SAFETY

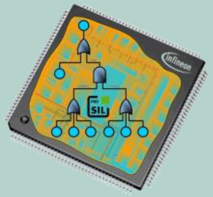
Safety Concept

AURIX™ TC3xx Microcontroller Training
V1.0 2020-09

Please read the Important Notice and Warnings at the end of this document

SAFETY
Safety Concept

Hardware designed for functional safety



Safety Documentation

External Safety Mechanisms

ISO 26262 part of Infineon‘s standardized development process

Highlights

- AURIX™ was developed as a Safety Element out of Context (SEooC) fulfilling the applicable objectives of ISO 26262 up to ASIL D

Key Features

ISO 26262 standardized development process

Hardware safety mechanisms

Safety documentation

Customer Benefits

- Support ISO 26262:2011 compliant applications development
- Supports protection against random faults as described in safety manual
- Accelerates the development of safety critical applications

SAFETY

ISO 26262 standardized development process

The scope of the SEooC comprises:

- The AURIX™ microcontroller hardware component
- Assumptions of use (AoU) related to the software elements that
  - support the integration to the AURIX microcontroller hardware components in a safety-related application
  - support the single point fault metric up to ASIL D for software applications target to utilize non-lockstep CPU core.
- Assumptions of use related to the hardware environment including assumed external safety mechanisms
- Assumptions of use related to the software environment
- Assumptions of use related to the use of the safety mechanisms provided by the SEooC

All of the above support the development of safety critical applications which are ISO 26262:2011 compliant.

SAFETY
Hardware safety mechanisms

Safe computing:

- Delayed Lockstep CPU with diverse layout

Safe data and code storage:

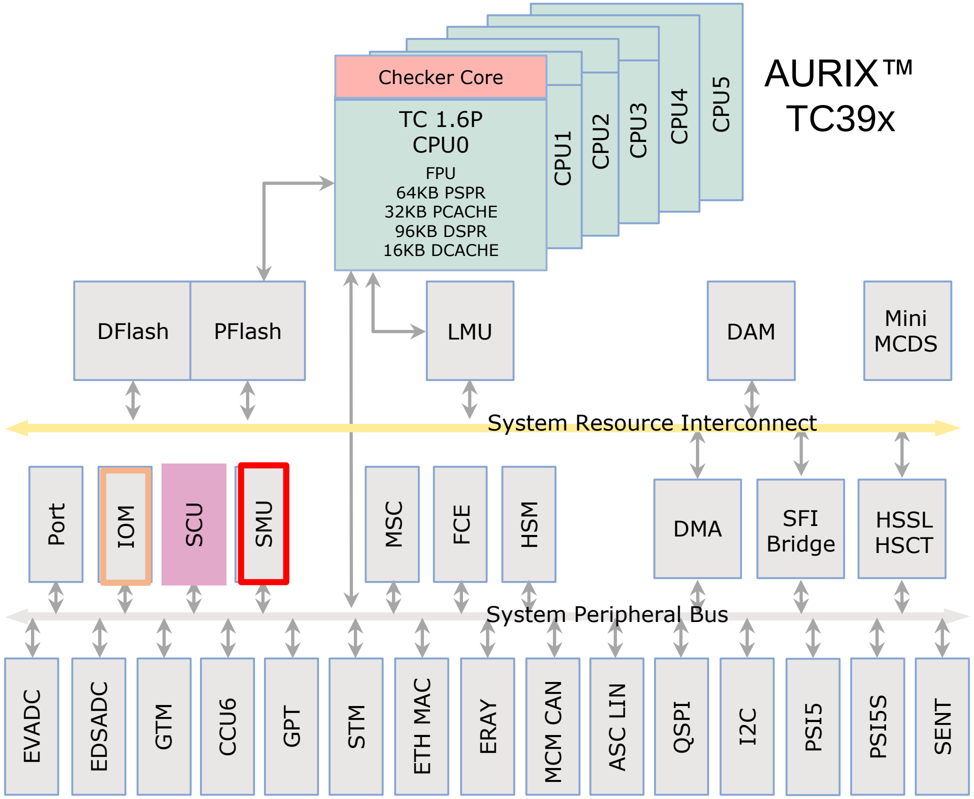
- Error Detection Codes ECC for RAM and Flash memories
- Memory Protection Unit MPU for code and data

Safe intra chip communication:

- SRI Cross Bar: End-to-End monitoring of data and address failures using ECC

Safe infrastructure:

- Clock frequency range monitors
- Power supply range monitoring
- Internal watchdog timers



Support for coexistence of elements:

- CPU Memory Protection
- Bus Memory Protection
- Register Access Protection

Safety management unit:

- Configurable error handling

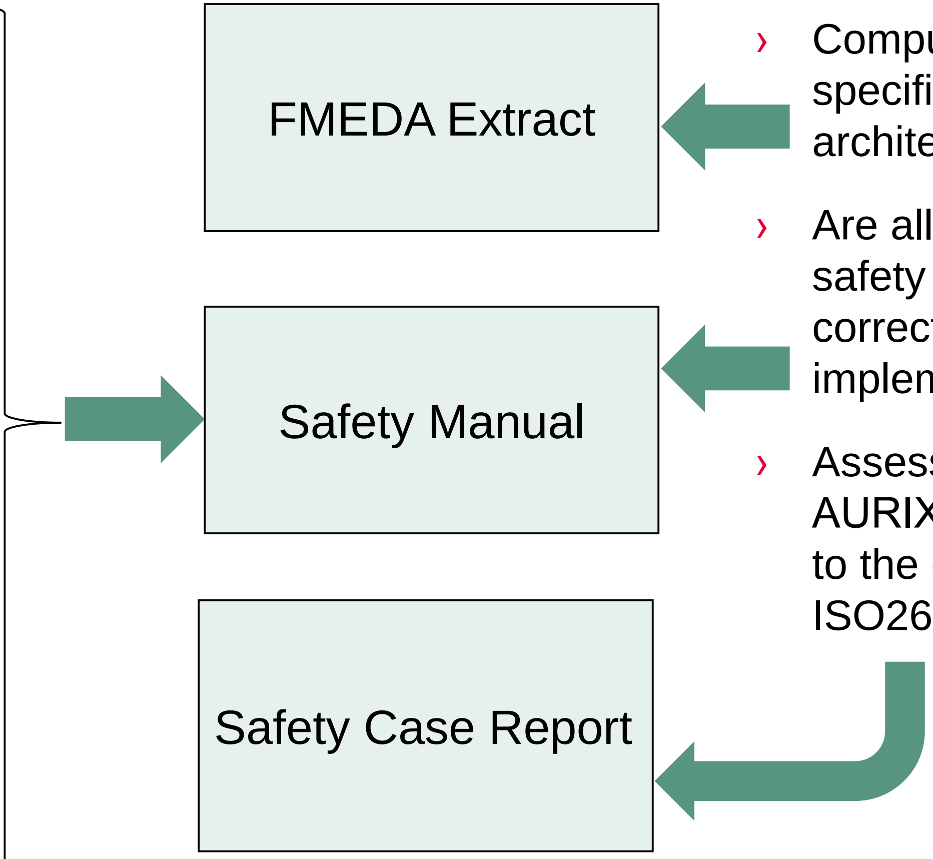
I/O Monitor:

- Flexible logic analyzer to monitor or compare digital signals

SAFETY
Safety documentation

System/Software Engineers

- › Which safety mechanisms are available in AURIX™ TC3xx hardware and how to use them?
- › Which external safety mechanisms are required?
- › Which safety mechanism shall be implement at the application-level?
- › How to monitor application dependent parts and which ones are independent?

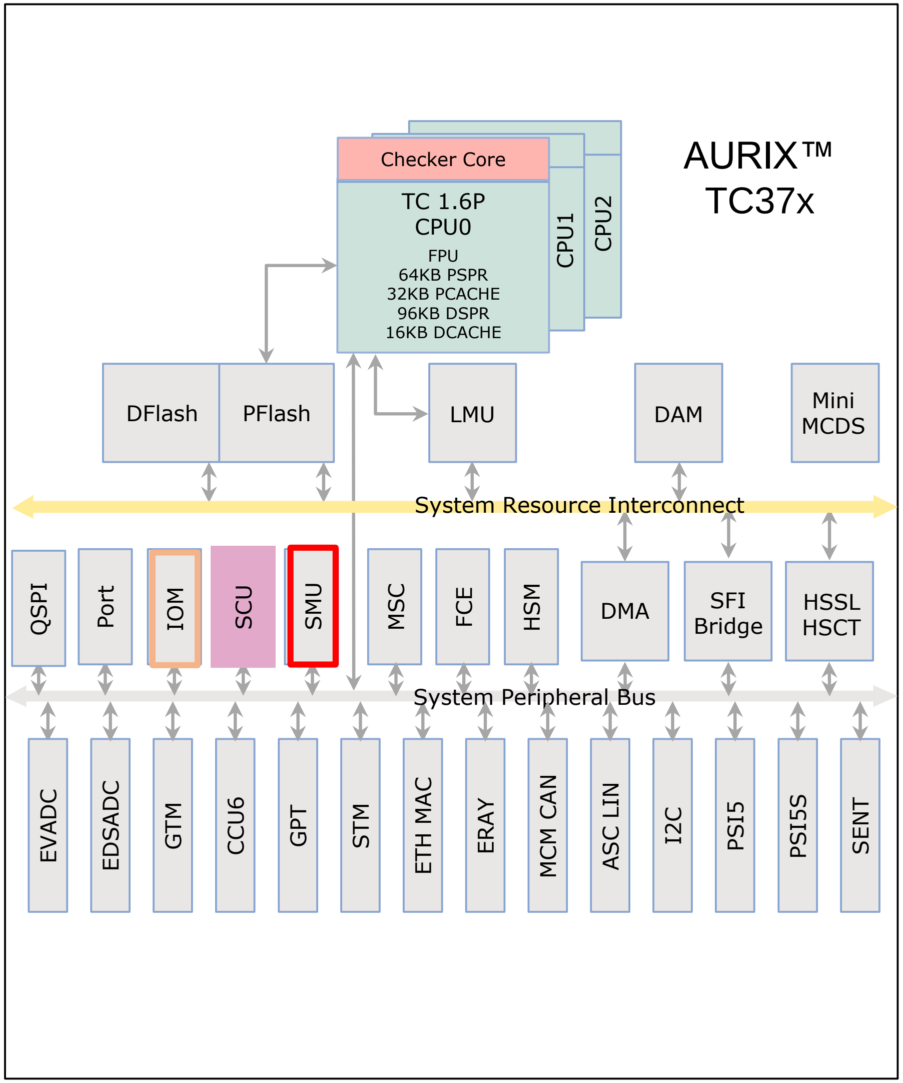


Functional Safety Managers/Engineers/QM

- › Computation of project specific hardware architectural metrics
- › Are all the required safety measures correctly implemented?
- › Assessment of AURIX™ compliance to the objective of ISO26262

SAFETY
System integration

- Safety as a concept is an integrated part of the AURIX™, nonetheless there are aspects that are application dependent such as:
  - Ensuring redundancy over the analog and digital Inputs / Outputs and over communication protocols
  - Configuration of individual modules (e.g. peripherals) in a safe manner
  - Implementation/Fulfillment of AoU according to the Safety Manual as applicable for respective application



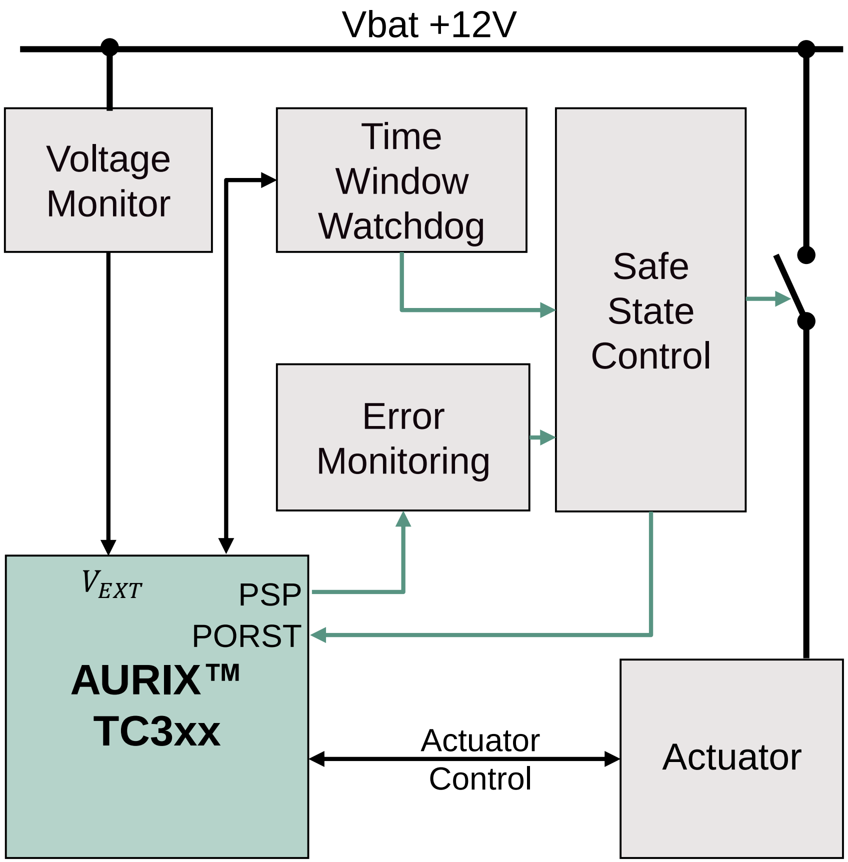
Application example
External safety mechanisms

Overview

- AURIX™ can manage different fail scenarios such as detecting under/over voltage of the external supply, dependent failures which cause the diagnostic system to fail too

Advantages

- For all these fail scenarios, recommended reactions can be implemented, such as bringing the system in its safe state
- Well defined reaction systems ensure that the faulty behavior of external components will not produce malfunctions



Note: the grey blocks represent functions to be allocated to external devices, not hardware components.

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

Edition 2020-09
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Email: erratum@infineon.com

Document reference
AURIX_Training_2_Safety_Concept

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie") .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, 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.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

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.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

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.