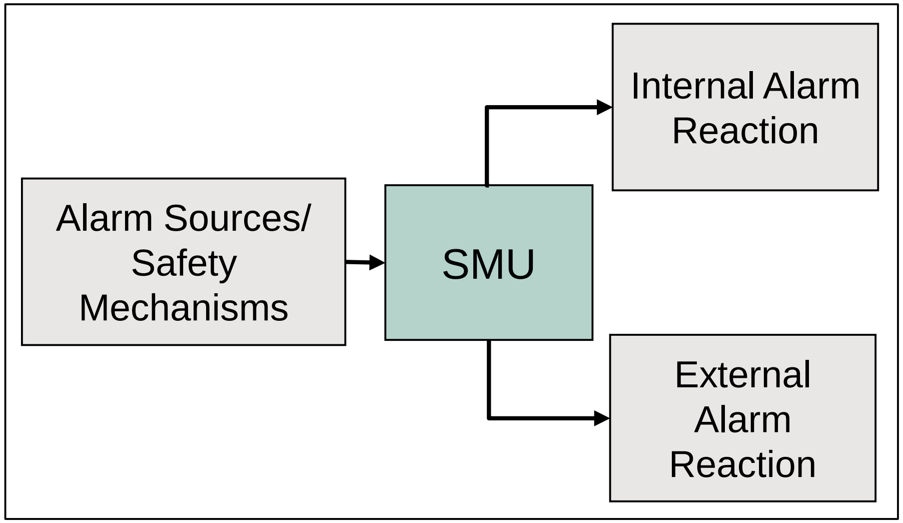
SMU

Safety Management Unit

AURIX™ TC3xx Microcontroller Training
V1.0 2020-09

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

SMU
Safety Management Unit



Highlights

The Safety Management Unit (SMU) is a central hardware module that collects the alarms from every hardware safety mechanism, as well as the error signals related to the architecture.

The severity of each alarm can be configured accordingly with the needs of the application.

Key Features

Unified fault management

Recovery timer

Bipartition of SMU

Customer Benefits

- Configurable internal and/or external reaction for each individually alarm
- Enables monitoring of duration of internal error handlers
- Robust behavior across all clock and power domains

SMU
Unified fault management

- With the SMU, pre-defined reaction can be configured individually for each alarm
- Whenever an input alarm event is detected and the SMU checks what are the configured reactions
- Alarm flags are stored in a diagnosis register that is only reset by Power-On Reset, in order to enable fault diagnosis and possible recovery
- Additionally, an SMU Alive alarm is implemented, which signals is the SMU is not triggering the configured reaction when an alarm is raised

External reaction

- Use **Fault Signaling Protocol** to transition from “fault free state” to “fault state”
- Request **Emergency Stop** to set selected pins in reset state

Internal reaction

- Issue **Non Maskable Interrupt** to all CPUs
- Issue **interrupt** to a configurable set of CPUs
- Issue an **application** or **system reset**
- Issue a **CPU reset** selectively

SMU
Recovery timer

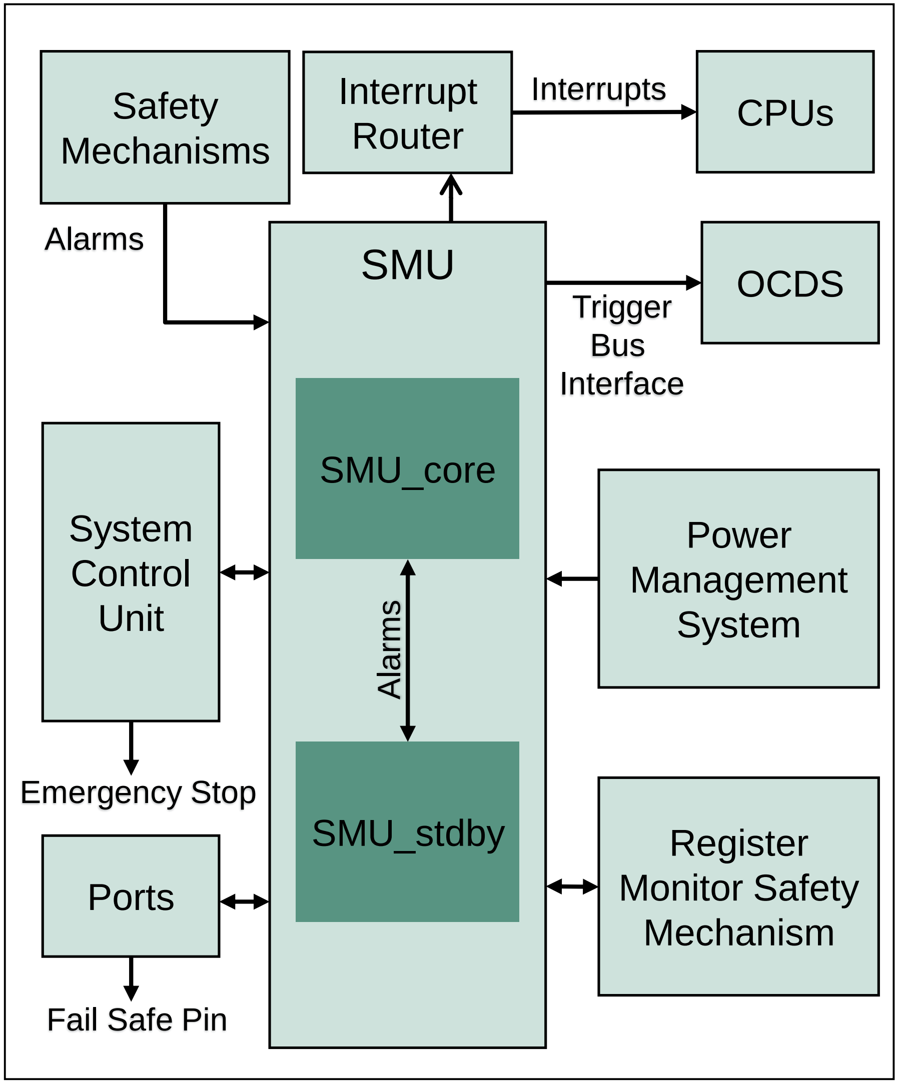
- Recovery timer (RT) is an internal watchdog, which is used to monitor the execution of critical software error handlers
- The recovery timer duration can be configured
- If a recovery timer is enabled and any of the configured alarm events occurs, the recovery timer is automatically started by hardware
- Once a recovery timer event occurs, the recovery timer starts and counts until software stops it
- If the timer expires, an internal SMU alarm (Recovery Timer Timeout) is issued

SMU
Bipartition of SMU

- In order to mitigate the potential common cause faults, the SMU is portioned in two parts:
  - SMU_core: located in the core domain
  - SMU_stdby: located in the stand-by domain
- The SMU_core and SMU_stdby are designed differently and they are located in different clock and power domains with a physical isolation between them
- The SMU_core collects the majority of alarm signals from the hardware monitors and safety mechanisms according to the safety concept, while the SMU_stdby collects alarms from modules which detect clock, power or temperature failures
- This enables the SMU to process any incoming alarm regardless of the clock frequency used to generate the alarm
- The SMU in combination with the embedded safety mechanisms ensure the detection and report of more than 99% of the critical failure modes of the microcontroller, within the fault tolerance time interval

SMU
System integration

- The SMU is connected to all safety mechanisms that are within the microcontroller
- The SMU is also connected to the System Control Unit, the Interrupt Router, the Ports and the Power Management System in order to trigger the configured reaction when an alarm is set



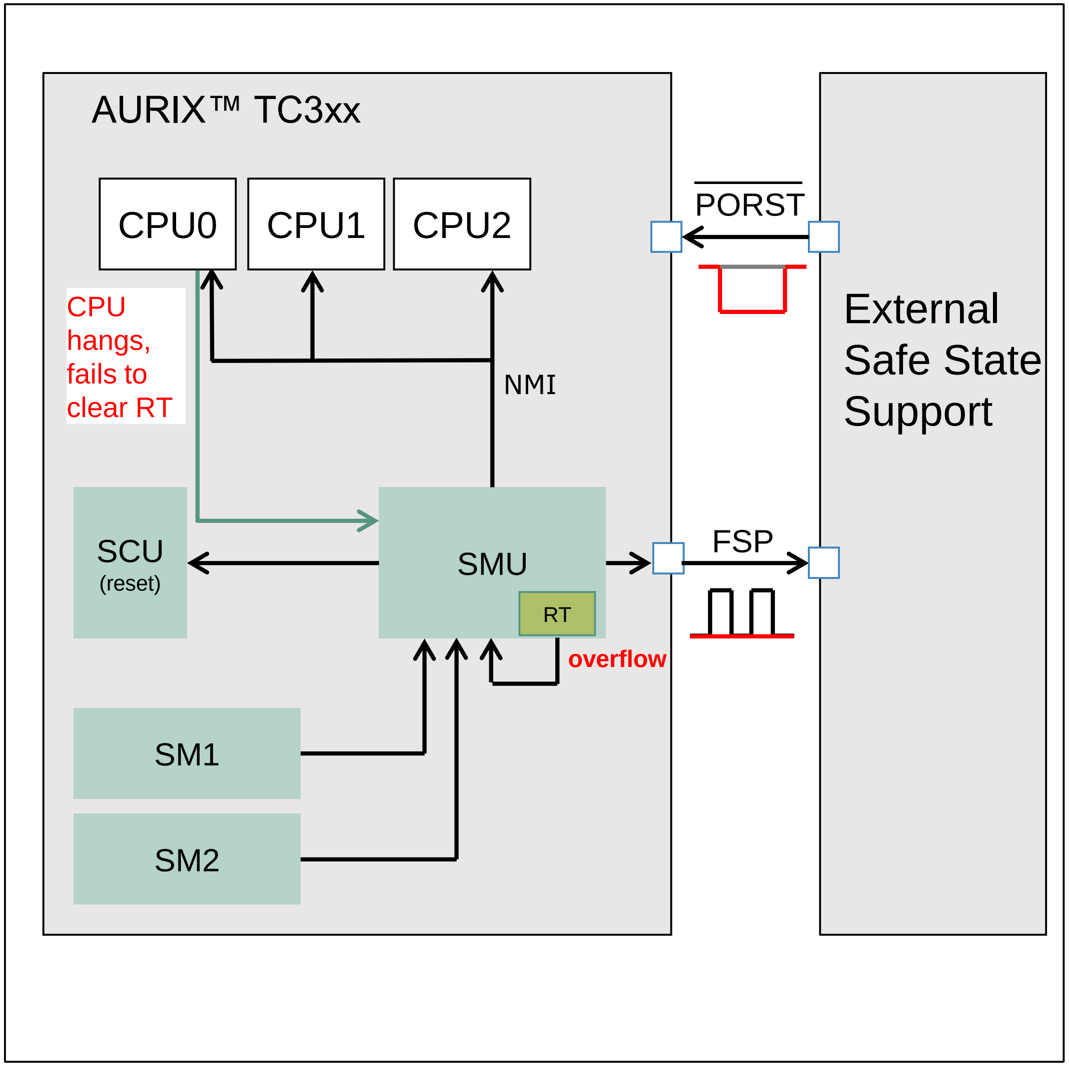
Application Example
Failure reaction example with recovery timer

Overview

- Description of issue: An alarm is triggered by a safety mechanism (SM)
- Procedure: SMU triggers an NMI and starts the recovery timer

Advantages

- Granular reaction concept
- Direct connection to external world via FSP Pin
- Possibility to recover from alarm via RT



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_Management_Unit

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.