Safety-integrated hardware solutions

In automotive and industrial applications, interactions between the human body and electrical/electronic systems are increasing significantly. Specifically when managing safety-critical decisions this can have a severe impact on a people's health.

As the evolution of advanced safety systems moves from passive to more active, including predictive safety and even autonomous vehicle concepts, the 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. 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 NXP Safe Assure program which applies to both automotive and industrial applications.

Safe Assure 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.

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. 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 functions 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 NXP, 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.

The NXP hardware system concept for the next generation of functional safety comprises the MPC5744P and the MC33907, the latest generation of system basis chip (SBC) designed to meet the ISO 26262 standard safety requirements. MC33907 and MC33908 system basis chips have received ▷

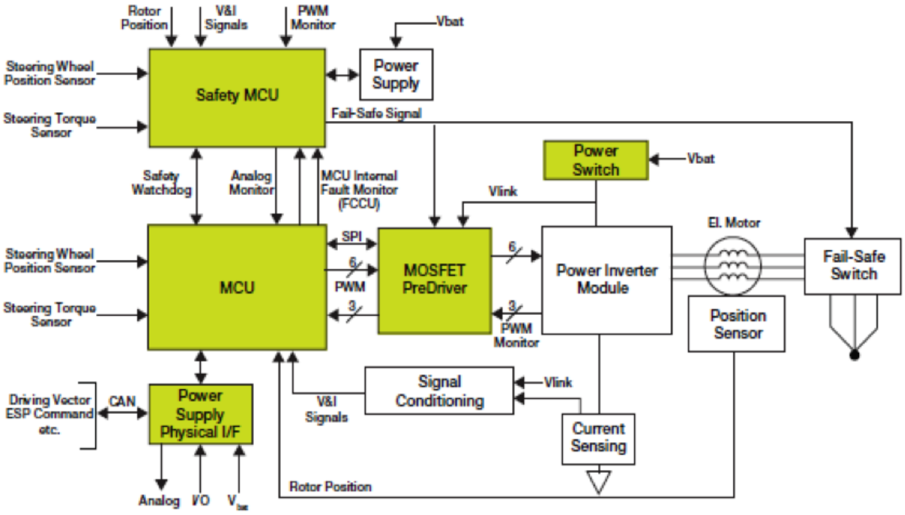

Figure 1: EPS Based on a Single Core and a Safety MCU (Photo: NXP)

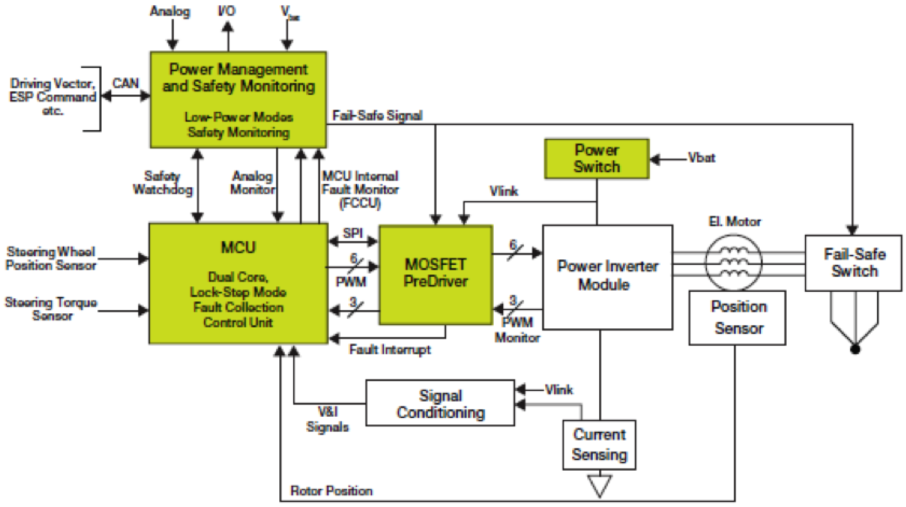

Figure 2: NXP-integrated Safety Architecture for an ASIL-D EPS System (Photo: NXP)

ISO 26262 functional safety assessments up to the ASIL-D level from one of the world's foremost automotive safety assessment organizations. The assessment was conducted by TÜV SÜD, an independent and renowned functional safety accredited appraiser, which assessed the NXP products up to the most stringent automotive safety integrity classification.

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 MPC5744P MCU. Its power management is associated with various safety mechanisms, developed in combination with the MC5744P, 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. Communication with other parts of the system (car, truck, industrial machines) is managed through the available CAN and LIN transceivers integrated in the MC33907.

The MPC5744P 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 MPC574xP 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 MPC5744P 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.

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 MPC5744P 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 Safe Assure 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 MPC5744P 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. ◀

Author

David Lopez
Yves Legrand
NXP Semiconductors
www.nxp.com