



FUNCTIONAL SAFETY WITH
POWER FET APPLICATIONS

More safety

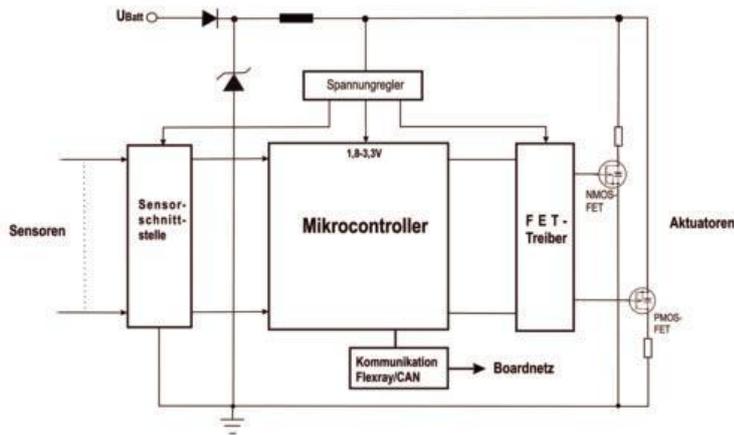
with functional safety

Realizing functional safety solutions in accordance with IEC 61508 and ISO 26262 affects the entire engineering procedure from the design of the ICs to processes and quality management. The new ISO 26262 standard aims to achieve a comparable and individual risk assessment for every single function in the automobile. This article outlines the situation with microcontroller platforms and their periphery and also examines the functional protective features of power FETs.

The majority of future innovations in the automobile will center around new electronics systems, such as electronic steering (x-by-wire), brake assist systems (BAS), electronic differential slipper (EDS) and also complete electric drives (hybrid/electric vehicle), for example. This in turn increases our dependency on an electronics setup that functions safely, reaching new heights in the hybrid or electric car. Up to now, constantly improved quality programs have managed to keep reliability at a high level – despite an increasing complexity of design and a great number of electronic subsystems built into each automobile. The use of electronics in safety-relevant functions, such as steering, handling, and automatic braking, demands that these processes function safely and cause no damage, even when simple failures occur. In 2004 it became imperative for reasons of liability that IEC 61508 be applied to all safety-relevant developments. As regards the automotive industry in particular, ISO 26262 governing functional safety is currently being standardized and is to come into force in the next two to three years. This new international standard has as its objective the documentation of a comparable and individual risk assessment for each and every function in a vehicle.

Intrinsically safe hardware

For many years now the design of safety ASICs/customized ICs has been characterized by the requirements of ABS and airbag systems and is state of the art. Yet if we take a look at microcontroller-based platforms for automotive electronics, the situation is very different. Figure 1 is a general block diagram showing an electronic control unit in a car. Besides the power supply from the battery, the microcontroller is the central unit processing local sensor signals, communication with other subsystems, and activation of the actuators via the power unit. Considerable progress has already been made in safety microcontroller software, design process management, and communication systems in automotive electronics with AUTOSAR, automotive SPICE/CMMI and FlexRay. A few microcontrollers have also already or soon will come onto the market which will be able to meet the demands of ISO 26262 to ASIL D (Automotive Safety Integrity Level D). As far as the design of the hardware is concerned, here several areas are currently in focus: voltage monitoring and the logical and functional monitoring of the sensors and transmission paths, followed by the faultless drive of the power unit. Sensors can be monitored both by the hardware and logically by the microcontroller software. Regarding transmission links, suitable protocols can help to reliably recognize faults and possibly rectify these. The design of power output stages is a particular challenge as, for example, a redundancy in the readback of the actuator state can be extremely cost-intensive.



© automotive

Figure 1: General block diagram of the electronic control unit in an automobile

Interface between the MCU and control unit

The goal is to safely operate the power unit using the output signals from the microcontroller. The trend towards increasingly complex microcontrollers with lower and lower power dissipation results in smaller supply voltages, lower core voltages, and slighter I/O voltages with a low load rating at the outputs. In complex microcontrollers, I/O voltages of 1.8 V to 3.3 V are now the norm. This counteracts the growing demands made of the power unit – and also long-term plans for a 48V vehicle power supply, intended to reduce currents and thus cable loss. Electronic drive, such as of the steering or brakes, can be extremely critical in the event of failure. Here, ISO 26262 defines four classes of risk (ASIL A to D), taking into account specific safety requirements and defining maximum permissible probabilities of failure. Risk reduction through technical solutions is also called for. In concrete terms, this means that critical faults must be detected and malfunctions should be actively prevented. The flawless activation of power FETs is thus of extreme significance. This naturally also applies to the FET driver, as this is the major link between the MCU and the power outputs. When designing the FET driver, it is important to include all of the design parameters. The following are typical:

- Error monitoring (losses from GND or the Vcc connections between the outputs)
- Drive power and startup behavior (e.g. 3-state for MCU I/Os)
- Required logic level shift (e.g. 1.8–5 V to 5 V or 10 V)
- Observations on power dissipation, current loads, and switching frequencies.

When looking at the functional safety of the driver, the chief concern is whether failures of the first order are detected and how the circuitry reacts to:

- Loss of the connection to ground due to defects on the printed board or in the components
- Loss of or fluctuations in the supply voltage
- Connections/short-circuiting between two outputs
- External burst transients
- Output overload and excessive temperature.



FMEA-Nr.: FMFLA1 Project: iC-MFL		Failure-Mode- and Effects-Analysis					iC-Haus		
Package: QFN24		Prepared by: Hz		Last revision date: 10.10.2007		Page 1 / 12			
FM-NR	Potential Effects of Failure	S	Potential Failure Mode	Potential Causes	Current Controls	O	Failure Detection Method	D	RPN
1	no effect	1	PIN 4 GNDR short to GND	Bondwire short to chipedge	SPC assembler	3	SPC assembler; optical inspection, electrical test	2	6
2	all OUTx = resistive lo (< 70 kOhm)	1	PIN 5 VCC open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compliance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4
				bond interruption	Compliance solderprocess parameters	3	Electrical test	1	3
			PIN 17 GND open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compliance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4
				bond interruption	Compliance solderprocess parameters	3	Electrical test	1	3
			PIN 4 GNDR short to PIN 5 VCC	Touched bondwires	SPC assembler	1	SPC assembler; optical inspection, electrical test	1	1
				Pin misalignment	SPC assembler; handle chips with care	2	SPC assembler; outgoing inspection, electrical test	1	2
				solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3	Optical inspection, electrical test	1	3
			PIN 5 VCC short to GND PIN 17 GND short to VCC PIN 4 GNDR short to VCC	Bondwire short to chipedge	SPC assembler	3	SPC assembler; optical inspection, electrical test	2	6
solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3		Optical inspection, electrical test	1	3			
solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3		Optical inspection, electrical test	1	3			
3	all OUTx= active lo (> 2 mA)	1	PIN 15 EN open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compliance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4

S = Severity O = Occurrence D = Detection Risk Priority Number RPN = Severity * Occurrence * Detection

FMFLA1.doc
Printed: 10.10.07

Figure 2: Excerpt from an FMEA.

© automotive

This evaluation automatically results in an FMEA or Failure Mode Effect Analysis. The aim here is to systematically document the possibilities and measures necessary to achieve functional safety according to IEC 61508 and ISO 26262.

Applying FMEA at driver level

An FMEA attempts to describe which functions the component has and which potential malfunctions or failures could occur. The cause and effect of a failure is analyzed and an assessment of the significance to the overall product and the user thereof is made. The question then has to be answered as to how probable it is that this failure will occur – and also how it can be detected and prevented to avoid any further damage. These detailed analyses are documented and become a composite part of the design planning of any integrated circuit. They are of course also integrated in the production process, IC testing, and the quality assurance of the product. By way of example, **Figure 2** gives the first page of an extensive FMEA for a FET driver. Avoiding a potential error is first and foremost, as is the reliable detection of such during production and in later operation. FMEA can be used to determine which potential errors are critical, how they can be pinpointed, and how the effects thereof can be avoided. This information directly affects the design of the subsequent IC.

FET driver as an example of functional safety

These specific safety measures shall now be explained in detail taking an IC model from a family of safe FET drivers by way of example. **Figure 3** gives the schematic drive circuit of an NMOS logic FET (such as an IRLZ44N), using iC-MFL as a driver. In the event of error the IC must prevent the NMOS logic FET being activated by a logic signal. With a failure of the first order, the drive output must thus stay at a safe LOW level. In addition to the basic functions, the level shift (from 1.8 V–3.3 V to 5 V), and the power FET input drivers, the design of iC-MFL is such that it safeguards against the following errors:

- Loss of ground or Vcc at the IC
- Open inputs (e.g. cable breaks or 3-state for the MCU I/O ports)
- Short-circuiting between two outputs.

The most critical situation is the loss of ground or of the supply voltage Vcc, in which standard FET drivers cannot guarantee a safe low at the outputs. In addition to the traditional VCC or supply monitor, a ground-monitoring facility has thus also been included in the device. If the ground connection is interrupted, without these measures no defined potential ratios would be available for the internal logic and the external FET would be activated via parasitic paths from the IC. The device thus has two grounds (GND and GNDR).

If one connection is broken, the monitor recognizes the fault and shuts down the output stages. If V_{cc} is interrupted, the outputs are also defined by an internal pull-down resistor with a value of about 30 k Ω that is connected to ground and thus switched to a safe operating mode. To increase safety, all inputs have been given Schmitt-Trigger stages and pull-down currents. In the microcontroller start phase, during which all I/O ports are 3-state, these pull-down currents ensure a defined input state of the FET driver. The FET driver outputs are active push/pull current sources, where the pull side connected to ground is stronger than the push side. If two outputs are short-circuited externally, where one drives a high level and the other a low, the low 'wins' and guarantees a low level. The outputs are overvoltage-proof to protect them against burst transients (18 V, 100 ms).

FMEA has also been carried out for the other instances of use, such as PMOS-FET drive circuits, for example, or for other input and output voltage ranges, in order to achieve the same single-failure protection. For both NMOS-FETs and PMOS-FETs there are safe driver devices available with an adjustable output voltage range of 5 V, 10 V and full scale. The above example merely describes the measures that safeguard against failure during operation and that are directly influenced by the IC design.

Outlook

As shown, putting functional safety systems into practice according to IEC 61508 and ISO 26262 affects the entire engineering process, from the design of the integrated circuits to the processes and quality management measures deployed. It inevitably leads to departments working together as a team and makes obvious the full extent of the time and effort required for development. Corresponding analyses are necessary in all other subareas of the electronics industry.

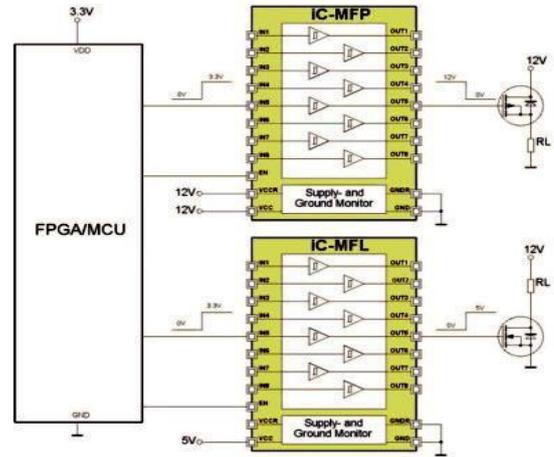


Figure 3: Safe power FET drive circuit.

© automotive

The same naturally also applies at complete system level, such as for steering or braking systems, for example. It is to be expected that functional safety will increasingly establish itself as a standard in both the automotive sector and in the industrial environment. (oe)



Dipl.-Ing. Thomas Franken is an IC designer specialized in FMEA design at iC-Haus GmbH.

iC-Haus: <http://www.ichaus.com/fmea>