Semper™ Flash: Enabling Functional Safety For Automotive and Industrial Systems

Sandeep Krishnegowda and Pritesh Mandaliya

Introduction

The focus on safety for critical applications in both automotive and industrial markets is significantly increasing as applications depend on more electronic systems to solve real-time, complex problems. Failure of these mission-critical systems is not an option and must be avoided at all costs. In the automotive industry, the ISO 26262 safety standard sets the requirements for designing safe automotive systems and the IEC 61508 safety standards specify the requirements for industrial control systems. This whitepaper provides an overview of the various safety features integrated into Cypress' Semper NOR Flash solutions that simplify system-level functional safety design in alignment with the ISO 26262 and IEC 61508 standards.

What is Functional Safety?

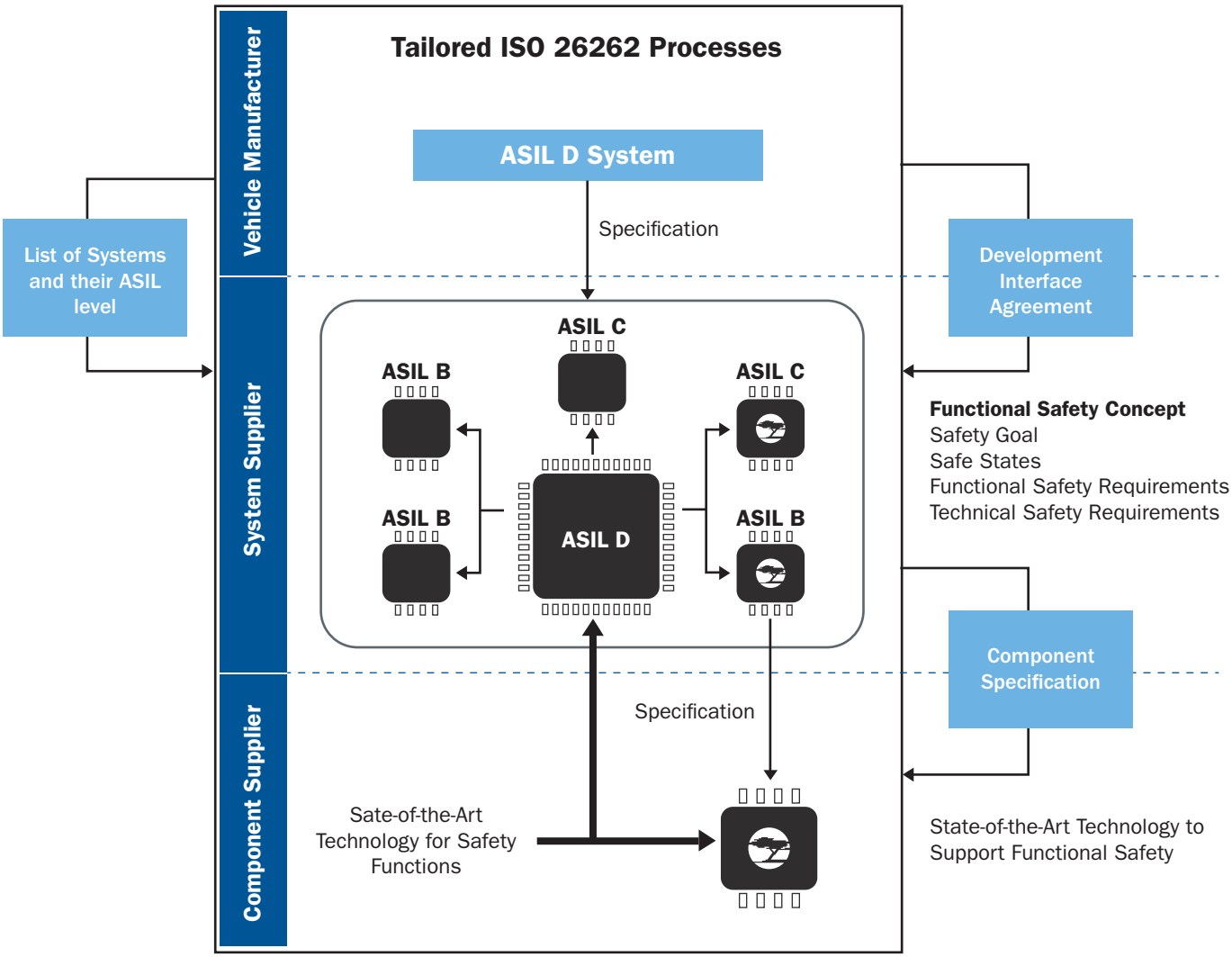
ISO 26262 defines functional safety as "The absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems." In electronic systems, the cause of failures leading to system malfunctions can be systematic faults in design or random faults due to soft error or probabilistic reliability failures over time. Functional safety ISO 26262 and IEC 61508 standards define safety integrity levels (e.g ASIL A to ASIL D for automotive and SIL 1 to SIL 4 for industrial systems) with each level denoting more stringent safety levels and less likelihood of failures, as shown in Table 1. Meanwhile, Figure 1 shows an example of how safety is implemented in automotive systems today, and the safety process that is followed by vehicle manufacturers, system suppliers, and component suppliers.

Table 1. Proposed Safety Integrity Levels

Industrial Standard (IEC 61508)	
Integrity Level	Random Failure Rate
SIL 4	$\geq 10^{-9}$ to $<10^{-8}$
SIL 3	$\geq 10^{-8}$ to $<10^{-7}$
SIL 2	$\geq 10^{-7}$ to $<10^{-6}$
SIL 1	$\geq 10^{-6}$ to $<10^{-5}$

Automotive Standard (ISO 26262)	
Integrity Level	Random Failure Rate
ASIL D	$<10^{-8}$
ASIL C	$<10^{-7}$
ASIL B	$<10^{-7}$

Figure 1. Safety Implementation in Automotive Systems



Semper NOR Flash ISO 26262 ASIL B Functional Safety Compliance

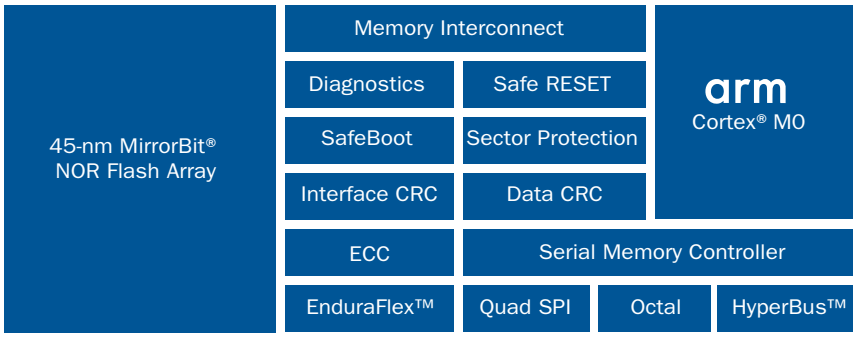
Automotive applications use external NOR Flash memories in safety-critical applications such as ADAS, for storing critical code, data, and graphic images that must be read at system power-up or during operation. Safety requirements for these external flash memory solutions depend on the different use cases in safety-critical applications.

Here are four different usage examples of an external flash memory:

1. Store and Download (SnD): The flash content is copied during start-up into the local RAM and is executed without accessing the flash.
2. EEPROM emulation: The flash is used to store safety-critical data.
3. Continuous read during run time: The host reads data from the flash during safety-critical operation.
4. Code execution: The safety-critical application executes directly from the external flash during operation.

The Semper NOR Flash family is architected and designed to meet the automotive industry's ISO 26262 functional safety standard for building failsafe embedded systems (See Figure 2). The family is AEC-Q100 automotive-qualified, ASIL B functional safety compliant, and provides superior endurance (1+ million cycles) and 25 years of data retention at extreme temperatures (-40°C to +125°C) common in automotive and industrial applications.

Figure 2: Semper NOR Flash Architecture Diagram



Key Functional Safety Features of Semper Flash

1. Error Correction Code (ECC)

Memories may encounter soft errors or hard errors. Hard errors are permanent once they manifest. They are caused by defects in the silicon, a disturbed bit, or metallization of the package because of aging, vibration, or environmental 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 impact the application's functionality. Semper NOR Flash devices support Single Error Correction and Double Error Detection (SECDED) by generating an embedded ECC during memory array programming. This ECC is then used for error detection and correction during read operations.

2. Data CRC

Data CRC in Semper flash devices performs a Cyclic Redundancy Check (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 to detect any faults during system boot or per user command.

3. Interface CRC

Semper NOR Flash devices are high-frequency memories supporting 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 system running safely, one of the most-critical aspects of communication between a host and a slave device is ensuring the integrity of the information transferred. Semper NOR Flash x8 interface devices have an Interface CRC, which is an error-detecting code used in devices to detect accidental faults during data transmission between the host and memory.

4. SafeBoot – Bootup Failure Recovery

Most automotive and industrial applications use NOR Flash devices to store code used during boot up. If the NOR Flash device itself does not boot up correctly, then the respective application may not initialize correctly, or in case of boot failure, the Semper NOR Flash device will stay in the busy state or report a boot failure through the status register.

5. Configuration Data Corruption

A power brownout or a hardware reset occurring during the update of the nonvolatile configuration registers means that the nonvolatile configuration data used to configure the device may get corrupted. The Semper NOR Flash device can detect a corrupted configuration and enter a default mode where the device can be accessed.

6. EnduraFlex™ Architecture

All flash memory is subject to physical degradation that can eventually lead to device failure. Some automotive applications need high endurance and high retention in flash devices, and lower data retention or endurance may affect the system functionality. Cypress' EnduraFlex™ architecture optimizes system design by enabling a Semper Flash device to be divided into multiple partitions, independently configured for either high endurance or long retention. For frequent data writes, a partition can be configured to deliver up to 1.28 million program-erase cycles for 512 Mb density parts and 2.56 million cycles for 1 Gb parts. For code and configuration storage, a partition can be configured to retain data for 25 years.

7. Advanced Sector Protection (ASP)

If the bits in an Program/Erase transaction sent by the host change because of a noisy channel or random failure, the flash device may perform the operation on the incorrect sectors, which can cause system operation failure. Semper NOR Flash devices offer the Advanced Sector Protection (ASP) feature, which protects any sectors from inadvertent program and erase operations.

8. Sector Erase Power Loss Detection

In normal flash devices, if a power failure occurs when the system is performing a sector erase operation, the system remains unaware of the status of the respective sector erase operation. Semper NOR Flash devices implement an erase power loss indicator for every sector to flag brownout events during sector erase.

9. Safe Reset

In situations when the flash device stops responding to the host/system, the Safe Reset feature in Cypress Semper Flash devices can initiate an SPI flash hardware reset, independent of the device's operating state using existing SPI signals: Chip Select (CS#), Serial Clock (CK), and Serial Input (SI/DQ0). This feature provides a hardware reset mechanism for any package type, including 8-pin packages.

10. Diagnostic Features

Semper NOR Flash supports the following diagnostic features which provide critical embedded operation status to the system.

- Programming error status flag reports program operation failure
- Program operation suspend status flag is used to indicate if the program operation is suspended
- Erasing error status flag reports erase operation failure. It indicates that there was an error in the last erasing operation.
- Sector erase success/failure status flag indicates whether the erase operation on the sector completed successfully
- Erase operation suspend status flag is used to indicate if the erase operation is suspended
- Memory array data crc suspend status flag is used to determine when the device is in memory array data crc suspend mode
- Memory array data crc abort status flag indicates that the memory array data crc operation was aborted
- Device ready/busy status flag indicates whether the device is performing an embedded operation, failure case, or standby mode ready to receive new transactions

Cypress Automotive Functional Safety Assurance Program

Cypress has been associated with automotive functional safety for more than 15 years and is one of the industry's leading providers of functionally safe automotive products (MCU, analog PMIC, memory, and software). Cypress is a key component supplier in the functional safety space. The relationships between the various suppliers in this industry are managed through Development Interface Agreements (DIA), which ensure that the safety standards are integrated from the beginning of the development process. Cypress has a group of experts responsible for defining and maintaining these standards from the beginning to the end of a project. These experts ensure that our products fulfill the ISO 26262 safety standards. They review and analyze the product features and customer feedback to make sure the products are compliant to safety standards and required grade level, and that Cypress is always ahead of the curve with its technology.

Cypress' business processes also have the backing of a dedicated and independent functional safety review board confirming execution of deliverables that are developed during the design process. Cypress' software QA department ensures the compliance of any deliverables during the software development process. The automotive software development process has been certified by TÜV SÜD to ensure ISO 26262 compliance.

Functional Safety Documentation

Cypress offers several ISO 26262-compliant functional safety documents to qualified customers upon request. Contact your local Cypress sales representative or create a support case to obtain the following functional safety documents for Semper NOR Flash devices:

- Device Safety Manual
  - Product safety architecture and assumed usage
- Safety Analysis Report Overview
  - Summary of FIT rate and FMEDA results
- Detailed Safety Analysis Report
  - Full safety analysis down to block level, safety mechanisms, and diagnostic coverage

Conclusion

- Automotive applications need functional safety because of increased dependency on electronic components and to ensure driver safety.
- The automotive industry is extensively adopting ISO 26262 compliance.
- Functional safety mechanisms and added features mentioned in the safety design section make Cypress' Semper NOR Flash devices robust and reliable for today's automotive and industrial systems.
- Cypress understands the requirement for functional safety in its products and is committed to designing next-generation automotive NOR Flash devices that are compliant with ISO 26262 and other key industry standards.

Read more about functional safety features of the Semper NOR Flash family at: http://www.cypress.com/semper.

Cypress Semiconductor Corporation
198 Champion Court, San Jose CA 95134
phone +1 408.943.2600 fax +1 408.943.6848
toll free +1 800.858.1810 (U.S. only) Press "1" to reach your local sales representative

© 2018 Cypress Semiconductor Corporation. All rights reserved. All other trademarks are the property of their respective owners.
002-23929 **