Functional safety solutions: SAE J1939-76 (CAN) and SAE J1939-77 (CAN FD)

Travis Breitkreutz (Caterpillar)

This paper discusses the two SAE J1939 standards for functionally safe communications on Classic CAN (SAE J1939-76) and CAN FD (SAE J1939-77). For SAE J1939-76, it describes the Safety Header Message (SHM) and Safety Data Message (SDM) pairing approach used to communicate safety-related data from a producing safety application to a consuming safety application. In addition, it details the features of the version as published in 2020 and lists the deficiencies of this version. Finally, it details features of the revision currently under development that make up for these deficiencies. For SAE J1939-77, it describes the use of space allocated for functional safety assurance information in the Multi-PG and FD Transport protocols to communicate safety-related data from a producing safety application to a consuming safety application. In addition, it describes the three profiles currently under development that are tailored to meet different system needs while still meeting functional safety requirements.

Introduction

IEC 61784-3 [1] describes various communication errors that can occur as well as safety measures that can be used to detect such errors to achieve the desired level of functional safety. SAE J1939-76 [5] and SAE J1939-77 [6] specify approaches for functional safety based on this information.

Communication Errors

Corruption

Corruption refers to the unexpected and undesired transformation of a message such that the message received does not exactly match the message transmitted. This error can occur, for example, when a device driver inadvertently swaps the byte order of a part of the message, or when noise emissions disrupt the bit patterns in communicated signals.

Unintended Repetition

Unintended repetition refers to the unexpected and undesired repetition of a message. This error can occur, for example, when a device driver fails to update its transmission queue after transmitting a message and so transmits the same message again.

Incorrect Sequence

Incorrect sequence refers to the out-of-order communication of messages in a sequence, e.g., the second message in a sequence gets received before the first message in the sequence. This error can occur, for example, when messages in the sequence get assigned different priorities before the messages are placed in a priority queue for transmission.

Loss

Loss refers to the failure to receive a message that was to be transmitted. This error can occur, for example, when a message is submitted for transmission to a queue that is already full, with the result being that the message is dropped and never actually transmitted. Another example, conversely, is when a message is received but cannot be added to a reception queue, with the result being that the message is dropped.

Unacceptable Delay

Unacceptable delay refers to the failure to receive a message within a permitted time window, thereby causing a delay in the system's response. This error can occur, for example, if several messages are communicated at or near the same time,

causing congestion on the communication medium.

Insertion

Insertion refers to the reception of a message from an unexpected or unknown source. This error can occur, for example, when two or more sources are transmitting the same messages.

Masquerade

Masquerade refers to the inadvertent handling of a message from a non-safety-related source as if it were from a safety-related source. This error can occur, for example, when a safety-related source, in addition to transmitting its own messages, is forwarding messages from a non-safety-related source. In this example, a recipient inadvertently treats those messages as if they were really from the safety-related source.

Addressing

Addressing refers to the delivery of a message to the wrong recipient, who nevertheless treats the reception as correct. This error can occur, for example, when a message is inadvertently addressed to a multicast/ broadcast address instead of to a unicast address.

Safety Measures

Sequence Number

A sequence number occupies space in a message and identifies the position of the message relative to other messages in the same stream. It changes from one message to the next in a manner such that both source and recipient can determine what the sequence number for the next message should be.

Time Expectation

A time expectation is when a recipient monitors the time between two consecutively communicated messages to determine whether the period exceeds a threshold; if it does, then the recipient assumes an error.

Connection Authentication

Connection authentication is where a message has a unique source and/or destination identifier for the safety-related participants.

Data Integrity Assurance

Data integrity assurance adds redundant data (e.g., a cyclic redundancy check or CRC) to a message to detect corruption in the message.

Redundancy with Cross-Checking

Redundancy with cross-checking communicates the safety data in separate instances, either in separate messages or in the same message. A safety-related recipient can then compare the data in both instances and flag an error if differences exist.

Different Data Integrity Assurance Systems
A different data integrity assurance system is a design in which communicated safety-related data use integrity mechanisms that are different from those used by communicated non-safety-related data. This ensures that non-safety-related messages do not affect a safety-related recipient.

Coverage

Table 1 describes the coverage of various communication errors by the safety measures employed in [5] and [6].

Communication Errors	Safety Measures					
	Sequence Number	Time Expectation	Connection Authentication	Data Integrity Assurance	Redundancy with Cross-Checking*	Different Data Integrity Assurance Systems
Corruption				•	•	
Unintended Repetition	•				•	
Incorrect Sequence	•				•	
Loss	•				•	
Unacceptable Delay		•				
Insertion	•		•		•	
Masquerade			•			•
Addressing			•			

*Both SHM1 and SHM2 versions in [5] employ redundancy with cross-checking for some, but not all, communicated data. Profiles in [6] do not employ redundancy with cross-checking.

SAE J1939-76

Overview

There are two versions of functional safety support specified in [5]; this support applies to Parameter Groups (PGs) whose parameter data payloads range from 0 to 8 bytes in length. Both versions use a Safety Data Group (SDG), which consists of a Safety Header Message (SHM1 or SHM2) and a Safety Data Message (SDM), to communicate safety-related data from a producer to a consumer. The SDM—which is simply any PG to which an SHM is associated—contains the safety-related parameter data to be used as part of a safety function. In contrast, the SHM contains the following additional functional safety assurance data:

- A 32-bit CRC.
- A Sequence Number.
- The Parameter Group Number (PGN), Destination Address (DA) for point-to-point PGs, and Source Address (SA) of the associated SDM.

Because of the need for two different messages, [5] specifies timing and order-of-transmission constraints to ensure that the right SHM instance appears with the right SDM instance.

The 2020 publication of [5] specified what's now called the SHM1 version of functional safety support. Later analysis showed that the SHM1 version had some deficiencies with regards to the CRC coverage and the size of the Sequence Number field, so SAE began development on the SHM2 version to correct those deficiencies.

SHM1 Version

Assurance Data

Figure 1 illustrates the format of the payload of SHM1. The EDP (Extended Data Page), DP (Data Page), PF (PDU Format), PS (PDU Specific), and SA fields are all bit-wise inverted; the values of these fields before inversion match the values in the SDM.

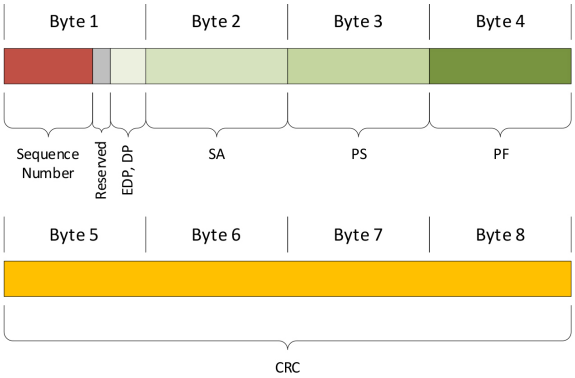

Figure 1: Format of SHM1 Payload

Benefits

- This version employs a CRC polynomial (labeled as CRC-32K/10 in [2]) with a relatively large Hamming distance for the expected payload size.
- A system can deploy this version over either J1919-21 communications as specified in [3] (based on Classic CAN) or J1939-22 communications as specified in [4] (based on CAN FD).
- This version has been available for several years.

Drawbacks

- This version's CRC calculation only covers the PG's parameter data payload in the SDM; it does not cover the PGN, DA for point-to-point PGs, SA, or Sequence Number fields provided in the SHM.
- The Sequence Number in this version is relatively small at 5 bits.
- This version doubles the bandwidth needed to communicate safety data.
- This version has some relatively complicated timing constraints due to the need for two messages per SDG.
- This version is not well suited for communications across routers due to a dependence on link-local addresses as part of its connection authentication.

SHM2 Version

Assurance Data

Figure 2 illustrates the format of the payload of SHM2. Unlike in SHM1, the EDP, DP, PF, and PS fields are not bitwise inverted; the values of these fields match the values in the SDM. The SA field is not in the payload, but

it appears in the CAN ID and matches the value in the SDM. The six least significant bits of the Sequence Number field are in the first byte of the payload, while the eight most significant bits of the field are in the second byte.

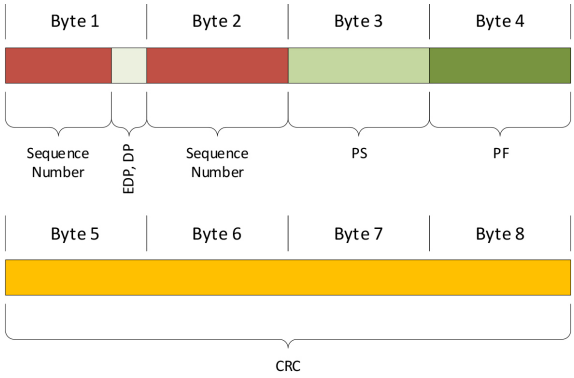

Figure 2: Format of SHM2 Payload

Benefits

- Like the SHM1 version, the CRC calculation in this version covers the PG's parameter data payload in the SDM; however, it also covers the PGN, DA for point-to-point PGs, SA, and Sequence Number fields in the SHM.
- The Sequence Number in this version is larger—14 bits—than that defined in the SHM1 version.
- Like the SHM1 version, a system can deploy this version over either J1939-21 communications or J1939-22 communications.

Drawbacks

- This version employs a different CRC polynomial (labeled as CRC-32K/9 in [2]) whose Hamming distance is slightly smaller than that used in the SHM1 version. (A different polynomial was necessary to cover the larger amount of data.)
- Like the SHM1 version, this version doubles the bandwidth needed.
- Like the SHM1 version, this version has some relatively complicated timing requirements.
- Like the SHM1 version, this version is not well suited for communications across routers.
- This version is still under development.

SAE J1939-77

Overview

There are three profiles specified in [6] for functional safety support; these profiles take advantage of the Multi-PG and FD Transport protocols specified in [4] for use over CAN FD. These protocols can allocate a separate space in their messaging for cybersecurity and/or functional safety assurance information for a PG's parameter data. As a group, these profiles support PGs whose parameter data payloads range from 0 to 65,526 bytes in length.
Each of the profiles specified in [6] provides the following functional safety assurance information:

- Either a 32-bit or a 64-bit CRC.
- A 32-bit Sequence Number.
- The Length of the data over which the CRC was calculated.

In addition, two of the profiles provide a system-specific connection authentication (DataID) that does not depend on link-local addressing. The definition of this authentication allows producers to communicate safety-related messages to consumers through routers.

Profile #1

Overview

This profile focuses on minimizing the amount of functional safety assurance information required. To accomplish this, the profile requires a fixed size for the PG's parameter data payload; it also requires incorporating link-local address information in the data's identification, which limits its usefulness for communication through routers. The resulting functional safety assurance data fits within 8 bytes.
Assurance Data

Figure 3 illustrates the format of the assurance data for Profile #1. The PGN, DA for point-to-point PGs, and SA fields all appear elsewhere in the Multi-PG messaging and so do not appear here.

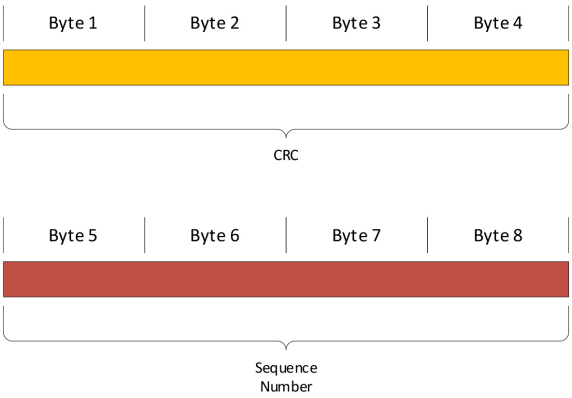

Figure 3: Format of Profile #1 Assurance Data

Benefits

- This profile has the smallest set of functional safety assurance data of any profile.
- This profile consumes less space inside the trailer of a single C-PG (Contained Parameter Group, a part of the Multi-PG protocol messaging) than the equivalent pair of C-PGs containing an SDG.
- The Sequence Number in this profile is much larger than that used in either the SHM1 or SHM2 versions.
- This profile uses the same CRC polynomial as that used in the SHM2 version.
- The CRC calculation in this profile covers the PG's parameter data payload as well as the PGN, DA for point-to-point PGs, SA, and Sequence Number fields.

Drawbacks

- This profile requires that the PG's parameter data payload be exactly 8 bytes.
- Like the SHM1 and SHM2 versions, this profile is not well suited for communications across routers.
- Like all profiles in [6], this profile is limited to J1939-22 communications.
- Like all profiles in [6], this profile is still under development.

Profile #2

Overview

This profile focuses on the following:

- Handling a PG's parameter data payload that is of variable length and that can be larger than 8 bytes.
- Supporting communication across routers by not relying on link-local addresses for connection authentication.

The resulting functional safety assurance data fits within 12 bytes.
Assurance Data

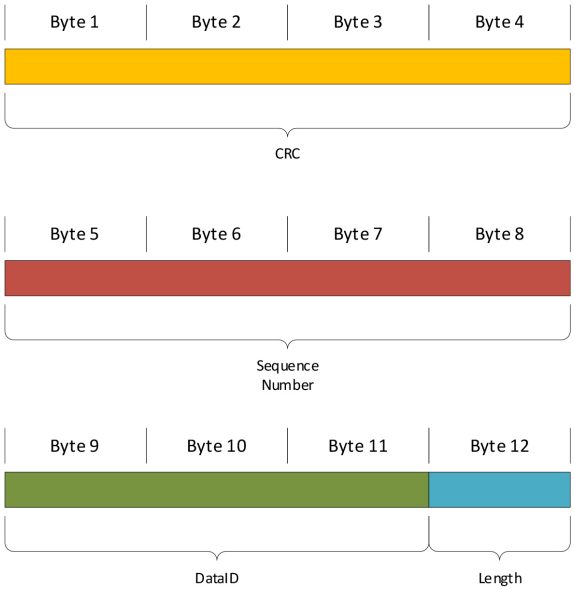

Figure 4: Format of Profile #2 Assurance Data

Figure 4 illustrates the format of the assurance data for Profile #2. The 8-bit Length field contains a count of the bytes over which the CRC was calculated.

Benefits

- This profile can handle a PG's parameter data payload whose length can range from 0 to 19 bytes.
- This profile is suitable for communications across routers due to its specification of a 24-bit data identifier, DataID, that provides connection authentication and that must be unique within a system.
- This profile uses the same CRC polynomial and Sequence Number as that used in Profile #1.
- The CRC calculation in this profile covers the PG's parameter data payload as well as the Sequence Number, DataID, and Length fields.

Drawbacks

- This profile cannot handle a PG whose parameter data payload is large enough to completely fill a CAN FD data frame.
- The scope of DataID definitions is specific to a system; there are no globally defined DataIDs.
- Like all profiles in [6], this profile is limited to J1939-22 communications.
- Like all profiles in [6], this profile is still under development.

Profile #3

Overview

This profile focuses on the following:

- Handling a PG's parameter data payload that is of variable length and that can be much larger than that supported by any other profile.
- Handling data that can only be communicated via the FD Transport protocol.
- Supporting communication across routers by not relying on link-local addresses for connection authentication.

The resulting functional safety assurance information fits within 17 bytes.

Assurance Data

Figure 5 illustrates the format of the assurance data for Profile #3. The 16-bit Length field contains a count of the bytes over which the CRC was calculated.

Benefits

- This profile can handle a PG's parameter data payload whose length can range from 0 to 65,526 bytes.
- This profile makes use of a CRC polyomial (labeled as CRC-64-ECMA in [2]) that results in a 64-bit CRC.
- The Sequence Number in this profile is the same as that used in Profile #1 and Profile #2.
- This profile uses the same DataID as that defined in Profile #2.
- The CRC calculation in this profile covers the PG's parameter data payload as well as the Sequence Number, DataID, and Length fields.

Drawbacks

- This profile has the largest set of functional safety assurance data of any profile.
- The CRC polynomial used by this profile is computationally more complex than that of any other profile.
- Like Profile #2, the scope of DataID definitions is specific to a system.
- Like all profiles in [6], this profile is limited to J1939-22 communications.
- Like all profiles in [6], this profile is still under development.

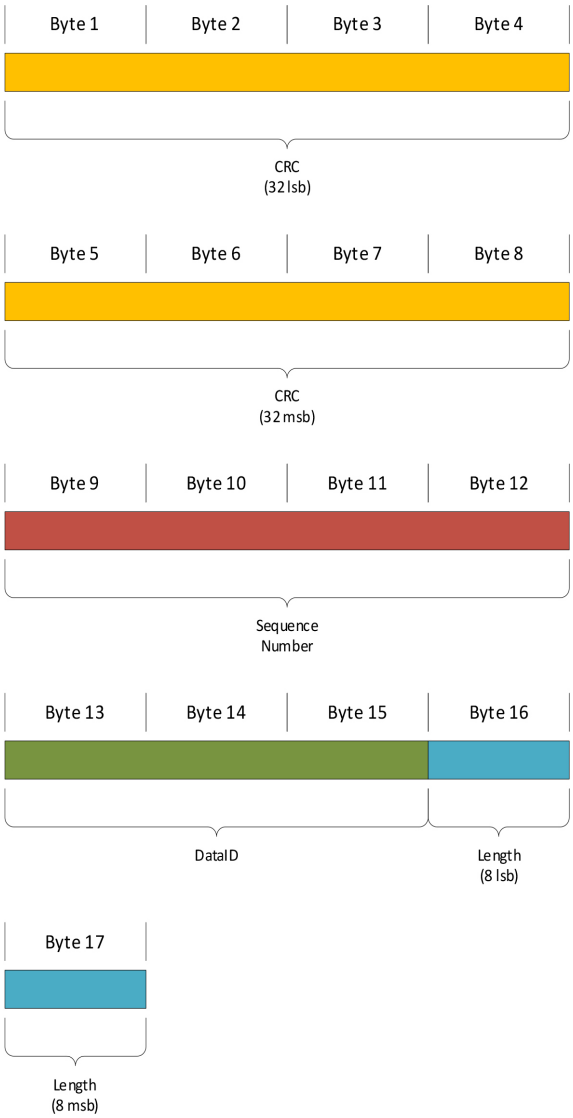

Figure 5: Format of Profile #3 Assurance Data

Conclusion

The communication errors and safety measures described in [1] serve as the basis for the functional safety support specified in [5] and [6]. These SAE J1939 standards provide different versions and profiles for this support over both Classic CAN and CAN FD, allowing safety-related applications to select the appropriate version or profile that meets both their systems' needs and their functional safety requirements.

References

[1] IEC 61784-3:2021: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions
[2] P. Koopman. Best CRC Polynomials, https://users.ece.cmu.edu/~koopman/crc/
[3] SAE J1939-21: Data Link Layer, May 2022
[4] SAE J1939-22: CAN FD Data Link Layer, September 2022
[5] SAE J1939-76: SAE J1939 Functional Safety Communications Protocol, February 2024 unpublished draft
[6] SAE J1939-77: SAE J1939 CAN FD Functional Safety Assurance Data, February 2024 unpublished draft

Travis Breitkreutz
Caterpillar
2300 Carl Rd.
US-75062 Irving, TX
www.cat.com