NXP Semiconductors
Application Note

Document Number: AN5259
Rev. 0, 04/2016

MPC574xP FCCU Fault Sources

Detailed Description

By: Peter Vlna

1. Introduction

This document describes the FCCU fault sources in detail. Because the fault-handling mechanisms are getting more and more complicated, it is necessary to understand fault managing on the MPC57xx devices.

Contents

2. Important FCCU Notes for MPC57xx Devices

All faults on the MPC57xx devices are non-critical by default. Define which faults are important and which faults to tolerate using the FCCU configuration registers. The default behavior when a fault is encountered is not to react.

3. FCCU fault sources mapping

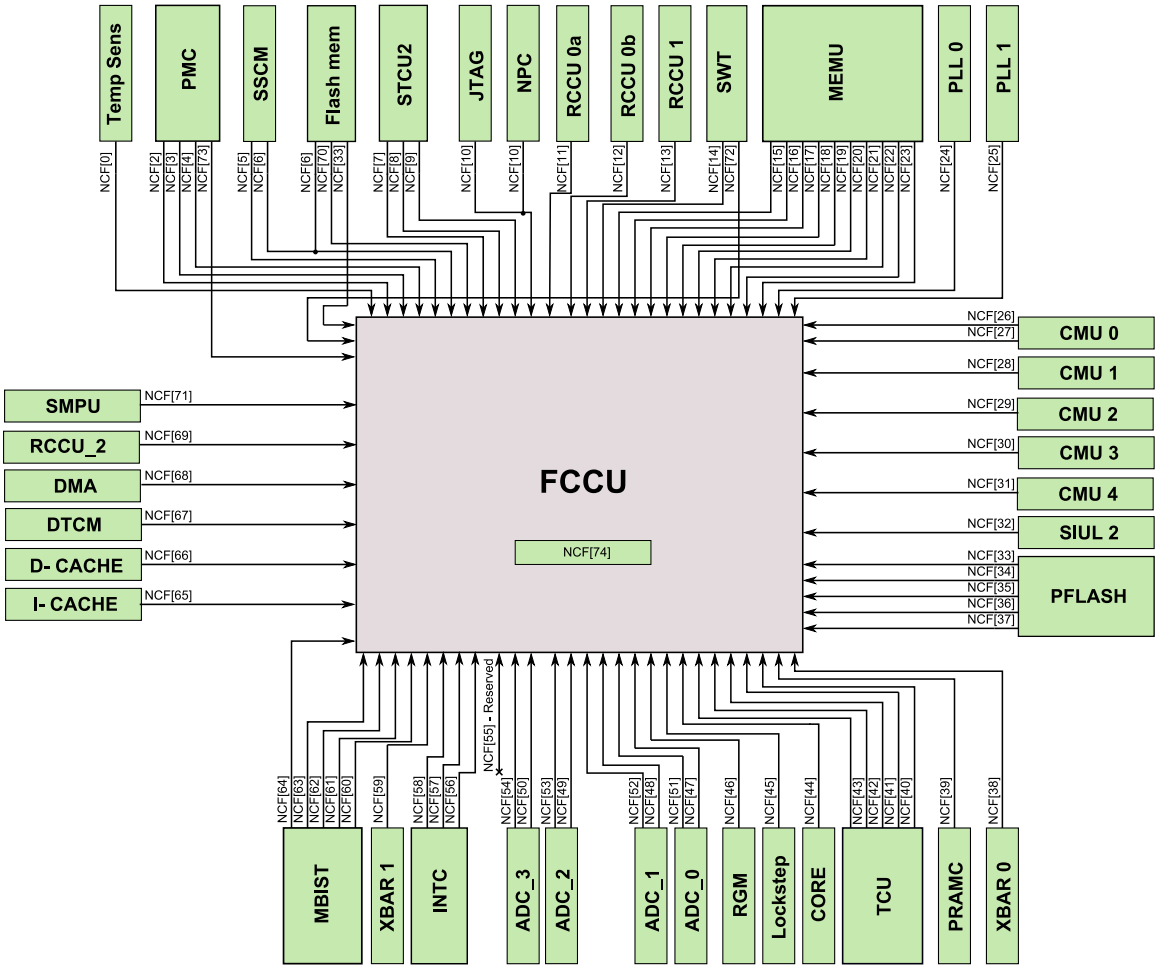

Figure 1. FCCU fault mapping

4. FCCU Fault Sources for MPC5744P

Table 1. FCCU Non-critical faults mapping

Non-critical fault	Source	Signal description
NCF[0]	Temp Sens 0/1	*Temperature out of range 0/1*
NCF[1]	Reserved	—
NCF[2]	PMC	*LVDs Ored*
NCF[3]	PMC	*HVDs Ored*
NCF[4]	PMC	*Safety error (BIST)*
NCF[5]	DCF/SSCM	*Memories DCF client safety error*
NCF[6]	SSCM/flash memory	*Safety error: SSCM transfer error (during STCU2 configuration loading) ORed with flash memory reset error*
NCF[7]	STCU2	*STCU2 fault condition (run in application mode)*
NCF[8]	STCU2	*BIST results (critical faults)*
NCF[9]	STCU2	*BIST results (non-critical faults)*
NCF[10]	JTAGC_NPC_MON	*JTAG/NPC monitor*
NCF[11]	RCCU_0a	*Core redundancy mismatch: interface (other than D-MEM or DMA) out of lockstep*
NCF[12]	RCCU_0b	*Core redundancy mismatch: D-MEM array interface out of lockstep*
NCF[13]	RCCU_1	*Core redundancy mismatch: DMA array interface out of lockstep*
NCF[14]	SWT_0	*Software watchdog timer*
NCF[15]	MEMU	*System RAMs correctable ECC error*
NCF[16]	MEMU	*System RAMs uncorrectable ECC error*
NCF[17]	MEMU	*System RAMs error overflow (ORing of all overflows)*
NCF[18]	MEMU	*Peripheral RAMs correctable ECC error*
NCF[19]	MEMU	*Peripheral RAMs uncorrectable ECC error*
NCF[20]	MEMU	*Peripheral RAMs error overflow (ORing of all overflows)*
NCF[21]	MEMU	*Flash correctable ECC error*
NCF[22]	MEMU	*Flash uncorrectable ECC error*
NCF[23]	MEMU	*Flash error overflow (ORing of all overflows)*
NCF[24]	PLL_0	*PLL Loss of lock*
NCF[25]	PLL_1	*PLL Loss of lock*
NCF[26]	CMU_0	*XOSC vs. IRCOSC clock frequency out of range*
NCF[27]	CMU_0	*Motor clock frequency out of range*
NCF[28]	CMU_1	*Core frequency out of range*
NCF[29]	CMU_2	*PBRIDGE frequency out of range*
NCF[30]	CMU_3	*ADC clock frequency out of range*
NCF[31]	CMU_4	*SENT frequency out of range*
NCF[32]	SIUL2	*Error input pin*
NCF[33]	PFLASH and embedded flash memory	*Address Encode Error ORed with voltage and current error of flash memory array.*
NCF[34]	PFLASH	*Error in the ECC correction logic through an EDC*
NCF[35]	PFLASH	*Alarm indicating the flash memory controller detected an error in the address ECC manipulation logic through an EDC*
NCF[36]	PFLASH	*Alarm indicating the flash memory controller detected a transaction monitor mismatch when compared to the flash safety feedback outputs*
NCF[37]	PFLASH	*Alarm indicating the flash memory controller detected a transaction monitor mismatch in the pseudo-replicated calibration evaluation hardware*
NCF[38]	XBAR	*XBAR transaction monitor mismatch*
NCF[39]	PRAMC	*System RAM controller alarm*
NCF[40]	TCU DFT0	*Combination of safety critical signals from TCU*

Table 1. FCCU Non-critical faults mapping

Non-critical fault	Source	Signal description
NCF[41]	TCU DFT1	*Combination of safety critical signals from TCU*
NCF[42]	TCU DFT2	*Combination of safety critical signals from TCU*
NCF[43]	TCU DFT3	*Combination of safety critical signals from TCU*
NCF[44]	Core	*Safety core exception indication*
NCF[45]	Lockstep	*Indication of disablement of Checker Core and DMA as well as RCCUs*
NCF[46]	MC_RGM	*Safe mode request*
NCF[47]	ADC_0_CF	*Internal self test*
NCF[48]	ADC_1_CF	*Internal self test*
NCF[49]	ADC_2_CF	*Internal self test*
NCF[50]	ADC_3_CF	*Internal self test*
NCF[51]	ADC_0_NCF	*Internal self test*
NCF[52]	ADC_1_NCF	*Internal self test*
NCF[53]	ADC_2_NCF	*Internal self test*
NCF[54]	ADC_3_NCF	*Internal self test*
NCF[55]	Reserved	—
NCF[56]	INTC_MON_0	*INTC latency monitor*
NCF[57]	INTC_MON_1	*INTC latency monitor*
NCF[58]	INTC_MON_2	*INTC latency monitor*
NCF[59]	SIPI/DMA/Ethernet concentrator	*SIPI_DMA_Ethernet concentrator transaction monitor mismatch*
NCF[60]	MBIST: D-cache	*Multiple D-cache and D-cache tag memory cuts*
NCF[61]	MBIST: I-cache	*Multiple I-cache and I-cache tag memory cuts*
NCF[62]	MBIST: D-MEM	*Multiple D-MEM memory cuts*
NCF[63]	MBIST: SRAM	*Multiple system RAM memory cuts*
NCF[64]	MBIST: peripherals	*Multiple CAN, FlexRay, Ethernet, and DMA memory cuts*
NCF[65]	I-cache	*I-cache memory feedback alarm*
NCF[66]	D-cache	*D-cache memory feedback alarm*
NCF[67]	DTCM	*Data TCM memory feedback alarm*
NCF[68]	DMA	*DMA memory feedback alarm*
NCF[69]	RCCU_2	*Redundancy mismatch: DSMC D-MEM out of lockstep*
NCF[70]	Flash memory	*Flash memory low power entry error: failure to enter Stop mode upon Stop mode entry request*
NCF[71]	SMPU	*SMPU transaction monitor mismatch*
NCF[72]	SWT_0	*First timeout interrupt request from Software Watchdog of Safety Core*
NCF[73]	PMC DCF	*Digital PMC initialization error during DCF data load (status is cleared if the fault is not persistent)*
NCF[74]	FCCU DCF	*Misconfiguration of error_out pin interface of the FCCU after reset (overwriting the respective configuration bits resolves this error)*

5. Faults Description

The following sections describe the particular faults.

5.1. Temperature out of range 0/1

This device contains two temperature sensor modules (TSENS_0 and TSENS_1), located in different peripheral lakes.

The junction temperature sensor generates output voltage that is directly proportional to the internal junction temperature of the device. Use the information provided by this sensor to implement an intelligent power control (such as reducing the frequency when the temperature is too high).

When the temperature exceeds the thresholds, the FCCU is informed about this event and takes appropriate actions, but the PMC can also send a request for reset to the RGM module if the PMC is configured to do so in the temperature reset event enable register (PMC_REE_TD).

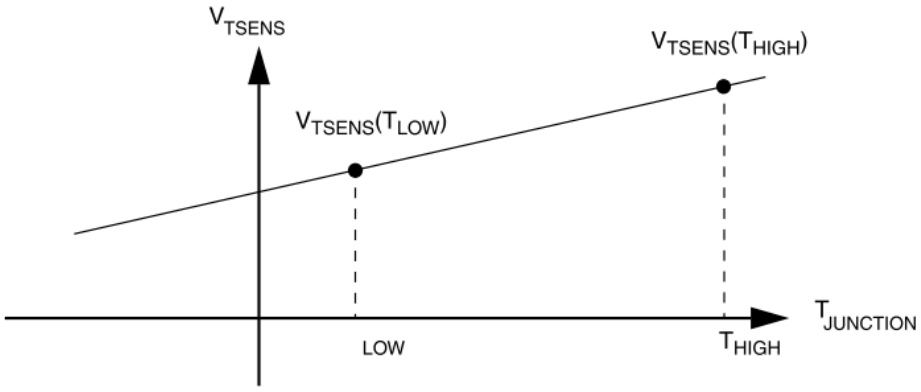

Figure 2. TSENS thresholds

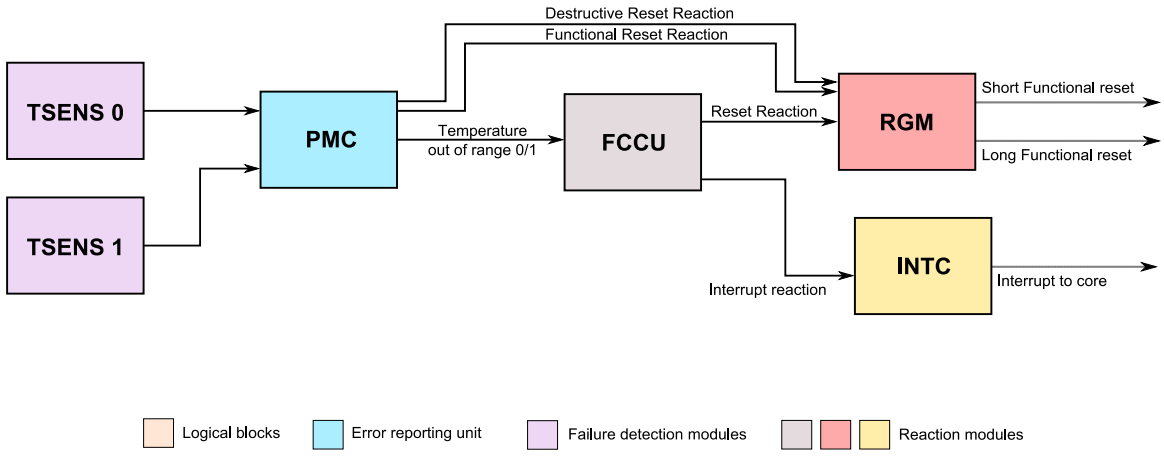

Figure 3. Temperature out of range 0/1

5.2. LVDs Ored

The PMC (Power Management Control unit) monitors the supply signals to generate the LVD events. When the voltage drops below the desired threshold, the PMC is informed and sends a fault signal to the FCCU.

- Regulator supply (VDDREG)
- Digital 1.2 V supply (LVD CORE)
- FLASH HV supply
- IO's HV supply
- ADC HV supply
- OSC HV supply
- LVD 1.2 V supply (LVD CORE BK)

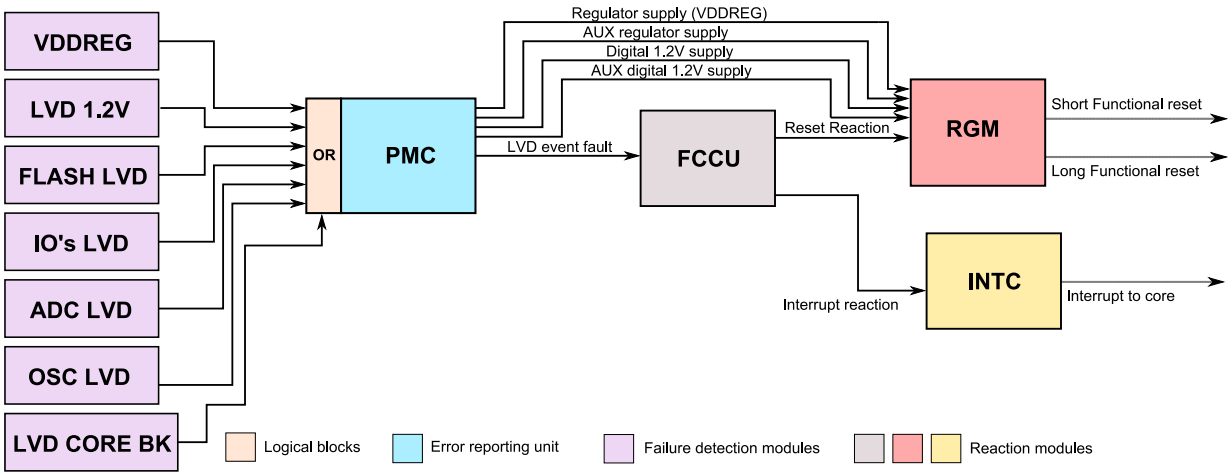

Figure 4. LVDs ORed

NOTE

A direct path from the PMC is implemented in case the FCCU is not able to react on a fault to prevent the device from damage or destruction. The direct reset path thresholds are set slightly lower than for the LVD event fault reported to the FCCU.

5.3. HVDs Ored

There are two HVD detectors. If a HVD detects a voltage above the maximum defined threshold, it sends a signal to the PMC. The PMC then sends the HVD event fault signal to the FCCU (as shown in Figure 4). The HVDs are:

1. HVD_CORE—high-voltage detector for the 1.25 V digital core supply (VDD_LV).
2. HVD_CORE_BK—high-voltage detector for the self-test of the HVD_CORE.

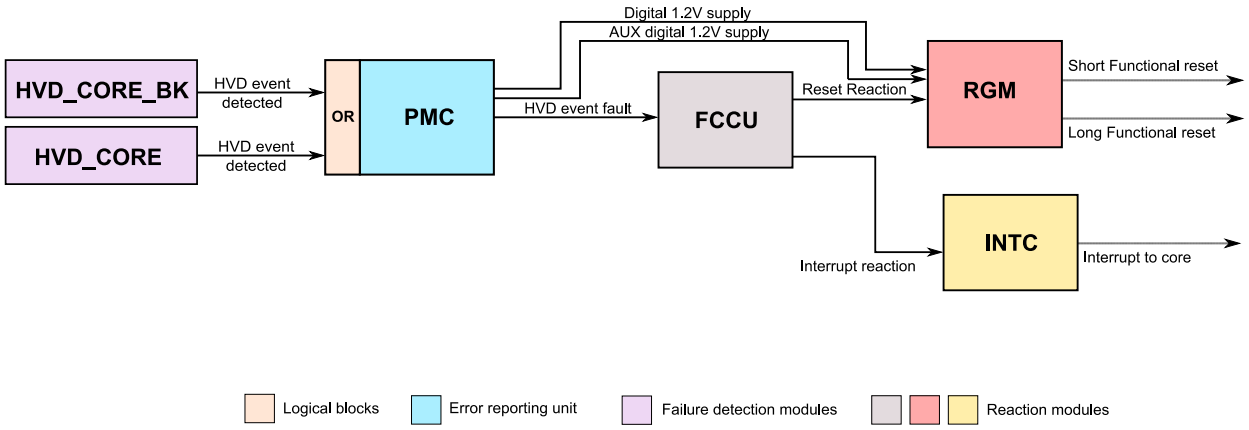

Figure 5. HVDs ORed

NOTE

A direct path from the PMC is implemented in case the FCCU is not able to react on a fault to prevent the device from damage or destruction. The direct reset path thresholds are set slightly lower than for the HVD event fault reported to the FCCU.

5.4. Safety error (BIST)

The safety error (BIST) fault is triggered when the LVD/HVD self-test fails. The PMC module contains a self-test to test the LVD/HVD and bandgap detectors. When this self-test fails, the PMC signals this failure to the FCCU module.

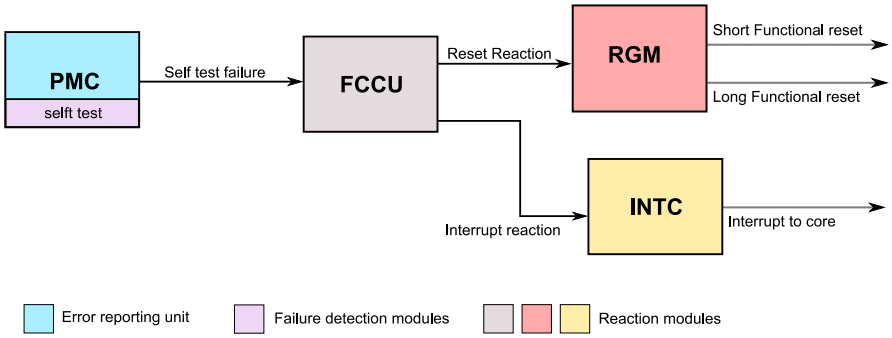

Figure 6. Safety error (BIST)

5.5. Memories DCF client safety error

The memories DCF client safety error is triggered when the DCF client reports an error to the SSCM (e.g., a triple voting violation is detected in the configuration registers within the DCF client). This error in the DCF client is forwarded to the FCCU by the SSCM.

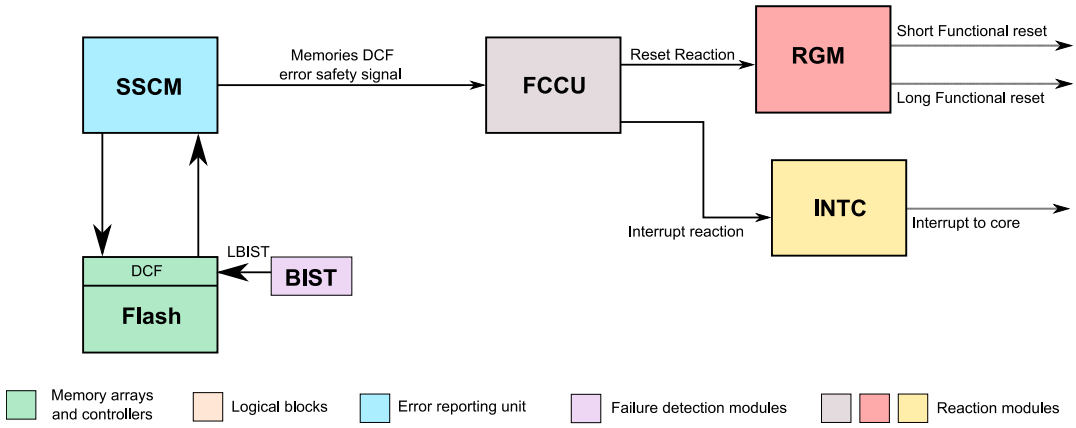

Figure 7. Memories DCF client safety error

5.6. Safety error: SSCM transfer error (during STCU2 configuration loading) ORed with flash memory reset error

The default chip configuration is stored in the DCF records. While the STCU configuration is being loaded from the DCF record flash memory, a fault can occur. To signal that the STCU loading is not done correctly, the SSCM module sends out an error signal to the FCCU.

This fault is also set when the flash memory encounters errors during its reset reads. This is caused by the ECC double-bit detections on the reset reads, as well as the coherency checks done on the test-row reads.

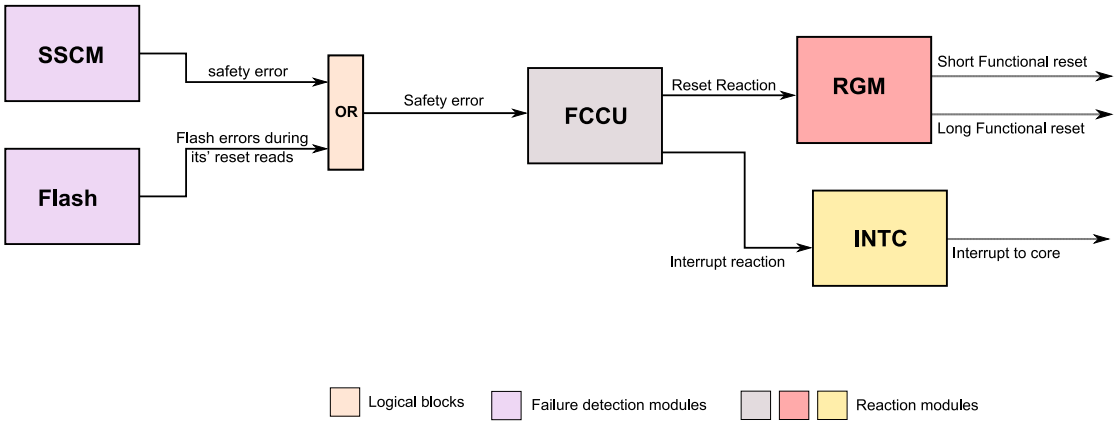

Figure 8. Safety error: SSCM transfer error

5.7. STCU2 fault condition (run in application mode)

The STCU module is the source of this signal. The STCU2 fault condition (run in the application mode) is triggered when the LBIST/MBIST control signals are getting into an unexpected state during application runtime, potentially putting a LBIST partition or a RAM array into the BIST mode during application execution.

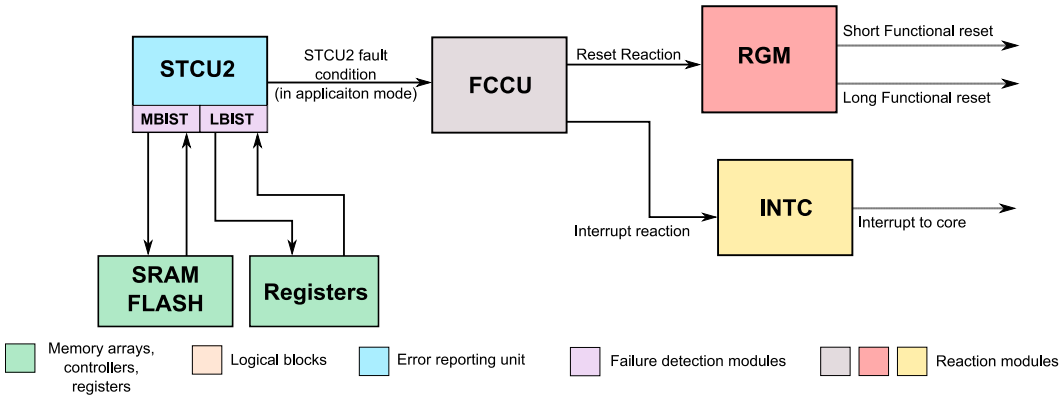

Figure 9. STCU2 fault condition (run in application mode)

5.8. BIST results (critical faults)

The BIST results (critical faults) signal triggers when the built-in self-test (LBIST/MBIST) finds a fault that is configured as unrecoverable. Although the built-in self-test is implemented to detect a permanent fault, it can be also triggered in case of transient faults. Therefore, the triggering of this signal does not mean that there is a permanent fault. A rerun may be appropriate.

In any case, this FCCU input triggers only during BIST execution (not when there is no BIST being executed).

The rate associated with this fault depends on the configuration of unrecoverable faults (critical faults) in the BIST DCF records, and it can range from 0 (none of the BISTs are configured as unrecoverable) to nearly the complete permanent and transient rate of the SoC (in case all MBIST RAMs and LBIST partitions are configured as unrecoverable).

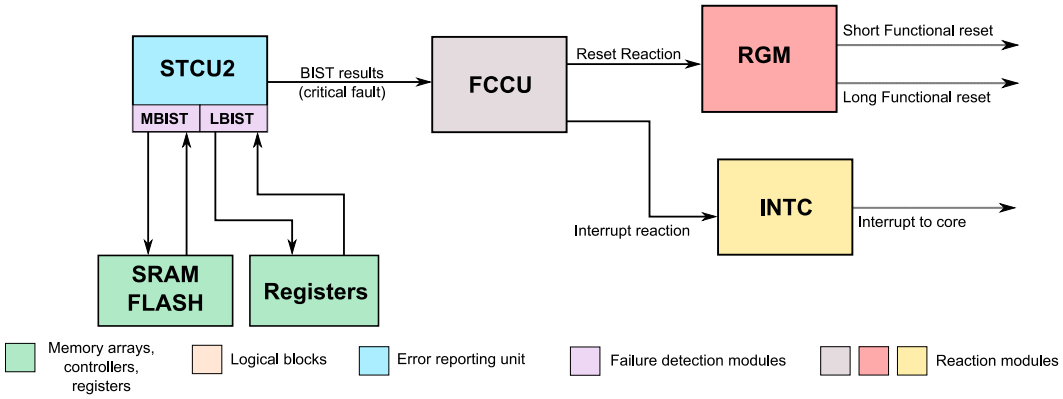

Figure 10. BIST results (critical faults)

5.9. BIST results (non-critical faults)

The BIST results (non-critical faults) signal triggers when the built-in self-test (LBIST/MBIST) finds a fault which is configured as recoverable. Although the built-in self-test is implemented to detect a permanent fault, it can be also triggered in case of transient faults. Therefore, the triggering of this signal does not mean that there is a permanent fault. A rerun may be appropriate.

In any case, this FCCU input triggers only during BIST execution (not when there is no BIST being executed).

The rate associated with this fault depends on the configuration of the recoverable faults (non-critical faults) in the BIST DCF records and can range from 0 (none of the BISTs are configured as recoverable) to nearly the complete permanent and transient rate of the SoC (in case all MBIST RAMs and LBIST partitions are configured as recoverable).

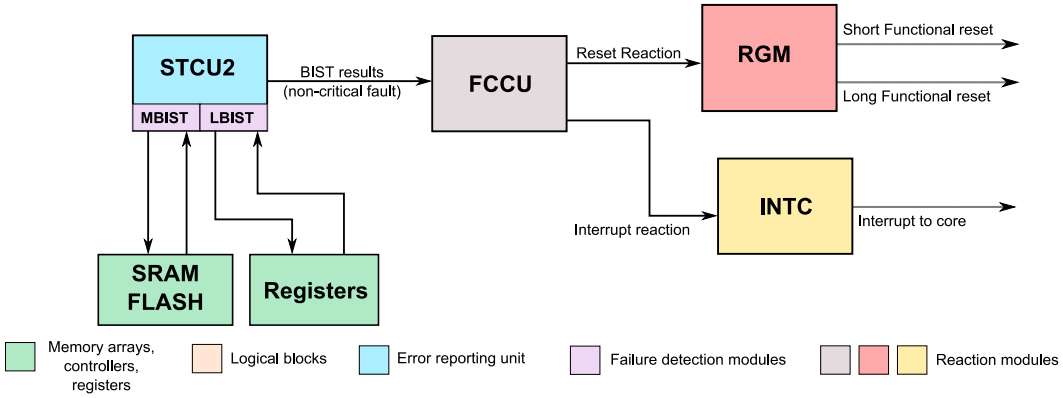

Figure 11. BIST results (non-critical faults)

5.10. JTAG/NPC monitor

The JTAG/NPC module contains a signal monitor. The JTAG/NPC monitor fault is triggered in case of a faulty activation of the JTAG/debug mode. Simulate this fault by unplugging the JTAG during debugging.

When this fault is detected, the JTAG/NPC sends a fault signal to the FCCU. The reaction to this fault depends on the FCCU configuration.

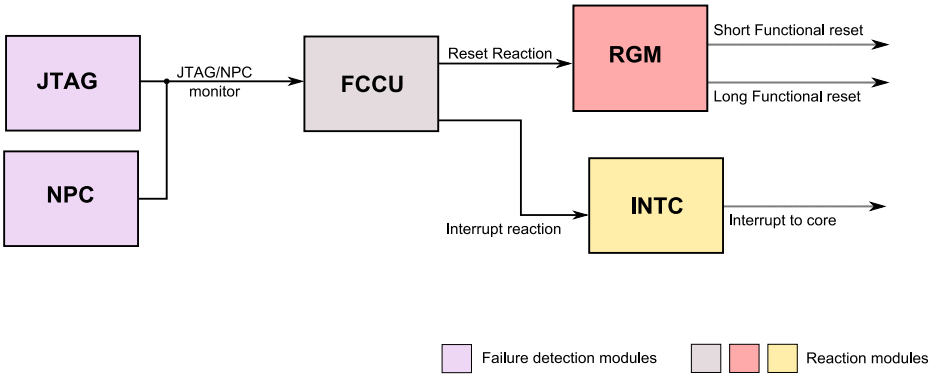

Figure 12. JTAG/NPC monitor

5.11. Core redundancy mismatch: interface (other than D-MEM or DMA) out of lockstep

This fault triggers when the redundancy checker (RCCU) detects a mismatch between an output of the safety lake and the equivalent output of the original lake (except for D-MEM and DMA).

The root cause can be a permanent fault or a transient fault (either in the safety lake or in the original lake) that propagated to any outputs of the lake.

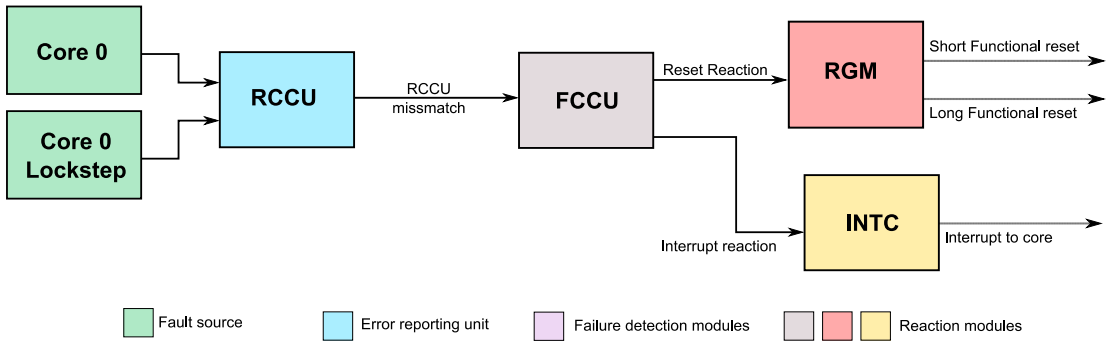

Figure 13. Core redundancy mismatch: interface

5.12. Core redundancy mismatch: D-MEM array interface out of lockstep

This fault triggers when the redundancy checker (RCCU) detects a D-MEM mismatch between an output of the safety lake and the outputs of the original lake.

The root cause can be a permanent fault or a transient fault (either in the safety lake or in the original lake) that propagated to any outputs of the lake.

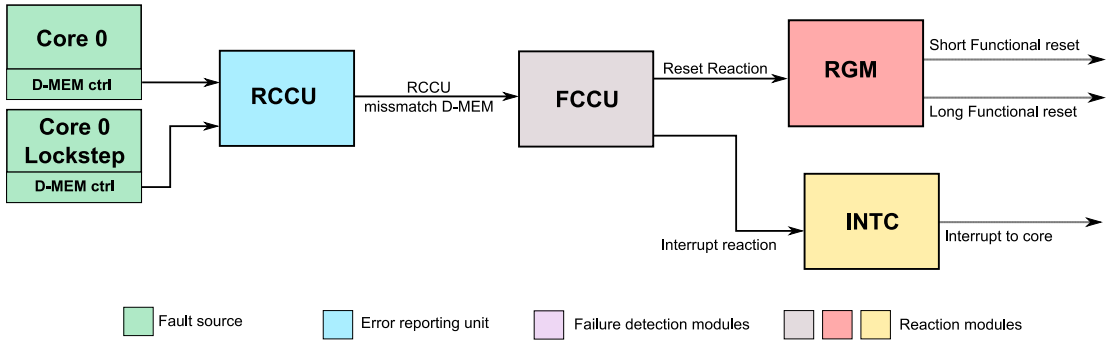

Figure 14. Core redundancy mismatch: D-MEM array interface out of lockstep

5.13. Core redundancy mismatch: DMA array interface out of lockstep

This fault triggers whenever the redundancy checker (RCCU) detects a DMA mismatch between an output of the safety lake and the equivalent output of the original lake.

The root cause can be a permanent fault or a transient fault (either in the safety lake or in the original lake) that propagated to any outputs of the lake. The DMA array itself is not replicated, but the DMA array interface (the DMA controller) is replicated.

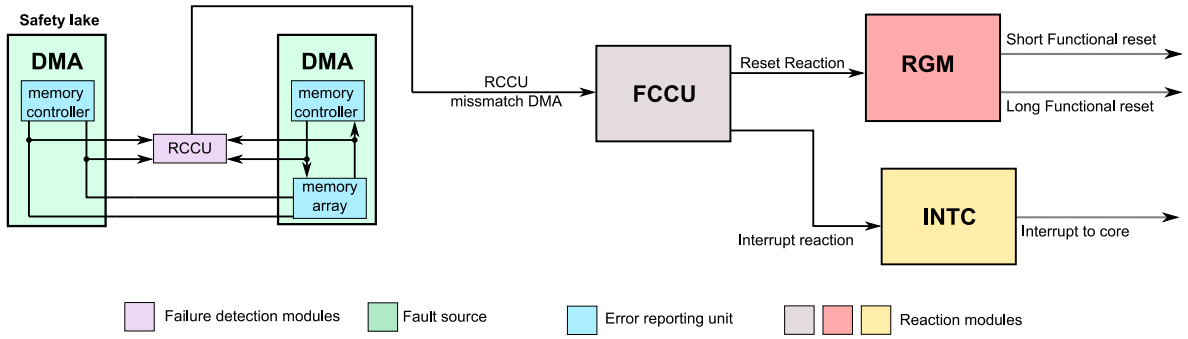

Figure 15. Core redundancy mismatch: DMA array interface out of lockstep

5.14. Software Watchdog Timer

When the Software Watchdog Timer (SWT) reaches the desired value, the timeout flag in the SWT module is set. The signal from the SWT module is sent to the FCCU module only after the second consecutive timeout, as shown in the following figure.

NOTE

The SWT is not connected directly to the RGM, and the FCCU is by default configured not to react on faults. When the SWT expires sooner than the FCCU is configured to react on a fault, no reaction is taken on the SWT timeout event.

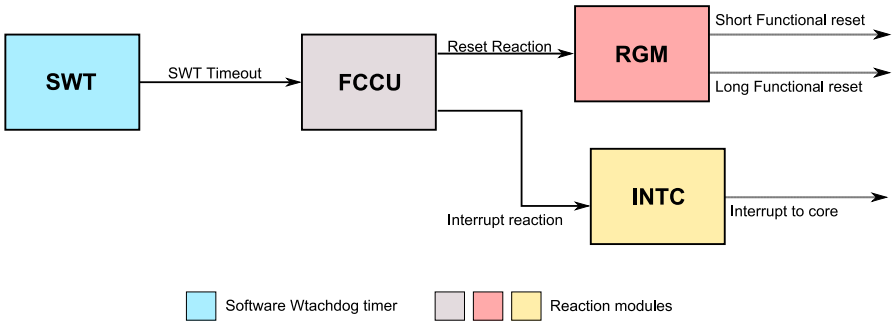

Figure 16. SWT timeout

5.15. System RAMs correctable ECC error

The MEMU handles the collection and reporting of error events associated with the ECC (Error Correction Code) logic used in the peripheral system RAM, SRAM, and flash memory.

When a correctable error event occurs in system RAMs, the MEMU receives an error signal. It causes the event to be recorded and the corresponding MEMU error flag to be set. This is then reported to the FCCU. This fault is generated whenever the ECC mechanism detects a single-bit error event and the error reporting is enabled.

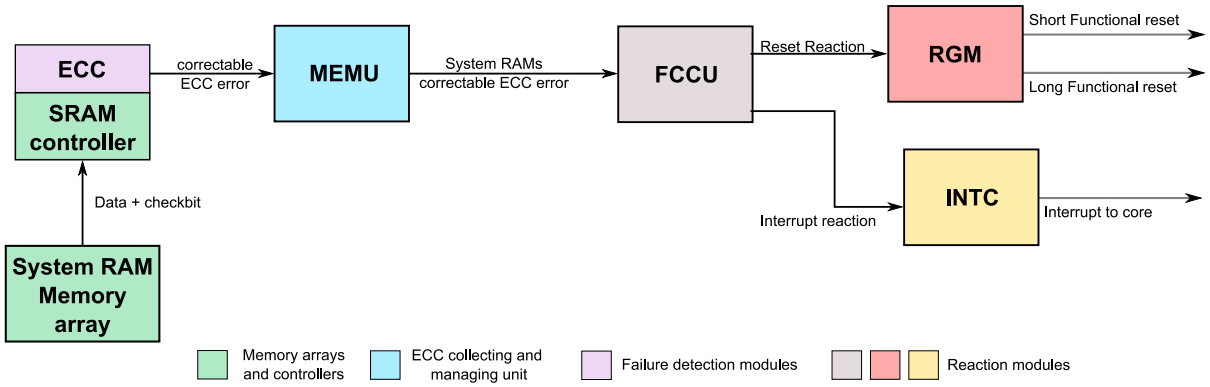

Figure 17. System RAMs correctable ECC error

5.16. System RAMs uncorrectable ECC error

The MEMU handles the collection and reporting of error events associated with the ECC (Error Correction Code) logic used in the peripheral system RAM, SRAM, and flash memory.

When an uncorrectable error event occurs in system RAMs, the MEMU receives an error signal. It causes an event to be recorded and the corresponding MEMU error flag to be set. This is then reported to the FCCU.

This fault is generated whenever the ECC mechanism detects a minimum double-bit (eventually multi-bit) ECC error event.

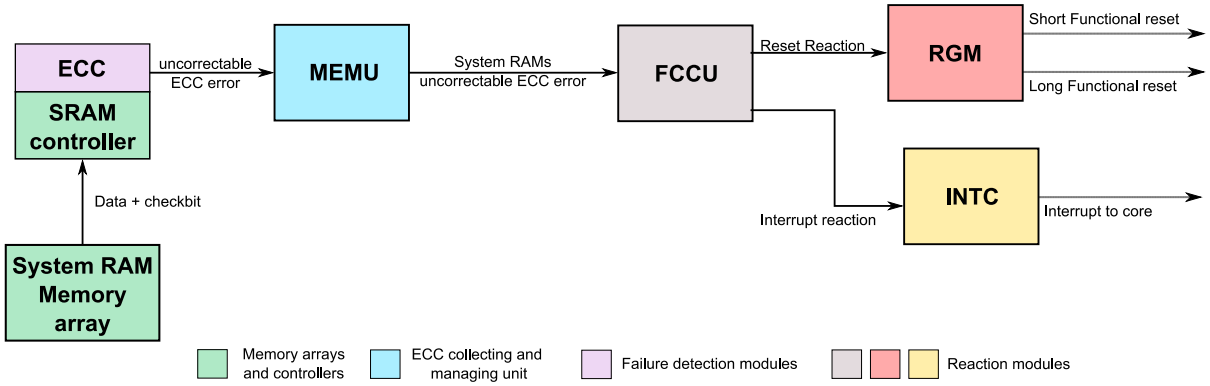

Figure 18. System RAMs uncorrectable ECC error

5.17. System RAMs error overflow (ORing of all overflows)

The ECC mechanism on the system RAM catches the ECC error and sends it to the MEMU unit. In case of ECC overflow in the MEMU, the corresponding fault signal is sent to the FCCU.

This fault is generated in special conditions when either of these faults occurs:

- The system RAM correctable error overflow flag is set.
- The system RAM uncorrectable error overflow is set.
- The system RAM buffer error overflow flag is set.

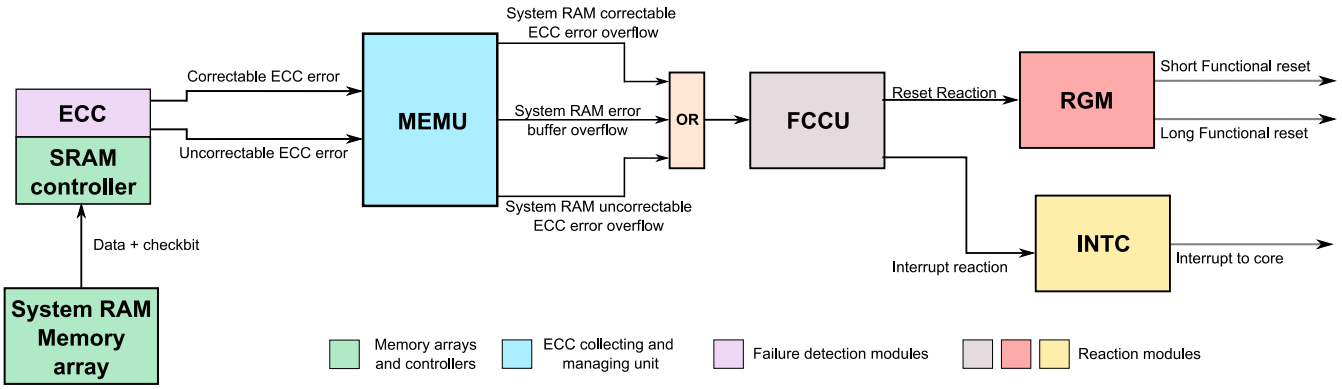

Figure 19. System RAMs ECC error overflow

5.17.1. Handling overflows (multiple error reporting)

When a bit in the overflow registers is asserted (either the error buffer or the reporting table, the overflow registers are the same), it indicates the occurrence of one of these conditions:

- Error buffer overflow—more than two memories report an error at the same instant, or the input ASYNC FIFOs reach the FULL level (overflow).
  - More than two errors are detected at the same time. This can lead to an overflow in the error buffer. The MEMU can process only one error at a time, while storing the other in the error buffer. This is indicated as an overflow. The uniqueness check in the input buffer does not guarantee that an ECC-supervised memory with only one error is not marked as the overflow source. If an error occurs together with two (or more) additional errors at the same cycle, it can be flagged as an overflow.
- Correctable/uncorrectable error overflow—the overflow in the correctable and uncorrectable reporting tables occurs only when a unique entry is to be stored, but the tables are already full (all entries have a valid bit set).
- The overflows are stored in a bit-wise order (if the error bit 31 reports an error, the bit 31 of the overflow register is set to 1).

5.18. Peripheral RAMs correctable ECC error

The MEMU is responsible for collection and reporting of error events associated with the ECC (Error Correction Code) logic used in the peripheral system RAM, SRAM, and flash memory.

When a correctable error event occurs in the peripheral RAMs, the MEMU receives an error signal. This causes an event to be recorded and the corresponding MEMU error flag to be set. This is then reported to the FCCU.

This fault is generated whenever the ECC mechanism detects a single-bit error event and the error reporting is enabled.

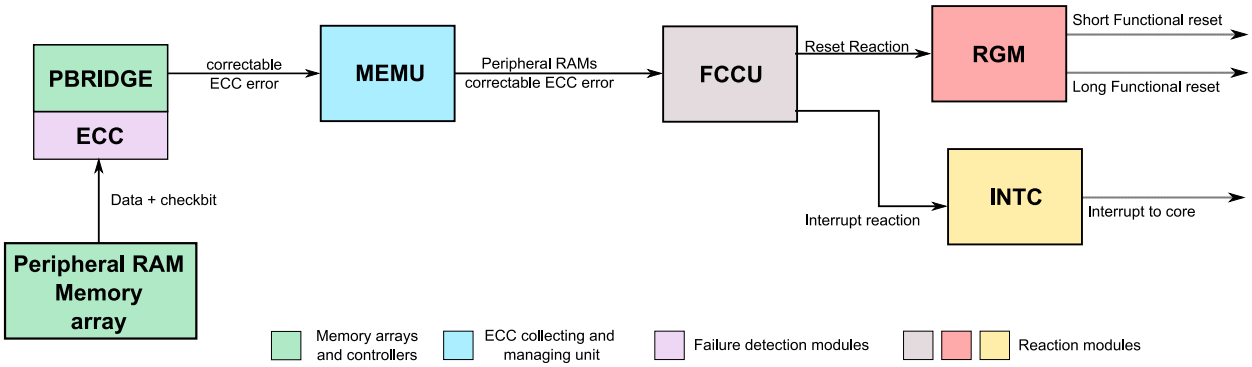

Figure 20. Peripheral RAMs correctable ECC error

5.19. Peripheral RAMs uncorrectable ECC error

The MEMU is responsible for collection and reporting of error events associated with the ECC (Error Correction Code) logic used in the peripheral system RAM, SRAM, and flash memory.

When an uncorrectable error event occurs in the peripheral RAMs, the MEMU receives an error signal. It causes the event to be recorded and the corresponding MEMU error flag to be set. This is then reported to the FCCU.

Uncorrectable error stands for a minimum double-bit (eventually multi-bit) ECC error event.

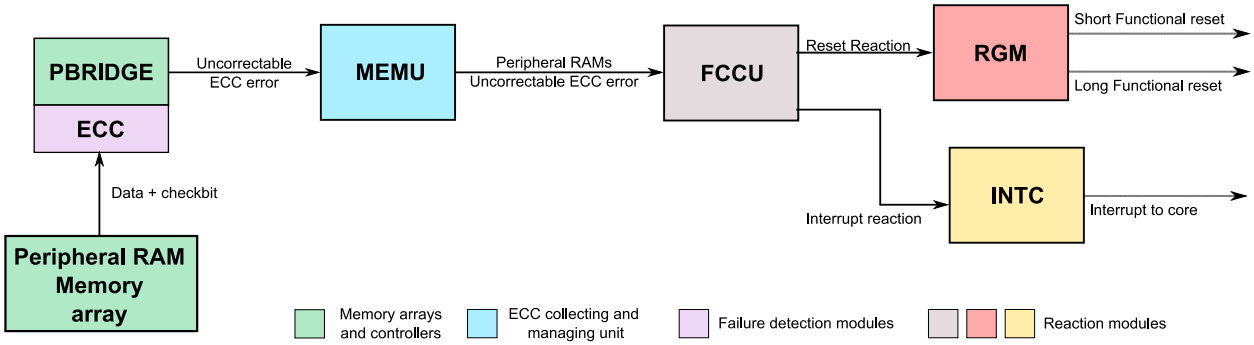

Figure 21. Peripheral RAMs uncorrectable ECC error

5.20. Peripheral RAMs error overflow (ORing of all overflows)

The ECC mechanism in the system RAM catches an ECC error and sends it to the MEMU unit. In case of an ECC overflow in the MEMU, the corresponding fault signal is sent to the FCCU.

This fault is generated in special conditions, when either of these faults occurs:

- The peripheral RAM correctable error overflow flag is set.
- The peripheral RAM uncorrectable error overflow is set.
- The peripheral RAM buffered error overflow flag is set.

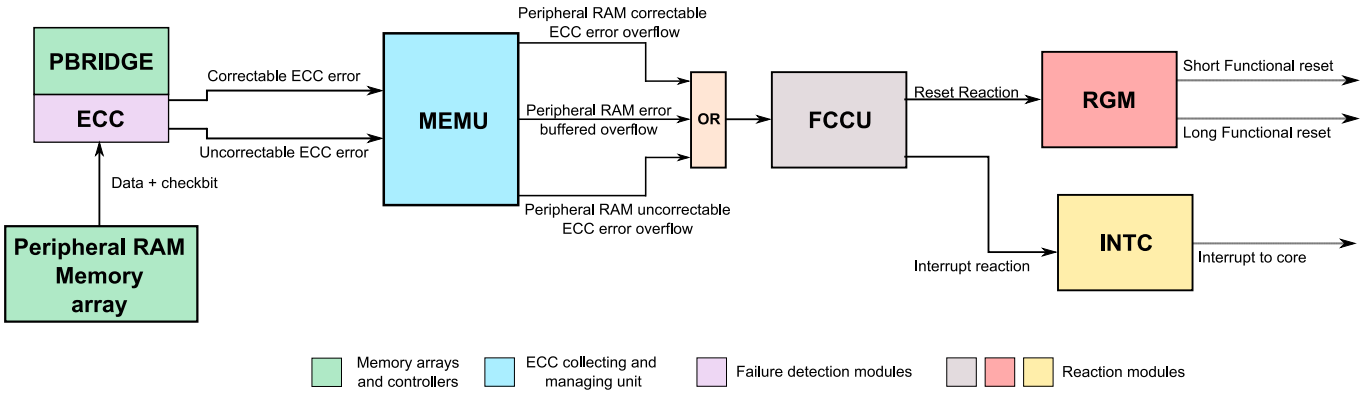

Figure 22. Peripheral RAMs error overflow

5.21. Flash correctable ECC error

The embedded flash memory supports fault tolerance through the Error Correction Code (ECC) and error detection. The ECC (implemented within the embedded flash memory) corrects single-bit failures and reports the ECC mismatch occurrence.

The ECC is recalculated serially on every read request to the flash, and if there is a mismatch between the ECC calculations (taking corrections or detections into account), a late error is reported. Whenever the array is programmed, the ECC bits are also programmed. The ECC is handled on a 64-bit boundary.

When an ECC error event occurs, the fault signal is sent from the PFLASH controller to the MEMU. If the reporting of the ECC single-bit faults is enabled, then the MEMU sends a signal to the FCCU. The actions taken by the FCCU depend on the FCCU NCF behavior configuration.

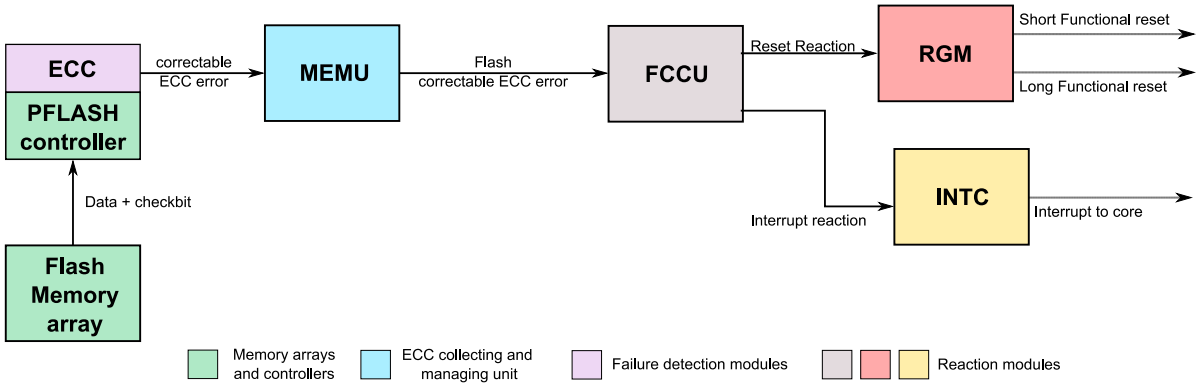

Figure 23. Flash correctable ECC error

5.22. Flash uncorrectable ECC error

The PFLASH controller implements the ECC mechanism. Whenever the array is programmed, the ECC bits are also programmed. The ECC is handled on a 64-bit boundary.

The ECC is recalculated serially on every read request to the flash, and if there is a mismatch between the ECC calculations, the double-bit (multi-bit) failures are reported to the MEMU unit.

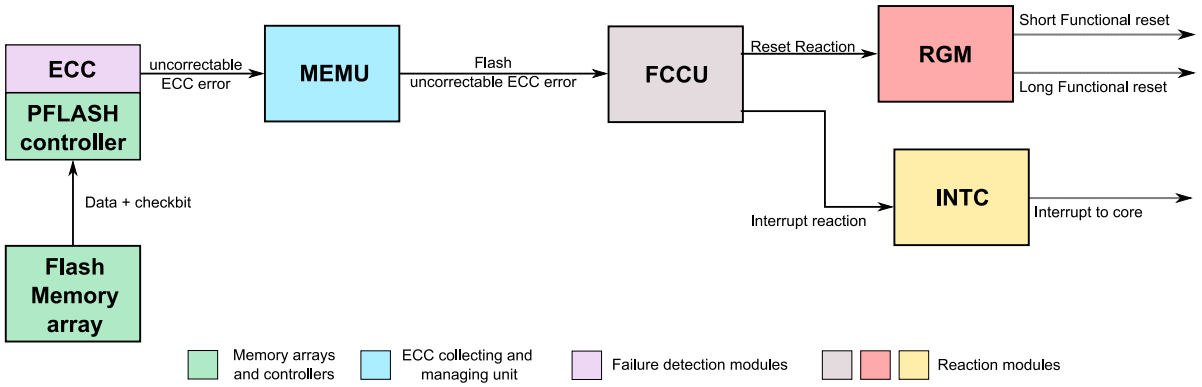

Figure 24. Flash uncorrectable ECC error

5.23. Flash error overflow (ORing of all overflows)

The ECC mechanism on the PFLASH controller catches an ECC error and reports it to the MEMU unit. In case of an ECC overflow in the MEMU, the corresponding fault signal is sent to the FCCU.

This fault is generated in special conditions, when either of these faults occurs:

- The flash correctable error overflow flag is set.
- The flash uncorrectable error overflow is set.
- The flash buffered error overflow flag is set.

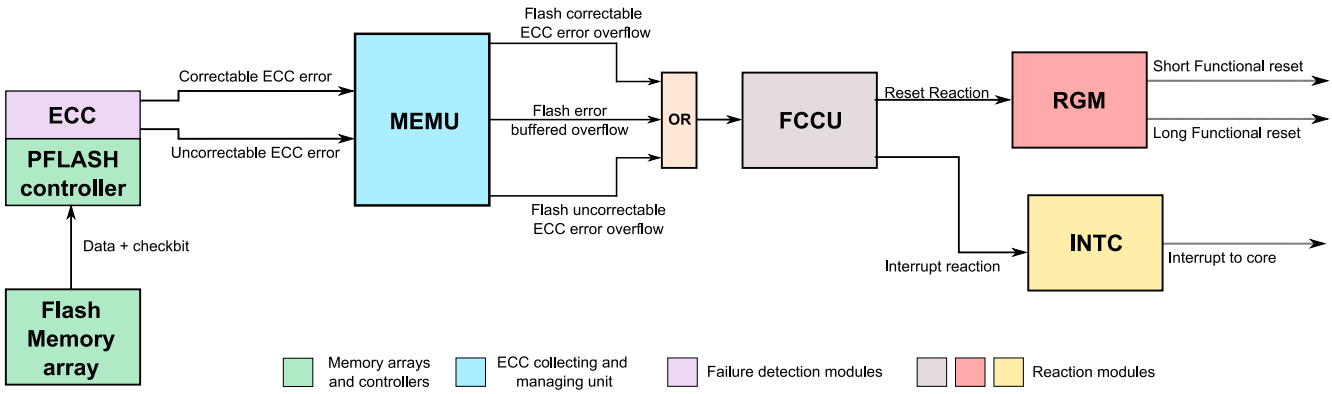

Figure 25. Flash error overflow (ORing of all overflows)

5.24. PLL Loss of clock

The MPC57XX MCUs have built-in mechanisms to detect the loss of the oscillator or the PLL clock, and to provide several reaction options to the loss of clock in the application. The following diagram shows a complete data flow through various blocks of the SoC. In case the oscillator or the PLL clock is lost, the loss of lock event is generated by the PLL.

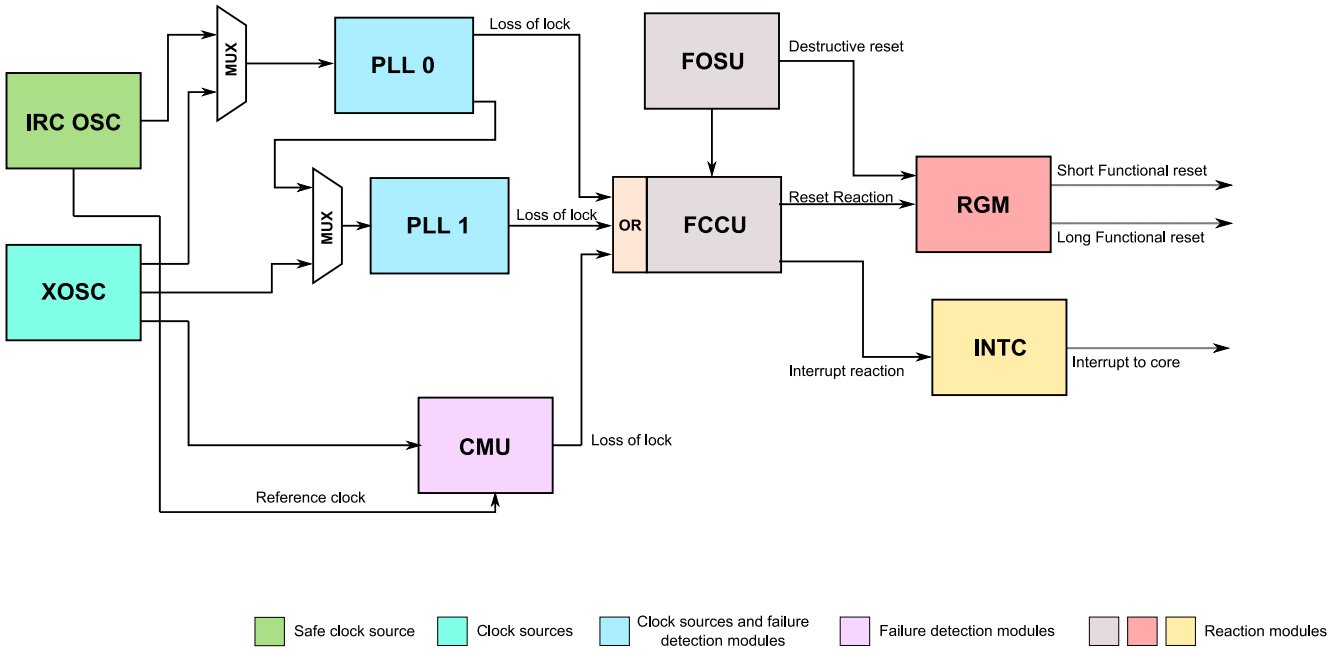

Figure 26. PLL loss of clock

5.25. XOSC vs. IRCOSC clock frequency out of range

The frequency of the IRCOSC clock is monitored by the frequency meter in the CMU_0. There is no automated trigger of the FCCU error condition if the IRCOSC fails. Because the IRCOSC is both the boot and the backup clock, the failure is catastrophic.

Each CMU's FHH and FLL event indicator is connected solely to the FCCU. Therefore, the CMU_0's connection to the FCCU in the following figure represents all CMU instances.

The period of the IRCOSC can be measured in the CMU0, using the XOSC as a reference. This enables the application trimming of the IRCOSC frequency.

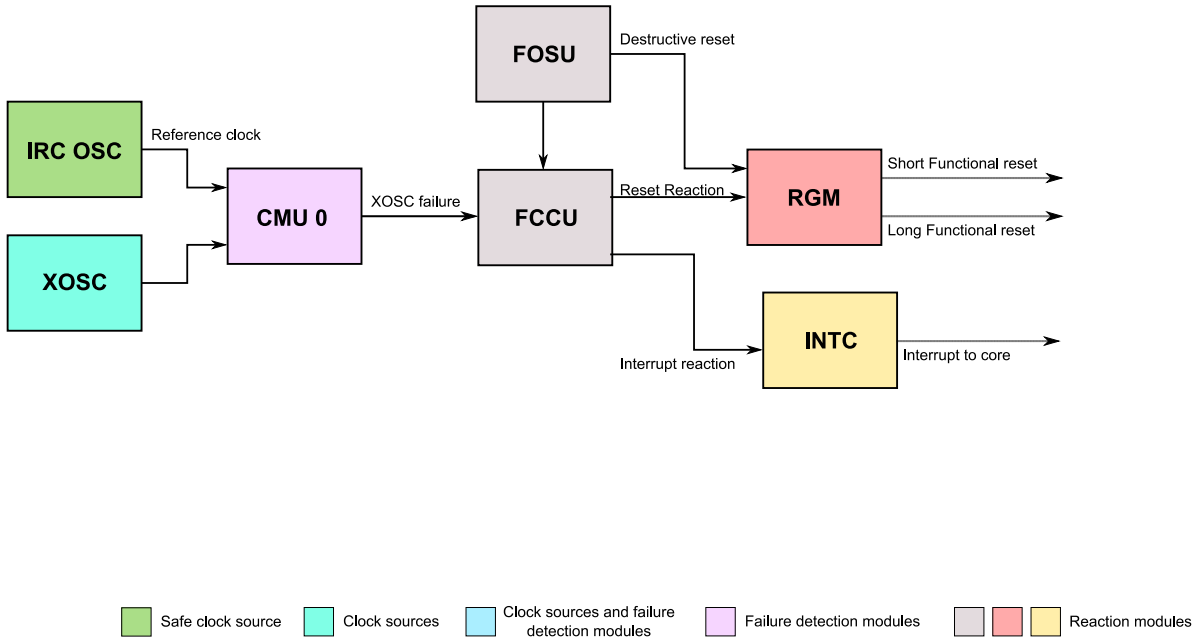

Figure 27. XOSC vs. IRCOSC clock frequency out of range

5.26. Motor clock frequency out of range

For all safety-critical clocks, the MCU detects a missing clock or an incorrect frequency. The CMUs (Clock Monitoring Units) are used for this. The IRCOSC and XOSC are used as the clock monitor reference for the CMU_0.

Software can program the upper and lower limits of the expected clock frequency. If the monitor is enabled and the measured frequency is above or below the limits, the corresponding flag bit is set in the CMU[ISR] register, and an interrupt is generated (if enabled). The default condition of the clock monitor is disabled. The CMU_0 also indicates this fault to the FCCU unit to add a safety-relevant reaction path.

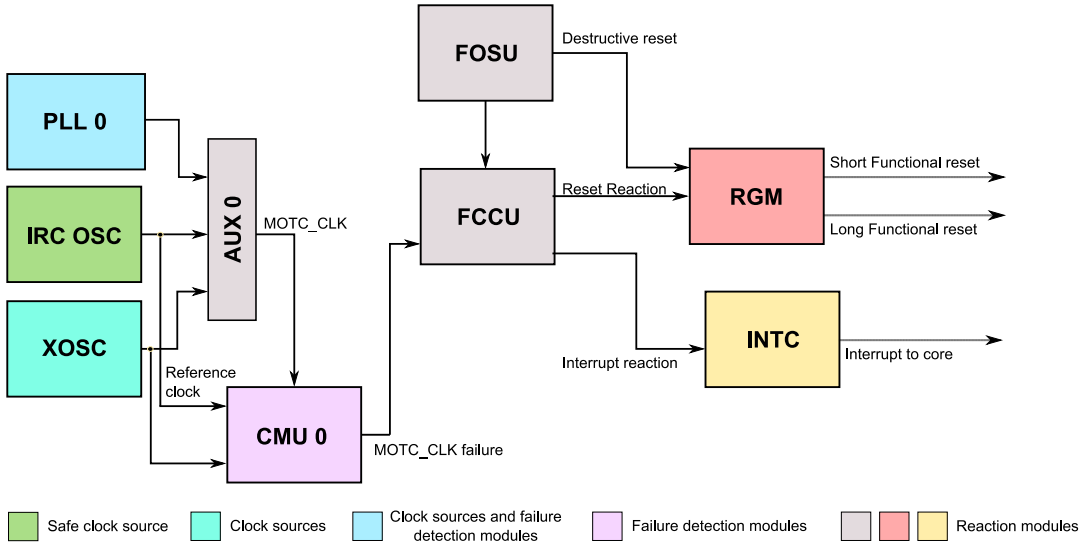

Figure 28. Motor clock frequency out of range

5.27. Core frequency out of range

For all safety-critical clocks, the MCU detects a missing clock or an incorrect frequency. The CMUs are used for this. The IRCOSC is used as the clock monitor reference for the CMU_1.

If the Checker Core, Main Core, RCCU_0, or SYSCLK clock frequency is above or below the limits, a flag bit is set, and an interrupt is generated (if enabled). The fault signal is automatically sent to the FCCU.

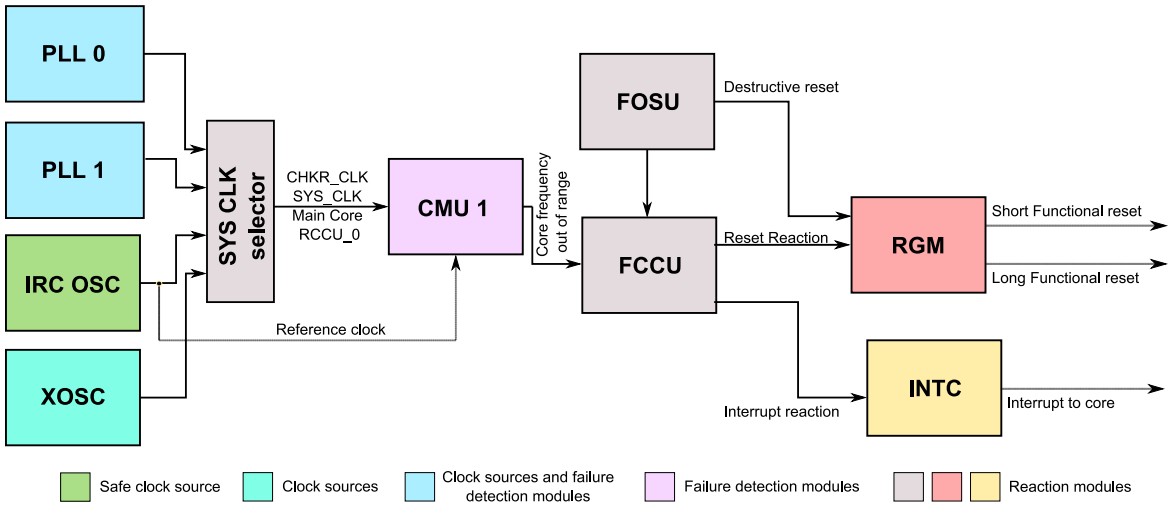

Figure 29. Core frequency out of range

5.28. PBRIDGE frequency out of range

The frequency of the PBRIDGE can be monitored by the CMU_2. If the frequency violates the programmed thresholds, the flag bit is set, and an interrupt is generated (if enabled). The fault signal is immediately sent to the FCCU, which can take safe actions. The fault-reporting path is shown in this figure:

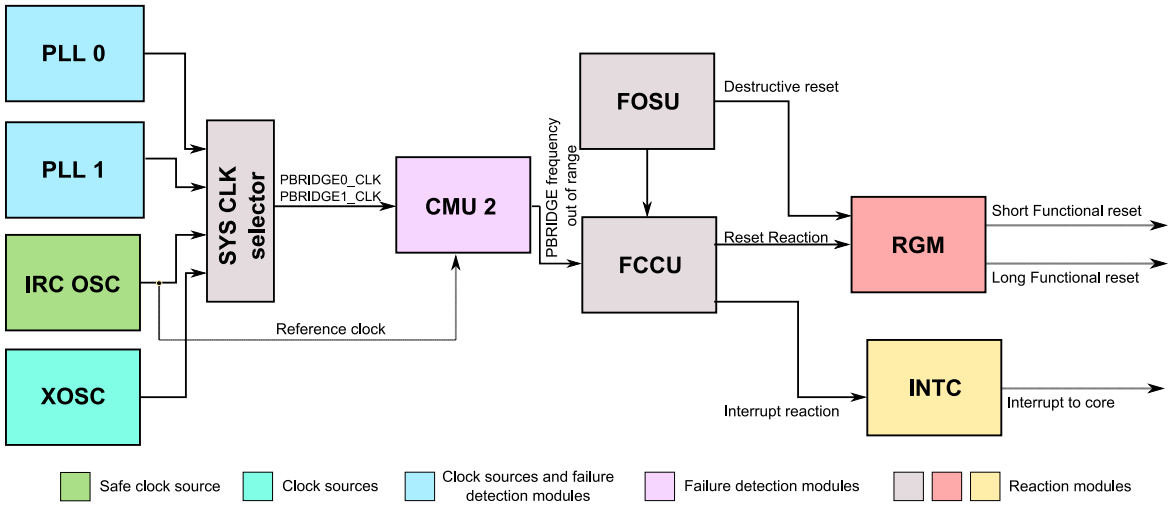

Figure 30. PBRIDGE frequency out of range

5.29. ADC clock frequency out of range

The ADC frequency can be monitored by the CMU_3. If the frequency violates the programmed thresholds, the flag bit is set, and an interrupt is generated (if enabled). The fault signal is immediately sent to the FCCU, which can take safe actions. The fault-reporting path is shown in this figure:

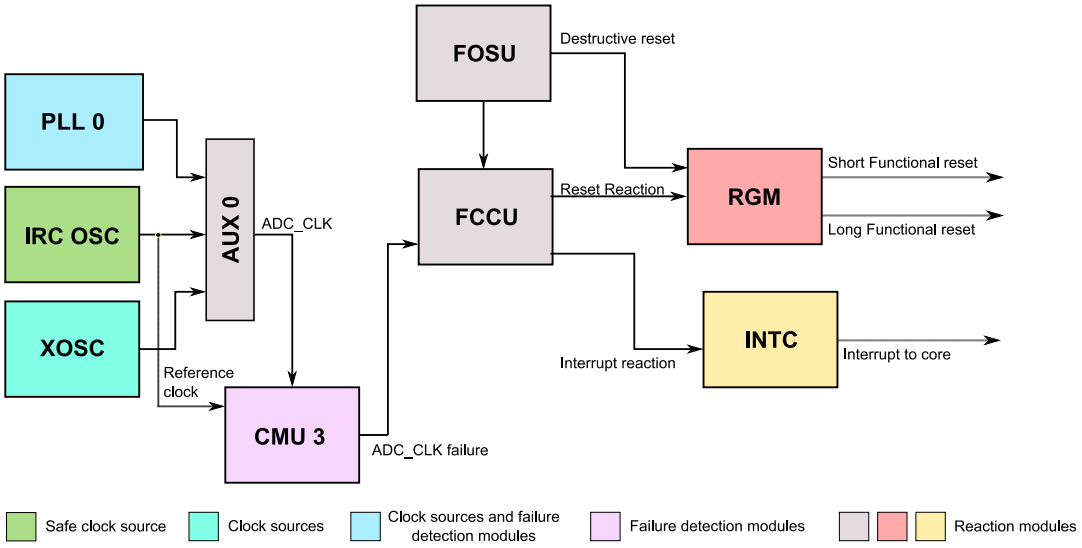

Figure 31. ADC clock frequency out of range

5.30. SENT frequency out of range

The SENT frequency can be monitored by the CMU_4. If the frequency violates the programmed thresholds, the flag bit is set, and an interrupt is generated (if enabled). The fault signal is also immediately sent to the FCCU, which can take safe actions. The fault-reporting path is shown in this figure:

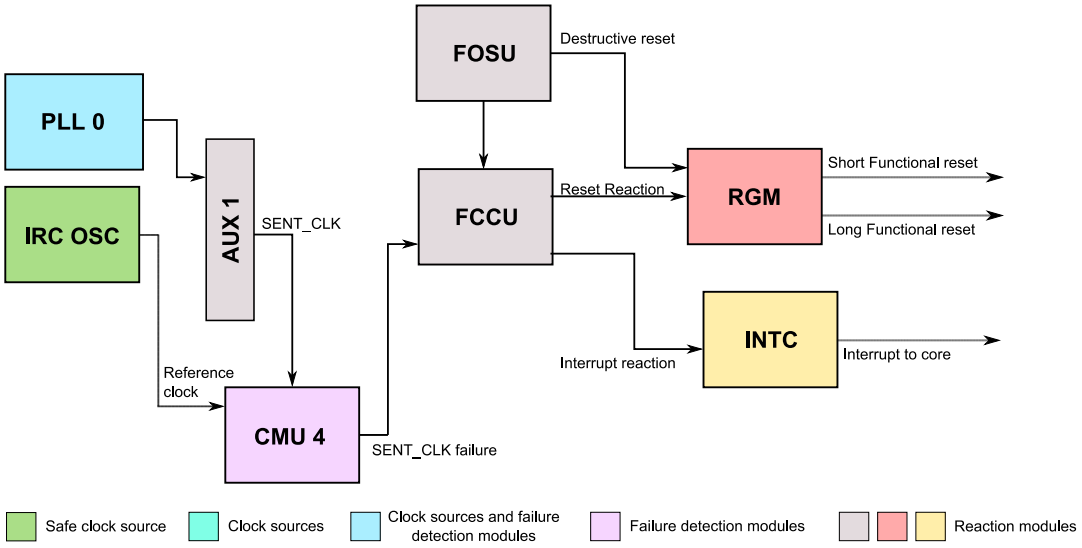

Figure 32. SENT frequency out of range

5.31. Error input pin

This fault triggers when an external circuitry reports an error to the MCU via the error input pin. Which particular faults this indicates depends on the application. It is not possible to determine a permanent or transient failure rate for it. This is the task of the ECU system integrator.

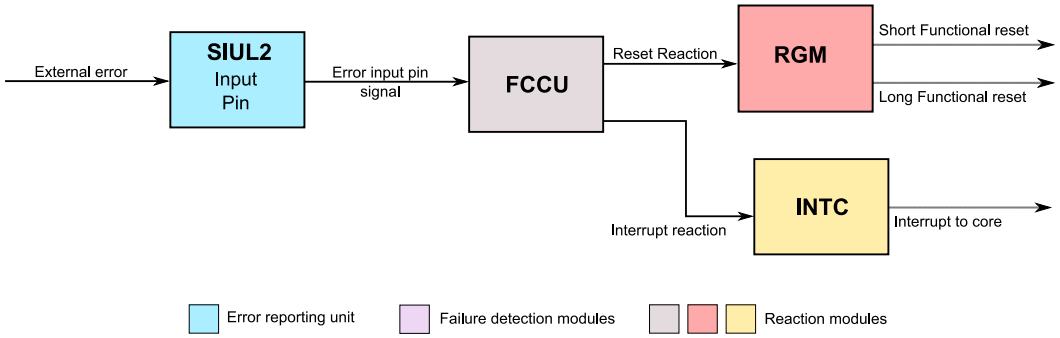

Figure 33. Error input pin

5.32. Address Encode Error ORed with voltage and current error of flash memory array

This fault is generated when any of these events occur:

- The ECC single-bit inversions are detected and repaired, but not indicated.
- Voltage error in the flash memory array.
  - This is a read voltage error. The read voltage is the voltage that is required on the flash bit cell to read it. It is generated internally via a charge pump.
- Current error in the flash memory array.
  - The read reference is an internal current that the MCU generates to compare against if the read bit is 0 or 1.

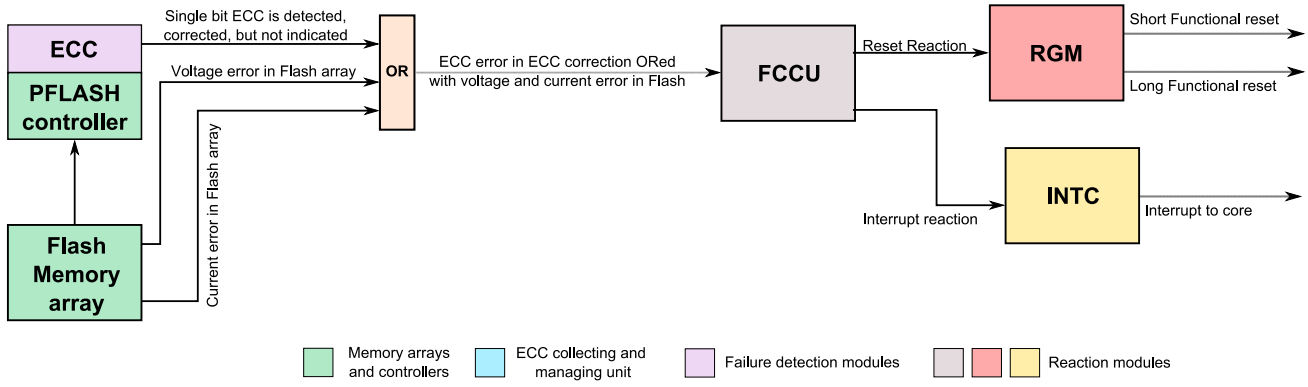

Figure 34. ECC error in ECC correction ORed with voltage and current error in flash

5.33. Error in the ECC correction logic through an EDC

The flash controller contains the ECC logic as well as the EDC logic. This error is a result of the EDC check after the ECC logic, which is implemented within the flash. The EDC is a decode logic looking for an error in the ECC logic, which is used to double check the ECC calculation logic. By recreating the decode bits, it is possible to double check whether the ECC calculation is correct. In this safety check, the decode logic is duplicated two times to enable the check.

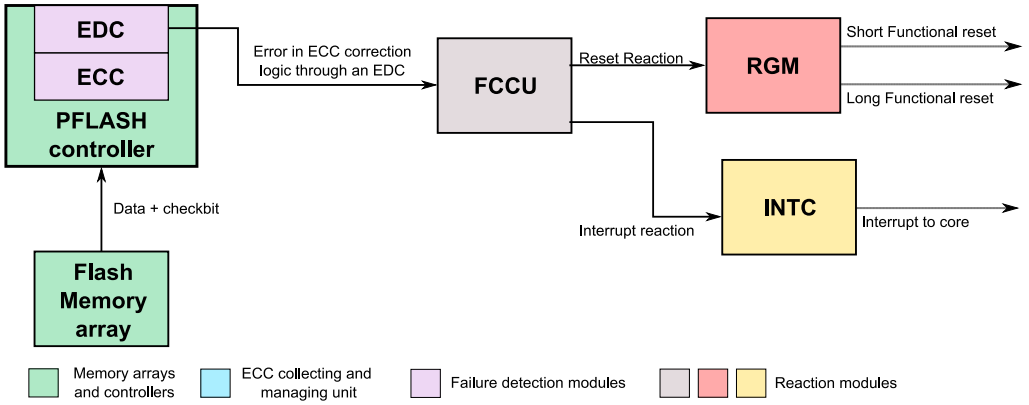

Figure 35. Error in ECC correction logic through EDC

5.34. Alarm indicating the flash memory controller detected an error in the address ECC manipulation logic through an EDC

When the data is returned from the flash, the accompanying ECC code word is appended within the address encoding to produce a full ECC code word that includes the address and data coverage. This full ECC code word is sent to the requesting master with the requested data. The EDC function in the flash controller performs a reverse-decode of the full ECC code word to remove the address contribution and then compares this result to the ECC code word originally supplied by the flash. The NCF[35] is generated whenever the ECC code word stored in the flash does not match the EDC code word.

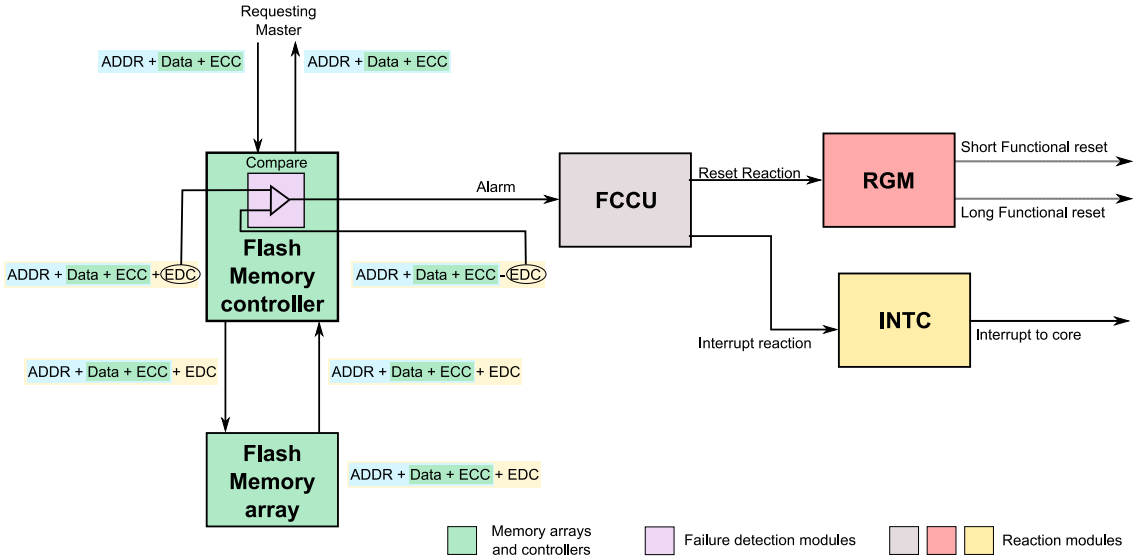

Figure 36. Error in address ECC manipulation logic through EDC

5.35. Alarm indicating the flash memory controller detected a transaction monitor mismatch when compared to the flash safety feedback outputs

This fault is generated whenever the control signals between the flash memory controller and the flash memory array do not match. The control signals (that the flash memory controller sends to the flash memory for any operation) are latched and sent back from the flash memory to the flash memory controller. The flash memory controller compares the received control signals to the transmitted control signals. If they do not match, the feedback alarm is generated.

This protection is applied as an end-to-end protection mechanism between the flash memory controller and the flash memory array because this part of the MCU is not replicated.

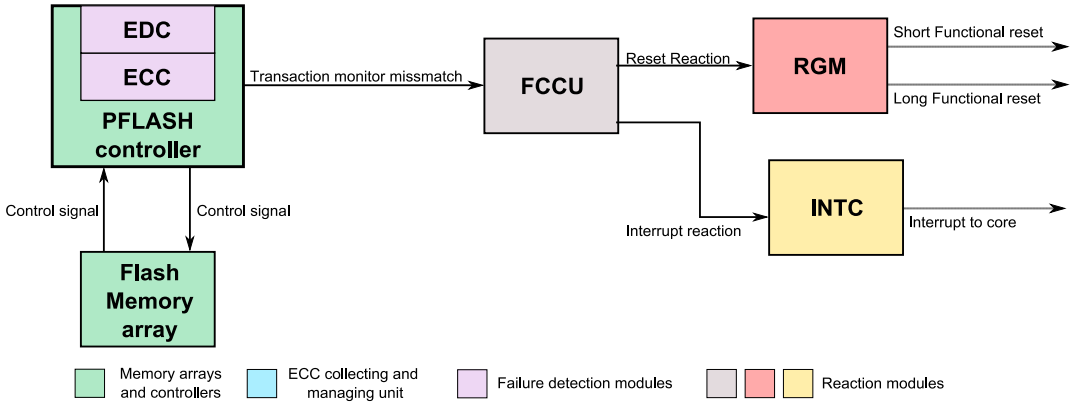

Figure 37. Flash memory controller transaction monitor mismatch

5.36. Transaction monitor mismatch in the pseudo-replicated calibration evaluation hardware

The flash memory controller supports the calibration development by providing a remapping function to route the flash accesses to the on-chip system RAM, which can be used as an overlay RAM. This enables the calibration of the constant data without the requirement for additional external RAMs and calibration memory interfaces.

The backdoor AHB port provides a connection from the flash controller to facilitate the calibration overlay access.

When the calibration function is established as safety-critical (PFCRCR[SAFE_CAL] = 1), the PFLASH controller considers the calibration region descriptors a collection of redundant resources. The total capacity for the calibration regions is reduced by a half.

When the region descriptor lockstep pairs are established, the PFLASH controller redundantly evaluates the lockstep pairs of the region descriptors on all incoming flash requests. If a mismatch is detected in the calibration overlay evaluation, NCF[37] is generated.

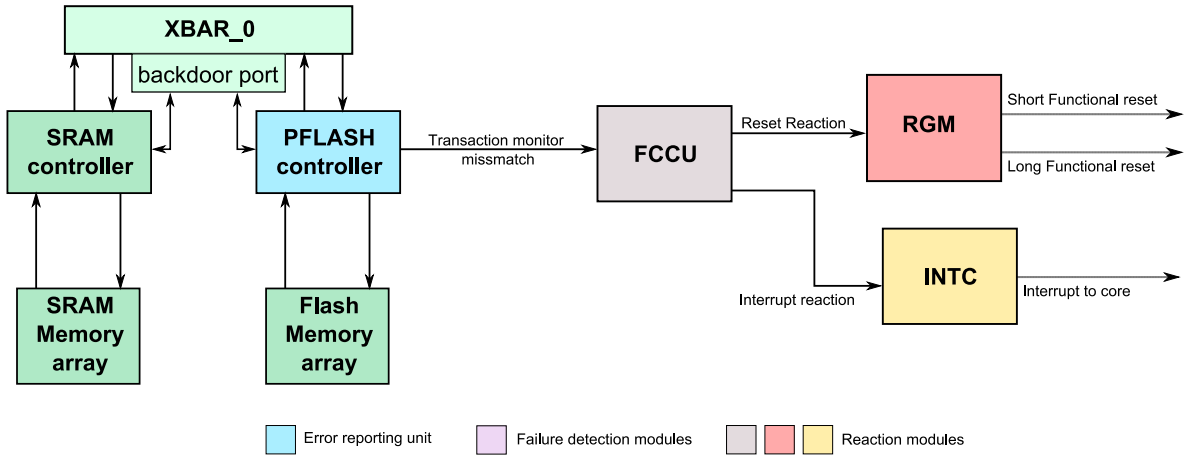

Figure 38. Transaction monitor mismatch in pseudo-replicated calibration evaluation hardware

5.37. XBAR transaction monitor mismatch

The XBAR transaction monitor mismatch fault is set whenever the XBIC_0 module (E2E protection on XBAR_0) detects a fault on the data transmitted via the XBAR_0. The fault signal is then sent to the FCCU module. For more details on XBIC_0, see Section 18, “Crossbar Integrity Checker (XBIC)” from *MPC5744P Reference Manual* (document MPC5744PRM).

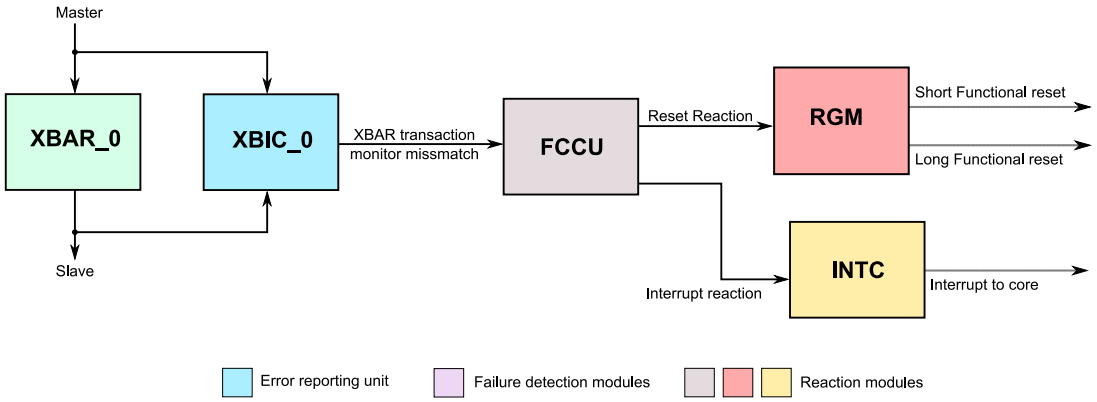

Figure 39. XBAR transaction monitor mismatch

5.38. System RAM controller alarm

The FCCU system RAM controller alarm input is triggered when the feedback check of the system RAM fails.

The system memory provides a feedback output for write enable, chip select, and address. In the SRAM controller, these signals are compared with the address, chip select, and write enable that are issued by the SRAM controller to check whether the data is written in the correct memory address.

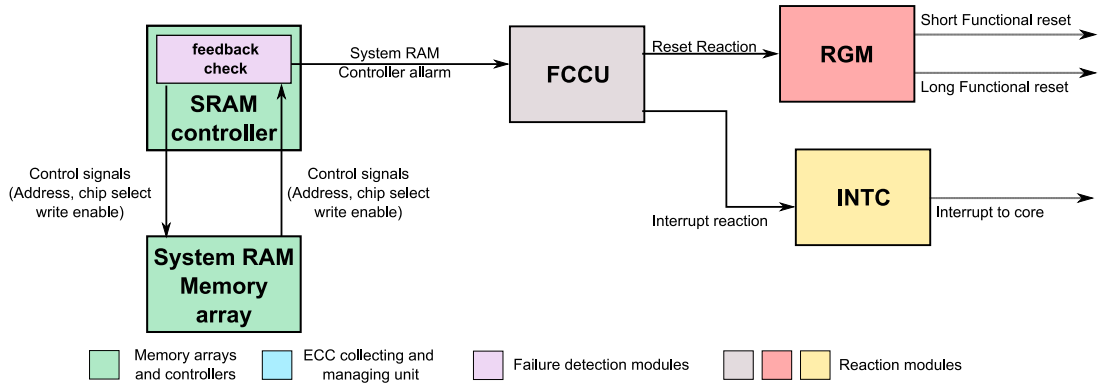

Figure 40. System RAM controller alarm

5.39. Combination of safety-critical signals from TCU

This description is common for NCF[40], NCF[41], NCF[42], and NCF[43].

The device observes the signals that are part of the TCU (Test Control Unit used for the production test). Because the device is not in the test mode with the customer, these signals must not toggle. If they do, the NCF is generated.

The diagnostic function test domains do this:

- TCU DFT0 generates NCF[40]
- TCU DFT1 generates NCF[41]
- TCU DFT2 generates NCF[42]
- TCU DFT3 generates NCF[43]

This figure represents the fault reporting and reaction path for NCF[40], NCF[41], NCF[42], and NCF[43] from the TCU module DFT, where “x” stands for the DFT module number from 0 to 3:

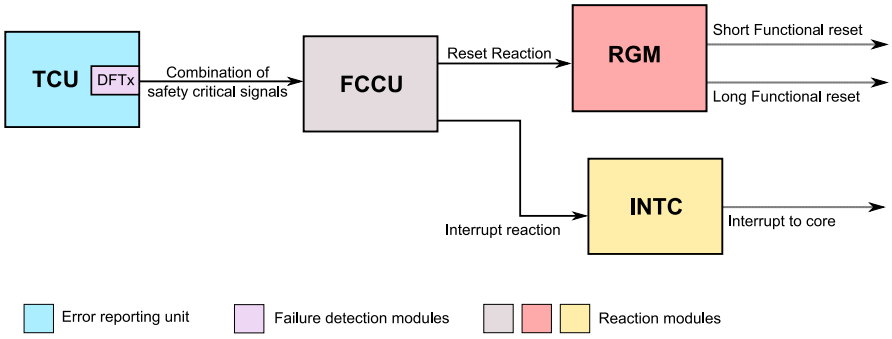

Figure 41. Combination of safety-critical signals from TCU

5.40. Safety core exception indication

The FCCU safety core exception indication input is triggered when the safety core runs into the machine check condition. No trigger rate can be determined for this fault.

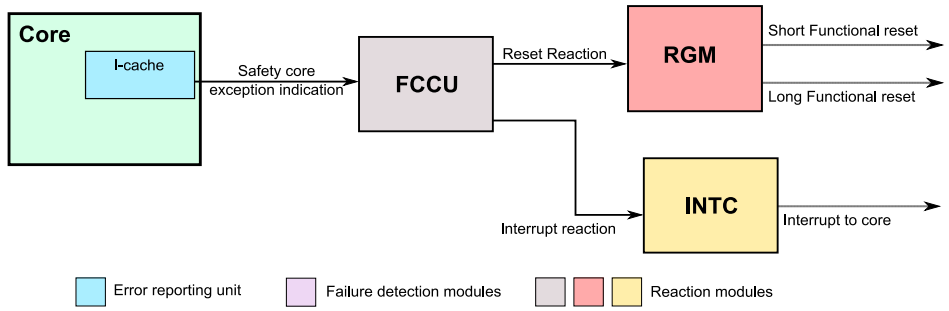

Figure 42. Safety core exception indication

5.41. Indication of disablement of Checker Core and DMA as well as RCCUs

The FCCU Indication of disablement of Checker Core and DMA as well as RCCUs input triggers when there is an erroneous disablement or malfunction of the lockstep.

If the RCCUs are disabled due to the debug mode entry, this fault is not triggered. If the RCCU disablement occurs for another reason, this fault is triggered. See Section 11.3, “Core lockstep and RCCU disablement in debug mode” from *MPC5744P Reference Manual* (document MPC5744PRM) for more information about the RCCU disablement in the debug mode.

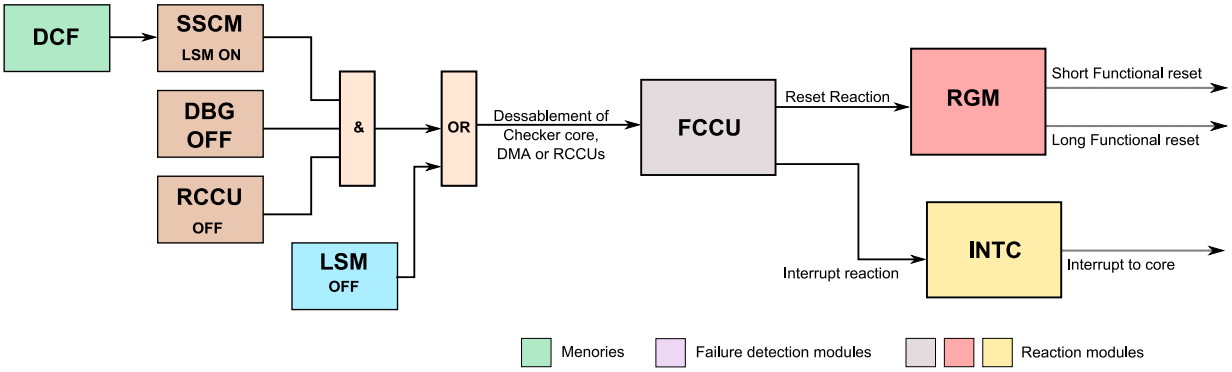

Figure 43. Indication of disablement of Checker Core and DMA as well as RCCUs

5.42. Safe mode request

The FCCU safe mode requests the input triggers when the Reset Generation Module (RGM) requests the SAFE mode upon certain events, based on its configuration. The SAFE mode is intended to enable the software to assess the failure and to reinitialize (or reset) the chip.

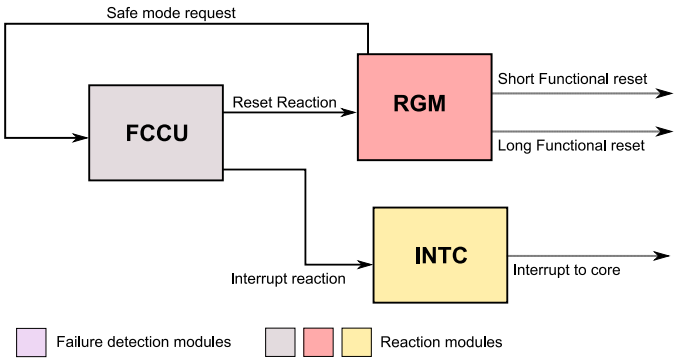

Figure 44. Safe mode request

5.43. Internal self-test

The FCCU Internal self-test input is triggered by a failing ADC self-test. A separate FCCU input is in place for all four ADC modules. Depending on the configuration, either the related NCF or the CF FCCU line triggers (mutually exclusive). The exact trigger rate depends on the configured ADC self-test thresholds.

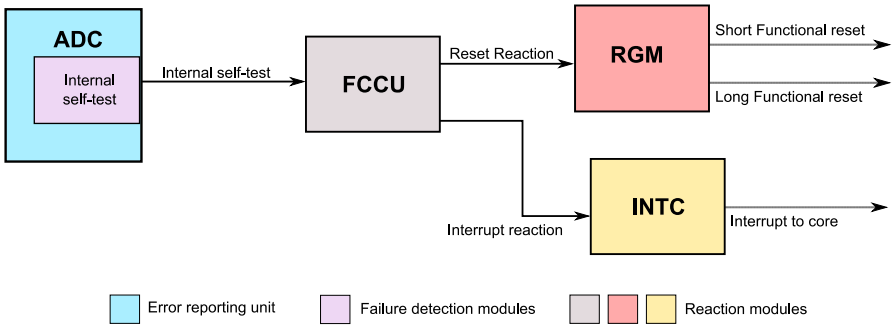

Figure 45. Internal self-test

5.44. INTC latency monitor

The FCCU INTC latency monitor input is triggered when the interrupt latency monitor expires. This depends heavily on the configuration of monitors and on the software execution. Certain hardware faults can also lead to the expiration of the interrupt latency monitor. However, they are manifold and the same faults can also trigger other FCCU inputs (e.g., SWT). Because of the high number of different root causes and the huge number of possible fault propagations within the MCU, it is not possible to determine the trigger rates for this FCCU fault source.

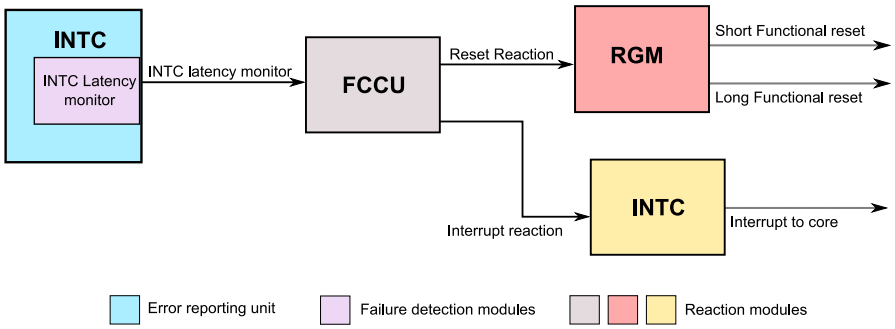

Figure 46. INTC latency monitor

5.45. SIPI_DMA_Ethernet concentrator transaction monitor mismatch

The SIPI_DMA_Ethernet concentrator is XBAR_1. On XBAR_1, there is a transaction monitor implemented for SIPI, DMA, and Ethernet, called the XBIC_1 module (E2E protection on XBAR_1).

Whenever the XBIC_1 module (E2E protection on XBAR_1) detects a fault on the data transmitted via XBAR_1, a fault signal is sent to the FCCU module. For more details on XBIC_0, see Section 18, “Crossbar Integrity Checker (XBIC)” from *MPC5744P Reference Manual* (document MPC5744PRM) .

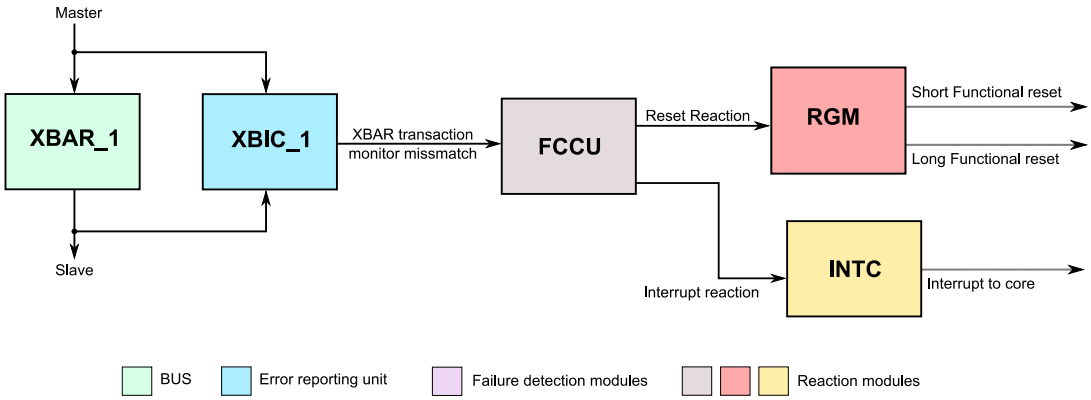

Figure 47. XBAR_1 transaction monitor mismatch

5.46. Multiple D-cache and D-cache tag memory cuts

The FCCU Multiple D-cache and D-cache tag memory cuts input is triggered when the MBIST finds a memory fault in the data cache. The fault can be either permanent or transient. In case of a permanent fault, retesting fails. In case of a transient fault, retesting passes.

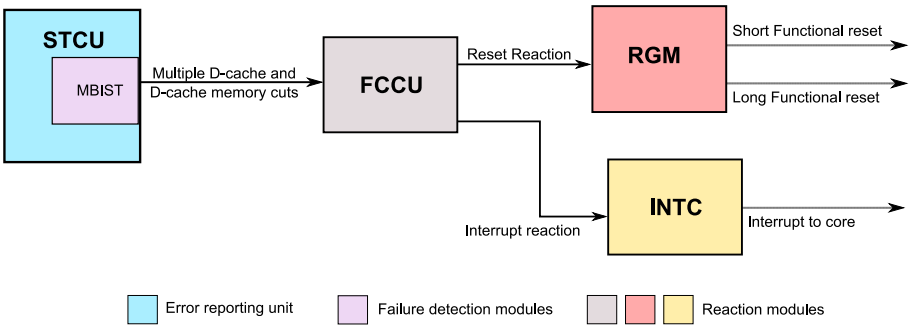

Figure 48. Multiple D-cache and D-cache tag memory cuts

5.47. Multiple I-cache and I-cache tag memory cuts

The FCCU Multiple I-cache and I-cache tag memory cuts input is triggered when the MBIST finds a memory fault in the instruction cache. The fault can be either permanent or transient. In case of a permanent fault, retesting fails. In case of a transient fault, retesting passes.

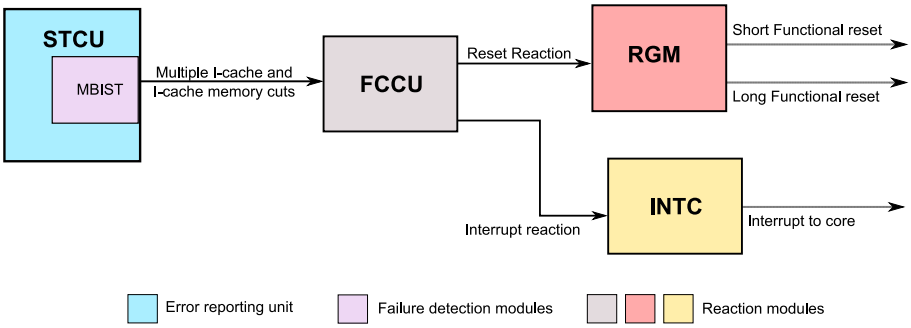

Figure 49. Multiple I-cache and I-cache tag memory cuts

5.48. Multiple D-MEM memory cuts

The FCCU Multiple D-MEM memory cuts input is triggered when the MBIST finds a memory fault in the D-MEM memory. The fault can be either permanent or transient. In case of a permanent fault, retesting fails. In case of a transient fault, retesting passes.

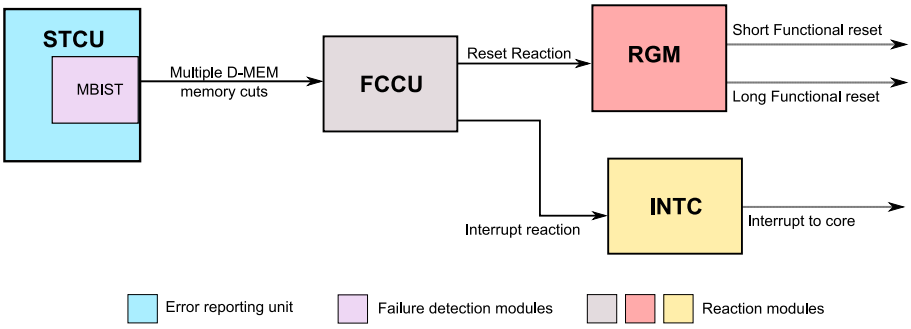

Figure 50. Multiple D-MEM memory cuts

5.49. Multiple system RAM memory cuts

The FCCU Multiple system RAM memory cuts input is triggered when the MBIST finds a memory fault in the system RAM memory. The fault can be either permanent or transient. In case of a permanent fault, retesting fails. In case of a transient fault, retesting passes.

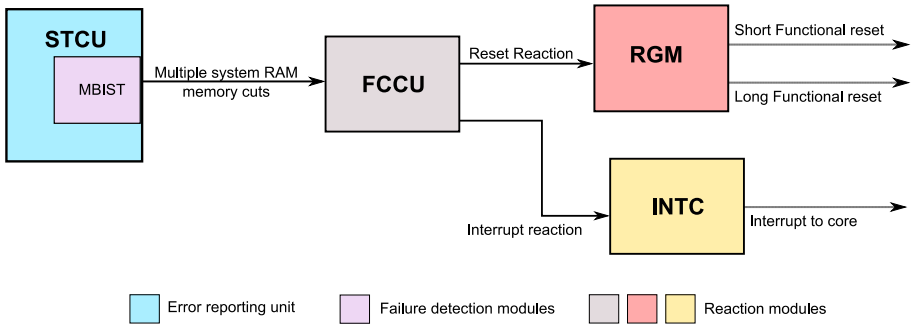

Figure 51. Multiple system RAM memory cuts

5.50. Multiple CAN, FlexRay, Ethernet, and DMA memory cuts

The FCCU Multiple D-MEM memory cuts input is triggered when the MBIST finds a memory fault in the CAN, FlexRay, Ethernet, and DMA memory. The fault can be either permanent or transient. In case of a permanent fault, retesting fails. In case of a transient fault, retesting passes.

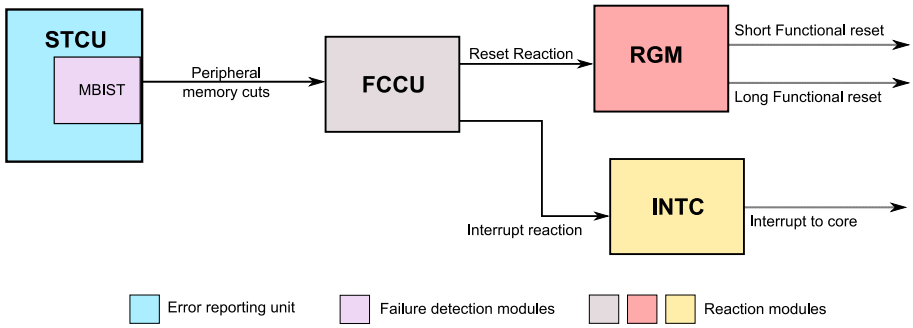

Figure 52. Peripheral memory cuts

5.51. I-cache memory feedback alarm

This fault is integrated as a safety check, because the cache memory array is not replicated in the safety lake (safety core). The control signals that the memory controller sends to the memory for any operation are latched and sent back from the memory to the memory controller. The memory controller compares these received control signals with the transmitted control signals. If they do not match, the feedback alarm is generated.

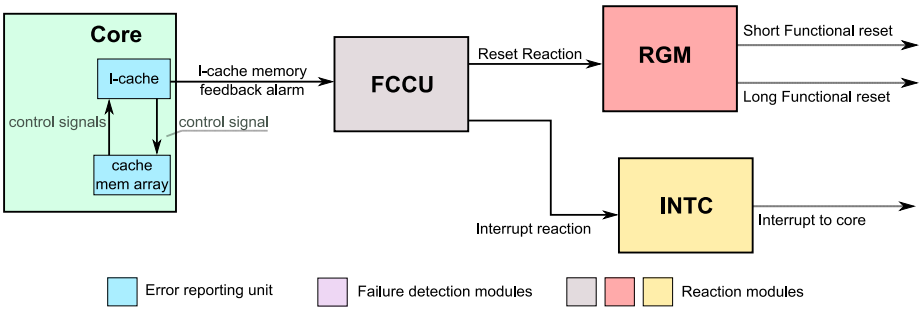

Figure 53. I-cache memory feedback alarm

5.52. D-cache memory feedback alarm

This fault is integrated as a safety check because the cache memory array is not replicated in the safety lake (safety core). The control signals that the memory controller sends to the memory for any operation are latched and sent back from the memory to the memory controller. The memory controller compares these received control signals with the transmitted control signals. If they do not match, the feedback alarm is generated.

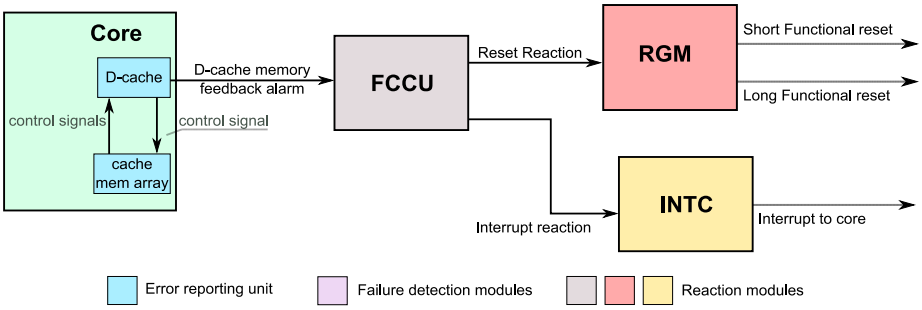

Figure 54. D-cache memory feedback alarm

5.53. Data TCM memory feedback alarm

To provide for the low-latency memory access for critical instruction routines and data operands, the local Data Memory (DMEM) capabilities are added to the processor cores.

This fault is integrated as a safety check for the DTCM (Data Tight-Coupled Memory) memory array, because it is not replicated in the safety lake (safety core). The control signals that the DTCM memory controller sends to the DTCM memory for any operation are latched and sent back from the DTCM memory to the DTCM memory controller. The DTCM memory controller compares the received control signals with the transmitted control signals. If they do not match, the feedback alarm is generated.

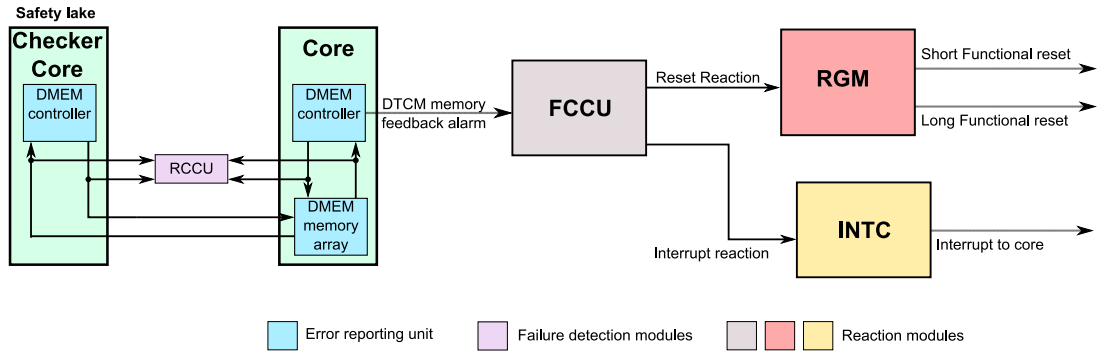

Figure 55. DTCM memory feedback alarm

5.54. DMA memory feedback alarm

This fault is integrated as a safety check, because the DMA memory array is not replicated in the safety lake (safety core). The control signals that the DMA memory controller sends to the DMA memory for any operation are latched and sent back from the DMA memory to the DMA memory controller.
The DMA memory controller compares the received control signals with the transmitted control signals. If they do not match, the feedback alarm is generated.

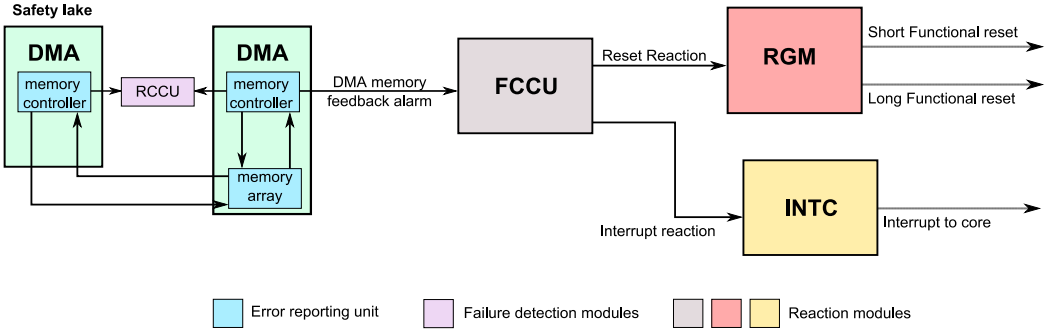

Figure 56. DMA memory feedback alarm

5.55. Redundancy mismatch: DSMC D-MEM out of lockstep

This FCCU fault is triggered whenever the RCCU detects a mismatch in the DMEM located on both cores. The DMEM is replicated and its outputs are monitored by the RCCU.

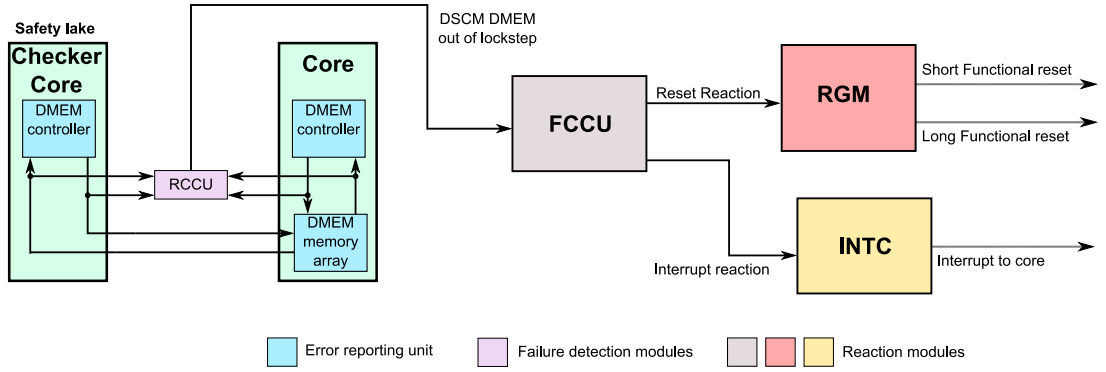

Figure 57. Redundancy mismatch: DSMC DMEM out of lockstep

5.56. Flash memory low power entry error: failure to enter Stop mode upon Stop mode entry request

This FCCU fault input is triggered if the entry to the flash low-power mode is not successful.

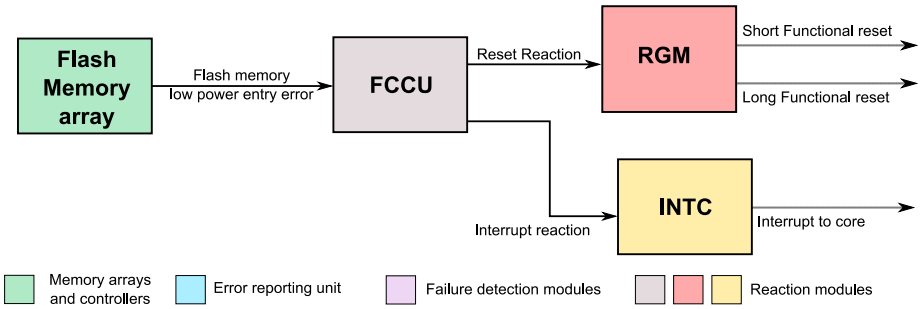

Figure 58. Flash memory low power entry error

5.57. SMPU transaction monitor mismatch

This FCCU fault is triggered whenever the SMPU transaction monitor detects a mismatch. This fault is not detected by the NCF[38] XBAR transaction monitor mismatch. Therefore, it is separately routed to the NCF[71] as the SMPU transaction monitor mismatch.

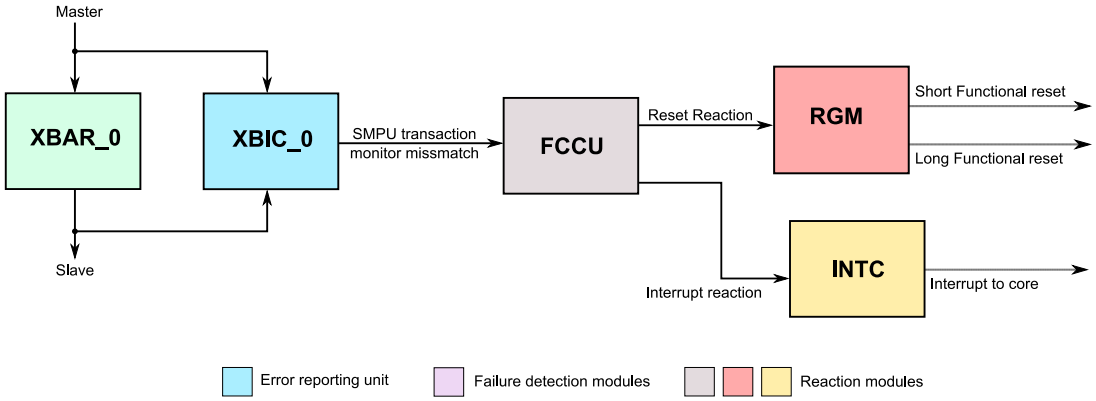

Figure 59. SMPU transaction monitor mismatch

5.58. First timeout interrupt request from Software Watchdog of Safety Core

The FCCU First timeout interrupt request from Software Watchdog of Safety Core fault is triggered when the software watchdog timer is not serviced by the software in time. The root cause can be a software fault or a random hardware fault that causes the system to hang.

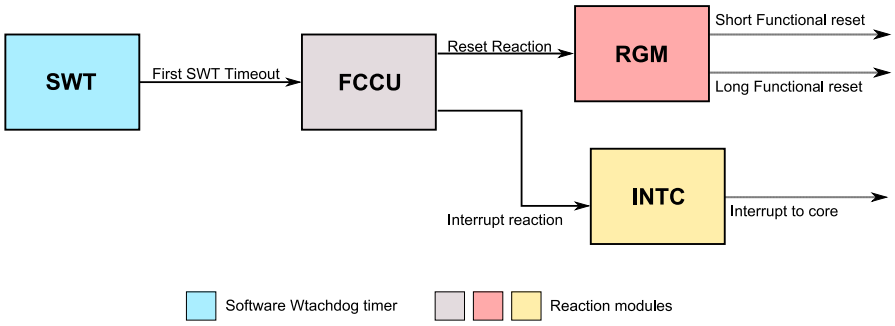

Figure 60. First timeout interrupt request from Software Watchdog of Safety Core

5.59. Digital PMC initialization error during DCF data load (status is cleared if the fault is not persistent)

This fault is signaled to the FCCU whenever the loading of the DCF records to the PMC module (during the initialization phase) is not executed correctly. This causes the PMC module to operate under unknown conditions. To prevent issues, NCF[73] is called. Its status is cleared when the fault is not persistent.

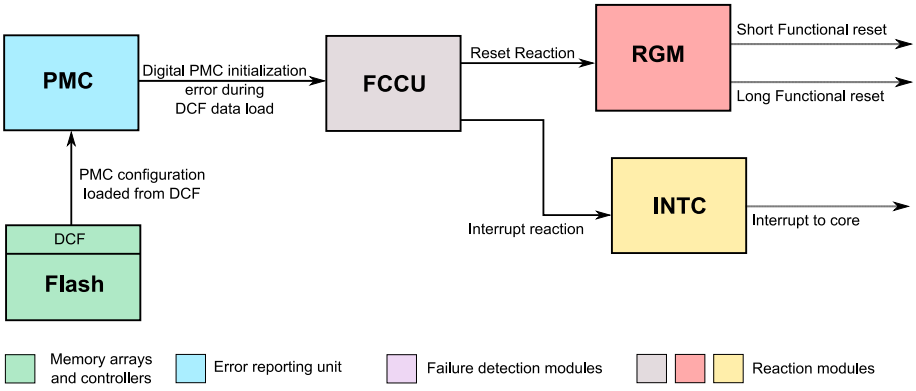

Figure 61. Digital PMC initialization error during DCF data load

5.60. Misconfiguration of error_out pin interface of the FCCU after reset (overwriting the respective configuration bits resolves this error)

This fault is triggered when the configuration of the error_out pin is incorrectly loaded from the DCF records into the FCCU module. Overwriting this configuration with a correct one resolves this fault.

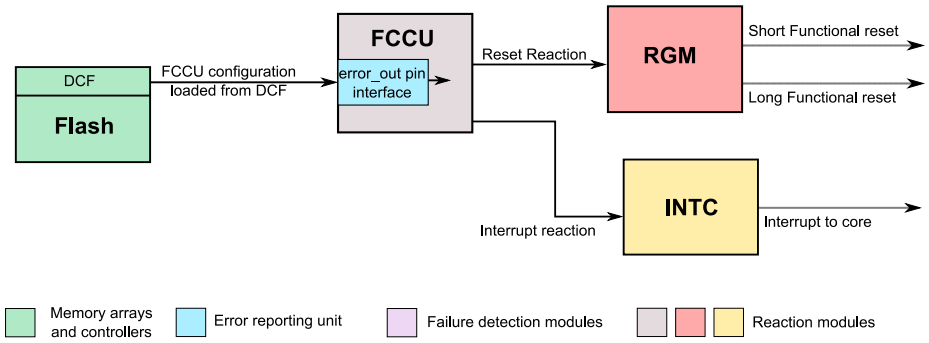

Figure 62. Misconfiguration of FCCU error_out pin interface

6. Definitions, Acronyms, and Abbreviations

Table 2. Acronyms and abbreviations

Acronym	Definition
ECC	Error Correction Code
EDC	Error Detection in Correction
SMPU	System Memory Protection Unit
NCF	Non-Critical Fault
DTCM	Data TCM (Tightly Coupled Memory)
FCCU	Fault Collection and Control Unit
RCCU	Redundancy Checker and Control Unit
DCF	Device Configuration Format
SoC	System on Chip
DSMC	Decorated Storage Memory Controller

7. References

- *Handling Crystal Failure for MPC57XX* (document AN4880)
- *MPC5744P Reference Manual* (document MPC5744PRM)

8. Revision History

This table summarizes the changes made to this document since the initial release:

Table 3. Revision history

Revision number	Date	Substantive changes
0	03/2016	Initial release.

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: AN5259
Rev. 0
04/2016