AURIX 2G Safety Management Unit(SMU)

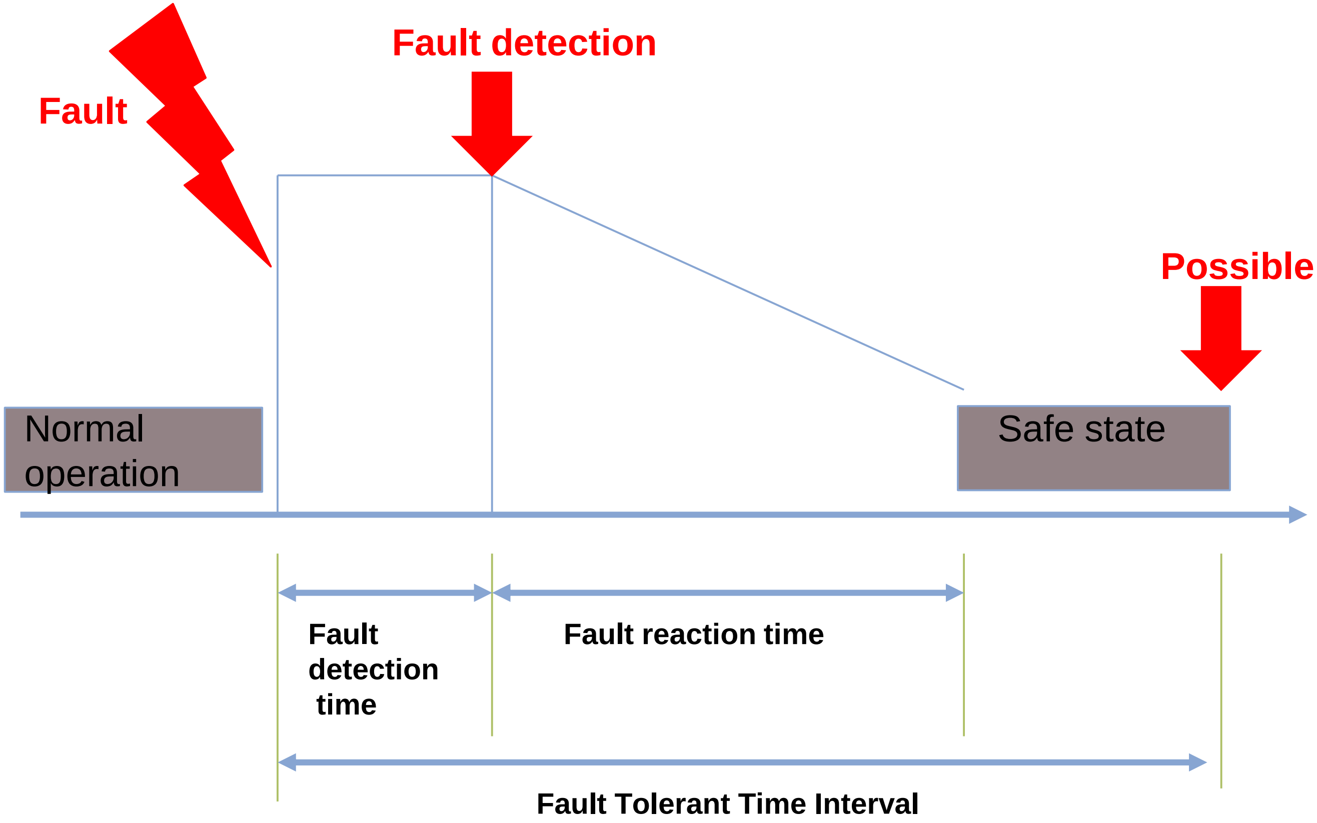
Thomas
IFCN ATV SMD GC SAE MC
2018/5/2

Content

1 Fault Management System(SMU) : Concept

2 SMU Safety Feature : Update

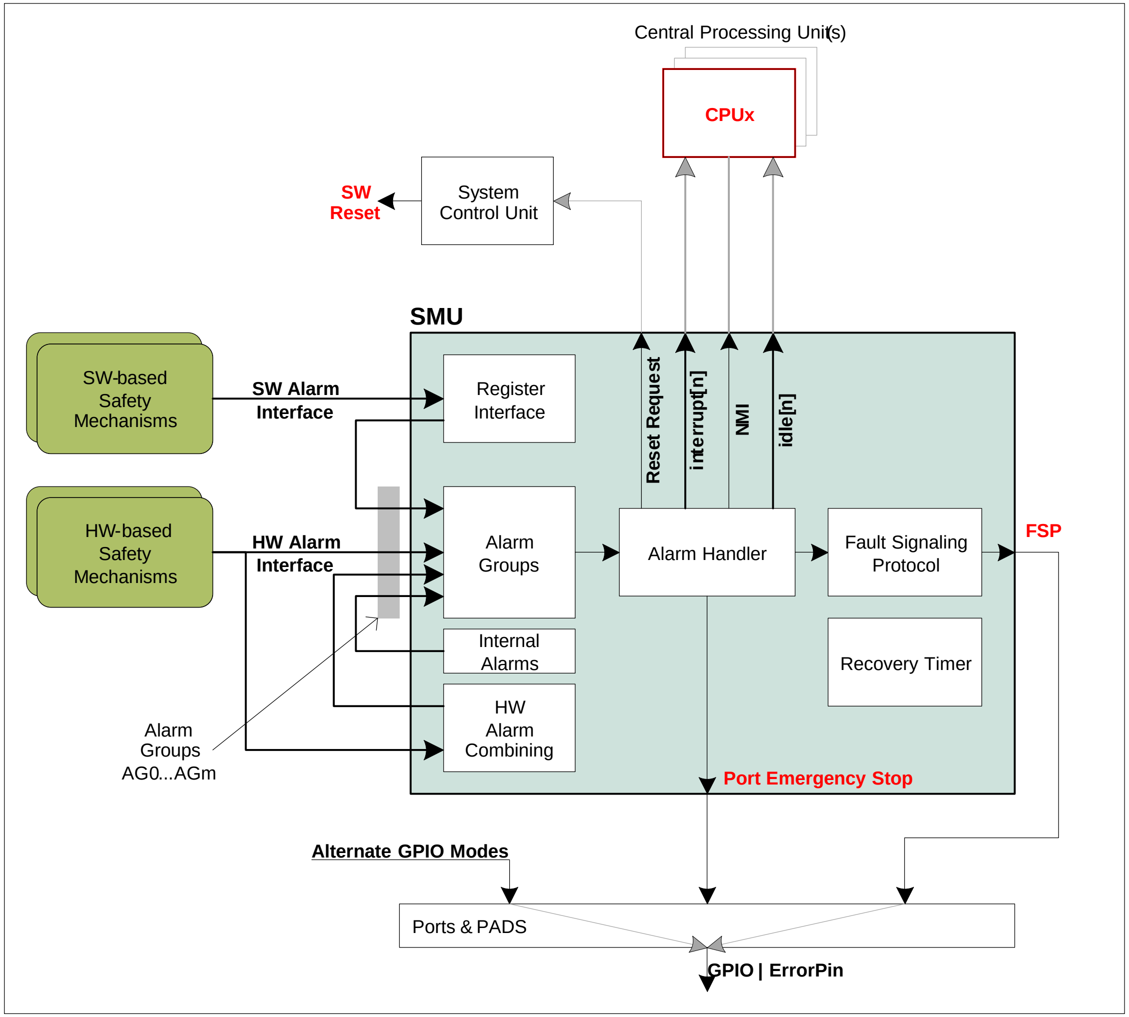
Fault Tolerant Time Interval



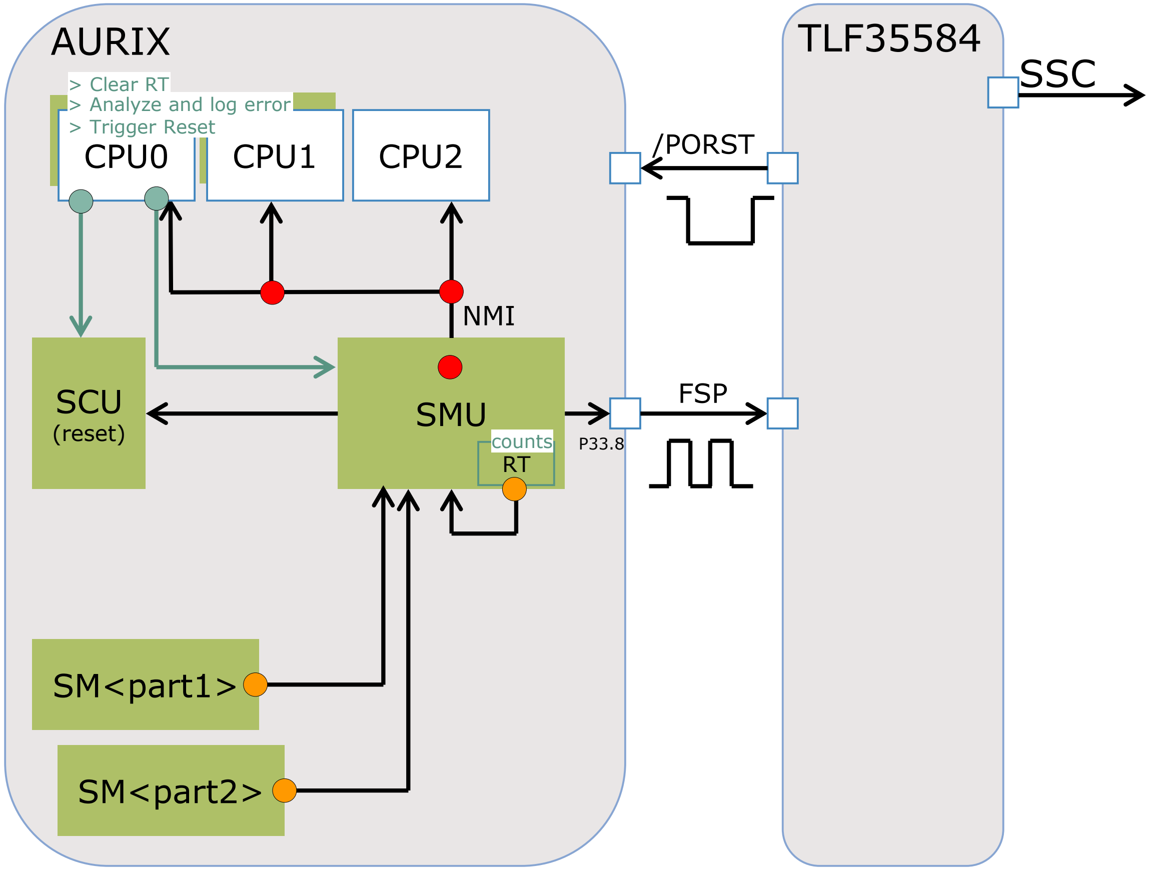
- AURIX supports **FTTI ≥ 10 ms**
- Fault detection time worst case is the software diagnostic time interval (application dependent)
- AURIX hardware safety mechanism provides a very fast fault detection time, in most cases way below 1µs @100MHz

AURIX Fault Reaction Concept

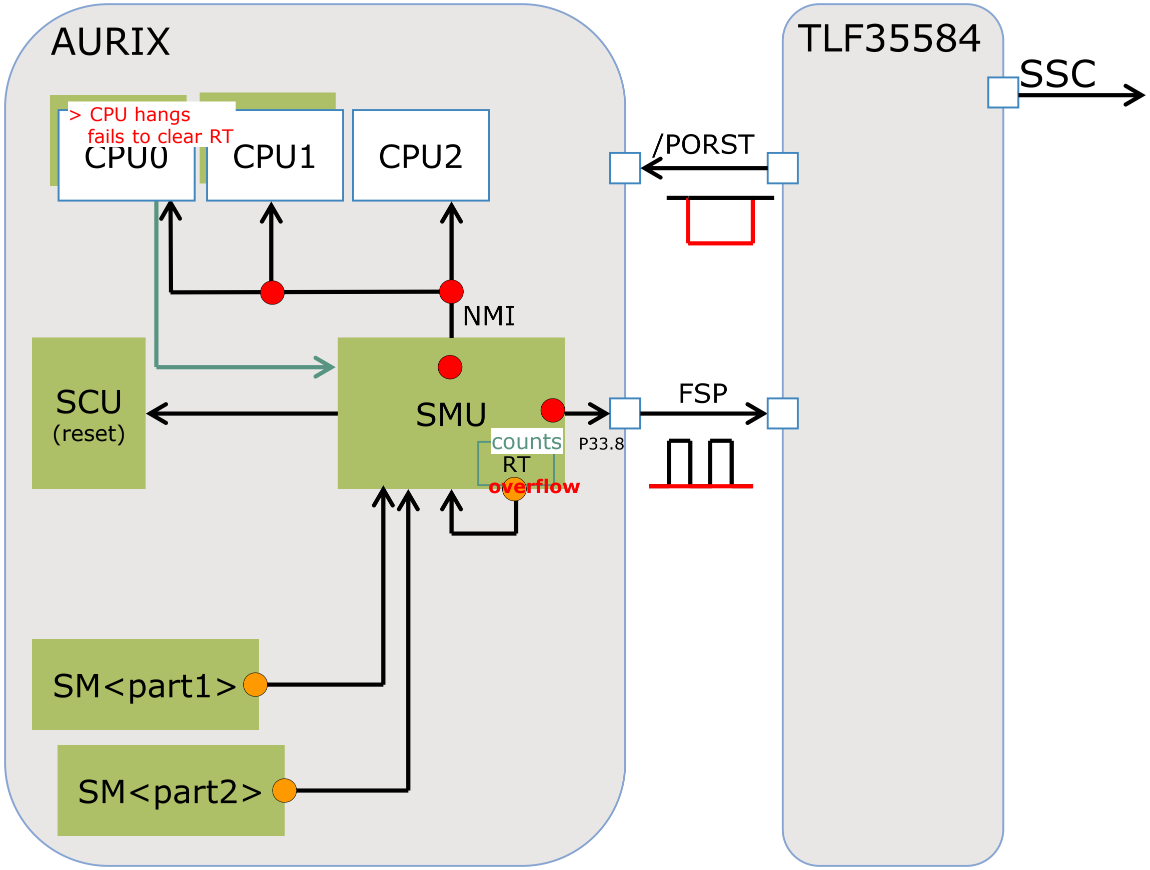
› Error management is centralized in the Safety Management Unit



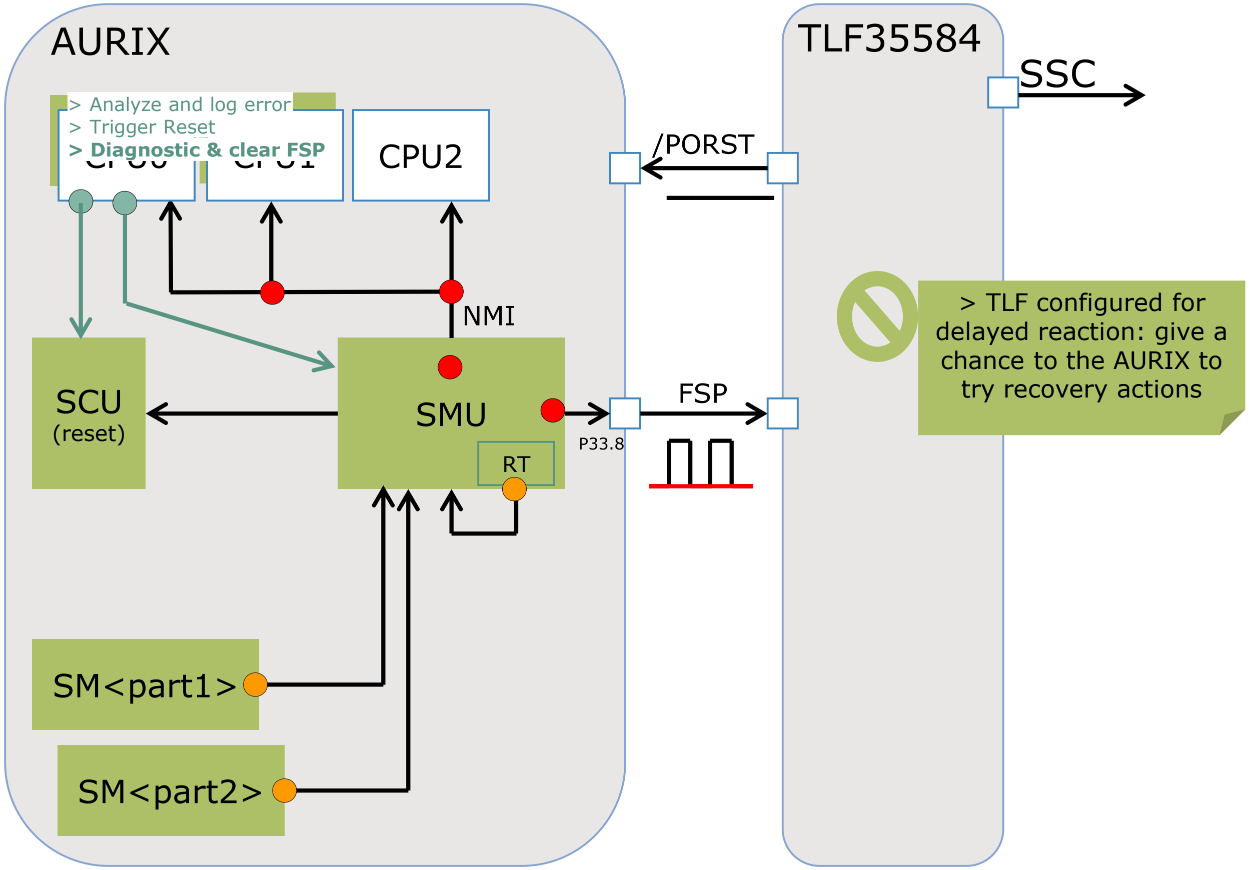
Failure Reaction Example
NMI + Internal Reset



Failure Reaction Example
Recovery Timer



Failure Reaction Example
NMI + FSP and SSC delayed reaction



> Analyze and log error
> Trigger Reset
> **Diagnostic & clear FSP**

> TLF configured for delayed reaction: give a chance to the AURIX to try recovery actions

Safety Management Unit

- Central hardware module that collects alarms from every hardware safety mechanisms as well as error signals related to the architecture (bus error,…)
- Unified fault management: dedicated alarms can also be triggered by the software
- Pre-defined reaction can be configured individually for each alarm:

External reaction

- transition Fail Safe Protocol on the error pin (P33.8) to "fault state"

Internal reaction, to be selected b/w

- Issue NMI to all CPUs
- Issue interrupt to a configurable set of CPUs
- Issue a system reset (recommended), or application reset
- Force a configurable set of CPUs into IDLE mode

Note: both external and internal reaction can be configured for a given alarm, for example FSP fault state activation + NMI

Application/System Reset

Reset Type	Reset Trigger	Modules affected by any reset	Modules affected additionally by System reset	Modules affected additionally by warm PORST	Modules affected additionally by Cold Power-on
Application Reset	▪ESR0/ESR1 ▪SMU ▪STMx ▪Software reset ▪Tuning protection	▪All CPUs ▪All Peripherals ▪Port pins in reset state ▪Parts of SCU ▪RAMs - Dcache invalid - Pcache invalid			
System Reset	▪ESR0/ESR1 ▪SMU ▪STMx ▪Watchdog (SMU) ▪Software reset		▪Flash memory ▪XTAL/ Osc./ PLL ▪ESRx pins		
Warm Power-on Reset	▪PORST pad asserted			▪JTAG interface ▪OCDS / MCDS SP pin	
Cold Power-on Reset	▪Startup ▪Ext. supply (SWD) < 3.0V ▪EVR33 supply < 3.0V ▪EVR13 supply < 1.17V				▪EVR ▪Internal clocks ▪RAMs -DSPRs/ PSPRs -LMU/BMU

A higher reset encapsulate

ower reset

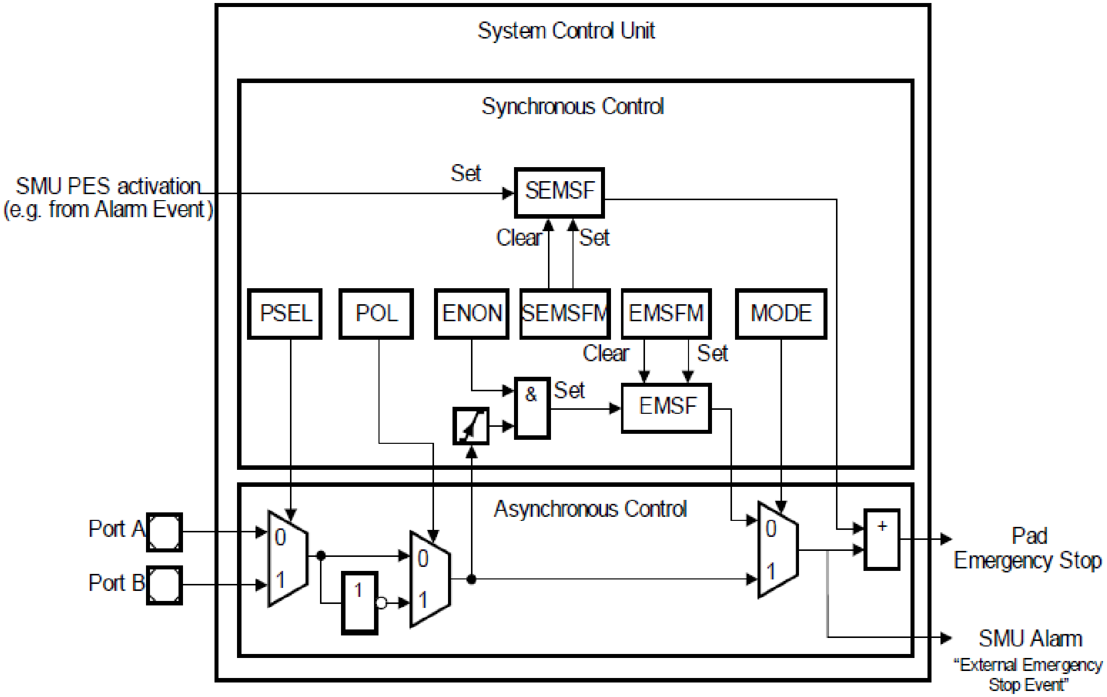
A higher reset resets all the modules reset by a lower reset

- System reset is the recommended internal reaction
- An application reset would not help to recover from FLASH, and clock related failures

- Failures related to the internally generated voltages may be recovered from with a cold power-on reset only

Port Emergency Stop

- Scope: used to disconnect quickly and reliably critical outputs in case of dangerous situation
- Possible usages: stop all communication on CAN bus, disconnect PWM signals from actuator,…
- All digital I/O ports have an emergency stop logic. It can be configured for each pin if it reacts on the global emergency stop signal in register Pn_ESR.
- The pin configuration is switched to the default state after reset (input function with internal pull-up, or tri-state)



Content

1 Fault Management System(SMU) : Concept

2 SMU Safety Feature : Update

Safety Feature Update

2.1 Architecture

2.2 SMU Changes

2.3 SMU More Details

Safety Management Unit (SMU) Introduction

- The SMU centralizes all the alarm signals related to the different hardware and software-based safety mechanisms

- Each alarm can be individually configured to trigger
  - internal actions and/or notify
  - externally the presence of faults via a fault signaling protocol

- The SMU in combination with the embedded safety mechanisms enable to detect and report more than 99% of the critical failure modes of the microcontroller within the fault tolerance time interval

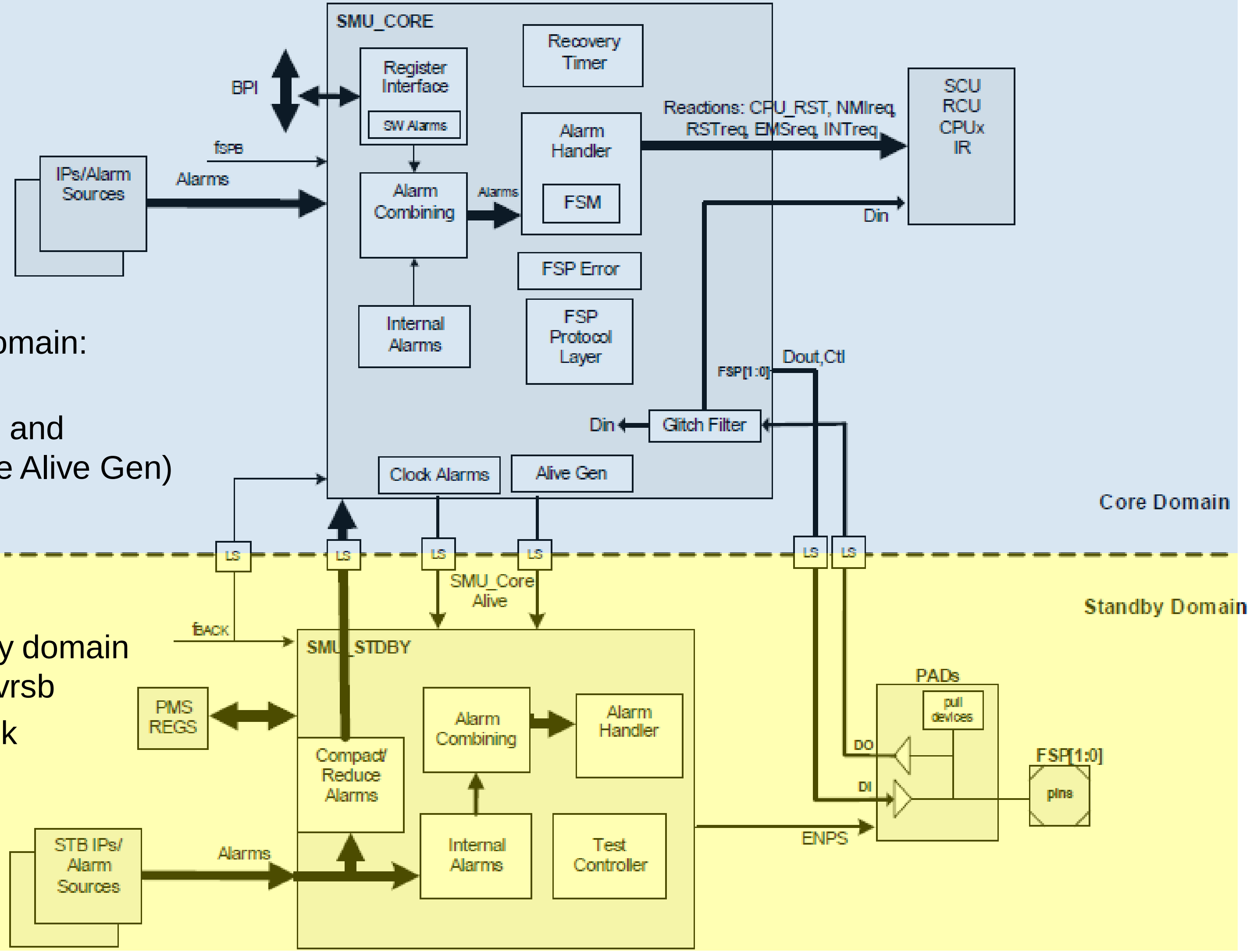
SMU Architecture update
: Redundancy & Diversity

SMU_Core

- Located in core domain: powered by V_dd
- Clocked by F_spb and F_back (e.g for the Alive Gen)

SMU_Stdby

- Located in standby domain : powered by V_evrsb
- Clocked by F_back



Safety Feature Update

2.1 Architecture

2.2 SMU Changes

2.3 SMU More Details

SMU Changes: Motivation

- Independent (power and clock domain) and redundant monitor for Alarms
- Control of Fault Management System Latent Faults and SEU(Single Event Upset)
- Control of Systematic Faults: alternative implementation to the SMU_Core
- State of the art on the market
- Consistent and simplified implementation for External Error Signalling (FSP) and monitoring
- Unified/systematic solution for both Power Domains: Core and Standby

SMU Changes

Software Compatibility:

- Much more alarms handled by AURIX™ TC3xx SMU than TC2xx
- Alarm grouping changed completely because of increased number of alarms
- „Alarm Executed" mechanism implemented.

  If one kind of Alarm-Handling (e.g. RST0 request) was executed, the Alarm Executed Status needs to be cleared before the same Alarm-Handling can be executed again.

Safety-related changes:

- CPU IDLE requests changed to CPU core reset requests.
- Alarm-Handlings which are triggered from Alarms coming at the same time are now executed concurrently (if different reactions are configured, if not then see Alarm Executed mechanism above).
- Safety FFs added to safety critical blocks (SSH, PMS, SCU,…) with alarms and self-test control in SMU

Redundant SMU in Standby Domain: SMU_Stdby:

- **Alive Alarm** from SMU_Core to SMU_Stdby
- Contains the **control of MONBIST**: enables users to test all alarm paths, alarm configurations, alarm reactions
- Upon SMU_Stdby alarm detection, FSP pins can be put into fault state.

FSP updates:

- Redundant FSP pin: FSP[1] → new protocol is introduced (Dynamic Dual Rail)
- Glitch filter for EMS input via Error Pin (FSP[0])

Safety Flip-Flops updates:

- Separated Register Monitor control and status bits per IP with SFF
- Both SMUs contain SFFs as SMs

SMU_STDBY

› SMU Standby Memory Map:

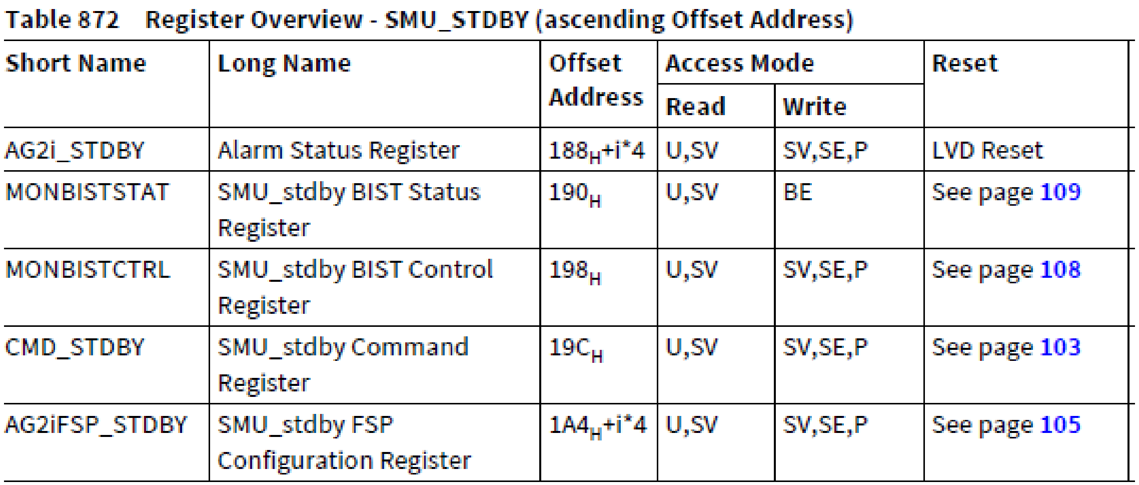
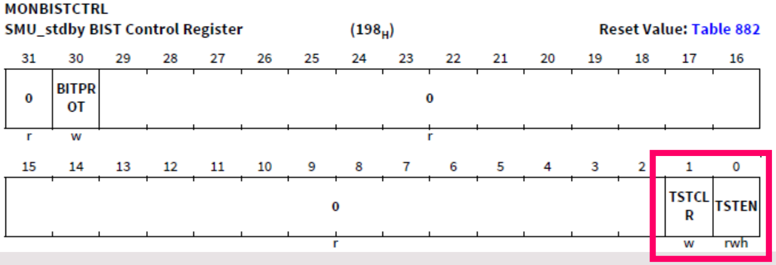


Table 872 Register Overview - SMU_STDBY (ascending Offset Address)

Short Name	Long Name	Offset Address	Access Mode		Reset
			Read	Write	
AG2i_STDBY	Alarm Status Register	188_H+i*4	U,SV	SV,SE,P	LVD Reset
MONBISTSTAT	SMU_stdby BIST Status Register	190_H	U,SV	BE	See page 109
MONBISTCTRL	SMU_stdby BIST Control Register	198_H	U,SV	SV,SE,P	See page 108
CMD_STDBY	SMU_stdby Command Register	$19C_H$	U,SV	SV,SE,P	See page 103
AG2iFSP_STDBY	SMU_stdby FSP Configuration Register	$1A4_H$+i*4	U,SV	SV,SE,P	See page 105

› SMU_stdby Built-In Self Test

- The SMU_stdby contains a built-in mechanism that enables users to test all alarm paths, alarm configurations, and alarm reactions.
- The **MONBISTCTRL** register enables the user to start the BIST of the SMU_stdby. Results of the BIST are available in the **MONBISTSTAT** register.

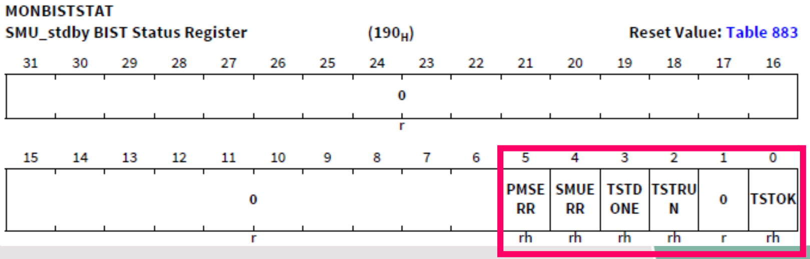


MONBISTCTRL

SMU_stdby BIST Control Register (198_H) Reset Value: Table 882

31	30	29–16
0	BITPROT	0
r	w	r

15–2	1	0
0	TSTCLR	TSTEN
r	w	rwh



MONBISTSTAT

SMU_stdby BIST Status Register (190_H) Reset Value: Table 883

31–16
0
r

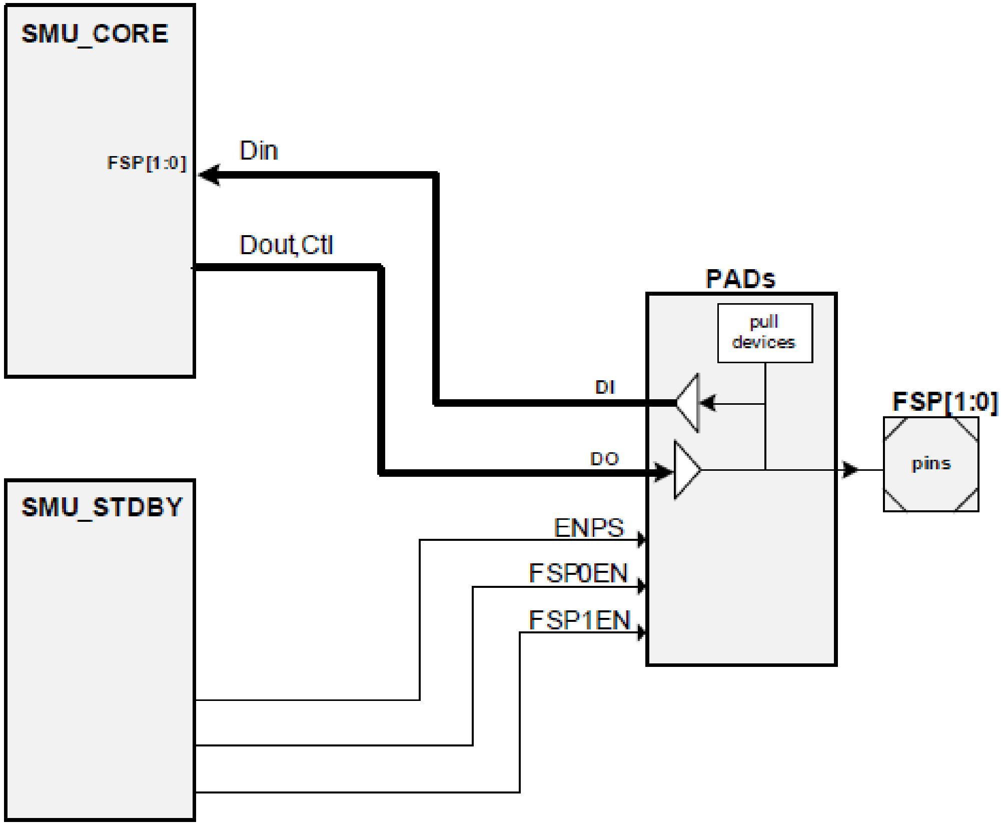
15–6	5	4	3	2	1	0
0	PMSERR	SMUERR	TSTDONE	TSTRUN	0	TSTOK
r	rh	rh	rh	rh	r	rh

SMU Changes: FSP pins

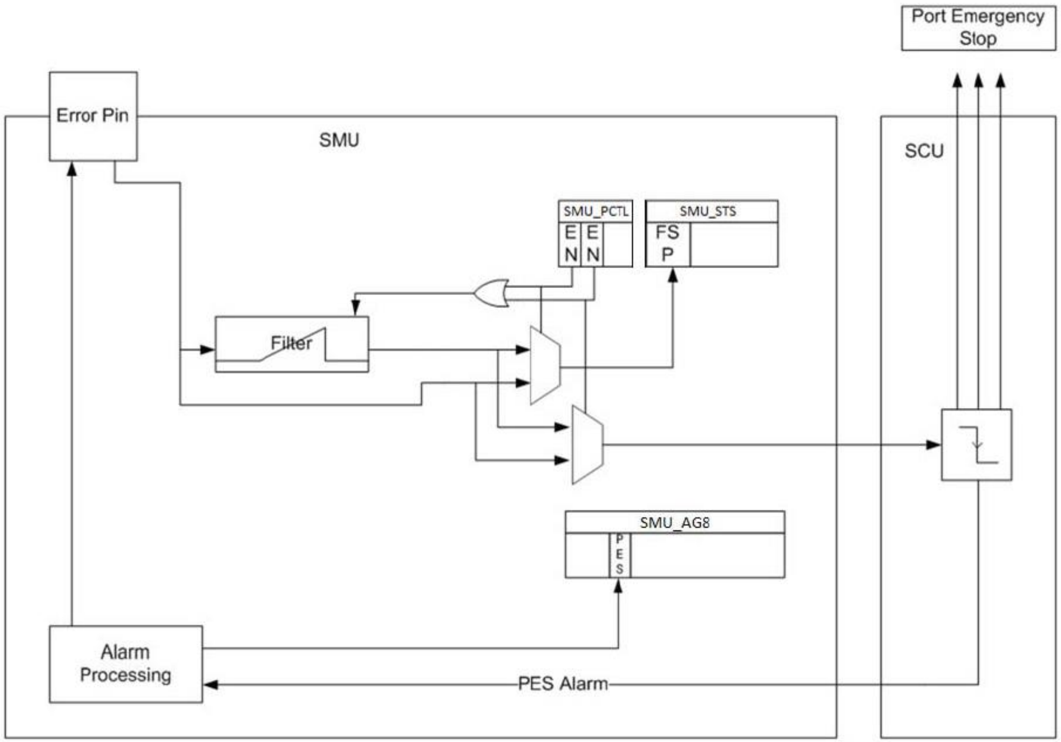
- FSP protocol layer block to support all 3 protocol:
  - Bi-stable (default)
  - **Dynamic dual-rail**
  - Time-switching protocols

- FSP status is generated/decoded by the FSP Protocol layer in SMU_CORE domain.

- FSP0EN (FSP[0]) and FSP1EN (FSP[1]) are controlled by the register CMD_STDBY.



SMU Changes: Glitch Filtered Error Pin



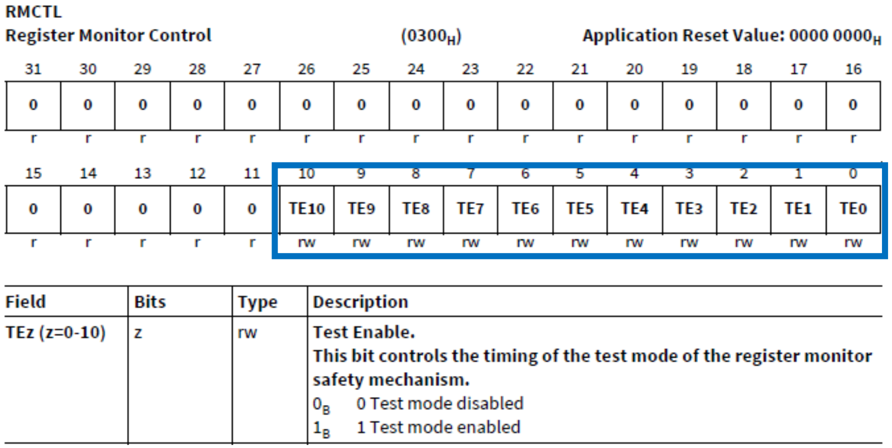
Glitch Filter (not available in TC39x A-Step)

In systems which are using the Error Pin in Open Drain mode, glitches up to 1.2 µs shall have no effect on the current system behavior. Therefore a glitch filter is available inside the SMU which suppresses glitches up to 1.2µs. There are two relevant pathes from the Error Pin in case of Open Drain mode usage:

- Error Pin to STS.FSP[0]
  - For this path the filter can be switched on/off in PCTL.GFSTS_EN
- Error Pin to SCU for Port Emergency Stop usage
  - For this path the filter can be switched on/off in PCTL.GFSCU_EN

SMU Changes: SFF Register Monitor

RMCTL, RMEF and RMSTS: Separated control and status bits per IP with SFFs



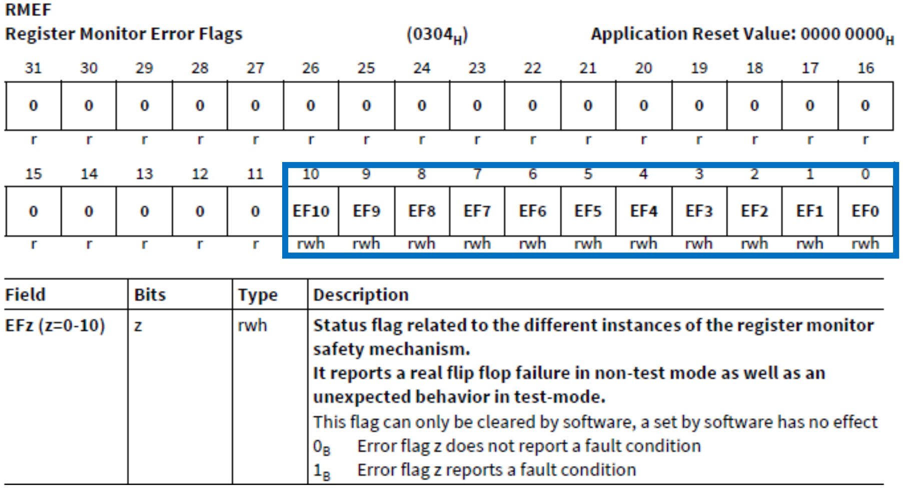
RMCTL
Register Monitor Control (0300$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	TE10	TE9	TE8	TE7	TE6	TE5	TE4	TE3	TE2	TE1	TE0
r	r	r	r	r	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Field	Bits	Type	Description
TEz (z=0-10)	z	rw	**Test Enable.** **This bit controls the timing of the test mode of the register monitor safety mechanism.** 0_B 0 Test mode disabled 1_B 1 Test mode enabled

SMU_RMEF[0]	MTU
SMU_RMEF[1]	IOM
SMU_RMEF[2]	IR
SMU_RMEF[3]	EMEM
SMU_RMEF[4]	SCU/SRU
SMU_RMEF[5]	PMS
SMU_RMEF[6]	DMA
SMU_RMEF[7]	SMU_core
SMU_RMEF[8]	CERBERUS
SMU_RMEF[9]	SYS_PLL/PER_PLL
SMU_RMEF[10]	CCU

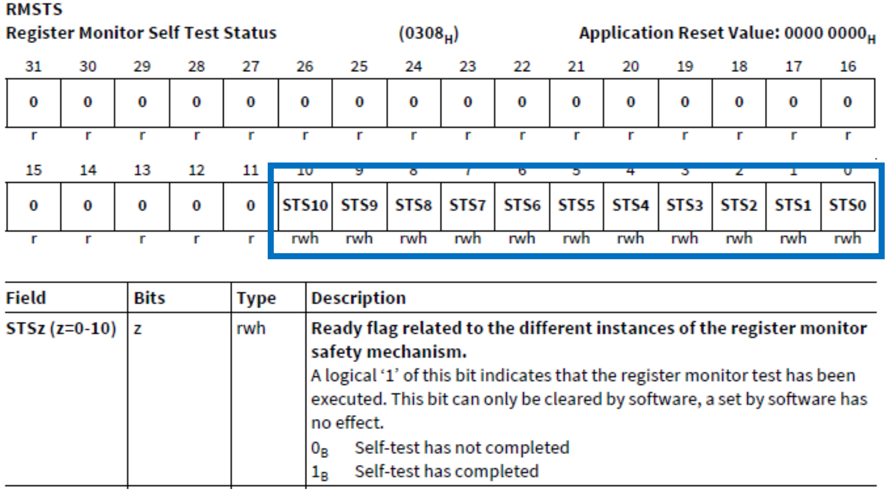


RMEF
Register Monitor Error Flags (0304$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	EF10	EF9	EF8	EF7	EF6	EF5	EF4	EF3	EF2	EF1	EF0
r	r	r	r	r	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh

Field	Bits	Type	Description
EFz (z=0-10)	z	rwh	**Status flag related to the different instances of the register monitor safety mechanism.** **It reports a real flip flop failure in non-test mode as well as an unexpected behavior in test-mode.** This flag can only be cleared by software, a set by software has no effect 0_B Error flag z does not report a fault condition 1_B Error flag z reports a fault condition



RMSTS
Register Monitor Self Test Status (0308$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

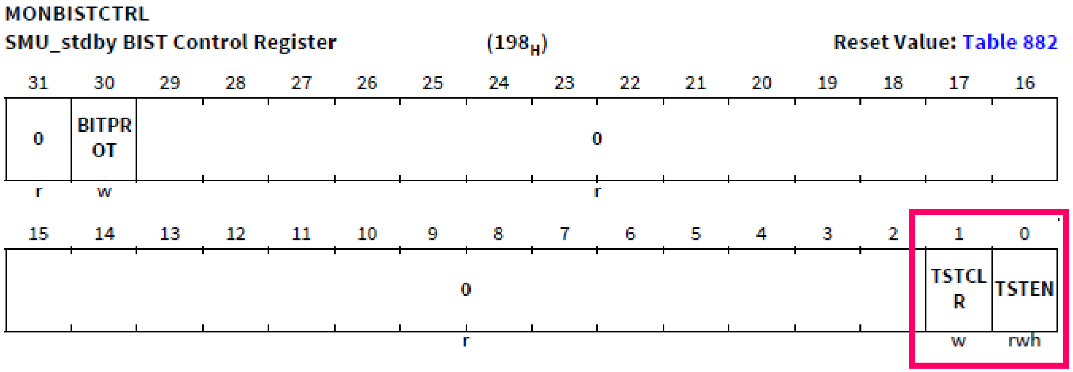
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	STS10	STS9	STS8	STS7	STS6	STS5	STS4	STS3	STS2	STS1	STS0
r	r	r	r	r	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh

Field	Bits	Type	Description
STSz (z=0-10)	z	rwh	**Ready flag related to the different instances of the register monitor safety mechanism.** A logical '1' of this bit indicates that the register monitor test has been executed. This bit can only be cleared by software, a set by software has no effect. 0_B Self-test has not completed 1_B Self-test has completed

SMU_Stdby BIST (MONBIST)

› SMU_Stdby Built-In Self Test control/status

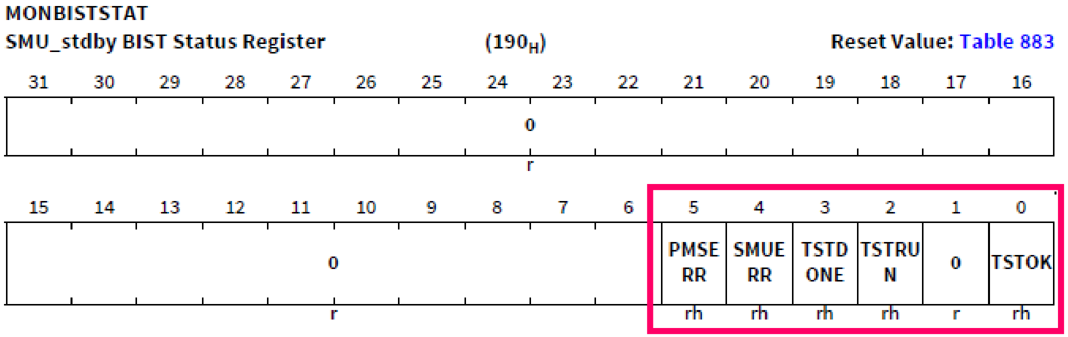
- The SMU_Stdby contains the control of MONBIST that enables users to test all alarm paths, alarm configurations, and alarm reactions.
- The **MONBISTCTRL** register enables the user to start the BIST of the SMU_Stdby. Results of the BIST are available in the **MONBISTSTAT** register.



MONBISTCTRL
SMU_stdby BIST Control Register (198$_H$) **Reset Value:** Table 882

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	BITPROT	0													
r	w	r													

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0														TSTCLR	TSTEN
r														w	rwh



MONBISTSTAT
SMU_stdby BIST Status Register (190$_H$) **Reset Value:** Table 883

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0															
r															

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0										PMSERR	SMUERR	TSTDONE	TSTRUN	0	TSTOK
r										rh	rh	rh	rh	r	rh

Safety Feature Update

2.1 Architecture

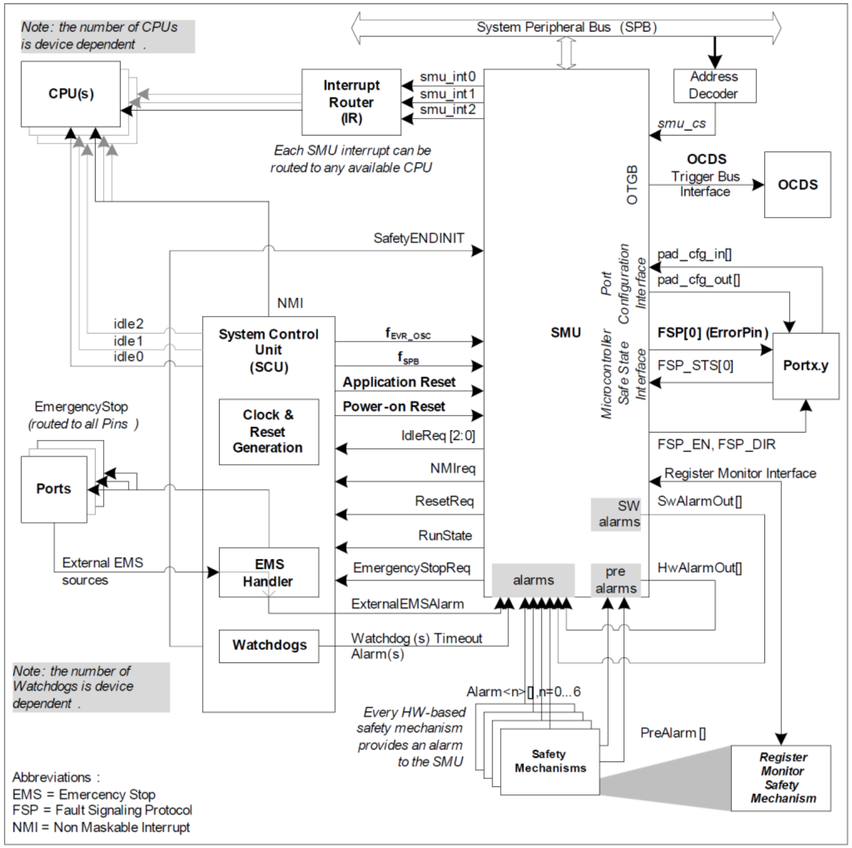
2.2 SMU Changes

2.3 SMU More Details

Safety Management Unit (SMU) Alarm Groups

Alarm are grouped into 11 alarm groups:

0. CPU0
1. CPU1
2. CPU2
3. CPU3
4. CPU4
5. CPU5
6. GTM, CAN, E-RAY
7. SRAM, Lockstep
8. CCU, SCU, IR, DMA
9. DTS,EVR,HSM,EMEM, SPU
10. Software
11. SRI (LMU,XBAR,DMU,HSSL,SFI)



Note: the number of CPUs is device dependent .

Each SMU interrupt can be routed to any available CPU

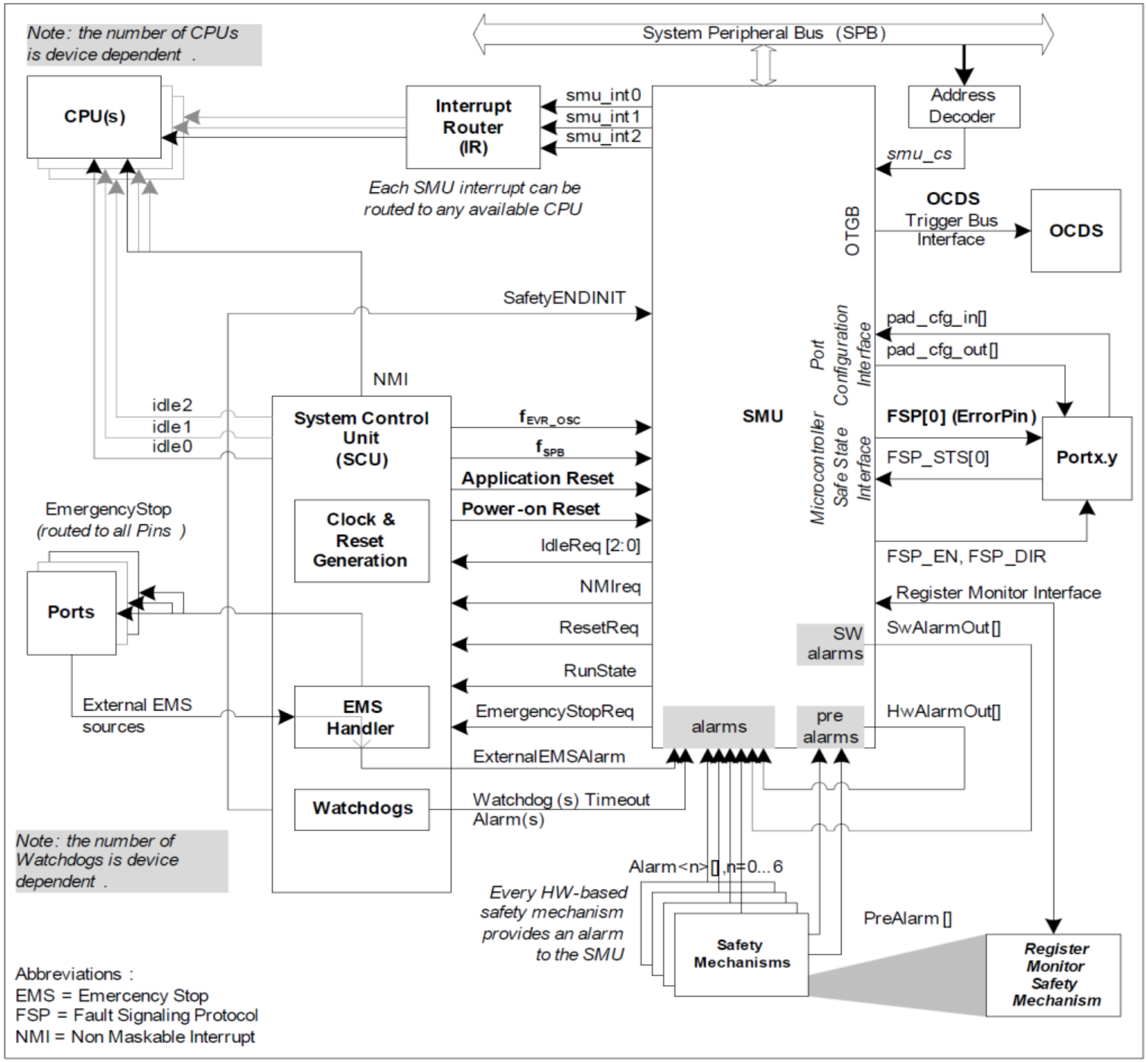
Note: the number of Watchdogs is device dependent .

Every HW-based safety mechanism provides an alarm to the SMU

Abbreviations :
EMS = Emercency Stop
FSP = Fault Signaling Protocol
NMI = Non Maskable Interrupt

Minor safety mechanisms are combined into pre-alarms prior to the alarm grouping

Safety Management Unit (SMU) Interfaces



Note: the number of CPUs is device dependent .

Each SMU interrupt can be routed to any available CPU

Note: the number of Watchdogs is device dependent .

Every HW-based safety mechanism provides an alarm to the SMU

Abbreviations :
EMS = Emercency Stop
FSP = Fault Signaling Protocol
NMI = Non Maskable Interrupt

Safety Management Unit (SMU)
Access, Configure and Lock

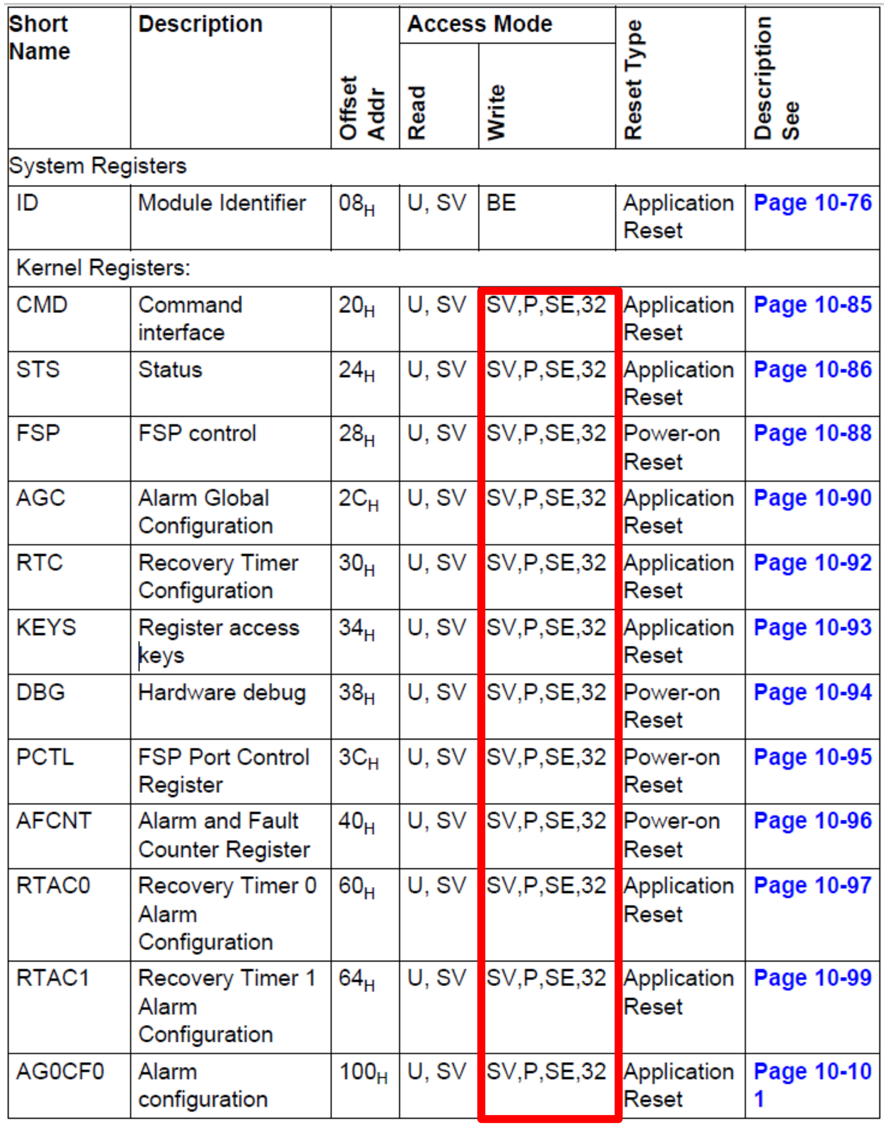
- In addition to the generic register access protection part of the microcontroller architecture, the SMU implements an **independent configuration locking** mechanism
- SMU registers protected by

1. Master protection mechanism
2. Safety ENDINIT
3. Lock mechanism for SMU module register AGC, RTC, RTACn, AGnCFx, AGnFSP(n=0…11), PCTL, RMCTL but not for CMD register
   - SMU_KEYS.CFGLCK enables to configure the registers
   - SMU_KEYS.PERLCK **will lock registers until application reset**

Safety Management Unit (SMU) Access, Configure and Lock

- Code example:

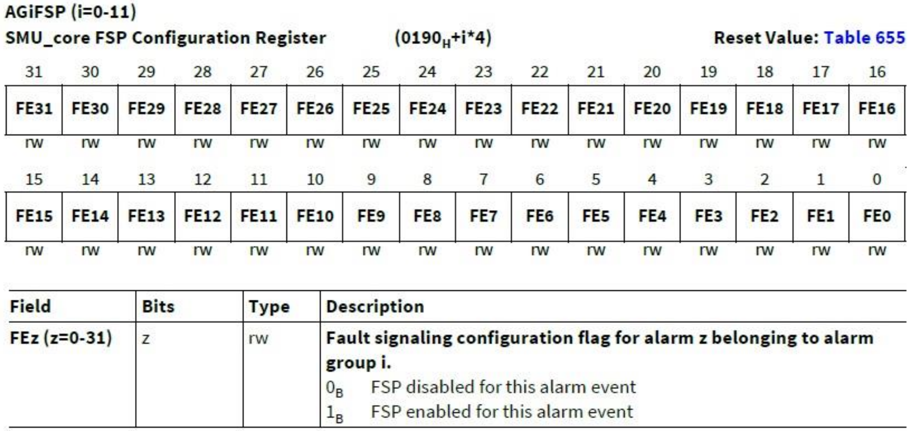
```
// Pre-condition: SV mode

// clear safety endinit bit
safety_endinit_clear();

// unlock configuration
SMU_KEYS = 0x00BC;

// configure SMU registers
…

// permanent lock
SMU_KEYS = 0xFF00;

// set safety endinit bit
safety_endinit_set();
```



Short Name	Description	Offset Addr	Access Mode		Reset Type	Description See
			Read	Write		
System Registers						
ID	Module Identifier	08_H	U, SV	BE	Application Reset	Page 10-76
Kernel Registers:						
CMD	Command interface	20_H	U, SV	SV,P,SE,32	Application Reset	Page 10-85
STS	Status	24_H	U, SV	SV,P,SE,32	Application Reset	Page 10-86
FSP	FSP control	28_H	U, SV	SV,P,SE,32	Power-on Reset	Page 10-88
AGC	Alarm Global Configuration	$2C_H$	U, SV	SV,P,SE,32	Application Reset	Page 10-90
RTC	Recovery Timer Configuration	30_H	U, SV	SV,P,SE,32	Application Reset	Page 10-92
KEYS	Register access keys	34_H	U, SV	SV,P,SE,32	Application Reset	Page 10-93
DBG	Hardware debug	38_H	U, SV	SV,P,SE,32	Power-on Reset	Page 10-94
PCTL	FSP Port Control Register	$3C_H$	U, SV	SV,P,SE,32	Power-on Reset	Page 10-95
AFCNT	Alarm and Fault Counter Register	40_H	U, SV	SV,P,SE,32	Power-on Reset	Page 10-96
RTAC0	Recovery Timer 0 Alarm Configuration	60_H	U, SV	SV,P,SE,32	Application Reset	Page 10-97
RTAC1	Recovery Timer 1 Alarm Configuration	64_H	U, SV	SV,P,SE,32	Application Reset	Page 10-99
AG0CF0	Alarm configuration	100_H	U, SV	SV,P,SE,32	Application Reset	Page 10-101

Safety Management Unit (SMU)
External and internal alarm behavior

- External
  Fault signaling protocol (FSP)
  SMU_AGnFSP (n=0...11)
- Internal
  SMU_AGnCFx (n=0...11)
  (x=0-2) 3-bit code (Table 10-25) is spread over 3 registers



AGiFSP (i=0-11)
SMU_core FSP Configuration Register (0190$_H$+i*4) **Reset Value: Table 655**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
FE31	FE30	FE29	FE28	FE27	FE26	FE25	FE24	FE23	FE22	FE21	FE20	FE19	FE18	FE17	FE16
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
FE15	FE14	FE13	FE12	FE11	FE10	FE9	FE8	FE7	FE6	FE5	FE4	FE3	FE2	FE1	FE0
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Field	Bits	Type	Description
FEz (z=0-31)	z	rw	**Fault signaling configuration flag for alarm z belonging to alarm group i.** 0_B FSP disabled for this alarm event 1_B FSP enabled for this alarm event

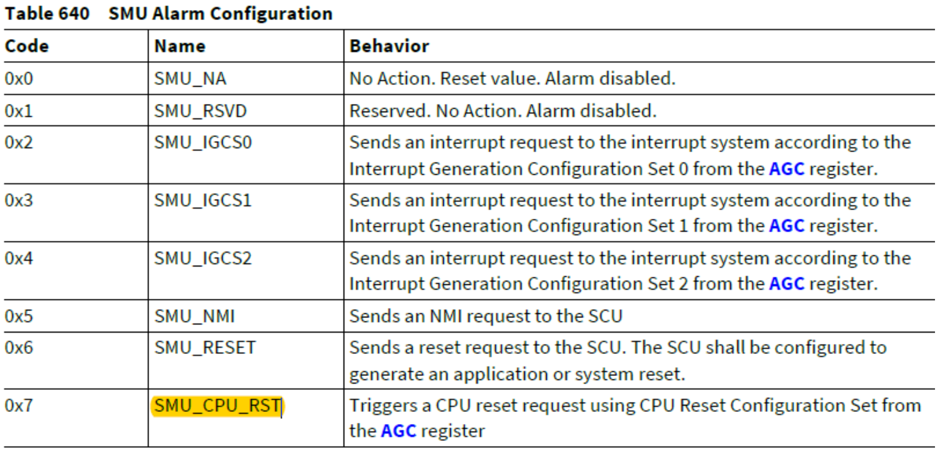
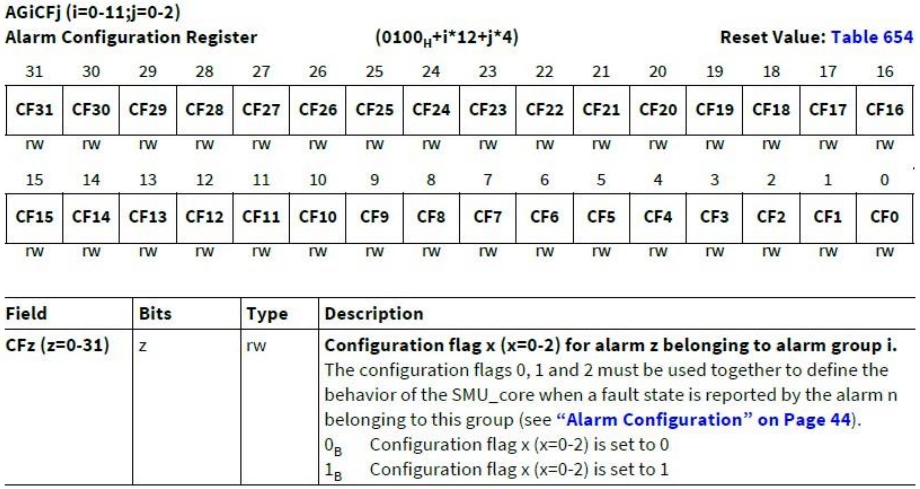


Table 640 SMU Alarm Configuration

Code	Name	Behavior
0x0	SMU_NA	No Action. Reset value. Alarm disabled.
0x1	SMU_RSVD	Reserved. No Action. Alarm disabled.
0x2	SMU_IGCS0	Sends an interrupt request to the interrupt system according to the Interrupt Generation Configuration Set 0 from the AGC register.
0x3	SMU_IGCS1	Sends an interrupt request to the interrupt system according to the Interrupt Generation Configuration Set 1 from the AGC register.
0x4	SMU_IGCS2	Sends an interrupt request to the interrupt system according to the Interrupt Generation Configuration Set 2 from the AGC register.
0x5	SMU_NMI	Sends an NMI request to the SCU
0x6	SMU_RESET	Sends a reset request to the SCU. The SCU shall be configured to generate an application or system reset.
0x7	SMU_CPU_RST	Triggers a CPU reset request using CPU Reset Configuration Set from the AGC register



AGiCFj (i=0-11;j=0-2)
Alarm Configuration Register (0100$_H$+i*12+j*4) **Reset Value: Table 654**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
CF31	CF30	CF29	CF28	CF27	CF26	CF25	CF24	CF23	CF22	CF21	CF20	CF19	CF18	CF17	CF16
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
CF15	CF14	CF13	CF12	CF11	CF10	CF9	CF8	CF7	CF6	CF5	CF4	CF3	CF2	CF1	CF0
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Field	Bits	Type	Description
CFz (z=0-31)	z	rw	**Configuration flag x (x=0-2) for alarm z belonging to alarm group i.** The configuration flags 0, 1 and 2 must be used together to define the behavior of the SMU_core when a fault state is reported by the alarm n belonging to this group (see **"Alarm Configuration" on Page 44**). 0_B Configuration flag x (x=0-2) is set to 0 1_B Configuration flag x (x=0-2) is set to 1

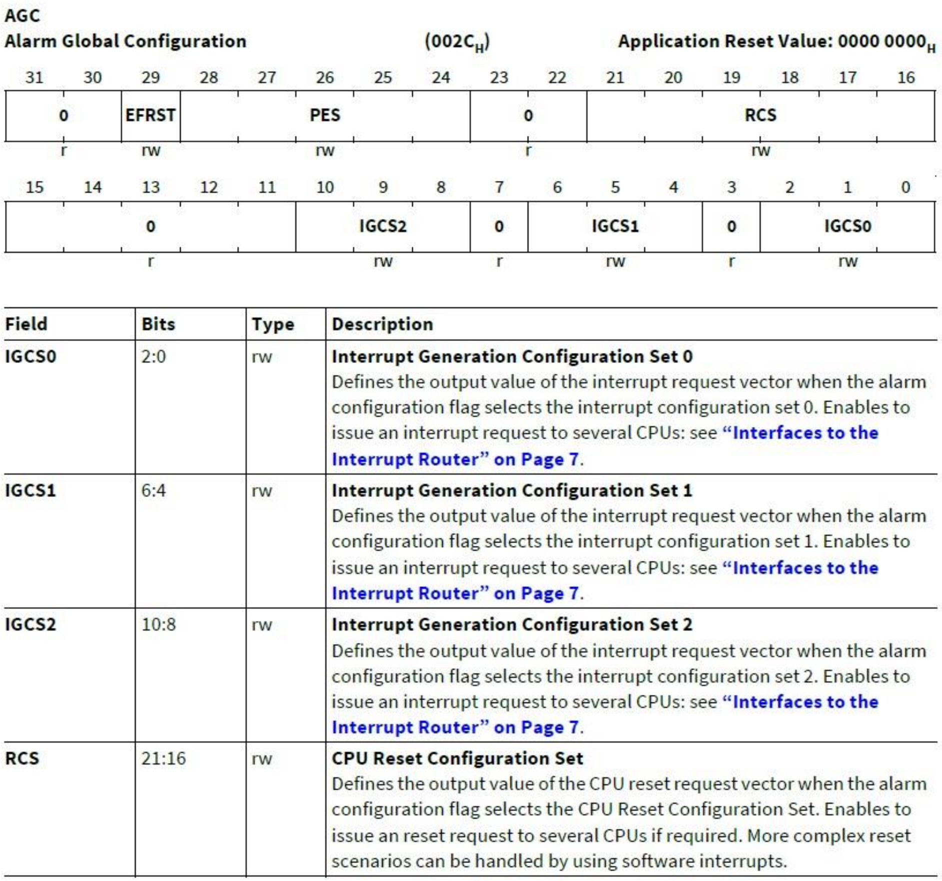
Safety Management Unit (SMU)
Internal alarm behavior: Alarm actions

- Available ***internal*** alarm actions:
  - No action (alarm disabled)
  - Generate an interrupt request (to one or all CPUs)
  - Generate an NMI request to all CPUs
  - Reset the microcontroller
  - Triggers a CPU reset request

Safety Management Unit (SMU)
Internal alarm behavior: Alarm Global Configuration

- Each bit in the Interrupt Generation Configuration Set SMU_AGC.IGCSn (n=0-2) configures one SMU Service Request SRC_SMUm (m=0-2)
- Example: ALM3[12] "EVR 1.3V digital over voltage" alarm should raise an
  CPU0 interrupt level 5 and
  CPU2 interrupt level 7

```
// Configure ALARM3[12] to use
// configurations set 0 (code 0x2)
SMU_AG3CF0[12]=0;
SMU_AG3CF1[12]=1;
SMU_AG3CF2[12]=0;

// select two outputs
SMU_AGC.IGCS0=3; // Two SRCs

// Service request TOS=CPU0,SRPN=5
SRC_SMU0= 0<<11 | 5;

// Service request TOS=CPU2,SRPN=7
SRC_SMU1= 2<<11 | 7;
```



AGC
Alarm Global Configuration (002C$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0		EFRST	PES					0		RCS					
r		rw	rw					r		rw					

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0					IGCS2			0	IGCS1			0	IGCS0		
r					rw			r	rw			r	rw		

Field	Bits	Type	Description
IGCS0	2:0	rw	**Interrupt Generation Configuration Set 0** Defines the output value of the interrupt request vector when the alarm configuration flag selects the interrupt configuration set 0. Enables to issue an interrupt request to several CPUs: see **"Interfaces to the Interrupt Router" on Page 7**.
IGCS1	6:4	rw	**Interrupt Generation Configuration Set 1** Defines the output value of the interrupt request vector when the alarm configuration flag selects the interrupt configuration set 1. Enables to issue an interrupt request to several CPUs: see **"Interfaces to the Interrupt Router" on Page 7**.
IGCS2	10:8	rw	**Interrupt Generation Configuration Set 2** Defines the output value of the interrupt request vector when the alarm configuration flag selects the interrupt configuration set 2. Enables to issue an interrupt request to several CPUs: see **"Interfaces to the Interrupt Router" on Page 7**.
RCS	21:16	rw	**CPU Reset Configuration Set** Defines the output value of the CPU reset request vector when the alarm configuration flag selects the CPU Reset Configuration Set. Enables to issue an reset request to several CPUs if required. More complex reset scenarios can be handled by using software interrupts.

Safety Management Unit (SMU)
External alarm behavior: Alarm actions

- Alarms can also trigger ***external*** alarm actions:
  - Assert fault state using **fault signaling protocol** (error pin)
  - Assert the port emergency stop
    - Enabled port pins switch from output mode to input mode (optionally with internal pull-up)

Safety Management Unit (SMU)

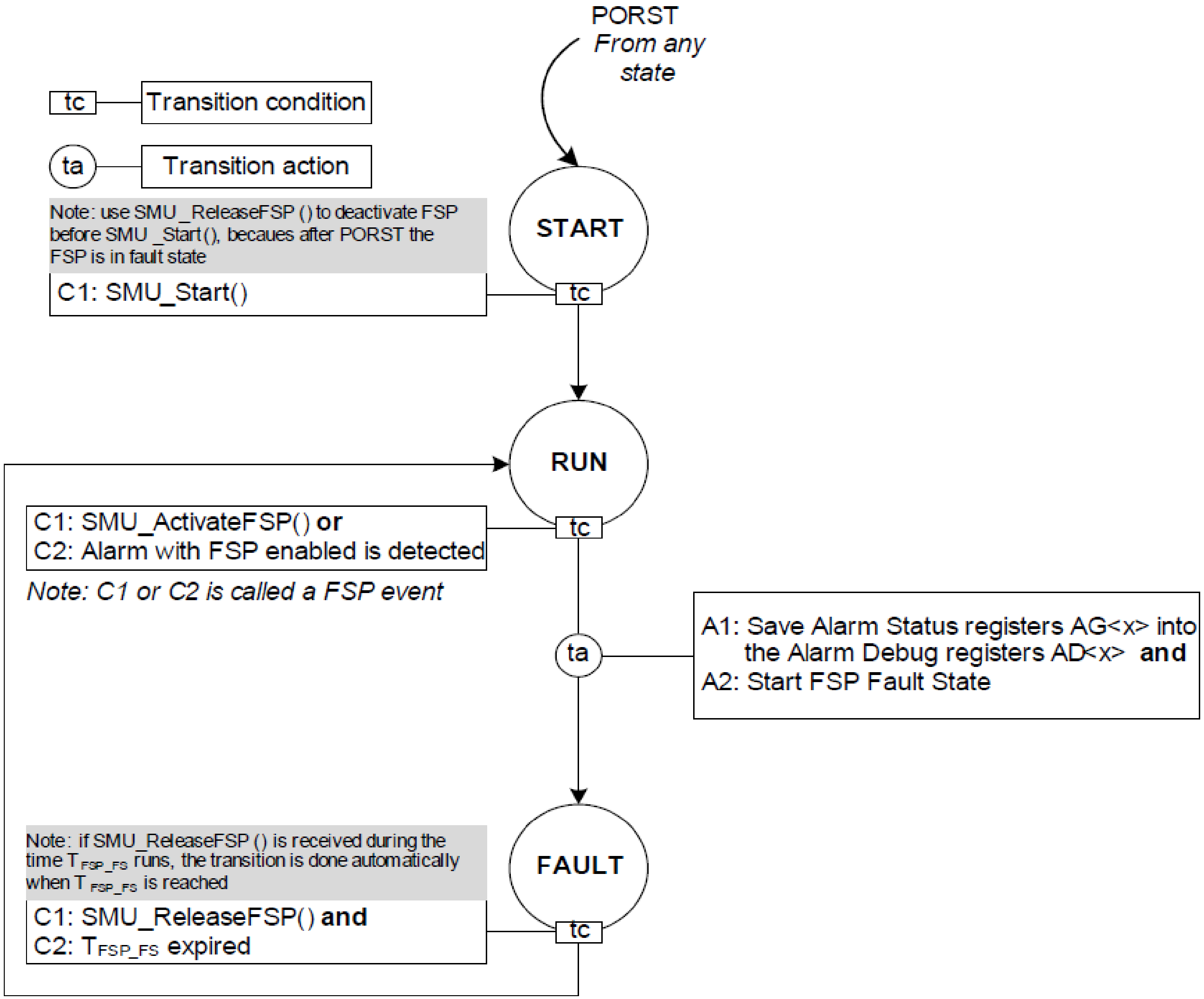
External alarm behavior: Fault Signaling protocol (Error pin)

- The error pin is push-pull active-low
  - low: error detected, system must be in a safe state
  - high: no error, system is free to work
- During a power on reset the error pin has high impedance
- After a power on reset the error pin is low, until set to high by SW
- SW sets SetErrorPin flag to zero/one, the error pin shall go to low/high
- A status flag represent the current logic status

Safety Management Unit (SMU)

SMU state machine (SSM): transition conditions and actions

Requirement: Any reset triggered by SW shall have no effect on the SSM



Note: use SMU_ReleaseFSP () to deactivate FSP before SMU _Start (), becaues after PORST the FSP is in fault state

C1: SMU_Start()

C1: SMU_ActivateFSP() **or**
C2: Alarm with FSP enabled is detected

Note: C1 or C2 is called a FSP event

A1: Save Alarm Status registers AG<x> into the Alarm Debug registers AD<x> **and**
A2: Start FSP Fault State

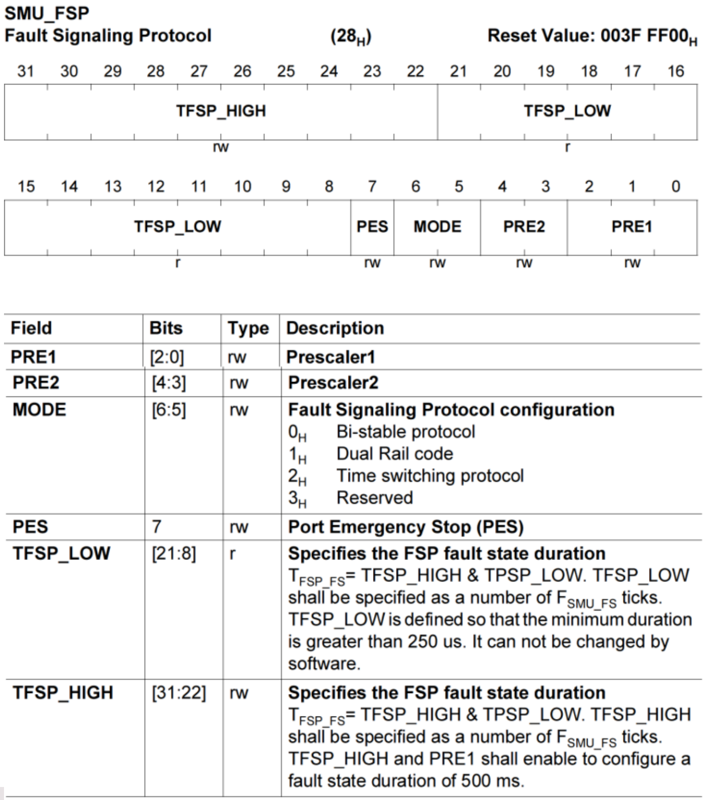
Note: if SMU_ReleaseFSP () is received during the time T_{FSP_FS} runs, the transition is done automatically when T_{FSP_FS} is reached

C1: SMU_ReleaseFSP() **and**
C2: T_{FSP_FS} expired

Safety Management Unit (SMU)
External alarm behavior: Fault Signaling Protocol (FSP)

- The Fault Signaling Protocol enables the microcontroller to report a critical situation to an external safety controller device in order to control the safe state of the safety system.
- Three different protocol modes can be configured
  - Bi-stable protocol (default)
  - Dynamic dual-rail protocol*
  - Time-switching protocol
- Two Prescaler define
  - Fault State Tick (PRE1) f_{SMU_FS}
  - Fault Free Tick (PRE2) f_{SMU_FFS}
- Min/Max of Fault State defined by TFSP_LOW/TFSP_HIGH

* not connected in AURIX™ Family



SMU_FSP
Fault Signaling Protocol **(28_H)** **Reset Value: 003F FF00_H**

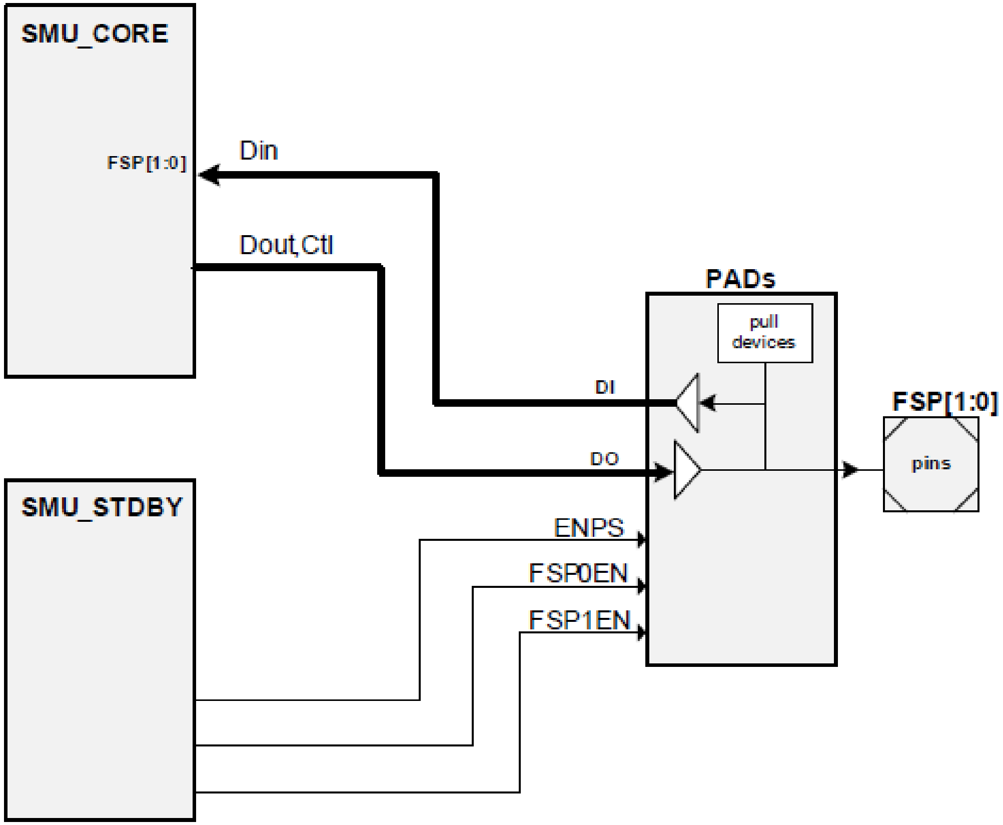
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
TFSP_HIGH										TFSP_LOW					
rw										r					

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
TFSP_LOW								PES	MODE		PRE2		PRE1		
r								rw	rw		rw		rw		

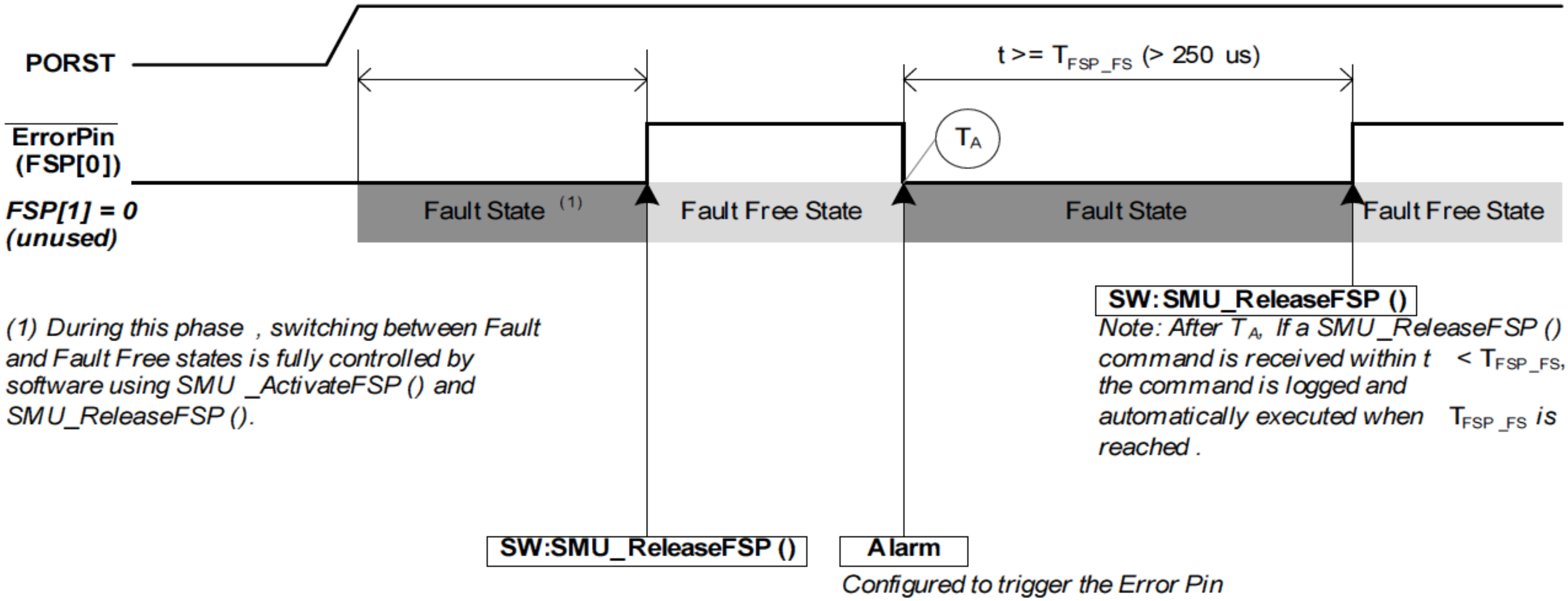
Field	Bits	Type	Description
PRE1	[2:0]	rw	**Prescaler1**
PRE2	[4:3]	rw	**Prescaler2**
MODE	[6:5]	rw	**Fault Signaling Protocol configuration** 0_H Bi-stable protocol 1_H Dual Rail code 2_H Time switching protocol 3_H Reserved
PES	7	rw	**Port Emergency Stop (PES)**
TFSP_LOW	[21:8]	r	**Specifies the FSP fault state duration** T_{FSP_FS}= TFSP_HIGH & TPSP_LOW. TFSP_LOW shall be specified as a number of F_{SMU_FS} ticks. TFSP_LOW is defined so that the minimum duration is greater than 250 us. It can not be changed by software.
TFSP_HIGH	[31:22]	rw	**Specifies the FSP fault state duration** T_{FSP_FS}= TFSP_HIGH & TPSP_LOW. TFSP_HIGH shall be specified as a number of F_{SMU_FS} ticks. TFSP_HIGH and PRE1 shall enable to configure a fault state duration of 500 ms.

FSP pins

- FSP protocol layer block to support all 3 protocol:
  - Bi-stable (default)
  - Dynamic dual-rail
  - Time-switching protocols
- FSP status is generated/decoded by the FSP Protocol layer in SMU_CORE domain.
- FSP0EN (FSP[0]) and FSP1EN (FSP[1]) are controlled by the register CMD_STDBY.



Safety Management Unit (SMU)
Fault Signaling Protocol (FSP): Bi-stable fault



PORST

ErrorPin (FSP[0])

FSP[1] = 0 (unused)

t >= T_{FSP_FS} (> 250 us)

T_A

Fault State [1]

Fault Free State

Fault State

Fault Free State

SW:SMU_ReleaseFSP ()

Note: After T_A, If a SMU_ReleaseFSP () command is received within t < T_{FSP_FS}, the command is logged and automatically executed when T_{FSP_FS} is reached .

SW:SMU_ReleaseFSP ()

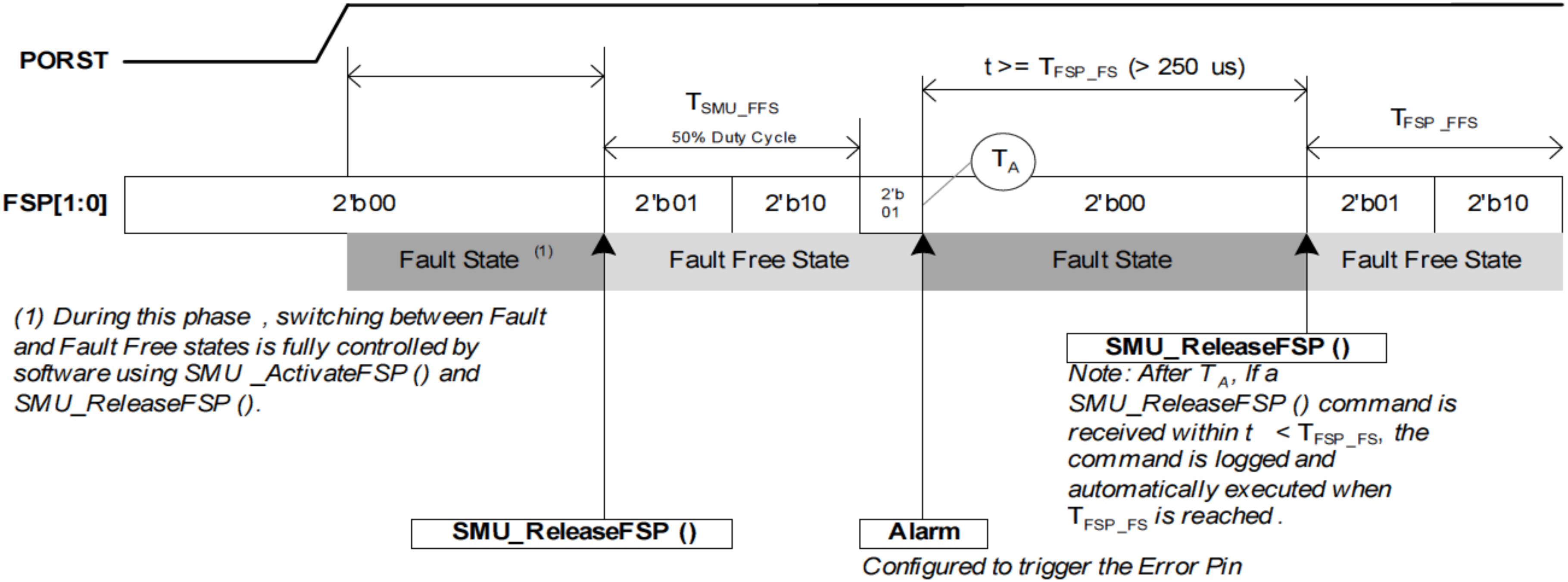
Alarm

Configured to trigger the Error Pin

(1) During this phase , switching between Fault and Fault Free states is fully controlled by software using SMU _ActivateFSP () and SMU_ReleaseFSP ().

Safety Management Unit (SMU)

Fault Signaling Protocol (FSP): Dynamic dual-rail fault



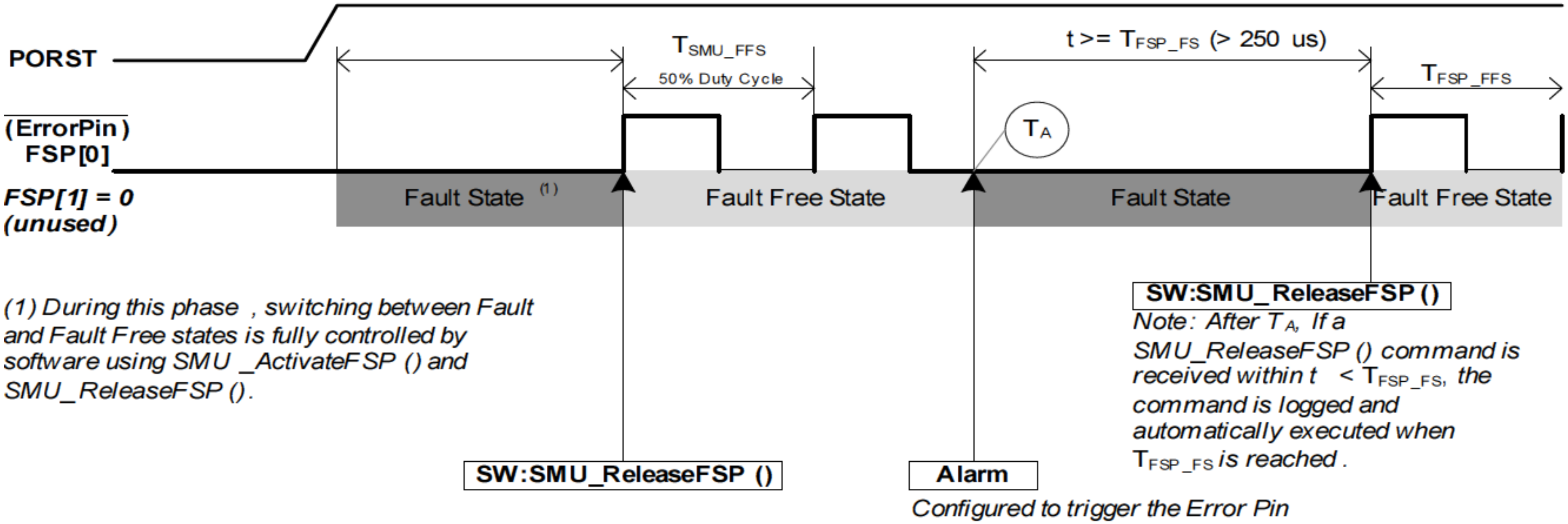
(1) During this phase , switching between Fault and Fault Free states is fully controlled by software using SMU _ActivateFSP () and SMU_ReleaseFSP ().

Configured to trigger the Error Pin

Note: After T_A, If a SMU_ReleaseFSP () command is received within t < T_{FSP_FS}, the command is logged and automatically executed when T_{FSP_FS} is reached.

Safety Management Unit (SMU)

Fault Signaling Protocol (FSP): Time switching protocol



(1) During this phase , switching between Fault and Fault Free states is fully controlled by software using SMU _ActivateF SP () and SMU_ReleaseFSP ().

Configured to trigger the Error Pin

Note: After T_A, If a SMU_ReleaseFSP () command is received within t < T_{FSP_FS}, the command is logged and automatically executed when T_{FSP_FS} is reached .

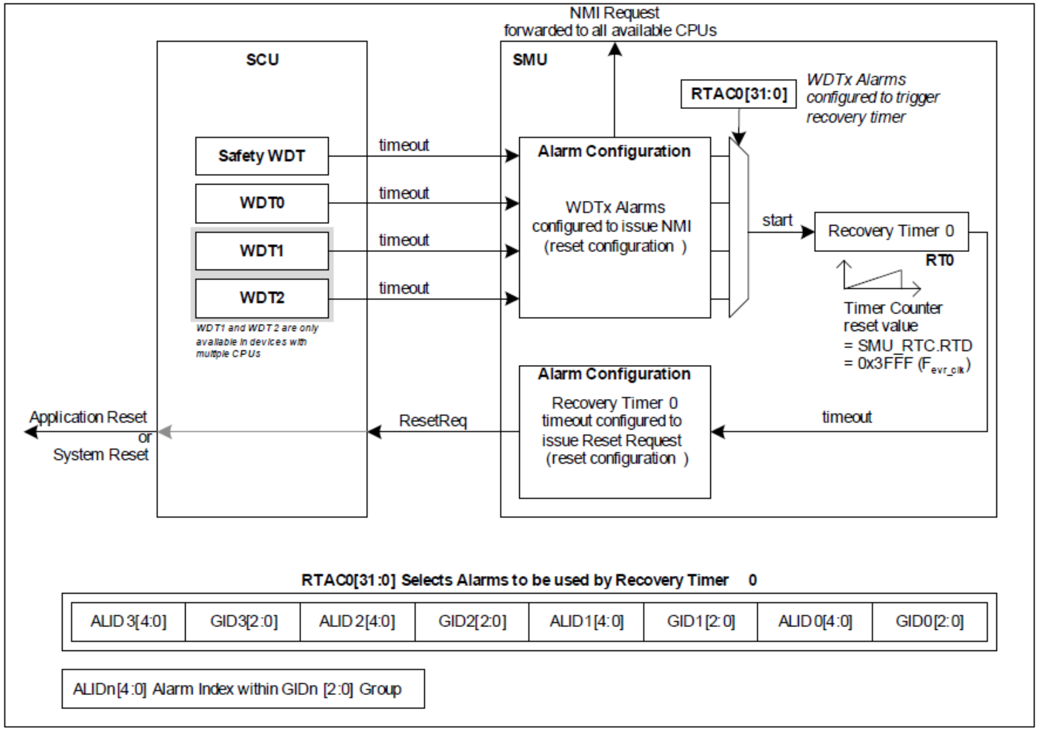
Recovery Timer

- Recovery timers allow time to react to alarms and attempt a recovery before a time-out occurs
  - If enabled, an alarm starts the recovery timer
  - At the same time, the alarm triggers an NMI or interrupt to start an error handler
  - The error handler software can attempt recovery, and if successful, stop the recovery timer
  - If the recovery timer is not stopped, it results in a recovery timer time-out alarm
    - The user can configure the action for this time-out alarm (for example, trigger a reset)

- The SCU implements two recovery timers
  - Each recovery timer can be started by up to four alarms

Recovery Timer and Watchdog Alarms

- Recovery timer 0 is used to support watchdog functionality
  - A watchdog time-out alarm triggers a NMI pre-warning to the CPUs
  - At the same time, recovery timer 0 is started
  - The recovery timer time-out triggers a reset


NMI Request
forwarded to all available CPUs
SCU
SMU
RTAC0[31:0]
WDTx Alarms configured to trigger recovery timer
Safety WDT
WDT0
WDT1
WDT2
timeout
timeout
timeout
timeout
Alarm Configuration
WDTx Alarms configured to issue NMI (reset configuration)
start
Recovery Timer 0
RT0
Timer Counter reset value
= SMU_RTC.RTD
= 0x3FFF (F_evr_clk)
WDT1 and WDT2 are only available in devices with multiple CPUs
Alarm Configuration
Recovery Timer 0 timeout configured to issue Reset Request (reset configuration)
timeout
ResetReq
Application Reset or System Reset

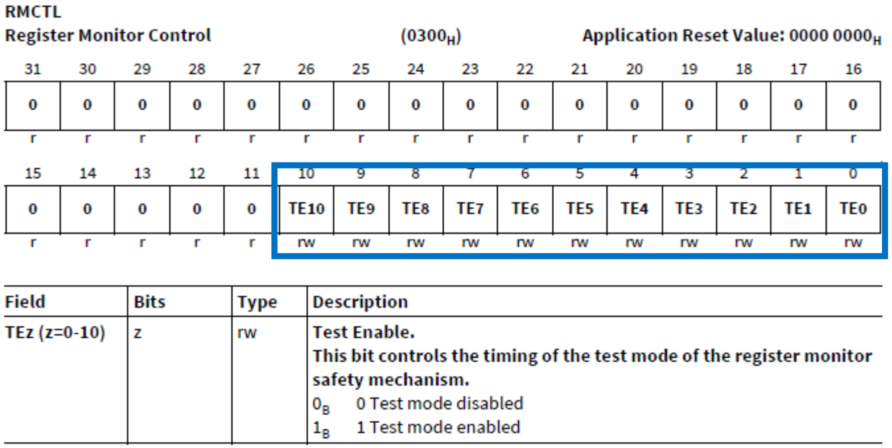
RTAC0[31:0] Selects Alarms to be used by Recovery Timer 0

ALID 3[4:0]	GID3[2:0]	ALID 2[4:0]	GID2[2:0]	ALID 1[4:0]	GID1[2:0]	ALID 0[4:0]	GID0[2:0]

ALIDn[4:0] Alarm Index within GIDn [2:0] Group

SFF Register Monitor

RMCTL, RMEF and RMSTS: Separated control and status bits per IP with SFFs



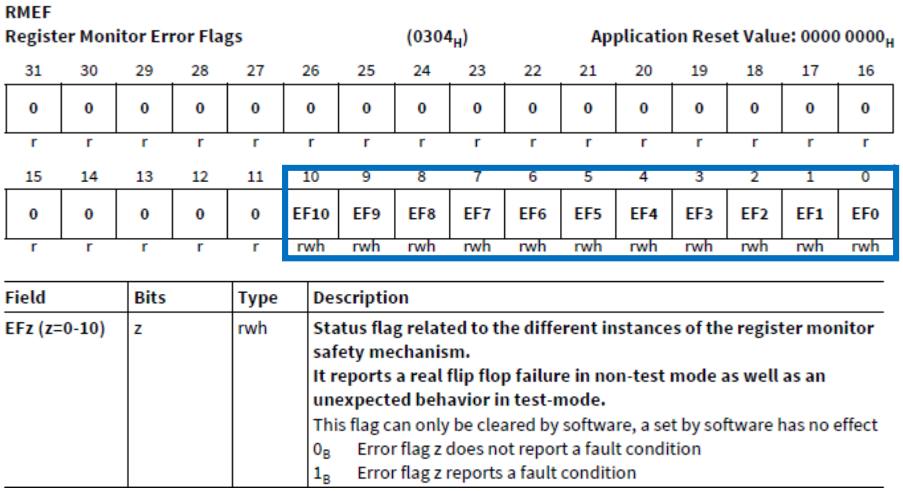
RMCTL
Register Monitor Control (0300$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	TE10	TE9	TE8	TE7	TE6	TE5	TE4	TE3	TE2	TE1	TE0
r	r	r	r	r	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Field	Bits	Type	Description
TEz (z=0-10)	z	rw	**Test Enable.** **This bit controls the timing of the test mode of the register monitor safety mechanism.** 0_B 0 Test mode disabled 1_B 1 Test mode enabled

SMU_RMEF[0]	MTU
SMU_RMEF[1]	IOM
SMU_RMEF[2]	IR
SMU_RMEF[3]	EMEM
SMU_RMEF[4]	SCU/SRU
SMU_RMEF[5]	PMS
SMU_RMEF[6]	DMA
SMU_RMEF[7]	SMU_core
SMU_RMEF[8]	CERBERUS
SMU_RMEF[9]	SYS_PLL/PER_PLL
SMU_RMEF[10]	CCU

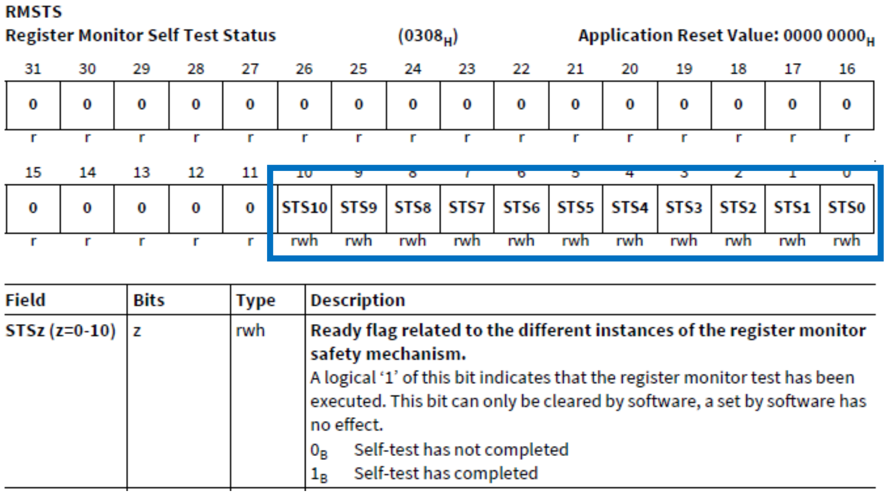


RMEF
Register Monitor Error Flags (0304$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	EF10	EF9	EF8	EF7	EF6	EF5	EF4	EF3	EF2	EF1	EF0
r	r	r	r	r	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh

Field	Bits	Type	Description
EFz (z=0-10)	z	rwh	**Status flag related to the different instances of the register monitor safety mechanism.** **It reports a real flip flop failure in non-test mode as well as an unexpected behavior in test-mode.** This flag can only be cleared by software, a set by software has no effect 0_B Error flag z does not report a fault condition 1_B Error flag z reports a fault condition



RMSTS
Register Monitor Self Test Status (0308$_H$) **Application Reset Value: 0000 0000$_H$**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	STS10	STS9	STS8	STS7	STS6	STS5	STS4	STS3	STS2	STS1	STS0
r	r	r	r	r	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh	rwh

Field	Bits	Type	Description
STSz (z=0-10)	z	rwh	**Ready flag related to the different instances of the register monitor safety mechanism.** A logical '1' of this bit indicates that the register monitor test has been executed. This bit can only be cleared by software, a set by software has no effect. 0_B Self-test has not completed 1_B Self-test has completed

Part of your life. Part of tomorrow.