

Functionally-safe J1939 communication

Commercial road and off-highway vehicles as well as off-road construction machines use often J1939-based application layers. To meet the increasing demand on functional safety, SAE has developed for CAN CC (classic) and CAN FD dedicated protocols: J1939-76 and J1939-77, respectively.

This article discusses the two SAE J1939 standards for functionally safe communications on CAN CC (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 original version as published in 2020 and lists the deficiencies of this version. Finally, it details features of the revised version currently under development that make up for these deficiencies. For SAE J1939-77, the article 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.

IEC 61784-3: Safety-relevant communication principles

The IEC 61784-3 standard defines various communication errors that can occur:

- ◆ **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** 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** 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** refers to the failure to receive a message that was 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** 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** 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** 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** refers to the delivery of a message to the wrong recipient, which 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.

Additionally, the IEC 61784-3 standard defines safety measures that can be used to detect such errors to achieve the desired level of functional safety:

- ◆ **Sequence numbers** embedded in the message identify the position of the message relative to other messages in the same stream. They change 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 expectations** are 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** is when a message has a unique source and/or destination identifier for the safety-related participants.
- ◆ **Data integrity assurance** adds redundant data (e.g., cyclic redundancy checks, also known as CRCs) to a message to detect corruption in the message. ▷

- ◆ **Redundancy with cross-checking** communicates the safety data in separate instances, either in separate messages or within 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 are designs, in which communicated safety-related data use different integrity mechanisms than those used by the communicated non-safety-related data. This ensures that non-safety-related messages do not affect a safety-related recipient.

Table 1 describes the coverage of various communication errors by safety measures employed in J1939-76 and J1939-77.

Table 1: Coverage of communication errors by employed safety measures (Source: Caterpillar, J1939-76, J1939-77)

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 J1939-76 employ redundancy with cross-checking for some, but not all, communicated data. Profiles in J1939-77 do not employ redundancy with cross-checking.

J1939-76: Two Safety Data Group (SDG) versions

There are two versions of functional safety support specified in J1939-76. This support applies to Parameter Groups (PGs) whose parameter data payloads range from 1 byte to 8 byte 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:

- ◆ one 32-bit CRC,
- ◆ one sequence number,
- ◆ the parameter group number (PGN),
- ◆ the destination address (DA) for point-to-point PGs,
- ◆ and the source address (SA) of the associated SDM.

Because of the need for two different messages, J1939-76 specifies timing and order-of-transmission constraints to ensure that the right SHM instance appears with the right SDM instance.

The original publication of J1939-76 in 2020 specified what is 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 (Society of Automotive Engineers) began with development of the SHM2 version to correct those deficiencies. ▶



Learn more



The adaptive machine

Your competitive advantage

Today's challenges

Mass customization

Product proliferation

Short product lifecycles

Adaptive machine solutions

Machines that make to order

Instant changeovers on-the-fly

Easy reconfiguration via digital twins

To win in a world of mass customization, e-commerce, direct-to-consumer and omnichannel, it takes machinery that's built to adapt. The first machinery concept that adapts to the products being produced and packaged! B&R enables adaptive manufacturing through intelligent mechatronic product transport integrated with robotics, machine vision and digital twins.

br-automation.com/adaptive



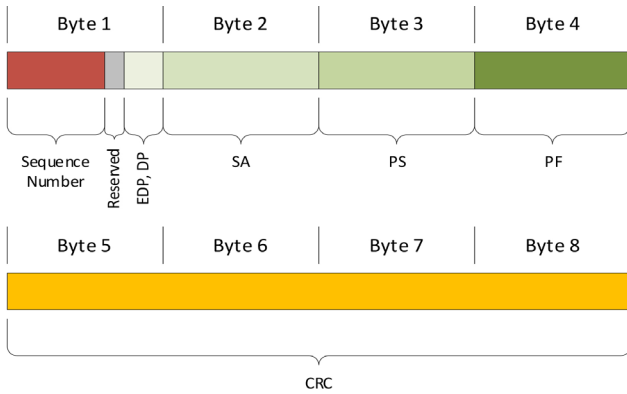


Figure 1: Format of the SHM1 payload specified in J1939-76 (Source: Caterpillar)

Figure 1 illustrates the format of the SHM1 payload. The EDP (Extended Data Page), DP (Data Page), PF (PDU Format), PS (PDU Specific), and SA fields are all bitwise inverted; the values of these fields before inversion match the values in the SDM. The arrangement of the CRC field is least-significant-byte-first. This approach has the following 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 (based on CAN CC) or J1939-22 communications (based on CAN FD).
- ◆ This version has been available for several years.

But there are also some drawbacks in this version:

- ◆ The 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 5-bit Sequence Number is relatively small.
- ◆ This version doubles the bandwidth needed to communicate safety data.
- ◆ 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.

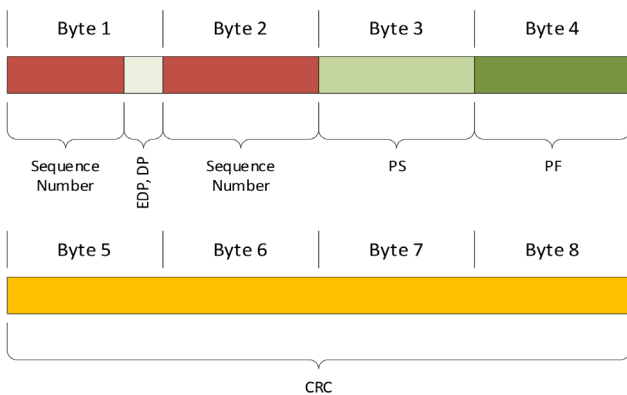


Figure 2: Format of the SHM2 payload specified in J1939-76 (Source: Caterpillar)

Figure 2 illustrates the format of the SHM2 payload. 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. The arrangement of the CRC field is least-significant-byte-first.

The benefits of this solution are:

- ◆ Like in 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 14-bit Sequence Number in this version is larger 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.

The drawbacks are:

- ◆ 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.

J1939-77: Three profiles

There are three profiles specified in J1939-77 for functional safety support. These profiles take advantage of the Multi-PG and FD Transport protocols specified in J1939-22 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 byte to 65526 byte in length.

Each of the profiles 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 is 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. All three profiles have the disadvantage that they are limited to J1939-22 communications and that they are still under development.

The Profile #1 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 the 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.

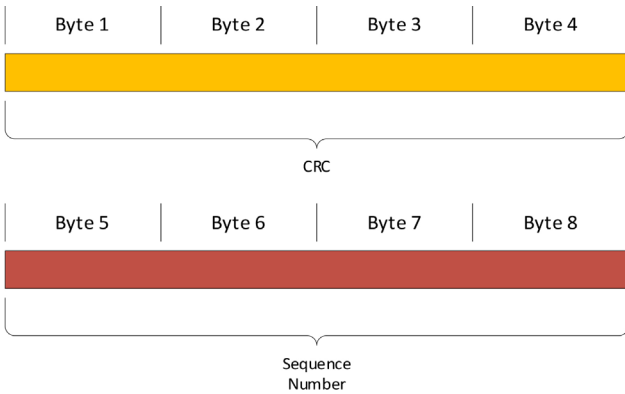


Figure 3: Format of Profile #1 assurance data specified in J1939-77 (Source: Caterpillar)

Figure 3 illustrates the format of the assurance data for Profile #1. The internal arrangement of both fields is least-significant-byte-first. 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.

The benefits are:

- ◆ 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.

There are some trade-offs:

- ◆ This profile requires that the PG's parameter data payload is exactly 8 byte.
- ◆ Like the SHM1 and SHM2 versions, this profile is not well suited for communications across routers.

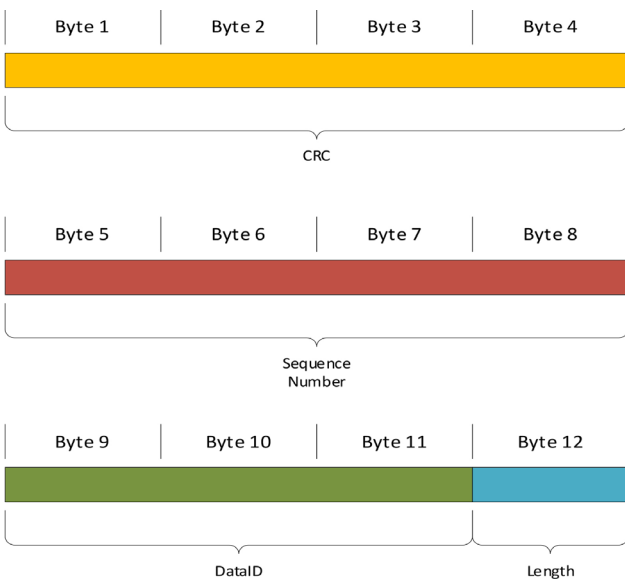


Figure 4: Format of Profile #2 assurance data specified in J1939-77 (Source: Caterpillar)

The Profile #2 focuses on the following:

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

The resulting functional safety assurance data fits within 12 bytes.

Figure 4 illustrates the format of the assurance data for Profile #2. The internal arrangement of all fields is least-significant-byte-first. The Length field contains a count of the bytes over which the CRC is calculated. This solution offers the following advantages:

- ◆ This profile can handle a PG's parameter data payload whose length can range from 0 byte to 19 byte.
- ◆ 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.

The drawbacks are:

- ◆ 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.

The Profile #3 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.

Figure 5 illustrates the format of the assurance data for Profile #3. The internal arrangement of all fields is least-significant-byte-first. The Length field contains a count of the bytes over which the CRC was calculated. The advantages are:

- ◆ This profile can handle a PG's parameter data payload whose length can range from 0 byte to 65526 byte.
- ◆ This profile makes use of a CRC polynomial (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.

Of course, there are also some 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.

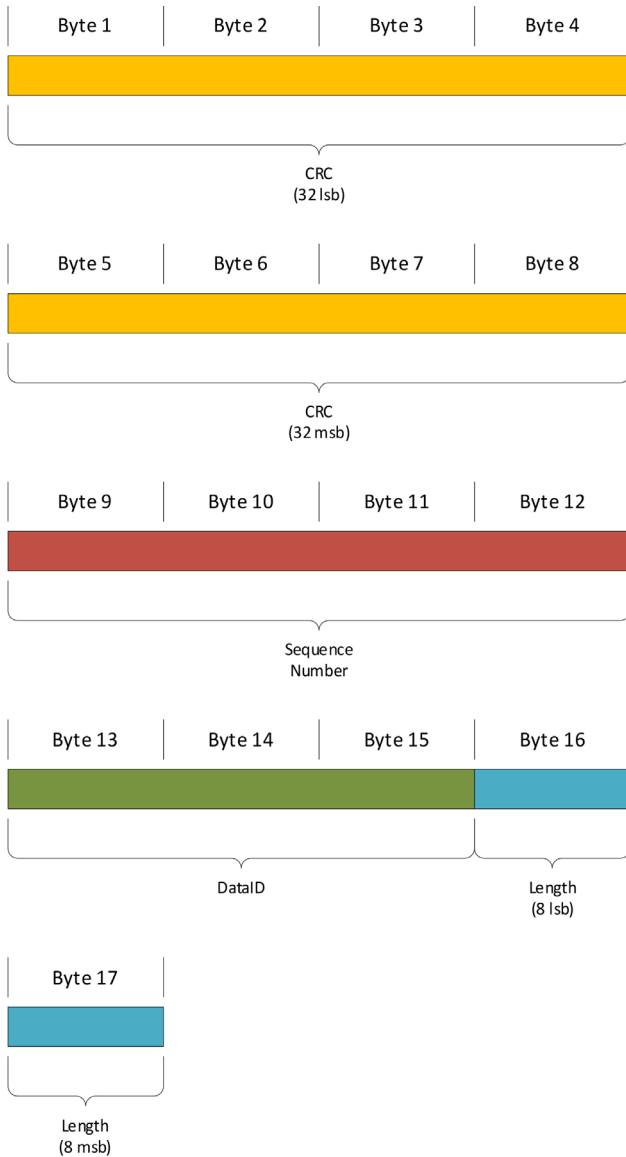


Figure 5: Format of Profile #3 assurance data specified in J1939-77 (Source: Caterpillar)

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

Conclusion

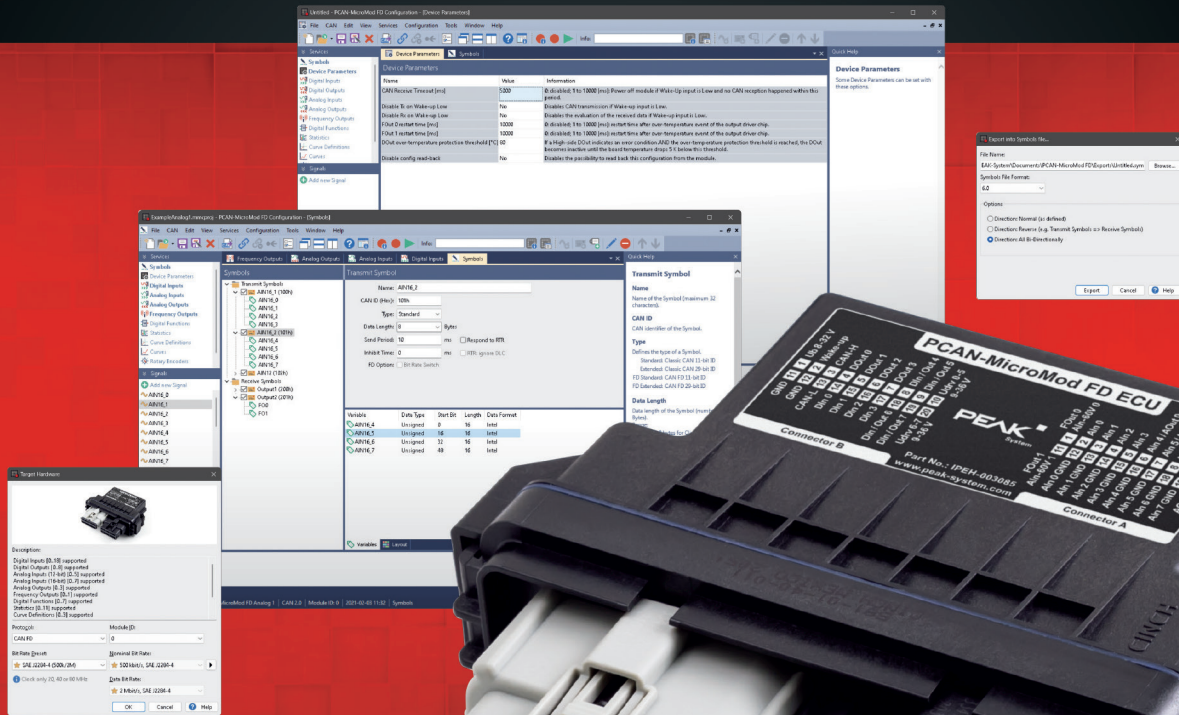
The communication errors and safety measures described in IEC 61784-3:2021 serve as the basis for the functional safety support as specified in SAE J1939-76 and SAE J1939-77. These SAE J1939 specifications provide different versions and profiles for this support over both CAN CC and CAN FD, allowing safety-related applications to select the appropriate version or profile that meets both their systems' needs and their functional safety requirements. ◀

(This article is based on the 18th international CAN Conference (iCC) presentation by Travis Breitreutz. The complete paper is published in the 18th iCC proceedings 2024; CiA, Nuremberg.)

Author



Travis Breitreutz
Caterpillar
breitreutz_travis_o@cat.com
www.cat.com



Configurable I/O Module for Automotive Applications

■ PCAN-MicroMod FD ECU

With CAN FD, a mix of digital and analog I/Os, and its tough case, the PCAN-MicroMod FD ECU can be your solution for integrating custom accessories in utility and heavy duty vehicles operating under harsh conditions.

The PCAN-MicroMod FD ECU can be configured with a Windows software via CAN. Besides simply mapping its I/Os to CAN messages, several function blocks for processing the data are available as well.

Specifications

- High-speed CAN connection (ISO 11898-2)
 - Complies with CAN specifications 2.0 A/B and FD
 - CAN FD bit rates for the data field (64 bytes max.) from 40 kbit/s up to 10 Mbit/s
 - CAN bit rates from 40 kbit/s up to 1 Mbit/s
- Wake-up by CAN bus or by separate input
- 4 digital inputs
 - Pull-up or pull-down configurable
- 8 digital outputs with High-side switches
 - 2 outputs with 5 A and 6 outputs with 2 A
 - 4 alternatively usable as a digital input or additionally for reading back the output level

- 8 analog inputs
 - Resolution 16 bit
 - Measuring range adjustable: ± 2.5 V, ± 5 V, ± 10 V, ± 20 V
- 4 of the analog inputs alternatively usable as analog output
 - Resolution 12 bit
 - Voltage range adjustable: 0 to 5 V or 0 to 10 V
- 2 frequency outputs
 - Low-side switches (3 A)
 - Adjustable frequency range from 0 to 20 kHz
 - Alternatively usable as analog inputs with voltage range from 0 to 60 V
- Connections for CAN, I/O, and power supply via two 20-pole automotive connectors (Molex MX150)
- Plastic casing with increased Ingress Protection IP67 and flange
- Operating voltage 8 to 32 V; suitable for use in 12 and 24 V vehicle electrical systems
- Extended operating temperature range from -40 to $+85$ °C (-40 to $+185$ °F)
- E1 type approval in progress

Please note: The PCAN-MicroMod FD ECU is expected to be available in Q3 2024.



www.peak-system.com

Take a look at our website for the international sales partners. Scan the QR code on the left to open that page.

PEAK-System Technik GmbH

Phone: +49 6151 8173-20
 Fax: +49 6151 8173-29
 E-mail: info@peak-system.com

