FuSa in a Nutshell - Introduction to functional safety

About this document

Scope and purpose

As requirements from functional safety standards in automotive, industrial and other fields are a challenging subject, this document intends to provide a first set of guidelines for users who are unfamiliar using Infineon microcontrollers unit (MCU) and other complex chips in a functional safety scope.

This application note is part of a series of document named “FuSa in a nutshell” and listed in [3].

Intended audience

This application note is intended for all those evaluating Infineon MCUs and other complex chips, including functional safety engineers on the customer side and application engineers. This includes designers of safety-related systems who:

- Are new to functional safety
- Want to know more about functional safety (also called “FuSa”) applications
- Want to understand in principle how functional safety can be implemented with hardware support
- Are looking for functional safety details that cannot be found in the user manual of the product

Structure of the document

To explain how to proceed when facing functional safety aspects using Infineon products, the following sections provide a brief introduction to basic safety concepts.

Disclaimer

This series of documents named “FuSa in a nutshell” are for training purposes only and are not to be taken as a blueprint for productive development.

Table of contents

1 Introduction to main safety concepts

1.1 Functional safety

Functional safety defines an entire domain of modern industrial activities. In general, safety is used in relation to situations that can cause harm to humans or generally, the risk of physical injury or damage to the overall health of people (that is, a safe system will not cause harm to humans). In general, no system can be created completely safe, so the functional safety domain focuses on reducing the risk of harm to an acceptable level. The acceptable level is society-dependent and can be differently evaluated depending on the social context.

Functional safety is described as follows:

- In the umbrella standard (IEC 61508:2010):

As part of the overall safety that relates to the following:

  - Equipment under control (EUC)
  - Control system of the EUC that depends on the correct functioning of the Electric/Electronic/Programmable (E/E/PE) safety-related systems
  - Other risk reduction measures

- In the automotive standard (ISO 26262:2018):

Absence of unreasonable risk due to hazards caused by the malfunctioning behavior of E/E systems.

The electronic components are clearly mentioned in the above two definitions; therefore, this domain is relevant to semiconductors.

The functional safety process starts with a hazard analysis and risk assessment (HARA) of the relevant system or subsystem 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/appliance or of the automated action in general.

To each of these goals, a corresponding safety integrity level (SIL) as specified in the umbrella standard IEC 61508 is assigned based upon the risk evaluation. In the automotive domain, the acceptable risk level is called Automotive Safety Integrity Level (ASIL).

From the system level, the safety goals are translated into safety requirements for subsystems and individual hardware components. Once the design is complete, verification is carried out by a combination of the component manufacturer and the system manufacturer following the ‘V’-model.

1.2 Systematic and random faults

Faults in a functional safety system can be broadly classified into the following two categories:

- Systematic faults: A fault in design or manufacturing that can be present in hardware and software. The existence of systematic faults can be reduced through continual and rigorous process improvement and robust analysis of any new technology or component.
- Random faults: A fault of a hardware element that follows a probabilistic distribution. Random faults are limited to hardware. The rate of random faults cannot be reduced. It is important to keep the focus on:
  - Prevention measures such as process and design (for example, layout rules)
  - Detection and mitigation by safety mechanisms (for example, ECC, redundant data storage)

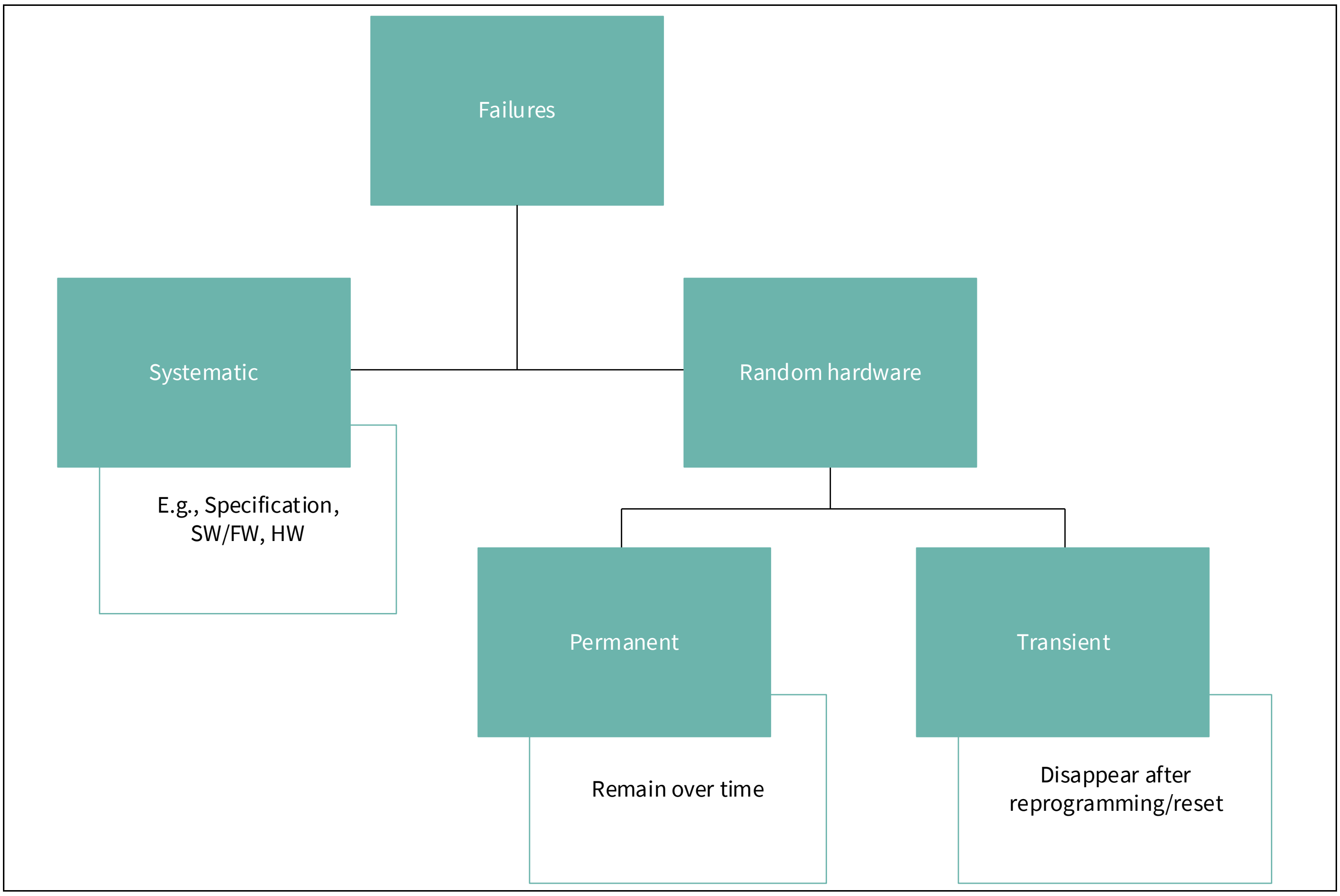

Figure 1 Faults classification

Random hardware faults can be permanent or transient. If the fault is permanent, it will stay there over time.

In case where errors are transient, they can be removed by writing or resetting or setting a new value. In Figure 2, it is possible to find a simplified representation of the major cause of transient faults in semiconductors. Alpha and neutron particles cause transient faults that need to be considered when determining the failure rate of a chip.

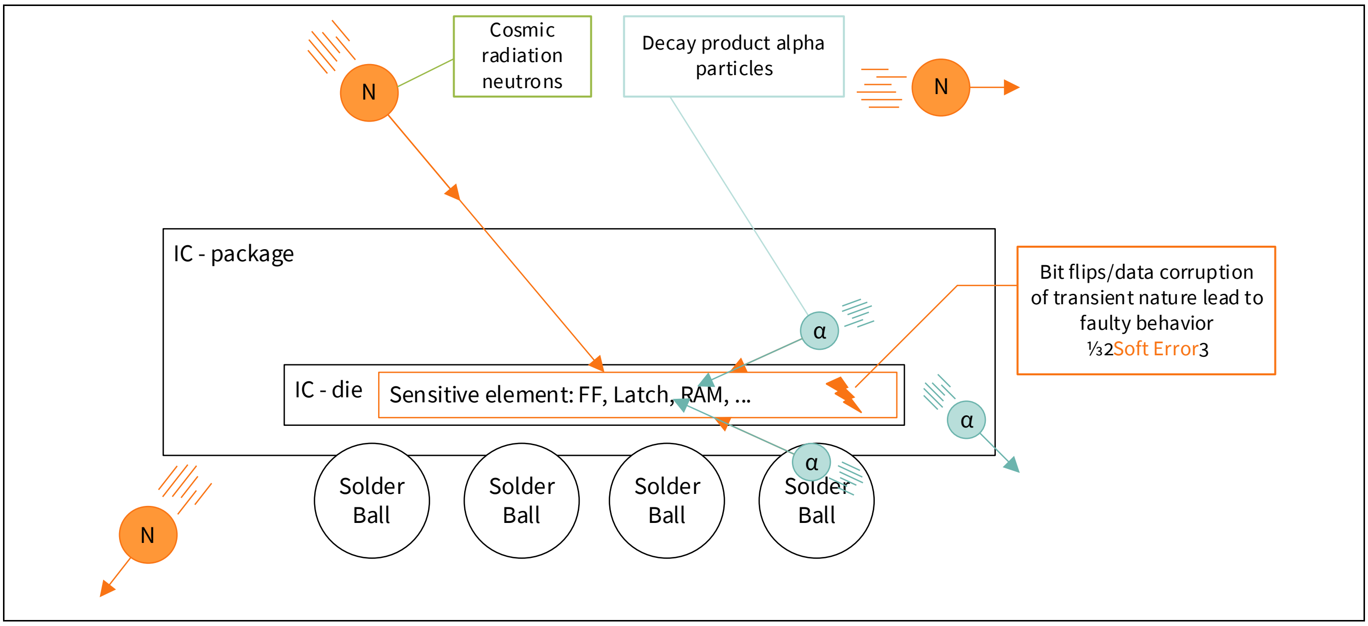
Cosmic radiation neutrons
Decay product alpha particles
N
N
N
IC - package
IC - die
Sensitive element: FF, Latch, RAM, ...
α
α
α
Bit flips/data corruption of transient nature lead to faulty behavior
⅓2Soft Error3
Solder Ball
Solder Ball
Solder Ball
Solder Ball

Figure 2 Alpha particles and neutron particles as possible causes of transient failures

1.3 ISO 26262 and IEC 61508 standards perspective

AURIX™ TC3xx was initially developed for automotive systems and is compliant with the ISO 26262:2018 standard. At the same time, compliance with IEC 61508:2010 was also assessed.

Table 1 summarizes the main differences between the two standards relating to their applicability to AURIX™ TC3xx.

Table 1 ISO 26262 and IEC 61508 standards applicability to AURIX™ TC3xx

Section	ISO 26262	IEC 61508
Application field	12-part standard that is strictly for on-road vehicles, such as passenger cars, trucks, buses and motorcycles, covering the concept up to the production stage for electrical/electronic systems. This standard is tailored to the needs of the automotive industry. Originated from IEC 61508 for automotive.	7-part industrial-related standard; most often used for machinery, oil wells, chemical plants, nuclear sites, forklifts and robots. This standard refers to industrially relevant technical standards for EMC, communication and cybersecurity.
Safety classification	Classification is based on Automotive Safety Integrity Levels (ASIL). ASIL: A (least stringent), B, C, D (most stringent)	Classification is based on Safety Integrity Level (SIL). SIL: 1 (least critical), 2, 3, 4 (most critical)
Functional Safety	definition is in ISO 26262-1:2018 clause 3.67	definition is in IEC 61508-4:2010 clause 3.1.12
Areas covered	it covers safety management, system/HW design, SW design, production and operation	Covers safety management, system/HW design, SW design, production and

Section	ISO 26262	IEC 61508
	of safety-critical E/E/PE systems, but the same is valid for components.	operation of safety-critical E/E/PE systems.
"Components" view	Automotive systems distinguish system design from hardware component design. "Components" used in the system require specific compliance with the ISO 26262 standard. One life cycle for all (tailoring concept). ISO 26262-11 is specific for semiconductor development.	A hardware component compliant with IEC 61508 is called a "compliant item". The HW component life cycle is introduced for "ASICs". ISO 61508-2 Annex E and F are for semiconductors.
How safety is implemented	The safety goal concept requires risk reduction to be a part of the initial control system design.	The safety function concept was initially based on the idea of defining equipment under control (EUC) and then building risk reduction measures for the system.
Documentation	ISO 26262 clearly defines work products for each requirement. Confirmation reviews with independent reviewers, dependent on ASIL, are requested.	General considerations on documentation are reported in Part 1, Clause 5. No confirmation reviews are requested; only assessments with independent assessors. Relating documents to be provided, there are less detailed requirements (no WPs).
SIL and ASIL determination	To determine the ASIL level of a system, a risk assessment must be performed for all hazards identified. Risk comprises three components: severity, exposure and controllability.	The SIL level of a product is determined by three factors: **Systematic capability rating**: If the quality management system meets the requirements of IEC 61508, a SIL capability rating is issued. **Architectural constraints for the element**: Architectural constraints are established by Route 1H or Route 2H. Route 1H involves calculating the Safe Failure Fraction for the element. **PFH (or PFDavg) calculation for the product**: **PFH** is the average frequency of a dangerous failure of the safety function [h-1] for high demand mode of operation or continuous mode of operation, while **PFDavg** is the average probability of a dangerous failure on

Section	ISO 26262	IEC 61508
		demand of the safety function operating in low demand mode of operation.
Corresponding terms	**Item** Defined in ISO 26262-1:2018 respectively at clause 3.41	**Functional unit** Defined in IEC 61508-4:2010 respectively at clause 3.4.5
Corresponding terms	**Element, Fault, Failure** Defined in ISO 26262-1:2018 respectively at clause 3.41, clause 3.54 and clause 3.50	**Element, Fault, Failure** Defined in IEC 61508-4:2010 respectively at clause 3.4.5, clause 3.6.1 and clause 3.6.4
Decomposition versus synthesis	ASIL decomposition is defined in ISO 26262-1:2018 clause 3.3 An ASIL D safety requirement can be decomposed as: ASIL D (D) + ASIL QM (D) or ASIL C (D) + ASIL A (D) or ASIL B (D) + ASIL B (D)	According to IEC 61508-2:2010, SIL synthesis essentially allows the synthesis (or combining) of two redundant elements with a systematic capability of ‘N’ to have a systematic capability of ‘N + 1’, with ‘N’ less than or equal to SIL 3. The rules for SIL synthesis according to IEC 61508 are: • SIL 2 + SIL 2 gives SIL 3 • SIL 1 + SIL 1 gives SIL 2 The IEC 61508 standard does not allow recursive SIL synthesis and in addition, the two combined elements should have the same SIL. IEC 61508 also requires a two-channel implementation for SIL 4 systems (the hardware fault tolerance has to be >0 for a SIL 4 function).
Failure rate (λ) Expressed in FIT (see Section 1.6)	$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}$	$\lambda = \lambda_{S} + \lambda_{D} = (\lambda_{SD} + \lambda_{SU}) + (\lambda_{DD} + \lambda_{DU})$
Definitions for the different component of failure rate	λ_{SPF} – Single-point faults λ_{RF} – Residual faults λ_{MPFDP} – Detected/perceived multi-point faults λ_{MPFL} – Latent multi-point faults $\lambda_{MPF} = \lambda_{MPFDP} + \lambda_{MPFL}$ – Multi-point faults λ_{S} – Safe faults Expressed in FIT	λ_{S} – Safe failure rate: No impact on safety function λ_{SD} – Safe detected failure rate – λ_{SU} – Safe undetected failure rate • λ_{D} – Dangerous failure rate – Impact on safety function – λ_{DD} – Dangerous detected failure rate – λ_{DU} – Dangerous undetected failure rate Expressed in FIT

Section	**ISO 26262**	**IEC 61508**
Metrics	In automotive systems, metric targets are mandatory on the item level and are related to both single- and multi-point faults.	In IEC 61508 metrics, the most relevant factors are single-point faults, even if they include common cause evaluation through a β factor.
Probabilistic metrics	**Probabilistic Metric for Random Hardware Failures (PMHF)**: Quantitative criteria for the residual risk of a safety goal violation due to random hardware failures. In simple terms: A metric to show the robustness of a safety architecture. $\mathrm{PMHF} = \lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}}$ $+ 0{,}5 \times \lambda_{\mathrm{SM1,\ DPF,\ latent}} \times \lambda_{\mathrm{IF,\ DPF}} \times T_{\mathrm{lifetime}}$ Expressed in FIT	**In an architecture without redundancy (1oo1)** $\mathrm{PFH} = \lambda_{\mathrm{DU}}$ PFH definition is in IEC 61508-4:2010 clause 3.6.19 Expressed in FIT
Similar metrics terms	**Single Point Fault Metric (SPFM)**: Quantitative criteria for the effectiveness of the safety architecture to cope with single-point and residual faults. In simple terms, metric for the share of remaining dangerous faults in relation to all faults. Expressed in percentage	**Safe Failure Fraction (SFF)**: Ratio of safe and dangerous (but detected) failures in a system safety function to the total failure rate. SFF exact definition is in IEC 61508-4:2010 clause 3.6.15 SFF is calculated at the element (component) or system level for a safety function. It should not be applied to sub-elements. Expressed in percentage
Metrics terms unique to ISO	**Latent Fault Metric (LFM)**: Quantitative criteria for the effectiveness of the safety architecture to cope with latent dual-point faults. In simple terms: A metric for the share of remaining critical latent faults in relation to all dual-point faults. Expressed in percentage	
Terms unique to IEC		**Low-demand** mode safety functions are required to operate at low frequencies, typically once or more per year. Low-demand functions have less stringent requirements on PFDavg (the average probability of a dangerous failure on demand of the safety function) to achieve a specific SIL.

Section	ISO 26262	IEC 61508
		High-demand mode safety functions are required to operate at high frequencies, typically many times per hour. High demand and continuous demand functions have more stringent requirements on PFH (average frequency of a dangerous failure of the safety function) to achieve a specific SIL. **Continuous-demand** mode safety functions operate continuously. For more details refer to IEC 61508-4:2010 clause3.5.16 **Type A products** are simple products in which all failure modes are known. For more details refer to IEC 61508-2:2010 clause 7.4.4.1.2. **Type B products** are complex products in which not all failure modes are known (for example, semiconductor). For more details refer to IEC 61508-2:2010 clause 7.4.4.1.3. **Hardware Fault Tolerance (HFT)** HFT is the number of faults that can occur without failure of the safety function. A hardware fault tolerance of N means that N+1 is the minimum number of faults that can cause a loss of the safety function. For more details refer to IEC 61508-2:2010 clause 7.4.4.1. For AURIX™ TC3xx, HFT is equal to 0. This means that the fault might be detected, but safety functionality is lost with one fault. With a hardware fault tolerance of 0 (in other words, 1oo1 redundancy), the maximum safety integrity level that can be achieved by a Type B (complex semiconductor) safety-related element is SIL 3. HFT > 0 requires redundancy.

Section	ISO 26262	IEC 61508
Fault Tree Analysis	A Fault Tree Analysis or equivalent top-down analysis is required in the case of ASIL C and ASIL D.	A Fault Tree Analysis or equivalent is only “R” (recommended) in IEC 61508.
Dependent Failure Analysis	DFA is the analysis to identify single events that can cause multiple sub-parts to malfunction (for example, intended function and its safety mechanism) and lead to a violation of a safety requirement or safety goal. DFA is qualitative in automotive standard.	DFA is quantitative and faults in the diagnostic circuit can contribute to FMEDA metrics with the so-called beta factor.

1.4 Safety Element out of Context (SEooC) in automotive

AURIX™ TC3xx is an MCU developed for various applications.

Since it is not tailored for a specific item, according to automotive safety standard ISO 26262 part 10, the AURIX™ TC3xx is a Safety Element out of Context (SEooC) hardware component.

As ISO 26262-10:2018 highlights, the development of an MCU starts with an assumption of system-level attributes and requirements. It is the responsibility of the system integrator to integrate the SEooC assumptions of use.

According to the ISO 26262 classification, the MCU is a hardware component that performs a set of functions at the item level as a part of a system. A system, as it is defined in ISO 26262-1, is composed of at least three related elements: a sensor, a controller and an actuator. Figure 3 shows the typical use of the AURIX™ TC3xx in the context of an electronic control unit (ECU).

- Inputs are provided by one or more sensors at the system level, processed by the HW components on the ECU and forwarded to the input channels of the MCU.
- The MCU processes the data and provides outputs to other hardware components.
- Hardware components drive one or multiple actuators or transmit data to another ECU via a communication network.

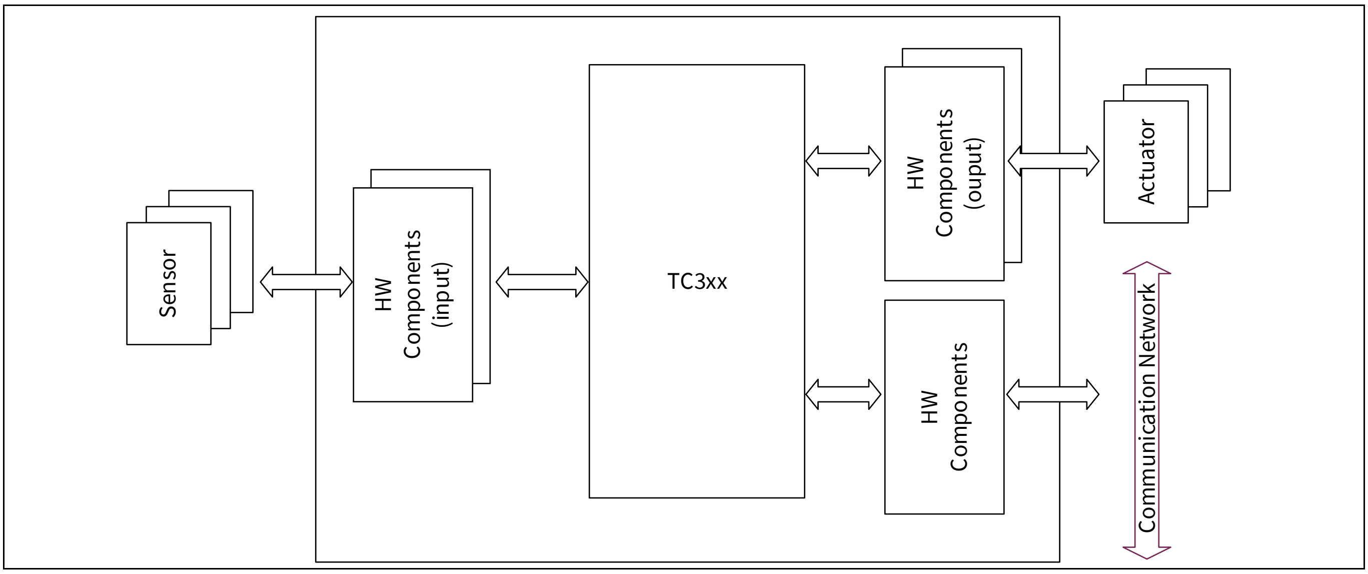

Figure 3 AURIX™ TC3xx in the context of an electronic control unit (ECU)

1.5 Fail-safe system

A system is said to be fail-safe if it is designed such that in the event of a failure of any element of the system, the system prevents harm to humans.

This is accomplished by having the system enter a safe state if any safety-relevant failure occurs or if it detects a "latent" failure that cannot be corrected immediately.

1.6 Failure rate

Failure rate is the frequency or rate with which a system or component fails, expressed in failures per hour.

Symbol: λ(lambda)

Unit: 1 FIT = 10^{-9} h^{-1} (failure in time)

Failure rates scale depending on time and the number of systems or components.

Examples of different meanings of 1 FIT:

- If there are 10^{9} systems or components, one of them will fail every hour.

or

- If there are 10^{5} systems or components working 10^{4} hours consecutively, one of them will fail.

1.7 Fault-related timings

1.7.1 ISO 26262 perspective

One of the key metrics for a functional safety system is the time to reach a safe state after a fault occurs.

This period, known as the Fault Handling Time Interval (FHTI), is the sum of two elements:

- Fault detection time (FDTI)

- Fault reaction time (FRTI)

A more commonly used term, similar to FHTI, is the Fault Tolerant Time Interval (FTTI) , which is defined in ISO 26262-1:2018 clause 3.61 and provides the minimum time before a system could become dangerous when a fault occurs.

Figure 4 shows a graphical representation of the relationship between these timings.

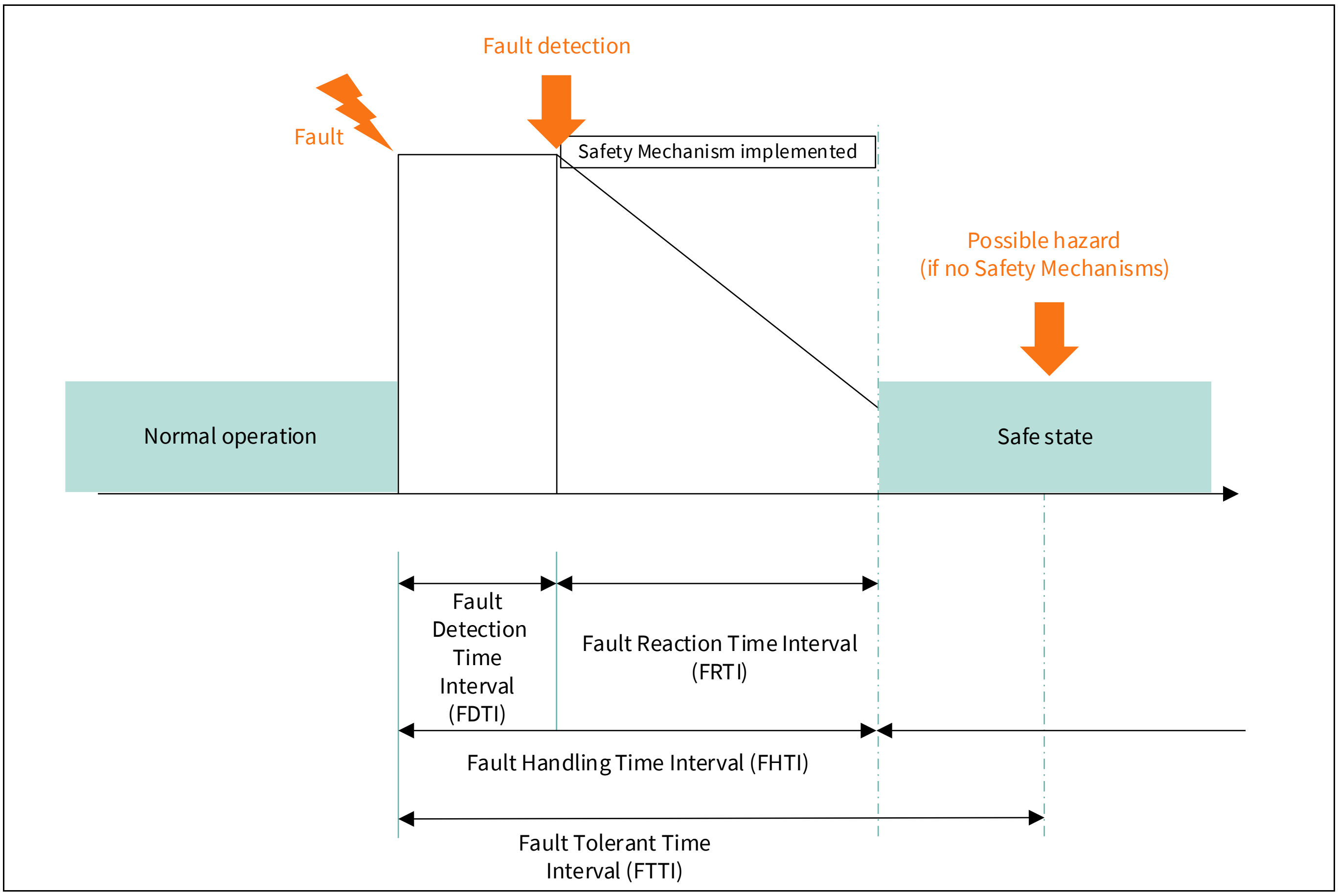
Fault detection
Fault
Safety Mechanism implemented
Possible hazard
(if no Safety Mechanisms)
Normal operation
Safe state
Fault Detection Time Interval (FDTI)
Fault Reaction Time Interval (FRTI)
Fault Handling Time Interval (FHTI)
Fault Tolerant Time Interval (FTTI)

Figure 4 Fault Tolerant Time Interval

The worst case for the fault detection time is application-specific and defined by the diagnostic time interval. All hardware safety mechanisms within AURIX™ TC3xx hardware provide a very fast fault detection time, in the order of microseconds.

1.7.2 IEC 61508 perspective

A term corresponding to FTTI in the IEC 61508 standard is the “process safety time”. This time is defined in IEC 61508-4:2010 at clause 3.6.20. In general, the time to react to a fault is longer in industrial applications with respect to automotive ones.

1.8 Protective measures

When the need for a protective measure is identified and the classification is determined, the measure must be implemented in the system.

Safety systems can have various principles of operation, for example:

- One single device is inherently fail-safe (so without integrated primary or secondary protection).
- One single device with periodic self-testing and monitoring, where the control layer and primary and secondary protection layers are integrated into one single device.
- Two independent devices are compared using the same or different technology. Secondary protection is provided by the comparison.

1.8.1 Single device, inherently fail-safe

Electronic fail-safe devices can include fuses, circuit breakers or current-limiting circuits, which interrupt electrical currents under overload conditions. As a result, they directly prevent damage to wiring or circuit devices.

1.8.2 Single device with periodic self-testing and monitoring

One of the most common safety architectures is what some industrial standards call a “single device with periodic self-testing and monitoring”. In this architecture, protective measures can be implemented in a number of layers, as shown in Figure 5.

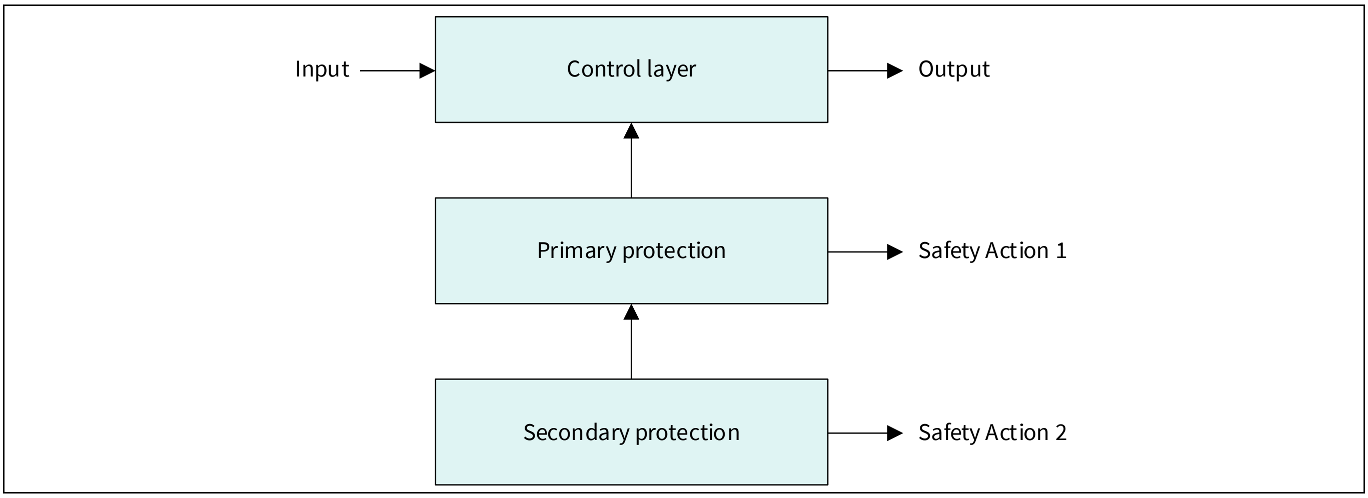

Figure 5 Layers of safety systems in the case of a single device with periodic self-testing and monitoring

Safety-classified functionalities that will lead directly to a hazard are implemented through a control layer plus a primary and secondary protection layer. This means that the system needs to be safe even when two independent faults occur.

The worst case is when two faults happen, one in the control layer and another in the primary protection layer, at a time distance that depends on the acceptable risk for the system (normally 12–24 hours in the most restrictive case). Statistically, it is considered that there is a very low probability that more than two independent faults occur.

The functional layer is intended as the component necessary for the control tasks such as receiving signals from sensors and sending control signals to actuators. This is referred to as the “control layer”. In the absence of any protective measures, failures in combination with normal conditions in the control layer can directly lead to a hazardous situation, such as sending a spurious control signal to operate a valve. Such failures are considered “critical failures”.

A second layer is necessary to implement safety measures to detect critical failures. These measures can be considered as forming the second functional layer (primary protection), whose task is to initiate a protective action in the event of a critical failure in combination with all defined “normal conditions”.

Faults that remain without leading to a critical failure are considered latent faults. Latent fault diagnostics can be executed with a lower frequency with respect to faults leading to safety-critical failures. This kind of fault, normally occurring in the protective function, nevertheless leads to a hazardous situation, even years later, in combination with a second fault.

It will be necessary to incorporate safety measures that prevent such a situation. To prevent a dropout of primary protection due to a latent fault, the proper functioning of the “safeguards” is supervised. The necessary function can be considered a third functional layer (secondary protection).

By implementing primary and secondary protection layers, a function with a high safety rating can be realized.

1.8.3 Two independent channels with comparison

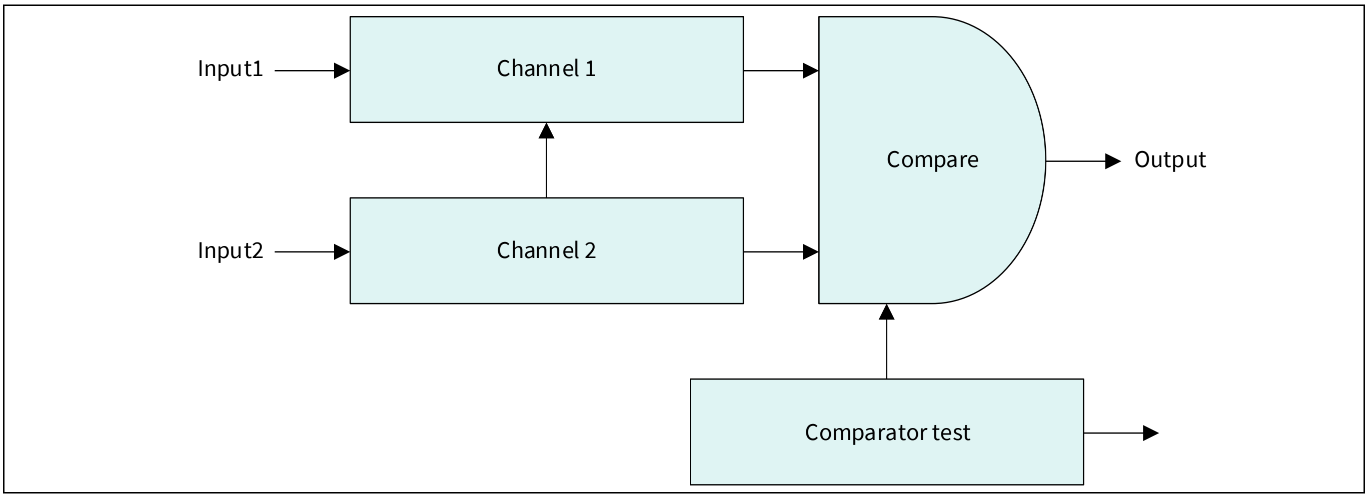

Figure 6 Layers of a safety system using two devices with comparison

When adopting the technique of two independent channels with comparison, these two can use the same or different technology targeting the same function. In other terms, it includes homogeneous redundancy or redundancy with diversity.

When applying diversity to a system, it is not necessary to use hardware components from different manufacturers; the goals can also be achieved by using components from a single manufacturer.

This approach is limited to detecting that there is a fault but not determining where the fault is, as opposed to redundant systems with higher number of instances where the majority of voters will determine which channel is faulty (this is, for example, the case of at least two channels giving the same information over three channels present).

The final layer of protection is then provided by the comparator. The comparator itself will be guaranteed in its functionality; therefore, tests need to be run on the comparator to detect faults leading directly to a hazard or to cover latent faults. The comparator itself should also be free from systematic faults as per the rest of the system.

References

[1] ISO 26262:2018 Road vehicles - Functional safety

[2] IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

[3] AN1000 - FuSa in a Nutshell - release note

Glossary

Table 2 Glossary

Definition	Description	Notes
Architectural Element	The smallest element on which the FMEDA is performed	
ASIL	Automotive Safety Integrity Level; refer to ISO 26262-1:2018, 3.6	
CCF	Common-Cause Failure; refer to ISO 26262-1:2018, 3.18	
DC	Diagnostic Coverage; refer to ISO 26262-1:2018, 3.33	
DFA	Dependent Failure Analysis identifies single events that can cause multiple sub-parts to malfunction (for example, intended function and its safety mechanism) and lead to a violation of a safety requirement or safety goal.	
DPF	Dual-Point Failure; for the definition refer to ISO 26262-1:2018, clause 3.38	
ECU	Electronic Control Unit	
FHTI	Fault Handling Time Interval is defined in ISO 26262 as the sum of three elements: The fault detection time, the fault reaction time and the time for the system to reach a safe state.	
FTTI	Fault Tolerant Time Interval; for the definition refer to ISO 26262-1:2018, clause 3.61	
FMEA	Failure Mode and Effects Analysis	
FMEDA	Failure Modes, Effects and Diagnostic Analysis Analysis of the effect of random hardware faults on a safety requirement or safety goal, including quantitative estimation of failure rates and the probability/rate of a safety goal violation	Quantitative Bottom-up HW only
FTA	Fault Tree Analysis Analysis in which a top-level failure mode is broken down to a combination of lower-level faults (root causes) using a Boolean logic approach	Qualitative (may be quantitative) Top-down HW only
HARA	Hazard Analysis and Risk Assessment; Refer to ISO 26262-1:2018, 3.76	
HW	Hardware	
IC	Integrated Circuit	
IEC	International Electrotechnical Commission	
ISO	International Organization for Standardization	
MCU	Microcontroller unit	
SW	Software	

Revision history

Document revision	Date	Description of changes
V1.00	2024-09-12	Initial release

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2024-09-12

Published by

Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference
AN1001

Important notice

The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.