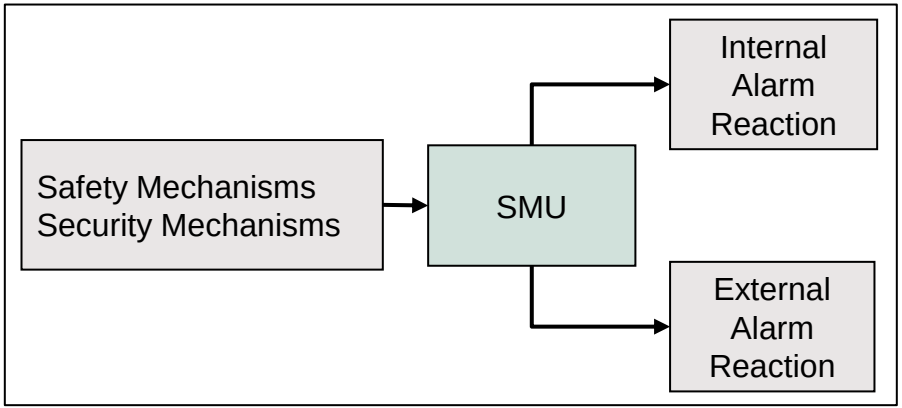
SMU
Safety and security alarm management unit

AURIX™ TC4xx Microcontroller

V1.0.0 2024-09

SMU
Safety and security alarm management unit



Highlights

- The Safety and security alarm management unit (SMU) is a central hardware module that collects the alarms from the safety mechanisms and from the security mechanisms
- The reaction for each alarm can be configured according to the needs of the application

Key Features

- Unified safety and security alarm management
- Recovery timer
- Bipartition of SMU

Customer Benefits

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

SMU
Unified safety alarm management

- With the SMU, a pre-defined reaction can be configured individually for each **safety** alarm
- Whenever an input alarm event is detected, the SMU checks what are the configured reactions
- Alarm flags are stored in a diagnostic 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 if the SMU is not triggering the configured reaction when an alarm is raised

External reaction

- Use **Fault Signaling Protocol (FSP)** 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 (NMI)** to all CPUs
- Issue an **interrupt request** to the Interrupt Router
- Issue an **application, system** or **module group reset**
- Issue a **CPU or PPU reset** selectively

SMU
Unified security alarm management

- With the SMU, a pre-defined reaction can be configured individually for each **security** alarm
- Whenever an input alarm event is detected, the SMU checks what are the configured reactions
- Alarm flags are stored in a diagnostic 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 if the SMU is not triggering the configured reaction when an alarm is raised

Internal reaction
• Issue **Non Maskable Interrupt (NMI)** to all CPUs • Issue an **interrupt request (IRQ)** to the Interrupt Router • Issue an **application, system** or **module group reset** • Issue a **lock all or lock debug keys** request to the CSS

SMU
Recovery timer

- Recovery timer (RT) is an internal timer used to monitor the execution of an alarm reaction performed by software (NMI or IRQ)
- The RT duration can be configured
- If a RT is enabled and any of the configured alarm events occurs, the RT is automatically started by hardware
- Once the RT is started, it will count until software stops it
- If the software fails to stop it, the RT expires, and 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 partitioned in two parts:
  - The core domain
  - The standby domain
- The core domain and the standby domain are supplied by independent clocks, power supplies and are physically isolated from each other
- The core domain collects the alarm signals from the safety and security mechanisms and triggers the previously mentioned internal and external reactions
- The standby domain monitors the correct operation of the core domain and triggers the FSP if an error is detected
- The standby domain also collects specific alarms associated with common cause failures (CCF) of the core domain like clock, power and temperature alarms
- The standby domain acts as a redundant error reporting interface in case the core domain fails

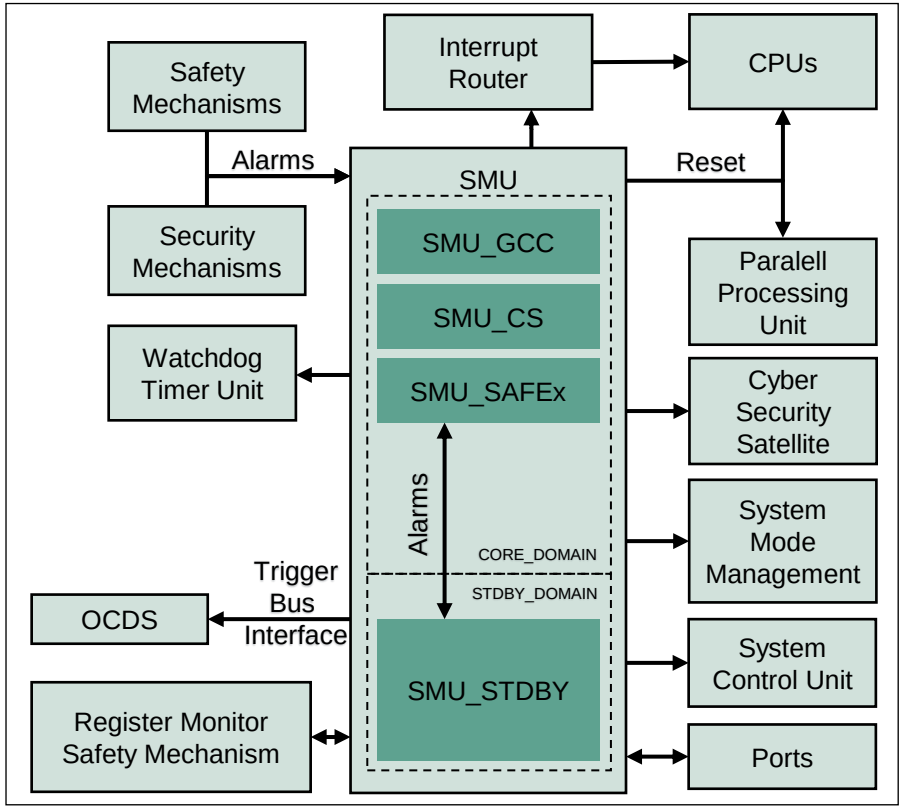
SMU
Bipartition of SMU

- The SMU in combination with the embedded safety mechanisms ensure the detection and reporting of more than 99% of the critical failure modes of the microcontroller within the fault tolerance time interval
- The core domain contains:
  - SMU_CS: cyber security alarm handling instance
  - SMU_SAFE0 and SMU_SAFE1: dual independent safety alarm handling instances
  - SMU_GCC: global control and configuration of alarm handling and other SMU functions
- The standby domain contains:
  - SMU_STDBY: collects the CCF alarms forwarded to the standby domain, the alive alarms from the SMU_SAFEx and SMU_CS instances and triggers a pre-configured FSP reaction

SMU
System integration

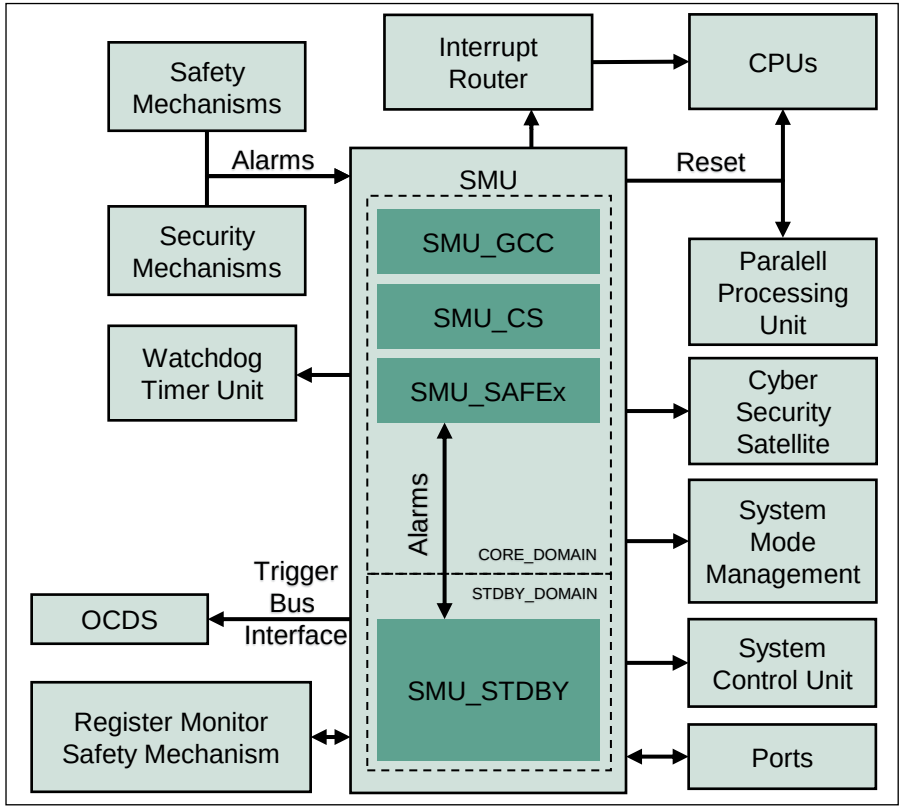
- The SMU receives the alarms coming from all safety and security mechanisms available in the microcontroller

- The SMU is also connected to the Interrupt Router, CPUs, Parallel Processing Unit, Cyber Security Satellite, System Mode Management, System Control Unit and Ports in order to trigger the configured reaction when an alarm is set



SMU
System integration

- The SMU is connected to the Watchdog Timer Unit to support the Unlock Restriction feature of the WTU
- The SMU is connected to the Register Monitor safety mechanism to trigger its test procedure and receive the test results
- The SMU is connected to the On Chip Debug System to support tracing of alarm events



Application example
Failure reaction example with recovery timer

Description

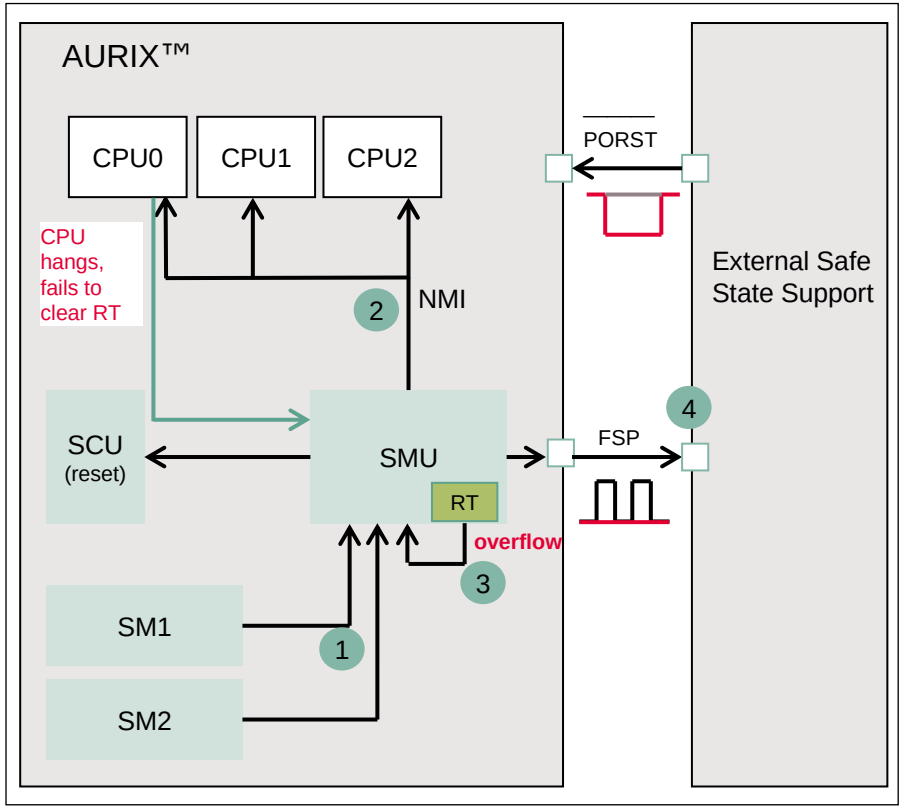
1. An alarm is triggered by a safety mechanism
2. SMU triggers an NMI and starts the RT
3. CPU hangs and fails to clear the RT; RT overflows and activates the FSP
4. The external device recognizes the FSP error and triggers a PORST

Advantages

› Cascaded reaction concept

› Direct connection to external world via FSP Pin

› Possibility to recover from alarm reaction error thanks to RT



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

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

Document reference
AURIX_3_Safety_and_security_alarm_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.


Infineon