as a series of segmented CAN data frames. For flow control, the FD Transport Protocol Connection Management (FD.TP.CM) PG is used to set up and close out the communication of the segmented PG data. The FD Transport Protocol Data Transfer (FD.TP.DT) PG is used to communicate the data in a series of CAN data frames (segments) containing the segmented data. Additionally, the FD Transport Protocol provides flow control and handshaking capabilities for destination specific transfers using Request to Send (RTS) and Clear to Send (CTS) messages.

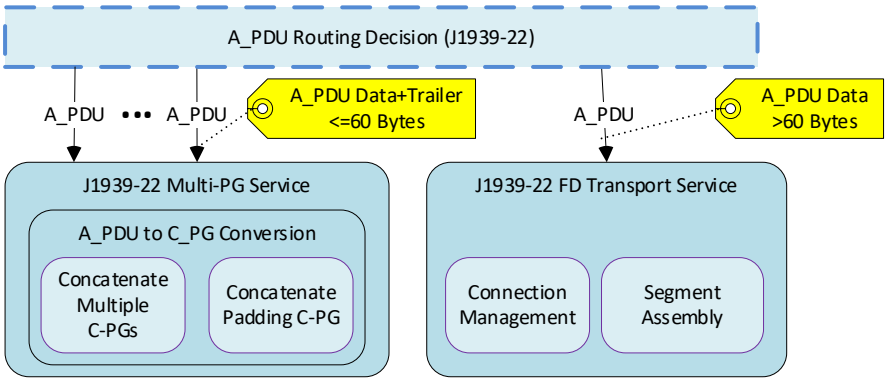


Figure 4 - A_PDU routing service

6.2 Datalink Layer Protocol Data Unit (D_PDU)

The available D_PDU Formats are illustrated in Figure 5. Two D_PDU Formats are defined when representing a PG with a FEFF CAN ID: D_PDU1 Format (PS = DA) and D_PDU2 Format (PS = GE). The D_PDU1 Format allows for direction of the CAN data frame to a specific DA (device). The D_PDU2 Format can only carry A_PDUs that are not destination specific. The third format, D_PDU3, is defined for use when FBFF CAN IDs are used and is also not destination specific. These formats are used when sending an A_PDU (like Address Claimed), for the Multi-PG CAN ID, and for segmented transport.

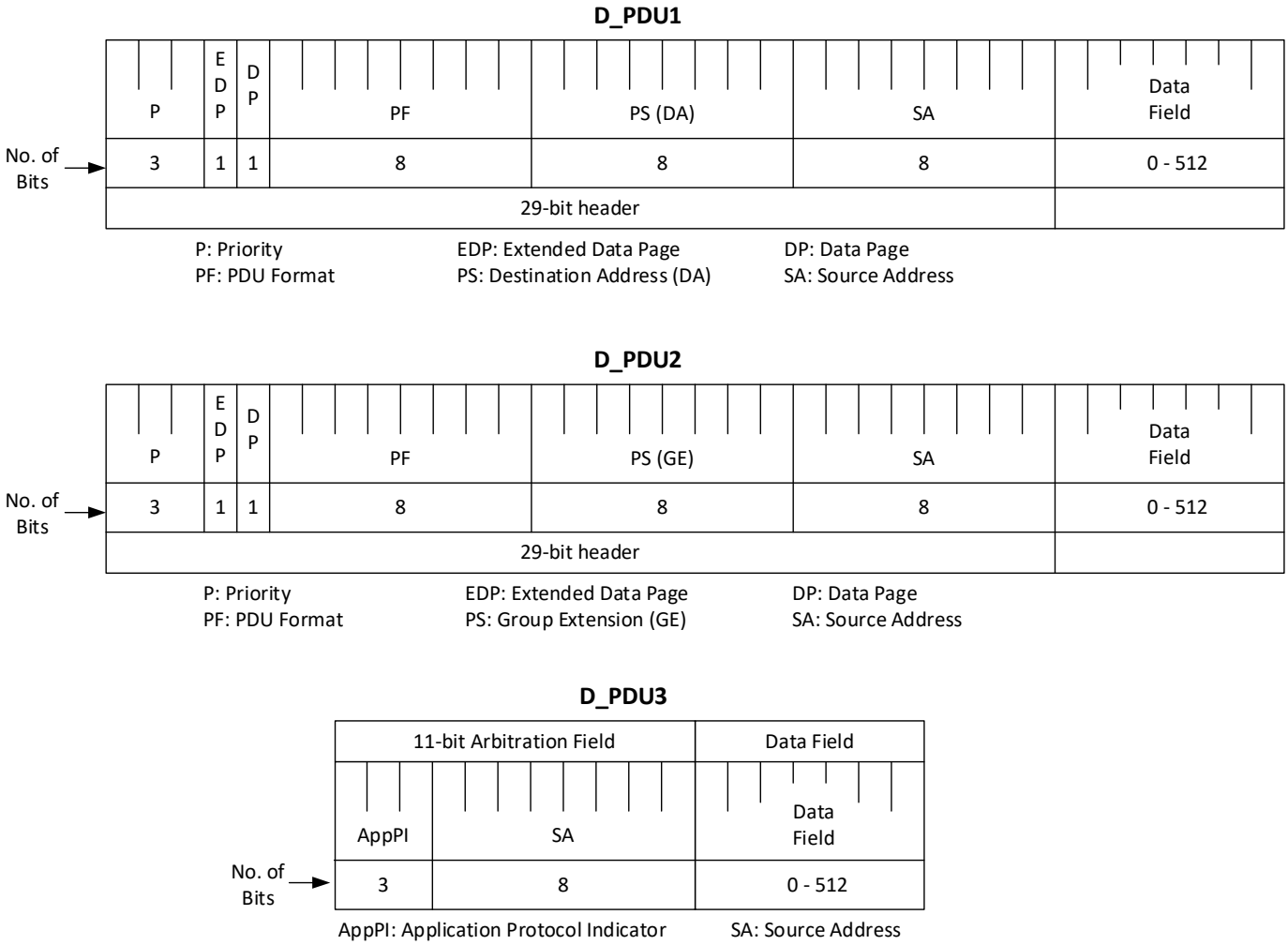


Figure 5 - D_PDU formats

6.2.1 D_PDU1 Format

This format allows applicable PGs to be sent to either a specific or global DA. The PS field contains a Destination Address (DA). The D_PDU1 Format can be used for content Requested by a CA or can be sent unsolicited.

The D_PDU1 Format is determined by the PF field. A PF field value between 0 to 239 is defined as a D_PDU1 Format. The formatting of a D_PDU1 message is illustrated in Figure 5. Also see Figure 6.

PGs requiring a DA and minimal latency are assigned starting with PF = 0 and incrementing to larger values. The term used for these is “PDU1 Fast.”

PGs requiring a DA where latency is not critical are assigned starting with PF = 238 and decrementing to smaller values. The term used for these is “PDU1 Slow.” The junction where PDU1 Slow meets PDU1 Fast is shown in Table 3 as boundary X.

Two D_PDU1 PGs, with EDP = 0 and DP = 0 or 1, are assigned for proprietary use. The Proprietary A PGN is 61184 and the Proprietary A2 PGN is 126720. See 6.10.4 for descriptions of the Proprietary A and Proprietary A2 PGs.

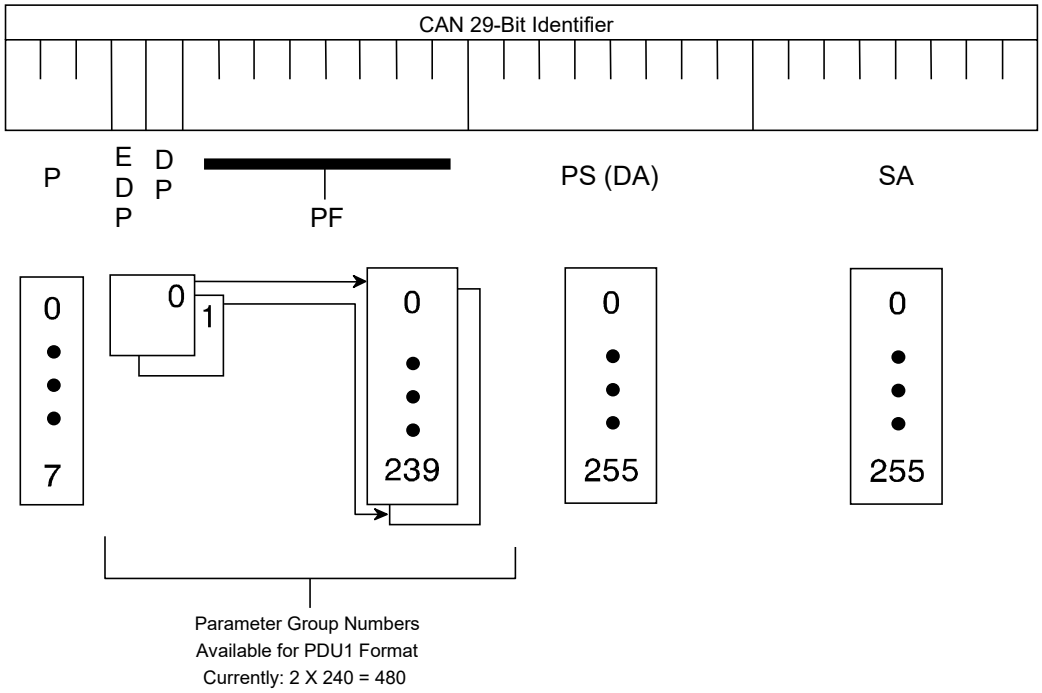


Figure 6 - D_PDU1 format

6.2.2 D_PDU2 Format

This format can only be used to communicate PGs to the global DA; the global DA is implied by the D_PDU2 Format and does not appear in the arbitration field. The D_PDU2 Format can be used for Requested or unsolicited content. Selection of D_PDU2 Format, at the time a PGN is assigned, prevents that PG from ever being able to be directed to a specific DA. The PS field contains a Group Extension (see 6.3.1.5.2).

The D_PDU2 Format has a PF field from 240 to 255 (see Table 3). The D_PDU2 Format is illustrated in Figure 5. Also see Figure 7.

The PGNs of messages that are sent at fast update rates (generally less than 100 ms) start with PF = 240 and increment in value.

The PGNs of messages that are only Requested, sent on change, or sent at slow update rates (generally greater than every 100 ms) start with PF = 254 and decrement in value.

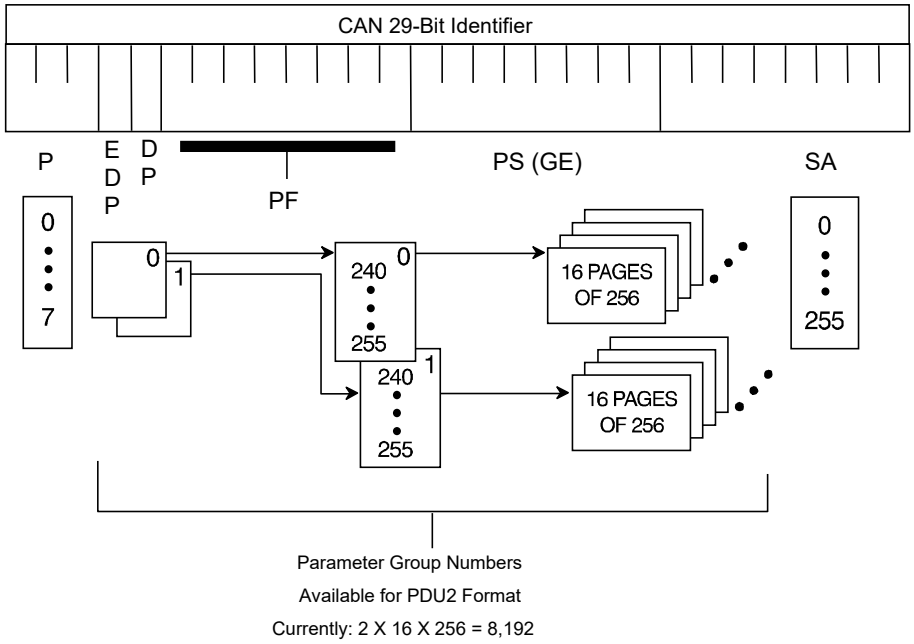


Figure 7 - D_PDU2 format

6.2.3 D_PDU3 Format

This format can only be used to communicate Multi-PG or Proprietary content globally; the global DA is implied by the D_PDU3 Format and does not appear in the arbitration field. Other protocols may use an 11-bit identifier field as well but are not defined in this document other than how to set the AppPI to denote which protocol is in use. The Source Address defines the sender of the message; so for a given protocol, there is only 1 proprietary CAN ID and 1 Multi-PG CAN ID which may be used in the D_PDU3 format for each source address. Figure 8 shows a representation of the bit positions and Table 6 indicates the full AppPI enumeration.

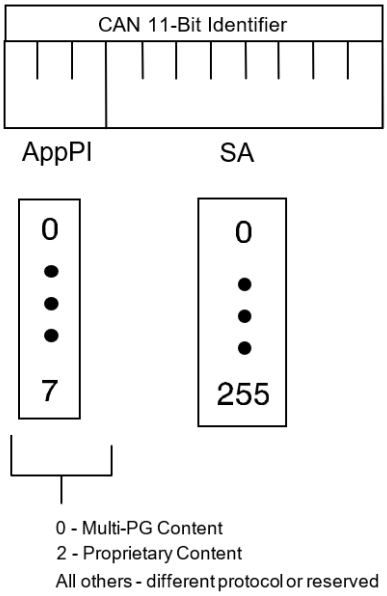


Figure 8 - D_PDU3 format

6.3 D_PDU Fields

The applications and/or network layer provide a string of information that is assimilated into a data link layer Protocol Data Unit (D_PDU). The D_PDU provides a framework for organizing the information that is key to each CAN data frame that is sent. The SAE J1939-22 FEFF D_PDU consists of seven fields: (1) P, (2) EDP, (3) DP, (4) PF, (5) PS (which can be a Destination Address or Group Extension), (6) SA, and (7) Data. The SAE J1939-22 FBFF D_PDU consists of three fields: (1) AppPI, (2) SA, and (3) Data. The fields are packaged into a CAN data frame and sent over the physical media to other network devices.

Some of the CAN data frame fields have been intentionally left out of the SAE J1939 D_PDU definition because they are defined entirely by ISO 11898-1. Fields that are controlled in this manner include the SOF, RRS, IDE, FDF, r0, BRS, ESI, CRC, ACK, and EOF fields. They are not forwarded to the application.

The D_PDU fields illustrated in Figures 9 and 10 are defined in the subsequent sections.

6.3.1 FEFF D_PDU Fields

6.3.1.1 Priority (P)

The CAN data frame priority shall be per ISO 11898-1. The value within the CAN ID field determines the priority. A low value (the identifier being all zeros) has a high priority, while the largest CAN ID has the lowest priority (the identifier being all ones).

Three bits are used by the application layer to optimize message latency for transmission onto the bus only. They shall be masked off by the receiver (ignored). The priority of any FEFF data frame can be set from highest, 0 (000_b), to lowest, 7 (111_b). The default for all control-oriented messages is 3 (011_b). The default for all other informational, proprietary, Request, and ACK messages is 6 (110_b). This permits the priority to be raised or lowered in the future as new PGNs are assigned and bus traffic changes. A recommended value is assigned to each PG when the PGN is assigned. However, the Priority field should be configurable to allow for network tuning by the OEM should the need arise.

NOTE: Undesired bus arbitration can occur between contending FBFF and FEFF frames. An FBFF frame will nearly always win bus arbitration over an FEFF frame because the first three CAN ID bits of most FBFF frames will be “000” which contends against the first three bits of the FEFF frame which are the Priority bits. When bus arbitration occurs between an FBFF frame and an FEFF frame with a Priority other than zero, then the FBFF frame will always win bus arbitration. When bus arbitration occurs between an FBFF frame and an FEFF frame with a “0” Priority, then the frame winning bus arbitration will depend on the SA of the FBFF frame and the PGN in the FEFF frame.

6.3.1.2 Extended Data Page (EDP)

The EDP is used in conjunction with the DP to determine the structure of the CAN ID field. See Table 4 for the defined meaning of the EDP and DP combinations. Future definitions with EDP set to 1 could expand the PDU Format field, define new PDU Formats, or increase the address space. When messages using these values are defined by the SAE J1939 committee, handling rules will be specified in a future version of the SAE J1939 documents.

6.3.1.3 Data Page (DP)

The DP is used in conjunction with the EDP to determine the structure of the CAN ID of the CAN data frame. With the EDP set to 0, the DP selects between page 0 and page 1 of PGN descriptions as shown in Table 4. Also see Table 3 to see the SAE J1939 Parameter Group Number template.

Table 4 - Definition of extended data page and data page use

Extended Data Page (bit 25) CAN ID (bit 25)	Data Page (bit 24) CAN ID (bit 24)	Description
0	0	SAE J1939 page 0 PGNs
0	1	SAE J1939 page 1 PGNs
1	0	SAE J1939 reserved
1	1	Reserved

6.3.1.4 PDU Format (PF)

The PDU Format is an 8-bit field that defines whether a PG has a PDU1 or PDU2 Format, and is one of the fields used to identify the PGN. When the PF value for a PG is below 240, then the PG has a PDU1 Format—a format that supports specifying the Destination Address for each instance of the PG. When the PF value is 240 to 255, then the PG has a PDU2 Format—a format that does not support any Destination Addressing.

6.3.1.5 PDU Specific (PS)

The PDU Specific field is an 8-bit field and its definition depends upon the PF field. Depending on the PF field, it can be a Destination Address (DA) or a Group Extension (GE). If the value of the PF field is below 240, then the PS field is a DA. If the value of the PF field is 240 to 255, then the PS field contains a GE value. See Table 5 for the PDU ranges. See Table 3 for the range of PGNs.

Table 5 - PDU specific

	PDU Format Field	PDU Specific Field
PDU1 Format	0 to 239	Destination Address
PDU2 Format	240 to 255	Group Extension

6.3.1.5.1 Destination Address (DA)

The PS field is interpreted as a Destination Address value when the PF value is 0 to 239. The Destination Address value identifies the specific address to which the message is being sent. Note that any other device should ignore this message. The global DA (255) as the Destination Address, requires all devices to listen and respond accordingly as message recipients.

6.3.1.5.2 Group Extension (GE)

The PS field is interpreted as a Group Extension value when the PF value is 240 to 255. The GE field serves as the least significant byte of the PGN number providing for 256 unique PGN values for a given PF value.

6.3.2 FBFF D_PDU Field

6.3.2.1 Application Protocol Indicator (AppPI)

The Application Protocol Indicator is a 3-bit enumeration defining how to interpret the contents of the data field. This field is only used in the identifier field of FBFF Frames as the first three bits (bits 28, 27, and 26). Bit 28 is the most significant bit of the three. See 6.2.3 and 6.4.2 for context. This document discusses usage of messages formatted using an AppPI value of 000_b and 010_b. Other values of AppPI can exist on the same datalink but are not explained in this document. The assigned values of AppPI are shown in Table 6.

Table 6 - Application protocol indicator

Value	Definition
000_b	Multi-PG
001_b	AUTOSAR CAN-NM (wake)
010_b	Proprietary
011_b	XCP
100_b	Reserved
101_b	Reserved
110_b	ISO15765 Functional Addressing
111_b	ISO15765 Physical Addressing

6.3.3 Common D_PDU Fields

6.3.3.1 Source Address (SA)

The Source Address field is 8 bits long. There shall only be one device on the network with a given SA. Therefore, the SA field assures that the CAN ID is unique. Address management and allocation is detailed in SAE J1939-81. Procedures are defined in SAE J1939-81 to prevent duplication of SAs. Refer to SAE J1939DA for preferred source address assignments.

6.3.3.2 D_PDU Data Field

The Data Field contains the payload of the D_PDU. The content is dependent upon the CAN ID. The byte length of the D_PDU Data field is required to be one of the valid lengths specified by the CAN Data Length Code (DLC), as described in ISO 11898-1.

The DLC indicates pre-defined sizes for data fields lengths for CAN FD of 0, 1, 2, 3, 4, 5, 6, 7, 8, 12, 16, 20, 24, 32, 48, and 64 bytes. The data field is required to be one of these defined valid lengths.

The DLC should be set to a code indicating a data field length that is greater than or equal to the application data field length. Unless specified otherwise, the unused bytes shall be padded with AA_h (alternating bits of 1 and 0) when the application data does not completely fill the specified message length. This padding value is selected in order to minimize the insertion of stuff bits.

6.4 Frame Format

All devices shall use FBFF and FEFF frames to transmit the messages defined in this document. Devices shall tolerate the reception of FBFF, FEFF, and CEFF frames. CEFF frames are tolerated for network configuration upon startup and for Address Claimed messages only. ISO 11898-1 specifies four frame formats (D_PDUs): Classical Base Frame Format (CBFF) and flexible data rate Base Frame Format (FBFF), which use 11-bit CAN IDs; and Classical Extended Frame Format (CEFF) and flexible data rate Extended Frame Format (FEFF), which use 29-bit CAN IDs.

The CAN specification referenced throughout this document is ISO 11898-1:2015. It should be noted that when there are differences between the ISO 11898-1 specification and this document, then this document is the guiding document. This document does not use all of the functions defined in ISO 11898-1.

Figure 9 specifies the use of identifier bits ID0 through ID28 in the arbitration field of data frames in the FEFF format. Figure 10 specifies the use of identifier bits ID18 through ID28 in the arbitration field of data frames in the FBFF format. The control field bits are unchanged from the ISO 11898-1 definition for either frame type.

6.4.1 SAE J1939 Message Format (Mapped to ISO 11898-1 Data Frames in FEFF Format)

The FEFF CAN ID field, shown in Figure 9, is divided into six fields. These fields are assimilated from information provided by the application and are identical to specifications given in SAE J1939-21. The fields specified in 6.3 are:

- Priority (P)
- Extended Data Page (EDP)
- Data Page (DP)
- PDU Format (PF)
- PDU Specific (PS, which can be a Destination Address or Group Extension)
- Source Address (SA)

ISO 11898-1 specifies that the data field is byte-wise scalable from 0 to 64 bytes. Byte 1's most significant bit is the first bit sent and follows directly after the control field. Byte 64's least significant bit is the last data bit of the data field and is followed by the CRC Field.

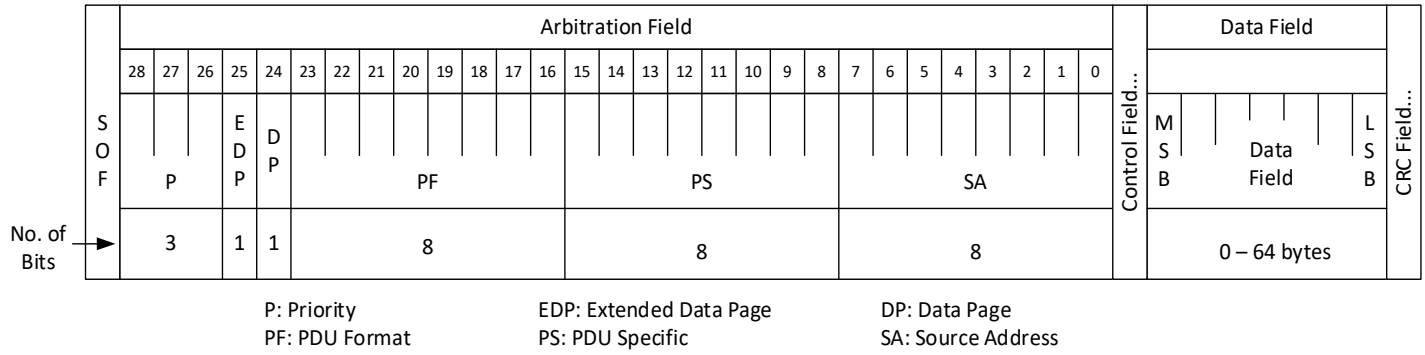


Figure 9 - 29-bit identifier layout

6.4.2 SAE J1939 Message Format (Mapped to ISO 11898-1 Data Frames in FBFF Format)

The FBFF CAN ID field, shown in Figure 10, is divided into two fields. These fields are assimilated from information provided by the application. The fields specified in 6.3 are:

- Application Protocol Indicator (AppPI)
- Source Address (SA)

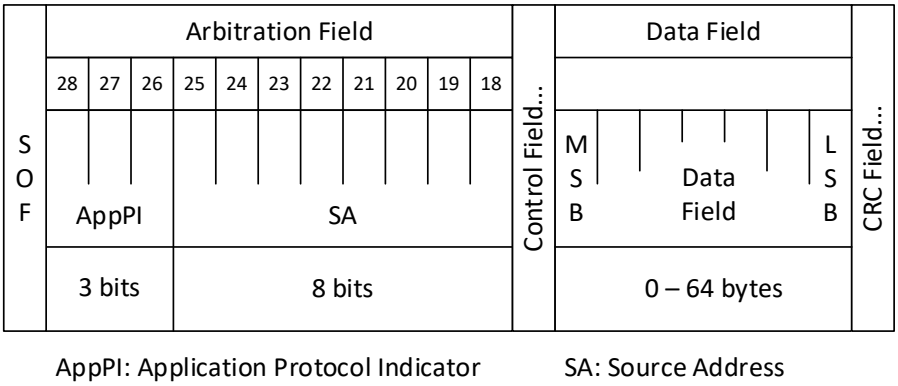


Figure 10 - 11-bit identifier layout

6.4.3 Support of CBFF and CEFF

Data frames in the CEFF format shall not be transmitted on an SAE J1939-22 network, except for the following two exceptions. The first exception allows the Address Claimed PG to be sent as single CEFF data frame, per SAE J1939-21. The second exception allows a device to transmit CEFF data frames (per SAE J1939-21) only to determine if the network is an SAE J1939-22 network. CEFF frames shall be ceased once a device determines it is connected to an SAE J1939-22 network.

CBFF data frames, per SAE J1939-21, shall not be transmitted on an SAE J1939-22 network. The content in the first 3 bits of the FBFF CAN ID has been defined in SAE J1939-22 differently from those same bits for the CBFF CAN ID defined in SAE J1939-21.

NOTE: It is recognized that controllers on existing SAE J1939-21 networks support CEFF and CBFF frame formats. These are not compatible with the SAE J1939-22 message structure which defines payloads larger than 8 bytes. It is also understood that many software stacks (particularly AUTOSAR compliant ones) will not expose the difference between messages mapped to CBFF/CEFF and FBFF/FEFF data frames and thus messages that are unique at the datalink layer are no longer unique at the application layer. For example, this is particularly important in the 11-bit identifier case where the first 3 bits in SAE J1939-21 are defined as priority bits but in SAE J1939-22 these bits are defined as an Application Protocol Indicator. So a message produced in SAE J1939-21 (CBFF) format but interpreted in an SAE J1939-22 (FBFF) format will not be interpreted correctly in most cases (unless the priority happened to be set as 010_b which is the proprietary identifier).

6.5 Multi-PG Protocol

Multi-PG protocol provides a transport mechanism to carry multiple SAE J1939 PGs in a single CAN FD data frame. Each PG, together with its Header content, included in the Multi-PG is referred to as a contained Parameter Group (C-PG). The C-PG format maintains the SP to PG relationship regardless of the physical layer or datalink layer used. This protocol can be used to transport multiple A_PDU1, multiple A_PDU2, or a combination of A_PDU1 and A_PDU2 messages in a single frame as specified in 6.5.2. Each A_PDU is formatted into a C-PG and multiple C-PGs may be packed into a single Multi-PG data frame. The Multi-PG protocol also provides a standard mechanism for optionally adding cybersecurity and/or functional safety to each C-PG within the Multi-PG.

6.5.1 Multi-PG Format

There are two forms of D_PDU for Multi-PG. The first form uses FEFF and is illustrated in Figure 11 and further defined in Figure 13. In this form, the PGN value shall be the Parameter Group Number shown in Figure 13. The other form uses FBFF as illustrated in Figure 12 and further defined in Figure 14. Both forms are used to implement a Multi-PG D_PDU.

The FEFF form of the Multi-PG is transmitted using the D_PDU1 format. The Multi-PG PG is a PDU1 type PG, allowing it to be sent to either a specific destination or to the global destination. When sent as D_PDU1 with a specific Destination Address in the PS field, this Multi-PG is referred to as a Destination Specific D_PDU1 Multi-PG. When sent as D_PDU1 with the global Destination Address (255) in the PS field, this Multi-PG is referred to as a Globally Addressed D_PDU1 Multi-PG.

The FBFF form of Multi-PG is transmitted using the D_PDU3 format and is referred to as a D_PDU3 Multi-PG message. The destination of a D_PDU3 Multi-PG message is always global. The FBFF form of the Multi-PG is identified by having 000_b for the AppPI in the CAN ID.

The destination of the Multi-PG D_PDU serves as the Destination Address of any contained A_PDU1 C-PGs, as specified in 6.5.3.6.2.

The number of C-PGs within a Multi-PG will vary as denoted by "z." For SAE J1939 PGs, "z" is likely not more than 9, depending on the Payload Length of each C-PG. There is no delimiter between C-PGs because the Header of the C-PG defines its length.

<table>
<tr><td rowspan="2">Priority</td><td rowspan="2">PGN + DA</td><td rowspan="2">SA</td><td>C-PG 1</td><td>C-PG 2</td><td>…</td><td>C-PG z</td></tr>
<tr><td colspan="4">Multi-PG</td></tr>
<tr><td colspan="3">CAN Identifier Field</td><td colspan="4">CAN FD Data Field</td></tr>
</table>

Figure 11 - FEFF multi-PG format overview (D_PDU1)

<table>
<tr><td rowspan="2">AppPI=0</td><td rowspan="2">SA</td><td>C-PG 1</td><td>C-PG 2</td><td>…</td><td>C-PG z</td></tr>
<tr><td colspan="4">Multi-PG</td></tr>
<tr><td colspan="2">CAN Identifier Field</td><td colspan="4">CAN FD Data Field</td></tr>
</table>

Figure 12 - FBFF multi-PG format overview (D_PDU3)

While all data field lengths defined in ISO 11898-1 may be used with Multi-PG, when communicating SAE J1939 PGs, the Multi-PG data frame is typically at least 8 bytes long. If the sum total length of all C-PGs packed in a Multi-PG data field does not result in a valid CAN FD data frame length (see 6.3.3.2), the remainder of the Multi-PG data field shall be packed using a padding service C-PG (see 6.5.3.5). The data field padding defined in 6.3.3.2 shall not be used to pad the Multi-PG data frame data field to the DLC length. A Multi-PG must have at least one C-PG within it.

When using a (D_PDU1) FEFF Multi-PG, the priority field in the CAN ID may be set according to the C-PG contents. As a general rule, it is appropriate to set the Multi-PG Priority to the highest priority of any of the C-PGs within it.

Parameter Group Name:	**FEFF (Extended Frame) Multi-PG (MCPG)**
Definition:	Used for the transfer of 1 or more PGs. Each PG follows the C-PG format.
Transmission repetition rate:	As needed
Data length:	4 bytes minimum up to 64 bytes maximum
Extended Date Page:	0
Data Page:	0
PDU Format:	37
PDU Specific:	Destination Address (global or specific)
Default priority:	Highest Priority of the C-PGs contained
Parameter Group Number:	9472 (002500_h)

Data Field:

The data field consists of 1 or more C-PGs of TOS 1 through 7 followed by a Padding C-PG (TOS = 0) if required.

For each C-PG where Type of Service is 1 through 7, the C-PG data format is as follows and repeats for each C-PG:

Byte:	(a) 1.8 to 1.6	Type of Service (6.5.3.1)
	(b) 1.5 to 1.1 & 2 to 3	Service Header (6.5.3.6)
	(c) 4	Payload Length (6.5.3.2)
	(d) 5 to X	C-PG Payload

Data repeats a, b, c, d, a, b, c, d, …

A Padding C-PG (TOS = 0) shall be included after the last C-PG (a, b, c, d) if required to pad the message to a DLC length. See 6.5.3.5 for details.

Figure 13 - FEFF (extended frame) multi-PG

Parameter Group Name:	**FBFF (Base Frame) Multi-PG**
Definition:	Used for the transfer of 1 or more PGs. Each PG follows the C-PG format.
Transmission repetition rate:	As needed
Data length:	4 bytes minimum up to 64 bytes maximum
Application Protocol Indicator:	0

Data Field:

The data field consists of 1 or more C-PGs of TOS 1 through 7 followed by a Padding C-PG (TOS = 0) if required.

For each C-PG where Type of Service is 1 through 7, the C-PG data format is as follows and repeats for each C-PG:

Byte:		
	(a) 1.8 to 1.6	Type of Service (6.5.3.1)
	(b) 1.5 to 1.1 & 2 to 3	Service Header (6.5.3.6)
	(c) 4	Payload Length (6.5.3.2)
	(d) 5 to X	C-PG Payload

Data repeats a, b, c, d, a, b, c, d, …

A Padding C-PG (TOS = 0) shall be included after the last C-PG (a, b, c, d) if required to pad the message to a DLC length. See 6.5.3.5 for details.

Figure 14 - FBFF (base frame) multi-PG

6.5.2 Packing C-PGs into Multi-PG

The Multi-PG method is used to transport one or more A_PDU1 or A_PDU2 in a single frame. Each A_PDU is formatted into a C-PG and multiple C-PGs may be packed into a single Multi-PG.

There are strict requirements for packing multiple A_PDU PGs (C-PGs) into a Multi-PG. See Table 7 for a summary and 6.7 for a decision tree. All D_PDU methods must be supported for reception but the implementer may choose which path or paths to support for transmission; the transport model implementation shown in Figure 39 shows the options.

- A C-PG must be fully contained within a single Multi-PG.
- The Destination Specific D_PDU1 instance of Multi-PG shall contain only A_PDU1 PGs for a single Destination Address (excluding the Global DA 255) and that same Destination Address shall be used in the Multi-PG D_PDU1 CAN ID.
- The Destination Specific D_PDU1 instance of the Multi-PG shall not contain A_PDU2 PGs, shall not contain globally addressed A_PDU1 PGs, and shall not contain A_PDU1 PGs for any other Destination Addresses.
- The Globally Addressed D_PDU1 instance of the Multi-PG shall contain only A_PDU2 PGs and globally addressed A_PDU1 PGs; and the Global DA (255) shall be used in the Multi-PG D_PDU1 CAN ID.
- The D_PDU3 instance of the Multi-PG shall contain only A_PDU2 PGs and globally addressed A_PDU1 PGs; this is permitted since the D_PDU3 is always global.

When packing multiple PGs into a single Multi-PG, the messages shall be packed in the same order they would have been sent if they were individually transmitted. Upon receipt, the ECU shall process the messages in the same order.

When packing multiple A_PDUs (C-PGs) into a Multi-PG message, the combined length of the C-PGs shall not exceed a single CAN FD frame. The FD Transport Protocol service shall not be used for any Multi-PG message. This restriction is established because the segmentation Transport Protocol would add unnecessary overhead and software complication.

Table 7 - Requirements for A_PDU1 and A_PDU2 usage in multi-PGs

Multi-PG D_PDU	A_PDU1 (Destination Specific PG)		A_PDU2 (Broadcast PG)
D_PDU Format	To Specific Address	To Global Address	
Destination Specific D_PDU1 (29-bit)	Allowed (only to same Specific Address)	Not allowed	Not allowed
Globally Addressed D_PDU1 (29-bit)	Not allowed	Allowed	Allowed
D_PDU3 (11-bit)	Not allowed	Allowed	Allowed

6.5.3 C-PG Format

There are two formats possible for a C-PG, shown in Figures 15 and 16. The C-PG format is associated with the Type of Service (TOS) value. Every C-PG consists of the C-PG Header followed by the C-PG Payload. The Type of Service (TOS) field occupies the first 3 bits of every C-PG Header.

For TOS values 1 through 7, the C-PG Header shall be 4-bytes in length and the last byte of the C-PG Header shall be the Payload Length (PL) field, which specifies the byte length of the C-PG Payload. The 21 bits of the C-PG Header between the TOS field and the PL field is known as the Service Header. The content and structure of the Service Header shall be specific to each TOS. This format structure allows a recipient to parse C-PGs from the Multi-PG message even if it encounters some C-PGs with unknown TOS values. This format structure is illustrated in Figure 15.

For TOS 0 (Padding Service), each bit in the C-PG Header shall be zero. The C-PG Service Header for the padding service can be 1, 2, or 3 bytes long but never less than 1 byte as the TOS field must be present. The TOS 0 C-PG (Padding Service) does not have a Payload Length field because it is only permitted as the last C-PG in the Multi-PG data field. This format structure is illustrated in Figure 16.

The maximum length of a C-PG is 64 bytes, except for a TOS 0 C-PG which has a maximum length of 15 bytes.

C-PG Header			C-PG Payload
TOS	Service Header	Payload Length	
3 bits	21 bits	8 bits	0 to 60 bytes

Figure 15 - C-PG format (TOS 1 through TOS 7)

C-PG Header			C-PG Payload
TOS	Service Header		
3 bits	21 bits		0 to 12 bytes
Byte 1	Byte 2	Byte 3	

Figure 16 - C-PG format (TOS 0)

6.5.3.1 TOS Field (Type of Service)

The Type of Service (TOS) field identifies the structure and type of content in the C-PG. Reserved values are available for future assignment. The value assignments are shown in Table 8. Descriptions for each are in the subsequent sections starting with the SAE J1939 service in order to provide context.

Table 8 - Coding of TOS field

TOS Value	Service	Reference
000_b	Padding Service	6.5.3.5
001_b	SAE J1939 Contained PG service with manufacturer specific assurance data	6.5.3.4
010_b	SAE J1939 Contained PG service with optional SAE defined assurance data support	6.5.3.3
011_b to 111_b	Reserved	

6.5.3.2 Payload Length Field (PL)

The Payload Length (PL) field specifies the byte length of the C-PG Payload. The C-PG Payload for the C-PG starts immediately following the PL field and continues the specified number of bytes. The Payload Length value is encoded as 1 byte per bit, ranging in value from 0 through 60.

The C-PG payload contains both the PG data and any functional safety/cybersecurity assurance data. Therefore, the Payload Length is the length of the PG data plus the length of any functional safety/cybersecurity assurance data.

Two examples are provided to show PL use cases. The first example in Figure 17 shows a C-PG for PGN 25600 consisting of 8 bytes of PG data and is protected with a 32-bit OEM functional safety assurance data. This example has a PL of 12 ($0C_h$) because the PG data of 8 bytes plus the manufacturer specific Functional Safety assurance data of 4 bytes add to 12 bytes.

The second example in Figure 18 shows a C-PG for PGN 61463 with 8 bytes of PG data and no functional safety/cybersecurity assurance data. It is sent as a standard message using TOS=2. This example has a PL of 8 because the PG data is 8 bytes long and there is no assurance data to add.

See 6.5.3.6.1 for the definition of TF (Trailer Format) used in these examples.

C-PG Header ($2864000C_h$): 4 bytes				C-PG Payload: 12 bytes	
3 bits	3 bits	18 bits	8 bits	64 bits (8 bytes)	32 bits
TOS	TF	CPGN	PL	PG Data	Functional Safety Assurance Data
1 (001_b)	2 (010_b)	25600 (6400_h)	$0C_h$	6720_h, $79E0_h$, $FFFF_h$, $FFFF_h$	$AF0387EF_h$

Figure 17 - C-PG example 1

C-PG Header ($40F01708_h$): 4 bytes				C-PG Payload: 8 bytes
3 bits	3 bits	18 bits	8 bits	64 bits (8 bytes)
TOS	TF	CPGN	PL	PG Data
2 (010_b)	0 (000_b)	61463 ($F017_h$)	08_h	67_h, 20_h, 79_h, $E0_h$, FA_h, EF_h, 00_h, FF_h

Figure 18 - C-PG example 2

6.5.3.3 C-PG Format for TOS=2

The TOS 010_b value indicates that the C-PG contains an SAE J1939 PG and may contain SAE defined assurance data. This Type of Service is used for any SAE J1939 PG without assurance data and for any SAE J1939 PG with SAE defined assurance data. Note: SAE standards for assurance data content are still being developed as this document goes to publication. This document will be updated with those references following their publication.

The C-PG format is shown in Figures 19 and 20. A C-PG is comprised of the C-PG Header and the C-PG payload. The C-PG Header is comprised of the Type of Service (TOS) field, the Service Header, and the Payload Length (PL) field. The Service Header is comprised of the Trailer Format (TF) field and the contained Parameter Group Number (CPGN). The C-PG Header consumes 4 bytes. The full length occupied by a C-PG with TOS=2 is the sum of the 4-byte C-PG Header length and the Payload Length.

The C-PG payload is comprised of the PG data and the optional functional safety/cybersecurity data (if used). A full PG Data of 60 bytes would only be possible if the functional safety/cybersecurity assurance data is not used since the Header consumes the remaining 4 bytes of a 64-byte CAN FD data frame.

If the A_PDU data length exceeds the C-PG size limit, then the A_PDU cannot be packaged into a C-PG and Multi-PG cannot be used; instead, the A_PDU must be sent using the FD Transport Protocol defined in 6.6.

C-PG Header: 4 bytes							C-PG Payload: 0 to 60 bytes	
3 bits	3 bits	18 bits				8 bits		0 to 64 bits
TOS	TF	CPGN				PL	PG Data	C-PG Assurance Data (Safety/Security)
		EDP	DP	PF	PS			
MSB								LSB

Figure 19 - C-PG format for TOS=1 and TOS=2

Figure 20 provides another view of Figure 19 but with bit positions and SPNs denoted.

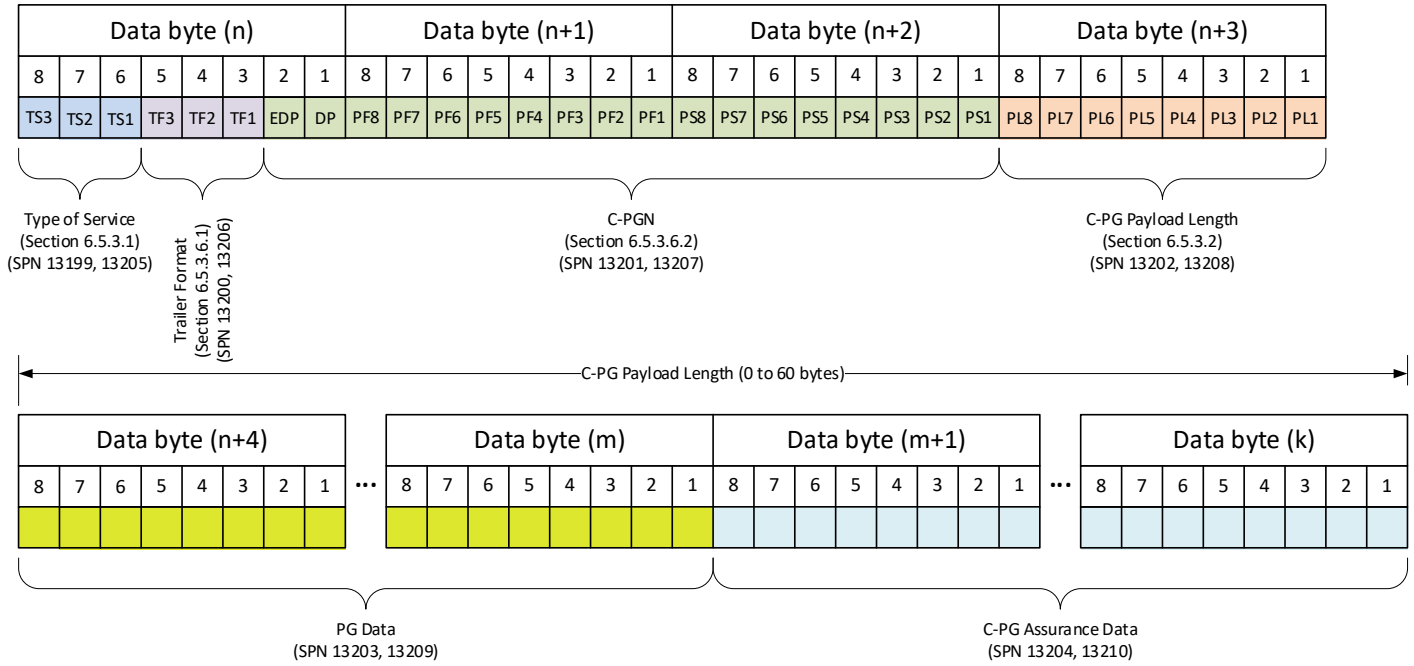


Figure 20 - C-PG bit placement model for TOS=1 and TOS=2

6.5.3.4 C-PG Format for TOS=1

The TOS 001_b value indicates that the C-PG contains an SAE J1939 PG accompanied by manufacturer specific assurance data. This Type of Service is used only when manufacturer specific assurance data accompanies the PG data.

The C-PG format found in Figures 19 and 20 is the same format used for TOS=1. The C-PG Payload is comprised of the related PG Data and the manufacturer specific (OEM) functional safety/cybersecurity assurance data.

If the A_PDU data length exceeds the C-PG size limit, then the A_PDU cannot be packaged into a C-PG and Multi-PG cannot be used; instead, the A_PDU must be sent using the FD Transport Protocol defined in 6.6.

6.5.3.5 C-PG Format for TOS=0

The TOS 000_b value indicates that the C-PG is a Padding Service C-PG. A Padding Service C-PG provides a method to fill the data field of a Multi-PG data frame to the next valid frame length. The Padding Service C-PG is required when the byte length of all C-PGs packed into a Multi-PG data field does not equal one of the CAN FD CAN Data Length Code (DLC) lengths (see 6.3.3.2). The data field padding defined in 6.3.3.2 shall not be used to pad the Multi-PG data frame data field to the DLC length.

The Padding Service C-PG shall only be used as the last C-PG in a Multi-PG because its length is undefined and is not explicitly indicated. The padding service C-PG uses a different C-PG format shown in Figures 21 and 22. The Padding Service C-PG shall have integral bytes of length. The smallest Padding Service C-PG is 1 byte in length and the largest Padding Service C-PG is 15 bytes. The Service Header shall be no less than 5 bits in order to fill a full byte together with the TOS field of 3 bits. In order to minimize stuff bits, the recommended content for the C-PG payload is alternating bits of 1 and 0. Use of bytes of 00_h for the Service Header has been done for AUTOSAR compatibility.

Using the recommended content, if 1 to 3 bytes of padding is required, then the Padding Service C-PG shall be 1 to 3 bytes of 00_h. If 4 to 15 bytes of padding is required, then the Padding Service C-PG shall be 3 bytes of 00_h followed by 1 to 12 bytes of AA_h.

3 bits	5 to 21 bits	0 to 96 bits
TOS=0	Service Header (all bits=0)	C-PG payload (alternating 1 and 0)

Figure 21 - C-PG format for TOS=0 (padding service)

Figure 22 provides another view of Figure 21 but with bit positions and SPN denoted.

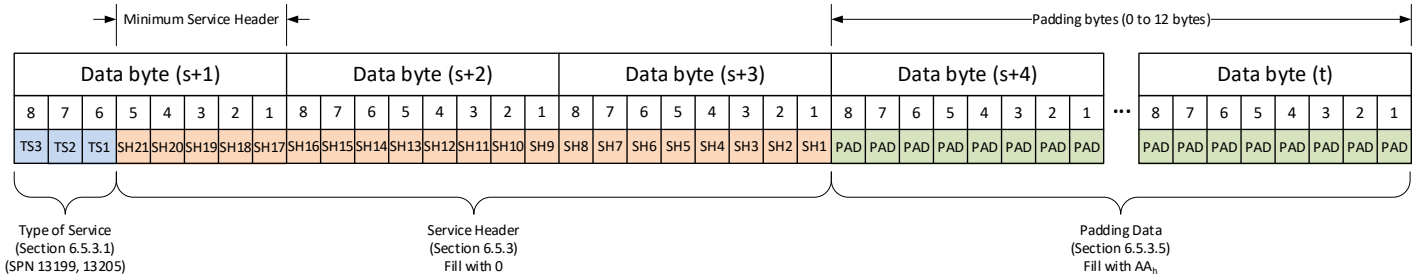


Figure 22 - C-PG bit placement model for TOS=0 (padding service)

For example, suppose the combined length of all C-PGs packed into a Multi-PG data field is 44 bytes. The smallest CAN FD valid data length that is greater than or equal to the length of all the C-PGs is 48 bytes (DLC = E_h). The unused 4 bytes of the CAN FD data field must be padded using a Padding Service C-PG that is 4 bytes in total length. The first byte of the Padding Service C-PG consists of three zeroes for the Type of Service (000_b) followed by the Service Header of 21 bits of 0. This is followed by a data byte of AA_h. An example of this is shown in Figure 23.

Bits	PGN
384	C-PG 1 (EC1)
	C-PG 2 (PADDING)

352	C-PG 1 HEADER	3	TOS	1 (001_b)
		3	TF	2 (010_b)
		18	CPGN	65251 ($FEE3_h$)
		8	PL	44 ($2C_h$)
	PAYLOAD	288	PG DATA	0384_h, 25_h, $04B0_h$, 57_h, … 10_h
		32	FS DATA	$CF0680EE_h$

32	HEADER	3	TOS	0 (000_b)
		21	SVC HDR	0 (000000000000000000000_b)
	PAYLOAD	8	PADDING	170 (AA_h)

Figure 23 - Padding example

6.5.3.6 Service Header

These definitions apply to the Service Header in the C-PG Header when the Type of Service equals 1 or 2.

6.5.3.6.1 TF Field (Trailer Format)

The use of an assurance data trailer is optional but the field is mandatory within the Service Header. When assurance data is used, the valid uses are described in Table 9. The TF field is specific to the Type of Service. A selection guide for the TOS and TF is provided in Figure 24.

Table 9 - Coding of TF field

TOS	TF Value	Trailer format
001_b	000_b	Reserved
001_b	001_b	32-bit manufacturer specific (OEM) cybersecurity assurance data
001_b	010_b	32-bit manufacturer specific (OEM) functional safety assurance data
001_b	011_b	32-bit manufacturer specific (OEM) cybersecurity followed by a 32-bit manufacturer specific (OEM) functional safety assurance data
001_b	100_b	Reserved
001_b	101_b	64-bit manufacturer specific (OEM) cybersecurity assurance data
001_b	110_b	64-bit manufacturer specific (OEM) functional safety assurance data
001_b	111_b	Reserved
010_b	000_b	SAE J1939 with no assurance data
010_b	001_b - 111_b	Reserved
011_b - 111_b	Reserved	Reserved

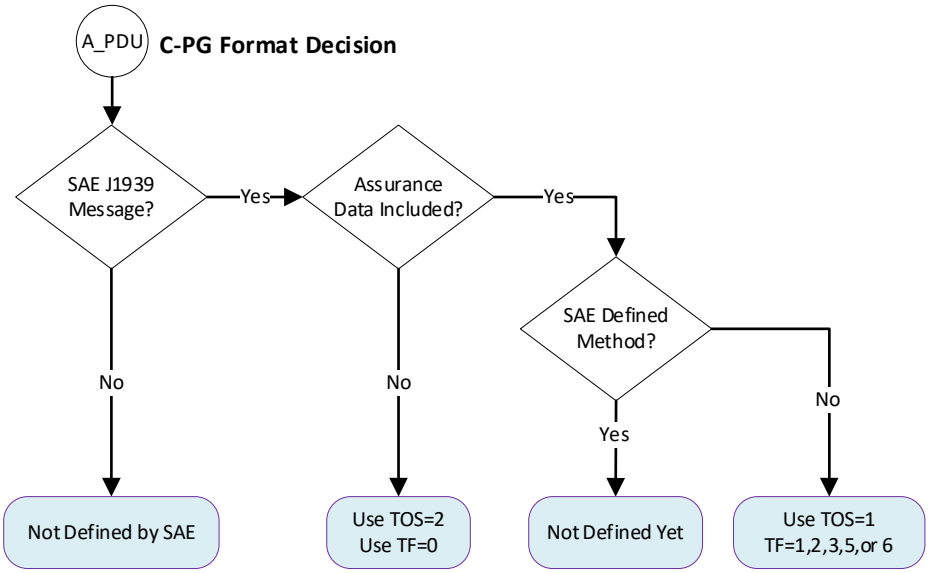


Figure 24 - TOS and TF selection guide

6.5.3.6.2 C-PG CPGN Field

The CPGN field indicates the PGN of the PG data included within the C-PG. It is included with the most significant bits first (the Extended Data Page and the Data Page bits). It is important to note the placement of the PGN bits in the C-PG Service Header uses an MSB placement order; this is different from the standard LSB first placement described in 6.1.3 and used elsewhere in SAE J1939 when the PGN value is part of the data field. See Figures 19 and 20 for an overview.

The PS field in the CPGN for an A_PDU1 C-PG shall not include the Destination Address. Instead, consistent with 6.1.3, the PS field for an A_PDU1 C-PG shall be zero. The Destination Address for the A_PDU1 C-PG shall be derived from the Multi-PG message addressing. The Destination Address of an A_PDU1 C-PG is global when sent in a Globally Addressed D_PDU1 Multi-PG message or a D_PDU3 Multi-PG message. The Destination Address of an A_PDU1 C-PG is the Multi-PG Destination Address when sent in a Destination Specific D_PDU1 Multi-PG message.

6.5.4 Optimizing Bus Utilization (Multi-PG D_PDU Transmit Control)

Bus utilization is illustrated by the D_PDU Transmit Control element in the Transmission Behavior Model shown in Figure 39. Bus utilization is optimized when the Multi-PG data space is filled so that the overhead of sending a C-PG is minimized. Applications are encouraged to implement designs that minimize bus utilization. The exact method to minimize bus utilization is up to each manufacturer; however, some recommendations are provided here.

One consideration is to group transmitted SAE J1939 PGs by transmission rate and combine C-PGs of those PGs into a Multi-PG message to minimize overhead. This consideration is especially useful for PGs with short transmission periods.

A general recommendation is to wait up to 10% of the transmission period to aggregate enough messages to fill a Multi-PG message as much as possible before transmitting it. Use of a separate buffer for each standard transmission rate used by the device is a logical method to allocate PGs to Multi-PG messages.

Another consideration is a FIFO (first in, first out) method of combining C-PGs into a Multi-PG message to minimize overhead.

If the SAE J1939 task associated with adding C-PGs to a Multi-PG at the D_PDU layer is able to receive A_PDUs from any task (and any core for multi-core microprocessors) then it will have the best opportunity to optimize bandwidth utilization. An example of different use cases is shown in Figure 25.

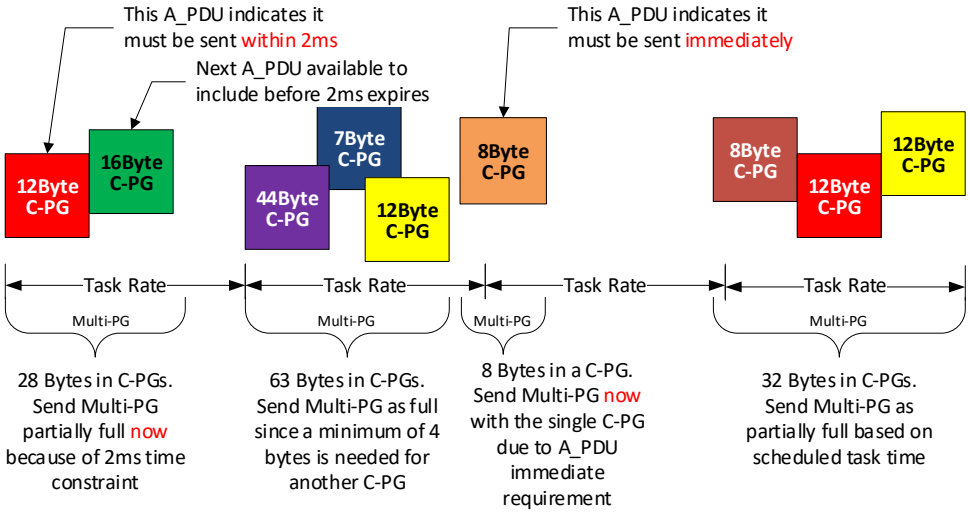


Figure 25 - Transmit control example

6.5.5 Multi-PG Content Examples

6.5.5.1 Multi-PG Example 1

The example in Figure 26 shows the data payload of a single Multi-PG with four C-PGs and C-PG padding as needed. The included C-PGs are addressed to the global address; therefore, the C-PGs must be sent in a globally destined Multi-PG. A globally destined Multi-PG can be either a Globally Addressed D_PDU1 Multi-PG or a D_PDU3 Multi-PG. This Multi-PG example uses the D_PDU3 format so by default it is a broadcast message to all devices on the network and shall not contain any destination specific C-PGs.

The first C-PG is the Request PG (PGN 59904) for PGN 60928 (Address Claimed) without assurance data to solicit the NAME from all devices on the network. The Request PG is a destination specific PG to be sent globally and, in this example, is addressed globally by including it in a D_PDU3 Multi-PG, which is a global message. For reference in setting the Multi-PG priority, the Request PG uses its default priority of 6.

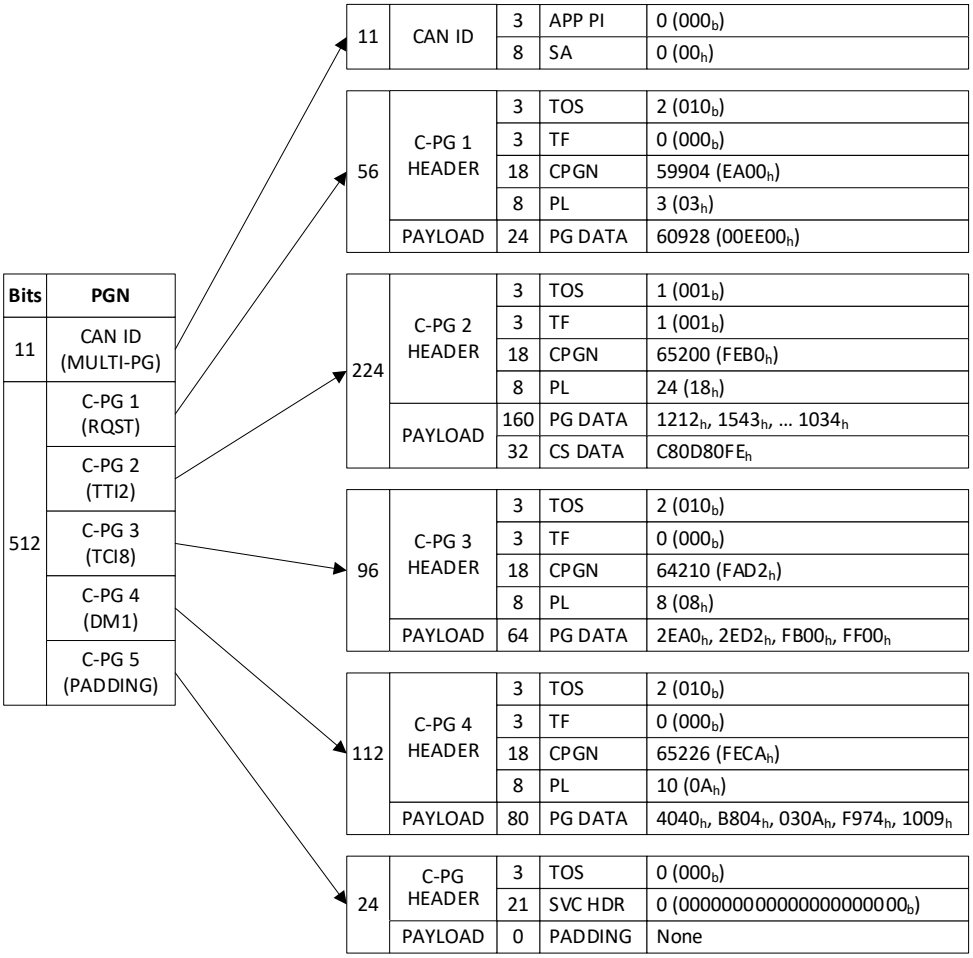
The second C-PG is Trip Time Information 2 (PGN 65200) with an OEM defined 32-bit cybersecurity assurance data. This PG is an “On Request” message being sent in response to a global Request, which is not shown. The TTI2 PG is an A_PDU2 PG being sent with 20 bytes which results in 24 bytes with the added OEM cybersecurity assurance data. For reference in setting the Multi-PG priority, the TTI2 PG uses its default priority of 7.

The third C-PG is a broadcast of Turbocharger Information 8 (PGN 64210) without assurance data. This PG is an A_PDU2 PG defined as 8 bytes and uses its default priority of 6.

The fourth C-PG is a DM1 message reporting two active DTCs and no assurance data resulting in a 10-byte payload. This PG is an A_PDU2 PG and uses its default priority of 6.

The length of the four C-PGs is 61 bytes. The remaining space is filled with a Padding Service C-PG to the next valid data frame size because 61 bytes is not a valid CAN FD data frame size. A 3-byte Padding Service C-PG is required to fill the Multi-PG data field to a valid CAN FD frame size. Using the required 0 fill in the Service Header, a Padding Service C-PG of 0 is added to the end of the Multi-PG data field. The Padding Service Data Field is truncated as it isn’t needed in order to have a total padding length of 3 bytes.

The lowest value (highest priority) of the four C-PG priority values is 6 so the priority would be 6 for a Globally Addressed D_PDU1 Multi-PG. However, this example uses the D_PDU3 format which does not have a Priority field. The transmitter of the Multi-PG in this example is using a Source Address of 0 representing the primary engine control module.



Bits	PGN
11	CAN ID (MULTI-PG)
512	C-PG 1 (RQST)
	C-PG 2 (TTI2)
	C-PG 3 (TCI8)
	C-PG 4 (DM1)
	C-PG 5 (PADDING)

11	CAN ID	3	APP PI	0 (000_b)
		8	SA	0 (00_h)
56	C-PG 1 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	59904 ($EA00_h$)
		8	PL	3 (03_h)
	PAYLOAD	24	PG DATA	60928 ($00EE00_h$)
224	C-PG 2 HEADER	3	TOS	1 (001_b)
		3	TF	1 (001_b)
		18	CPGN	65200 ($FEB0_h$)
		8	PL	24 (18_h)
	PAYLOAD	160	PG DATA	1212_h, 1543_h, … 1034_h
		32	CS DATA	$C80D80FE_h$
96	C-PG 3 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	64210 ($FAD2_h$)
		8	PL	8 (08_h)
	PAYLOAD	64	PG DATA	$2EA0_h$, $2ED2_h$, $FB00_h$, $FF00_h$
112	C-PG 4 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	65226 ($FECA_h$)
		8	PL	10 ($0A_h$)
	PAYLOAD	80	PG DATA	4040_h, $B804_h$, $030A_h$, $F974_h$, 1009_h
24	C-PG HEADER	3	TOS	0 (000_b)
		21	SVC HDR	0 (000000000000000000000_b)
	PAYLOAD	0	PADDING	None

Figure 26 - Multi-PG example 1

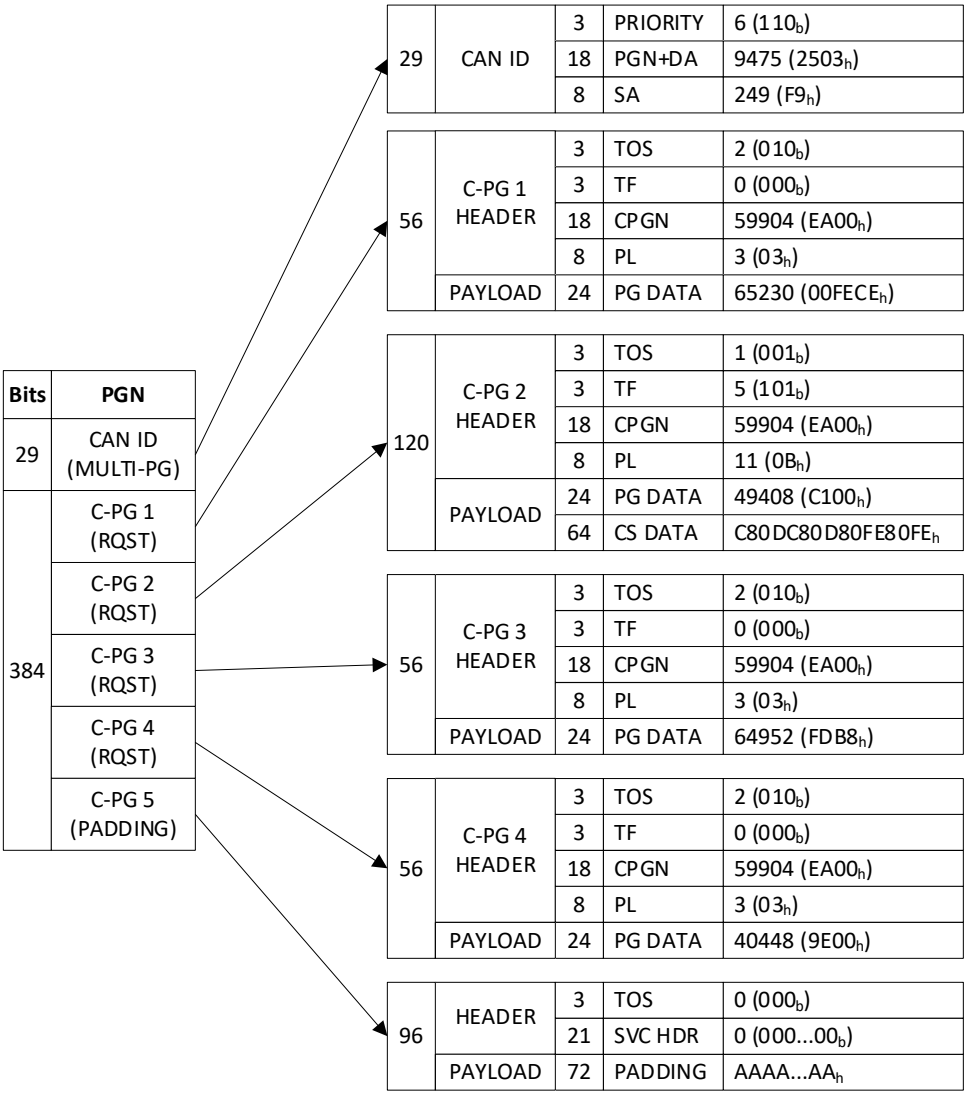
6.5.5.2 Multi-PG Example 2

The example in Figure 27 represents a Destination Specific D_PDU1 Multi-PG message. In this example, a tool (SA 249) is sending four Request PGs to the transmission controller (SA 03) requesting DM5, DM21, DM26, and DM29.

Since all of the Request PGs are to be sent to the same destination address, all four of the C-PGs for these Request PGs can be grouped into the same Multi-PG message addressed to SA 03. The destination address (03) is specified in the PF field of the D_PDU1 data frame for the Multi-PG instance containing these four C-PGs. The C-PG for the Request of DM21 (PGN 49408) includes an 8-byte manufacturer specific cybersecurity assurance data so this C-PG shall have Type of Service equal to 1. All of the C-PGs in this example use a priority of 6, so the D_PDU1 Priority field is also 6. The total length of the four C-PGs is 36 bytes so a 12-byte Padding Service C-PG is needed to reach the next valid FD data frame of 48 bytes.

Two of the requested PGs (DM21 and DM29) are destination specific PGs (PDU1) so the responses for those PGs will be sent using destination specific Multi-PG messages. The other two requested PGs (DM5 and DM26) are broadcast PGs (PDU2) so the responses for those PGs will be sent using globally addressed Multi-PG messages.

The arrows represent continuity from line to line; all content is in a single CAN FD message.



Bits	PGN
29	CAN ID (MULTI-PG)
384	C-PG 1 (RQST)
	C-PG 2 (RQST)
	C-PG 3 (RQST)
	C-PG 4 (RQST)
	C-PG 5 (PADDING)

29	CAN ID	3	PRIORITY	6 (110_b)
		18	PGN+DA	9475 (2503_h)
		8	SA	249 ($F9_h$)
56	C-PG 1 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	59904 ($EA00_h$)
		8	PL	3 (03_h)
	PAYLOAD	24	PG DATA	65230 ($00FECE_h$)
120	C-PG 2 HEADER	3	TOS	1 (001_b)
		3	TF	5 (101_b)
		18	CPGN	59904 ($EA00_h$)
		8	PL	11 ($0B_h$)
	PAYLOAD	24	PG DATA	49408 ($C100_h$)
		64	CS DATA	$C80DC80D80FE80FE_h$
56	C-PG 3 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	59904 ($EA00_h$)
		8	PL	3 (03_h)
	PAYLOAD	24	PG DATA	64952 ($FDB8_h$)
56	C-PG 4 HEADER	3	TOS	2 (010_b)
		3	TF	0 (000_b)
		18	CPGN	59904 ($EA00_h$)
		8	PL	3 (03_h)
	PAYLOAD	24	PG DATA	40448 ($9E00_h$)
96	HEADER	3	TOS	0 (000_b)
		21	SVC HDR	0 ($000...00_b$)
	PAYLOAD	72	PADDING	$AAAA...AA_h$

Figure 27 - Multi-PG example 2

6.6 FD Transport Protocol

The FD Transport Protocol provides the means for communicating large messages. For the purposes of this protocol, a large message is considered to be an SAE J1939 PG A_PDU that has more than 60 data bytes or an SAE J1939 PG A_PDU that cannot fit in a Multi-PG C-PG because the combined size of the PG data and its assurance data is greater than 60 bytes. The FD Transport Protocol communicates large messages by fragmenting the large message data into a sequenced series of 60 byte segments, sequentially transmitting those segments, and then reassembling those segments into the original large message data. The FD Transport Protocol functions are performed as part of a virtual connection between the large message originator and the large message recipients.

FD Transport Protocol functions are described as a part of the data link layer with the recognition that FD Transport Protocol functionality is subdivided into three major categories of functions: Data Segmentation and Reassembly, Data Transfer, and Connection Management. Data Segmentation and Reassembly functions deal with fragmenting the large message data into a sequenced series of segments and then reassembling the transmitted segments into the original large message data. Data Transfer functions deal with sequentially transmitting the segments. Connection Management functions deal with distributed exchanges to open the virtual connection, flow control for data segment transfers, assurance data exchange, and to close the connection at the completion of the large data exchange.

There are two types of FD Transport transfer methods: RTS/CTS Transfer and BAM (Broadcast Announce) Transfer. RTS/CTS Transfer (point to point) is used when a large message is to be sent to a specific Destination Address. BAM transfer is used when a large message is to be sent globally, or non-destination specific.

In the FD Transport Protocol sections, the term “originator” corresponds to the source of the large data message and the term “responder” corresponds to the receiver of the large data message. In the context of an RTS/CTS transfer, the originator is the transmitter of the RTS and DT messages, and the responder is the transmitter of the CTS message and receiver of DT messages. In the context of a BAM transfer, the originator is the transmitter of the BAM and DT messages, and a responder is any node that is the receiver of the BAM and DT messages.

6.6.1 Operational Overview

6.6.1.1 BAM (Broadcast) Transfer

Broadcast Announce (BAM) transfer is used when a large message is to be sent globally, or non-destination specific. BAM transfers use the Connection Management operations to announce the start of the transfer session and to announce the completion of the transfer session. Connection management flow control and explicit closure exchanges are not used with BAM sessions since the transfer is from one to many recipients. See Figure A6 for a sequence diagram example of a BAM transfer.

The BAM transfer shall be used for all PDU2 PGs and for PDU1 PGs being sent globally.

For BAM transfer, the maximum A_PDU data size that can be transferred is limited to 15300 bytes.

A BAM transfer session is initiated when the originator transmits the FD.TP.CM_BAM message to the global Destination Address. This message announces to all nodes on the network that a globally destined large message transfer is about to take place.

After sending the FD.TP.CM_BAM message, the originator begins sending the PG data using a series of Data Transfer (FD.TP.DT) messages to the global Destination Address.

After sending the Data Transfer (FD.TP.DT) message for the final data segment, the originator transmits the FD.TP.CM_EndOfMsgStatus (EOMS) completion message to close the connection. The EOMS message includes Assurance Data, if applicable.

After receiving the Data Transfer (FD.TP.DT) message for the final data segment and receiving the EOMS message, a responder shall verify the entire message was received and reassembled correctly.

6.6.1.2 RTS/CTS (Destination Specific) Transfer

RTS/CTS (destination specific) transfer is used when a large message is to be sent to a specific Destination Address. RTS/CTS transfers use the Connection Management operations to initiate the transfer session, data flow control, transfer complete, and explicit connection closure. The originator and the responder are able to utilize an abort connection management operation. See Figure A1 for a sequence diagram example of an RTS/CTS transfer.

The RTS/CTS transfer shall be used for PDU1 PGs being sent to a specific Destination Address. The RTS/CTS transfer shall not be used for PDU2 PGs.

For RTS/CTS transfer, the maximum A_PDU data size that can be transferred is 16777215 bytes.

An RTS/CTS transfer session is initiated when the originator transmits the FD.TP.CM_RTS (RTS) message to a specific responder Destination Address. Upon receipt of the RTS message, the responder may elect to accept the connection or to reject it. To accept the connection, the responder transmits a FD.TP.CM_CTS (CTS) message to the originator Destination Address. The responder must ensure that it has sufficient resources to handle the message size it is accepting. To reject the connection, the responder sends a FD.TP.Conn_Abort message. The connection can be rejected for any reason, although lack of resources, memory, etc., are likely to be the causes. Sending an Abort message allows the originator to move on to a new connection without having to wait for a timeout.

The connection is considered established for the originator when the originator receives the CTS message from the responder in response to its RTS message. The connection is considered established for the responder when it has successfully transmitted its CTS message in response to the RTS message.

After receiving a FD.TP.CM_CTS (CTS) message from the responder, the originator begins sending Data Transfer (FD.TP.DT) messages to the responder Destination Address. The series of FD.TP.DT (DT) messages will contain the PG data segments according to the “next segment” and “number of segment” values specified in the CTS.

While more PG data remains to be received, the responder shall send another CTS for the next set of data segments after it receives the last FD.TP.DT message per the previous FD.TP.CM_CTS. Upon receiving a subsequent FD.TP.CM_CTS (CTS) message from the responder, the originator begins sending Data Transfer (FD.TP.DT) messages with the next set of cleared data segments.

After sending the Data Transfer (FD.TP.DT) message for the final data segment, the originator transmits the FD.TP.CM_EndOfMsgStatus (EOMS) completion message to the responder. This message informs the responder that the originator has transmitted all of the data segments. The EOMS message shall include functional safety and/or cybersecurity assurance data, if applicable.

After receiving the Data Transfer (FD.TP.DT) message for the final data segment and receiving the EOMS message, the responder shall verify the entire message was received and reassembled correctly. Once verification is completed, the responder transmits the FD.TP.CM_EndOfMsgACK (EOMA) message to the originator to explicitly close the transfer and connection.

6.6.1.3 Concurrent Sessions and Session Numbers

Up to 8 concurrent RTS/CTS sessions per originator and responder address pair are allowed. Up to four concurrent BAM sessions per originator address are allowed and can be simultaneous with RTS/CTS sessions. For example, a BAM connection using session 0 can be differentiated from an RTS/CTS connection also using session 0 by the Destination Address. Due to the Request service capability for both global and destination specific Requests, if large message transport support is provided, both BAM and RTS/CTS shall be supported.

An ECU may support any number of concurrent sessions for RTS/CTS and/or BAM messages up to the maximum allowed. Support requirements are application specific. Since receivers have no minimum support requirement, an originator using multiple sessions (for example, using BAM) may not be able to expect all nodes to receive every concurrent session of data.

BAM transfers shall only use Session numbers 0 to 3. RTS/CTS transfers shall only use Session numbers 0 to 7. Session numbers 8 to 15 are reserved by SAE for future use. The originator chooses the session number to be used when it initiates a transfer session. The session value used by the originator in the RTS message shall also be used by the responder in the CTS, EOMA, and Abort messages which correlate to the same connection. The originator shall also use the same session value in the EOMS message and Abort message. Likewise, the same session value shall be used in the related Data Transfer messages. The session value used by the originator of a BAM message shall also be used for the EOMS, Abort, and Data Transfer of the same connection.

A transfer session (connection) is unique to the combination of the originator source address, responder source address, and the session number. The responder source address shall be used to differentiate RTS/CTS from BAM sessions. For a BAM transfer the responder source address shall be the global Destination Address. For an RTS/CTS transfer, the responder source address shall never be the global Destination Address. Connection management, segmentation, reassembly, and data transfer operations shall use source address, destination address, and session number data in FD.CM and FD.TP.DT messages to associate those messages to the appropriate FD Transport session.

6.6.1.4 Assurance Data

Protection of PG data may be added to any large message transport. Either or both functional safety and cybersecurity assurance content is possible. This protection is not required but available when needed. When assurance data is used, the calculation method shall be defined in the RTS or BAM message for the responder's benefit. This definition is provided in the Assurance Data Type (ADT) field (see Figure 30). The originator will then provide the calculated Assurance Data in the End of Message Status (EOMS) message at the completion of the transport (see Figure 33). This assurance data is not related to any assurance data defined within the PG data from SAE J1939DA (like a TSC1 checksum).

6.6.2 FD Transport Protocol Functions

6.6.2.1 Data Segmentation and Reassembly

Data Segmentation and Reassembly are complementary FD Transport Protocol functions. Data Segmentation and Reassembly functions deal with fragmenting the large message data into a sequenced series of 60 byte segments and then reassembling the transmitted segments into the original large message data. Segmentation, performed by the originator, is the process of fragmenting the large PG Data into a sequenced series of, up to, 60 byte segments that can each be transmitted in individual FD Data Transfer (FD.TP.DT) data frames. Reassembly, performed by the responder, is the process of parsing the sequenced data segments from the received individual FD Data Transfer (FD.TP.DT) data frames and reconstructing the original large data.

6.6.2.1.1 Segmentation

Segmentation is the process of fragmenting the large PG Data into a sequenced series of smaller data segments that can each be transmitted in an FD Data Transfer (FD.TP.DT) data frame. All data segments shall be 60 bytes in length, except for the last data segment which may be shorter than 60 bytes. The first Data Transfer (FD.TP.DT) segment is identified as segment number one and contains the first (up to) 60 bytes of the data. The second FD.TP.DT segment is identified as segment number two and contains the next (up to) 60 bytes of the data. The third FD.TP.DT segment is identified as segment number three and contains the next (up to) 60 bytes of data. This process is repeated until all the A_PDU PG data has been placed into FD Data Transfer messages and transmitted.

Note that an FD Transport transfer with a single data segment is a valid transfer. See 6.6.2.3 for an explanation.

6.6.2.1.2 Reassembly

Reassembly is the process of parsing the sequenced data segments from the received individual FD Data Transfer (FD.TP.DT) data frames and reconstructing the original large data. Data segments shall be received sequentially. Each data segment shall be assembled, in order of segment number, into a single array of bytes. The assembled data segments need to be truncated to remove any data bytes of padding. The assembled data segments may be larger than the original large data if the FD.TP.DT message for the last data segment required byte padding. The "Total Bytes" value reported in the BAM or RTS message specifies the byte length of the original large data. The original large data is parsed from the assembled data by taking the first "Total Bytes" number of bytes from the assembled data segments and discarding any remaining bytes. This array of bytes is passed to the controller application responsible for the large message along with other relevant metadata (see Table 1).

6.6.2.2 Connection Management

Connection Management (CM) is concerned with the opening, use, and closure of virtual connections for large data transfer between Controller Applications. A virtual connection, in the SAE J1939 environment, may be considered a temporary association of two Controller Applications for the purpose of transferring a single large message that is described by a single PGN. When the virtual connection is directed from one Controller Application to another Controller Application (using RTS/CTS), there are flow control and closure operations (see Figures A1 and A2). In cases where the connection is from one to many, there is no flow control or closure provided (see Figure A6).

Connection management messages shall never be included as C-PGs within a Multi-PG.

6.6.2.2.1 Connection Management for Broadcast (BAM) Transfer

Broadcast Announce (BAM) transfer is used when a large message is to be sent globally, or non-destination specific. Connection Management for BAM sessions only consists of the opening announcement of the transfer session and the end of message status alerts from the originator. To initiate a BAM transfer session connection, the originator shall transmit the FD.TP.CM_BAM (BAM) message to the global DA. This message constitutes a large message notification. The BAM message contains the PGN to be sent, the PG data size, the number of segments into which the PG data has been fragmented, and the session to be used. It can also indicate an Assurance Data Type to be used for functional safety and/or cybersecurity protection. Controller Applications interested in the data shall allocate the resources necessary to receive and reassemble the message.

After sending the Data Transfer (FD.TP.DT) message with the final data segment, the originator shall transmit the FD.TP.CM_EndOfMsgStatus (EOMS) completion message to the global address. This message notifies all responders that the originator has transmitted all of the data segments. There is no explicit connection closure messaging by responders for a BAM transfer. The PG data size reported in the FD.TP.CM_BAM message is only the length of the PG data. The reported PG data size value does not include the four bytes associated with segment numbers, session identification, or reserved bits that are added to the contents of each FD.TP.DT segment. The reported PG data size value also does not include any Assurance Data included in the EOMS message.

If the originator needs to abort a BAM transfer after it sends the FD.TP.CM_BAM message and before it sends the FD.TP.CM_EndOfMsgStatus message, then the originator shall send a FD.TP.Conn_Abort message to inform all responders that the transfer is canceled.

6.6.2.2.2 Connection Management for Destination-Specific (RTS/CTS) Transfer

RTS/CTS (point to point) transfer is used when a large message is to be sent to a specific Destination Address. Connection Management for RTS/CTS sessions consist of connection opening, flow control operations, and connection closure. The originator and the responder are able to abort the connection.

The originator initiates an RTS/CTS transfer session by transmitting an FD.TP.CM_RTS (RTS) message to a specific responder DA. The RTS message indicates the PGN of the large message to be sent, the PG data size, the number of segments into which the PG data has been fragmented, the maximum number of segments that can be sent in response to one Clear to Send (CTS) message from the responder, and the session used for the transfer. It can also indicate an Assurance Data Type to be used for functional safety and/or cybersecurity protection.

The responder transmits FD.TP.CM_CTS (CTS) messages to control the flow of data segments. The responder transmits CTS messages in response to an RTS message and after receiving the last data segment cleared by the previous CTS message. The CTS message contains the matching session number, the number of segments that can be sent for this CTS, and the segment number of the next segment it is expecting. The responder uses the “number of segments” and “next segment” fields in each CTS message to control the flow. These fields allow the responder to adjust the number of segments transmitted following the CTS, pause the transfer of data segments, and request the retransmit of data segments.

The originator transmits the FD.TP.CM_EndOfMsgStatus (EOMS) completion message after sending the Data Transfer (FD.TP.DT) message for the final data segment of the PG data. This message indicates to the responder that the originator has transmitted all of the data segments. The EOMS message shall include assurance data, if applicable.

The responder transmits the FD.TP.CM_EndOfMsgACK (EOMA) message to explicitly close the transfer and connection. The responder transmits the EOMA message after receiving the final data segment Data Transfer (FD.TP.DT) message and receiving the EOMS message.

The originator and the responder are able to abort an RTS/CTS transfer at any time. To abort the transfer session, the originator or the responder shall transmit a FD.TP.Conn_Abort message to inform the other Controller Application in the session that it has ceased its support of the transfer session.

6.6.2.3 Minimum Data Size

The requirement to use FD Transport Protocol is not based only on the length of the A_PDU's PG data. FD Transport Protocol shall be used for any A_PDU where the combined length of the PG data and assurance data is greater than 60 bytes. For Multi-PG, the C-PG payload contains both the PG data and assurance data with a maximum payload of 60 bytes.

For FD Transport, the FD.TP.DT (Data Transfer) messages transfer only the PG data for an A_PDU; any assurance data is sent separately in the FD.TP.CM_EndOfMsgStatus (EOMS) message. Therefore, it is possible for an FD Transport session to only need a single FD.TP.DT transfer segment.

In Figure 28, the left image shows an example of an A_PDU with 60 bytes in total comprised of 52 bytes PG data and 8 bytes assurance data. In this first example, the A_PDU fits in a Multi-PG D_PDU. The right image shows an example of an A_PDU with 61 bytes in total comprised of 53 bytes of PG data and 8 bytes assurance data. In this second example, the combined length (61 bytes) exceeds the Multi-PG capability and must be sent using the FD Transport Protocol. There is only one FD.TP.DT message containing the 53 bytes of PG data and the 8 bytes of assurance data is reported in the FD.TP.CM_EndOfMsgStatus (EOMS) message. Other FD.TP connection management messages such as RTS, CTS, and EOMA are not shown.

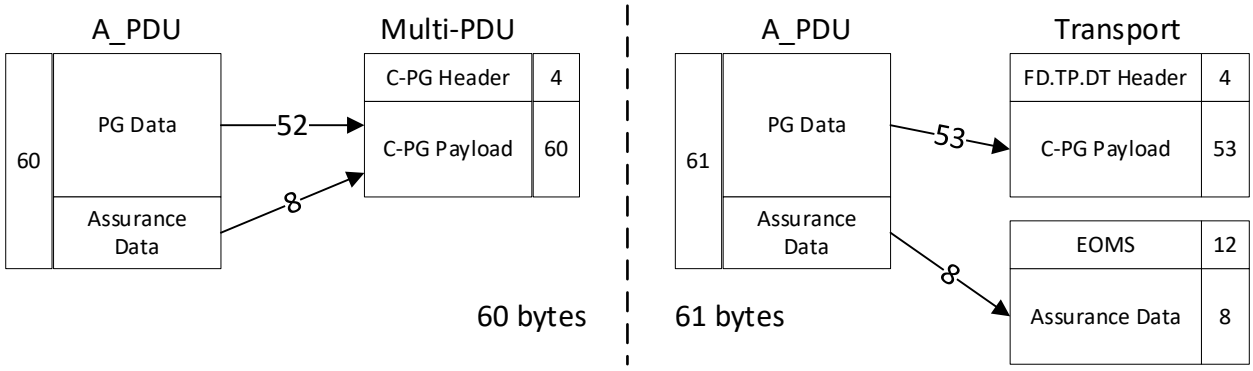


Figure 28 - A_PDU data size

6.6.2.4 Data Transfer

Data Transfer involves the transfer of the sequenced segments of the A_PDU's PG data from the originator to the recipient/responder.

The FD.TP.DT (Data Transfer) (DT) PG is used to transmit each segment. Each DT message is sent as a single D_PDU1 FEFF data frame with the FD.TP.DT PGN specified in the 29-bit CAN identifier. The FD.TP.DT PG shall never be transmitted as a C-PG within a Multi-PG message. The data field of the DT PG contains the session number, the sequential segment number, and the segment data bytes.

For a BAM transfer session, data transfer begins after the originator transmits the FD.TP.CM_BAM (BAM) message. The originator sends DT messages for all of the data segments without flow control.

For an RTS/CTS transfer session, data transfer begins after the originator receives the CTS message from the responder.

The responder uses the CTS message to control the data flow from the originator. The originator shall only send the data segments corresponding to the “number of segments to send” and “next segment to send” in the CTS message from the responder. After sending DT messages with those data segments, the originator shall wait for the subsequent CTS message before sending more DT messages for that session. Responders shall comply with the “maximum number of segments per CTS message” in the RTS message from the originator. This requirement is further explained in 6.6.3.2.

For an RTS/CTS transfer session, if the responder wants to stop data flow momentarily for an open connection, it shall send a CTS message with the “number of segments to send” field equal to zero. The responder may send consecutive CTS messages with the “number of segments to send” field equal to zero once per T_h to assure the originator the connection is not closed. The PGN and session fields shall be populated according to the session in use and the PGN being transferred. All remaining fields are set to the don’t care/not used state using FF_h in each byte. When the responder is ready to resume the data flow, then the responder sends a CTS message with the “number of segments to send” and “next segment to send” appropriate for the last segments received.

6.6.2.5 Connection Closure

FD Transport connections can be closed normally after completing the data transfer in the absence of errors.

For a BAM transfer, the connection is closed normally with transmit of the FD.TP.CM_EndOfMsgStatus (EOMS) message, which alerts recipients that the originator has transmitted all data segments. See 6.6.3.3. The connection is closed for the originator upon successful transmit of the EOMS message, and the connection is closed for each responder upon reception of the EOMS message.

For an RTS/CTS transfer, normal connection closure involves the exchange of the FD.TP.CM_EndOfMsgStatus (EOMS) and the FD.TP.CM_EndOfMsgACK (EOMA) messages. The originator initiates the connection closure by transmitting the EOMS message. Upon receipt of the EOMS message, the responder transmits the EOMA message to the originator to indicate that the connection is considered closed by the responder. Sending the FD.TP.CM_EndOfMsgACK message is required to free the connection for subsequent use by other devices without waiting for a timeout. See 6.6.3.3 and 6.6.3.4.

FD Transport connections also can be aborted at any time during the data transfer.

For a BAM transfer, the connection can only be aborted by the originator. The originator shall send an FD.TP.Conn_Abort message to notify all responders that the transfer has been canceled. Upon receipt of the FD.TP.Conn_Abort message, recipients shall abandon any message segments already transmitted. Responders in a BAM transfer cannot abort the connection. See 6.6.3.4 and 6.6.3.5.

For an RTS/CTS transfer, the connection can be aborted at any time by the originator or the responder. To abort the connection, a Controller Application shall send an FD.TP.Conn_Abort message to the other Controller Application of the connection. See 6.6.2.2.2 for an explanation of when a connection is considered established for the originator and responder. If the responder should, for example, determine that there are no resources available for processing the message, it may simply abort the connection by issuing the FD.TP.Conn_Abort with abort reason 2 (see Table 11). Upon receipt of the FD.TP.Conn_Abort message, any message segments already passed will be abandoned.

All timeout values are defined in 6.14.

A failure of either node can cause closure of a connection. For example:

1. Responder has failed to receive an FD.TP.DT message in more than (T1) seconds since the previous FD.TP.DT message when more FD.TP.DT messages are expected (CTS allowed more);

2. Responder has failed to receive an FD.TP.DT message in more than (T2) seconds after a CTS was transmitted (originator failure);

3. Responder has failed to receive an FD.TP.DT message in more than (T1) seconds after a BAM was transmitted (originator failure);

4. Originator has failed to receive a CTS or FD.TP.CM_EndOfMsgACK for more than (T3) seconds after the FD.TP.CM_EndOfMsgStatus was transmitted (responder failure);

5. Originator has failed to receive a CTS message for more than (T4) seconds after receiving a FD.TP.CM_CTS message with “number of segments to be sent” set to zero, i.e., “hold the connection open”;

6. A failure of flow control where a responder receives more segments than Requested in its CTS message;

7. A failure of flow control where an originator receives a CTS Request to send more segments than allowed in its RTS message;

8. Responder has failed to receive an FD.TP.CM_EndOfMsgStatus for more than (T1) seconds after the FD.TP.DT message containing the last (final) data segment was transmitted (originator failure).

See Figures A1, A4, A5, and A6 and 6.14 regarding timeouts. When either the originator or responder decides to close out a connection for any reason including a timeout, it shall send the FD.TP.Conn_Abort message with abort reason 3 from Table 11.

With the definitions in this section and those in all sections under 6.6 the following observations can be made.

- A BAM data transfer connection is considered closed when the originator:
  - Sends the FD.TP.CM_EndOfMsgStatus
  - Sends a FD.TP.Conn_Abort
- A BAM data transfer connection is considered closed when the responder:
  - Receives the FD.TP.CM_EndOfMsgStatus
  - Has a T1 connection timeout
- An RTS/CTS data transfer connection is considered closed when the originator:
  - Receives the FD.TP.CM_EndOfMsgACK once the entire PG data transfer is completed
  - Sends a FD.TP.Conn_Abort for any reason (e.g., due to a T3 or T4 timeout)
  - Receives a FD.TP.Conn_Abort
- An RTS/CTS data transfer connection is considered closed when the responder:
  - Sends the FD.TP.CM_EndOfMsgACK once the entire PG data transfer is completed
  - Receives a FD.TP.Conn_Abort
  - Sends a FD.TP.Conn_Abort for any reason (e.g., including stopping the session early if desired, for a T1 or T2 connection timeout, etc.)

6.6.3 FD Transport Protocol - Connection Management Messages (FD.TP.CM)

The FD.TP.CM message is used to initiate and close FD Transport connections and, for RTS/CTS transfers, control the data flow. Each FD.TP.CM message shall be sent as a single D_PDU1 FEFF data frame with the FD.TP.CM PGN specified in the 29-bit CAN identifier. The FD.TP.CM PG shall never be transmitted as a C-PG within a Multi-PG message.

The FD.TP.CM message is used for the following six connection management messages: the Connection Mode Request To Send (RTS), the Connection Mode Clear To Send (CTS), the End of Message Status (EOMS), the End of Message Acknowledgment (EOMA), the Connection Abort (Abort), and the Broadcast Announce Message (BAM). The common Connection Management message format uses 12-bytes as shown in Figures 29 and 30. Table B1 in has the SPN assignments to parameters in this message.

RTS	S	CTRL=0	TOTAL BYTES			TOTAL # OF SEGMENTS			MAX SGMTS	AD TYPE	PGN						
CTS	S	CTRL=1	RESERVED			NEXT SEGMENT NUMBER			XFR SGMTS	RQST	PGN						
EOMS	S	CTRL=2	TOTAL BYTES			TOTAL # OF SEGMENTS			AD SIZE	AD TYPE	PGN			OPTIONAL ASSURANCE DATA			
EOMA	S	CTRL=3	TOTAL BYTES (RECEIVED)			TOTAL # OF SEGMENTS (RECEIVED)			RESERVED	RESERVED	PGN						
BAM	S	CTRL=4	TOTAL BYTES			TOTAL # OF SEGMENTS			RESERVED	AD TYPE	PGN						
ABORT	S	CTRL =15	RESERVED			RESERVED			RESERVED/ ROLE	REASON	PGN						
	4 bit	4 bit	LSB		MSB	LSB		MSB			LSB		MSB	LSB	...	MSB	
Msg Byte	1		2	3	4	5	6	7	8	9	10	11	12	"AD SIZE" bytes long			

Figure 29 - Connection management data frame overview

Parameter Group Name:	**FD Transport Protocol—Connection Management (FD.TP.CM)**
Definition:	Used for managing the transfer of PGs whose data and any assurance data cannot be transferred using the Multi-PG message. A definition of each specific message defined as part of the Transport Protocol is contained in the 6.6.3.1 through 6.6.3.5.4.
Transmission repetition rate:	As required
Data length:	12 bytes (up to 64 bytes for EOMS with functional safety/cybersecurity assurance data)
Extended Date Page:	0
Data Page:	0
PDU Format:	77
PDU Specific:	Destination Address (global or specific)
Default priority:	7
Parameter Group Number:	19712 ($004D00_h$)
Data ranges for parameters used in this Parameter Group:	
Control Type:	Byte 1.1 to 1.4: 0 to 15 (4 bits) in lower bits of the first byte
Session Number:	Byte 1.5 to 1.8: 0 to 15 (4 bits) in upper bits of first byte (see 6.6.1.3)
Total Message Size, number of bytes:	Bytes 2 to 4: maximum of 16,777,215 (3 bytes)
Total Number of Segments:	Bytes 5 to 7: 1 to 16,777,215 (3 bytes), zero is not allowed
Or Next Segment Number to be Sent:	Bytes 5 to 7: 1 to 16,777,215 (3 bytes), zero is not allowed
Maximum Number of Segments:	Byte 8: 1 to 255 (1 byte), zero is not allowed
Or Num of Segments that can be sent:	Byte 8: 0 to 255 (1 byte)
Or Assurance Data Size	Byte 8: 0 to 52 (1 byte)
Or Role of Sender	Byte 8.1 to 8.2: 0 to 3 (2 bits)
Assurance Data Type:	Byte 9: 0 to 255 (1 byte)
Or Request Code:	Byte 9: 0 to 255 (1 byte)
Or Reason Code:	Byte 9: 0 to 255 (1 byte)
PGN:	Bytes 10 to 12: 0 to 262144 (3 bytes using 18 bits) (see 6.1.3)
Assurance Content:	Bytes 13 to X: 0 to 52 bytes

Figure 30 - Format of messages for FD transport protocol

Connection Mode Request to Send (FD.TP.CM_RTS): Destination Specific
- Byte: 1.1 to 1.4 Control Type = 0000_b, Destination Specific Request_To_Send (RTS)
- 1.5 to 1.8 Session Number
- 2 to 4 Total message size, number of bytes
- 5 to 7 Total number of segments
- 8 Maximum number of segments that can be sent in response to one CTS.
- 9 Assurance Data Type (ADT)
- 10 to 12 PGN of the segmented message
  - Byte 10 LSB of PGN
  - Byte 11 2nd byte of PGN
  - Byte 12 MSB of PGN

Connection Mode Clear to Send (FD.TP.CM_CTS): Destination Specific
- Byte: 1.1 to 1.4 Control byte = 0001_b, Destination Specific Clear_To_Send (CTS)
- 1.5 to 1.8 Session Number
- 2 to 4 Reserved for assignment by SAE, these bytes should be filled with FF_h in each
- 5 to 7 Next segment number to be sent
- 8 Number of segments that can be sent.
- 9 Request code
- 10 to 12 PGN of the segmented message

End of Message Status (FD.TP.CM_EndOfMsgStatus): Destination Specific or Global Destination (for BAM)
- Byte: 1.1 to 1.4 Control byte = 0010_b, End_of_Message Status
- 1.5 to 1.8 Session Number
- 2 to 4 Total message size transmitted, number of bytes
- 5 to 7 Total number of segments transmitted
- 8 Size of Assurance Data
- 9 Assurance Data Type (must match RTS or BAM indication of ADT)
- 10 to 12 PGN of the segmented message
- 13 up to 64 Assurance Data of full message calculated using AD Type. Total length = Size in byte 8.

End of Message Acknowledgment (FD.TP.CM_EndOfMsgACK): Destination Specific
- Byte: 1.1 to 1.4 Control byte = 0011_b, End_of_Message Acknowledge
- 1.5 to 1.8 Session Number
- 2 to 4 Total message size, number of bytes
- 5 to 7 Total number of segments
- 8 Reserved for assignment by SAE, this byte should be filled with FF_h
- 9 Reserved for assignment by SAE, this byte should be filled with FF_h
- 10 to 12 PGN of the segmented message

Connection Abort (FD.TP.Conn_Abort): Destination Specific
- Byte: 1.1 to 1.4 Control byte = 1111_b, Connection Abort
- 1.5 to 1.8 Session Number
- 2 to 4 Reserved for assignment by SAE, these bytes should be filled with FF_h in each
- 5 to 7 Reserved for assignment by SAE, these bytes should be filled with FF_h in each
- 8.1 to 8.2 Role of Sender
- 8.3 to 8.8 Reserved for assignment by SAE, these bits should be filled with ones
- 9 Connection Abort reason
- 10 to 12 PGN of the segmented message

Broadcast Announce Message (FD.TP.CM_BAM): Global Destination
- Byte: 1.1 to 1.4 Control byte = 0100_b, Broadcast Announce Message
- 1.5 to 1.8 Session Number
- 2 to 4 Total message size, number of bytes
- 5 to 7 Total number of segments
- 8 Reserved for assignment by SAE, this byte should be filled with FF_h
- 9 Assurance Data Type
- 10 to 12 PGN of the segmented message

Figure 30 - Format of messages for FD transport protocol (continued)

6.6.3.1 Connection Mode Request to Send (RTS)

The FD.TP.CM_RTS (RTS) message, shown in Figure 31, informs a responder that the originator wishes to open a virtual connection with it for the purpose of sending SAE J1939 PG data to the responder. The RTS message is identified by a Control Byte value of 0. This message is only transmitted by the originator in an RTS/CTS transfer. The destination of the RTS message shall be a specific source address; it shall never be the global Destination Address.

The RTS message indicates the PGN of the large message to be sent, the PG data size, the number of segments into which the PG data is to be fragmented, the maximum number of segments that can be sent in response to one Clear to Send (CTS) message from the responder, and the session to be used. It can also indicate an Assurance Data Type to be used for functional safety and/or cybersecurity protection. The Maximum Number of Segments (MAX SGMTS) field allows the originator to limit the number of segments that can be sent following a CTS message.

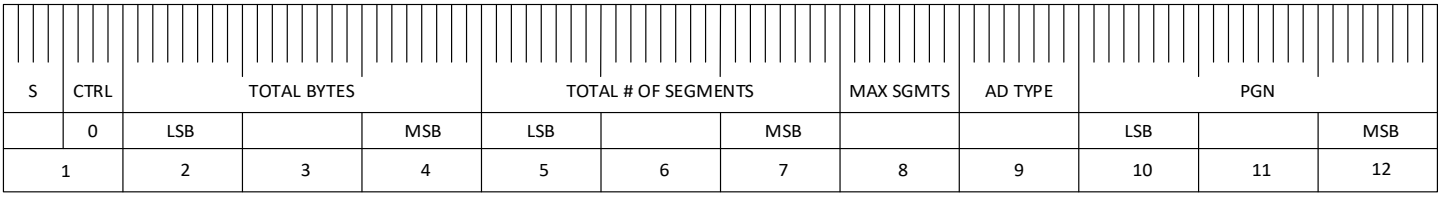


Figure 31 - Data format of RTS message

If multiple RTS messages are received from the same SA for the same PGN and session, then just the final RTS message shall be acted on and the other RTS messages shall be abandoned. No FD.TP.Conn_Abort message shall be sent for the abandoned RTS messages in this specific case.

The originator shall receive either an FD.TP.CM_CTS message or FD.TP.Conn_Abort message within T2 time after sending the FD.TP.CM_RTS message.

6.6.3.1.1 Session Number

The Session Number field (S) is used to uniquely identify a transport session. This field provides support for concurrent sessions. The session number together with the source address and destination address of the FD.TP.CM_CTS message shall be used to associate the message to a specific FD Transport connection. See 6.6.1.3 for further details.

6.6.3.1.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The RTS message uses a value of 0 for this field.

6.6.3.1.3 Total Message Size

The Total Message Size field (TOTAL BYTES) specifies the byte length of only the PG data. The value does not include the length of any assurance data. The value also does not include the four bytes of the FD.TP.DT message associated with segment numbers, session identification, or reserved bits. The Total Message Size can be 60 bytes or less and thus fit in a single FD. TP.DT frame. See 6.6.2.3 for an explanation of the minimum data size. For RTS/CTS transfer, the maximum A_PDU data size that can be transferred is 16777215 bytes.

6.6.3.1.4 Total Number of Segments

The Total Number of Segments field (TOTAL # OF SEGMENTS) specifies the number of data segments that are required to transmit the PG data. The minimum number of segments is 1. The maximum number of segments is 279621. See 6.6.2.3 for additional information.

6.6.3.1.5 Maximum Number of Segments

The Maximum Number of Segments field (MAX SGMTS) allows the originator to limit the number of segments the responder specifies in the CTS message. See Figure A3 in Appendix A for an example of this behavior. A responder shall comply with this limit to ensure that the originator can always retransmit segments that the responder may have not received for whatever reason. The Maximum Number of Segments shall always be less than or equal to the Total Number of Segments.

The originator shall have the ability to retain in its memory the number of data segments, as specified by "Maximum Number of Segments", until the responder sends a CTS indicating a desire to receive the next set of data segments. The responder has the option to Request some or all of the data segments associated with the most recent CTS before sending a CTS to continue on to the next set of segments. An example of this behavior is represented in Figure A2.

Flexibility is allowed for the maximum number of segments to be transmitted for a single CTS. This may be used by the system designer to minimize the bandwidth consumed by large message transfers. It is up to the implementer to determine how to utilize this capability.

6.6.3.1.6 Assurance Data Type

For functional safety or cybersecurity, an assurance field that covers the entire Data Transfer may be used. If used, the format and calculation method shall be indicated in byte 9 of Figure 31.

This field (AD TYPE) is an enumeration indicating the format and calculation method used for the assurance data to be later included in the FD.TP.CM_EndOfMsgStatus. Similar to the TF field for Multi-PG (see 6.5.3.6.1), only manufacturer specific formats are defined at the time of this publication. When companion SAE J1939 documents are published for cybersecurity and functional safety, this document will be updated to include any cited additions to the enumerations in this field. The current enumeration list is found in Table 10.

Table 10 - Coding of AD type field

ADT Value	Referenced Method/Format
0	No assurance data (default)
1	Manufacturer specific cybersecurity assurance data
2	Manufacturer specific functional safety assurance data
3	Manufacturer specific combined cybersecurity followed by functional safety assurance data
4 - 255	Reserved

6.6.3.2 Connection Mode Clear to Send (CTS)

The FD.TP.CM_CTS (CTS) message, shown in Figure 32, is used to inform the originator that the responder is ready to receive a certain amount of large message data. The CTS message is sent in response to the RTS message and following the reception of the last data segment per the previous CTS message. A CTS shall not be sent after receiving the final data segment unless the responder requires a resend of segments from the data segments of the previous CTS message. The CTS message is identified by a Control Byte value of 1. This message is only transmitted by the responder in a RTS/CTS transfer.

The CTS message contains the matching session number, the number of segments the node will accept, and the segment number of the next segment the responder is expecting. The responder uses the “number of segments” and “next segment” fields in each CTS message to control the flow. These fields allow the responder to adjust the number of segments transmitted following the CTS, pause the transfer of data segments, and request the retransmit of data segments. The responder can limit the number of data segments following a CTS message by increasing or decreasing the “number of segments” value. The responder can Request the retransmit of data segments using the “next segment” field. The responder can pause the data transfer by reporting zero for “number of segments to send.”

When sending an FD.TP.CM_CTS response to an FD.TP.CM_RTS, the responder shall send the FD.TP.CM_CTS message within T_r time after receiving FD.TP.CM_RTS. When sending an FD.TP.CM_CTS following the last FD.TP.DT message for the previous CTS and more data segments remain, the responder shall send the FD.TP.CM_CTS message within T_r time after receiving the last FD.TP.DT message.

In the case where the responder needs the data flow to be stopped for some number of seconds, the responder shall send a CTS message once per T_h time with the “number of segments to send” value equal to zero; this assures the originator that the connection is not closed. See 6.14 for the timing constraints.

The responder shall expect to receive a FD.TP.DT message for the session within T2 time after sending the FD.TP.CM_CTS message with “number of segments to send” greater than zero.

The CTS message not only controls the flow but also confirms correct receipt of all data segments since the prior CTS message was sent. Therefore, if information for the previous CTS was corrupted or missing, then a CTS to have the corrupted segment(s) repeated shall be sent before sending a CTS to continue on to the next set of segments. An example of this behavior is represented in Figure A2.

S	CTRL	RESERVED			NEXT SEGMENT NUMBER			XFR SGMTS	RQST	PGN		
	1	FF_h	FF_h	FF_h	LSB		MSB			LSB		MSB
1		2	3	4	5	6	7	8	9	10	11	12

Figure 32 - Data format of CTS message

If multiple CTS messages are received for the same session and with the same data (other than zero segments of transfer used to keep a connection open) after a connection is already established and before completing the Requested operation, then the connection can be aborted. When the originator aborts the connection, it shall send FD.TP.Conn_Abort with abort reason 4 from Table 11.

The responder will not send the next CTS until it has received the last data segment Requested in the previous CTS message, or it has timed out. In the case of time out the responder has the choice whether to send a connection abort or to send another CTS message to attempt to keep the connection open.

The following cases exist when data transfer happens with errors:

- A missing or errant segment(s) is detected and the last segment is successfully received. The responder will send a CTS Requesting retransmission starting from the missing segment.
- If the last segment is not received, a T1 time out shall occur. In this case, the responder may choose to send a CTS asking to repeat the last segment or send a FD.TP.Conn_Abort with reason 3 from Table 11. See Figure A5.
- Missing the FD.TP.CM_EndOfMsgStatus message before time out T1. In this case, the responder can choose to send a CTS Requesting a retransmission of the FD.TP.CM_EndOfMsgStatus or a FD.TP.Conn_Abort with reason 4 from Table 11. See Figure A5.

When the CTS message is used to Request the retransmission of data segment(s), it is recommended not to use more than 2 retransmit Requests. When the maximum number of retransmit Requests have been sent, the responder shall send a FD.TP.Conn_Abort with reason 5 from Table 11.

If a CTS message is received while a connection is not established, it shall be ignored.

6.6.3.2.1 Session Field

The Session field (S) is used to uniquely identify a transport session. This field provides support for concurrent sessions. The session field value together with the source address and destination address of the FD.TP.CM_CTS message shall be used to associate the message to a specific FD Transport connection. See 6.6.1.3 for further details.

6.6.3.2.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The CTS message uses a value of 1 for this field.

6.6.3.2.3 Next Segment Number

The Next Segment Number field specifies the segment number of the first data segment to be sent in the next set of data segments.

The Next Segment Number shall be set to 1 for the CTS message sent in response to the RTS message.

When all data segments for the previous CTS are received successfully, then the Next Segment Number shall be one greater than the last segment number cleared per the previous CTS.

If any data segments for the previous CTS were not received successfully, then the Next Segment Number shall be one greater than the last segment number received per that previous CTS.

A responder is not permitted to specify a Next Segment Number that is less than the Next Segment Number specified in the previous CTS.

If the responder requires the originator to resend segments associated with the previous CTS, then the Next Segment Number shall be a segment number within the range of segments cleared with the previous CTS. For a resend Request, the Next Segment Number shall be greater than or equal to the Next Segment Number in the previous CTS and shall be less than or equal to the last segment number cleared by the previous CTS.

When the Request field (RQST) is set to 1 (i.e., Requesting a resend of the EOMS message), then the Next Segment Number shall be set to $FFFFFF_h$.

6.6.3.2.4 Number of Segments to Send

The Number of Segments to Send field (XFR SGMTS) allows the responder to specify the number of segments expected to be sent by the originator in response to the CTS message.

The Number of Segments value shall always be less than or equal to the “Maximum Number of Segments that can be Sent” specified in the RTS by the originator. Consequently, it will always be less than or equal to the “Total Number of Segments” specified in the RTS by the originator as well.

The Number of Segments value shall always be less than or equal to the number of segments remaining to be sent.

When the Request field (RQST) is set to 1 (i.e., Requesting a resend of the EOMS message), then any value can be reported for the Number of Segments value since this field shall be ignored by the originator.

Flexibility is allowed for the number of segments to send for a single CTS. This may be used by the system designer to minimize the bandwidth consumed by large message transfers. It is up to the implementer to determine how to utilize this capability.

6.6.3.2.5 Request Field

The Request field (RQST) allows the responder to Request the originator to resend the FD.TP.CM_EndOfMsgStatus (EOMS) message. The originator is required to send the EOMS after it transmits the final data segment for the PG data. If the responder fails to receive the EOMS, the responder shall use this field to Request the EOMS to be resent.

The responder may Request the FD.TP.CM_EndOfMsgStatus to be resent prior to the T3 timeout by sending a CTS message with the RQST field set to 1 and the and the Next Segment Number set to $FFFFFF_h$. In this case, the Number of Segments to Transfer may be set to any value as it should be ignored by the originator. When used, this Request must be sent prior to sending the FD.TP.CM_EndOfMsgACK.

The Request Field shall be set to 0 for all other instances of CTS message. Originators shall ignore this field until all FD.TP.DT segments have been sent.

6.6.3.3 End of Message Status (EOMS)

The FD.TP.CM_EndOfMsgStatus (EOMS) message, shown in Figure 33, is used to inform the responder(s) that the originator has transmitted all of the PG data and optionally to provide the Assurance Data for the PG data. Figure 33 shows the message format with and without Assurance Data. This message is only transmitted by the originator in both RTS/CTS transfer and BAM transfer.

The originator shall automatically send this message within T_r time timeout following its transmit of the last (final) FD.TP.DT segment. For an RTS/CTS transfer, the originator shall also send this message if it has transmitted the last (final) FD.TP.DT segment and it receives, from the responder, a CTS message with the Request field set to 1.

The originator shall receive either an FD.TP.CM_CTS within T3 time or FD.TP.CM_EndOfMsgACK within T5 time after the FD.TP.CM_EndOfMsgStatus was transmitted.

If the Assurance Data is used, the AD size must be included to indicate to the receiver how much of the data following the PGN is the Assurance Data. The calculation method (ADT) must also be indicated when Assurance Data is used so the recipient can properly calculate a match.

The length of this message is variable. It will be 12 bytes if no Assurance Data is provided. It will be up to 64 bytes if Assurance Data is provided. See 6.6.3.1.6 for details of the ADT enumeration. If assurance data is provided and the resulting data content does not match a valid FD DLC, then padding bytes, as specified in 6.3.3.2, shall be added following the assurance data.

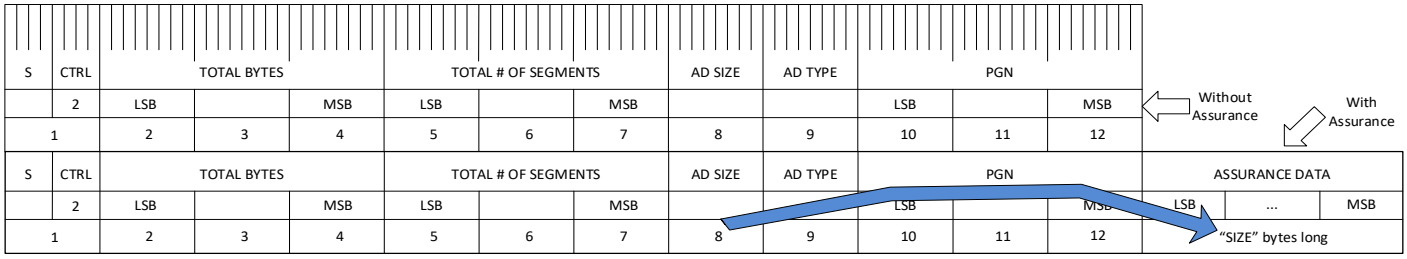


Figure 33 - Data format of EOMS message

6.6.3.3.1 Session Field

The Session field (S) is used to uniquely identify a transport session. See 6.6.1.3 for further details.

6.6.3.3.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The EOMS message uses a value of 2 for this field.

6.6.3.3.3 Total Message Size

The Total Message Size field (TOTAL BYTES) specifies the byte length of only the PG data. See 6.6.3.1.3.

6.6.3.3.4 Total Number of Segments

The Total Number of Segments field (TOTAL # OF SEGMENTS) specifies the number of data segments that are required to transmit the PG data. See 6.6.3.1.4.

6.6.3.3.5 Assurance Data Type

The Assurance Data Type field (AD TYPE) specifies the format and calculation method used for the assurance data in the FD.TP.CM_EndOfMsgStatus. See 6.6.3.1.6.

6.6.3.3.6 Assurance Data Size

The Assurance Data Size field (AD SIZE) specifies the byte length of the assurance data that follows the PGN field in the message. The AD SIZE allows the responder to know how many bytes after the PGN field are part of the Assurance Data versus part of message padding.

The AD SIZE value shall be reported as zero when there is no assurance data.

6.6.3.3.7 Assurance Data

The Assurance Data field (ASSURANCE DATA) contains any assurance data associated with the PG data. The maximum length of the Assurance Data field is 52 bytes. The Assurance Data field is omitted (or 0 bytes long) when no assurance data is provided.

6.6.3.4 End of Message Acknowledgment (EOMA)

The FD.TP.CM_EndOfMsgACK (EOMA) message, shown in Figure 34, is used to inform the originator that the entire large data was received and reassembled correctly. This message is only transmitted by the responder in an RTS/CTS transfer.

The responder shall send the FD.TP.CM_EndOfMsgACK within T3 time of receiving the EOMS message, unless the responder sends a FD.TP.CM_CTS to Request a resend of segments from the final CTS. The responder can keep the connection open after the EOMS message by not immediately sending the EOMA message. This delay tactic allows the responder time to perform final processing of the data, such as assurance data validation.

The FD.TP.CM_EndOfMsgACK shall include the PGN which was received, the session it was received on, and the amount of data that was received as shown in Figure 34.

S	CTRL	TOTAL BYTES (RECEIVED)			TOTAL # OF SEGMENTS (RECEIVED)			RESERVED	RESERVED	PGN		
	3	LSB		MSB	LSB		MSB	FF_h	FF_h	LSB		MSB
1		2	3	4	5	6	7	8	9	10	11	12

Figure 34 - Data format of EOMA message

If an FD.TP.CM_EndOfMsgACK is received by the originator prior to the final Data Transfer, then the originator shall ignore that FD.TP.CM_EndOfMsgACK.

FD.TP.CM_EndOfMsgACK is only transmitted by the responder and only if the transfer method is destination specific.

6.6.3.4.1 Session Field

The Session field (S) is used to uniquely identify a transport session. See 6.6.1.3 for further details.

6.6.3.4.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The EOMA message uses a value of 3 for this field.

6.6.3.4.3 Total Message Size

The Total Message Size field (TOTAL BYTES (RECEIVED)) specifies the byte length of the PG data received. See 6.6.3.1.3.

6.6.3.4.4 Total Number of Segments

The Total Number of Segments field (TOTAL # OF SEGMENTS (RECEIVED)) specifies the number of data segments that were received for the PG data. See 6.6.3.1.4.

6.6.3.5 Connection Abort (Abort)

The FD.TP.Conn_Abort (Abort) message, shown in Figure 35, is used to indicate that the FD transfer has been canceled by the message originator or shall be canceled. This message may be transmitted by either the originator or responder in an RTS/CTS transfer. This message may be transmitted only by the originator in a BAM transfer. This message shall not be transmitted by the responder(s) in a BAM transfer.

The originator shall stop transmitting FD.CM and FD.TP.DT messages for the session after it receives the FD.TP.Conn_Abort message from the responder. The process to stop transmitting data segments shall take no more than 32 data segments and shall not exceed 50 ms. After sending or receiving a FD.TP.Conn_Abort message, the responder shall ignore all data segments of the session.

S	CTRL	RESERVED			RESERVED			RESERVED	ROLE	REASON	PGN		
	15	FF_h	FF_h	FF_h	FF_h	FF_h	FF_h	FC_h			LSB		MSB
1		2	3	4	5	6	7	8		9	10	11	12

Figure 35 - Data format of abort message

When either the originator or responder decides to close a connection for any reason, prior to completing the data transfer, including a timeout, it shall send a FD.TP.Conn_Abort message shown in Figure 35 with the appropriate Connection Abort reason (see 6.6.3.5.3) and the appropriate Role of Sender (see 6.6.3.5.4).

6.6.3.5.1 Session Field

The Session field (S) is used to uniquely identify a transport session. See 6.6.1.3 for further details.

6.6.3.5.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The Abort message uses a value of 15 for this field.

6.6.3.5.3 Reason Field

The Reason field is used to identify the abort code from Table 11.

Table 11 - Connection abort reason

Value	Description
0	Reserved for SAE assignment
1	Cannot support another transport session
2	System resources were needed for another task so this connection managed session was terminated
3	A timeout occurred and this is the connection abort to close the session
4	CTS messages received when data transfer is in progress
5	Maximum retransmit Request limit reached
6	Unexpected data transfer segment
7	Bad sequence/segment number (software cannot recover)
8	Duplicate sequence/segment number (software cannot recover)
9	“Total Message Size” exceeds system resources
10	Assurance Data does not match expected value (software cannot recover)
11	Assurance Data not received (if required)
12-249	Reserved for SAE assignment
250	If a Connection Abort reason is identified that is not listed in the table, use code 250
251-255	Per SAE J1939-71 definitions

6.6.3.5.4 Role of Sender Field

The Role of Sender is used to identify the specific transport connection that has been canceled or shall be canceled. The Role of Sender indicates the role of the Conn_Abort sender as being either the originator or the responder in the transport connection associated with the Abort message. The Role of Sender values are listed in Table 12. The Role of Sender value is used together with the Session value to associate the Abort message to the transport connection where the Conn_Abort sender is either the originator or the responder in that transport connection.

It is possible to have simultaneous transport connections with the same Session number that are transferring data in the opposite direction between the same two Controller Applications. The Role of Sender differentiates transport connections with the same Session value by specifying the role of the Conn_Abort sender in the transport connection. For example, it is possible to have simultaneous RTS/CTS FD.TP connections, both identified as Session 1, where one connection has CA1 as originator and CA2 as responder and the other connection has CA2 as originator and CA1 as responder. If CA1 sends a 'Session 1' Conn_Abort message to CA2, the Role of Sender value clarifies which Session 1 FD.TP connection is to be aborted, either the session where CA1 is the originator or the session where CA1 is the responder.

When the originator Controller Application aborts a FD.TP connection, it shall set the “Role of Sender” to 00_b. When the responder Controller Application aborts a FD.TP connection, it shall set the “Role of Sender” to 01_b. If there are two FD.TP connections between two Controller Applications that have the same Session number and a Controller Application choses to abort both FD.TP connections, then it shall send two FD.TP.Conn_Abort messages: one for “Role of Sender” set to 00_b, and one for “Role of Sender” set to 01_b.

When a FD.TP.Conn_Abort is received with the “Role of Sender” set to 11_b, the Controller Application shall terminate all FD.TP connections that have the specified Session number with the Controller Application that sent the FD.TP.Conn_Abort. A value of 11_b shall only be used by applications developed to the JUL2021 or prior release of this document.

Table 12 - Connection abort role of sender

Value	Description
00_b	Conn_Abort sender is the originating Controller Application in the transport connection
01_b	Conn_Abort sender is the responding Controller Application in the transport connection
10_b	Reserved for assignment by SAE
11_b	Role of Conn_Abort sender role in the transport connection is not specified

6.6.3.6 Broadcast Announce Message (BAM)

The FD.TP.CM_BAM (BAM) message, shown in Figure 36, is used to inform all the nodes of the network that a large message is about to be broadcast. The destination of the BAM message shall be the global Destination Address. This message can be transmitted only by the originator in a BAM transfer.

After a BAM message is sent, the originator shall begin sending the FD.TP.DT messages for the segmented PG data.

The responder shall expect to receive an FD.TP.DT message for the session within T1 seconds after receiving the FD.TP.CM_BAM message.

S	CTRL	TOTAL BYTES			TOTAL # OF SEGMENTS			RESERVED	AD TYPE	PGN		
	4	LSB		MSB	LSB		MSB	FF_h		LSB		MSB
1		2	3	4	5	6	7	8	9	10	11	12

Figure 36 - Data format of BAM message

6.6.3.6.1 Session Field

The Session field (S) is used to uniquely identify a transport session. See 6.6.1.3 for further details.

6.6.3.6.2 Control Field

The Control field (CTRL) is used to identify the type of Connection Management message in use. The BAM message uses a value of 4 for this field.

6.6.3.6.3 Total Message Size

The Total Message Size field (TOTAL BYTES) specifies the byte length of only the PG data. See 6.6.3.1.3.

6.6.3.6.4 Total Number of Segments

The Total Number of Segments field (TOTAL # OF SEGMENTS) specifies the number of data segments that are required to transmit the PG data. See 6.6.3.1.4.

6.6.3.6.5 Assurance Data Type

The Assurance Data Type field (AD TYPE) specifies the format and calculation method used for the assurance data in the FD.TP.CM_EndOfMsgStatus. See 6.6.3.1.6.

6.6.4 FD Transport Protocol - Data Transfer Message (FD.TP.DT)

The FD.TP.DT (DT) message, shown in Figure 37, is used to transmit each segment of PG data within a FD Transport session.

Each DT message shall be sent as a single D_PDU1 FEFF data frame with the FD.TP.DT PGN specified in the 29-bit CAN identifier. The FD.TP.DT PG shall never be transmitted as a C-PG within a Multi-PG message. The FD.TP.DT message is only transmitted by the originator.

The FD Transport Protocol communicates large messages by fragmenting the PG data into a sequenced series of 60 byte segments and then sequentially transmitting those segments using the FD.TP.DT PG to the responder(s). Every data segment shall contain 60 bytes of the PG data, except the last segment which can be as short as 1 byte. Under certain circumstances, FD Transport Protocol is required for PGs with 60 bytes or less of PG data (see 6.6.2.3). When FD Transport is required for PG data up to 60 bytes long, then there shall be only 1 data segment.

Each DT message transmits a single segment of the segmented PG data for a transport session.

The DT message data field contains the session number, the PG data segment, and the sequential order of the data segment among all of the data segments. The data segments shall be transmitted in increasing sequential order. The segment number field in the DT message specifies the sequential order of the associated data segment. For example, if the PG data must be fragmented into 5 segments in order to be communicated, then 5 DT messages would be required to transmit the PG data denoted as segments 1 through 5, respectively. Examples showing DT messages in use can be seen in Appendix A.

The DT message source address, Destination Address, and session field value shall be used to associate the DT message to a specific FD Transport connection. For an RTS/CTS data transfer, the Destination Address of each DT message shall be the responder's source address. For a BAM data transfer, the Destination Address of each DT message shall be the global Destination Address.

The time between consecutive FD.TP.DT messages for a BAM data transfer session shall be 10 to 200 ms. The time between consecutive FD.TP.DT messages for an RTS/CTS data transfer session shall be 0 to 200 ms. For an RTS/CTS data transfer, the time between consecutive FD.TP.DT messages only applies when the CTS “Number of Segments to Send” value is greater than 1. Responders must be aware that back-to-back CAN data frames can occur and they may contain the same CAN ID. The responder shall use a timeout of T1 (provides margin allowing for the maximum spacing of 200 ms). For all timeouts, see 6.14.

Figure 38 shows the FD.TP.DT message frame structure.

Table B1 has the SPN assignments to parameters in DT shown in Figure 37.

Parameter Group Name:	**FD Transport Protocol—Data Transfer (FD.TP.DT)**
Definition:	Used for the transfer PG data segments using the FD Transport Protocol.
Transmission repetition rate:	10 - 200ms for BAM data transfers No more than 200ms for RTS/CTS data transfers
Data length:	Up to 64 bytes
Extended Data Package:	0
Data Page:	0
PDU Format:	78
PDU specified field:	Destination Address (global or specific) Global DA = 255 is used for BAM data transfers Global DA is not allowed for RTS/CTS data transfers
Default priority:	7
Parameter Group Number:	19968 ($004E00_h$)

Data ranges for parameters used in this Parameter Group:

Byte:	1.1 to 1.4	Data Transfer Format Indicator
	1.5 to 1.8	Session Number
	2 to 4	Segment Number
	5 up to 64	Segmented data. Note the last segment of a segmented PG could contain fewer bytes than the previous segments.

Figure 37 - FD transport protocol - data transfer message (FD.TP.DT)

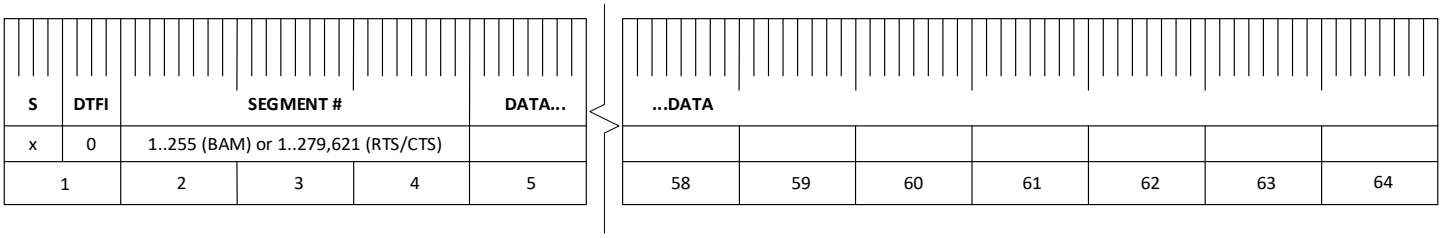


Figure 38 - FD transport protocol - data transfer message

6.6.4.1 Session Field

The Session field (S) is used to uniquely identify a transport session. This field provides support for concurrent sessions. The session field value together with the source address and destination address of the FD.TP.DT message shall be used to associate the FD.TP.DT message to a specific FD Transport connection. This field provides support for concurrent sessions. See 6.6.1.3 for details.

6.6.4.2 DT Format Indicator Field

The DT Format Indicator field (DTFI) is used to indicate the format of the message field. The DTFI shall be reported as 0 to indicate the current standard format. Non-zero values in this field are reserved for future SAE J1939-22 use. Future values can be as high as 15. Content after the first byte may be formatted differently than shown here for non-zero values.

6.6.4.3 Segment Number Field

The Segment Number field (SEGMENT #) is used to identify the absolute segment order of the contained data content. A segment number of 0 is not valid. Segments shall be transmitted in order using a monotonically increasing segment number.

The minimum valid segment number is 1. The maximum segment number for an RTS/CTS transfer is 279621.

The maximum segment number is 255 for a BAM transfer.

6.6.4.4 Data Field

The Data field (DATA) is used to contain the identified sequential data segment of the PG data. The Data field shall contain the 60 byte segment of the PG data, except for the last segment of the PG data. If the last segment of the PG data is less than 60 bytes in length and the message length doesn't equal one of the standard CAN FD data frame lengths, then padding bytes, as specified in 6.3.3.2, shall be added following the data segment data. Responders shall use the Total Bytes value reported in the RTS or BAM message to parse out the data segment bytes from any padding bytes in the Data field of the final FD.TP.DT message.

6.6.5 Connection Constraints

For an RTS/CTS connection Request, if the responder cannot handle another session, then it should reject any additional connection initiations. In such cases, the additional Requested session shall be rejected by sending a FD.TP.Conn_Abort with abort reason 1 from Table 11. This allows the originator of the desired connection to move on to a new connection without having to wait for a timeout.

Data coherency is the responsibility of the application and the system designer. Some design rules to consider include:

- Consider the receiver actions if the same PG is sent in a manner that could result in older data being received later than newer data. For example, consider a situation where the same PG is sent on multiple transport sessions simultaneously between the same two nodes or on more than one BAM channel simultaneously from the same source address.

- Consider a situation where variable length messages are sent using both Multi-PG and Transport depending on the length at the time. For example, consider a situation where DM1 is being transmitted using BAM. Before that BAM completes, another DM1 message (short enough to be sent using Multi-PG) is transmitted and received. This could happen when some events become previously active and so they are removed from DM1.

6.6.5.1 Number and Type of Connections a Node Must Support

Each node on the network can originate up to eight RTS/CTS data transfer connections with a given DA at a time.

Each node on the network can originate up to four BAM transfers.

Responders must recognize that multiple FD.TP.CM and FD.TP.DT messages can be received, interspersed with one another, from different originator SAs as well as the same originator SA.

Nodes are not required to support large message transports using BAM or RTS/CTS. However, if a node does support large message transport, the node must be able to support reception of at least one RTS/CTS session and at least one BAM session from the same SA. Gateway devices, telemetry devices, and other devices with a lot of data to send or receive are recommended to support more than one connection of each type.

Regardless of whether a node can support multiple simultaneous Transport Protocol sessions (RTS/CTS and/or BAM), it must assure that FD.TP.CM and FD.TP.DT messages from the same SA with different sessions can be differentiated. Receivers must use the session number, DA, and SA to associate each message with the correct transfer session.

6.6.5.2 Concurrent PG Transmission

It is possible that a PG defined as variable length may sometimes be sent in a Multi-PG and other times sent using FD Transport Protocol. Simultaneous transmission of the same PG using Multi-PG and transport should be avoided. It is acceptable to abort an in-process transport session if a shorter Multi-PG update to the PG becomes available prior to completing a transport.

An example of this case is DM1 because it is triggered by change of state of its contents. A transport session may be required to send the DM1 but, before the initial transport is completed (due to interframe spacing requirements), a change to the data making it shorter could trigger another transmission of the DM1 which now can be sent using Multi-PG. In this case, the original DM1 transport session may be aborted by the originator.

If a PG and its assurance data can be sent using Multi-PG, then the Multi-PG format shall be used. If it is too large for Multi-PG, then a Transport Protocol session shall be used.

6.7 Message Transmit Behavior

An A_PDU may be transmitted in multiple ways depending on size and PDU Type. Figure 39 shows the decision tree for which method to use in transmitting a given PG.

Figure 39 includes a Multi-PG D_PDU Transmit Control block. This feature is further described in 6.5.4.

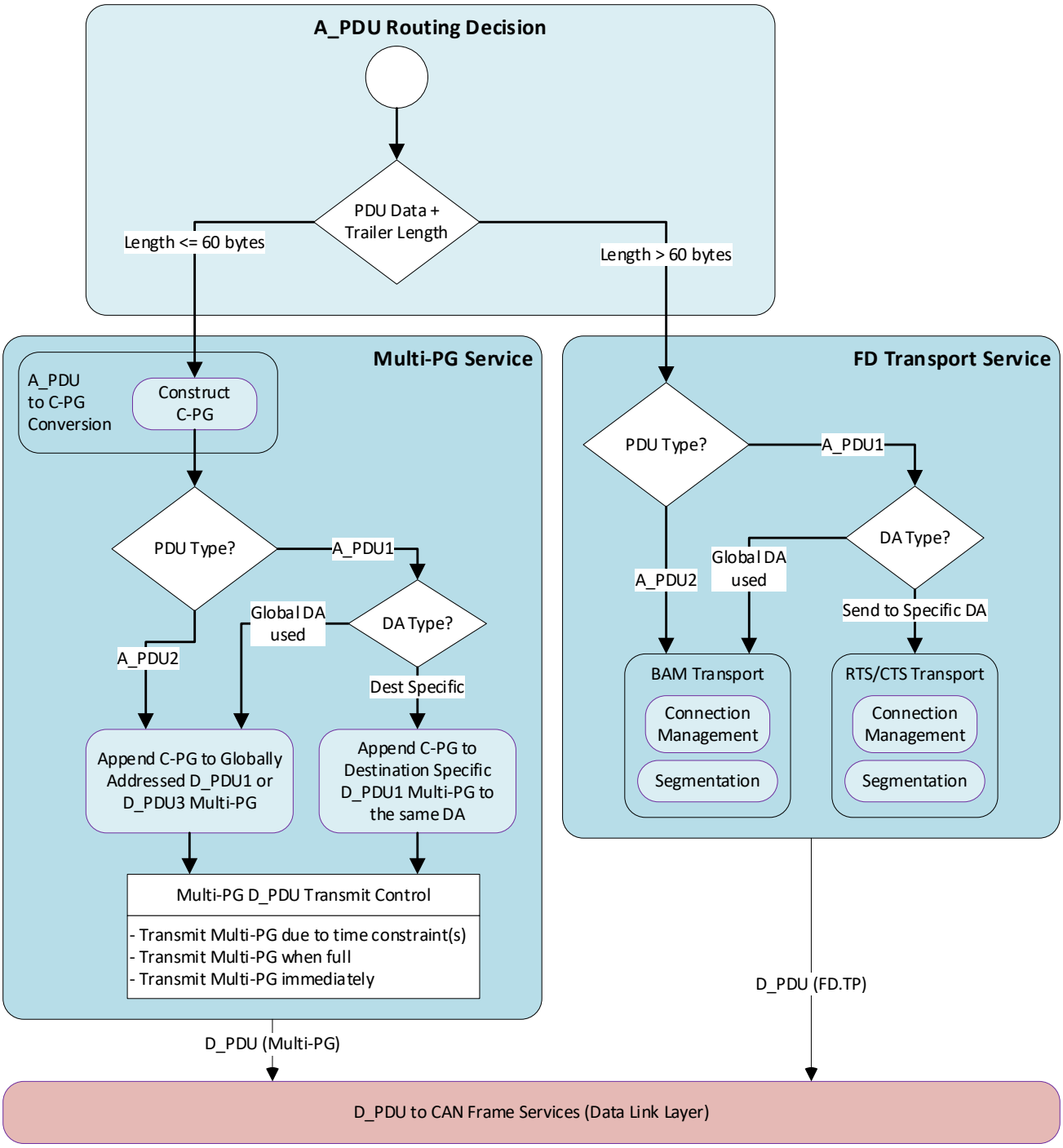


Figure 39 - Transmit behavior model

6.8 Address Claimed Service

The Address Claimed service is described in SAE J1939-81. The Address Claimed service shall be transmitted using a globally addressed D_PDU1 frame without using Multi-PG. It is a special exception of an 8-byte PG transmitted without using Multi-PG to allow special reception handling. This handling path is shown in Figures 1 and 2 to indicate the unique requirements. The Address Claimed PG may be sent using a CEFF or FEFF frame although FEFF is preferred.

Note that because the Address Claimed PG must be sent without using Multi-PG, it is not possible to protect its contents with assurance data for cybersecurity or functional safety.

6.9 Message Types

There are seven message types (uses) currently supported. These types are the following: Commands, Requests, Broadcasts/Responses (Data Messages), Acknowledgment, Transfer, Group Function, and Proprietary Communications. The specific message type is recognized by its assigned PGN. Refer to SAE J1939DA document for examples of PGN assignments.

6.9.1 Command

This message type categorizes those PGs that convey a command to a specific or global destination from a source. The destination is then expected to take specific actions based on the reception of this command message type.

Both PDU1 Format (PS = DA) and PDU2 Format (PS = GE) PGs can be used for commands. Example command type messages may include “Transmission Control,” “Address Request,” “Torque/Speed Control,” etc.

6.9.2 Data Messages

This Message Type categorizes those PGs that convey operational status data, measurement data, or diagnostic data. PGs of this type may be sent as an unsolicited broadcast of information from a device or as a response to a Command or a Request.

6.9.3 Request

This message type categorizes those PGs that convey a solicitation for a PG. Such solicitations may be used to Request information globally or from a specific DA. Requests specific to one DA are known as destination specific Requests. Request services exist for both standard PGs and proprietary PGs.

6.9.4 Acknowledgment

This message type categorizes PGs that convey an acknowledgement, either positive or negative, as a response to a specific command or Request. The Acknowledgment PG is a type of Group Function message.

Acknowledgment in this document refers to a specific message not to be confused with the ACK field described in ISO 11898-1.

6.9.5 Transfer

This message type categorizes PGs that convey data on behalf of devices not located directly on the same CAN segment. It is useful in cases where a given ECU is tasked with reporting a PG and data about more than one controller application. Examples include PGs such as Vehicle Identification, Component ID and Software Identification. The Transfer PG contains the response data being Requested. The Transfer PG is a type of Group Function message.

6.9.6 Group Function

This message type categorizes PGs that require additional handling to interpret the specific purpose of the message. Most of the messages that employ the Group Function concept have not been labeled in any way with the Group Function moniker. Example Group Function PGs include: proprietary functions, Request2, Acknowledgement, network management functions, multipacket transport connection management, and Multi-PG. Group functions are unique and specific to the PGN with which they are associated. See Figures 43 and 44 for examples. The group function feature is defined within the data structure (often the first byte of the data field). For example, the Acknowledgment PG (Figure 44) includes a Control Byte in the first byte position of the data. The value of this Control Byte defines how the remaining 7 bytes are to be interpreted. More detailed explanation of the group function is provided with its PG definition.

6.9.7 Proprietary Communications

This message type categorizes PGs that convey manufacturer specific data. The Proprietary message types provide a common set of PGNs used by all manufacturers to transmit proprietary content. The definition of proprietary PGs has been established allowing all D_PDU Formats to be used. The interpretation of the proprietary information varies by manufacturer. For example, engine manufacturer “A’s” proprietary communications are likely to be different than engine manufacturer “B’s” even though they both use the same source address.

512 PGNs have been assigned for non-destination specific proprietary communications using PDU2, another 1 PGN has been assigned using PDU3, and two PGNs have been assigned for destination specific proprietary communications using PDU1. This allows for two functions: (a) a specific SA can send its proprietary message in a PDU2 Format (non-destination specific) with the PS field identified as desired by the user; or (b) a specific SA can send its proprietary message in a PDU1 Format (destination specific) to a specific DA. For example, destination specific proprietary messages can be used in situations where a service tool must direct its communication to a specific DA out of a possible group of controllers. The global DA should not be used with Proprietary A and Proprietary A2 PGs.

A case can arise when an engine uses more than one controller but wants to be able to perform diagnostics while all of its controllers are connected to the same network. In this case the proprietary protocol needs to be able to be destination specific.

Proprietary communications are useful in two situations:

a. Where it is unnecessary to have standardized communications.

b. Where it is important to communicate proprietary information.

Some of the communications between nodes constructed by a single manufacturer do not require standardization. The information communicated is not generally useful to other devices on the network. In this situation the proprietary PGNs can be used.

6.10 Message Services

These application layer protocol services shown in Figure 40 are used to support application requirements for the communication of PG data using a standard method. Some PG data transfers will need to be secured for functional safety and/or cybersecurity reasons. Additional assurance services may exist to support those needs.

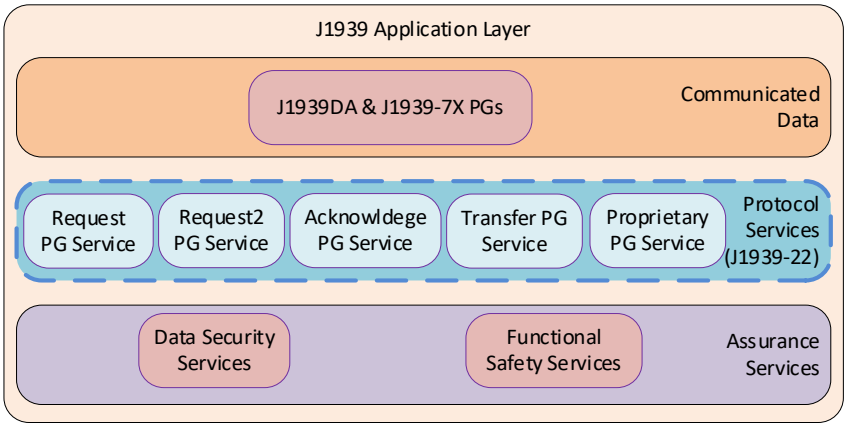


Figure 40 - Services

6.10.1 Request Service

The Request Service is identical to the Request Service in SAE J1939-21 though presented differently here. A Request PG is sent as a C-PG in a Multi-PG.

The information in Figure 41 shows the PG definition for the Request PG. Table B1 in Appendix B has the Suspect Parameter Number (SPN) assignment to the parameter in this message.

Parameter Group Name:	**Request (RQST)**
Definition:	Used to Request a Parameter Group from a network device or devices.
Transmission repetition rate:	Per user requirements, generally recommended that Requests for the same PG occur no more than two or three times per second.
Data length:	3 bytes
Extended Data Page:	0
Data page:	0
PDU Format:	234
PDU Specific:	Destination Address (global or specific)
Default priority:	6
Parameter Group Number:	59904 ($00EA00_h$)
Byte 1, bits 8-1	LSB of PGN being Requested (most significant at bit 8)
Byte 2, bits 8-1	Second byte of PGN being Requested (most significant at bit 8)
Byte 3, bits 8-1	MSB of PGN being Requested (most significant at bit 8)

(see 6.1.3 for additional clarification on byte content)

Figure 41 - Request PG definition

When requesting a PDU1 PGN, the LSB (Byte 1) of "PGN being Requested" in the data shall be 00_h (see 6.1.3). Do not include the Destination Address within the "PGN being Requested" value. In addition, per 6.5.3.6.2, the PF field for the Request PG in the C-PG Header shall be 00_h, since the Request PG is an A_PDU1 PG, and the Request PG Destination Address is derived from the Multi-PG D_PDU.

If a device fails to get a response (either the PG or the ACKM) to a Request within T_r, then the device may resend or retry the same Request. The number of retries for a specific Request should be limited to two retries, i.e., the Request is issued a total of three times. If the device fails to get a response (either the PG or the ACKM) to the Request after the third retry, then the device should abandon further Request attempts for the same information or the device may wait for an extended period of time (minutes rather than seconds) before attempting to Request the same information.

Packing multiple requests into a single Multi-PG can result in an impossible response timing situation for some Controller Applications. For example, when requesting multiple PGs which all require Transport Protocol, the responding CA must support multiple sessions in order to avoid violating the response time (T_r = 200 ms) constraints on any PG after the first one. The transport layer cannot know of these constraints so the application should consider spreading the requests over more time if it knows the responding CA would not be able to honor the requests in time.

6.10.1.1 Request Response Behavior

Table 13 iterates the Request/response possibilities for A_PDU1 and A_PDU2 PGs. The transmitter of the Request response will determine whether the message is sent destination specific or global based on whether the Request was included in a Destination Specific D_PDU1 Multi-PG (DA Specific), in a Globally Addressed D_PDU1 Multi-PG (DA Global), or D_PDU3 Multi-PG (DA Global). Note that some PGs require FD Transport Protocol (FD.TP) use, so several CAN data frames can occur as a result of a single Request. Also note, a Request response including any assurance data shall be packed in a Multi-PG with other PGs if it doesn't require transport. When it is packed with other PGs, the expectations here still apply.

Table 13 - A_PDU1 and A_PDU2 transmit, Request, and response requirements

A_PDU Format of Requested PG	Data Length of Requested PG Including Optional Assurance Content	Request Method Used	Response	Response Type Used
1	≤60 bytes	DA Global	DA Global	Global Addressed D_PDU1 or D_PDU3 Multi-PG
1	≤60 bytes	DA Specific	DA Specific	Destination Specific D_PDU1 Multi-PG
1	>60 bytes	DA Specific	DA Specific	RTS/CTS FD Transport
1 or 2	>60 bytes	DA Global	DA Global	BAM FD Transport
2	>60 bytes	DA Specific	DA Global	BAM FD Transport
2	≤60 bytes	DA Specific	DA Global	Global Addressed D_PDU1 Multi-PG or D_PDU3 Multi-PG
2	≤60 bytes	DA Global	DA Global	Global Addressed D_PDU1 or D_PDU3 Multi-PG

Notes to Table 13 - General rules of operation for determining whether to send a PG to a global or specific destination:

1. If the Request or applicable PG is sent to the global DA (global Request), then the response is sent to the global DA.
   a. A NACK (ACKM with control byte = 1) must not be generated if the controller does not support the Requested PG.
   b. A BUSY (ACKM with control byte = 3) may be generated if the controller supports the Requested PG but cannot respond within T_r for the network segment.
   c. An ACKM (control byte = 0 or 1) is not desired as a response to a global Request for a supported PG. However, a global Request is allowed to be responded to with an ACK or a NACK for the result of the action taken when the Requested PG (e.g., DM3, DM11) is supported by a node and the Requested PG allows or requires an ACKM response. These cases will be documented in the appropriate SAE J1939 Recommended Practice document.
   d. An ACKM (with control byte = 2) may be generated as warranted.
   e. A controller shall not send both an ACKM and a PG response.
2. If the Request or applicable PG is sent to a specific DA, then a response is required.
   a. A NACK is required if the PGN is not supported.
   b. Responses shall be made to a specific DA, with the following exceptions:
      i. The Address Claimed PG is sent to the global DA even though the Request for it may have been to a specific DA (refer to SAE J1939-81). This PG shall not be incorporated in a Multi-PG data frame. It must be sent individually.
      ii. The Acknowledgment PG response uses a global DA even though the PG that causes Acknowledgment was sent to a specific DA.
3. An exception to these rules does exist and is specifically noted when this is the case in the applicable document and section where the PG is defined. This exception is when the response DA does not specify the SA of the Request but uses the global DA instead. Some examples have been noted above (e.g., Address Claimed PG and Acknowledgment PG).

Figure 42 documents the Table 13 Request and response rules in a flowchart format. The flowchart specifies the A_PDU to be transmitted. See 6.7 for the method used to transmit the A_PDU.

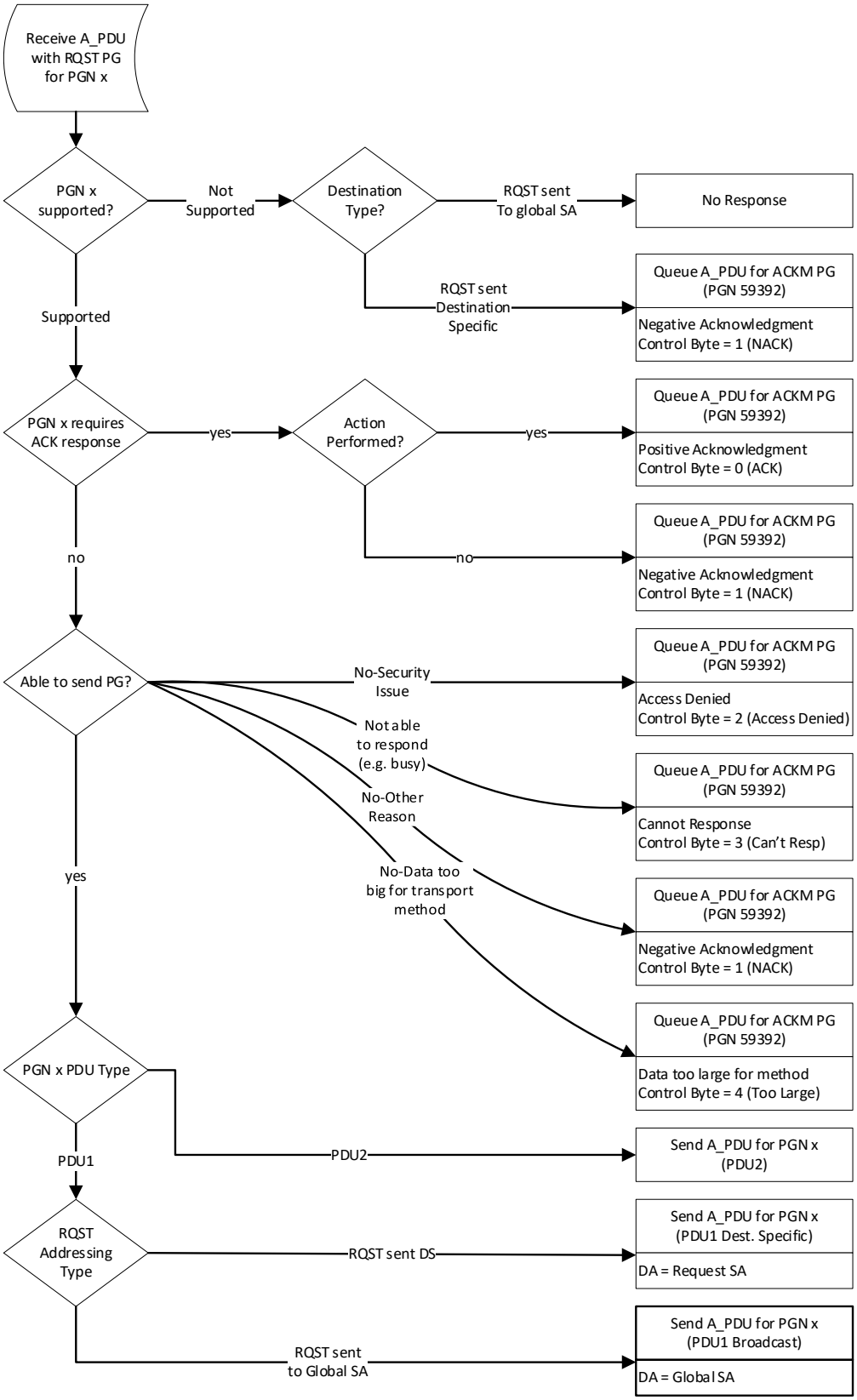


Figure 42 - Request response model

6.10.1.2 Investigative Request Use

The Request PG can be directed to a specific DA to determine if a specific PG is supported (i.e., does the Requested DA transmit the specific PG?). The response to the Request determines whether the PG is supported. If it is supported, then the responding device shall send the Requested information. If the Acknowledgment PG is appropriate, then the control byte shall be set appropriately. If it is not supported, the responding device sends the Acknowledgment PG with the control byte set to one, for NACK. The remaining portions of the SAE J1939 PDU Format and PG must be filled in appropriately (see 6.10.3.1). Note that per the definitions in this paragraph the phrase “not supported” means that the PG is not transmitted. It is not possible to determine whether a device will act upon the received PG by using this method.

6.10.1.3 Request Scheduling

The scheduling of a Request should be canceled if the information to be Requested is received prior to the Request being sent. That is, if the information is received 50 ms prior to Request scheduling, the Request shall not be issued. PGs should not be Requested if they are defined with a periodic transmit behavior. Exceptions may arise when the defined broadcast time exceeds a special case need.

6.10.1.4 Required Responses

A PG data response is required for a global Request from all devices that support the Requested PG, including the Requester. Devices that do not support the Requested PG shall not send the Acknowledgment PG for global Requests (except as outlined in the notes to Table 13, Item 1c, 6.10.1.1, which indicates than an ACK response is permitted for certain PGNs, such as DM3 and DM11).

A device which sends a Request to the global DA (255) (e.g., “Global Address Claimed Request”) shall itself send the Requested PG data response if it supports the Requested PG. This is a requirement because all devices are expected to respond. If the device issuing the Request does not respond, then the other network devices may draw the wrong conclusion about the Requested information.

Note that a device may be unable to respond to a global Request for a supported PG if the response requires a TP.BAM session and all TP.BAM queues are already in use (as per 6.6.5.1). For this reason, a Requesting device should issue multiple Requests (following an initial timeout) before concluding that PG data is not available. More detail is provided in 6.10.1.

6.10.1.5 Error Recovery

Error recovery for conditions that are not described in this document, where responses to queries were not received, are the responsibility of the individual application requirements. These application requirements may be described in another SAE J1939 document or in the device producer’s design requirements for a device or subsystem. For example:

1. There is no error recovery method directly specified for a timed out destination specific query; that is, a Request message sent to a non-existent DA will never be answered.

2. When the DA is known to exist, then an error condition is indicated by the lack of response, especially when a Control Byte value of 1 (Negative Acknowledgement) should have been sent.

In general, it is the responsibility of the Requester to determine whether to repeat the query to meet the needs of the application. It may be the case that the Requested data was assigned (or partitioned) to a different device or controller application at another SA. In such a case, a recovery plan may be to send a global Request instead of the destination specific Request. Like the recovery described in 6.10.1 for timed out global Requests, such recovery methods shall be limited to a reasonable number of attempts and a limited duration of time.

6.10.2 Request2 Service

Content in this section is identical to the Request2 section in SAE J1939-21. A Request2 group function PG is sent as a C-PG in a Multi-PG.

The Request2 PG provides the capability for the requestor to specify whether the responder should use the Transfer PG (PGN 51712). By identifying that the responder should use the Transfer PG, it provides the ability for the responder to report the data for the Requested PG for all of the devices it is tasked with reporting (see 6.10.5). All devices include the data the responding device would normally report upon receiving the same Requested PGN in a Request PG (PGN 59904) (properly formatted for Transfer PG) and the data set for each device it is tasked to report. For instance, if the “Use Transfer PG” parameter is 01_b, the response shall include all data known relative to the Requested PG. When “Use Transfer PG” is 00_b, the effect of the Request2 PG is the same as if the Request PG (PGN 59904) was used. See Figure 43 for a description of the Request 2 PG. Table B1 has the SPN assignments to parameters in this message.

The Request2 and Transfer PGs are required in cases where a given ECU is tasked with reporting a PG and data for more than one controller application; otherwise, Request2 is optional. Examples include PGs such as Vehicle Identification, Component ID, and Software Identification.

If a device fails to get a response (either the Requested PG or NACK) to a Request within T_r, then the device may resend or retry the same Request. The number of retries for a specific Request should be limited to two retries, i.e., the Request is issued a total of three times. If the device fails to get a response (either the Requested PG or NACK) to the Request after the third retry, then the device should abandon further Request attempts for the same information or the device may wait for an extended period of time (minutes rather than seconds) before attempting to Request the same information.

A Proprietary Index may be used by some manufacturers in proprietary Parameter Groups to indicate the data format of the other bytes within the data field. In those cases, the Proprietary Index replaces the Extended Identifier Type.

Parameter Group Name:	**Request2 (RQST2)**
Definition:	Used to Request a PG from network device or devices and to specify whether the response should use the Transfer PG or not.
Transmission repetition rate:	Per user requirements, generally recommended that Requests occur no more than two or three times per second. When a device supports the Request2 PG and the device receives a destination specific Request2 PG where the "Requested PGN" is not supported by the device, then the device shall respond with a NACK (see PGN 59392).
Data length:	8 bytes (segmented transport supported)
Extended Data Page:	0
Data Page:	0
PDU Format:	201
PDU Specific:	Destination Address (global or specific)
Default priority:	6
Parameter Group Number:	51456 ($00C900_h$)
Bytes 1 to 3:	Requested PGN
Byte 4:	Special Instructions
4.6 to 4.8:	Reserved for SAE assignment
4.3 to 4.5:	Control Indicating Extended Identifier Type (Extended Identifier conveyed in data bytes 5 through 7)
4.1 to 4.2:	Use Transfer PG for response (00_b = No, 01_b=Yes, 10_b = undefined, 11_b = NA)
Byte 5:	Extended Identifier Byte 1 (least significant byte)
Byte 6:	Extended Identifier Byte 2
Byte 7:	Extended Identifier Byte 3 (most significant byte)
Byte 8:	Reserved for SAE assignment

Figure 43 - Request2 PG format

Data ranges for parameters used by this Message Type:

Control Indicating Extended Identifier Type: 000_b to 111_b. See definitions below.

000_b - No Extended Identifier. None of the data bytes are used for identifier/control values. Used when requesting a PG that does not have Proprietary Index/Extended Identifier bytes. Indicator that the device supports the new Request2 special instruction functionality. Data bytes 5 to 7 of the Request 2 PG are set to 255 (FF_h).

001_b - One Byte Extended Identifier. Data byte 5 of the Request2 PG contains the 1-byte identifier/control value that would match the Requested PG's data byte 1. Data bytes 6 to 7 of the Request2 PG are set to 255 (FF_h).

010_b - Two Byte Extended Identifier. Data byte 5 of the Request2 PG contains the byte identifier/control value that would match the Requested PG's data byte 1 and data byte 6 of the Request2 PG contains the identifier/control value that would match the Requested PG's data byte 2. Data bytes 7 of the Request2 PG is set to 255 (FF_h).

011_b - Three Byte Extended Identifier. Data byte 5 of the Request2 PG contains the byte identifier/control value that would match the Requested PG's data byte 1, data byte 6 of the Request2 PG contains the identifier/control value that would match the Requested PG's data byte 2, and data byte 7 of the Request2 PG contains the identifier/control value that would match the Requested PG's data byte 3.

100_b to 110_b - Reserved for future SAE definition.

111_b - Take no action. Not applicable.

Index Value	0 to 250	Definition is specific to the individual PG, when applicable.
	251 to 255	Follows conventions defined in SAE J1939-71.

6.10.3 Acknowledgment Service

Content in this section is identical to the Acknowledgment section in SAE J1939-21 but includes additional abort reasons (Table 11) using abort codes 10 and 11. An Acknowledgement PG is sent as a C-PG in a Multi-PG.

The definition of the Acknowledgment PG (ACKM) is contained in Figure 44. Table B1 has the SPN assignments to parameters in this message. The type of acknowledgment required for some PGs is defined in application layer documents.

For Proprietary PGs (see 6.10.4) the Proprietary Index parameter allows a receiver to identify the specific indexed PG that is being acknowledged. The Proprietary Index values are unique to each Proprietary PG.

Each form of the Acknowledgment PG includes an address acknowledge byte that contains the SA of the originator of the Request that the Acknowledgment PG is directed towards. Since the Acknowledgment PG is always directed to the global DA, these parameters allow the receiver to know the target being acknowledged. In 6.10.3.1 these parameters, in byte 5, are Address Acknowledged, Address Negative Acknowledgment, Address Access Denied, and Address Busy.

Parameter Group Name:	**Acknowledgment (ACKM)**
Definition:	The Acknowledgment PG is used to provide a handshake mechanism between transmitting and receiving devices. See Table 13 and Notes to Table 13 for further information about using the Acknowledgement PG.
Transmission repetition rate:	Upon reception of a PGN that requires this form of acknowledgment.
Data length:	8 bytes
Extended Data Page:	0
Data Page:	0
PDU Format:	232
PDU Specific:	Destination Address = Global (255)
Default priority:	6
Parameter Group Number:	59392 (00E800h)

Data ranges for parameters used by this Message Type:

Control byte: See detailed message definitions immediately following the parameter definitions:

0 - Positive Acknowledgment (ACK)
1 - Negative Acknowledgment (NACK)
2 - Access Denied
3 - Cannot Respond
4 - Data Size too large for required transport type
5 to 127 Reserved for assignment by SAE

SPECIAL ACKNOWLEDGEMENT CASES ONLY FOR WHEN THE REQUEST2 UTILIZES THE EXTENDED IDENTIFIER TYPE

128 - Positive Acknowledgment (ACK) for Request2 having an Extended Identifier Type of "One Byte Extended Identifier."
129 - Negative Acknowledgment (NACK) for Request2 having an Extended Identifier Type of "One Byte Extended Identifier."
130 - Access Denied for Request2 having an Extended Identifier Type of "One Byte Extended Identifier."
131 - Cannot Respond for Request2 having an Extended Identifier Type of "One Byte Extended Identifier."
132 to 143 - Reserved for assignment by SAE.

144 - Positive Acknowledgment (ACK) for Request2 having an Extended Identifier Type of "Two Byte Extended Identifier."
145 - Negative Acknowledgment (NACK) for Request2 having an Extended Identifier Type of "Two Byte Extended Identifier."
146 - Access Denied for Request2 having an Extended Identifier Type of "Two Byte Extended Identifier."
147 - Cannot Respond for Request2 having an Extended Identifier Type of "Two Byte Extended Identifier."
148 to 159 - Reserved for assignment by SAE.

160 - Positive Acknowledgment (ACK) for Request2 having an Extended Identifier Type of "Three Byte Extended Identifier."
161 - Negative Acknowledgment (NACK) for Request2 having an Extended Identifier Type of "Three Byte Extended Identifier."
162 - Access Denied for Request2 having an Extended Identifier Type of "Three Byte Extended Identifier."
163 - Cannot Respond for Request2 having an Extended Identifier Type of "Three Byte Extended Identifier."
164 to 254 Reserved for assignment by SAE.

255 Don't care/take no action.

Proprietary Index 0 to 250 Definition is specific to the individual PG, when applicable. Most often it is located as the first byte in the Data field of the applicable Proprietary PG.
251 to 255 Follows conventions defined in SAE J1939-71.

Figure 44 - Acknowledgment PG definition

6.10.3.1 Detailed Message Definitions

Positive Acknowledgment: Control byte = 0

Byte:		
	1	Control byte = 0, Positive Acknowledgment (ACK)
	2	Proprietary Index (If applicable)
	3 to 4	Reserved for assignment by SAE, these bytes should be filled with FF_h
	5	Address Acknowledged
	6	PGN of Requested information (LSB of Parameter Group Number, bit 8 most significant)
	7	PGN of Requested information (2nd byte of Parameter Group Number, bit 8 most significant)
	8	PGN of Requested information (MSB of Parameter Group Number, bit 8 most significant)

Negative Acknowledgment: Control byte = 1

Byte:		
	1	Control byte = 1, Negative Acknowledgment (NACK)
	2	Proprietary Index (if applicable)
	3 to 4	Reserved for assignment by SAE, these bytes should be filled with FF_h
	5	Address Negative Acknowledgement
	6 to 8	PGN of Requested information (see above)

Access Denied: Control byte = 2

Byte:		
	1	Control byte = 2, Access Denied (PGN supported but cybersecurity denied access)
	2	Proprietary Index (if applicable)
	3 to 4	Reserved for assignment by SAE, these bytes should be filled with FF_h
	5	Address Access Denied
	6 to 8	PGN of Requested information (see above)

Cannot Respond: Control byte = 3

Byte:		
	1	Control byte = 3, Cannot Respond (PGN supported but ECU is busy and cannot respond now. Re-Request the data at a later time.)
	2	Proprietary Index (if applicable)
	3 to 4	Reserved for assignment by SAE, these bytes should be filled with FF_h
	5	Address Busy
	6 to 8	PGN of Requested information (see above)

Data size too large: Control byte = 4

Byte:		
	1	Control byte = 4, Data size too large for Requested transport type (PGN supported but BAM transport type cannot be used because the data exceeds the size limits set for this transport type. Re-Request using Destination Specific Request instead.)
	2	Proprietary Index (if applicable)
	3 to 4	Reserved for assignment by SAE, these bytes should be filled with FF_h
	5	Address data size too large for Requested transport type
	6 to 8	PGN of Requested information (see above)

6.10.3.2 Special Request2 Acknowledgement Cases

Special acknowledgement cases for when the REQUEST2 utilizes the extended identifier type are listed here. The extended identifier type is denoted when the Control byte equals 128 to 163. In some proprietary use cases, the Extended Identifier Type is replaced with a Proprietary Value indicating a manufacturer specific purpose.

Positive Acknowledgment: Control byte = 128 and Extended Identifier Type "One Byte Extended Identifier":

Byte:		
	1	Control byte = 128, Positive Acknowledgment (ACK) Extended Identifier Type
	2	Proprietary Value = Extended Identifier Type (LSB) - byte 1
	3	Proprietary Value = Extended Identifier Type - filled with FF_h
	4	Proprietary Value = Extended Identifier Type (MSB) - filled with FF_h
	5	Address Acknowledged
	6	PGN of Requested information (LSB of Parameter Group Number, bit 8 most significant)
	7	PGN of Requested information (2nd byte of Parameter Group Number, bit 8 most significant)
	8	PGN of Requested information (MSB of Parameter Group Number, bit 8 most significant)

Negative Acknowledgment: Control byte = 129 and Extended Identifier Type "One Byte Extended Identifier":

Byte:	1	Control byte = 129, Negative Acknowledgment (NACK)
	2	Proprietary Value = Extended Identifier Type (least significant byte)
	3	Proprietary Value = Extended Identifier Type - filled with FF_h
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Negative Acknowledgement
	6 to 8	PGN of Requested information (see above)

Access Denied: Control byte = 130 and Extended Identifier Type "One Byte Extended Identifier":

Byte:	1	Control byte = 130, Access Denied (PGN supported but cybersecurity denied access)
	2	Proprietary Value = Extended Identifier Type (least significant byte)
	3	Proprietary Value = Extended Identifier Type - filled with FF_h
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Access Denied
	6 to 8	PGN of Requested information (see above)

Cannot Respond: Control byte = 131 and Extended Identifier Type "One Byte Extended Identifier":

Byte:	1	Control byte = 131, Cannot Respond (PGN supported but ECU is busy and cannot respond now. Re-Request the data at a later time.)
	2	Proprietary Value = Extended Identifier Type (least significant byte)
	3	Proprietary Value = Extended Identifier Type - filled with FF_h
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Busy
	6 to 8	PGN of Requested information (see above)

Positive Acknowledgment: Control byte = 144 and Extended Identifier Type "Two Byte Extended Identifier":

Byte:	1	Control byte = 144, Positive Acknowledgment (ACK) Extended Identifier Type
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Acknowledged
	6 to 8	PGN of Requested information (see above)

Negative Acknowledgment: Control byte = 145 and Extended Identifier Type "Two Byte Extended Identifier":

Byte:	1	Control byte = 145, Negative Acknowledgment (NACK)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Negative Acknowledgement
	6 to 8	PGN of Requested information (see above)

Access Denied: Control byte = 146 and Extended Identifier Type "Two Byte Extended Identifier":

Byte:	1	Control byte = 146, Access Denied (PGN supported but cybersecurity denied access)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Access Denied
	6 to 8	PGN of Requested information (see above)

Cannot Respond: Control byte = 147 and Extended Identifier Type "Two Byte Extended Identifier":

Byte:	1	Control byte = 147, Cannot Respond (PGN supported but ECU is busy and cannot respond now. Re-Request the data at a later time.)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - filled with FF_h
	5	Address Busy
	6 to 8	PGN of Requested information (see above)

Positive Acknowledgment: Control byte = 160 and Extended Identifier Type "Three Byte Extended Identifier":

Byte:	1	Control byte = 160, Positive Acknowledgment (ACK) Extended Identifier Type
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - byte 3
	5	Address Acknowledged
	6 to 8	PGN of Requested information (see above)

Negative Acknowledgment: Control byte = 161 and Extended Identifier Type “Three Byte Extended Identifier":

Byte:	1	Control byte = 161, Negative Acknowledgment (NACK)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - byte 3
	5	Address Negative Acknowledgement
	6 to 8	PGN of Requested information (see above)

Access Denied: Control byte = 162 and Extended Identifier Type “Three Byte Extended Identifier":

Byte:	1	Control byte = 162, Access Denied (PGN supported but cybersecurity denied access)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - byte 3
	5	Address Access Denied
	6 to 8	PGN of Requested information (see above)

Cannot Respond: Control byte = 163 and Extended Identifier Type “Three Byte Extended Identifier":

Byte:	1	Control byte = 163, Cannot Respond (PGN supported but ECU is busy and cannot respond now. Re-Request the data at a later time.)
	2	Proprietary Value = Extended Identifier Type (least significant byte) - byte 1
	3	Proprietary Value = Extended Identifier Type - byte 2
	4	Proprietary Value = Extended Identifier Type (most significant byte) - byte 3
	5	Address Busy
	6 to 8	PGN of Requested information (see above)

6.10.3.3 Example Acknowledgement Cases

Figure 45 shows a positive ACK response to a Request PG requesting DM3 (PGN 62228). For simplicity, the Multi-PGs are shown with only the C-PGs for the Request PG requesting DM3 and the ACK response (ACKM PG PGN 59392). In practice, other C-PGs may be included in the same Multi-PG. Assurance data is not included in this example. The C-PG with the Request PG is sent in a destination specific D_PDU1 Multi-PG addressed to Destination Address 1, and the C-PG with the ACK response is sent using a globally addressed D_PDU1 Multi-PG. Byte ordering is not considered in the data representations.

Tool Request to DA=01:

Multi-PG	29	CAN ID	3	PRIORITY	6 (110_b)
			18	PGN+DA	9473 (2501_h)
			8	SA	250 (FA_h)
	56	C-PG 1 HEADER	3	TOS	2 (010_b)
			3	TF	0 (000_b)
			18	CPGN	59904 ($EA00_h$)
			8	PL	3 (03_h)
		PAYLOAD	24	PG DATA	62228 ($00F314_h$)

ACK Response:

Multi-PG	29	CAN ID	3	PRIORITY	6 (110_b)
			18	PGN+DA	9727 ($25FF_h$)
			8	SA	1 (01_h)
	96	C-PG 1 HEADER	3	TOS	2 (010_b)
			3	TF	0 (000_b)
			18	CPGN	59392 ($E800_h$)
			8	PL	8 (08_h)
		PAYLOAD	64	PG DATA	0, 255, 255, 255, 250, 62228 (00_h, FF_h, FF_h, FF_h, FA_h, $00F314_h$)

Figure 45 - ACK example

Figure 46 shows a Negative ACK response due to a DM3 Request. The Request is identical to the ACK Example and not repeated. Only the NACK response is shown. In this case, the D_PDU3 Multi-PG is shown.

Multi-PG	11	CAN ID	3	APP PI	0 (000_b)
			8	SA	1 (01_h)
	96	C-PG 1 HEADER	3	TOS	2 (010_b)
			3	TF	0 (000_b)
			18	CPGN	59392 ($E800_h$)
			8	PL	8 (08_h)
		PAYLOAD	64	PG DATA	1, 255, 255, 255, 250, 62228 (01_h, FF_h, FF_h, FF_h, FA_h, $00F314_h$)

Figure 46 - NACK example

6.10.4 Proprietary Message Service

Content in this section is identical in purpose to the Group Function section in SAE J1939-21 but with larger data payload capability. A Proprietary PG is sent as a C-PG in a Multi-PG.

The Proprietary message service provides a means to transmit proprietary messages using a pre-defined set of PGNs. These PGNs are available to all manufacturers. Caution should be exercised when using the Proprietary PGNs because multiple SAs can use the same Proprietary PGN for different purposes. It is necessary to identify the sending ECU using its NAME in order to properly understand the PG content.

Some manufacturers multiplex (apply the group function type) the proprietary message content of some Proprietary PGs. If an application receives an SAE J1939 Request (PGN 59904) for a Proprietary PG and the application multiplexes that Proprietary PG using a proprietary index, the application may respond to the Request with an Acknowledgement PG instead of the Proprietary PG. The Acknowledgement PG identifies the Requested Proprietary PG with the appropriate acknowledgement control byte value. Once support is determined, the specific data will be retrieved using the Request2 (see 6.10.2) method.

Table B1 has the SPN assignments to parameters in these messages. The function itself is defined within the data structure (typically the first byte of the Data field). Each of the three proprietary PGs are defined in Figures 47, 48, and 49.

Parameter Group Name:	**Proprietary A (PROPA)**
Definition:	This proprietary PG uses the destination specific A_PDU1 Format allowing manufacturers to direct their proprietary communications to a specific destination node. How the data field of this message is used is up to each manufacturer. Use of proprietary messages is at the manufacturer's discretion with the constraint that significant percentages (2% or more) of vehicle network utilization should be avoided.
Transmission repetition rate:	Per user requirements
Data length:	0 to 16777215 bytes (segmented transport supported)
Extended Data Page:	0
Data Page:	0
PDU Format:	239
PDU Specific:	Destination Address. The global DA should not be used.
Default priority:	6
Parameter Group Number:	61184 ($00EF00_h$)
Bytes: 1 to 16777215	Manufacturer specific use (see 6.1.3)
Data range: Not specified by SAE	

Figure 47 - Proprietary A PG definition

Parameter Group Name:	**Proprietary A2 (PROPA2)**
Definition:	This proprietary PG uses the destination specific A_PDU1 Format allowing manufacturers to direct their proprietary communications to a specific destination node. How the data field of this message is used is up to each manufacturer. Use of proprietary messages is at the manufacturer's discretion with the constraint that significant percentages (2% or more) of vehicle network utilization must be avoided.
Transmission repetition rate:	Per user requirements
Data length:	0 to 16777215 bytes (segmented transport supported)
Extended Data Page:	0
Data Page:	1
PDU Format:	239
PDU Specific:	Destination Address. The global DA should not be used.
Default priority:	6
Parameter Group Number:	126720 ($01EF00_h$)
Bytes: 1 to 16777215	Manufacturer specific use
Data range: Not specified by SAE	

Figure 48 - Proprietary A2 PG definition

Parameter Group Name:	**Proprietary B (PROPB)**
Definition:	This proprietary PG uses the A_PDU2 Format message allowing manufacturers to define the PS (GE) field content as they desire. However, significant percentages (2% or more) of vehicle network utilization must be avoided. The PS (GE) and data fields of this message are manufacturer dependent. Therefore, if two transmission manufacturers use the same GE value, they could have different Data Length Codes. Receivers of this information would need to differentiate between the two manufacturers.
Transmission repetition rate:	Per user requirements
Data length:	0 to 15300 bytes for BAM (segmented transport supported)
Extended Date Page:	0
Data Page:	0 or 1
PDU Format:	255
PDU Specific:	Group Extension (manufacturer assigned); allowed range is 0 to 255
Default priority:	6
Parameter Group Number:	65280 to 65535 ($00FF00_h$ to $00FFFF_h$) 130816 to 131071 ($01FF00_h$ to $01FFFF_h$)
Bytes: 1 to 15300	Manufacturer defined usage

Data range:

Manufacturer defined usage allows the Data Length Code to be different per component supplier and SA. Caution should be used when using the Proprietary B PGNs because multiple SAs can use the same Proprietary B PGN for different purposes.

Figure 49 - Proprietary B PG definition

6.10.5 Transfer Service

Content in this section is identical to the Transfer section in SAE J1939-21. A Request PG (PGN 59904) is sent as a C-PG in a Multi-PG when the data size is appropriate. When the data size dictates the need for Transport Protocol, the FD.TP protocol shall be used.

The Transfer PG will be used in response to a Request2 receipt.

The Transfer PG provides a mechanism for reporting multiple data sets for a given PG in response to a Request2 (see 6.10.2). See Figure 50 for the definition of a “data set.” These multiple sets of data for a given PG require that each data set have a length and be labeled with four bytes from the SAE J1939-81 Name. The four bytes of the Name identify each device. The device responding to the Request shall report the same information it would with Request PG as the first data set in this response. If a device only has one data set, then it shall respond with the one data set utilizing the Transfer PG.

The Request2 and Transfer PGs are useful in cases where a given ECU is tasked with reporting a PG and data about more than one controller application. Examples include PGs such as Vehicle Identification, Component ID, and Software Identification.

See Figure 50 for the Transfer Service PG format. Table B1 has the SPN assignments to parameters in this message. The Transfer PG may be sent as a C-PG in a Multi-PG data frame or may be sent using FD.TP Transport Protocol if greater than 60 bytes of data.

Parameter Group Name:		**Transfer (XFER)**
Definition		Used for transfer of data in response to a Request2 when the “Use Transfer PG for response” is set to “Yes”
Transmission repetition rate:		In response to a Request2 PG with “Use Transfer PG” = 01_b
Data length:		Maximum of 16777215 bytes (segmented transport supported) Maximum of 15300 bytes if global Destination Address (BAM limit)
Extended Data Page:		0
Data Page:		0
PDU Format:		202
PDU Specific:		Destination Address (global or specific)
Default priority:		6
Parameter Group Number:		51712 ($00CA00_h$)
Bytes 1 to 3:		(a) PGN Requested by Request2 (see Table 2 for PGN ordering)
Byte 4:		(b) Length of data for the reported PG associated to the device identified (e.g., Controller Application Identity in bytes 5-8). Length value is the total of this byte, length of identity bytes (i.e., bytes 5-8), and the associated PG data. So the length is b + c + d.
Bytes 5 to 8:		(c) Identity of device associated to the PGN and data (i.e., Controller Application Identity) SAE J1939-81 defines the four bytes of the Name used here in bytes 5 through 8.
Byte 5:	5.4 to 5.8	Function Instance (most significant at bit 8)
	5.1 to 5.3	ECU Instance (most significant at bit 3)
Byte 6:		Function (most significant at bit 8)
Byte 7:	7.2 to 7.8	Vehicle System (most significant at bit 8)
	7.1	Reserved
Byte 8:	8.8	Arbitrary Address Capable
	8.5 to 8.7	Industry Group (most significant at bit 7)
	8.1 to 8.4	Vehicle System Instance (most significant at bit 4)
Bytes 9 to x:		(d) Data of reported PGN in bytes 1-3
Byte x+1 to n		Repeating information for 2nd and following shall contain: “Controller Application Identity,” Length, and “PGN Requested by Request2’s data.” See format definition below.

Format:

a,b,c,d,b,c,d,b,c,d...

a: PGN Requested by Request2 when “transfer mode” is set to yes
b: First Data Set: Length of concatenated ECU identity and associated PG data
The length = b + c + d
c: Identity of Controller Application to which field “d” is associated
d: Requested PG’s data for specific Controller Application
b: Second Data Set: Length of concatenated Controller Application Identity and associated PG data
c: Identity of Controller Application to which field “d” is associated
d: Requested PG’s data for second specific Controller Application
... etc.

Figure 50 - Transfer PG format

Example: For a given vehicle the engine ECU knows the VIN numbers for the tractor and the trailer. Another device sends the Request2 directed to the global destination, Requesting the VIN with “Use Transfer PGN” set to 01_b. The response from the engine might be:

- BAM transfer of the Transfer PG reporting the VIN for the tractor and VIN for the trailer

If the Request had the “Use Transfer PG” set to 00_b, the response would be:

- BAM transfer of the VIN for the tractor but not utilizing the Transfer PG

6.11 CAN Frame Error Detection

CAN frame error detection is fully specified in ISO 11898-1. Content in this section is a brief summary of the error detection implemented at the CAN controller hardware layer. This is separate from Assurance Content. Assurance content is needed for functional safety and cybersecurity which is not provided by the hardware layer detection.

The following measures are taken for detecting errors:

a. 17-bit Cyclic Redundancy Check (CRC) for data frames up to 16 bytes

b. 21-bit Cyclic Redundancy Check (CRC) for data frames larger than 16 bytes

c. Variable Bit Stuffing with a stuff width of 5 and stuff bit counter

d. Frame format check

6.12 Assurance Content

There are two supported content assurance methods for A_PDU content. The two methods are functional safety and cybersecurity. The assurance content within the data field is both optional and available in multiple sizes to support different assurance requirements. Each C-PG within a Multi-PG may individually include assurance content. Large transport using FD Transport Protocol, both BAM and RTS/CTS transfers, supports end-to-end assurance of the complete transfer.

6.13 CAN Receive Buffer Management

Devices must have appropriate CAN receive buffer management to prevent losing messages when the data link is at 100% utilization. This also means that in low utilization situations, when there are back-to-back CAN data frames, each device must be able to manage the messages fast enough not to lose messages due to their back-to-back nature. Processing the CAN data frames fast enough does not mean that a response has to be immediately generated but that a new CAN data frame must not overrun previous CAN data frames.

For SAE J1939-22, almost all FEFF data frames will be for three PGs: Multi-PG, FD.TP.CM, and FD.TP.DT. See Appendix C for a complete listing.

6.14 Timeout Defaults

These default values are referenced in multiple sections within this document.

T_r = 200 ms (Maximum Response Time)

T_h = 500 ms (Maximum time, for responder, between transmits of consecutive CTS messages during hold)

T1 = 750 ms (Transport Segment Interval)

T2 = 1250 ms (Maximum time, for responder, to receive a DT segment after a CTS - Originator Failure)

T3 = 1250 ms (Maximum time, for originator, to receive a CTS after last DT segment - Responder Failure)

T4 = 1050 ms (Maximum time, for originator, to receive the next CTS messages since the previous “hold” CTS to hold a connection open)

T5 = 3000 ms (Maximum time, for originator, to receive EOMA after sending EOMS)

All devices, when required to provide a response, must do so within T_r. All devices expecting a response must wait for at least the T3 interval before giving up or retrying. These times assure that any latencies due to bus access or message forwarding across bridges do not cause unwanted timeouts. Different time values can be used for specific applications when required. For instance, for high-speed control messages, a 20 ms response may be expected. There is no restriction on minimum response time. See 6.5.4 for concepts related to packing Multi-PG messages.

Below is an example using the 1250 ms (T3) timing. The time-out was established for network architecture with no more than ten bridges between any two controllers (including an off-board tool).

a. Maximum forward delay time within a bridge is 50 ms (per SAE J1939-31).

   Total number of bridges = 10 (i.e., 1 off-board tool adapter, 1 tractor, 5 trailers, 4 dollies).
   Total network delay is 500 ms in one direction.

b. Number of Request retries = 2 (3 Requests total); this includes the situation where the CTS is used to Request the retransmission of data segment(s). If the retransmit Request limit is reached, then the connection abort shall be sent with abort reason 5 from Table 11.

c. 50 ms margin for timeouts.

Figures A1, A4, A5, and A6 have the timing requirements identified. In Figure A1, the time numbers are computed assuming the worst-case number of bridges, ten bridges. The timeout numbers for receivers are identified as a time value while transmitter requirements are specified as a less than or equal to time value. Note that an originator has transmitter and receiver requirements and that a responder has transmitter and receiver requirements.

7. NOTES

7.1 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 SAE TRUCK AND BUS CONTROL AND COMMUNICATIONS NETWORK COMMITTEE OF THE SAE TRUCK AND BUS ELECTRICAL/ELECTRONICS STEERING COMMITTEE

APPENDIX A - FD TRANSPORT PROTOCOL TRANSFER SEQUENCES

A.1 RTS/CTS DATA TRANSFER

Under normal circumstances, the flow model for the RTS/CTS data transfer resembles the exchange illustrated in Figure A1.

In the Figure A1 example, the originator sends the FD.TP.CM_RTS indicating there are 207 bytes in the segmented message, which will be transferred in four segments. The originator indicates it is capable of sending 255 messages for a CTS. The PGN for the data in the example transfer is 65259, Component Identification. For simplicity, this example does not include assurance data coverage. Session number 1 is used in the example.

The responder replies with a CTS indicating that it is ready to receive two segments, beginning with segment 1.

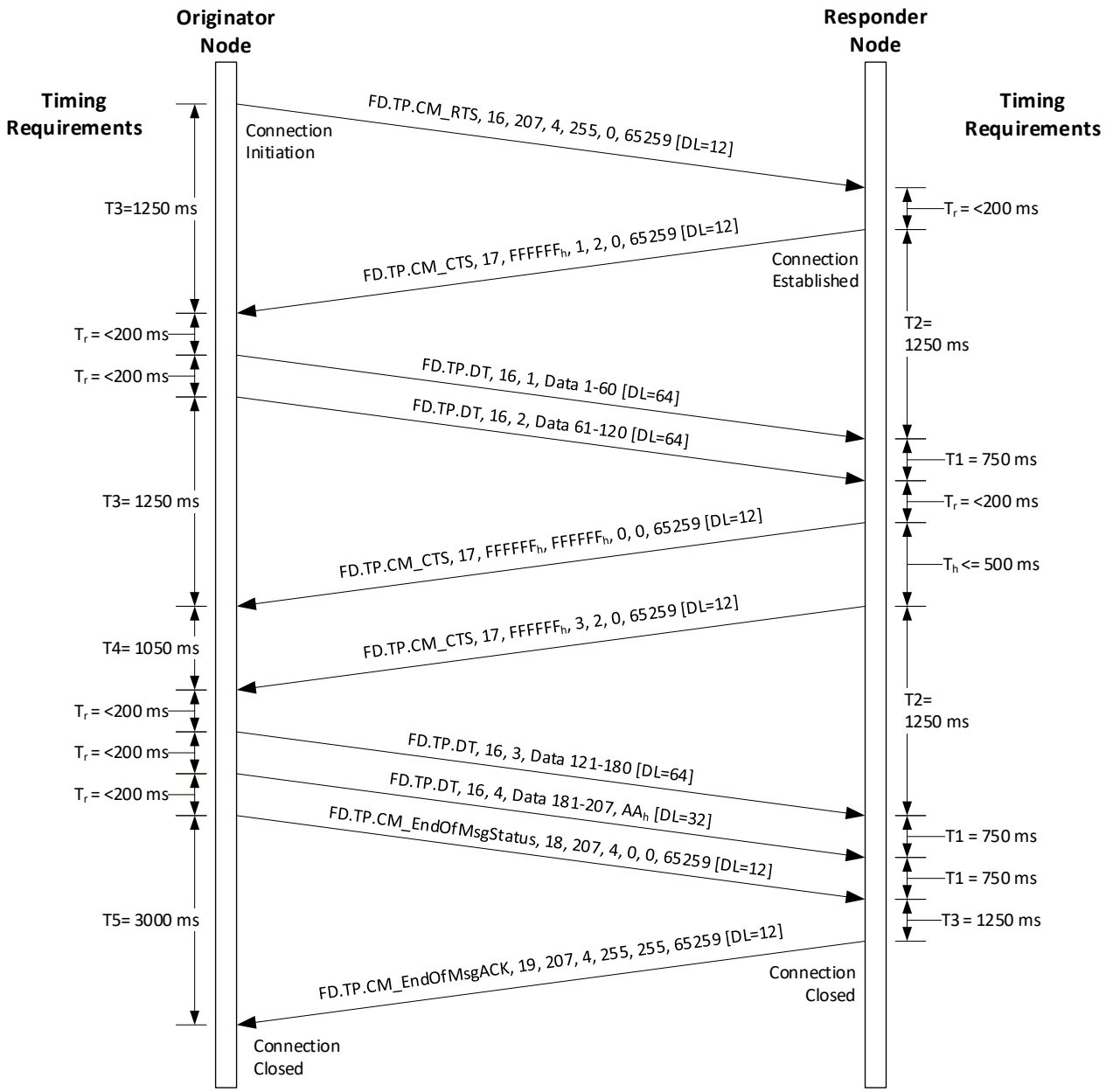
In response to the CTS, the originator transmits two FD.TP.DT messages with the segments 1 and 2, in sequential order.

Upon receiving the two FD.TP.DT messages from the previous CTS, the responder issues a CTS indicating that it wants to hold the connection open but cannot receive any segments right now. The responder reports the “number of segments to send” as 0 for this CTS. The responder must send another CTS message within T_h time, either a CTS to continue holding the connection or a CTS to Request additional segments. In this example the responder sends the next CTS indicating that it is ready to receive two more segments, beginning with segment 3.

In response to the last CTS, the originator transmits two FD.TP.DT messages with segments 3 and 4, in sequential order. Segment 4 only contains 27 bytes of PG data, so a single padding byte of AA_h is appended after the segment data. Adding the FD.TP.DT data field, the session field, DTFI (Data Transfer Format Indicator field), the segment number field, and a padding byte yields a 32 byte length. The padding byte is done as specified in 6.3.3.2. The FD.TP.DT messages for segments 1 through 3 used a 64-byte data frame; only the FD.TP.DT message for segment 4 happened to be a 32 byte data frame.

After the FD.TP.DT message for segments 3 and 4 have been transferred, the originator transmits a FD.TP.CM_EndOfMsgStatus indicating that all the segments were transmitted.

In response to the FD.TP.CM_EndOfMsgStatus message, the responder transmits a FD.TP.CM_EndOfMsgACK message indicating that all the segments expected were received and that the connection is now considered closed. When the responder assembles the data segments from the FD.TP.DT messages, the responder has received 208 bytes (207 bytes of PG data and the 1 byte of AA_h padding). Using the Total Bytes of 207 specified in the RTS message, the responder knows to use the first 207 bytes as the PG data and discards the remaining bytes.



NOTE: Timeouts (T_r, T1, T2, T3, T4) are described in 6.14.

Figure A1 - RTS/CTS data transfer without errors

Figure A2 illustrates an RTS/CTS example with a Request to resend a missed data segment. In this example, the responder has an issue/error with the FD.TP.DT for segment 2 and Requests to have it resent before continuing. The responder's issue with FD.TP.DT for segment 2 is irrelevant—it could have been lost or corrupted. This example uses the same PGN and session as the Figure A1 example.

The responder transmits a CTS message Requesting a resend of a single segment beginning with segment 2; this tells the originator to resend the previous segments starting with segment 2. In response to the CTS, the originator complies by transmitting a single FD.TP.DT message with segment 2 data. Upon successfully receiving the segment 2 FD.TP.DT message, the responder sends a CTS indicating the responder is ready to receive two more segments, beginning with segment 3. Once segments 3 and 4 have been transferred, the originator transmits a FD.TP.CM_EndOfMsgStatus indicating that all the segments were transmitted. Once the FD.TP.CM_EndOfMsgStatus is received correctly, the responder passes a FD.TP.CM_EndOfMsgACK signaling that the entire message has been correctly received.

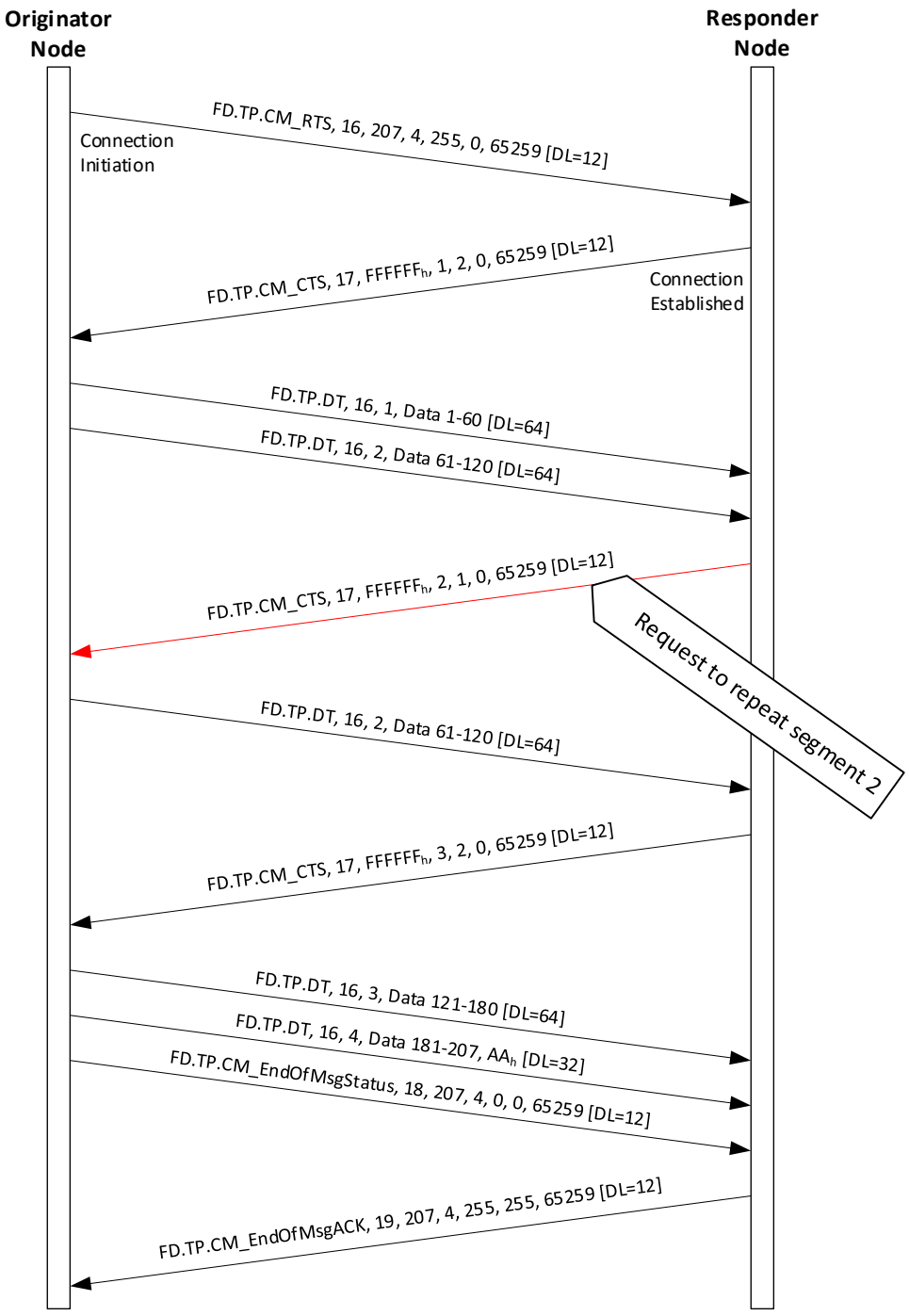


Figure A2 - RTS/CTS data transfer with error

Figure A3 illustrates an example where the Maximum Number of Segments value in the RTS message is used to limit the number of segments the responder can Request in its CTS messages. The originator sends an RTS indicating a Request to send 207 bytes of data for PGN 65259 using 4 segments with a maximum of 3 segments at a time. The responder sends a CTS Requesting 3 segments beginning with segment 1. After receiving the first 3 data segments, the responder sends a CTS Requesting 1 segment beginning with segment 4 since there is only 1 segment remaining. Session number 2 was used in this example.

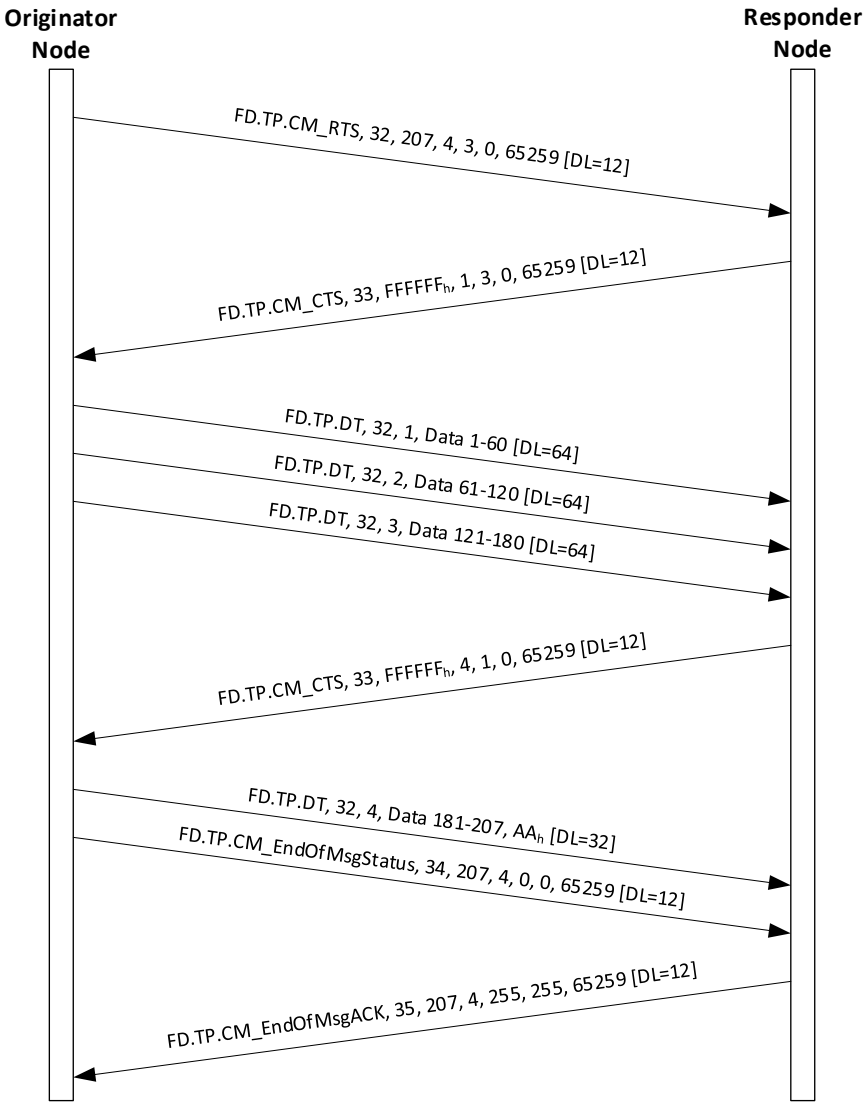


Figure A3 - RTS/CTS data transfer utilizing RTS maximum number of segments capability

Figure A4 illustrates an RTS/CTS transfer where the responder attempts to recover from two issues to avoid aborting the session. In the first issue, the FD.TP.DT message for segment 2 for the first CTS is not received. For this issue, the responder sends a CTS Requesting the resend of the missed data segment. In the second issue, the responder fails to receive the FD.TP.CM_EndOfMsgStatus, with manufacturer specific Functional Safety, after receiving the FD.TP.DT message for the final segment (segment 4). For this issue, the responder sends a CTS with the “Request” code set to 1 to Request the originator to resend FD.TP.CM_EndOfMsgStatus rather than aborting the connection. Session 2 is used in this example.

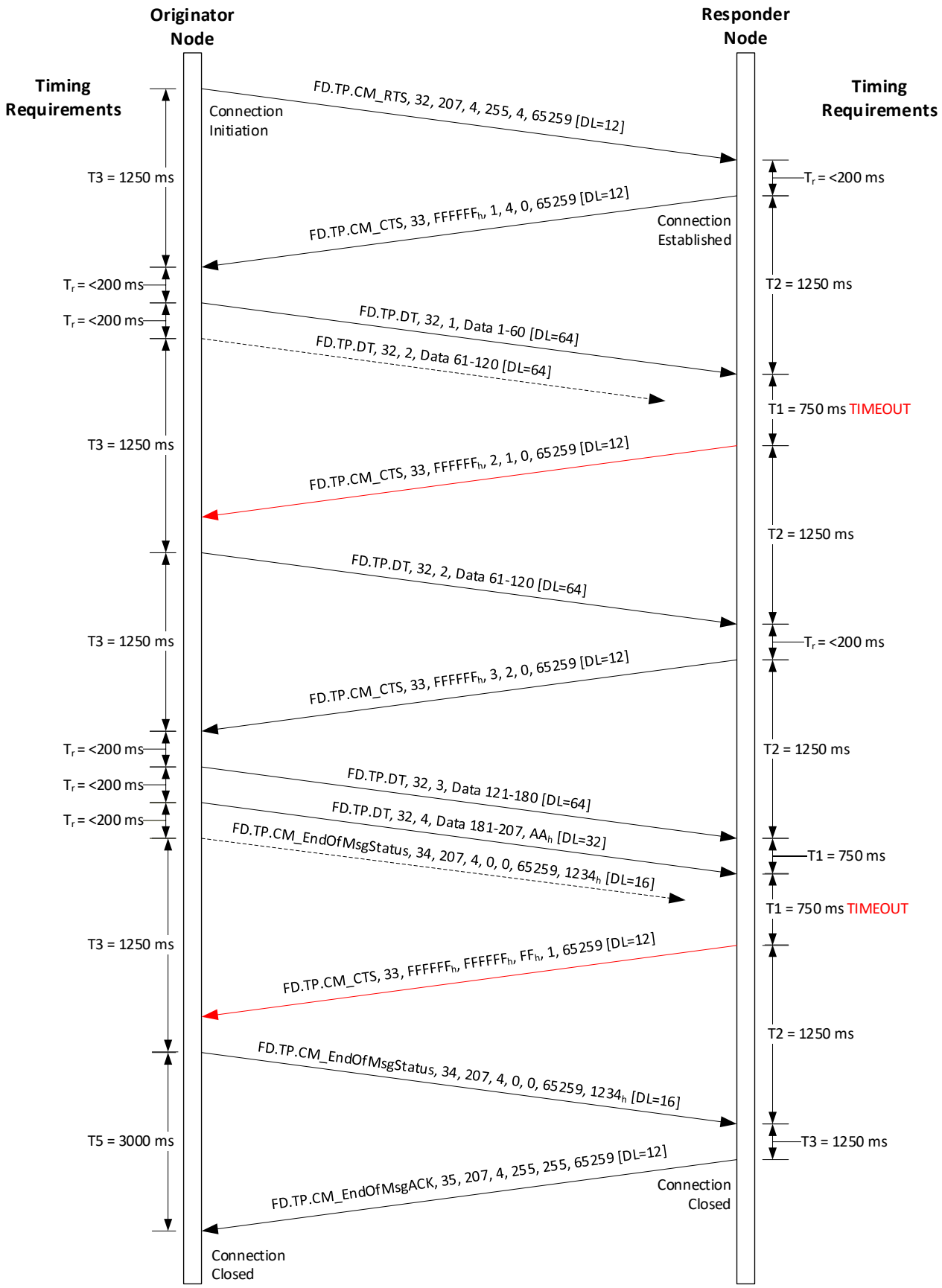


Figure A4 - Responder sending CTS after a time out to prevent session abort

Figure A5 illustrates two separate RTS/CTS transfers where the responder retransmits a CTS message when missed FD.TP.DT messages cause a T1 timeout. Session 0 is used in these examples.

In the left sequence diagram, the originator is using a longer time interval between consecutive FD.TP.DT messages. When the responder has a T1 timeout due to missed FD.TP.DT messages after segment 2, it retransmits a new CTS Requesting the resend of the last ten segments starting with segment 3. Due to the longer time between FD.TP.DT messages, the originator is still transmitting FD.TP.DT messages for the most recent CTS when it receives the new CTS message. The originator aborts the session with abort reason 4. This is a possible example where the retransmit CTS does not avoid the session abort.

In the right sequence diagram, the originator is using a shorter time interval between consecutive FD.TP.DT messages. When the responder has a T1 timeout due to missed FD.TP.DT messages after segment 2, it retransmits a new CTS Requesting the resend of the last 10 segments starting with segment 3. Due to the shorter time between FD.TP.DT messages, the originator has transmitted the last FD.TP.DT message for the most recent CTS with it receives the new CTS message. In this situation, the originator is able to receive the CTS and avoid aborting the session.

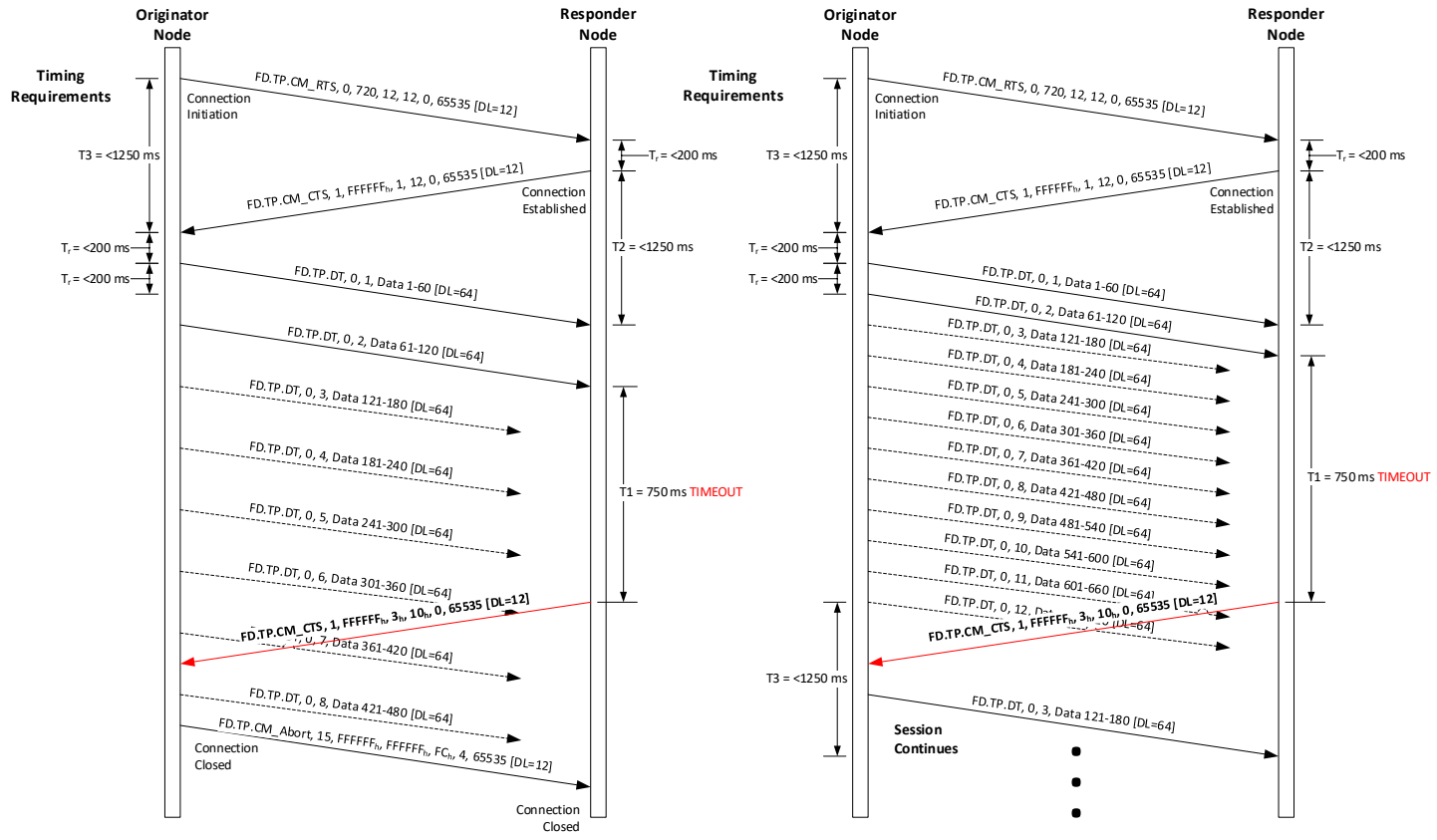


Figure A5 - RTS/CTS transfer with originator reaction to a retransmit CTS

A.2 BAM DATA TRANSFER

The typical flow model for a BAM data transfer resembles the exchange illustrated in Figure A6.

In the Figure A6 example, the originator sends the FD.TP.CM_BAM message to the global Destination Address to alert all nodes on the network that it is about to broadcast the transfer of a large message using Transport Protocol. The BAM message indicates the transfer will be for 142 bytes of data for PGN 65260 (Vehicle Identification) which will be transferred using 3 data segments and that manufacturer specific cybersecurity assurance data will be provided. Session 0 is used for this BAM transfer.

After sending the FD.TP.CM_BAM message, the originator begins sending each of the 3 data segments in the FD.TP.DT messages to the global Destination Address. Data segment 3 only contains 22 bytes of PG data, so 10 padding bytes of AA_h are appended after the segment data so the FD.TP.DT data field, including the session, DTFI, and segment number fields, is 32 bytes in length. The padding byte is done as specified in 6.3.3.2.

After sending the Data Transfer (FD.TP.DT) message for the final data segment, the originator transmits the FD.TP.CM_EndOfMsgStatus (EOMS) completion message, including 8 bytes of cybersecurity assurance data, to the global Destination Address. This message alerts all nodes that the originator has transmitted all of the data segments.

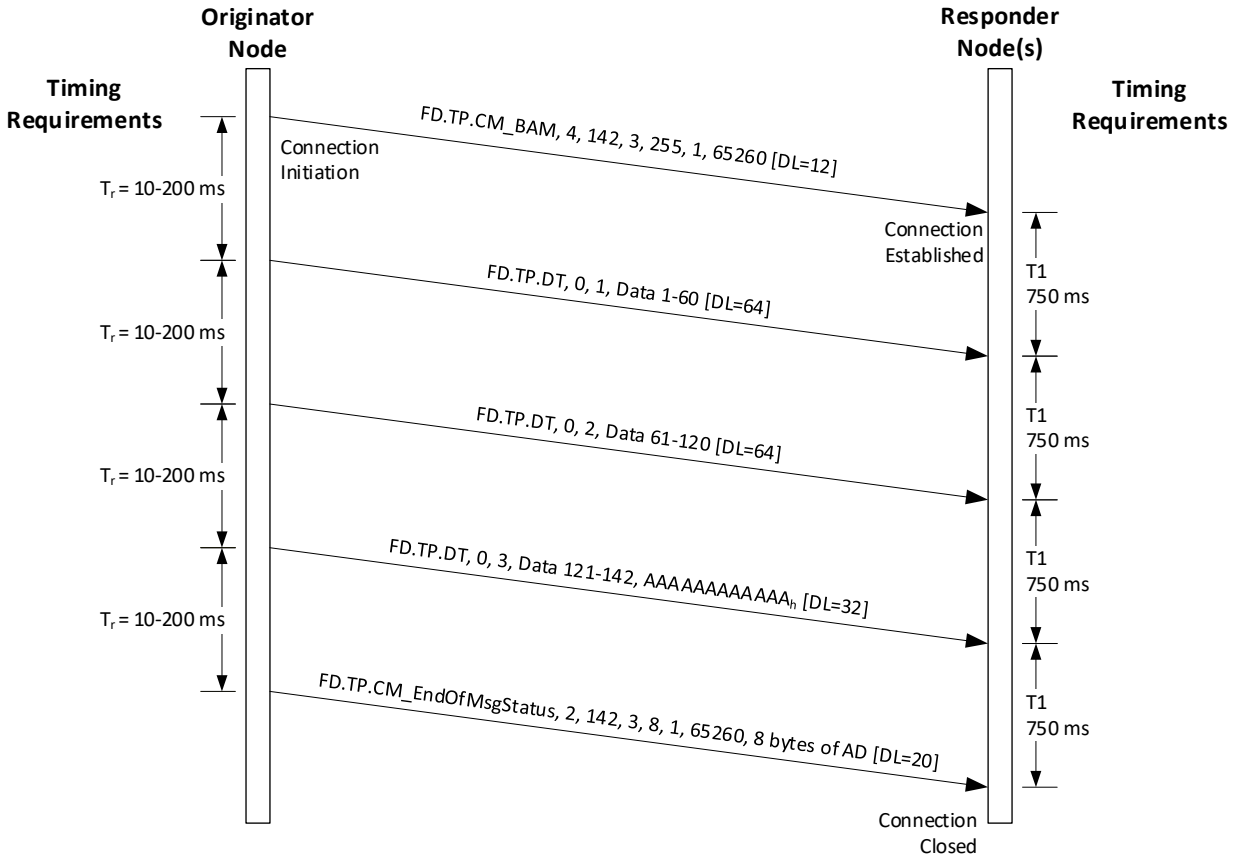


Figure A6 - BAM data transfer with cybersecurity

APPENDIX B - ASSIGNMENTS OF SPNS FOR SAE J1939-22

B.1 SPN ASSIGNMENTS FOR SAE J1939-22

Table B1 shows the SPN assignments for SAE J1939-22 items.

Table B1 - SAE J1939-22 SPN assignments

PG or Other Reference	PGN	SP Name	SPN
Request	59904	Parameter Group Number (RQST)	2540
Acknowledgement	59392	Control Byte (ACKM)	2541
		Proprietary Value (ACK) Or Proprietary Value = Extended Identifier Type (least significant byte) - byte 1	2542 7334
		Proprietary Value = Extended Identifier Type - filled with FF_{16}	7335
		Extended Identifier Type (most significant byte) - filled with FF_{16}	7336
		Address Acknowledged (ADD_ACK)	3290
		Parameter Group Number (ACK)	2543
		Proprietary Value (NACK)	2544
		Address Negative Acknowledgement (ADD_NACK)	3291
		Parameter Group Number (NACK)	2545
		Proprietary Value (NACK_AD)	2546
		Address Access Denied (ADD_AD)	3292
		Parameter Group Number (NACK_AD)	2547
		Proprietary Value (NACK_Busy)	2548
		Address Busy (ADD_BUSY)	3293
		Parameter Group Number (NACK_Busy)	2549
Proprietary A	61184	Manufacturer Specific Information (PropA_PDU1)	2550
Proprietary A2	126720	Manufacturer Specific Information (PropA2_PDU2)	3328
Proprietary B	65280 to 65535	Manufacturer Defined Usage (PropB_PDU2)	2551
Request2	51456	Parameter Group Number (RQST2)	2574
		Control Indicating Extended Identifier Type	7337
		Use Transfer Mode	2575
		Extended Identifier Byte 1 (least significant byte)	7338
		Extended Identifier Byte 2	7339
		Extended Identifier Byte 3 (Most significant byte)	7340
Transfer	51712	Parameter Group Number of Requested Information (XFER)	2552
		Length of data for the reported PGN (XFER)	2553
		“Controller Application Identity” of the ECU for specific data subsets	2554
		Transfer Data	2555
FD Transport Protocol-Connection Management	19712	Control Type	13182
		Session Number	13183
		Total Message size	13184
		Total Number of Segments	13185
		Next Segment Number to be sent	13186
		Maximum Number of Segments	13187
		Number of Segments to be sent	13188
		AD Type	13189
		AD Size	13190
		Request Code	13191
		Connection Abort Reason	13192
		Connection Abort Role	11745
		Parameter Group Number of segmented message	13193
		Assurance Data	13194

PG or Other Reference	PGN	SP Name	SPN
FD Transport Protocol-Data Transfer	19968	Session Number	13195
		DT Format Indicator	13196
		Segment Number	13197
		Segmented Data	13198
Multi-PG FEFF Type	9472	Type of Service	13199
		Trailer Format	13200
		Contained Parameter Group Number (CPGN)	13201
		C-PG Payload Length	13202
		Parameter Group Data	13203
		C-PG Assurance Data	13204
Multi-PG FBFF Type	N/A	Type of Service	13205
		Trailer Format	13206
		Contained Parameter Group Number (CPGN)	13207
		C-PG Payload Length	13208
		Parameter Group Data	13209
		C-PG Assurance Data	13210

APPENDIX C - POSSIBLE CAN IDS

C.1 CAN IDENTIFIERS WHICH MAY APPEAR ON THE NETWORK

Table C1 shows the CAN identifiers for SAE J1939-22 messages which may appear on the network using the FEFF format. Table C2 shows the CAN identifiers for SAE J1939-22 messages which may appear on the network using the FBFF format. Non-SAE J1939 messages are not shown in the tables.

Where “X” is shown within the CAN ID, it denotes that any value is possible in this position.

Table C1 - SAE J1939-22 FEFF CAN IDs

Priority	PGN	SA	CAN ID	Message Name
7 (111b)	19712 (004D00h)	0 - 253	1C4DXXXXh	FD.TP Connection Management
7 (111b)	19968 (004E00h)	0 - 253	1C4EXXXXh	FD.TP Data Transfer
0 - 7	9472 (002500h)	0 - 253	XX25XXXXh	Multi-PG (D_PDU1 Type)
6 (110b)	60928 (00EE00h)	0 - 255	18EEXXXXh	Address Claimed

Also possible on the network is the FBFF form of the Multi-PG message. This form uses much of the addressable range. The remainder of the addressable range is used by messages defined outside of SAE J1939-22.

Table C2 - SAE J1939-22 FBFF CAN IDs

AppPI	SA	CAN ID	Message Name
0 (000b)	0 - 253	0XXh	Multi-PG (D_PDU3 Type)
2 (010b)	0 - 253	2XXh	Proprietary message