Safety design for modern vehicles – including EV/HEV

An integrated hardware approach delivers significant benefits

› Robert Wegrzyn, System Application Engineer, Infineon Technologies
› Steve Gross, Safety Application Marketing, Infineon Technologies
› Vikram Patel, Segment Marketing Manager, Infineon Technologies
› Atilla Bulmus, Senior Staff System Application Engineer, Infineon Technologies
› Cuauhtemoc Medina Rimoldi, Powertrain and EV Marketing, Infineon Technologies

www.infineon.com

Contents

Introduction

When purchasing a new vehicle, consumers usually have a long list of the things that they want. One thing that is never on anybody's list is 'surprises'. When we purchase a vehicle, we are putting a lot of faith in the designer's ability – our lives, the lives of our families and other road users depend on the vehicle performing as intended, all of the time and every time.

As such, comprehensive safety standards exist for every aspect of the vehicle which could cause injury or worse if it malfunctioned. Grouped under the heading of 'Functional Safety', these requirements are fundamental to the design strategy of the vehicle and continue throughout the lifetime of the vehicle.

In modern electric vehicles (EV) and hybrid electric vehicles (HEV) electrification of traditionally mechanical functions including the drivetrain are bringing greater efficiency and are better for the environment, but they also deliver a new challenge in terms of safety issues. Even in traditional Internal Combustion Engine (ICE) vehicles, electronic power steering (EPS) delivers advancement, but has new safety implications.

In this technical white paper, Infineon will examine the Functional Safety process and how it impacts the design process for EVs and HEVs and look at two critical examples: EPS assist systems and the high power inverter that forms the drive train. The white paper will then consider some of the essential work products defined in the ISO 26262 standard, including the hardware, documentation and support.

The automotive world is undergoing some of the most fundamental changes since the invention of the vehicle itself, driven in part by consumer demands and also by governmental policy and legislation.

Efficiency is one of the most significant topics and this is at the heart of many of the changes. Fossil fuel reserves are depleting and prices are, in general rising, so consumers are looking to increased fuel efficiency as a way of reducing the costs of driving. However, environmental concerns are also pushing the industry to be more efficient. The European Union has set a goal of reducing greenhouse gas emissions by 80% by 2050 and have set specific near-term targets for passenger car emissions (CO_2 to reduce from 130g/km to 95g/km by 2020) as controlling vehicle emissions will form a large part of this goal.

In the US, the Corporate Average Fuel Economy (CAFE) standards are driving automotive manufacturers to improve economy across their entire ranges, with a 49 MPG average being expected by 2022.

It comes as no surprise that EV and HEV are at the forefront of this initiative. Electronics content in vehicles is currently one-third of the over all cost and this is predicted to rise to one-half by 2030, according to Statista. Beyond the drivetrain itself, many mechanical functions of vehicles are being replaced by electrical equivalents that are smaller and lighter, thereby contributing to overall efficiency gains. In fact, some of these systems such as EPS are equally applicable to ICE vehicles as they are to EV/HEV.

While sales of EV are still relatively low, according to a recent study by BIS Research, there were 1 million EV deployed in 2015, rising to 2 million in 2016 and this growth will continue with an estimated CAGR of 28.3% until 2026.

Fully autonomous driving has been demonstrated by multiple companies and elements of this technology are now being seen in mass-produced vehicles. One of the major drivers behind this technology is safety – with the NHTSA reporting that 94% of accidents are caused by some form of driver error, the sooner decisions are made for the driver, the safer our roads and highways will be.

While we are in the early stages of the journey towards full automation, at least as far as mainstream vehicles are concerned, SAE International has mapped out a detailed path that defines the six stages between full driver control and full system control.

SAE level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of dynamic driving task	System capability (driving modes)
Human driver monitors the driving environment						
0	**No automation**	The full-time performance by the **human driver** of all aspects of the **dynamic driving task**, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver assistance**	The **driving mode**-specific execution by a driver assistance system of either steering or acceleration/ deceleration using information about the driving environment and with the expectation that the **human driver** perform all remaining aspects of the **dynamic driving task**	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial automation**	The **driving mode**-specific execution by a driver assistance system of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the **human driver** perform all remaining aspects of the **dynamic driving task**	**System**	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving environment						
3	**Conditional automation**	The **driving mode**-specific execution by an **automated driving system** of all aspects of the dynamic driving task with the expectation that the **human driver** will respond appropriately to a **request to intervene**	System	**System**	Human driver	Some driving modes
4	**High automation**	The **driving mode**-specific execution by an automated driving system of all aspects of the **dynamic driving task**, even if a **human driver** does not respond appropriately to a **request to intervene**.	System	System	**System**	Some driving modes
5	**Full automation**	The full-time performance by an **automated driving system** of all aspects of the **dynamic driving task** under all roadway and environmental conditions that can be managed by a **human driver**	System	System	System	**All driving modes**

Figure 1: The steps leading to full vehicle automation as defined by the SAE J3016 standard [Source: SAE International].

While there may be some justified debate as to some of the details of this progression, it will clearly have a huge impact on vehicles and their systems. In order to have the sensory capability and intelligence to monitor the environment, make good decisions – and execute them, vehicles will need many new and improved systems throughout.

However, amidst all this change, innovation and development, one fundamental aspect of vehicles, their design and usage will never change. Safety is paramount as an unsafe vehicle risks the lives of those on board as well as other road users. Safety will be the most important consideration at each stage of the SAE model. In fact, the ability to execute each stage safely becomes a precursor to being able to move to the next stage. Whatever the innovation, whether it replacing a mechanical system on an ICE vehicle with an electronic one, or developing a completely new electrical drivetrain for an EV/HEV, safety is always at the forefront of the designer's mind.

As the systems become more sophisticated, so the potential failure modes increase and safety considerations have to adapt to recognize this.

2. Functional Safety in the automotive world

Given the critical importance of safety in the automotive world, it should come as no surprise that the processes and steps to be taken are very carefully defined in internationally-recognized standards. The 'master' safety standard is IEC61508 that deals with safety in many industrial applications. ISO26262 is a sector-specific extension of this standard that deals with the functional safety of electrical, electronic and electromechanical systems within vehicles. The standard is very comprehensive and contains 10 sections with around 750 clauses, covering some 450 pages.

Functional safety (FuSa) is defined by the standard as ' the absence of an unreasonable risk'. These risks could be caused by a malfunction or failure of all, or part, of an electronic system within the vehicle. FuSa is a 'whole-life' approach and deals with random hardware issues from concept through development, production, repair and ultimately decommissioning of the vehicle. FuSa is not a measure of reliability; systems can fail, provided that they do so safely.

The FuSa process starts with a hazard analysis and risk assessment of the relevant system or sub-system by suitably qualified and experienced personnel. From the analysis and assessment, individual safety goals are defined with the specific objective of avoiding harm during an operational condition of the vehicle.

Each of these goals is then assigned a corresponding Automotive Safety Integrity Level (ASIL) based upon an allocation table within the standard, which ranges from 'A' (least stringent) to 'D' (most stringent). The basis for allocation requires evaluation of three parameters – Exposure (how often the situation may occur), Controllability (whether the driver can overcome the issue) and Severity (how severe could the consequences be?).

From the system level, the safety goals are translated into safety requirements for sub-systems and individual hardware components and, once the design is complete, verification is carried out by a combination of the hardware manufacturer and the system (vehicle) manufacturer under the so-called 'V'-model defined in ISO26262.

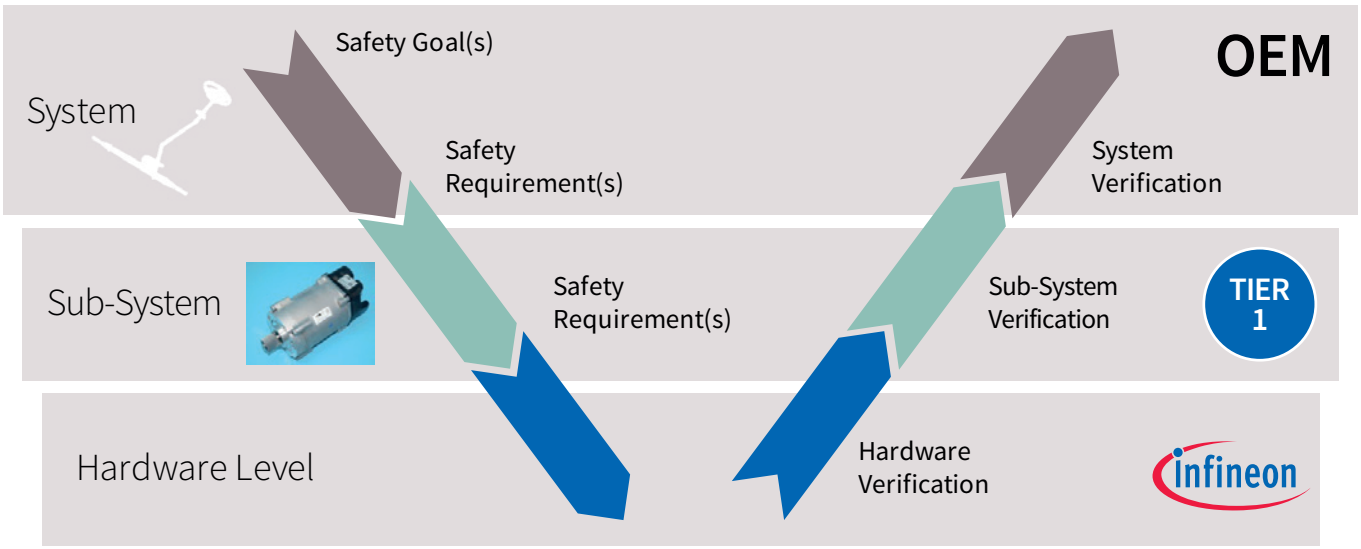

Figure 2: The 'V'-model as defined by ISO26262

Within FuSa, techniques to protect against hazardous failure include redundancy and diversity. Redundancy covers the use of two identical systems with the same function, while diversity refers to the use of two disparate systems, each with the same function. When applying diversity to a system, it is not necessary to use hardware components from different manufacturers, the goals can be achieved by using a single manufacturer.

3. Practical Application – EPS

EPS uses an electric motor to assist the steering of a vehicle. A sensor detects the torque exerted on the steering wheel by the driver and an electronic control unit (ECU) applies assisted torque via the motor, which connects to the steering mechanism. The mechanical linkage between the steering wheel and the steering gear is retained as a backup, so the driver is still able to manually steer the car, should the need arise.

EPS applies equally to ICE vehicles as well as EV/HEV. The main advantage is that it is only active during the actual steering movement and, by dispensing with the belt-driven hydraulic pump, increases fuel efficiency in ICE vehicles, or extends range in EV/HEV.

For a fail-safe EPS-assist system the three safety goals are most often defined as:

- ‘No unintended steering’ [ASIL D] – this could occur if the assist motor is driven without command or if the assistance provided is too great or insufficient, causing oversteer or understeer.
- ‘No blocking of steering’ [ASIL D] – there should be no loss of steering due to unintended motor activation blocking the ability of the driver to override manually if needed.
- ‘No sudden loss of assist’ [ASIL B/C] – the assistance should be constant – if assist is lost then the driver is startled and must immediately compensate for the loss of assist. In some physically weaker drivers, this may not be possible.

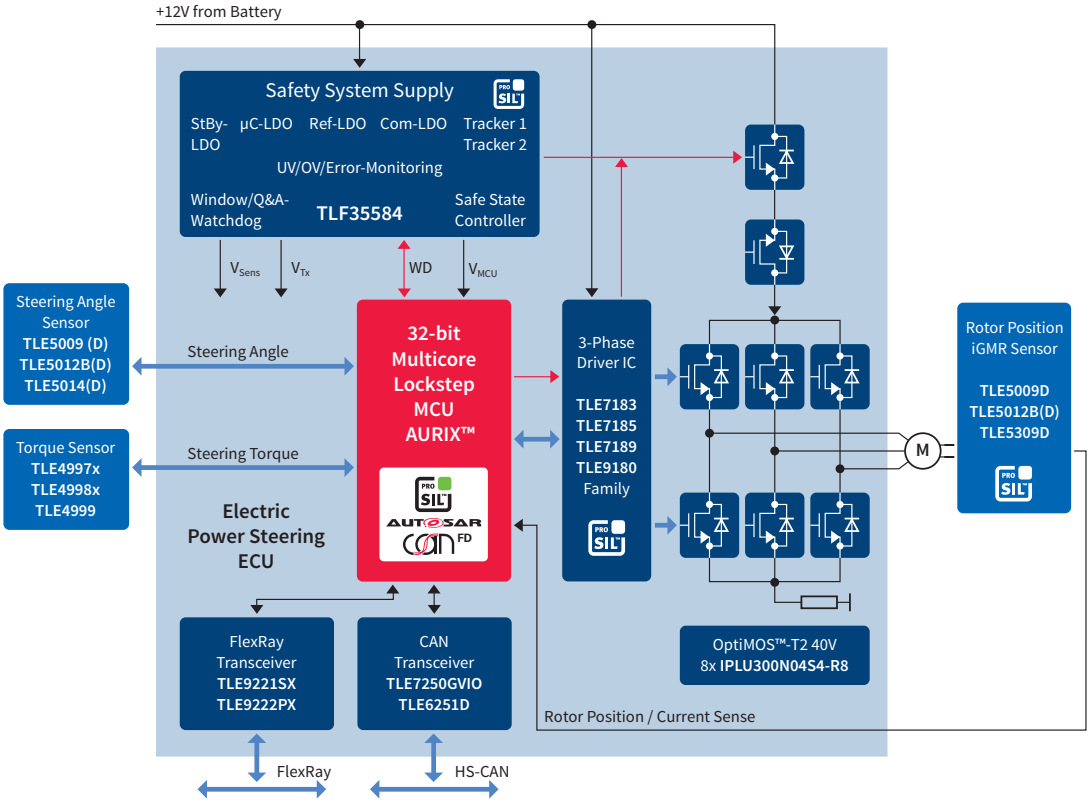

Figure 3: Block diagram of a modern EPS-assist system

The 32-bit microcontroller is selected to support the required ASIL levels and generates the correctly timed and synchronized PWM signals that trigger the gate driverthat, in turn, drives the MOSFET power stage that produces the AC signal to drive the motor.

The gate driver IC is required to monitor and safely drive the MOSFET switches. These switches control the power to the electric motor that provides the required torque for the EPS assist function.

The safety power supply not only monitors system voltages, but also other key safety indicators and has the ability to return the system to a safe state, should that be required.

4. Practical Application – Drivetrain Inverter

Within EV / HEV, the ICE is replaced by electric motors and an inverter controls the motors through the delivery of power. Regardless of whether the motor is synchronous, asynchronous or brushless DC (BLDC), the inverter is very similar and controlled by a logic board that includes a microcontroller, gate drivers, and a gate driver board that includes the gate driver ICs.

The vehicle battery supplies DC power to the inverter that converts to AC power to drive the motors through a power / switch stage that comprises high power IGBTs or MOSFETs. As well as driving the electric motors, a regenerating block could also capture energy and feeds this back to the main battery.

The proposed safety goal for this analysis is: 'No unintended torque'. This is categorized as ASIL C or D and simply requires that the acceleration torque requested by the driver is the same as the torque that is supplied / measured. There are several failure modes directly related to this safety goal for example:

- IGBT state deviates "too much" from the PWM command issued by the µC
- Active short circuit
- IGBT module destruction (implying safe state can not be reached)

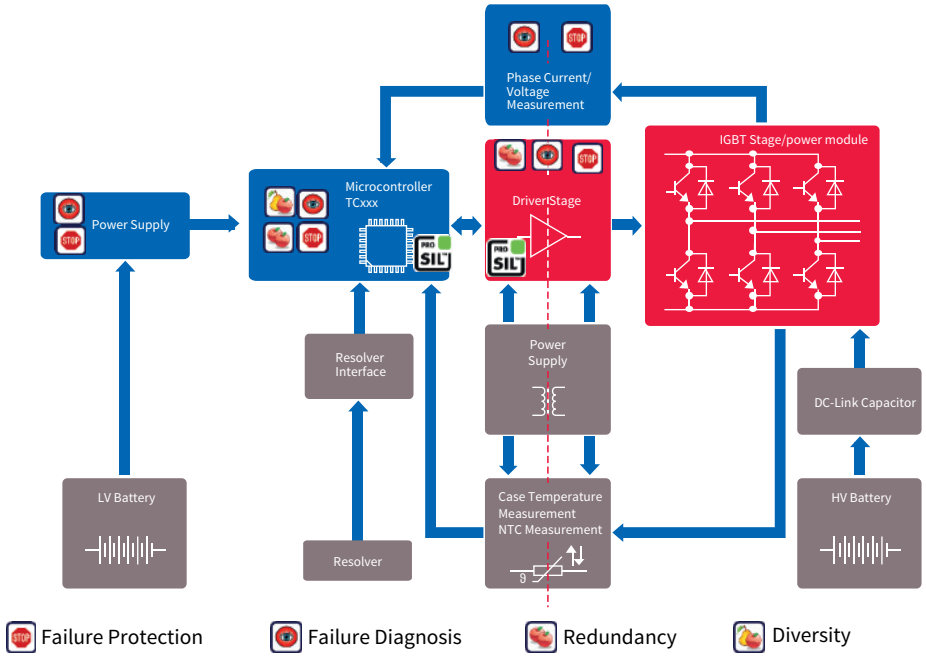

Figure 4: Block diagram of an inverter-based drivetrain

The 32-bit microcontroller is selected to support the required ASIL levels and generates the correctly timed and synchronized PWM signals that trigger the gatedriver that, in turn, drives the IGBT / MOSFET power stage that produces the AC power to move the vehicle via the motors.

The gate driver IC drives the switches in the power module that, in inverter applications, are required to drive electric motor loads that can exceed 200 kW at frequencies in the range of 10 kHz. Besides the microcontroller in the system, a configurable and intelligent gate driver provides flexibility to the safety case designer.

The current sensor is a key component in inverter applications and should be highly accurate over both temperature and time. Given the electrically harsh environment of the inverter, and the fact that currents can often exceed thousands of Amperes, Hall Effect technology based sensors are a good fit for the application, as they avoid issues such as saturation and hysteresis that can occur with other sensor types. Detection of under voltage or over voltage conditions could also be valuable when developing a safety case.

5. Technology overview

Considering the two practical examples that we have discussed, it can be seen that, while they relate to very different areas and functionality within the vehicle, the FuSa requirements are very similar. In fact, apart from the sensing which is application-specific, the basic architectures are also similar and incorporate many of the same hardware components.

At the heart of each of these systems is the microcontroller, typically a device from Infineon's AURIX™ family of devices that are specifically designed for use in safety-critical applications.

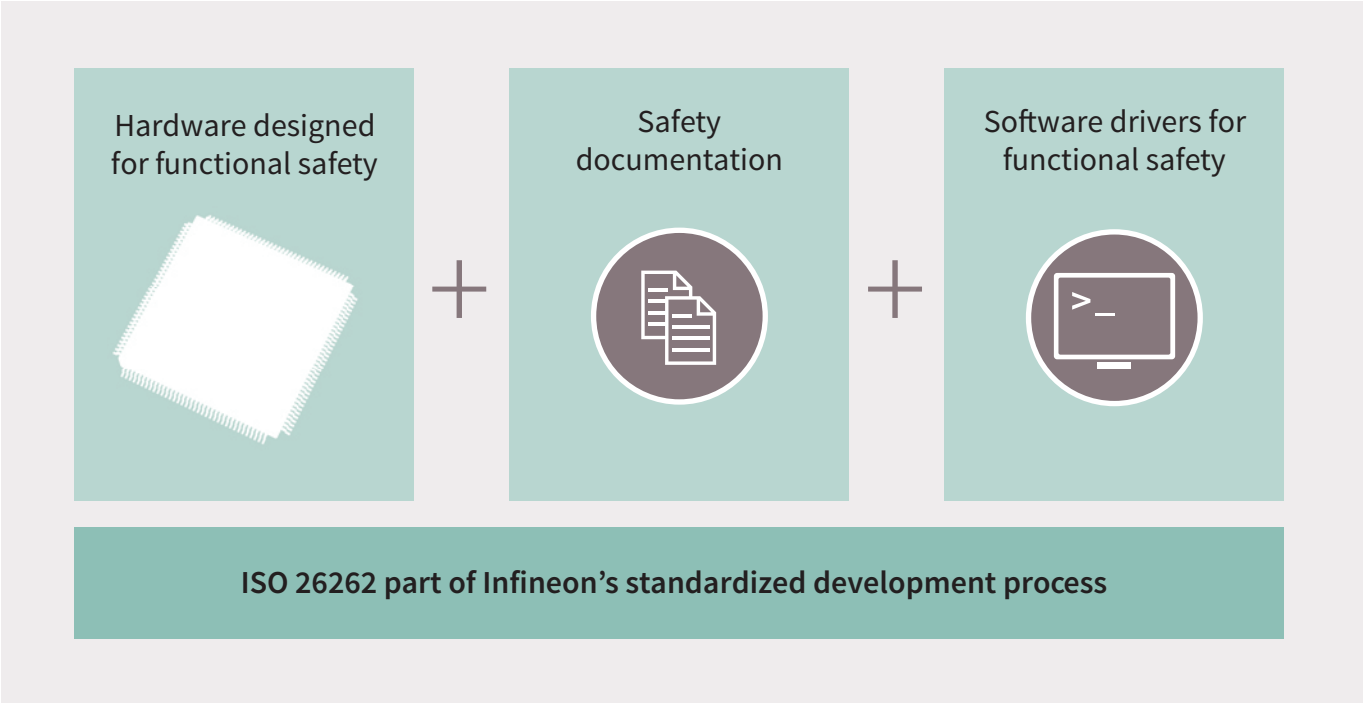

Figure 5: The principal cornerstones of the AURIX safety concept

The AURIX safety concept has three principal cornerstones:

- The hardware is designed for FuSa, with ISO26262 forming an integral part of Infineon's standardized development process. Key elements include single point fault detection with a lockstep CPU, ECC/EDC on the memory components and buses, and redundant peripheral devices. Also included is latent fault detection with both hardware built-in self tests (BISTs) and software based self tests. Common cause failure mitigation includes clock and voltage monitors, layout diversity, functional diversity and multiple watchdogs.
- Other than the basic operating data sheets and application notes, full safety documentation is supplied including a comprehensive safety manual, FMEDA, safety analysis summary report and a safety case report.
- SafeTlib is a set of supplied software functions for the self-testing of relevant safety hardware.

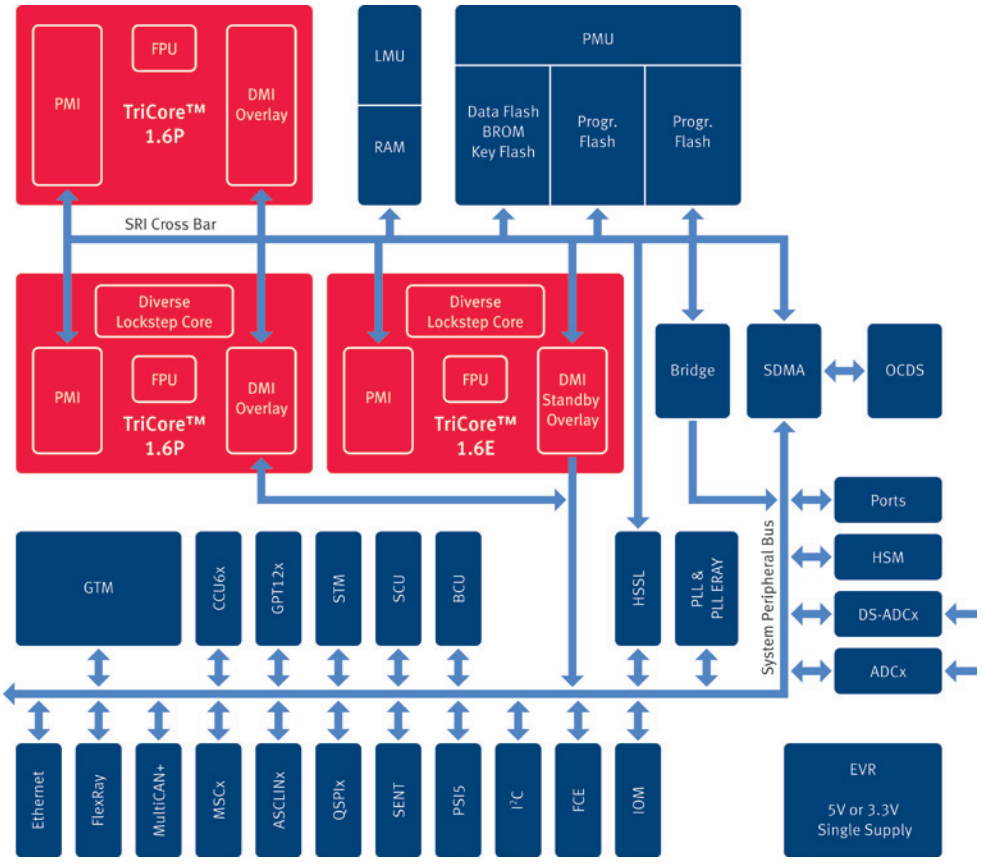

Figure 6: Block diagram of AURIX architecture

One of the key metrics for a FuSa system is the time taken to return to a safe state after a fault occurs and is detected. This period, known as the fault tolerant time interval (FTTI) is the sum of three elements – the fault detection time, the fault reaction time and the time for a safe state to be established.

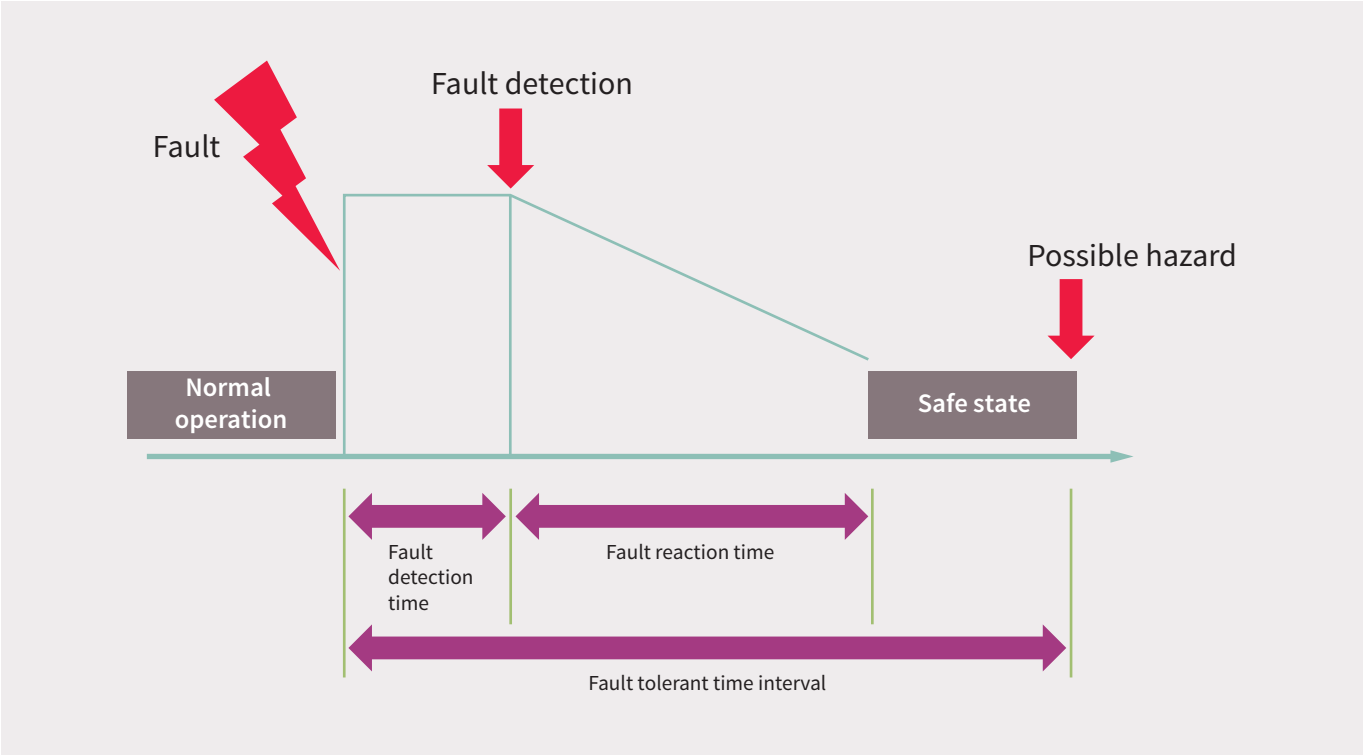

Figure 7: FTTI measures the time taken to return to a safe state after a fault condition

The worst case for the fault detection time is application specific and defined by the software diagnostic time interval. The hardware safety mechanisms within AURIX hardware provide for a very fast fault detection time which is significantly less than 1µs when operating at 100 MHz.

The high power gatedriver is another crucial element of the overall safety concept and contains a number of important safety features. A well known device that fulfils FuSa considerations for the inverter application is the 1EDI2002AS EiceDRIVER™ from Infineon.

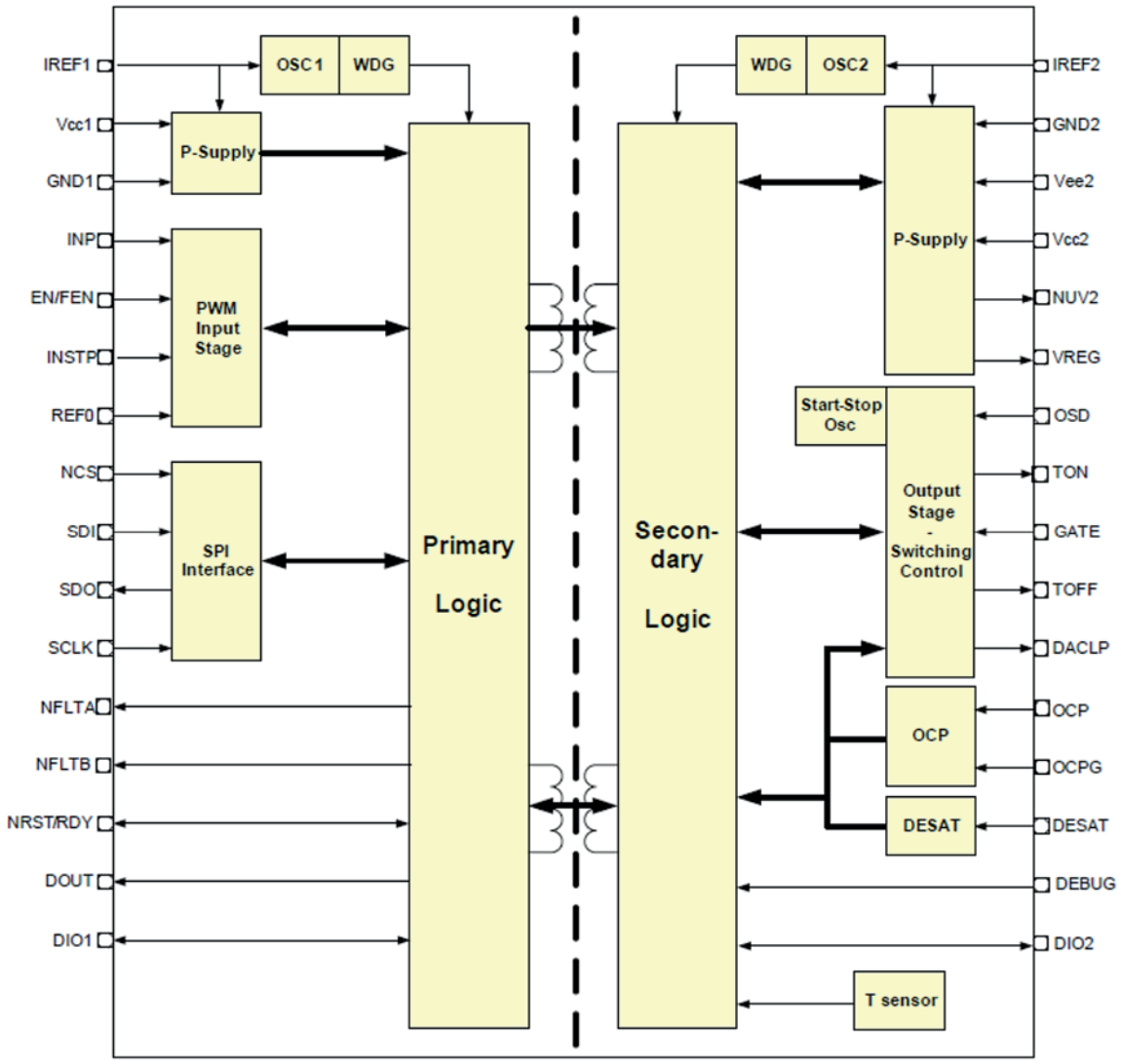

Figure 8: The 1EDI2002AS EiceDRIVER™ from Infineon contains several safety features

This IGBT driver provides on-chip Basic galvanic isolation and ensures faithful driving of the power module due to its low propagation delay and negligible PWM distortion. The AEC-Q100 qualified device contains several safety relevant features including gate signal monitoring which checks the IGBT gate voltage and signal waveform during the turn-on or turn-off sequence, current sense protection and support for active short circuit detection and strategies implementation such as output stage disabling to prevent cross current.

Perhaps one of the most critical component in terms of safety is the TLE35584 safety power supply.

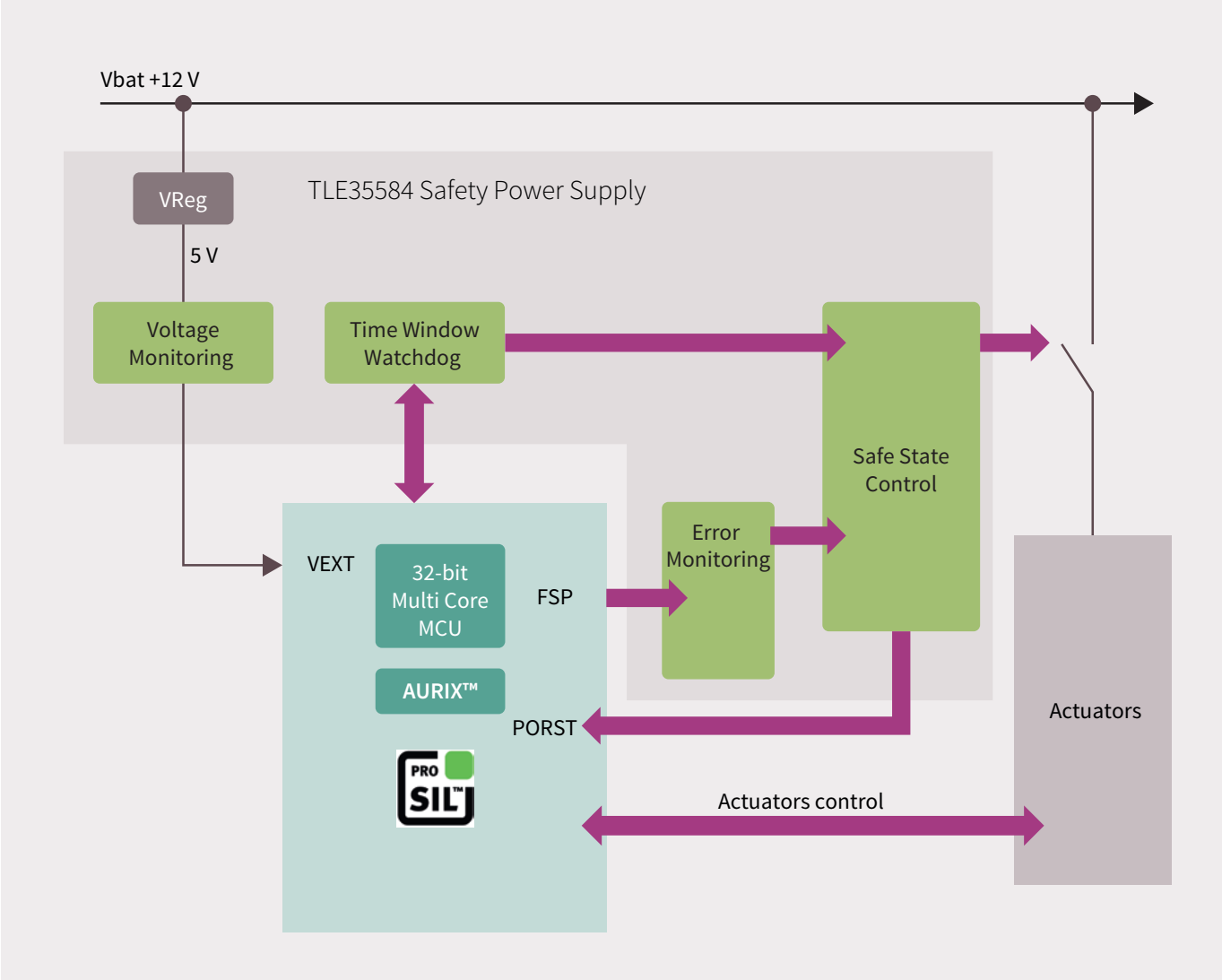

Figure 9: The safety power supply is heavily integrated into the FuSa system

One of the primary roles of this device is to monitor the voltage supplies of the system, internally generated by the device or from other on-board regulators, and, if necessary, disconnect the microcontroller from the power supply to avoid a violation of the safety goals. It is also capable of detecting dependent failures that affect both the function as well as the diagnostic (such as a watchdog error). Should this happen, then the safety power supply can initiate a return to a safe state by driving output pins to disconnect the power feed to the actuators and / or triggering a reset of the microcontroller.

The safety power supply also monitors the fault signalling pin (FSP) of the microcontroller that signals an internal failure, meaning that the MCU response is no longer reliable. In this case the power supply is the 'last man standing' and its built-in safe state controller triggers a safe state in order to meet the Safety Goals for the system.

As the building blocks of a FuSa system are reviewed and understood, the benefits of sourcing from a single supplier become immediately apparent. Each of the elements of the AURIX system are specifically designed and tested to work alongside each other and contain signals and controls that significantly ease the task of building a system capable of reaching ASIL levels.

6. Summary

Although at first, ISO26262 and FuSa may seem to be a challenging subject, this paper has shown that for two quite different systems (EPS and drivetrain inverter) the approach to delivering safety is, in fact, quite similar and uses similar hardware architectures in both cases.

For designers, selecting a solution set that offers high levels of integration and interoperability between the required hardware elements is half of the battle. The other half of the battle is not with the hardware, but with the support tools, documentation and other 'premium support' that is available from the semiconductor manufacturer. By selecting a solution such as Infineon's AURIX, designers can be sure that they are 'buying into' an established solution that has years of experience and know-how built in.