Enabling Functional Safety with Semper Flash

About this document

Scope and purpose

AN218566 introduces functional safety and the role of Cypress’ NOR flash devices in functional safety in automotive applications.

Table of contents

About this document ........................................................................................................... 1
Table of contents ................................................................................................................. 1
1 Introduction ....................................................................................................................... 1
2 What is Functional Safety? .............................................................................................. 3
  2.1 Standards for Functional Safety ................................................................................ 3
  2.2 ISO 26262 Outline .................................................................................................... 4
  2.3 Safety Integrity Levels .............................................................................................. 5
  2.4 Product Development Process and Deliverables ...................................................... 6
    2.4.1 V-Model-Based Flow that Integrates Safety Requirements into Development Process .................................................................................. 6
    2.4.2 Safety Team and Deliverables During Product Development ......................... 6
  2.5 Safety Implementation in Automotive Systems ......................................................... 8
3 Cypress Functional Safety for Semper NOR Flash Memories ....................................... 10
  3.1 Safety Process ......................................................................................................... 10
  3.2 Safety Design .......................................................................................................... 10
    3.2.1 Error Correcting Code (Error Detection and Correction) ................................ 11
    3.2.2 Interface CRC (Cyclic Redundancy Check) .................................................... 12
    3.2.3 Data Integrity Check ....................................................................................... 14
    3.2.4 SafeBoot - Bootup (Initialization) Failure Recovery ........................................ 15
    3.2.5 SafeBoot – Detecting Corruption of Configuration ......................................... 15
    3.2.6 EnduraFlex™ ................................................................................................. 16
    3.2.7 Advanced Sector Protection .......................................................................... 17
    3.2.8 JEDEC SPI Reset Method .............................................................................. 18
    3.2.9 Sector Erase Count ......................................................................................... 19
  3.3 External Flash Use Cases and Functional Safety Evaluation .................................. 20
  3.4 Safety Deliverables ................................................................................................. 20
4 Summary ....................................................................................................................... 21
Revision history .................................................................................................................. 22
1 Introduction

The automotive industry is growing rapidly, and vehicles are becoming more reliant on electronic systems. The current generation car has more than 170 sensors, 85 control units, and 150 actuators, which will ultimately improve driver safety with self-driving and connected cars. However, these intricate systems need to be designed infallible for drivers; such a methodology is called Functional Safety.

Cypress has been associated with the Automotive and Functional Safety community for more than 15 years. At present, Cypress is one of the leading providers of automotive products (MCU, analog, memory, and software) in the industry and offers ASIL-compliant products. The cross-functional team (Product Safety Manager and Product Development Team) on functional safety is driving all automotive products to be ISO 26262-compliant by extending the development process to fulfill the ISO requirements and add the safety requirements to the products.

Cypress is introducing ISO 26262-compliant Semper™ NOR flash (HS-T, HL-T families) devices for automotive applications. These memory devices are designed to be ASIL B-compliant and can be used to generate ASIL-D compliant systems. The following sections describe functional safety, standards of functional safety, Cypress' implementation of functional safety requirements for NOR flash, advantages of applications using Cypress’ NOR flash devices, and key functional safety-related deliverables to customers.

Note: If you are well versed in ISO 26262 and basics of functional safety, you may skip Section 2.
Enabling Functional Safety with Semper Flash

What is Functional Safety?

2. What is Functional Safety?

Functional safety ensures the freedom from unreasonable risk of physical injury or damage to the health of people. If a system is capable of harming people in case of a malfunction, there must be safety measures to achieve functional safety.

There are systems in many application sectors where failures can lead to a physical injury or damage to the health of people. Safety relevance of critical systems like a nuclear power plant, some types of industrial machinery, or an airplane is obvious. Vehicles in general, braking and steering systems especially, need to take care of safety. Even systems like a microwave oven or a washing machine, used every day, could harm people in case of a malfunction.

The purpose of functional safety is to bring the risk down to an acceptable level and to reduce its negative impact; however, there is no such thing as zero risk. Functional safety measures the risk by determining how likely it is that a given event will occur and how severe it would be; in other words: how much harm it could cause.

Functional safety can be achieved through different approaches:

2.1 Standards for Functional Safety

Standards exist for functional safety in different application sectors. These standards provide guidelines and allow the comparison of different systems.

IEC 61508 is a central standard for electrical, electronic, and programmable electronic safety-related systems, which was first released in 1998. This standard can be seen as the parent standard from which other standards have been derived for many specific applications. These standards give guidelines on how to address functional safety within a certain application sector.

Figure 1 shows some of the application-specific standards for safety systems. All of these are electrical, electronic, or programmable electronic safety-related systems, so the general standard of IEC 61508 can be applied. Nevertheless, dedicated standards better fit actual applications.
Enabling Functional Safety with Semper Flash

What is Functional Safety?

**IEC 61508**

**ISO 26262**

**Automobile**

**EN 50129**

**Railway**

**IEC 61513**

**Nuclear Power**

**IEC 60601**

**Medical**

**IEC 61511**

**Process Industry**

**IEC 60335**

**Household Application**

**IEC 62061**

**Machinery**

**IEC 50156**

**Furnaces & Ancillary**

**DO-178**

**Avionics**

**What is Functional Safety?**

**IEC 61508**

**ISO 26262**

**Automobile**

**EN 50129**

**Railway**

**IEC 61513**

**Nuclear Power**

**IEC 60601**

**Medical**

**IEC 61511**

**Process Industry**

**IEC 60335**

**Household Application**

**IEC 62061**

**Machinery**

**IEC 50156**

**Furnaces & Ancillary**

**DO-178**

**Avionics**

**Figure 1**

**Functional Safety Standards**

### 2.2 ISO 26262 Outline

ISO 26262 is an international functional safety standard specifically designed for the application sector of electric, electronic, or both systems within road vehicles. It is intended to be applied to safety-related electric and electronic systems that are installed in series-production passenger cars with a maximum gross vehicle mass up to 3,500 kg. The ISO 26262 was first published in 2011; in 2018 it has been revised and now also applies to motorcycles, trucks, and busses. As shown in Table 1, ISO 26262 consists of 12 parts: 10 of them are normative, and parts 10 and 11 are informative guidelines.

#### Table 1 Parts of ISO 26262

<table>
<thead>
<tr>
<th>Part</th>
<th>Part Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vocabulary</td>
<td>There are 185 vocabulary of terms, definition, and abbreviations that are used within the standard. For example: Component (a part of a system, either in hardware or in software), Latent Fault (multiple-point fault, which is not detected by a safety mechanism)</td>
</tr>
<tr>
<td>2</td>
<td>Management of functional safety</td>
<td>Defines the required management tasks during the safety lifecycle of the product</td>
</tr>
<tr>
<td>3</td>
<td>Concept phase</td>
<td>In the concept phase, the item to be developed will be defined, thus initiating the safety lifecycle. The ISO 26262 defines four different levels for the Automotive Safety Integrity Level, known as ASIL: D, C, B, A. If there are no safety requirements at all, the classification is “quality managed” (QM).</td>
</tr>
<tr>
<td>4</td>
<td>Product development at the system level</td>
<td>Defines the refinement of functional safety requirements into technical safety requirements. The system level can be composed of both hardware and software components.</td>
</tr>
<tr>
<td>5</td>
<td>Product development at the hardware level</td>
<td>Defines the refinement of technical safety requirements into hardware safety requirements. The refinement allows a hand-over to the design team for implementation and verification.</td>
</tr>
</tbody>
</table>
Enabling Functional Safety with Semper Flash

What is Functional Safety?

<table>
<thead>
<tr>
<th>Part</th>
<th>Part Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Product development at the software level</td>
<td>Defines the refinement of technical safety requirements into software safety requirements. The refinement allows a hand-over to the software team for implementation and verification.</td>
</tr>
<tr>
<td>7</td>
<td>Production and operation</td>
<td>Specifies all requirements that are important for safety from production, operation, and maintenance service until the decommissioning of the product.</td>
</tr>
<tr>
<td>8</td>
<td>Supporting processes</td>
<td>Contains the requirements for all supporting processes that are used in the previous parts of ISO 26262. This includes, for example, requirements on configuration and change management, on how to manage requirements, and on prerequisites for reusing existing software or hardware components.</td>
</tr>
<tr>
<td>9</td>
<td>Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses</td>
<td>Contains detailed requirements on the different safety analyses that need to be performed on system level for the software and hardware. These analyses include both qualitative analyses such as Failure Modes and Effects Analysis (FMEA) or Fault Tree Analysis (FTA), and quantitative analyses such as Failure Modes, Effects and Diagnostics Analysis (FMEDA)</td>
</tr>
<tr>
<td>10</td>
<td>Guideline on ISO 26262</td>
<td>This part of the ISO 26262 is an informative part. It is a guideline on how to apply the previous nine parts.</td>
</tr>
<tr>
<td>11</td>
<td>Guideline on application of ISO 26262 to semiconductors</td>
<td>This newly added informative part gives additional guidance specifically on how to address and analyze semiconductor components in the life cycle.</td>
</tr>
<tr>
<td>12</td>
<td>Adaption of ISO 26262 for motorcycles</td>
<td>Any specifics with respect to motorcycles are handled, including the introduction of MSIL, the safety integrity level for motorcycles.</td>
</tr>
</tbody>
</table>

2.3 Safety Integrity Levels

Automotive applications have a range of subsystems with different levels of safety measures. For example, the systems related to airbag or braking require higher safety levels as compared to instrument cluster or front/rear view camera systems. A failure in the airbag or braking system could be dangerous to driver in contrast with other subsystems in the vehicle. Therefore, ISO 26262 defines Automotive Safety Integrity Levels (ASIL), i.e., ASIL A, ASIL B, ASIL C, and ASIL D. ASIL A is the lowest level of integrity and ASIL D is the highest ASIL classification, which is only assigned in hazardous or life-threatening cases or has a high-risk exposure and is difficult to control.

ISO 26262 recommends the levels of three key metrics:

- **Single Point Faults (SPF)**: One fault leads directly to the violation of the safety goal.
- **Latent Faults (LF)**: Multiple-point faults whose presence is not detected by a safety mechanism nor perceived by the driver.
- **Failure in Time (FIT)**: Probability of hardware failure. FIT is the number of failures per billion hours of operation.

Table 2 shows the proposed ISO 26262 metrics for ASIL B, ASIL C and ASIL D.

<table>
<thead>
<tr>
<th>Target</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single point fault</td>
<td>≥90%</td>
<td>≥97%</td>
<td>≥99%</td>
</tr>
<tr>
<td>Latent faults</td>
<td>≥60%</td>
<td>≥80%</td>
<td>≥90%</td>
</tr>
</tbody>
</table>
Enabling Functional Safety with Semper Flash

What is Functional Safety?

<table>
<thead>
<tr>
<th>Target</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure In Time (FIT)</td>
<td>(&lt;10^7 \text{ / h} \ (&lt;100 \text{ FIT}))</td>
<td>(&lt;10^7 \text{ / h} \ (&lt;100 \text{ FIT}))</td>
<td>(&lt;10^8 \text{ / h} \ (&lt;10 \text{ FIT}))</td>
</tr>
</tbody>
</table>

2.4 Product Development Process and Deliverables

2.4.1 V-Model-Based Flow that Integrates Safety Requirements into Development Process

Figure 2 illustrates the V-model-based development flow from assumptions on the system level, via requirements on hardware, and software level to the actual design. On the right part of the 'V', the testing of the design versus the requirements is shown.

![V-Model-Based Product Development Flow](image)

2.4.2 Safety Team and Deliverables During Product Development

The scope of a functional safety organization must cover all aspects of functional safety required both for hardware and software products. It includes the following:

- Functional Safety Managers (FSM) to lead the safety activities and certify the safety team members
- Project Safety Managers (PSM) that execute the safety plan of a project
- Functional Safety Center of Excellence (FS CoE) – safety team experts to drive safety initiatives in the company

This organization needs to generate a number of safety documents during the product development phase. If necessary, some of these documents need to be delivered to customers with the product. The main safety documents are:
Enabling Functional Safety with Semper Flash

What is Functional Safety?

1. **Safety Plan**: The safety plan is the first document that must be available. It describes the safety lifecycle with all planned safety activities within a project. It is the safety specification for a project and maintained by the project safety manager. The safety plan defines the different roles and responsibilities within the project and assigns resources to the roles. This assignment can be integrated into the project plan.

2. **Safety Element out of Context (SEooC) Specification**: As many suppliers do not develop an item on vehicle level but just a component, it is infeasible to fulfill all requirements from ISO 26262. Thus, the concept of a “Safety Element out of Context” (SEooC) is introduced.

An SEooC is a safety-related element (hardware or software) that is not developed for a specific item. This means that it is not developed in the context of a particular vehicle or system.

This specification defines the project from the safety perspective. It contains all assumptions about the environment, the target usage of the product, and the safety-related functions provided by the product. This includes assumptions about safety goals.

![Figure 3: SEooC Development Assumptions](image)

3. **Software/Hardware Safety Requirements Specification (SW/HWSRS)**: It contains all requirements derived from the SEooC specification. Traceability is maintained up to the assumptions in the SEooC specification and down to implementation specifications and verification of the requirements.

4. **Dependent Failure Analysis (DFA)**: It confirms the independence of safety mechanisms and freedom from interference, and tries to unveil common-cause failures.

5. **Failure Modes, Effects and Diagnostics Analysis (FMEDA)**: FMEDA is only done for hardware SEooCs. It is a detailed analysis on failure modes for different parts of the hardware, and assigns safety mechanisms to failure modes. This allows the calculation of the hardware architectural metrics and residual FIT rates to confirm that the required metrics for the ASIL are met.

6. **Safety Manual**: It documents all assumptions that need to be fulfilled by the integrator. This allows for the validation of the SEooC within the system. The safety manual also provides detailed information on how to use the product in a safety application.

7. **Safety Case**: It provides an argumentation how safety is achieved for a product. It collects the evidence for all required safety documents and, can be used as the starting point for any audit or assessment.
Enabling Functional Safety with Semper Flash

What is Functional Safety?

2.5 Safety Implementation in Automotive Systems

The following table shows how vehicle manufacturers determine the ASIL of different systems with respect to functional safety.

<table>
<thead>
<tr>
<th>Table 3</th>
<th>ASIL Determination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity Class</td>
<td>Exposure Class</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>S1 - Light and moderate injuries</td>
<td>E1-Very low</td>
</tr>
<tr>
<td></td>
<td>E2-Low</td>
</tr>
<tr>
<td></td>
<td>E3-Medium</td>
</tr>
<tr>
<td></td>
<td>E4-High</td>
</tr>
<tr>
<td>S2 - Severe and life-threatening injuries (survival probable)</td>
<td>E1-Very low</td>
</tr>
<tr>
<td></td>
<td>E2-Low</td>
</tr>
<tr>
<td></td>
<td>E3-Medium</td>
</tr>
<tr>
<td></td>
<td>E4-High</td>
</tr>
<tr>
<td>S3 - Life-threatening injuries (survival uncertain), fatal injuries</td>
<td>E1-Very low</td>
</tr>
<tr>
<td></td>
<td>E2-Low</td>
</tr>
<tr>
<td></td>
<td>E3-Medium</td>
</tr>
<tr>
<td></td>
<td>E4-High</td>
</tr>
<tr>
<td>S0 - No Injuries</td>
<td>If a hazard is assigned to severity class S0, no ASIL assignment is required.</td>
</tr>
<tr>
<td>E0 - Incredible</td>
<td>If a hazard is assigned to exposure class E0, no ASIL assignment is required.</td>
</tr>
<tr>
<td>C0 - Controllable</td>
<td>If a hazard is assigned to the controllability class C0, no ASIL assignment is required.</td>
</tr>
</tbody>
</table>

*QM (Quality Managed) is essential to ASIL for the safety function, but no explicit requirements from standard are applied.

Primarily, three organizations are involved during the implementation of safety in today’s automotive systems: Vehicle Manufacturer, System Supplier, and Component Supplier.

- The vehicle manufacturer defines a system and determines the required ASIL through a hazard and risk assessment. A specification of potential subsystems and a functional safety concept is provided to the system supplier.
- A development interface agreement sets the responsibilities and interfaces between the vehicle manufacturer and system supplier.
- Component suppliers develop components mostly as an SEooC because they supply to several customers with different applications and the components need to have state-of-the-art safety functions.

Figure 4 shows an example of how safety is implemented in automotive systems today.
Enabling Functional Safety with Semper Flash

What is Functional Safety?

Figure 4  Safety Implementation in Automotive Systems
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

3 Cypress Functional Safety for Semper NOR Flash Memories

3.1 Safety Process

Cypress is following an extended ISO/TS 16949 process for hardware development and extended Automotive Software Process Improvement and Capability Determination (SPICE) for software development process. Now, the development process has been extended to fulfill ISO 26262 requirements. Figure 5 shows the Cypress Semper flash device development flow with functional-safety-related tasks.

![Figure 5] Cypress Hardware Development Flow with Functional Safety Tasks

3.2 Safety Design

Cypress NOR flash devices play a significant role in several automotive applications such as advanced driver assistance system (ADAS), power train, instrument cluster, infotainment, gateway, keyless entry, and event data recorders. Some of these applications use external NOR flash devices as part of system-level safety functions that require safety mechanisms to be implemented in the NOR flash itself. Cypress ASIL B-compliant Semper flash devices encapsulate safety solutions into the device in alignment to ISO 26262 definition. The following section describes the functional-safety-related mechanisms and features in HS-T and HL-T NOR flash devices. See the relevant datasheet for details on the features.

<table>
<thead>
<tr>
<th>Safety Type</th>
<th>Safety Item</th>
<th>KL/SS12S</th>
<th>KL/SS256S</th>
<th>KL/SS128S</th>
<th>HyperFlash 1.8/3V</th>
<th>FS512S</th>
<th>FS256S</th>
<th>FS128S</th>
<th>FL512S</th>
<th>FL256S</th>
<th>FL128S</th>
<th>SPI 1.8V</th>
<th>SPI 3V</th>
<th>Semper Flash HS-T, HL-T, 1.8/3V</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262</td>
<td>ISO 26262-compliant development process</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Safety plan and elements added</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Safety documents availability | FMedA                  |          |           | FMedA for 512 Mb | None              | All | SEooC, HWSRS, FMedA, DFA,
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

<table>
<thead>
<tr>
<th>Safety Type</th>
<th>Safety Item</th>
<th>KL/S512S</th>
<th>KL/S256S</th>
<th>KL/S128S</th>
<th>HyperFlash 1.8/3V</th>
<th>FS512S</th>
<th>FS256S</th>
<th>FS128S</th>
<th>FL512S</th>
<th>FL256S</th>
<th>FL128S</th>
<th>Semper Flash HS-T, HL-T 1.8/3V</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Mechanism</td>
<td>Error- Correcting Code (SEC/DED)</td>
<td>Yes</td>
<td>SEC only</td>
<td>SEC only</td>
<td>Yes</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface CRC</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes (x8 Only)</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Integrity Check</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety-Added Feature</td>
<td>SafeBoot – Boot Failure Recovery</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EnduraFlex™</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Longer retention or higher endurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced Sector Protection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Sector protection scheme</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>JEDEC SPI Reset method</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Reset on regular SPI ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sector erase failure check</td>
<td>Yes</td>
<td>Yes for 512 Mb</td>
<td>No</td>
<td>Yes</td>
<td>Erase Power Loss Indicator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2.1 Error Correcting Code (Error Detection and Correction)

Memories can face soft errors or hard errors. Hard errors are permanent once they manifest, caused by defects in the silicon, disturbed bit, or metallization of the package because of aging, vibration, or environment stress. Soft errors are caused by charged particles, radiation, or cosmic rays. When a flash memory cell is affected with such errors, the read data will be corrupted and might affect the application functionality.

Figure 6 Operation with Non ECC NOR Flash Devices
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

- Cypress Semper flash devices support error detection and correction by generating an embedded error correction (ECC) code during memory array programming. This ECC code is then used for error detection and correction during read.
- The ECC feature can correct 1-bit errors and detect 2-bit errors: Single Error Correction (SEC) and Double Error Detection (DED).
- ECC errors are reported to the system by enabling an interrupt (x8 devices) or by collecting the error information to be read by the system MCU. The error information includes the following:
  - ECC Data Unit Status provides the status of 1-bit or 2-bit errors in data units
  - ECC Status register provides the status of 1-bit or 2-bit errors since the last ECC clear or reset
  - Address Trap register captures the address of the first ECC error encountered during a memory array read
  - An Error Detection counter keeps a tally of the number of 1-bit or 2-bit errors that have occurred in data units during reads
  - The Interrupt (INT#) output can be enabled in x8 devices to indicate when either a 1-bit or 2-bit error is detected as data is read
  - In HyperBus™ interface, a mode may be enabled to cause the Data Strobe (DS) to stop toggling (stall) when reading a half-page containing a 2-bit error

Figure 7 shows how Semper Flash with ECC provides the solution for the errors and increases the functional safety of the automotive applications.

![Figure 7](image_url)

**Figure 7** Operation with ECC NOR Flash Devices

### 3.2.2 Interface CRC (Cyclic Redundancy Check)

Semper flash devices are high-speed memories. The signals between the host and the flash device are running up to 200 MHz double-data-rate speed. The raw data might be corrupted because of a noisy channel or errors introduced by the transmitter, receiver, or both. Therefore, to keep the automotive system running safely and securely, one of the most critical aspects of communication between a host and a slave device is ensuring the integrity of the information transferred.

1 The Interface CRC feature is supported on the Semper Flash with Octal and HyperBus Interfaces.
x8 Semper flash devices have an Interface CRC, which is an error-detecting code commonly used in devices to detect accidental changes in raw data.

- A CRC-enabled slave device calculates a fixed-length binary sequence, known as the CRC checksum, for each block of data. The host device reads the CRC checksum from the slave device using the Read Interface CRC register. The slave device includes the Read Interface CRC command and address as part of the CRC checksum and then places the checksum data on the I/O bus. If the host device, upon receiving the slave’s CRC checksum, finds a mismatch with its own calculated CRC checksum, it can reissue the Write instruction sequence to the slave device to receive the data again.

**Note:** Rewriting is not trivial and may not help in noisy channels. However, detecting the problem allows the system to respond safely.

- Cypress Semper Flash devices use the following 32-bit polynomial (CRC-32C) to generate a CRC checksum.

\[ X^{32} + X^{28} + X^{27} + X^{26} + X^{25} + X^{23} + X^{22} + X^{20} + X^{19} + X^{18} + X^{14} + X^{13} + X^{11} + X^{10} + X^8 + X^6 + 1 \]
3.2.3 Data Integrity Check

Soft or hard errors can cause upsets within the NOR flash memory that can violate the system functional safety.

---

**Figure 10** Operation Without Data Integrity Check Feature

- The transaction sequence of the data integrity check in Semper devices causes the device to perform a CRC calculation over a user-defined address range. The CRC process calculates the check value on the data contained at the starting address through the ending address. It uses the same 32-bit polynomial as the interface CRC.
- The CRC calculation can be initiated only when the device is in standby mode and no flash memory embedded operation is suspended. When the CRC calculation is completed, the device returns to standby mode and the calculated check value is available in the CRC register. The CRC register contains the check value bits 0–31 and can be read using the Read Any Register transaction.
- The host can periodically check the particular address range and update the flash device if CRC checksum values do not match as shown in **Figure 11**.

---

**Figure 11** Operation with Data Integrity Check Feature

```c
if (MCU Array CRC Checksum == Memory Array CRC Checksum)
{
    Array data is correct;
    No Action;
}
else if
{
    Send data block again to Flash;
}
```
### 3.2.4 SafeBoot - Bootup (Initialization) Failure Recovery

Most of the automotive applications use NOR flash devices to store code and boot up using NOR flash devices. If the NOR flash device itself does not boot up correctly and the system does not have any indication about the next step, the automotive application may not initialize correctly.

![Diagram: Operation without SafeBoot Feature](image1)

**Figure 12**  Operation without SafeBoot Feature

The NOR flash device will stay in the busy state or report a boot failure through the status register. The host should access the Status Register 1 polling sequence to determine if a flash initialization failure has occurred in the device. The Status Register 1 should show 0x61 as a failure signature.

![Diagram: Boot Failure Detection](image2)

**Figure 13**  Boot Failure Detection

### 3.2.5 SafeBoot – Detecting Corruption of Configuration

If during a Write Status/Configuration Register or Write Any Register transaction sequence to nonvolatile configuration registers, a brownout or a hardware reset occurs, the transactions are interrupted, and the device returns to the standby mode within 300 µs. However, it means that the nonvolatile configuration data used to configure the device is most likely corrupted.
The device can detect a corrupted configuration and enter the default mode where the device can be accessed. The host must go through a Status Register polling sequence to determine whether a configuration corruption has occurred in the device. The device provides a configuration corruption signature (0x41) in its Status Register 1, which the host can detect to initiate reprogramming the nonvolatile configuration registers’ data.

### 3.2.6 EnduraFlex™

In recent years, larger density (512 Mb and higher) nonvolatile NOR flash devices have become a popular choice in embedded systems to accommodate not only boot code storage but also storage data. As a result, the NOR flash devices can experience a shorter lifespan when writing to these devices with a very high frequency. Flash memory is subject to physical degradation that can eventually lead to device failure. Flash memory degrades faster at higher temperatures, with more number of program/erase cycles, and short interval between program/erase cycles. Some automotive applications need high endurance and high retention in the flash devices; a flash device with a lower data retention or endurance may affect system functionality.
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

Figure 16  Flash with Typical Data Integrity Specification

The EnduraFlex feature in Cypress Semper flash makes these devices safer and reduce the FIT rate when used in safety applications. This feature provides an option to select multiple partitions to provide high endurance (more than 1.28 million cycles for 512 Mb device) or long data retention (25 years).

Figure 17  Semper Flash with Improved Data Integrity Specification

3.2.7 Advanced Sector Protection

Many automotive applications perform program or erase operations on particular flash device sectors. To perform such operations, the host sends the respective transaction with command and address/data. If the bits in transaction, sent by the host change because of a noisy channel or random failure, the flash device may perform the operation on unwanted sectors, which can fail the system operation.
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

Figure 18  Operation with Unprotected NOR Flash

Cypress Semper flash devices offer the Advanced Sector Protection (ASP) feature that provides a set of independent hardware and software methods to disable or enable programming or erase operations, individually, in any or all sectors. The sectors with ASP will be protected from program and erase operations.

Figure 19  Operation with Protected NOR Flash

3.2.8  JEDEC SPI Reset Method

In situations when the flash device stops responding to the host/system unexpectedly, the JEDEC SPI Reset feature in Cypress Semper flash devices can initiate an SPI flash hardware reset, independent of the device's operating mode, using existing SPI signals: Chip Select (CS#), Serial Clock (CK), and Serial Input (SI/DQ0).

This reset sequence is not intended to be used at normal power ON, but to be used only when the device is not responding to the system. This reset sequence will be operational from any state that the device may be in.
Enabling Functional Safety with Semper Flash

Cypress Functional Safety for Semper NOR Flash Memories

3.2.9 Sector Erase Count

In normal flash devices, if a power failure occurs when the system is performing the sector erase operation on the flash device the system remains unaware of the status of the respective sector erase operation.

![Diagram of sector erase operation without power loss logic]

**Figure 20** Erase Operation without Power Loss Logic

In such situations, Semper flash devices have a Sector Erase Count Register, which stores logical counter for each sector. The logical counter stores the number of erase cycles performed by a host for every logically addressed sector. The counter is accessible through the Sector Erase Count transaction with an address differentiation.

The Sector erase count register bits [22:0] denote the erase count number with a maximum count of 8 million cycles. The register bit 23 is a flag to indicate that the register has been reset to ‘0’ because there was a power loss during an erase operation of the sector and the register may have been corrupted. The MCU reads the bit 23 of the register to verify the erase transaction status.

See **Figure 21**. Sector erase count register bits [22:0] increment properly until Step 3 because of the successful sector erase operation. When a power loss during sector erase operation in step 4, SEC register counter bits [22:0] reset to ‘0’ and bit [23] flag indicates power loss during sector erase operation. This flag is reset when sector erase operation is successful; the counter starts again incrementing accurately as shown in Step 5.

![Diagram of erase operation with power loss logic]

**Figure 21** Erase Operation with Power Loss Logic
3.3 External Flash Use Cases and Functional Safety Evaluation

Safety requirements for an external flash depend on the use case of the external flash. Cypress functional safety team has analyzed the following important use cases for external flash memory devices and tabulated respective ASIL grades for these use cases.

Table 5 External Flash Use Cases and ASIL Grades

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
<th>ASIL Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store and Download (SnD)</td>
<td>The flash content is copied at startup into the local RAM and being executed without using the flash anymore.</td>
<td>ASIL B, ASIL D ready</td>
</tr>
<tr>
<td>Data/image read during operation in cluster applications</td>
<td>The cluster MCU reads image-related data from flash during safety operation</td>
<td>ASIL B, ASIL D ready</td>
</tr>
<tr>
<td>Execution from external flash</td>
<td>Safety applications execute directly from the external flash during runtime.</td>
<td>Quality Managed</td>
</tr>
</tbody>
</table>

3.4 Safety Deliverables

The Product Safety Manager (PSM) works with the product development team and creates required functional safety documents during the project life cycle as shown in the Safety Process section. Cypress offers the functional safety documents to qualified customers upon request.

Please contact your local Cypress sales representative or create a support case to obtain the functional safety documents for Semper flash devices.
4  **Summary**

- Automotive applications need functional safety because of increasing dependency on electronic components and driver safety.
- Automotive industry is extensively accepting ISO 26262 compliance.
- Functional safety mechanisms and added features mentioned in the **Safety Design** section make Cypress’ Semper flash devices robust and reliable product in today’s automotive and industrial systems.
- Cypress understands the requirement of functional safety in the products and is committed to design next-generation automotive NOR flash devices that is in compliance with ISO 26262 and IATF16949.
## Revision history

<table>
<thead>
<tr>
<th>Document version</th>
<th>Date of release</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>**</td>
<td>2018-04-26</td>
<td>New Application Note</td>
</tr>
<tr>
<td>*A</td>
<td>2019-05-02</td>
<td>Minor Updates</td>
</tr>
<tr>
<td>*B</td>
<td>2021-02-25</td>
<td>Migrated to Infineon template</td>
</tr>
</tbody>
</table>
IMPORTANT NOTICE
The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

WARNINGS
Due to technical requirements 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 Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.