High-Voltage (HV) Inverter Safety System Concept for ISO 26262 Compliance

Abstract

Increasing market demand and legislation are driving the need for performance and functional safety in electric vehicles (EV). In particular, two new challenges need to be addressed to ensure the future of EVs: improved SoC definition aligned to functional safety and the concerns from customers about time to market. NXP has developed a functional safety concept for an HV traction inverter that addresses these two points. It defines several system deliverables that customers can use to build their own concept more quickly.

This paper will introduce this functional safety concept for HV battery electric vehicles, according to ISO 26262 recommendations regarding embedded safety system development. It will cover ISO 26262 methodology and consider the different work-products that NXP completed for this safety concept:

- Item definition, risk assessment, safety goal definitions, ISO Part 3
- Functional safety concept for the HV traction inverter, ISO Part 3
- Technical safety architecture for the HV traction inverter, ISO Part 4
- System faults detection and reaction, ISO Part 4

Table of Contents

Introduction

One of the indisputable facts about the automotive industry is that the overall electronic system content in vehicles is increasing. As vehicles become more sophisticated and include features that sense, think and act for the driver, the type of electronic content changes. In particular, there will be massive growth in hybrid electric vehicle and electric vehicle content, as well as automated drive functions.

There is a multi-step process to move toward fully battery electric vehicles. It involves moving through basic electrification systems to more feature-rich systems that include the migration of all high-power loads. A key challenge for the industry in this move is to ensure the robustness of the systems against peaks.

Market growth is rapid. Government incentives help this growth in many countries. Concerns for long-term sustainability mandate stricter legislation around emissions, materials and manufacturing processes. However, the current business model for electric vehicles is not profitable long term for OEMs, and it needs to be addressed. The average estimated cost for base electric vehicles is still a major concern. OEMs will be looking to close this gap by bringing more design back in-house, or by bypassing Tier 1 suppliers to talk directly to IC suppliers. The disrupter here will be to integrate embedded electronic architectures by combining ECUs and clustering functions in a new way.

This is why NXP is working closely with partners across the industry to accelerate how these constraints are met. One way is by developing reference designs that combine our system know-how with our safety expertise. This means that reference designs include key safety system elements from the outset. To develop safety concepts for hardware reference designs, NXP has to be able to define the safety goals, concept and functions for the intended item to be able to identify the right system implementation into our system design. The safety documentation that NXP delivers is designed for reuse by our customers.

ISO 26262 V CYCLE PROCESS FLOW

ISO 26262 provides the recommendations and guidelines for each of the development phases for developing vehicle safety system products and achieving the right level of maturity for functional safety. ISO addresses the process and methodology in parts 2, 8 and 9, and also the technical aspects with specific work products and reviews to perform all along the V cycle project development (Figure 1). This V cycle considers functional safety development, starting from the top, OEM, to IC suppliers, via the Tier 1 suppliers, or system providers. Depending on the company responsibilities into EV development, parts 3, 4, 5, 6 and 7 may apply or be tailored during the development phases.

If we take the example of a system provider developing an inverter module as SEooC for an electric vehicle, Parts 3- for assumption of use; 4 -system; 5- hardware; 6 – software; and then 7 -for the master production will apply. Parts 10 and 11 are guidelines for the application of ISO 26262.

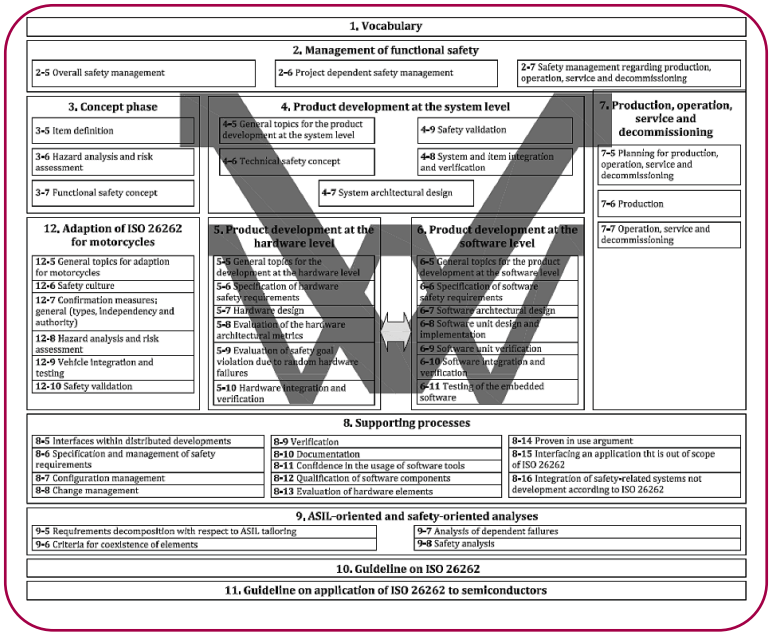

Figure 1: ISO 26262 V Cycle Process Flow

V CYCLE FOCUS FOR A REFERENCE DESIGN SAFETY CONCEPT

As mentioned in the introduction, IC suppliers like NXP anticipate and develop the system ECU in the same way a traditional Tier 1 does. By doing this, we can speed development time and provide standard deliverables that are of benefit throughout the development chain. The goal is not necessarily to provide a solution with the same level of maturity that a tier 1 could provide, rather to accelerate the development of the work products for the tier 1. However, to properly define the safety concept as close as the one for customers, the exercise of developing each part of the ISO should be run. The focus for the IC supplier is then to address each part from the V cycle (Figure 2), except for part 7 which is dedicated to Tier 1s for mass production.

Part 3 provides the guidance to establish the safety concept. It defines the item within the targeted system. It also includes the preliminary functional safety architecture with the potential hazard and safety goals that the functional safety concept shall not violate. This part helps customers to easily understand if the context of the NXP proposed reference design matches their own application.

Part 4 is the technical description and definition per requirement of the system architecture for the desired system product. This part also defines and analyzes all the system failures so that the diagnostics are defined to achieve the right safety level.

Parts 5 and 6 are the V cycle of the hardware and software architecture development with the associated prototypes. Here, all the safety verification and validation points are covered to verify the safety concept.

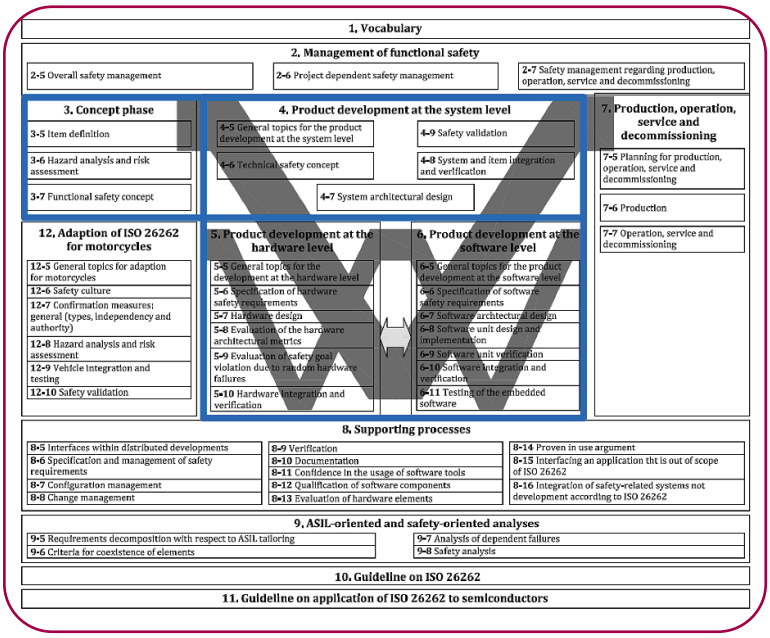

Figure 2: ISO 26262 V cycle process flow

HV INVERTER DEVELOPMENT

ITEM DEFINITION

ISO 26262 states that the item needs to be defined to start the system concept development. This will clarify the scope and the boundaries of the intended item and system, along with the preliminary item architecture (Figure 3) and the allocated functional assumptions.

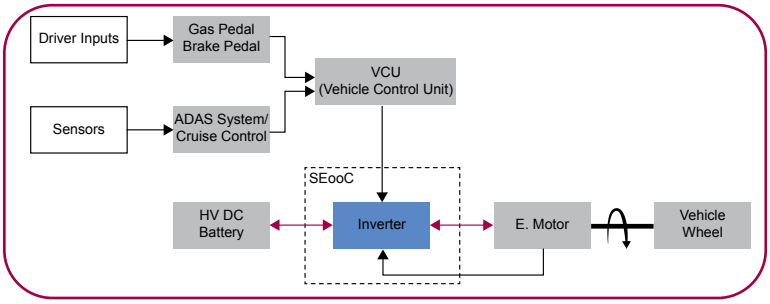

Figure 3: HV Inverter for EVs

In the example of an HV inverter for EVs, the functional assumption could be resumed as follows: an inverter is the main traction system of an electric vehicle. It controls energy conversion between an electric source (HV DC battery) and the mechanical shaft of the electric motor, based on torque requested from the vehicle control unit (VCU). The VCU interprets the command from the driver as an acceleration or deceleration request for the electric motor. The inverter translates this torque request into phase currents going into the traction motor. In a state-of-the-art battery electric vehicle, a simple gearbox without a clutch usually makes the connection between the motor shaft and the vehicle wheel.

This is our first assumption. It is important to be specific here, since the safety concept and the safe states would be different if the vehicle had a clutch. In our case, if a hazard should occur, it is impossible for the driver or the electrical system to stop the traction of the vehicle by simply opening the connection between the electric motor and the wheels of the car.

HARA AND SAFETY GOALS

The definition of the HaRa and the safety goal is normally a huge analysis done at OEM Level and delivered to the Tier 1 supplier as requirements for the system to be developed. This process is defined in ISO 26262 Part 3 with a goal of analyzing the impact on humans due to malfunctioning behavior of the defined item. All possible EE system malfunctions associated to all possible driving and non-driving scenarios are identified, while considering the operating and environmental conditions (Figure 4).

Scenerio No	Vehicle Operating Condition	Driving Situation
1	Parked	Parked in parking lot or garage
2	Parking	Parking car in parking garage
3	Stopped	At crossing or red light
4	Driving	On highway road/overtaking

Figure 4: EE system scenarios

The ISO 26262 ASIL table (Figure 5) uses a set of risk parameters to define ASIL levels ranging from Quality Management (QM) through ASIL D at the most severe. Hazards can therefore be assigned relevant ASIL levels following this ranking. Once the hazard and the safety goals are identified, the safe state and fault tolerant time interval can be defined for each hazard. The safety goals are the highest level of functional safety requirement from which all the other safety requirements are derived.

Severity S	Exposure E	Controllability C		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Figure 5: ASIL table

As NXP is a Tier 2 supplier, getting these safety goals and hazards from the OEM is quite difficult. Nevertheless, NXP has to be able to provide clear evidence on the use cases considered for any system we develop, including a reasonable analysis of the HaRa to clarify the safety goals for our customers. A reasonable selection of scenarios is considered and mainly focused on the worst cases. The list of example hazards and safety goals for an EV HV inverter would be:

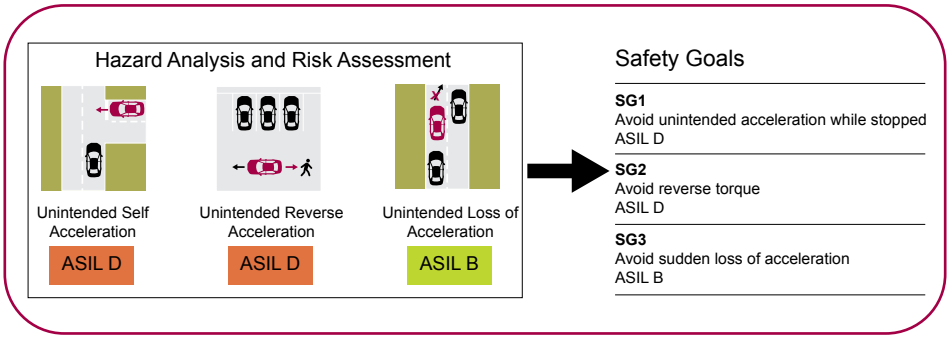

Figure 6: Examples of hazards and safety goals for an EV HV inverter

FUNCTIONAL SAFETY CONCEPT

With these assumptions, item definition and hazard and safety goals, the first high-level system functionalities can be defined. The first functional requirements (FR) and associated high-level functional safety requirements (FSR) are then defined for the functional safety architecture (Figure 7).

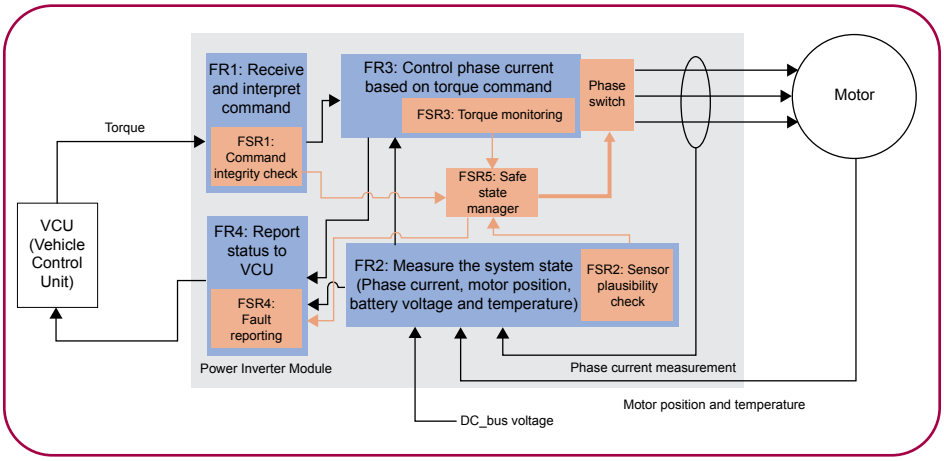

Figure 7: Functional safety architecture

The functional safety architecture for an HV inverter can be resumed to the following main functions and safety functions presented here:

Function	Goal	ASIL	FTTI
FR1	(command) The Inverter shall analyze the request from VCU, then command the following functions, traction, brake and battery regeneration.	QM	
FSR1	The inverter shall check the command from the VCU and alert in case of fault	ASIL D	FTTI 200 ms
FR2	(measure)The Inverter shall measure the state of the Motor (Phase current, Position and Temperature) and Battery voltage.	QM	
FSR2	The inverter shall check the plausibility of the sensors feedback and alert in case of fault	ASIL D	FTTI 200 ms
FR3	(control) The inverter shall correctly translate the torque request into a current request, and regulate the current flowing into the electric motor by switching high voltage to respect this current reference	QM	
FSR3	The inverter shall monitor the torque provided to the motor and alert in case of fault	ASIL D	FTTI 200 ms
FR4	(report) The inverter shall provide feedback of the system status to VCU.	QM	
FSR4	The inverter shall report its own faults and status to the VCU	ASIL D	FTTI 200 ms
FSR5	The inverter shall implement a Safety Manager to collect faults and react to bring the vehicle into a safe state (motor command stopped).	ASIL D	FTTI 200 ms

Figure 8: Functional and safety functions

The ASIL level and FTTI are associated with the safety requirements derived and inherited directly from the safety goals. They are then used to propagate the ASIL level to the lower requirements and technical system safety architecture addressed by the ISO in Part 4.

So at this functional level, the item definition, hazard and safety goal assumptions and functional safety architecture with requirements are the first top deliverables for IC supplier customers. These top deliverables should help them to understand if the case study and development of the reference design matches the application that they want to develop. If it is not fully compliant, then the gaps can be analyzed and a plan of action established to merge the safety concepts from both the customer and the supplier.

TECHNICAL SAFETY CONCEPT

The technical safety concept is the system architectural design completed by the safety and non-safety requirements. It provides the rationale for the suitability of the system architecture to fulfil the safety requirements and design constraints from the item definition, safety goals and the functional safety requirements implemented in Part 3.

The technical safety concept is then the split and representation of all the hardware and software sub-element functions that are needed to achieve the intended item and system functionality. All safety mechanisms and reactions to these fault detections have to be specified to avoid the violation of the safety goals in the case of malfunction of a technical function.

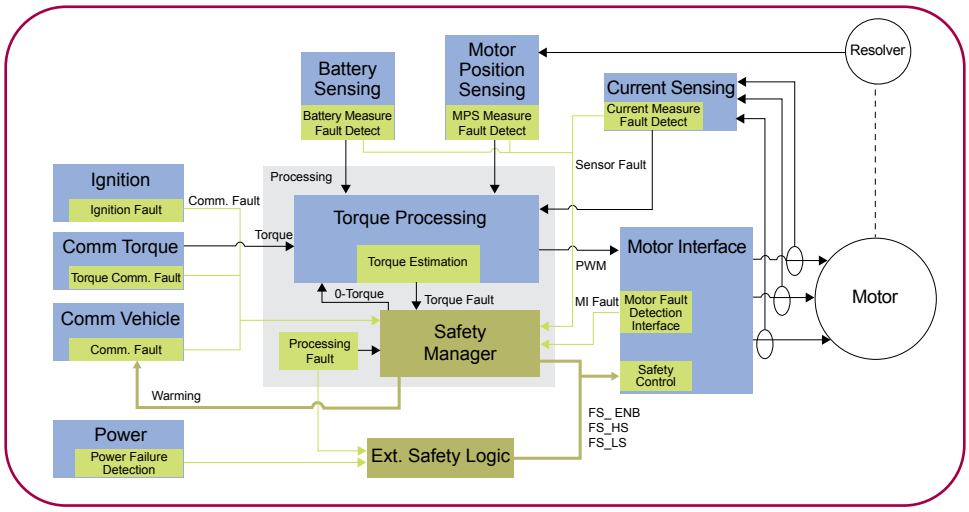

Figure 9: Technical safety concept

ISO 26262 recommends running a safety analysis on the system design architecture, such as a FTA or safety FMEA, in order to define these safety measures. This helps to exhaustively identify all system failures which potentially violate the safety goals either as single point fault, or as a latent fault. A fault detection function is then addressed to each of the failures to mitigate the fault and reduce its severity.

Using this safety analysis, a list of safety mechanisms can be established and derived into new safety requirements. They are then allocated to all system architecture blocks that are safety related and identified during the safety analysis. All the safety mechanisms are defined according to the operational, technical and timing conditions applied to detect the fault (Figure 10). The technical definition of the safety mechanism provides the evidence along with the appropriate reactions. This is sufficient to achieve the safe state in a time less than the FTTI and to not violate the safety goals of the item.

Safety mechanisms can be hardware or software, or both. The list of failures and safety mechanisms will help to define the hardware architecture and the software architecture, as well as to run the FMEDA from Parts 5 and 6 of the ISO.

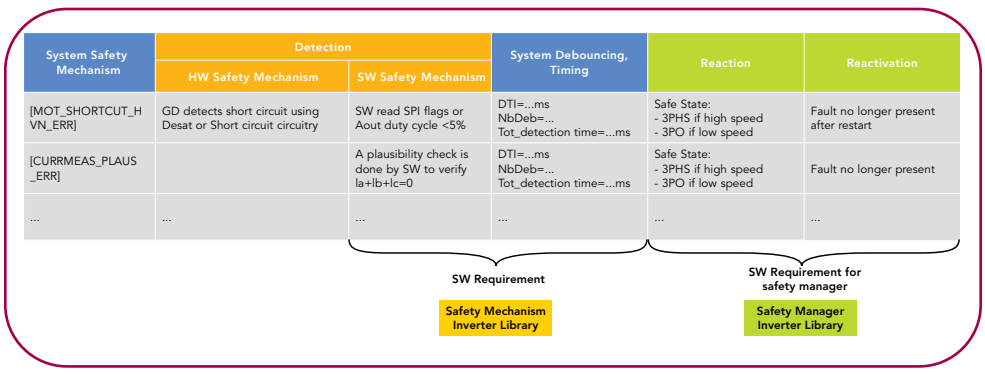

Figure 10: Fault reaction definition

The reaction for each fault detection is defined. This reaction flow is developed with the intention of bringing the system to the safe state. In the case of an EV HV inverter, the definition of the safe state is quite complex due to a high amount of energy flowing into the electrical motor. In some cases this can result in unstable behavior instead of ensuring the safe state that is requested by the system.

Therefore, the list of system failures aggregated by the defined safety mechanisms should be properly completed by the appropriate safe state associated to those failures. This matrix of system failure detection and reactions is part of a deliverable that NXP provides in the scope of system safety enablement (Figure 10).

The different work products that are developed in Part 4 of ISO 26262, including the technical safety architecture and requirements, the safety analysis and the system failure matrix, are useful for the customer for evaluating the reference design that NXP proposes. They bring the evidence of the safety completeness to achieve the expected functional safety integrity. These work products are arguments and rationale that the TSC fulfils the top-level safety requirements of the item. Beyond this, they provide the customer with data that can be reused and fine-tuned to personalize an NXP reference design to their own application development.

SAFE STATE DEFINITION

The safe state definition plus all the failure events which request to transit in these safe states are also an important part of the technical safety concept. The safe state machine, the safe state definition and diagrams, plus the transition requirements, are defined in this technical safety concept.

In the case of the inverter module, several complex safe states exist. The safe state goal in case of failure is to stop the propulsion of the vehicle, so to provide 0 torque to the electrical motor. The obvious solution would be to open all the inverter's IGBTs so that current is no longer provided to the electrical motor. However, depending on the driving condition, this can create a high braking force on the motor—directly on the vehicle wheels—especially at high speeds. This condition would then be a dangerous event for the driver.

Opening all the IGBTs is not always the solution to bring the vehicle to a safe state. In the example above, the safe state would be to short the three phases of the motor, so opening or closing all three high-side or low-side IGBTs. The table below resumes the three main safe states for an HV inverter system. Other options, such as degrading the power or insuring 0 torque control by PWM, also exist.

ID	Description
SS_HSS	Short the 3 HS switches
SS_LSS	Short the 3 LS switches

Figure 11: Active short circuit of the three motor phases

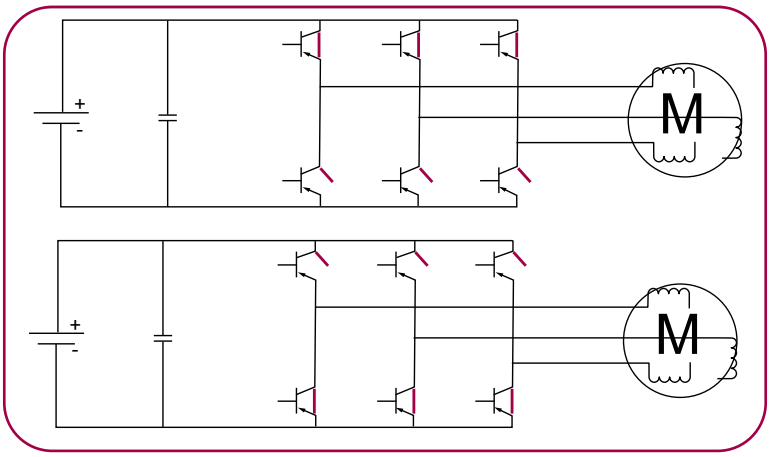

Figure 11.1: Active short circuit of the three motor phases

ID	Description
SS_3PO	Controlled open: the PIM opens the 6 power bridge switches

Figure 11.2: 3-phase open circuit

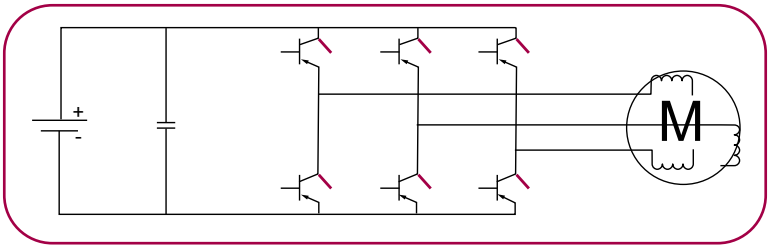

Figure 11.3: 3-phase open circuit

SAFETY ARCHITECTURES

For this part of ISO 26262, most of the hardware and software work products are tailored in a similar manner to the hardware and software requirement specification. Only the hardware and software architectures, schematics and layouts are developed at this stage. As mentioned, the goal is not to do a certified inverter module as a Tier 1 would, but just to create a reference design that is usable by customers as an Asample prototype that includes the safety concept. With this, the customer already gains three to six months in the development and prototyping phase.

HW SAFETY ARCHITECTURE

To produce an Asample prototype, it is assumed that the process flow and work products identified above are mature and detailed enough to be able to build a proper Asample hardware safety architecture and bring the evidence to the customer so that their safety concerns are considered and fulfilled.

These assumptions and definitions are then used to derive the hardware safety architecture from the system safety concept. All IC components are chosen and attached to fulfill the safety requirements regarding diagnostics and reaction to safe state. In this reference design proposed by NXP, the full architecture is built with NXP ICs. To enable the safety system, the hardware architecture is prototyped to be able to validate the safety concept by injecting some system faults. System failures and safety mechanisms defined in the technical safety concept are tested. The prototypes support both the software application development and the safety mechanism library that NXP delivers as part of this safety system enablement package.

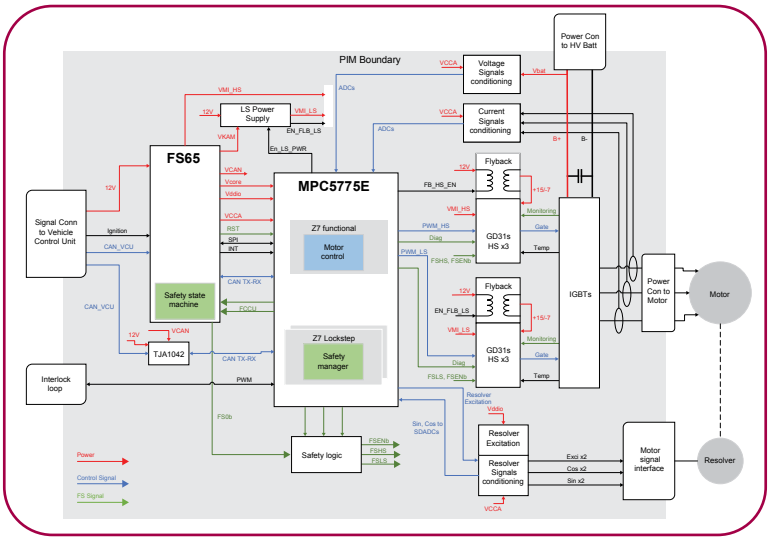

Figure 12: Hardware safety concept

HARDWARE FMEDA WITH IC SYSTEM FAILURE MODE

An important part of ISO 26262 is the safety analysis. Safety analyses such as FMEDA are performed at different levels of the systems. It is an important deliverable that NXP shares with our customers. Since the purpose of the FMEDA at IC level is to perform a detailed and exhaustive analysis of the IC failures, it is often too detailed to be useful at system level.

To simplify the results of these detailed FMEDAs, failure needs to be regrouped from the IC fault model in system failure modes. For example, all failures of the internal logic of the gate driver could be regrouped into one failure mode (FM) internal logic with the associated λsafe, λMPF and a λRF. These numbers can then be introduced at a higher level FMEDA at system level.

While the idea is simple, the complexity comes from the granularity required for the systems safety analysis. Some faults can easily be regrouped; some will be important to maintain with a low level of detail. For example, in the power management IC, the input responsible for the ignition of the system is only protected by system safety mechanism, not by IC safety mechanism. In such cases, it will be important to make sure to study this pins and failures independently and not to regroup it with other blocks to avoid single point fault.

SOFTWARE SAFETY ARCHITECTURE

The fault reaction table developed in figure 10 as part of the ISO 26262 Part 4, highlights a list of periodic checks and reactions that the systems need to do. Most of these checkers are done in software. To ease the use of this safety concept, NXP has developed a software library deliverable that implements theses checkers and library (Figure 12).

This library is composed of several modules:

- A checker is a group of diagnostics of the application that are called upon periodically, e.g., motor intense check, torque monitoring checkers, and current sensors checkers.
- The safety manager is responsible for counting the fault and calling the reactions manager when a threshold is passed. It also verifies that each checker works correctly by injected fault during the Init phase.
- The reactions sequencer is responsible for the transition of the system into a safe state once the safety manager has detected a fault.
- Some additional modules are necessary, such as an inter-core communication to manage the sharing of information between the non-safety core (QM) doing the motor control, and the safety core (ASIL D) doing the safety check, as well as a memory management to guarantee the isolation between cores.

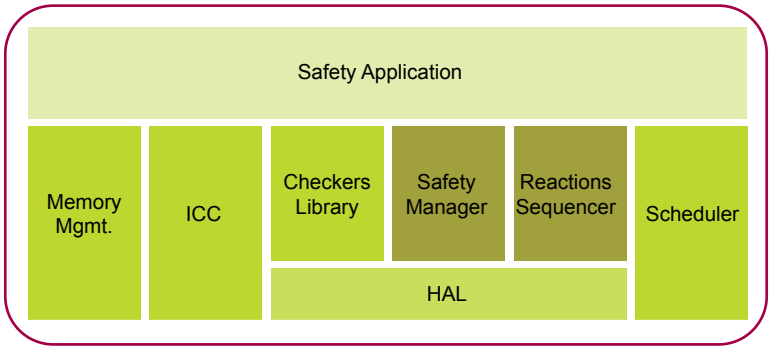

Figure 13: Simplified architecture of NXP Safety Inverter Library

CONCLUSION

A reference design that follows the ISO 26262 development process and that delivers the technical work products that are described in this paper is valuable to customers. It not only helps speed development time, but also provides a level of technical safety architecture that describes the failures and safety mechanisms allocated to each failure type. The evidence of this achievement of the safety integrity level for the proposed hardware architecture is part and parcel of this package. Customers are therefore able to judge, re-use and modify the content as needed to achieve their own concept assumptions.

Contributors

Antoine Dubois
Erik Santiago

How to Reach Us:

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

USA/Europe or Locations Not Listed:
NXP Semiconductors USA, Inc.
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:
NXP Semiconductors Germany 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 Japan Ltd.
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
+0120 950 032 (Domestic Toll Free)
https://www.nxp.jp/
https://www.nxp.com/support/support:SUPPORTHOME

Asia/Pacific:
NXP Semiconductors 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/ask

Document Number: HVINVERTERWPA4 REV 0