Safe and Robust Functional Safety System Basis Chip (SBC) For Future Transportation Systems

David Lopez, Marketing & Application Manager, Safety & Power Management

Maxime Clairet, Application Engineer, Safety & Power Management

June 2016

Abstract

Combining functional robustness and functional safety on power management circuits to secure and simplify design of embedded E/E transportation systems.

The automotive market is moving towards electrification of the car and autonomous driving to lower emissions, optimize traffic congestion and reduce other hazards. This trend needs electronic systems that are capable of taking decisions and acting in the place of a human driver. These systems decide and act on safety applications such as steering, braking or transmission without causing injury to car passengers through wrong operations.

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

All safety electronic systems require a safety microcontroller and a reliable, safe source of power 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 presentation will present the latest functional safety innovations at the power management level (SBC); from the development phase to system design, underscoring the link to reliability and how to enable hardware that is safety ready. The paper will also demonstrate how using 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) This test shows the robustness of the safety architecture and how the safe state is activated in case of destruction by an Electrical Over Stress (EOS).

Table of Contents

About ISO 26262 Functional Safety Standards

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 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. These 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 26262:2011(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. 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.

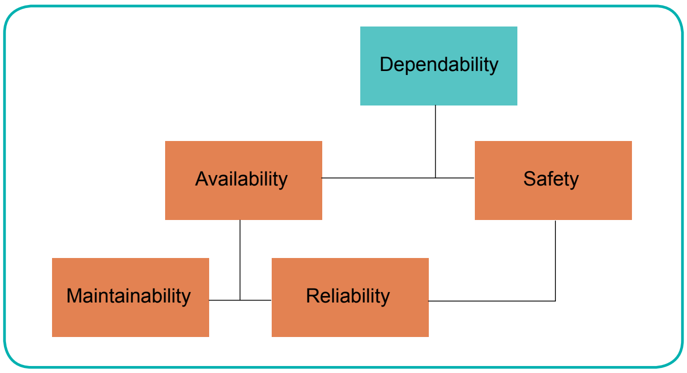


Figure 1: The dependability tradeoff for functional safety.

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

From System Requirements to IC Architecture Definition

ISO 26262 defines a System Integrity Level that depends on severity, occurrence and controllability. The following table summarizes the various Automotive System Integrity Levels (ASIL) that are system related.

Severity Extent of hard to individual(s) that can occur in hazardous situations	**Exposure** Probability of exposure regarding operational situations	**Controllability** Ability to avoid a specific hard through timely reations		
		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: Automotive System Integrity Level.

To translate this requirement into IC level, the probability of failure is needed; this is calculated through FIT rate.

Quantitative Analysis – From Reliability to Functional Safety

Functional safety metrics are calculated based on the Failure In Time metric (FIT), that quantifies the risk of failure during the lifetime of an application, according to IEC 62380. This FIT rate depends on technology, package and application conditions (mission profile). Based on hardware deterioration, the FIT rate calculation helps to determine the following ISO 26262 metric.

The FIT rate of the device is distributed to the device functions based on their representative die size, and for each function it is equally distributed to all possible failure modes. If the failure mode of a safety related function violates one of the application safety goals, a safety mechanism is required to detect it. One FIT represents one failure in 109 device hours, or 114 years.

$$\lambda = \left\{ \underbrace{\left\{ \lambda_1 \text{ x } N \text{ x } e^{-0.35\text{x}a} + \lambda_2 \right\} \text{x} \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \tau_i}{\tau_{on} + \tau_{off}} \right\}}_{\lambda_{die}} + \left\{ \underbrace{2.75 \text{ x } 10^{-3} \text{ x } \pi_a \text{ x } \left[\sum_{i=1}^{z} (\pi_n)_i \text{ x } (\Delta T_i)^{0.68} \right]}_{\lambda_{package}} \text{ x } \lambda_3 \right\} + \left\{ \underbrace{\pi_I \text{ x } \lambda_{EOS}}_{\lambda_{overstress}} \right\} \right\} \text{x} 10^{-9} /h$$

Figure 2 – FIT Rate calculation according to IEC TR 62380 standard, used by NXP on SafeAssure Components

This FIT rate is an input of a SafeAssure tool developed by NXP. The Dynamic FMEDA calculates three metrics required to qualify for ASIL level.

The SPFM (Single Point Fault Metric) represents a failure rate coverage which violates an application safety goal: >99% for ASIL D. Depending on the diagnostic coverage of the safety mechanism, low-60%, medium-90% or high-99%, the residual FIT of the undetected failure mode is calculated.

SPFM = 1 – [∑ (λRF) / λSR] where λSR = FIT rate of safety related functions.

The LFM (Latent point fault) failure in the safety detection mechanism (also called monitoring) can lead to the violation of the application safety goal in conjunction with a single point fault: >90% for ASIL D. The same approach is applied to the LFM, using the residual FIT of the latent failure mode not detected (by BIST example).

LFM = 1 – ∑ (λMPF) / [∑ λRF) – λSR)] where λMPF = residual FIT of latent faults.

The PMHF (Probability Metric of Hardware Failure), concerns the residual probability of breaching a safety goal (<10-8 for ASIL D).

The PMHF is than calculated from SPFM and LFM for the application life time (at least 15 years in automotive). Based on these three metrics, the fit for ASIL IC levelling can be addressed. The table below summarizes the level of metrics required to achieve a fit for ASIL level, at IC level.

	ASIL B	ASIL C	ASIL D
PMHF = Random hardware failure	<10-7	<10-7	<10-8
SPFM	>90%	>97%	>99%
LFM	>60%	>80%	>90%

Table 2 – SPFM, LFM and PMHF targets versus ASIL target

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 this is why 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.

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.

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.

The FS65 device family combines efficient DC/DC power management that can be switched into a low-power mode (30 µA). The safety goal of the FS65 is to secure the power supply to the system and monitor the MCU. Its power management is associated with various safety mechanisms, developed in combination with the MPC5744P, to avoid a malfunction in an application that could result in a system dreaded event. Using both devices in a system can reduce the effort needed to achieve an ASIL D system level solution.

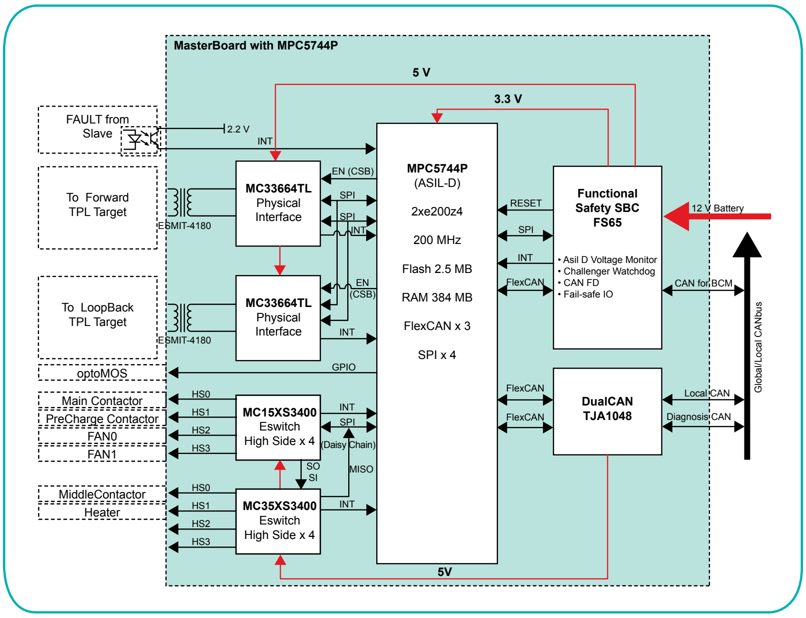


Figure 3 – System example – MCU & SBC backbone of BMS ASIL D safety architecture.

Combining Power Management and safety hardware monitoring helps to simplify system architecture and and standardize the safety backbone of the embedded system, to fit for ASIL through adequate quantitative analysis; However, quantitative analysis is not sufficient to enable system dependability; the behavior of the device after failure detection is a critical and complementary aspect to consider.

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 architectures.

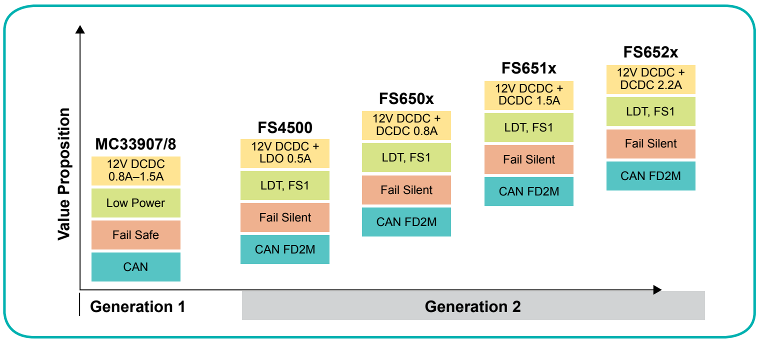


Figure 4 – Two generations of safety SBCs

The above figure shows the evolution of functional safety behavior inside NXP's safety SBC portfolio and in particular the safe state conditions that are system dependent.

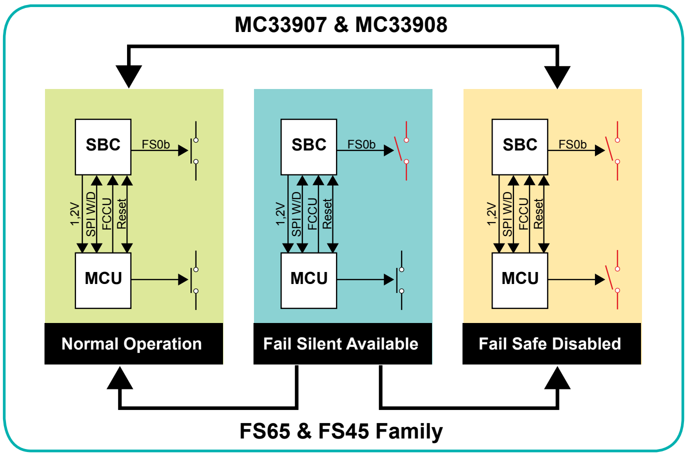


Figure 5 – evolution of system architecture.

Fail silent mode is a new software configurability offered at the hardware level, to have 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.

In the BMS example above, this specific solution enables the system to work in degraded mode, even after the failure, with the right level of availability to continue managing the car's energy in the E/E architecture.

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, generates a configurable delay signal (called FS1) versus FS0 used for equivalent application conditions and helps the system to simplify and secure the motor fail safe state.

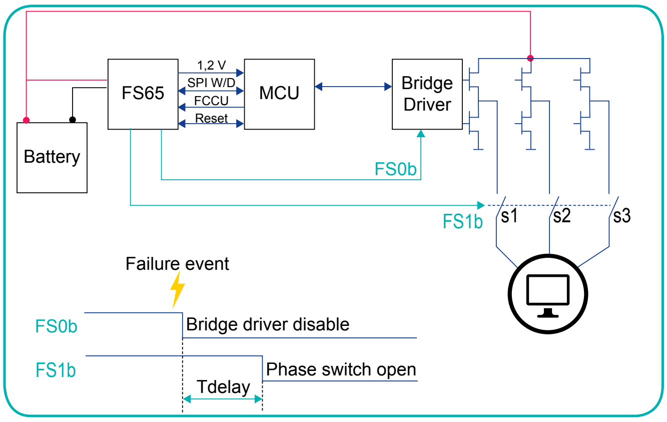


Figure 6 – managing system safety delay for electric motor architectures

This example shows that 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.

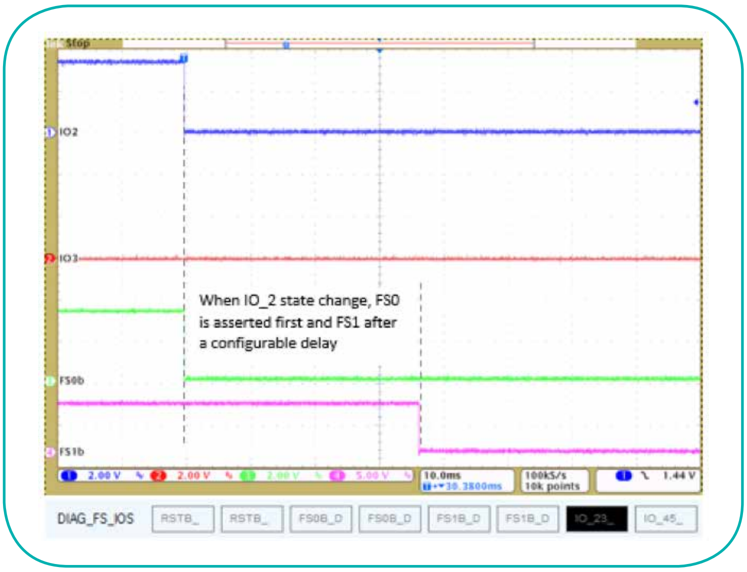
Now that the link between reliability and functional safety has been demonstrated, the final chapter will complete the picture on transportation IC performance. It will focus on the functional robustness and validation tests performed on Analog IC's to satisfy ISO 26262, but also characterizes the technology in extreme and system failing conditions.

Validation: The Proof Point For System Solutions

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).

For example, the MCU Fault Collection Control Unit (FCCU) pins monitoring by the SBC is verified. In normal conditions, the MCU provides two FCCU signals in differential voltages to the SBC safety input IO_2 and IO_3. In fault conditions, the MCU changes one of its FCCU signals and sends the same voltage to the SBC. The SBC detects the change on IO_2/3 from the expected differential voltage and reacts by asserting its safety outputs FS0 and FS1 after a configurable delay. Moreover, the SBC provides diagnostic through the activation of a flag in the SPI register, that the MCU can check in order to know the reason of the safe state activation after the MCU has been reset (Figure 9).



When IO_2 state change, FS0 is asserted first and FS1 after a configurable delay

Figure 7 – Safe state activation by FCCU detection and associated SPI diagnostic

All the failure modes listed in the FMEDA as violating a safety goal defined in the safety concept are injected to the device and the associated safety mechanism is verified.

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.

Figure 10 demonstrates that the safe state is still activated (FS0 activated low) when the device is damaged after the battery voltage (18 V) is applied to the pre-regulator (Vpre) which is specified at 8 V of max rating.

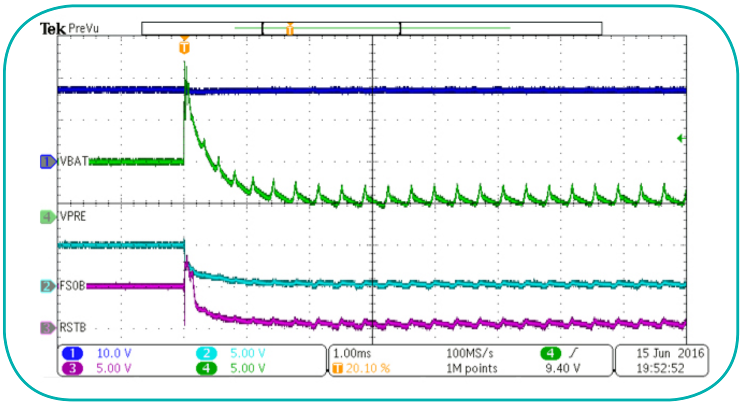


Figure 8 – Safe state activation after device destruction (Vpre > max rating)

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 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. In order 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.

This unique platform is based on analog and MCU hardware, MCU embedded software and Windows® based Graphical User Interface on your computer. It is also used to validate our MCU attach strategy and verify the SBC behavior when transient loads are applied to the SBC regulator rails.

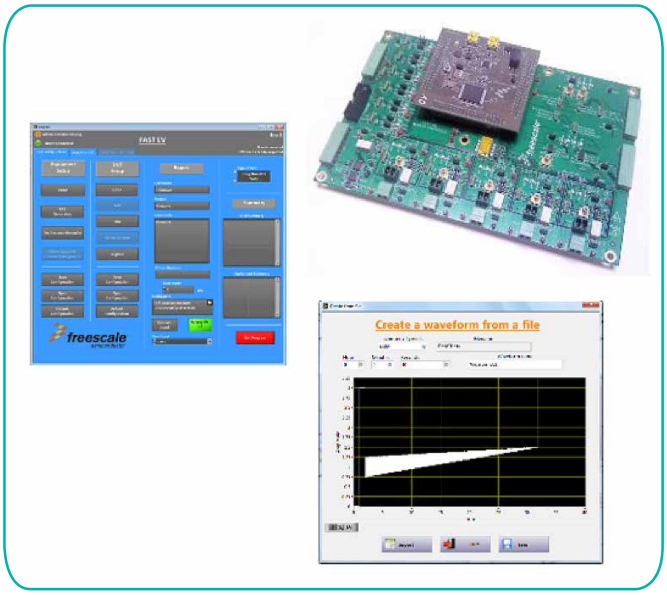


Figure 9 – Automated non ISO pulse platform

EMC and ESD

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 and EMC compliant to IBBE and J2962-2. 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 12 KV contact discharged according to IEC 61000 and ISO 10605 standard.

Extended Reliability Performance

The FS65 was designed and qualified with the expectation of longer ON cycles required by the Electrical Vehicle mission profiles, as well as the higher temperatures required in the new drivetrain applications for the autonomous driving car.

Conclusion—Reliability, Robustness and Safety as Key Pillars of Simplified Embedded Solutions

This article highlights the complementary approach of quantitative and qualitative safety analysis for external hardware monitoring devices like SBCs that is based on a certified ISO 26262 development process. This is precisely what NXP proposes with this 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 article shows the link between quality and functional safety, in particular the relation between FIT rate and mission profile for transportation solutions.

Now, how the system behaves after failure is also a critical aspect of the analysis and the safety behavior of the IC. The evolution of configurability of safe state enables applications to decide their dependability as the right tradeoff between safety and availability of the E/E system.

Validation of automotive semiconductors is also changing and requires more system tests to secure the behavior of the component within aggressive and noisy environments and after failure. This validation methodology has been developed to secure the V&V validation and provides documents with proof points.

Last but not least, this new generation of 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 push the limits of functional robustness.

As a conclusion, this advanced safety architecture simplifies ECU design, helps to size the risk, improves system robustness and also helps designers to predict system after failure, through configurable fail safe or fail silent behavior

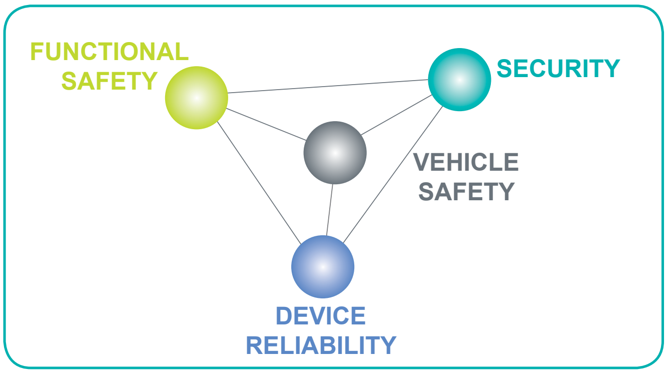


Figure 10 Critical technologies to enable car electrification and autonomous drive

Safety SBCs are developed following certified ISO 26262 process with a quantitative and qualitative safety analysis. This risk analysis combined with functional robust design, with flexible fail safe system architecture and with advanced security architecture opens the horizon for the autonomous vehicle by preparing fault tolerant and secured transportation systems.

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

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXPHalbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Semiconductor
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014 or +81 3 5437 9125
support.japan@nxp.com

Asia/Pacific:
NXP Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

www.nxp.com/safeassure