

SAFETY
Safety concept

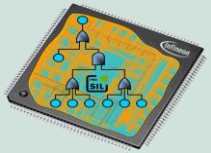
AURIX™ TC4xx Microcontroller

V1.0.0 2024-09

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

SAFETY
Safety concept

Hardware designed for functional safety



Safety Documentation



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 requirements of ISO 26262 up to ASIL D

Key Features

ISO 26262 standardized development process

Pre-defined and verified safety use cases

Hardware and software safety mechanisms

Customer Benefits

- Support ISO 26262:2018 compliant applications development
- Accelerates the development of safety critical applications
- Performance and flexibility

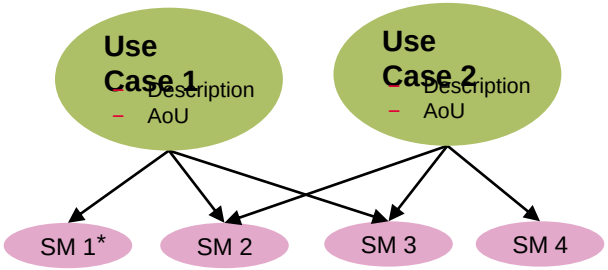
Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
ISO 26262 standardized development process

The AURIX™ microcontroller was developed as an ISO 26262 certified SEooC.

The scope of the SEooC comprises:

- The AURIX™ microcontroller hardware component
- Definition of the different safety use cases for the microcontroller
- System level assumptions of use (AoU) for each use case
- List of mandatory safety mechanisms for each use case
- Description of safety mechanisms and how to use them



The system integrator selects the available use cases that fit the safety application and implements them by following the instructions in the documentation.

All of the above support the development of safety critical applications which shall be ISO 26262:2018 compliant.

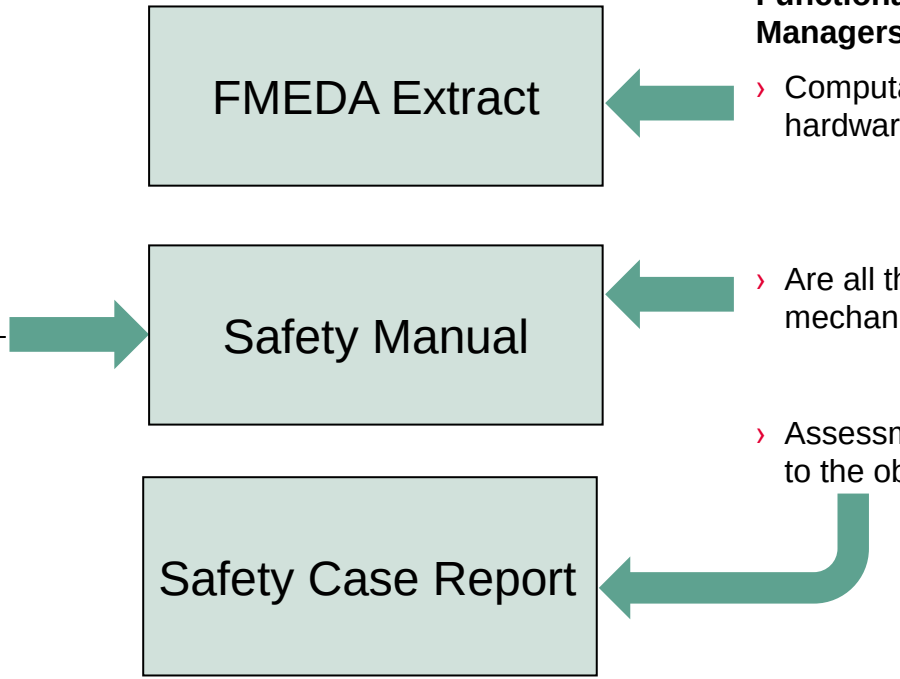
*SM = safety mechanism

Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
Pre-defined and verified safety use cases

System/Software Engineers

- What TLSR use cases (TUC*) are available for a particular AURIX™ TC4xx device?
- What is the description of each TUC?
- Which system level assumptions of use (AoU) shall be considered for a particular TUC?
- What safety mechanisms are required by a particular TUC?
- How to use a safety mechanism?



Functional Safety Managers/Engineers/QM

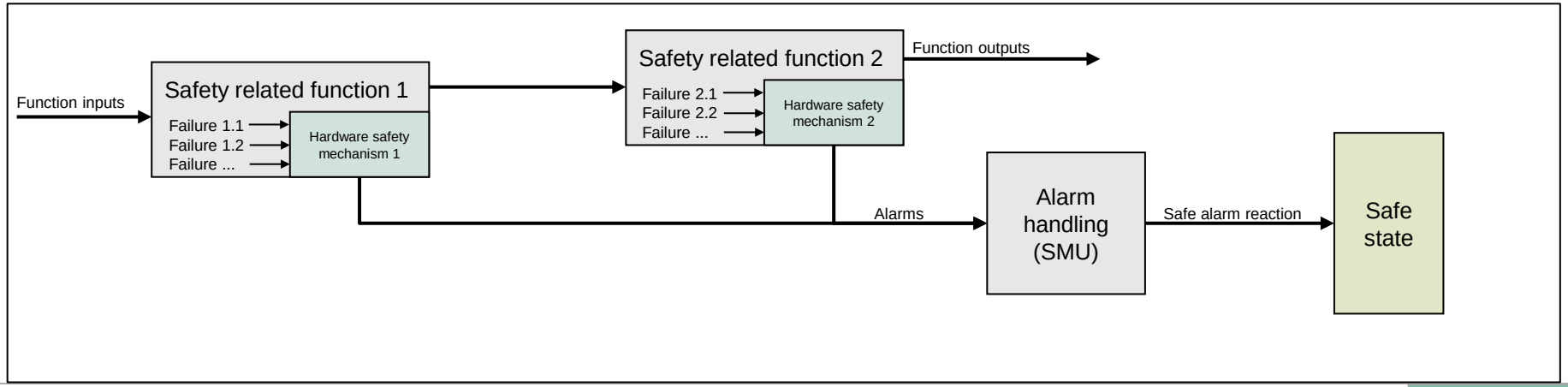
- Computation of project specific hardware architectural metrics
- Are all the required safety mechanisms correctly implemented?
- Assessment of AURIX™ compliance to the objectives of ISO26262

*TUC examples:
- Diverse redundant ADC channels (ASIL D)
- CAN single channel communication (ASIL D)

Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
Hardware safety mechanisms

- Hardware safety mechanisms are implemented inside the microcontroller
  - Detect a high percentage of failures occurring inside each safety related function
  - No impact on processing performance
  - Notify the failure detection through alarms
  - System integrator configures a safe alarm reaction in the SMU to ensure that the safe state is reached



Copyright © Infineon Technologies AG 2024. All rights reserved.

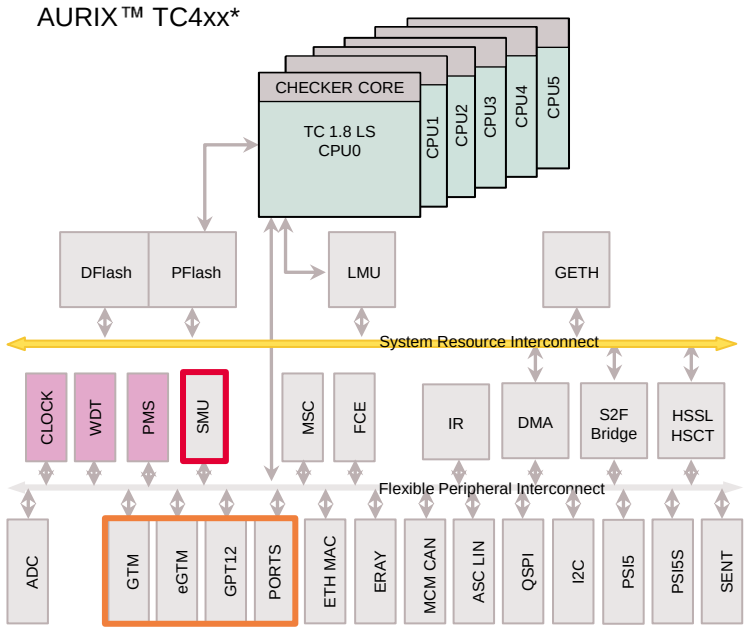
SAFETY
Hardware safety mechanisms

Safe computing:
- Delayed Lockstep CPU with diverse layout

Safe data and code storage:
- Error Detection Codes ECC for RAM and Flash memories
- CPU Memory Protection Unit (MPU) for code and data
- Bus Access Protection Unit (APU)

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 MPU
- Bus APU
- Register Access Protection

Safety management unit:
- Configurable error handling

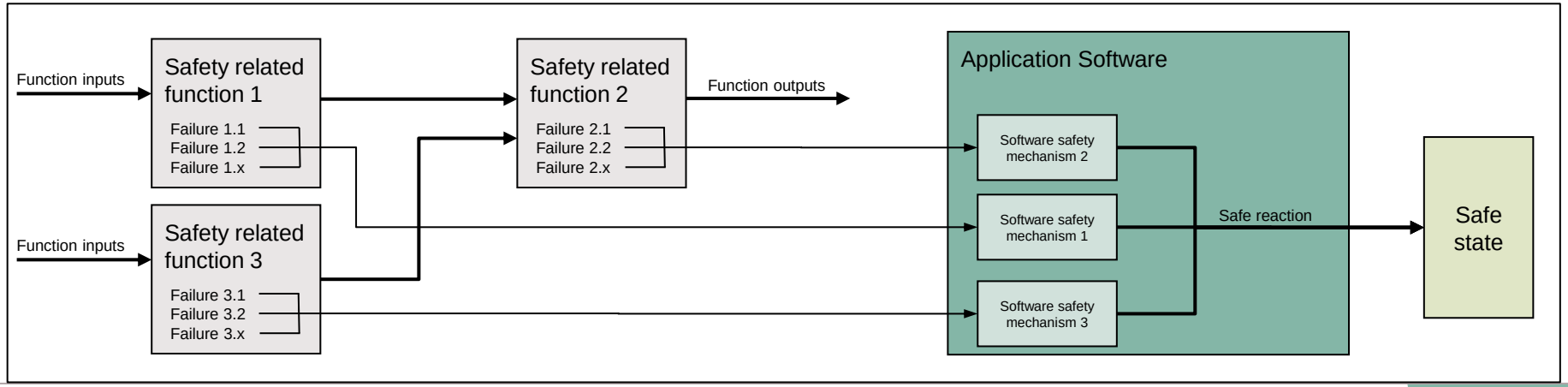
Digital I/O:
- Flexible peripherals to generate, monitor or compare digital signals

*simplified diagram, some features not available in all devices

Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
Software safety mechanisms

- Software safety mechanisms are implemented by the user in the application software
  - Detect failures in the safety related functions through monitoring, plausibility checks, result comparison and other methods
  - The user has the flexibility to implement them to better fit the application
  - Upon detection of an error the application software triggers a safe reaction to ensure that the safe state is reached



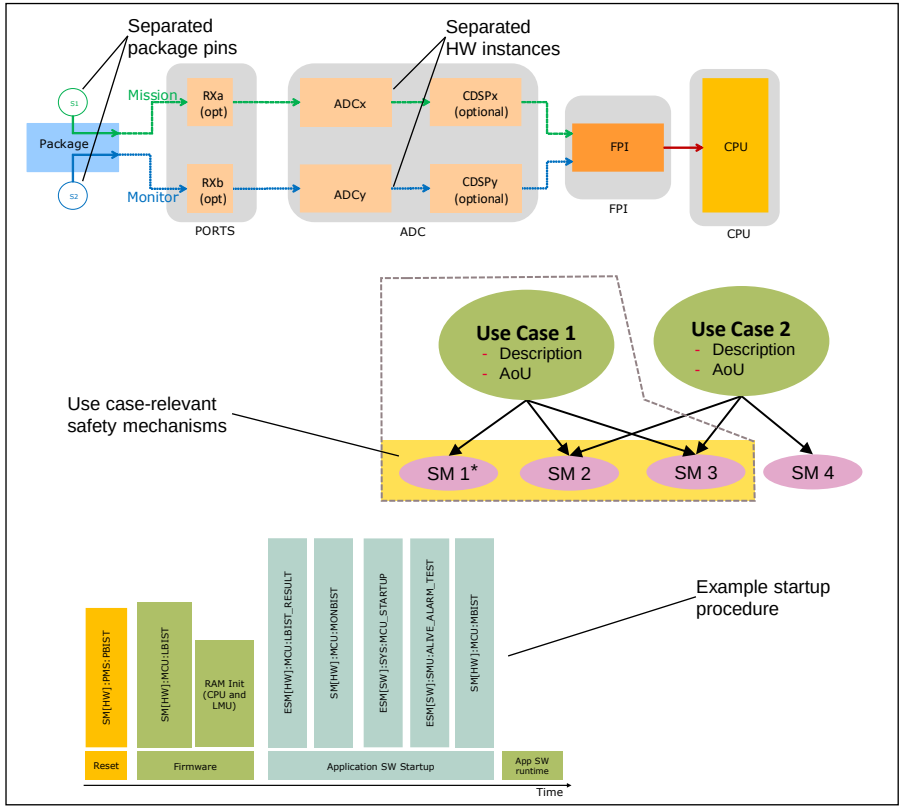
Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
System integration

- Safety as a concept is an integrated part of the AURIX™, nonetheless there are aspects that the system integrator must consider

- For example:
  - For redundancy use cases, selection of package pins and hardware instances that feature sufficient separation
  - Ensure that all safety mechanisms required for a particular use case have been configured and activated
  - Perform the application software actions required during the startup sequence

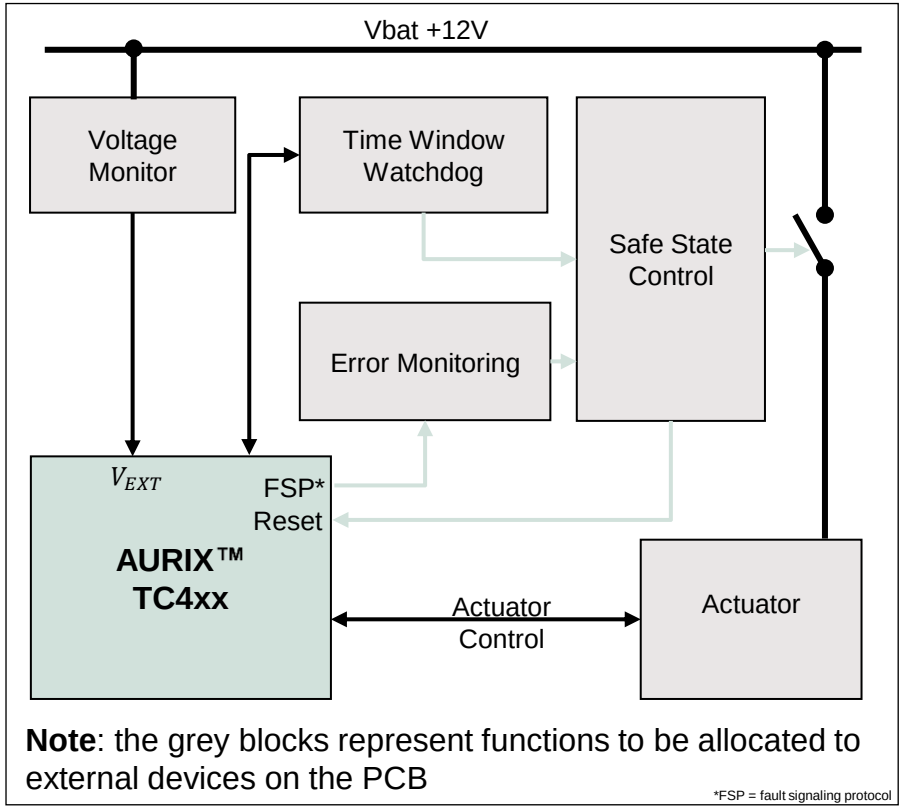
- Integration requirements are provided in the safety manual



Copyright © Infineon Technologies AG 2024. All rights reserved.

SAFETY
System integration

- Regardless of the extensive built-in safety features, in very rare cases the AURIX™ microcontroller can fail or become unresponsive
- For this rather unlikely event, the system integrator shall ensure that the application remains safe
- With the help of external monitoring and reaction systems, it can be ensured that a system unsafe condition is avoided



Note: the grey blocks represent functions to be allocated to external devices on the PCB

*FSP = fault signaling protocol

Copyright © Infineon Technologies AG 2024. All rights reserved.

Trademarks

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

Edition 2024-09
Published by
Infineon Technologies AG
81726 Munich, Germany

© 2024 Infineon Technologies AG.
All Rights Reserved.

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

Document reference
AURIX_3_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.

Copyright © Infineon Technologies AG 2024. All rights reserved.


Infineon