EXCELON™ F-RAM functional safety

EXCELON™ Auto, EXCELON™ Ultra

Abstract

Advancements in automotive technologies such as electric vehicles and autonomous driving have the potential to increase the risk of injury to vehicle occupants and others. For example, electric vehicles are designed with high-voltage power buses and high-energy battery packs that can be extremely hazardous if not properly managed. Similarly, electronics in automotive are becoming more complex and systems are becoming more dependent on them while taking critical decisions which can create more risks for human safety if they are not designed with adequate safety nets.

Safety becomes the fundamental requirement of automotive application development. For that purpose, ISO 26262 has laid out functional safety guidelines to protect road users from injuries caused by faults or malfunctions in the vehicle electronics and software. To meet these rigorous safety requirements, Infineon EXCELON™ F-RAM offers a broad portfolio of functional safety-ready products that encompass various safety features and support collateral to help you achieve the required ISO 26262 Automotive Safety Integrity Level (ASIL).

Table of contents

1 Functional safety

The ISO26262 – Road Vehicles – Functional Safety standard defines functional safety as “the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical or electronic systems.” The purpose of functional safety is to establish various safety requirements to reduce risks to an acceptable level and smoothly manage and track these safety requirements. Therefore, designing safe and reliable automotive applications to ensure human safety becomes more critical.

1.1 Automotive Safety Integrity Level (ASIL)

ASIL expresses the criticality associated with a function of the system. It defines the safety requirements that must be fulfilled by the design and development of the system so that even in conditions of failure, the system provides a sufficient margin of safety for the users (driver, passengers, road traffic participants, etc.). ASIL is a risk classification system defined by the ISO 26262 standard. It establishes safety requirements for automotive components to be compliant with the ISO 26262 standard based on the probability and acceptability of harm in systems.

Various systems and subsystems in a vehicle are classified for expected ASIL performance using a four-level categorization from “ASIL A” – for low risk to “ASIL D” – for high risk. For example, as classified in **Figure 1**, systems such as powertrain, smart airbag, and advanced driver assistance system (ADAS) require an ASIL-D grade - the highest rigor applied to safety assurance because these systems present a high risk of injury in the event of failure when the vehicle is in motion. On the other end of the safety spectrum, failure of the components in infotainment systems such as the radio or media player do not present serious risk of harming anyone and are classified as ASIL A. **Figure 2** plots the ASIL levels.

There is another ASIL category Quality Management (QM) level that represents hazards that do not dictate any safety requirements beyond meeting basic qualities. QM systems just need to follow standard quality management processes. Systems that fall in the QM category don't have to comply with any specific objectives in ISO 26262 because the risks associated with the systems are acceptable for safety.

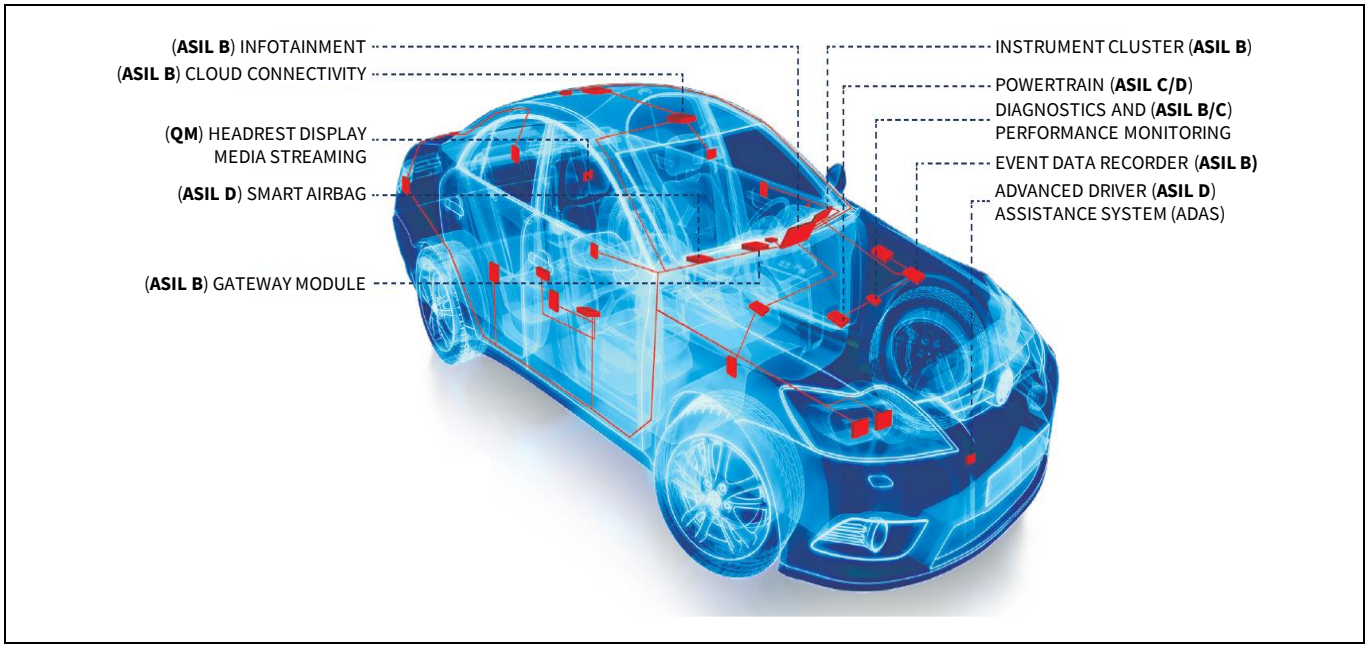

Figure 1 Typical automotive functional safety classifications

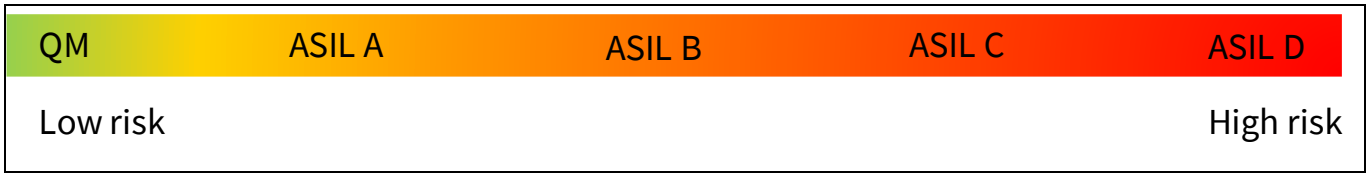

Figure 2 ASIL levels

1.2 ASIL assessment/measurement

ASILs are established by performing risk assessment and hazard analysis. The following system's variables are analyzed and measured to determine the applicable ASIL in the automotive subsystems:

- **Severity** (type of injuries on driver, passenger, pedestrians) – i.e., if a system were to fail, how bad could the safety consequences potentially be on the driver, passengers, or nearby pedestrians and vehicles.
- **Exposure** (occurrence of the vehicle exposure to the hazard) – i.e., the likelihood of an operational situation that can be hazardous if coincident with the failure mode under analysis.
- **Controllability** (how much the driver can do to prevent the injury)

Each of these variables is further broken down into sub-classes.

1.2.1 Severity

Severity has four classes ranging from S0 to S3, as shown in **Table 1**.

Table 1 Class of severity (ISO 26262-3)

Class	S0	S1	S2	S3
Description	No injuries	Light to moderate Injuries	Severe to life-threating (survival probable) injuries	Life-threating to fatal (survival uncertain) injuries

1.2.2 Exposure

Exposure has five classes ranging from E0 to E4, as shown in **Table 2**.

Table 2 Class of probability of exposure regarding operational situations (ISO 26262-3)

Class	E0	E1	E2	E3	E4
Description	Incredibly unlikely	Very low probability. Injury could happen only in rare operating conditions	Low probability	Medium probability	High probability. Injury could happen under most operating conditions

1.2.3 Controllability

Controllability has four classes ranging from C0 to C3, as shown in **Table 3**.

Table 3 Class of controllability (ISO 26262-3)

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

All variables and sub-classifications are analyzed and combined to determine the required ASIL. For example, a combination of the highest hazards (S3, E4, and C3) would result in an ASIL D classification.

1.3 ASIL determination

ASIL determination is the result of hazard analysis and risk assessment. In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system and likelihoods of the hazard manifesting those effects. Because many variables – exposure, severity, and controllability – are involved for ASIL determination, engineers are required to make certain assumptions. To summarize, ASIL definitions are informative rather than prescriptive; ASIL classification depends on the context and interpretation. **Figure 3** demonstrates a typical flowchart for ASIL classification.

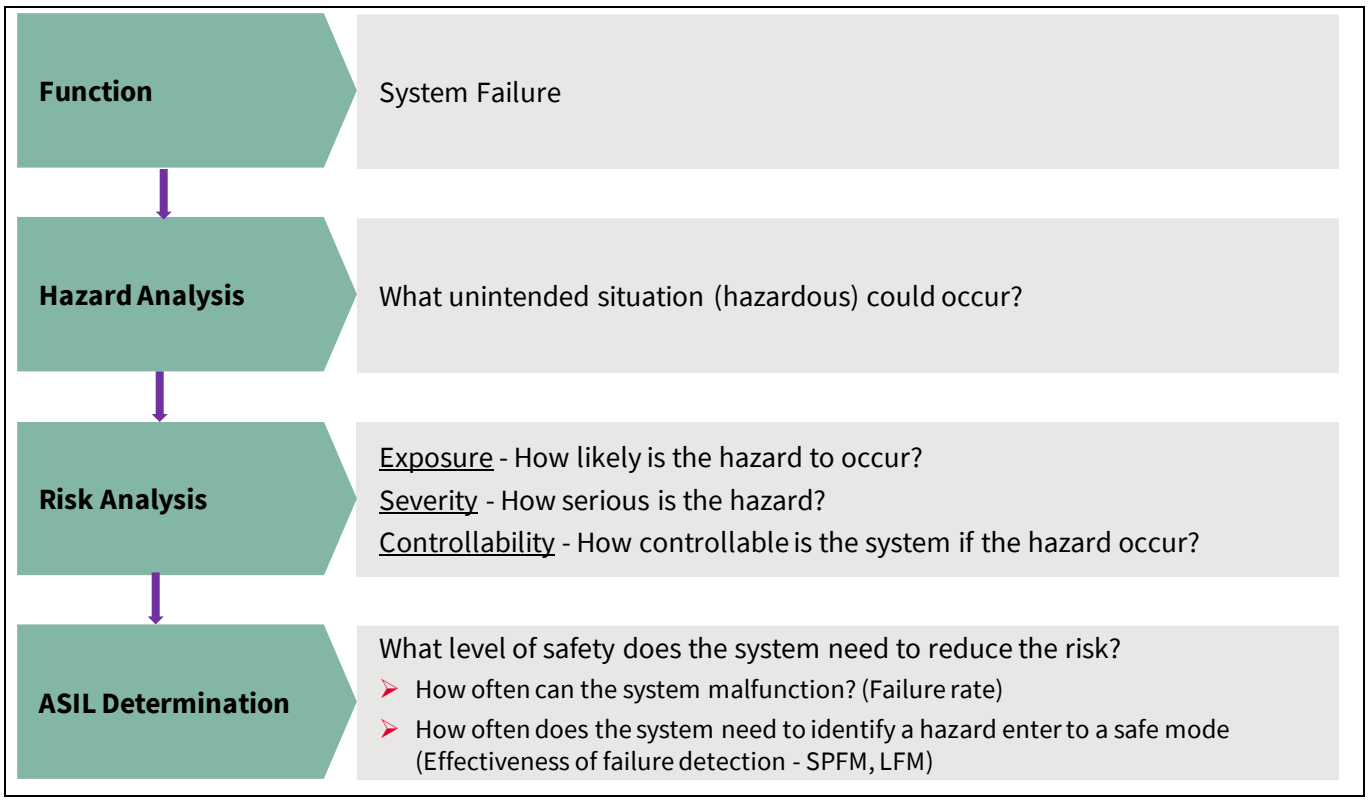

Figure 3 Automotive functional safety level classification

Figure 4 shows the determination of ASIL using parameters S, E, and C.

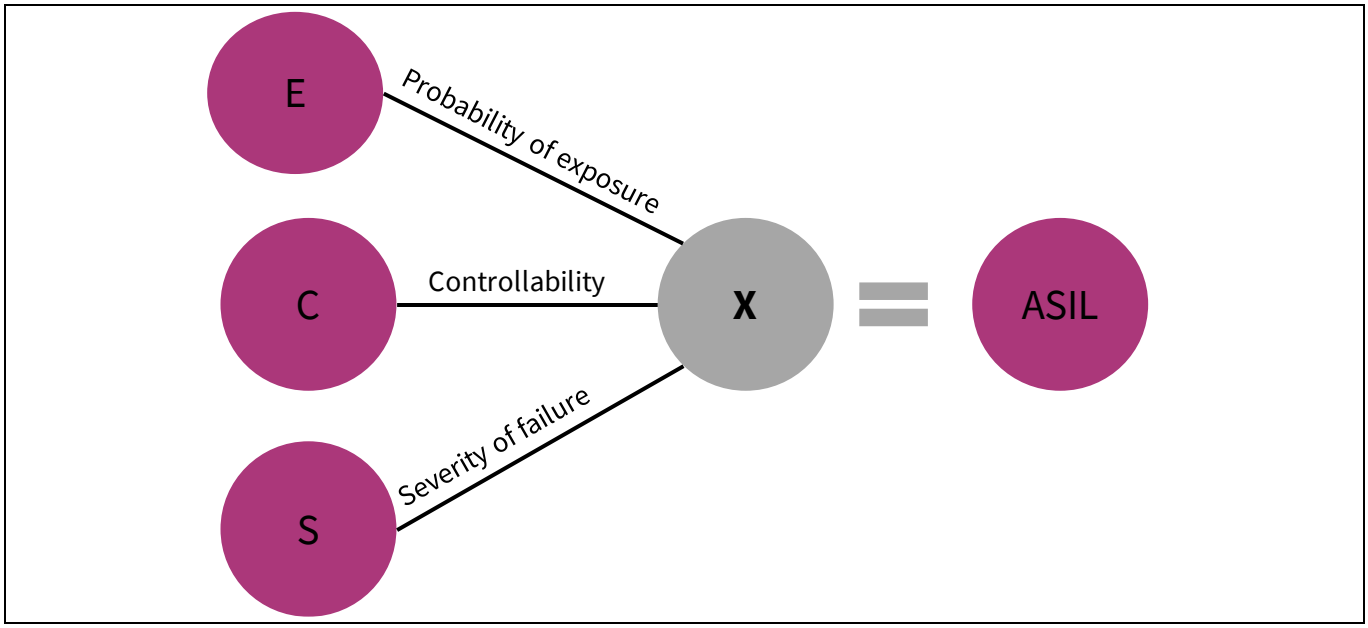

Figure 4 Automotive ASIL determination

ASIL levels – ASIL A, B, C, and D are assigned based on an allocation table defined by the ISO 26262 standard, as shown in **Table 4**.

Table 4 ASIL allocation (ISO 26262)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

1.4 ASIL decomposition

Under certain circumstances, the ASIL can be lowered through ASIL decomposition. The standard describes the ASIL decomposition procedure as a technique to reduce the criticality of a functional safety requirement by splitting it into multiple redundant requirements, each with a lower ASIL value. **Figure 5** shows the possible decomposition combinations as illustrated in the standard. The notation ASIL X(Y) is used to track the original functional safety requirement and to ensure that the proper system-level analysis is performed at ASIL *Y* level while using the decomposed ASIL *X* levels.

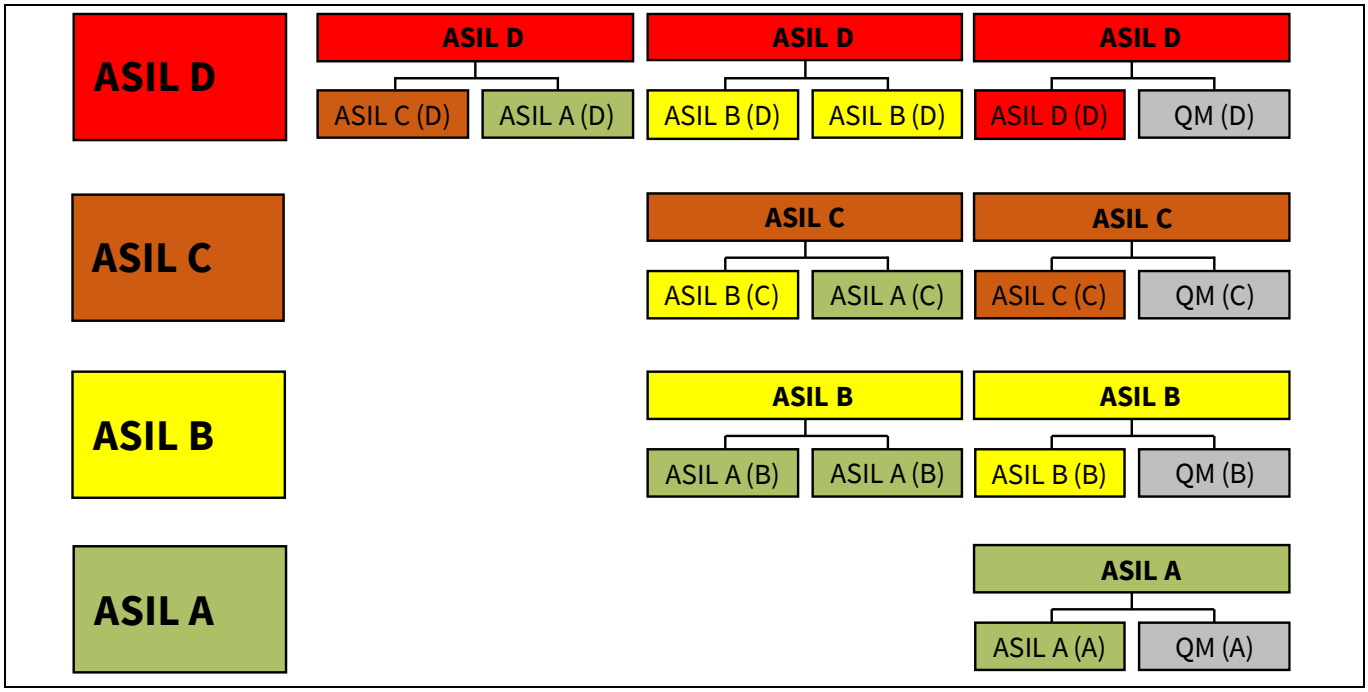

Figure 5 Automotive ASIL decomposition

1.5 ISO 26262 failure rate metrics

ISO 26262 failure rate metric covers the evaluation of the hardware architectural metrics. Specifically, these metrics are intended to evaluate the effectiveness of the hardware architecture in dealing with random failures. The metrics defined in this part are:

1.5.1 Single-point faults (SPF)

SPF reflects the robustness of the design to single-point and residual faults.

1.5.2 Latent faults (LF)

LF reflects the robustness of the design to multi-point faults whose presence are neither detected by a safety mechanism nor perceived by the driver.

1.5.3 Failure-in-time (FIT)

Probability of hardware failure. FIT is the number of failures per billion hours of operation. A smaller FIT number of a component or a system makes it less susceptible to a failure.

ISO fault metrics only apply to higher ASIL functions (i.e., B, C, or D), as summarized in **Table 5**.

Table 5 ISO 26262 failure rate metrics

ASIL	Failure rate metric		
	Single-point faults (SPF)	**Latent faults (LF)**	**Failure-in-time (FIT)**
ASIL A	Not applicable	Not applicable	<1000 FIT
ASIL B	≥90%	≥60%	<100 FIT
ASIL C	≥97%	≥80%	<100 FIT
ASIL D	≥99%	≥90%	<10 FIT

2 Functional safety for Infineon EXCELON™ F-RAM

Infineon's EXCELON™ F-RAM portfolio with safety packages is compliant with ISO 26262 ASIL B and designed for use in safety-critical applications.

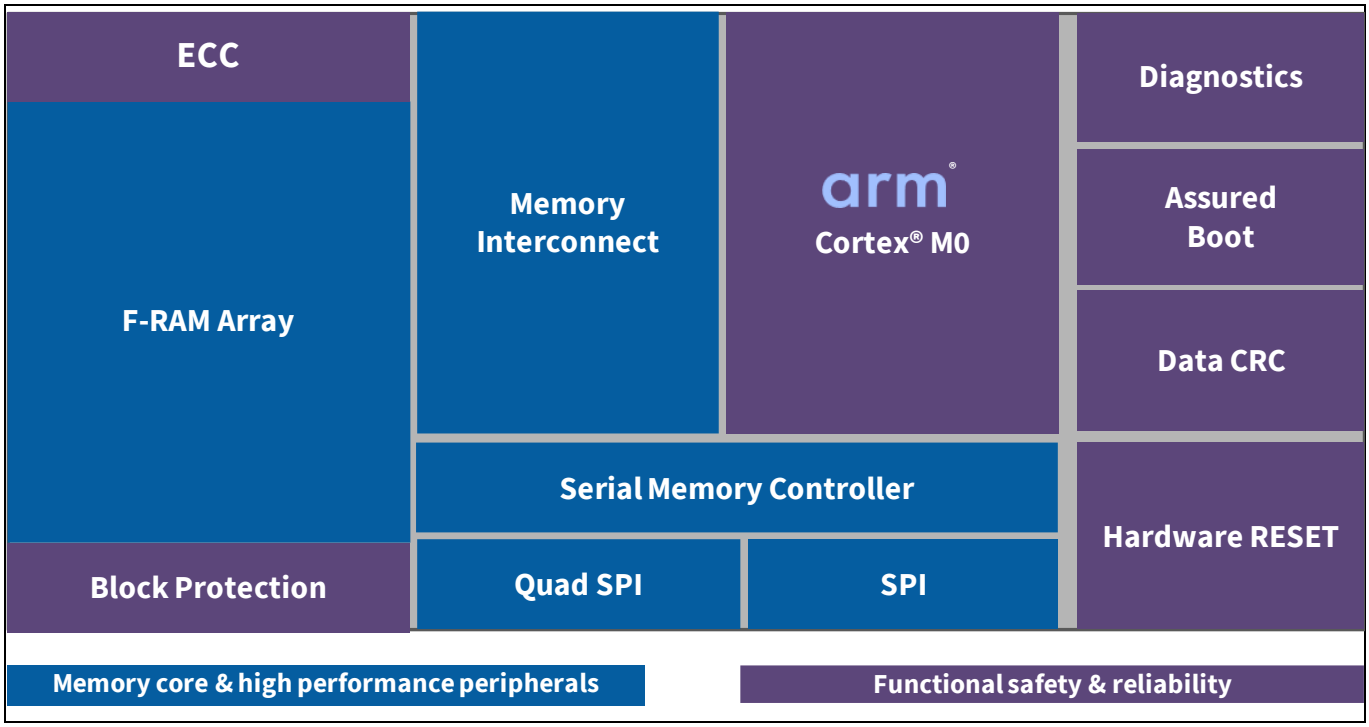

Figure 6 EXCELON™ F-RAM device architecture

2.1 Embedded ECC

EXCELON™ F-RAM has on-chip error correcting code (ECC) which executes on-the-fly, at bus speed, and is used to detect and correct single-bit or double-bit errors in every 64-bit (8-byte) data unit.

8-Mbit and lower density parts in 8-pin packages support single-bit error correct/double-bit error detect (SECDED). 8-Mbit and higher density parts in 24-pin package support double-bit error correct/triple-bit error detect (DECTED).

2.1.1 Single-bit error correct, double-bit error detect (SECDED)

2.1.1.1 Single-bit error

Function/system error type: Single-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: Single-bit errors are automatically corrected by the on-chip ECC circuit. The F-RAM executes write-back (refresh) after every read operation which reprograms the corrected bit in the F-RAM cell. Therefore, single-bit errors reside in the F-RAM cell only until the specific memory location is accessed (write/read). No action is needed by the host after one-bit errors occur.

2.1.1.2 Double-bit error

Function/system error type: Double-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: Double-bit errors can be detected by the on-chip ECC circuit but they cannot be corrected. The host can check the 2BD ECC flag after every read operation to determine whether any double-bit errors occurred in the read data unit and to determine any required appropriate action.

2.1.1.3 Triple- or more-bit error

Function/system error type: Three or more-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: The on-chip ECC cannot detect or correct errors in three or more bits. If necessary, the host can perform the 3-bit error detection/ correction in firmware and store the ECC checksum in the F-RAM along with the data. Alternatively, the application can also use the redundancy method where a duplicate (redundant) data copy is stored at different F-RAM locations and for every read both data copies are read and compared before using it.

2.1.2 Double-bit error correct, triple-bit error detect (DECTED)

2.1.2.1 Single-bit and double-bit error

Function/system error type: Single- or double-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: Single- or double-bit errors are automatically corrected by the on-chip ECC. The F-RAM executes a write-back (refresh) after every read operation which reprograms the corrected bit in the F-RAM cell. Therefore, single- or double-bit errors reside in the F-RAM cell only until the specific memory location is accessed (write/read). No action is needed by the host after single- or double-bit error occurs.

2.1.2.2 Triple-bit error

Function/system error type: Triple-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: Triple-bit errors can be detected by the on-chip ECC circuit, but they cannot be corrected. The host can check the 3BD ECC flag after every read operation to determine if any triple-bit error occurred in the read data unit and determine any required appropriate action.

2.1.2.3 Four- or more-bit error

Function/system error type: Four or more-bit error occurred in the 64-bit (8-byte) data unit.

EXCELON™ F-RAM coverage and system workaround: The on-chip ECC cannot detect or correct errors in four or more bits. If necessary, the host can perform four-bit error detection/correction in firmware and store the ECC checksum in the F-RAM along with data. Alternatively, the application can also use the redundancy method where a duplicate (redundant) data copy is stored at different F-RAM locations and for every read both data copies are read and compared before using it.

2.2 Data cyclic redundancy check (CRC)

Function/system error type: Stored data in the F-RAM array is corrupted due to either soft error or a timing glitch during the transmission which can change the CRC calculation on the block of data stored.

EXCELON™ F-RAM coverage and system workaround:

- The host calculates the CRC on the block of data before writing it to the F-RAM.
- (Optional) The host stores the CRC checksum in the F-RAM.
- The host issues CRC command which calculates the CRC on the block of data stored in the F-RAM. The F-RAM stores the results in the checksum register which can be read by the host.
- The host compares the two checksums (by the host and by the F-RAM) to verify if the transmitted data matches with the received data in the F-RAM.

2.3 Memory block protection

Function/system error type: Unintended write to the F-RAM due to the system malfunction.

EXCELON™ F-RAM coverage and system workaround: The F-RAM protects blocks of memory (selected address range) from an unintended write by making the blocks read-only by setting the block protect bits BP[2:0] in the status register.

2.4 Write disable

Function/system error type: Unintended write to the F-RAM due to the system malfunction.

EXCELON™ F-RAM coverage and system workaround: Write to the EXCELON™ F-RAM requires the Write Enable Latch (WEN) bit set to '1' in the status register by executing the WREN opcode. Similarly, the WRDI opcode clears the "WEN" latch in the status register. Clearing "WEN" protects the memory and the status register from an unintended write.

2.5 Assured boot

Function/system error type: Device fails to boot up after power up or after the hardware reset (RESET#).

Coverage and system workaround: The EXCELON™ F-RAM always boots up to a known state. In case the boot up failure is detected either due to memory internal config corruption or due to any other reason, the device always boots up to a known state and sets the boot failure signature in its status register which can be read by the host to determine next action.

2.6 HW reset (RESET#)

Function/system error type: Device enters into an unknown access mode or state.

Coverage and system workaround: The hardware reset function via RESET# pin brings the EXCELON™ F-RAM to a known state in case the device enters an undefined state due to a wrong configuration setting.

2.7 Return to known device config (Go-home)

Function/system error type: The host and the device access modes are out of sync, due to a power glitch or system reset; the host starts in a default access mode which can differ from the EXCELON™ F-RAM present access mode.

Coverage and system workaround: The host can keep the EXCELON™ F-RAM non-volatile configuration register settings to either factory default or user default. The system may use the volatile register counterpart

of the non-volatile register to change the device configuration after every power cycle or HW reset so that if EXCELON™ F-RAM enters to an unknown status during runtime, the hardware reset or power cycle can bring the device back to a known state.

2.8 Diagnostic features

Function/system error type: Device status or stored data integrity is compromised.

Coverage and system workaround: The EXCELON™ F-RAM supports the following diagnostic features which provide critical embedded operation status to the system.

- **Two-/three-bit error status:** The 2BD/3BD ECC flag is used to determine data corruption in the F-RAM. If the error flag is set, it indicates the data unit has errors which couldn't be corrected by the on-chip ECC.
- **Memory array data CRC suspend status:** This flag is used to determine whether CRC is in suspend mode.
- **Memory array data CRC abort status:** This flag is used to determine whether CRC is aborted.
- **Device ready/busy status:** This flag indicates whether the device is performing an embedded operation like CRC, boot-up failure case, in standby mode, and is ready to receive new transactions.

Table 6 EXCELON™ F-RAM safety/integrity feature summary

Safety and reliability mechanism			EXCELON™	
			SPI	QSPI
Embedded on-chip ECC	SECDED	Single-bit error correct	Yes	Yes
		Double-bit error detect		Yes
	DECTED	Single/double-bit error correct	Yes	Yes
		Triple-bit error detect		Yes
Data CRC				Yes
Block protect				Yes
Write protect			Yes	Yes
Assured boot			Yes	Yes
HW reset				Yes
Return to known device config (Go-home)			Yes	Yes
Diagnostic features			Yes	Yes

3 Safety deliverables

Infineon offers the functional safety documents to qualified customers upon request. The EXCELON™ F-RAM safety package consists of failure modes effects and diagnostics analysis (FMEDA) reports and safety manuals to accelerate safety assessments and help you reach your target ASIL. Contact Infineon **Technical Assistance Center (TAC)** to request the EXCELON™ F-RAM functional safety package.

4 Summary

The automotive industry is extensively demanding ISO 26262 compliance for the system and peripheral devices. Automotive applications need functional safety because of increasing dependency on electronic components and driver safety. Functional safety mechanisms and added features described in this document make Infineon EXCELON™ F-RAM a robust and reliable product family in today's automotive and industrial systems for critical and reliable data logging.

5 References

[1] **EXCELON™ Auto F-RAM memory**

[2] **EXCELON™ Ultra F-RAM memory**

[3] EXCELON™ F-RAM memory safety case (Document Number: 002-27070)

[4] EXCELON™ F-RAM family safety manual (Document Number: 002-24823)

[5] **ISO 26262-1:2018 Road vehicles — Functional Safety — Part 1**

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Go to www.infineon.com/support

Document reference

002-35690 Rev. **

IMPORTANT NOTICE

This document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.