Safety and Power Architectures that Enable Autonomous Driving Embedded Systems

The electrification of the car and the transformation to autonomous driving will lower emissions, reduce traffic congestion and other hazards. This will be made possible by Advanced Drivers Assistance Systems (ADAS) that act on safety applications to control steering, braking and transmission without taking inappropriate actions.

To manage the risk of operations, the development of these systems follows the highest ISO 26262 [1] Automotive Safety Integrity Level (ASIL D) to guarantee a safe state activation when a safety goal is violated.

All safety electronic systems require a safety microcontroller and a reliable, safe source of power management connected to the car battery: this is the System Basis Chip (SBC). Safety microcontrollers and safety system basis chips are the backbone of embedded system architectures that includes independent hardware monitoring.

This article highlights the latest functional safety innovations at the power management level (SBC), from the development phase to system design, and underscores the link to reliability and how to enable hardware that is safety ready. It will also demonstrate how an architecture developed for ASIL D can help improve the functional robustness of an embedded system with a destructive test performed on the Integrated Circuit (IC).

Introduction to ISO 26262 functional safety standard

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 2 types of failures that can occur.

1- **Systematic failures** can only be eliminated by a change in the design of the manufacturing process, operational procedures, documentation or other relevant factors. The probability of a systematic failure occurring is reduced through a robust development process and quality management.

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 system architectures and/or IC detection strategy. This is one of SBC's purposes.

The automotive industry released ISO 26262 on November 15, 2011. This standard, specifically modified for "Road vehicles - Functional safety," is an adaptation of the functional safety standard IEC 61508 [7] for automotive electrical/electronic (E/E) systems. Applications must maintain functionality and be dependable. 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. The dependability tradeoff for functional safety interaction is illustrated in Figure 1.

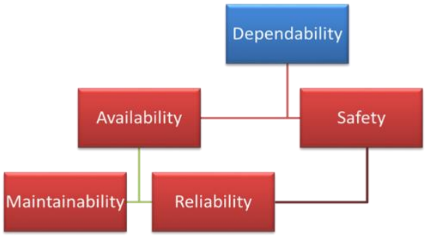
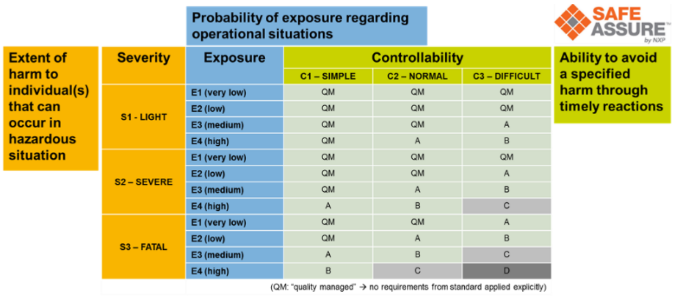


Figure 1.

NXP created a brand called SafeAssure™ that includes any product designed to be dependable through the effective combination of availability, safety and reliability.

I. From system requirements to IC architecture definition

ISO 26262 defines a System Integrity Level that depends on severity, occurrence and controllability. Table 1 summarizes the Automotive System Integrity Level (ASIL) that is system related. To translate this requirement into IC level, the probability of failure is needed. This is calculated through Failure In Time (FIT) rate.



Probability of exposure regarding operational situations

SAFE ASSURE by NXP

Extent of harm to individual(s) that can occur in hazardous situation

Ability to avoid a specified harm through timely reactions

Severity	Exposure	Controllability		
		C1 – SIMPLE	C2 – NORMAL	C3 – DIFFICULT
S1 - LIGHT	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 – SEVERE	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 – FATAL	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

(QM: "quality managed" → no requirements from standard applied explicitly)

Table 1

I. Why combine power management & functional safety hardware monitoring?

External safety monitoring measures are required by the microcontroller to verify the timings (advanced watch dog with challenger), the voltage level (over-voltage/under-voltage) and the computing (FCCU monitoring). These critical system functions have been standardized and integrated inside the power management circuit to create a new generation of safety System Basis Chips (SBC). The safety SBC is the integration of power management, connectivity and system. Its main purpose is to power and monitor the embedded system.

Combining the MCU and the SBC represents the safety backbone of the embedded system and therefore qualitative analysis of fail-safe is also required, i.e. how the component behaves following a failure diagnostic, to align IC safe state with the system safety goal. The first generation of NXP Safety SBC (MC33907 and MC33908) was positively assessed by TUV SUD in June 2015, to fit for ASIL D applications.

NXP's leading hardware system for functional safety solution is comprised of the MPC5744P safety MCU combined with the FS65 family, the latest generation of Safety SBC family, designed to meet the ISO 26262 standard safety requirements.

Combining Power Management and safety hardware monitoring simplifies system architecture and standardizes the safety backbone of embedded system, to fit for ASIL level through adequate quantitative analysis.

I. Qualitative analysis: from fail safe to fail silent

Different applications have different safe state conditions and in some cases the system architect prefers a hard stop such as reset, fail safe pin activation. In other scenarios, soft stop or a degraded mode may be preferred as this allows application continuity. Battery Management is a perfect example of the second case and this is the main driver for enabling fail silent architecture.

Fail silent mode is a new software configurability offered at the hardware level providing a flexible safety behavior that is adapted to multiple safety goals of the application. Reset and fail safe activation are configurable and safe, meaning the right level of dependability at the system level can be selected.

I. Safe delay – managing system timing conditions after failure

In cases, such as safe state, motor control applications require a sequential power disconnect after failure detection. This scenario requires specific handling of timing between detection and fail safe state activation. Due to the inductive load of the motor, this timing helps the system to avoid system failure due to demagnetization.

A configurable and safe delay has been defined, implemented and verified to support ISO 26262 implementation, and support this safe energy demagnetization. This timing management, with digital and analog redundancy,

Functional safety on the hardware side is a combination of quantitative analysis to reach the ASIL level and qualitative analysis to support various safety goals for a Safety Element Out of Context IC.

Now that the link between reliability and functional safety has been demonstrated, the final chapter will complete the picture on transportation IC performance.

II. Experimental results

A. The hardware integration test.

The safety architecture of safety SBCs is verified during ISO 26262 hardware integration testing, especially during the Fault Injection Test, to validate the safe state activation for all FMEDA failure modes violating a safety goal. When the FMEDA analysis is complete and the silicon is available, then it’s time to verify that the safety concept works as defined and implemented. To do so, faults are physically injected to the device to verify that the associated safety mechanism detects and reacts by activating the safe state within the Fault Interval Tolerant Time (FTTI).

B. Extended verification.

To assess the limits of the technology and to assess the robustness of the safety architecture implemented in NXP safety SBCs, some extended tests have been performed. These tests were carried out until the complete destruction of the device. The max rating specified in the datasheet was exceeded, with the unique goal to verify that the safe state remained activated even though the device is damaged. Even in such an extreme case, the safety goal is attained, meaning the human car driver would not be injured due to an uncontrolled reaction of a safety critical ECU.

I. Automated System Validation.

Every power management component connected to the electrical transportation network needs to be immune to ISO pulse transients, per the ISO 7637 [3] standard, as well as other voltage pulse variations called non-ISO pulses as they are car OEM specific. The number of non-ISO pulses is unlimited since they are OEM specific and each OEM has its own non-ISO pulse catalog based on experience. To avoid module validation failure from non-ISO pulse injection at the end of the validation process, it’s better to anticipate and predict IC behavior upfront.

To do so, NXP developed an in-house validation platform. This creates the non-ISO pulse pattern, automated injection and monitoring during the pulse, as well as a traceability report that may be needed after the results analysis to support ISO 26262 requirements. This platform validates the IC against a data base of several thousands of non-ISO pulses over only a few weeks. It has a 100% reproducibility based on the original setup even several months or years later.

The safety SBCs developed by NXP have CAN and LIN physical layers integrated to communicate through the car network. The second generation FS65 has been upgraded with the latest CAN FD 2 Mbits/s and are electrically compliant to ISO 11898 [4] and EMC compliant to IBEE [9] and SAEJ2962-2 [8]. They can therefore respond to the heavy load data communication requirements in the new car models. They also offer outstanding ESD GUN robustness up to 12KV contact discharged according to IEC61000 [6] and ISO10605 [2] standard.

III. Conclusion

NXP proposes a complementary approach to quantitative and qualitative safety analysis for external hardware monitoring devices like SBCs that is based on a certified ISO 26262 development process with its latest generation of fail silent safety SBCs.

Quality management and zero defect methodology is the foundation of functional safety analysis. It provides the FIT rate calculation to support functional safety metrics analysis and combined with fail safe hardware monitoring architecture helps to reach the quantitative goals and target the right level of ASIL.

This new generation of NXP devices has been tested until destruction to evaluate the architecture redundancy, showing a predictive behavior of the fail-safe signal (active low) as aligned with the safety concept. This extended characterization pushes the limits of functional robustness.

The critical technologies to enable car electrification and autonomous drive are summarized in Figure 9. This advanced safety architecture simplifies ECU design, helps to size the risk, improves system robustness and helps designers to predict system after failure, through configurable fail safe or fail silent behavior.

IV. References

[1] ISO26262:2011 - Road vehicles - Functional safety

[2] ISO10605:2008 - Road vehicles - Test methods for electrical disturbances from electrostatic discharge

[3] ISO7637-2:2011 - Road vehicles - Electrical disturbances
from conduction and coupling

[4] ISO11898-5:2006 - Road vehicles - Controller area network

[5] IECTR62380:2004 - Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment

[6] IEC61000-4-2 - Electrostatic Discharge Immunity Test

[7] IEC61508 - Electrical, electronic and programmable electronic safety related systems

[8] SAEJ2962-2 - Communication Transceivers Qualification Requirements – CAN

[9] IBEE: IEC TS 62228, Hardware requirements for LIN, CAN and FlexRay interfaces in automotive application – AUDI, BMW, Daimler, Porsche, Volkswagen – Revision 1.3/ 2012