freescale.com

White Paper

Safety-Integrated Hardware Solutions to Support ASIL-D Applications

Contributors:

Valerie Bernon-Enjalbert
Mathieu Blazy-Winning
Regis Gubian
David Lopez
Jean-Philippe Meunier
Mark O'Donnell

Abstract

Real-time control of safety-critical applications has been a longtime challenge for engineers. Application functions are becoming more complex and industry standards require more sophisticated functional safety concepts in both the automotive and industrial markets. Assessing functional safety of a system requires a significant level of engagement and verification. Freescale introduced its SafeAssure program to help system manufacturers simplify this assessment to more easily achieve compliance with International Standards Organization (ISO) standards. This white paper covers the implementation of various safety architectures, the details behind an innovative integrated safety solution that simplifies system-level functional safety design and alignment with the ISO 26262 standard.

Table of Contents

Introduction

In automotive applications, interactions between the human body and electrical/electronic systems are increasing significantly, specifically when managing safety-critical decisions that can have a severe impact on a driver's health. As the evolution of these advanced safety systems moves from passive to more active, including predictive safety and even autonomous vehicle concepts, the automotive industry has and will continue to demand that strict requirements be met.

Managing these safety-critical decisions is trending toward increased complexity and additional software content in safety systems. With greater complexity, there are increasing risks of systematic and/or random hardware failures. To help ensure the highest safety standards and influence the development of safe automotive systems, the industry has released the latest automotive safety standard: ISO 26262.

This paper addresses the implementation of various safety architectures and introduces an innovative, integrated safety solution that simplifies system-level functional safety design, including alignment with the ISO 26262 standard.

What is Functional Safety?

By definition, Functional Safety means the absence of unreasonable risk due to hazards caused by the malfunction of systems. To significantly reduce the risk of malfunction, it is critical to understand and assess the type of failures that can occur. These failures can be classified in two categories:

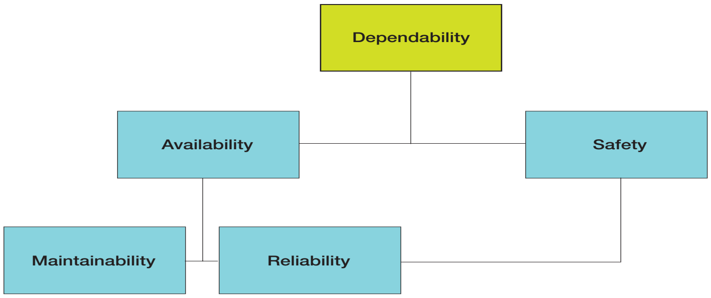
1. Systematic failures, which can be attributed to a certain cause, can only be eliminated by a change in the design during the manufacturing process, operational procedures, documentation or other relevant factors. The probability of a systematic failure occurring is reduced through a robust development process.
2. Random failures, which occur unpredictably during the lifetime of a hardware element, follow a probability distribution. Those failures could result from a permanent or transient occurrence of a perturbed environment or from the intrinsic technology's performance across the system's lifetime. Risk reduction linked to the random failure is covered by dedicated architectures and IC strategy.

The automotive industry released ISO 26262:2011(E) on November 15, 2011. This standard, specifically modified for “Road vehicles—Functional safety,” is an adaptation of the functional safety standard IEC 61508 for automotive electrical/electronic (E/E) systems.

To keep people on the road safe, applications must maintain functionality and be dependable. In order to be dependable, E/E systems must be designed with the optimal balance of safety and availability.

Availability is a fine balance of maintainability and reliability, while safety depends primarily on system reliability. This interaction is illustrated in the following diagram.

The Dependability Tradeoff for Functional Safety



Freescale SafeAssure products are designed to be dependable by effectively combining availability, safety and reliability.

Managing Safety Development: The SafeAssure Process

Assessing the functional safety of a system requires a significant level of engagement and verification. Simplifying this assessment is one of the main objectives of the Freescale SafeAssure program that was developed and launched in September, 2011. The program applies to both automotive and industrial applications.

SafeAssure products are designed to reduce the complexity of functional safety systems—a key objective of the manufacturers of these systems. The program was developed with a strong emphasis on failure modes and effects analysis (FMEA), continuous process improvement (CPI) and zero defects. The new product development (NPD) flow, tools and metrics have also been modified to incorporate and manage functional safety requirements. Specifically, the product definition phase now includes system-level assumptions as part of describing the system-level context. For semiconductor devices, these assumptions are made as a Safety Element out of Context (SEooC). Since MCUs and analog companion chips are developed as standard solutions to address multiple applications in multiple industries, the SEooC is a safety-related element that is not developed for a specific system or a particular vehicle platform.

Quantify the Residual Risk—Architectural Metrics

Architectural metrics are used to assess the IC performance in terms of safety-related failures. They are used to drive the choice of architecture (including detection and protection) and allow the user a selection of self-check mechanisms.

ISO 26262:2011(E) defines the safety target to be achieved based on the Automotive Safety Integrity Level (ASIL) of the original equipment manufacturer (OEM). The standard also provides a guide to evaluate the resulting metrics.

One of the methods of evaluation consists of individually examining the residual of each single-point fault and each dual-point failure that results in a violation of a specific safety requirement.

The evaluation must be applied iteratively during IC design. Several architectures with different levels of integration can be applied to achieve the desired level of system requirements.

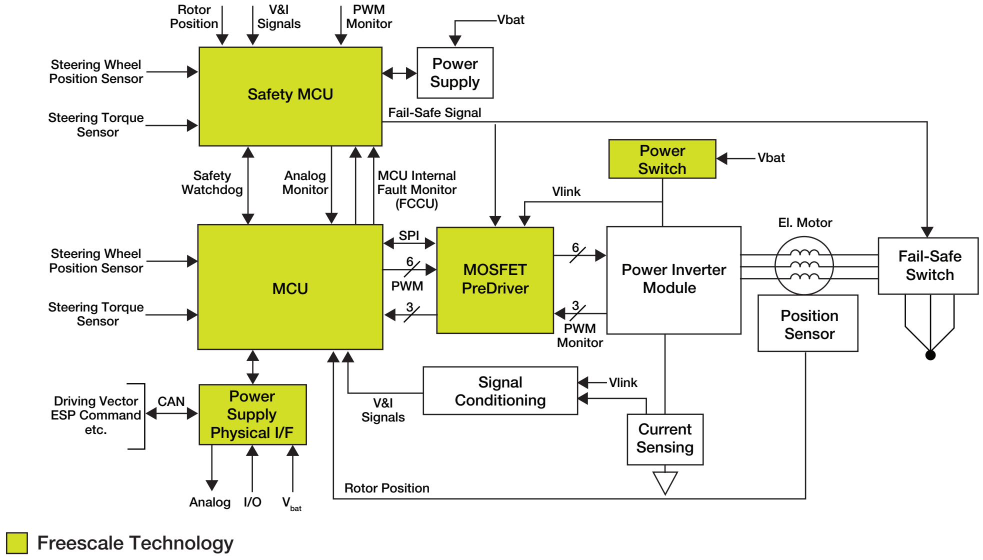
ASIL-D Solutions and the Influence of Safety Architecture

Electric power steering (EPS) is one of many automotive applications that requires a high level of safety to ensure a vehicle's steering system is predictive and deterministic.

Depending on the combination of hardware and software interaction used to meet ASIL-D requirements in a particular application, several approaches or system architectures are possible.

The first approach is to use two MCUs to conduct an external comparison of safety outputs.

EPS Based on a Single Core and a Safety MCU



The advantage of this architecture is the physical duplication of safety- and non-safety-related functions and features.

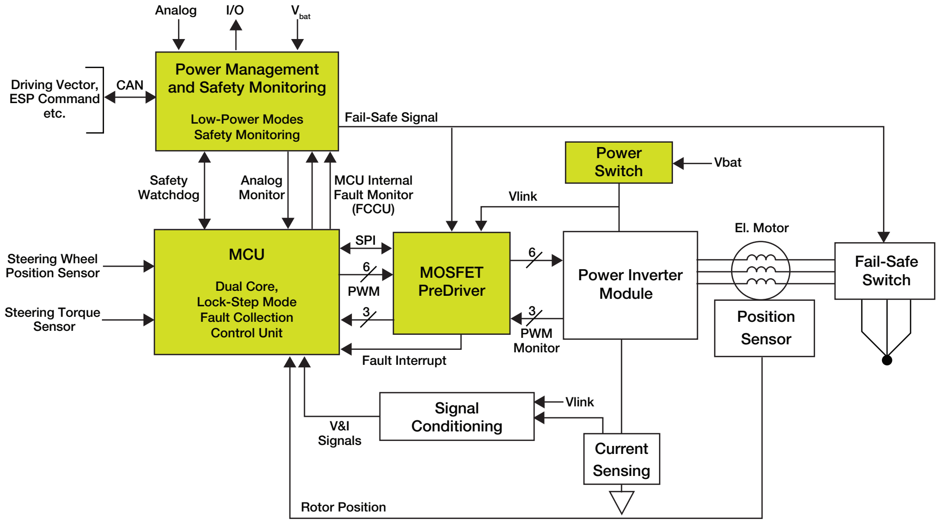
However, the high complexity of this configuration combined with software synchronization and increased PCB space create a major challenge and barrier for this approach. Because of the increased number of devices, the reliability and the availability of system function are reduced.

This configuration may introduce a transient fault such as a single event upset and does not facilitate having a good tolerance in this regard.

An alternative approach, developed by Freescale, uses the latest generation of multicore MCUs operating in lock-step mode. The design includes an internal self test combined with advanced analog power management solutions that monitors the MCU and controls the fail-safe system state.

The increased integration of the second approach reduces the size of the board and the complexity of the system. Using the lock-step mode and integrating the monitoring into the power supply device improves availability and allows a high level of safety. In addition, software development is less complex than in the first approach.

Freescale-Integrated Safety Architecture for an ASIL-D EPS System



🟨 Freescale Technology

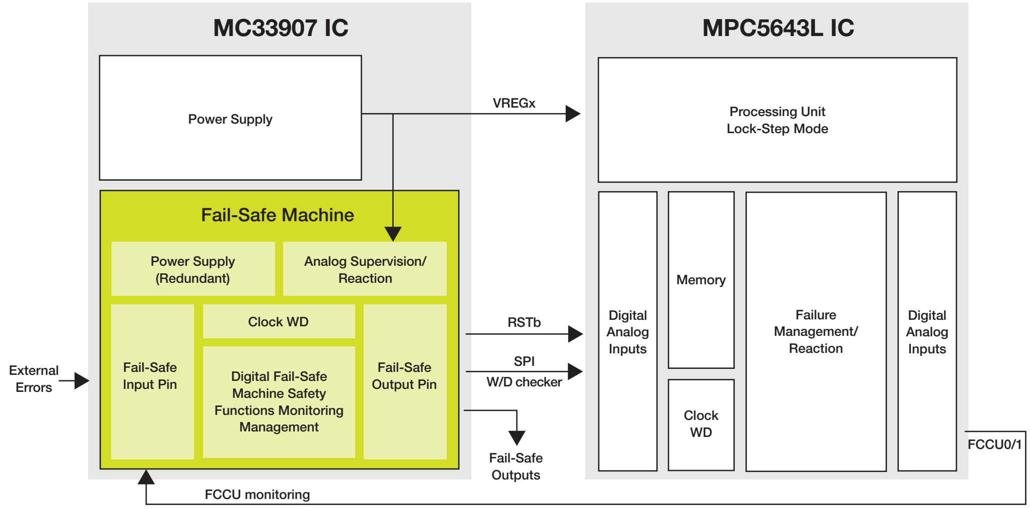
The Freescale hardware system concept for the next generation of functional safety comprises the MPC5643L and the MC33907, the latest generation of system basis chip (SBC) designed to meet the ISO 26262 standard safety requirements.

The MC33907 combines an energy management unit (EMU) based on an efficient DC/DC power supply that can be switched into a low-power mode. The main functions of the MC33907 are to supply and monitor the MPC5643L MCU. Its power management is associated with various safety mechanisms, developed in combination with the MC5643L, to avoid a malfunction in an application that results in a dreaded event. Using both devices in a system can reduce the effort needed to achieve an ASIL-D system-level solution.

The MPC5643L is a dual-core lock-step MCU with integrated safety architecture. Built-in self test (BIST) mechanisms are provided for the cores, memories, crossbars, communication blocks and peripherals. In addition, the device is optimized to prevent common cause failures induced by clock or voltage-supply issues. The MPC564xL family provides hardware blocks for detection of clock deviations as well as hardware monitors for main voltages such as internal core voltage and flash supply voltage. The dual-core MPC564xL replicates other key hardware blocks in addition to the cores. These include the crossbar, memory protection units, interrupt controller, DAM and a software watchdog timer. The main benefit of this sphere of replication is the capability of the MCU to detect single-point failures that tend to occur more frequently as soft errors, not only in the cores but also in key sub-modules.

The diagram below shows the MPC5643L and MC33907 with their cross-check mechanisms that help ensure system-level safety.

Freescale Functional Safety System Solution



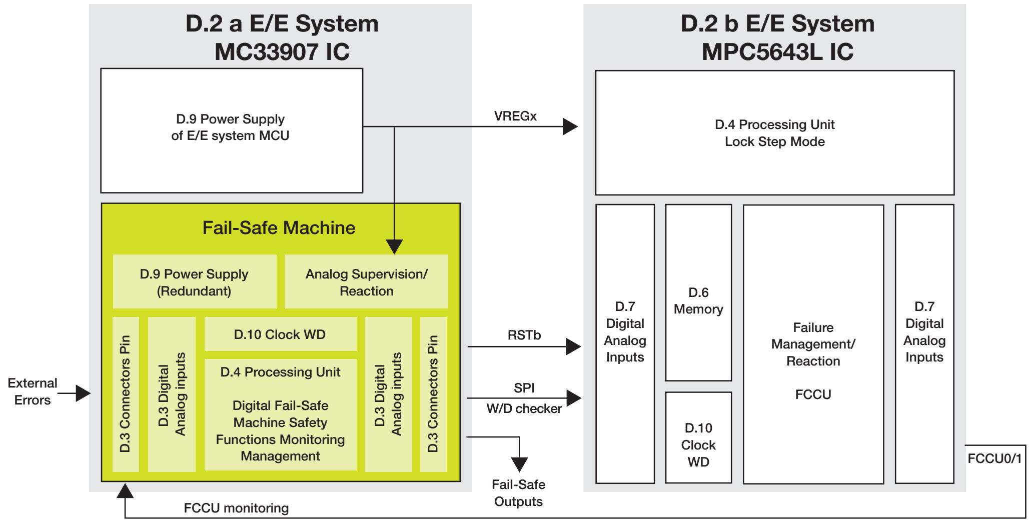
🟨 Independent, isolated, robust, fail-safe machine in the main IC

Freescale is committed to providing their customers hardware solutions that support the requirements described in Annex D of ISO 26262-5:2011(E).

The Freescale approach to functional safety fits the generic hardware of an embedded system defined in Annex D of ISO 26262-5:2011(E), where each component (MCU and analog) is developed as a safety element out of system context. The solution comprises a D.2b E/E system IC (the MPC5643L MCU) and a D.2a E/E system IC (the MC33907 MCU), which is the SBC analog solution (see figure below).

The specific semiconductor elements used in the two system ICs are referenced as D.1 to D.10 in the Annex D of ISO 26262-5:2011(E) (see figure below). This facilitates the decomposition of the elements and indicates the diagnostic coverage.

Functional Safety System Solution, Including ISO 26262 Annex D Measures



🟨 Independent, isolated, robust, fail-safe machine in the main IC

The following table provides a summary of:

- A list of hardware elements in the Freescale safety system
- The safety mechanism/measure implemented for each element
- The typical diagnostic coverage that is considered to be achievable for each safety mechanism/measure, as defined by the Annex D of ISO 26262-5:2011(E)

Combined values of MC33907 and MPC5643L to meet ASILD requirements

Element	SAFETY Mechanism/Measure	Typical Diagnostic Coverage Considered Achievable	Notes for Freescale Hardware Solution	
D.3 Connector—Pin	Failure detection by online monitoring	High	√	Short-circuit detection
D.4 Processing Unit	Hardware redundancy	High	√	Dual-core lock step
D.5 ROM	Memory monitoring using error-detection-correction codes	High	√	Integrity check and ECC
D.6 RAM	Memory monitoring using error-detection-correction codes	High	√	BIST and ECC
D.7 Analog and Digital I/O	Test patterns	High	√	BIST, error-injection check
	Monitored output	High	√	Short-circuit detection (includes physical layers)
D.8 Communication Bus	Combination of information redundancy, frame counter and timeout monitoring	High	√	SPI-protocol checker
D.9 Power Supply	Voltage control (output)	High	√	Undervoltage (UV) and overvoltage (OV) detection on outputs
D.10 Program Sequence Monitoring/Clock	Combination of temporal and logical monitoring of program sequences with time dependency	High	√	Integrated watchdog

This table is a summary of implementations of the ISO 26262 standard: Integrated hardware architectures satisfy the ASIL-D level of requirements through high diagnostic coverage intended to significantly reduce the probability of a dangerous failure and use deterministic behavior for each failure condition.

Source: In reference to Annex D of ISO 26262-5:2011(E) and Freescale hardware solutions (MPC5643L and MC33907).

The combination of the SafeAssure MCU and analog system basis chip, designed as an SEooC, facilitates the assessment of the safety of a system. These devices are developed to support the ISO 26262 standard requirements and provide a scalable approach to simplify development of systems that need to comply with functional safety standards. The optimal interaction between each element makes the system simpler and stronger. Moreover, this architecture enables the number of components at the system level to be reduced, addresses the functional safety requirements and increases reliability.

Inside the MC33907, the power-management unit and the fail-safe machine combine to interact with the MCU. Four safety measures are implemented to secure the interaction between the MCU and SBC uninterrupted supply, fail-safe inputs to monitor critical signals, fail-safe outputs to drive a fail-safe state and watchdog for advanced clock monitoring. When combined with the MPC5643L MCU, each safety measure is optimized for the highest level of safety performance.

During the development of the components, a complete failure modes, effects and diagnostics analysis (FMEDA) was developed to measure the safety performances in terms of single point of failure, latent failure and common cause failures (CCF). This type of safety analysis is part of the support deliverables for the SafeAssure products and is the result of a mixed-device failure mode analysis to determine system safety. Device architectures have been implemented with the specific goal of reducing FMEDA risks.

As an example, the reduction of CCF is addressed by segregating the main function (supply and communication) and the fail-safe machine (a group of independent safety features, such as monitoring, detection, and safe-state control). This specific measure has been implemented to reduce the CCF and, combined with analog and digital BIST, contributes to reduce latent failures.

At the system level, safety-check mechanisms proposed by the MPC5643L can be monitored by the MC33907 through the bi-stable protocol of the fault collection control unit (FCCU). This IC cross-checking, like the challenger for monitoring timing, provides external measurement of the system and offers a redundancy to further secure fault detection.

In line with safety architecture of the system basis chip family, a redundant path for safety-state activation occurs through dedicated fail-safe outputs. These outputs complement the MCU fail-safe outputs by setting the application into a deterministic state when a failure condition occurs.

These hardware implementations help software engineers simplify the software architecture and implement a software-development strategy that focuses on safety using a single MCU approach.

Finally, detailed documentation is provided that describes functional safety, the safety goals and the safety implementation of each component, thus enabling the use of standard semiconductor devices for the management of various safety applications.

Conclusion

The new ISO 26262 standard for implementing safety-relevant features at the silicon level is in its infancy from both a measures and an architectural perspective. The right tradeoff between redundancy and simplicity is the key to developing cost-effective, safe solutions.

It is possible to achieve ASIL-D level status using various types of architectures, but for now the proper implementation of an MCU and an SBC makes the system simpler, faster, more reliable and cost-effective. The combination of the MC33907 SBC and MPC5643L MCU allows designers to more easily add functional safety to critical systems by incorporating our SafeAssure process into hardware, software and support. This combination of devices along with comprehensive documentation (such as the FMEDA and safety manual) is designed to simplify hardware architecture and reduce the time to market for any ISO 26262 application. Please see application note, **“Integrating the MPC5643L and MC33907/08 for Safety Applications”**.

Our unique approach is designed to simplify functional safety, reduce the risk and decrease costs in the developmental process. Anticipating the risk and reducing the impact of potential failures early in the development process—before production—contributes to an improvement in the safety of drivers and passengers, as well as reduces the cost of quality to manufacturers.

freescale.com

Support

Visit **freescale.com/support** for a list of phone numbers within your region.

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document.

Freescale reserves the right to make changes without further notice to any products herein. Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at: **freescale.com/SalesTermsandConditions**.

For more information, please visit freescale.com

Freescale and the Freescale logo are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. SafeAssure and the SafeAssure logo are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2013 Freescale Semiconductor, Inc.