NXP Semiconductors
Safety Manual

Document Number: MPC5777M_GMSM
Rev. 1.1, 10 Apr 2017

Safety Manual for MPC5777M

Table of Contents

1 Preface

Assumption: This document provides guidelines for the proper use of the MPC5777M Microcontroller Unit (MCU) in ASIL D applications. It will help guide the user with the steps necessary to integrate the MPC5777M into their application.

Assumption: The MPC5777M will be used as a component within a safety related application. To allow an analysis of the MCU's capability to reach the required safety level, assumptions have been made (following the concept of SEooC described in the ISO26262). These assumptions are on the scope of the MCU (for example, including external components interacting with the MCU) and on its usage by application software. The FMEDA provided with the MPC5777M was conducted under inclusion of these assumptions.

Assumption: [SCG18.098]A typical safety function operates by reading input from the MPC5777M's I/O facilities (including network connections), processing this input possibly using, generating, and storing results valid for several calculation cycles, and sending output to other system components (for example, actuators or other MCUs) again using the MPC5777M's I/O facilities [end].

This document considers:

- The system assembly that contains the MPC5777M MCU
- The “Safety Element out of Context” section in the “Road vehicles - Functional safety - Part 10: Guideline [ISO 26262-10:2012]” standard
- Certain assumptions about the assembly's functional safety needs based on that standard

and determines whether a measure is an assumption or not based on these factors.

What this means for designers using the MPC5777M is that if they don’t fulfill a specific Safety Manual (SM) assumption they have to show that their alternative solution is similarly efficient concerning the safety requirement in question (for example, provides the same coverage, avoids Common Cause Failure (CCF) as effectively, and so on), show that the particular issue is irrelevant for their application (for example, the module is not used), or estimate how much the failure rate increases and the failure metrics (SPFM/LFM) decrease due to the deviation. Otherwise, the FMEDA provided with the MPC5777M is not valid.

This document also contains guidelines on how to configure and operate the MPC5777M for ASIL D applications. These guidelines are preceded by one of the following bold text statements:

- Implementation hint
- Recommendation

NOTE

> Further information about safety configuration and operation can be found in the *MPC5777M Reference Manual’s* “Functional Safety” chapter.

These guidelines are considered to be useful approaches for the specific topics under discussion, but are not mandatory. The user will need to use discretion in deciding whether these measures are appropriate for their applications.

This document is only valid under the assumption that:

- **Assumption:** [SCG18.170]the MPC5777M is used in automotive applications for use cases requiring a fail-silent or a fail-indicate MCU. [end]
- the environmental conditions given in the *MPC5777M Data Sheet* are maintained.

As for all devices, device errata must be taken into account during system design and implementation. For a safety-related device such as the MPC5777M, this also concerns safety-related activities such as system safety concept development. The FMEDA and Safety Concept are valid if the listed assumptions in the text are covered.

Assumption: [SM_FMEDA_131] All relevant hardware safety mechanisms are enabled and configured correctly when using any of the information in this document. [end]

General failure rate, or even an FMEDA (Failure Modes, Effects & Diagnostic Analysis) report, is available upon request when covered by a NXP Semiconductors NDA (contact your NXP Semiconductors representative).

2 General information

2.1 Mission profile

Lifetime for a MPC5777M is 20 years which is equivalent to 20000 hours of active operation for the MCU. The assumed mission profile is:

- Lifetime: 20 years
- Total operating hours: 20000 hours
- **Assumption:** [SCG18.002] Trip time (driving cycle): 12 hours [end]
  - This is the maximum time of operation of the MPC5777M without a start-up reset.
- **Assumption:** [SCG18.003] Fault-Tolerant Time Interval (FTTI, also known as Process Safety Time, PST) = 10 ms[end]
  - FTTI is the time the controlled system will not transition to a hazardous state, despite the MPC5777M failing.

NOTE

> This is a conservative estimate since the actual number depends on MCU application (See Section 2.6, Failure indication time, for exact calculation instructions).

The MPC5777M was designed to work within a maximum operational temperature profile (see the *Qorivva MPC5777M Microcontroller Data Sheet*).

Assumption: [SM_FMEDA_001] The device is to be handled according to JEDEC standards J-STD-020 and J-STD-033. [end]

2.2 Functional safety – ISO 26262 compliance

Assumption: [SCG18.201]The MPC5777M MCU was developed in accordance with ISO 26262 as a Safety Element out of Context (SEooC). [end]

The MPC5777M is suitable to be used in safety-relevant applications including systems that are classified as ISO 26262 ASIL A, ASIL B, ASIL C or ASIL D.

Assumption: [SCG18.202]The development process of the MPC5777M fulfills ASIL D requirements of ISO 26262. [end]

2.3 Safety goals

The safety goals of the MCU are defined as follows:

- [SCG18.100]The **primary safety goal** is that the MPC5777M does not leave its safe states for intervals equal or longer than the FTTI (10 ms) unless configured by the application software to do so. [end]
- [SCG18.101]The **secondary safety goal** is that the MPC5777M, or the software running on the MPC5777M, shall be able to detect the permanent unavailability of any safety mechanism that is necessary to achieve the primary safety goal, and this shall be done at least once per driving cycle (12 hours). [end]

The ASIL for the first goal is D, for the second it is B.

2.3.1 Safe state

A Safe state of the system is named Safe state$_{\text{system}}$ whereas the Safe state of the MPC5777M is named Safe state$_{\text{MCU}}$. A Safe state$_{\text{system}}$ of a system is an operating mode without an unreasonable probability of occurrence of physical injury or damage to the health of persons.

Assumption: [SCG18.004]The safety goals are achieved by transitioning or holding the MPC5777M in the following Safe state$_{\text{MCU}}$:[end]

- **Assumption:** [SCG18.005]Completely unpowered [end]
- **Assumption:** [SCG18.006]In reset [end]
- **Assumption:** [SCG18.007]Operating correctly (See Section 2.4, Correct operation) [end]
- **Assumption:** [SCG18.008]Explicitly indicating an internal error [end]

If the MPC5777M continuously switches between a standard operating state and the reset state, without any device shutdown, the MCU is not considered to be in a Safe state$_{\text{MCU}}$ (See Section 3.2.7, Reset Generation Module (MC_RGM) for details).

Assumption: [SM_FMEDA_002] The application shall identify and signal such switching as a failure condition. [end]

If the MPC5777M signals an internal failure via its error out signals (FI[0], FI[1]), the surrounding subsystem should no longer use the MPC5777M outputs for safety functions since these signals are no longer considered reliable. This means that if an error is indicated, the system must be able to remain in a Safe state$_{\text{system}}$ without any additional actions by the MCU. Depending on its configuration, the system may disable or reset the MCU as a reaction to the error signal.

Assumption: [SCG18.009]It is assumed that the system reacts safely to the MPC5777M being in or entering all safe states shown in Section 2.3.1, Safe state. [end]

2.4 Correct operation

Assumption: [SCG18.010]Correct operation of the MPC5777M is defined as: [end]

- **Assumption:** [SCG18.011]Vital system modules (ViMos) and other supporting modules (SuMos) are operating according to specification. [end]
- **Assumption:** [SCG18.012]Peripheral modules (PeMos) are operating according to specification. [end]
- **Assumption:** [SCG18.013]Non-safety modules (NoSaMos) are not interfering with the operation of other modules. [end]
- Other support modules (SuMo) are safety-relevant and in principle potential members of the ViMos category, and cannot lead to a violation of the safety goal on their own. Typically, these will only have multiple point faults, but not single point faults.

NOTE

[SCG18.902]See “Module classification” table in the *MPC5777M Reference Manual’s* “Functional Safety” chapter for specific module safety classification. [end]

2.5 Failure indication signaling

The Fault Collection and Control Unit (FCCU) offers a hardware channel to collect errors and to bring the device to a Safe state$_{MCU}$ when a failure is present in the device. The FCCU provides two error output pins (bidirectional FI[0] and FI[1], on PB[11] and PC[2], respectively) as a failure indication to the external world.

Different protocols for the error output pins are supported:

- Dual rail protocol
- Time switching protocol
- Bi-stable protocol

If bi-stable protocol is selected, it is possible to use only one of the two error output pins on the MPC5777M. Since the pin multiplexing that is utilized for each of the error output signals works differently, FI[0] should be the signal used in this configuration.

After start-up reset, the error output signal FI[0] is in high impedance while FI[1] is functionally a GPIO input with a weak pullup. The error output pins transition to the operational state only on software request.

A functional reset has no influence on FI[0] but sets FI[1] to high impedance with a pullup. To avoid changing FI[1] during functional reset when time switching or bi-stable protocol is used, it is recommended to write 0 to FCCU_CFG[PS].

Refer to Section 4.5, Error Out Monitor (ERRM) for details on specific requirements for connecting FI[0] and FI[1] to an external device.

2.6 Failure indication time

Failure indication time is the time it takes from the occurrence of a failure to when the indication of that failure is visible by driving the error out pins or by assertion of reset.

The failure indication time of the MPC5777M is finite. It must be taken into account when determining application safety strategies since failure indication time plus reaction time on this indication by the system must be less than the FTTI.

[SCG18.128]Failure indication time has three components, two of which are influenced by certain configuration choices:
Failure indication time = **recognition time** + **internal processing time** + **indication time**.

Each component of failure indication time is briefly described as follows:

- **Recognition time** is the maximum of the recognition time of all involved safety mechanisms. The two mechanisms with the longest times are:
  - — Recognition time related to the FMPLL loss of clock: This time depends on the FMPLL configuration. This time is approximately 20 µs.
  - — Diagnostic cycle time of software self-tests. This time depends closely on the software implemented.
- **Internal processing time** lasts a maximum 10 IRCOSC clock cycles (nominal frequency of IRCOSC is 16 MHz).
- **Indication time** is the time to notify an observer about the failure. This time depends on the indication protocol in the FCCU:
  - — Dual Rail protocol and time switching protocol –
    - — FCCU configured as “fast switching mode”: indication delay is maximum 64 µs. As soon as the FCCU receives a fault signal, it reports the failure to the outside world via an output pin (if properly configured).
    - — FCCU configured as “slow switching mode”: an indication delay could occur. The maximum delay is equal to the period of the error out signal, which toggles at a frequency of 61 Hz.
  - — Bi-stable protocol: indication delay is maximum 64 µs. As soon as the FCCU receives a fault signal, the FCCU reports the failure via an output pin (if properly configured).

If the configured reaction to a fault is an interrupt, an additional delay (interrupt latency) can occur until the interrupt handler is able to start executing (for example, higher priority IRQs, XBAR contention, register saving, and so on). [end]

Assumption: [SCG18.022]The overall failure indication time shall be less than the FTTI of the application (assumed FTTI shown in Section 2.1, Mission profile). [end]

2.6.1 Minimum failure indication time

When a failure event occurs, one or both error output signals (F*n*) are set to show an error condition for a minimum time (T_min), even if software attempts to reset the state of the error out signals. The external failure indication stays in failure mode for a configurable minimum time as shown in Equation 1. For bi-stable protocol the time DELTA_T is configurable by software up to a maximum of 10 ms by configuring FCCU_DELTA_T[DELTA_T].

$$\text{T\_min} = 250\ \mu\text{s} + \text{FCCU\_DELTA\_T[DELTA\_T]}\ \mu\text{s} \qquad \textit{Eqn. 1}$$

In case another failure event happens within T_min after the first failure event, the timer measuring T_min is restarted.

2.7 Failure handling

The FCCU is responsible for reacting to internal failures. A different reaction can be configured for each failure source.

Failure sources include:

- All failure indication signals from the modules within the MCU
- Control logic and signals monitored by the FCCU itself
- Software-initiated failure indications
- External failure input (via FI[0] pin)

The different failure sources, as represented by the FCCU failure inputs, are shown in “FCCU failure inputs” table in the “Functional Safety” chapter of the *MPC5777M Reference Manual*.

Available failure reactions include:

- Maskable interrupt
- Non-maskable interrupt
- Reset
- Change the state of the failure indication pin(s)
- No reaction

Additionally, the transmission capabilities of the communication controllers can be disabled when the FCCU transitions to the error state (see “Disabling of communication controllers” in the “Functional Safety” chapter of the *MPC5777M Reference Manual*).

Software can read the failure source that caused a fault from the FCCU_RF_S[0:3] registers and can do so either before or after a functional reset. Software can also reset the failure by resetting the respective status bit, but the external failure indication will stay in failure mode for a configurable amount of time (see Equation 1).

Error handling can be split into two categories:

- Handling of errors during runtime
- Handling of errors during boot-time (for example, LBIST, MBIST)

Assumption: [SM_FMEDA_003] Runtime errors shall be handled in a time shorter than the FTTI. [end]

Assumption: [SM_FMEDA_004] Boot-time failure handling shall be handled before the safety function starts execution. Typically, the reaction is to not let the safety function start and give a failure indication to the user. [end]

3 Functional safety requirements for application software

This section gives an overview of the necessary or recommended measures when using the individual components of the MPC5777M. If a module in the MPC5777M is used without following the required actions, there is a risk that the safety certificate for the entire MCU, or other modules if the failure interferes with their operation, may be invalidated.

It is possible to ignore the required measures if equivalent measures to manage the same failures are alternatively included.

Modules not explicitly covered by this document do not require any safety specific software measures.

To assist continuous product improvement, it is recommended to report field failures which occur despite following these measures to NXP Semiconductors in accordance with ISO 26262-7 Chapter 6.4.2.1.

3.1 Disabled modes of operation

The system and application software must ensure that the functions described in this section are not activated while running safety-relevant operations.

3.1.1 Debug mode

The debugging facilities of the MPC5777M are a potential source of failure when activated during the operation of safety-relevant applications. They can halt the cores, cause breakpoint hits, write to core registers and the address space, and activate boundary scan. The MCU must therefore not enter debug mode to avoid interference with the normal operation of the application software.

The state of the JCOMP pin determines whether the system is being debugged or whether the system operates in normal operating mode. When the JCOMP pin is logic low, the JTAGC TAP controller is kept in reset for normal operating mode. When it is logic high, the JTAGC TAP controller is enabled and the system can enter debug mode if requested. The system must ensure that it does not attempt to enable debug mode by externally asserting the JCOMP pin during boot up. Otherwise, a fault condition signal will be sent to the FCCU.

Assumption: [SCG18.023]Debugging will be disabled in the field while the device is being used for safety-relevant functions. [end]

Assumption: [SCG18.024]For normal operation, software needs to configure any module that is safety relevant (such as SWT) to continue execution during debug mode and to not freeze the module operation if debug mode is entered. [end]

3.1.2 Test mode

Several mechanisms of the MPC5777M can be circumvented in test mode, undermining the safety concept. Test mode is used for comprehensive factory testing and should not be used in normal operating mode.

The TEST pin is for testing purposes only and should be allowed to float in the user application. The system must ensure the TEST pin is not asserted during boot to enable test mode. (The TESTMODE pad has an internal pull-down that is always active to keep it from asserting during normal operation.) The activation of test mode is supervised by the FCCU and will signal a fault condition when test mode is entered.

Assumption: [SCG18.025]Test mode will be disabled in the field while the device is being used for safety-relevant functions. [end]

To avoid unwanted activation of the testing circuitry the Design For Testability (DFT*n)* FCCU error inputs must be enabled even if they are not needed by the application. The FCCU channels for DFT[1:4] are 46 to 49, respectively. These error inputs are enabled by setting the appropriate bits in the following registers:

- FCCU_RF_CFG
- FCCU_RFS_CFG
- FCCU_RF_TOE
- FCCU_RF_E
- FCCU_IRQ_ALARM_EN
- FCCU_NMI_EN
- FCCU_EOUT_SIG_EN

3.2 Initial checks and configurations

After start-up, the application software must ensure the conditions described in this section are satisfied before safety-relevant functions are enabled. Additional configuration is needed to ensure freedom from interference between cores and between concurrent software (see Section 3.4, Operational interference protection).

3.2.1 I/O ball configuration

Assumption: [SCG18.120]The user shall avoid configurations that place redundant signals on neighboring pads or pins. [end]

[SCG18.121]To determine whether two functions on two package balls are adjacent to each other, refer to the mechanical drawings of the packages (see the *MPC5777M Data Sheet*) together with the spheres (balls) number information of the packages as seen in the *MPC5777M Reference Manual's* “System Integration Unit Lite2 (SIUL2)” section together with the ball information provided in the document "MPC5777M_System_IO_Description_and_Input_multiplexing_tables" that is attached to the *MPC5777M Reference Manual*. [end]

3.2.2 MCU configuration

Assumption: [SCG18.051]Safety software running on the Safety Core shall check correct initialization of the MPC5777M before activating the safety-relevant functionality. [end]

NOTE

> See the “DCF Client List” table in the “Device Configuration Format (DCF) Records” chapter of the *MPC5777M Reference Manual* for details.
>
> See the “IOP applies device settings” section in the “Reset and Boot” chapter of the *MPC5777M Reference Manual* for details on the IOP phase of the boot

Assumption: [SM_FMEDA_005]FMEDA assumes that the device is properly configured by the DCF records in the UTEST sector of the flash memory to enable the Hardware Security Module (HSM) I/O Processor (Core 2) handshaking during the boot phase. [end]

NOTE

> See the “Reset sequence flow based on initial device condition” section of the “Reset and boot” chapter of the *MPC5777M Reference Manual* for details.

The MCU memory configuration and the JTAG Part ID number can be read in the SSCM_MEMCONFIG register (JTAG Part ID = SSCM_MEMCONFIG[JPIN]).

This information is normally used for debugging purposes, and is not necessary for the safety function.

Assumption: [SM_FMEDA_006]Application software does not use the JTAG Part ID, nor does it affect safety critical operations. [end]

With the System Status and Configuration Module (SSCM) it is possible to configure different MCU behaviors (for example, determine primary and HSM boot vector, abort disable/enable).

Assumption: [SM_FMEDA_008]SSCM shall be configured to trigger an exception in case of any access to a peripheral slot not used on the device (SSCM_ERROR register). [end]

Assumption: [SM_FMEDA_009]After boot has completed, the application should perform an access to unimplemented memory space and check for the expected abort to occur. [end]

The FCCU can be configured to trigger a NMI to the Safety Core if a fault is detected. In the case of a functional reset, this NMI is masked by hardware and is unmasked during BAF execution. The NMI service routine is executed as soon as the Safety Core is activated.

In the worst case, this flow can cause an unwanted functional reset loop. For example, assume a situation which can not be recovered by software, and the NMI service routine can only trigger a functional reset. After the reset, the BAF unmasks the NMI which triggers the Safety Core. Which cause the NMI to execute again.

Assumption: Pending FCCU faults shall be cleared before enabling the Safety Core after a functional reset.

From an application standpoint this means:

1. Do not activate the Safety Core automatically during or after the BAF.
2. Initialize the FCCU (may be preceded by a software reset of the FCCU).
3. Activate the Safety Core.

3.2.3 Mode Entry (MC_ME)

To overcome faults in the wakeup and interrupt inputs to the MC_ME, the following is assumed if the application uses Low Power mode (LP):

- **Assumption:** [SM_FMEDA_010] The duration in LP mode is monitored. If the system does not wake up within a specified time frame, the system will be reset by the monitor (for example, SWT can provide the time monitoring). [end]
- **Assumption:** [SM_FMEDA_011]Software will perform a test of entry and exit to and from LP mode at startup. [end]

An incorrect clock source as the system clock could be selected due to faults, resulting in multiple faults. In order to improve detection of such faults, and the effect by the clock monitors:

- **Assumption:** [SM_FMEDA_012]It is assumed that the nominal frequency of different clock sources that are available as the system clock have different frequencies. [end]

The mode configuration registers of MC_ME take effect only when the mode transition request is initiated. Thus, instead of the configuration registers the global status register should be CRCed (if configuration register CRCing is done) as that represents the current state.

Assumption: [SM_FMEDA_013] Application software shall check the target mode configuration immediately before issuing a mode transition request. [end]

Assumption: [SM_FMEDA_014] In order to check that a mode transition has been correctly executed, after initiating a mode transition request, software shall verify the mode transition status within the expected completion delay. Also, the new configuration is compared with the intended configuration. This does not apply if the target mode transition is to LP mode. [end]

NOTE

> The MC_ME implements a register to request a mode transition and registers that report the status of the transition (for example, MC_ME_MCTL to request mode transitions, MC_ME_IMTS to provide the cause of an invalid mode interrupt, and MC_ME_DMTS to show the status of the mode transition).

The monitoring and types of reactions can be enabled in the FCCU for the following fault inputs[1]:

- [SM_FMEDA_015]Compensation disable (FCCU ch 53)[end]
- [SM_FMEDA_016]SAFE mode (FCCU ch 52)[end]

[1] See the “Module classification” table in the *MPC5777M Reference Manual’s* “Functional Safety” chapter for specific module safety classification.

3.2.4 Start-up configuration check

During boot, start-up software is not executed on the Safety Core.

Assumption: [SM_FMEDA_017]Safety software running on the Safety Core shall check correct initialization of the MPC5777M before activating the safety-relevant functionality. This check shall not be executed on the core executing the start-up software. [end]

3.2.5 Dual core lockstep mode

The MPC5777M device operates in delayed lockstep mode (LSM) to allow the highest safety level to be reached. The Checker Core will receive all inputs delayed by two clock cycles. Outputs of the Checker Core will be compared with outputs of the Master Core. Any differences will be flagged as an error which will be processed by the FCCU.

For safety operation, the LOCKSTEP_EN bit in the flash memory UTEST miscellaneous DCF client must not be set to disabled. If the LSM is disabled, the Checker Core and the Redundancy Checker Control Units (RCCUs) are disabled. This triggers a fault indication to the FCCU. The Checker Core will not work independently from the Master Core. No dynamic switching is possible between LSM on and LSM off (any change to the LOCKSTEP_EN bit will only take effect after the next reset).

Before starting safety-relevant operations, the application software shall check that lockstep mode is enabled (confirm MC_ME_CS[S_CORE1] = 1 (master) and MC_ME_CS[S_CORE2] = 1 (checker), confirm that no failure is signalled on alarm #51, for example) and configure the FCCU to react to lockstep disablement.

Assumption: [SCG18.027]Before starting safety-relevant operations, the application software shall check that lockstep mode is enabled (for example, confirm MC_ME_CS[S_CORE1] = 1 (core_0, master) and MC_ME_CS[S_CORE2] = 1 (core_0s, checker), and no failure is signalled on FCCU fault 51 (Lockstep mode)), then configure the FCCU to react to lockstep disablement. [end]

3.2.6 FCCU fault reaction configuration

The Fault Collection and Control Unit (FCCU) collects faults and manages the reaction to these faults. A mechanism is usually provided to allow software to check the integrity of the different error paths. Most reactions are disabled at boot time so software configuration is required. Refer to Section 2.7, Failure handling for the valid FCCU fault reactions.

Assumption: [SM_FMEDA_018]Application software shall check the FCCU configuration once after programming. [end]

The FCCU is checked by the FCCU Output Supervision Unit (FOSU) which provides a secondary path for the failure indication and reports to the Reset Generation Module (MC_RGM). The FOSU only causes a reset if the FCCU fails to react to an enabled incoming enabled fault within a fixed time interval (8000 IRCOSC cycles). The FOSU does not require software configuration. While the FCCU is in its CONFIG state, the FOSU does not monitor the FCCU for faults or the resulting reaction.

Assumption: Application software shall check and clear any pending faults when it moves the FCCU out of the CONFIG state.

Assumption: [SM_FMEDA_019] Before starting safety-relevant operations, software must configure the fault reactions to each fault that is safety-relevant for the application. [end]

To configure the fault reaction to each fault, the FCCU state machine is placed in the CONFIG state. Safety analysis assumes that the CONFIG state of the FCCU is not a Safe state$_{MCU}$.

To avoid a stuck condition in the CONFIG state due to a failure, the FCCU implements an internal watchdog which, in case of a timeout condition, automatically transitions the FCCU state machine from CONFIG to NORMAL state and restores default values of the configuration registers (see section “FCCU CFG Timeout Register (FCCU_CFG_TO)” in the *MPC5777M Reference Manual*).

NOTE

Implementation hint: Software must program the FCCU configuration registers (for example, FCCU_RFS_CFG*n*, FCCU_NMI_EN*n*, FCCU_EOUT_SIG_EN*n*) to configure the fault reaction of each fault. These registers are writable only if the FCCU is in the CONFIG state.

Assumption: [SM_FMEDA_020] The integrity of the entire error reaction path shall be verified at least once after the boot. [end]

NOTE

Different approaches to verify the functionality of the error reaction paths can be used. Some error reaction paths are checked during LBIST and don’t require the development of additional software, whereas others require application software.

The table “FCCU failure inputs” from in the “Functional Safety” chapter of the *MPC5777M Reference Manual* shows the suggested approach for each FCCU failure input.

The FCCU will come out of reset with most of the failure inputs disabled. Failures which occur during boot will, for the most part, not be acknowledged by the FCCU as a failure. To check whether such errors have occurred, SW can read the FCCU failure status registers for any latched error and act on the status of those bits accordingly (FCCU_RF_S[0:3]).

NOTE

The *MPC5777M Reference Manual’s* “FCCU failure inputs” table in the “Functional Safety” chapter lists failure sources, associated FCCU channels and how they can be tested.

The error indication on pins, FI[0] and FI[1], are controlled by the SIUL2 and FCCU. The field SIUL2_MSCR[SMC] can be configured to have the output buffer disabled when the MPC5777M enters Safe mode (for example, for FI[0], SIUL2_MSCR27[SMC] = 0, and for FI[1], SIUL2_MSCR34[SMC] = 0). The FCCU_CFG register is used to configure other FI[*n*] options like signal polarity, switching mode, software control, and so on.

Assumption: [SM_FMEDA_124] It is assumed that whenever error indication is enabled on FI[*n*], the SMC bit in associated MSCR register are always programmed to 1 with register access protection enabled. [end]

The FCCU together with the INTC, can lead to cyclic reset. For example consider the following situation:

1. Error indication arrives at FCCU
2. FCCU triggers IRQ
3. SW analyzes fault and causes a reset
4. MCU comes out of reset and hands over to SW
5. SW configures INTC
6. SW gets the same IRQ again (because FCCU still holds the IRQ line), analyzes fault and causes a reset ad infinitum (or rather till the reset escalator engages and causes a destructive reset).

To avoid this situation the following assumption is considered.

Assumption: [SCG18.500]It is assumed that FCCU pending fault status should be cleared before the INTC is configured. [end]

Since the NMI is edge triggered, even if it is kept active during a functional reset until the fault status is cleared, it will not interrupt the Safety Core and the described cyclic reset can't be seen.

Assumption: [SCG18.900]If the clock driving the FCCU (IRCOSC) fails, software must find other ways to signal an error other than using the FCCU control of the error output pin(s) (FI[*n*]). [end]

NOTE

There are different methodologies that could be used to satisfy this assumption. For example, issuing a reset, or switching FI[*n*] pin control to a GPIO and using it to drive an error signal instead of using FI[*n*].

Assumption: [SCG18.901] If the FCCU uses NMI as a failure reaction, the Safety Core will not be enabled after a reset during the first mode transition of the MC_ME module but earliest at the second transition which will initiated earliest several IRCOSC cycles after the first. [end]

Unwanted activation of LBIST/MBIST causes a violation of the safety goal.

Assumption: [SM_FMEDA_028] Software shall always enable FCCU reactions to error events indicating unexpected STCU2 activations. [end]

3.2.7 Reset Generation Module (MC_RGM)

The MC_RGM is the central point for resetting the MCU. One of its tasks is to prevent reset cycling caused by reset escalation. It also can transition to SAFE mode. The SAFE mode has not been considered a Safe state$_{\text{MCU}}$ during safety analysis.

Permanent cycling through otherwise safe states or permanent cycling between a safe state and an unsafe state is considered a violation of the safety goal. Specifically, this scenario relates to a continuous Reset – Start, Operation – Reset or Reset – Self-test – Reset sequence. Allowing such cycles would be problematic as it would allow an unlimited number of attempts of the test that is causing the cycle which could possibly endanger its ability to detect device failures.

To detect a loop of continuous functional resets, the MPC5777M supports functional reset escalation which can be used to generate a destructive reset if the number of functional resets reaches the programmed value. Once the functional reset escalation is enabled, the Reset Generation Module

(MC_RGM) increments a counter for each functional reset that occurs. When the number of functional resets reaches the programmed value in the MC_RGM_FRET, the MC_RGM initiates a destructive reset. The counter can be cleared by software, destructive reset or start-up reset.

A similar mechanism to detect a loop of continuous destructive resets is implemented in the MC_RGM. When the destructive reset counter reaches the programmed value, the MCU will be held in reset until the next power-on reset. The destructive reset counter can be cleared by software or by a power-on reset.

Assumption: [SCG18.028]Safety software will reset the functional and destructive reset counters every time it has finished checking its environment (for example, before making the F*n* pin active). [end] The MC_RGM_FRET (functional reset counter) and MC_RGM_DRET (destructive reset counter) registers allow the user to select the number of functional and destructive resets that can occur before action is taken (see “Reset Generation Module (MC_RGM)” in the *MPC5777M Reference Manual* for details).

Assumption: [SM_FMEDA_022] Software shall enable functional reset escalation for the condition when multiple functional resets occur consecutively. [end]

NOTE

> Functional reset escalation is enabled by writing a non-zero value to the MC_RGM_FRET register (see the *MPC5777M Reference Manual’s* ‘Reset Generation Module (MC_RGM)).

Reset escalation is a hardware mechanism that provides protection against a loop of continuous resets. The time between these loops can be so short that the application software doesn’t have time to take any action to manage them. Longer reset cycles must be managed by application software.

Assumption: [SCG18.029]Before clearing the reset counters of the escalation mechanism, the safety software shall ensure that longer reset cycles can be detected by the software. [end]

NOTE

> There are various methods to implement this requirement. For example, safety software, before clearing the reset counters, reads (and saves) the FCCU error status indication (if any faults were found) and compares the status with previous saved versions. If too many resets due to faults are observed, software can react by triggering a destructive reset.

For some events, the MC_RGM can be configured to react not with a functional reset, but with a transition to the SAFE mode (see the description of the MC_RGM_FEAR in the *MPC5777M Reference Manual*). In such a case, one watchdog shall be kept enabled. If this watchdog times out, the FCCU shall move the MCU into one of its safe states.

Assumption: [SCG18.030] If the MC_RGM is configured to react with a transition into SAFE mode, at least one watchdog timer shall remain enabled. The FCCU shall be configured to react to a timeout of this watchdog with a long functional reset or driving the error out signals to a fault condition. [end]

Assumption: [SM_FMEDA_023]Software will read the reset status after boot ensuring that the reset cause is indicated. Then software will clear the register, and read back the value verifying that it is actually cleared. [end]

Assumption: [SM_FMEDA_024]Resets during normal operation will be executed only as a reaction to an error, not as a functional measure. This avoids undetected faults due to interrupts that are not being generated. [end]

3.2.8 Self-test completion

To ensure absence of latent faults, the self-test executes both a Logic Built-In Self-Test (LBIST) and a Memory Built-In Self-Test (MBIST) during boot while the device is still under reset (offline). The boot time BIST includes the scan-based LBIST to test the digital logic and the MBIST to test all RAMs and ROMs[1].

NOTE

> The overall control of LBISTs and MBISTs is provided by the Self-Test Control Unit (STCU2). The STCU2 will execute automatically after a power-on reset[2] (POR), external reset and destructive reset, and will also execute when initiated by software (online self-test). The MPC5777M logic is grouped into ten LBIST partitions used for both production testing and self-test.
>
> The *MPC5777M Reference Manual's* “Self-Test Control Unit (STCU2)” chapter and “Use cases and limitations” section discusses details on how to correctly execute offline and online self-tests.
>
> The section “Online Logical BIST (LBIST)” of the *MPC5777M Reference Manual's* “Functional safety chapter” shows tables of the module groupings of each LBIST partition.

Assumption: [SCG18.125]If there is an LBIST failure, or MBIST detects uncorrectable failures, the STCU2 will cause a destructive reset, causing execution of the self-test again. This is to ensure that a self-test, which fails only due to a transient error, will not block device usage. If several self-tests fail in a row, the desctructive reset escalation will activate and hold the MCU in reset. [end]

On the other hand, if MBIST detects correctable failures, software must decide whether to continue or halt execution. In fact, the MBIST may detect and report two (or more) Single Bit Errors (SBEs) occurring in multiple test passes instead of one Multiple Bit Error (MBE).

Assumption: [SM_FMEDA_025] Software will determine if two or more errors reported by the MBIST as SBEs combine to create an uncorrectable error by examining the entries in the System RAM Memory Management Unit (MEMU) instance. If several entries exist for the same address with different bit numbers, this data word actually has an MBE instead of the several SBEs discovered by the MBIST. [end]

Assumption: [SM_FMEDA_026] After start up (and more in general, always after the execution of MBISTs), software will cross check MBIST status in the STCU2 (pass or fail) with the content of MEMU MBIST buffer (same as system RAM) to detect failures affecting the reporting of MBIST errors. This can

[1] This does not include flash memory.

[2] The customer must enable the self-test in the shadow sector of the flash memory since the factory default configuration will be to not run the self-test).

be due to faults affecting the reporting path for MEMU or STCU2 logic. (notice that STCU2 is not part of any LBIST partition and only a pass/fail flag is available). [end]

Assumption: [SCG18.031]After start-up and before the safety application starts, application software shall confirm that all LBISTs and MBISTs finished successfully, MISRs contain the expected values, and no critical failure is flagged. The critical failures may include LBIST failures, MBIST MBEs, MBIST SBEs exceeding the maximum tolerated number (<= 8 due to MEMU buffer size) and self-test failures. [end]

NOTE

> See the “Off-Line Self-Test Sequence” section in the *MPC5777M Reference Manual* for details about test sequencing and completion validation.

The STCU2, as well as LBIST and MBIST controllers, are themselves subject to failures, which may prevent self-tests from executing correctly (for example, no self-test execution, or execution of the wrong algorithm). For latent faults affecting LBIST execution, checking the MISR register upon LBIST completion is considered sufficient. For MBIST only a pass/fail flag is provided (besides the collection of detected MBIST errors in the MEMU).

The following must be followed to improve the detection of latent faults, particularly those affecting correct MBIST execution:

- **Recommendation:** LBIST should be scheduled before MBIST since LBISTs also cover the logic running memory self-tests and the MEMU BIST error collection logic/buffers; this will help to detect latent faults responsible for the wrong or incomplete execution of memory self tests or wrong reporting of their results.
- **Recommendation:** The STCU2 CRC feature should be enabled to check that the signals exchanged between the STCU2 and MBIST/LBIST controllers are correct (for example, STCU2 commands and LBIST/MBIST responses).

NOTE

> The expected signature depends on the sequence of tests. Customers can determine the expected signature by running the desired sequence of tests and reading the resulting CRC upon test completion. One signature must be computed for each test sequence (for example, one for the start-up test sequence and one for each on-line test performed).

As far as the STCU2 error reaction path is concerned, the following are given:

- **Assumption:** [SM_FMEDA_027] SW will check the integrity of the STCU2 Unrecoverable Fault/Recoverable Fault (UF/RF) error lines that signal the FCCU and the MC_RGM (UF only) via the fake error injection register interface provided by STCU2. Before running the test, FCCU and MC_RGM shall be configured in order not to cause undesired reaction. [end]
- **Recommendation:** During the execution of the safety function, and when no on-line self-test is requested, software should disable the FCCU and MC_RGM reactions to STCU2 UF/RF error indications to avoid false trip to the safe state or interference in case of unexpected error indications.

The STCU2 provides a key-based mechanism to prevent unauthorized write accesses to its register interface. The integrity of such protection mechanism can be checked by running the following test: [end]

- **Assumption:** [SM_FMEDA_029] SW shall perform a write access to one of the STCU2 registers without providing the requested key pair and check for the generation of the expected transfer error. [end]

The STCU2 allows execution of logic and memory BIST also during runtime upon a SW request. If the I/O (including FI[*n*]) pins need a defined state during on-line LBIST, the following is recommended:

- Reset SIUL prior to on-line LBIST (using the MC_RGM_PRST0[SIUL_RST] field).
- Set pins to a desired state (if the reset-state does not meet requirements).

The following **Assumptions** have to be satisfied when the on-line BIST feature is used:

- [SM_FMEDA_030] SW shall verify that STCU2 configuration is correct before triggering the execution of on-line BISTs. [end]
- [SM_FMEDA_031] STCU2 status has to be checked after the execution of on-line LBIST/MBIST to verify that all scheduled tests have been executed and completed successfully. [end]
- [SM_FMEDA_032] Software shall supervise the execution time of on-line self tests using the SWT or any other available timer. The internal STCU2 WDT might suffer from CCFs causing either no, or slower, test execution. This may mean that no WDT timeout occurs (as internal WDT and STCU2 core logic share the same clock). [end]

NOTE

During start-up, no safety function is executed and the start up time is supervised by the external WDT. The internal prescaler feeding both the STCU2 WDT and core logic can be checked by running an on-line test and checking its execution time.

- [SM_FMEDA_033] On completion of the on-line LBIST software shall check whether reset was correctly applied to the partition(s) under test. This can be done by checking one or more registers (at least 2 recommended) for their expected reset value. Testing is not necessary if a global system reset is applied at the end of the test. [end]
- [SM_FMEDA_034] On exiting from a functional reset, software will check the status of the STCU2 to verify there are no running BISTs nor any hardware aborted tests. [end]

NOTE

BISTs still running after a functional reset are the result of incorrectly handled hardware abort requests by the STCU2 that occurred while on-line BISTs were executing.

- [SM_FMEDA_035] If STCU2 interrupt capabilities are used to notify end of test session execution, application will handle the case of missing interrupt(s) (for example, by supervising test execution time or periodically polling STCU2 status (checking STCU2_RUNSW[RUNSW], or STCU2_INT_FLG[MBIFLG] (for MBIST) and STCU2_INT_FLG[LBIFLG] (for LBIST)). [end]

3.2.9 MEMU initial checks

MBISTs report detected faults to the same MEMU reporting block used for System RAM ECC failures. Errors are in general distinguished between single-bit and multi-bit. However, it is not guaranteed that single-bit errors found in different steps on the same address are reported as multi-bit errors

Recommendation: The application software can write known error addresses into the MEMU reporting table to prevent reporting of those errors to the FCCU in case the addresses are accessed again.

3.2.10 Flash memory configuration and tests

MPC5777M provides 8.7 MB of programmable non-volatile (NVM) flash memory with ECC which can be used for instruction and/or data storage.

Assumption: [SM_FMEDA_036]To detect failures where a wrong or multiple selection targets a different block while programming, application SW shall configure flash memory blocks as read only when not the target of a write operation. [end]

NOTE

> See the “Program software locking” section in the “Embedded Flash Memory” chapter of the *MPC5777M Reference Manual* for details.

The flash memory array integrity self check detects possible latent faults affecting the flash memory array, including potential data integrity issues, or the logic involved in read operations (for example, sense amplifiers, column mux’s, address decoder, voltage/timing references). It calculates a MISR signature over the array content and thus validates the content of the array as well as the decoder logic. The calculated MISR value is dependent on the array content and must be validated by software.

The array integrity MISR value is calculated after ECC detection and correction. Flash memory ECC logic accounts for single-bit correction (SBC) opportunities, and will output corrected data into the MISR calculation.

Single bit correction reporting still occurs in the FLASH_MCR[SBC] bit and the FLASH_ADR during AI if FLASH_UT0[SBCE] = 1.

The AI breakpoint feature allows to break the Array Integrity Check execution if an event is a single bit correction or a double bit detection. Array Integrity Check can be resumed by the application after verifying the source of the correction/error and clearing the respective status bit (for example, MCR[SBC] or MCR[EER]).

Assumption: [SCG18.032]The application software shall run the flash memory AI at start-up to detect possible latent faults. [end]

NOTE

> See the “Array Integrity Self Check” section in the *MPC5777M Reference Manual* for details.

In the event of a user detected single-bit correction through user reads or an array integrity check, a margin read may be done to check for a possible second bit failing within the selected margin levels.

Assumption: [SCG18.151] A margin read test should be executed after a new single-bit error correction has occurred in flash memory. The margin read test does not need immediate execution, but it needs to be run within the next few trip cycles. Multiple single-bit errors can be the first indications of a data retention problem that could have the potential of causing multi-bit errors. [end] The MEMU can be used to store the address of the location reporting the error event.

NOTE

Implementation hint: Refer to the *MPC5777M Reference Manual's* "User margin read" section of the "Embedded Flash Memory (c55fmc)" chapter for details.

3.2.11 Voltage monitor configuration

To assist in maintaining functional safety, the Power Management Controller (PMC) monitors various supply voltages of the MPC5777M device. The "POR and voltage monitors description" table in the "Power management" chapter of the *MPC5777M Reference Manual* shows a detailed list of the LVDs and HVDs embedded in the MPC5777M.

Apart from the self-test, the use of the PMC for ASIL D applications is transparent to the user because the operation of the PMC is automatic (see SM_FMEDA_037 below, on page 21).

PMC failures primarily report to the MC_RGM. Since safety-relevant voltages have the potential to disable the failure indication mechanisms of the MPC5777M (the FCCU and its error out signals), their error indication directly causes a transition into a Safe state$_{\text{MCU}}$ by reset. Additionally, LVDs and HVDs also report errors to the FCCU, but under the recommended configuration (MCU reset by MC_RGM enabled) this is irrelevant.

Assumption: Software shall not disable the direct transition into a safe state due to an overvoltage or undervoltage indication.

The customer can, at their own risk, disable the direct triggering of resets by the MC_RGM and rely on the FCCU reactions to overvoltage and undervoltage, even when FCCU is configured for IRQs as the reaction. In general, the FCCU reaction (clocked by the IRCOSC) will take more time than the MC_RGM reaction (asynchronous). So, if the FCCU is to trigger an IRQ reaction, there is an increased probability that a fast voltage drop could cause a brownout condition on the device before a reaction occurs. If IRQs are selected as the FCCU reaction, there will be no guarantee that Diagnostic Coverage of overvoltage or undervoltage will be properly detected, and the safety analysis (FMEDA) of the MCU, will not be valid with respect to this failure mode.

To check the LVDs and HVDs for latent faults, which could impact their ability to correctly trigger when an undervoltage or overvoltage situation occurs, it is assumed there will be two software self-tests that will be executed by during startup.

Assumption: [SM_FMEDA_037]Reference voltages, and input voltages of LVDs/HVDs, shall be acquired using the ADC. The conversion values shall be compared with the expected ADC values. The application software shall initiate the hardware assisted self-test to detect LVD/HVD failures after start-up. [end]

NOTE

This is to check that the voltage supervised by the LVD/HVD is actually the correct one and not influenced by opens or shorts in such a way that it never could cross the LVD/HVD threshold. The LVDs/HVDs are monitored by SARADC_B input channels 96 to 101 and 112 to 119(see the *MPC5777M Reference Manual's* "Analog-to-Digital Converters (ADC) Configuration" chapter and the "SARADC_B analog test channel assignment" table for details).

Assumption: [SM_FMEDA_150] Software shall initiate a self-test of LVD/HVD comparator. [end]

NOTE

This is to check that a LVD/HVD will trigger at approximately correct value (see the *MPC5777M Reference Manual's* "Power Management Controller digital interface (PMC_dig)" chapter, section "Voltage Detect User Mode Test Register (VD_UTST)", and the "Device Configuration" chapter, "LVD / HVD self test" section, "LVD /HVD self test decoding" table).

To run the LVD/HVD self-test, application software shall execute the following steps:

1. Mask LVD/HVD by clearing the Reset Event Enable Register (PMC_REE_TD, PMC_REE_VDn registers) of the PMC (see the "Power Management Controller digital interface (PMC_dig)" chapter in the *MPC5777M Reference Manual*).
2. Clear LVD/HVD in Event Pending Register (PMC_REE_TD, PMC_REE_VDn).
3. Write the PMC_VD_UTST register to the desired LVD/HVD to test.
4. Enable VD_UTST bits in MCR (PMC_MCR) by setting USER_SELF_TEST_EN to start testing.
5. Verify test results by polling the Event Pending Registers (PMC_EPR_VDn or PMC_EPR_TD) flag:
   a) If the flag is set, the LVD (or HVD) test passed as expected.
   b) If the flag is not set, self-test failed.

NOTE

Software may configure a timeout period to be sure the flag asserts within a specified time (this time shall be greater than 20 µs).

6. Disable the VD_UTST bits in MCR (PMC_MCR) by clearing the USER_SELF_TEST_EN to end the test.
7. Clear PMC_VD_UTST.
8. Clear the LVD (or HVD) flag in the Event Pending Register (PMC_EPR_TD or PMC_EPR_VDn).
9. Wait for the PMC_GR_S bit to be de-asserted.

NOTE

Software may configure a timeout period to be sure the flag or flags clear within a specified time.

10. Enable the LVD (or HVD) by setting the appropriate field in the Reset Event Enable Register (PMC_REE_TD or PMC_REE_VDn).

These steps shall be repeated for each LVD (or HVD) to be tested. See the following sections of the *MPC5777M Reference Manual*:

- “Power Management Controller digital interface (PMC_dig)” chapter, “Voltage Detect User Mode Test Register (VD_UTST)” section
- “Device Configuration” chapter, “LVD / HVD self test” section

3.2.12 Temperature monitoring configuration

The MPC5777M supports a temperature sensor to detect over-temperature conditions. The temperature sensor can be configured to provide an analog measurement of the temperature using SARB input channel 120.

To set a proper threshold the customer must consider the maximum operating junction temperature (see the *MPC5777M Data Sheet* for the temperature sensor accuracy and maximum junction temperatures).

3.2.13 Clock monitoring configuration

Clocks are supervised by the Clock Monitoring Units (CMUs). The CMUs are driven by the 16 MHz internal reference clock oscillator (IRCOSC) to ensure independence from the monitored clocks. The CMUs flag errors associated with conditions due to clocks being out of programmable bounds, and loss of reference clock. If a supervised clock leaves the specified range for the device, an error signal is sent to the FCCU. MPC5777M includes the CMUs as shown in the “Clocking” chapter of the *MPC5777M Reference Manual*. It is the responsibility of the software to verify that the IRCOSC and XOSC are valid before starting the CMUs.

Assumption: [SM_FMEDA_040]The CMU frequency thresholds shall be configured for high and low limits which are used to compare with the MCU operating frequency. [end]

Assumption: [SCG18.035]The potential exactness (or the required inexactness) of the CMU thresholds shall be taken into account for both the IRCOSC and clock, or clocks, being monitored. [end]

NOTE

Implementation hint: For example, for the upper threshold customer should target CLKnominal_freq + CLKacc% and convert it into the number of IRC cycles in the worst case (slowest possible IRCOSC), for example IRC_freq = IRCnominal_freq – IRCacc%. The opposite applies to the lower threshold.

Assumption: [SM_FMEDA_041] For ASIL D applications, the use of the CMUs is mandatory. If the related modules are used by the application safety function, the user shall verify that the CMUs are not disabled and their faults are managed by the FCCU. The FCCU’s default configuration does not manage the CMU faults, so it shall be configured accordingly. [end]

Assumption: [SM_FMEDA_042]Application software shall check the configuration of the CMU once after programming. [end]

Assumption: [SM_FMEDA_043]Once after the boot the application shall measure the CLKMT0_RMN frequency (IRCOSC) with CLKMN0_RMT (XOSC) as reference clock exploiting the CMU frequency measurement feature. To detect failure of the IRCOSC, the application software shall utilize the CMU’s frequency meter to read the IRCOSC frequency and compare it against the expected value of 16 MHz[1][end]

Assumption: [SM_FMEDA_044]After start-up, the CMU reaction path shall be tested by modifying the CMU threshold. [end]

Assumption: [SM_FMEDA_045]To detect delays in clock mode switching and lost clock switching, the software shall ensure the CMU is reprogrammed with the new expected clock frequency minimum and maximum values within the FTTI. [end]

[1] Nominal frequency of the IRCOSC is 16 MHz, but a post trim accuracy over voltage and temperature must be taken into account (see the ‘Internal RC Oscillator electrical specifications’ in the *MPC5777M Data Sheet*).

NOTE

> The frequency range of the CMU must be increased before switching clock modes. The requirement is to program the CMU with the correct minimum and maximum values for the new frequency soon after the switch.

Recommendation: The application may run the IOSC_A001_SW (on page 24) once per FTTI to verify proper IRCOSC operation.

3.2.14 System clock availability

At start-up, the CMUs are not initialized and the IRCOSC is the default system clock. Stuck-at faults on the external oscillator (XOSC) are not detected by the CMUs at start-up since the monitoring units are not initialized and the MPC5777M is still running on the IRCOSC.

Assumption: [SM_FMEDA_047]The software shall verify that the clocks are valid by checking the state of the following:[end]

1. MC_ME_GS[S_XOSC] = 1, verifies valid XOSC
2. MC_ME_GS[S_IRC] = 1, verifies valid IRCOSC
3. The quality of the IRCOSC frequency is determined by clock metering and measuring the IRCOSC against the XOSC (see the *MPC5777M Reference Manual's* “Clock Monitoring Unit (CMU)” chapter for details)
4. Based on measurement from 3, software shall update the user trim bits of the internal oscillator (IRCOSC_CTL[USER_TRIM]).
5. Enable CMUs since we have valid XOSC and IRCOSC
6. MC_ME_GS[S_PLL0] = 1 and MC_ME_GS[S_PLL1] = 1, verifies valid PLL0 and PLL1 outputs

Assumption: [SM_FMEDA_048] Software shall check that the system clock is available, and sourced by the FMPLL (PLL1), before running any safety element function or setting the FCCU into the operational state. [end]

3.2.15 Clock Generation Module (MC_CGM)

The CMUs are the main mechanism used to check the integrity of MCU clocks, but other indirect measures like delayed lockstep, fault tolerant communication protocols and replicated usage of peripherals may also be used. The following assumptions are necessary to cover the clock failures that escape these safety mechanisms which can potentially lead to the failure of specific modules.

Assumption: [SM_FMEDA_049]The sample time for the SARADC will be at least one clock cycle longer than the minimum time required. This avoids clock glitches on the SAR clock from affecting sampling. [end]

Assumption: [SM_FMEDA_050]Detecting failures of either CLKOUT0 or CLKOUT1 is the sole responsibility of user application software. [end]

Assumption: [SM_FMEDA_051]To detect PSI5 reception failures due to a clock glitch, PSI5 will use the three bit CRC included in the protocol. [end]

3.2.16 PLL generated clocking

MPC5777M provides dual PLLs (PLL0 and PLL1) for separate system and peripheral clocks. [SCG18.145]Each PLL provides a glitch-free and fast clock to the MPC5777M and provides a loss of lock signal that is routed to the FCCU. [end]

To reduce the impact of glitches stemming from the XOSC, the FMPLL (PLL1) should be used as the system clock.

Assumption: [SM_FMEDA_052] Application software shall ensure that the system is using the FMPLL (PLL1) clock as the system clock before running any safety functions, or before the FCCU indicates a system that is functioning correctly (for example, on FI[*n*]). [end]

Assumption: [SM_FMEDA_053] Application shall configure the FCCU to react to both PLL loss of locks. [end]

Both FlexRay and CAN feature modes in which they are directly clocked from the XOSC. For applications targeting ASIL D, using these clocking modes increases the risk of a communication failures.

Assumption: [SM_FMEDA_054] Application software will not use FlexRay or CAN modules directly clocked by the XOSC, or the used fault-tolerant communication layer will be capable of handling failures induced by clock glitches (for example, timing errors, sampling errors and complete failure of logic due to setup/hold time violations). [end]

3.2.17 XBAR configuration

The multi-port XBAR switch allows for concurrent transactions from any master (cores, DMA, FlexRay) to any slave (memories, peripheral bridge). The XBAR module includes a set of configuration registers for arbitration parameters, including priority, parking and arbitration algorithm. Faults in the configuration registers affect slave arbitration so software countermeasures must detect these faults.

Assumption: [SCG18.042]Masters of the XBAR which are not ViMos or SuMos shall have a lower arbitration priority on the XBAR than safety-relevant masters. [end]

Assumption: [SM_FMEDA_055] In cases where it is not possible to set the XBAR arbitration appropriately, a failure probability shall be estimated for such cases. An example case is when FlexRay, which is a PeMo, needs highest priority. [end]

Assumption: [SM_FMEDA_056] To prevent spurious XBAR accesses by the HSM to stall or delay the safety function, the XBAR will be configured assigning low priority to the HSM. [end]

XBAR data and address lines are covered by E2E ECC. Some failures, particularly those affecting muxing logic, might introduce multi-bit errors on data and addresses. Though ECC coverage is limited on a single transaction the probability of detecting the fault is higher when multiple transactions are affected.

3.2.18 Platform flash memory controller

PFLASH controller configuration controls aspects related to flash memory remapping. It can remap logical flash accesses to on-chip calibration RAM, extended off-chip calibration RAM or on-chip system RAM.

Assumption: [SM_FMEDA_059]To avoid incorrect remapping due to non-initialized remap descriptors, unused PFLASH remap descriptors shall be initialized to an unused logical address[end].

NOTE

> Remapped PFLASH regions are initialized by configuring PFLASHC_PFCRDE and PFLASHC_PFCRD*n* registers.

If flash memory remapping is used during safety-relevant application execution, safe calibration needs to be enabled via PFCRCR[SAFE_CAL]. After reset, calibration overlay regions are considered to be safety-relevant (PFCRCR[SAFE_CAL] = 0, see section “e2eECC and Calibration Accesses” of chapter “e2eECC and Calibration Accesses” in the *MPC5777M Reference Manual* for details).

3.2.19 Wake-Up Unit (WKPU) / External NMI

Assumption: [SM_FMEDA_167] NMI will only be used for error notifications or other uses where all dangerous failures are latent failures.

Assumption: [SM_FMEDA_168] Application shall check the WKPU configuration and its functionality at once after the boot. [end]

NOTE

> The configuration can be verified by reading the configuration registers and comparing them with the expected values.
>
> Functionality can be tested by triggering the external NMI and check for the expected reaction. Reset request to the MC_RGM can be reconfigured to generate a SAFE mode or interrupt request.

3.2.20 Cache

Assumption: [SM_FMEDA_130] ECC/EDC protection of caches is assumed to be enabled (setting of the Data Cache Error Checking Enable field in the L1 Cache Control and Status Register 0, L1CSR0[DCECE] = 1). It is also assumed that ECC/EDC errors are handled by correction and invalidation.

Handling ECC/EDC errors by a machine check is also possible if the machine check handler initiates appropriate SW countermeasures (to achieve the former, L1CSR0[DCEA] = 01b). The handling of the errors is assumed to occur as soon as the caches are enabled (see “Core Complex Overview” and “e200z425Bn3 Core Description” chapters in the *MPC5777M Reference Manual*). [end]

3.2.21 Software Watchdog Timer (SWT)

Assumption: [SM_FMEDA_104] These requirements apply to the SWT for ASIL D applications: [end]

- The SWT shall be enabled and configuration registers have to be protected against undesired accesses using one or more hardware mechanism implemented (for example, SMPU, REG_PROT).

- The SWT time window settings shall be set to a value less than the FTTI. Detection latency shall be smaller than the FTTI.
- Before the safety function is executed, the software shall verify that the SWT is enabled by reading the SWT control register (SWT_CR).

3.2.22 Analog to Digital Converters

MPC5777M includes both SD and SAR ADCs. One of the SAR ADCs is considered the supervisor, or monitor, ADC (for example, SAR ADCB). The others ADCs have normal functionality.

The basic idea to verify the integrity of the functional ADCs is to implement software redundancy. This redundancy is supported by hardware allowing acquisition of analog inputs using independent ADC modules[1].

Figure 1 shows the block scheme of connection of the SAR ADCs, including the supervisor. Through a second level of multiplexing, all analog inputs connected to the functional ADCs (both SD and SAR), are connected to the supervisor ADC.

[1] Simultaneous sampling of two ADCs on the same analog input is not allowed (see the *MPC5777M Reference Manual* for details).

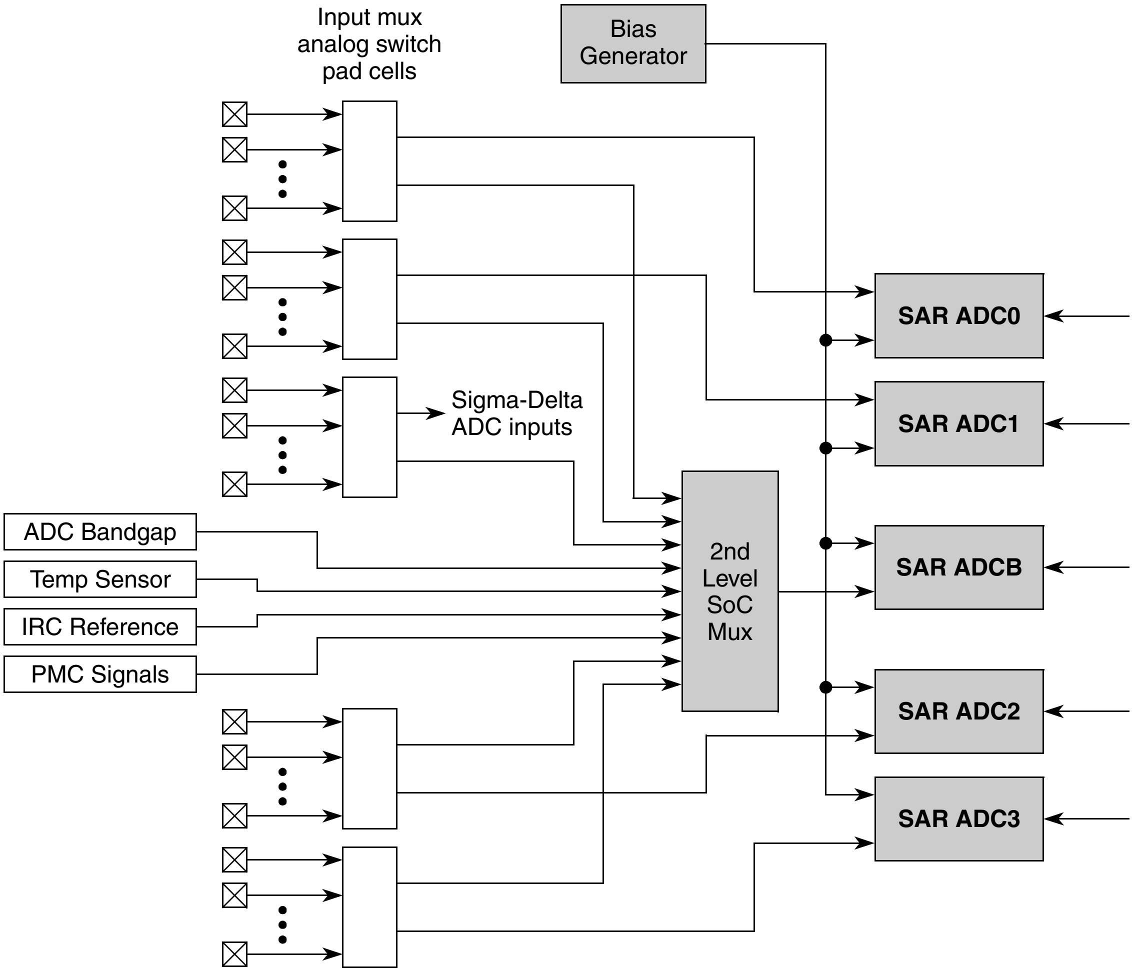

Figure 1. Block scheme of the SAR ADCs, including the supervisor ADC

The supervisor ADC can be a source of latent failures. To detect these latent failures, before it can be used to verify the behavior of functional ADCs, a test shall be executed once after the boot.

Assumption: [SM_FMEDA_153]To detect latent failures, the supervisor ADC shall acquire some known internal analog voltages and compare them with the expected values before the supervisor ADC can be used for monitoring the functional ADCs. [end]

Values which must be acquired are:

- [SM_FMEDA_154]Bandgap ADC measurement. [end]
- Internal analog voltages listed in section “Internal reference” of the “Analog-to-Digital Converters (ADC) Configuration” chapter of the *MPC5777M Reference Manual*.

A similar procedure shall be applied on the functional ADCs that will be used for acquiring safety relevant data as described hereafter.

Assumption: [SM_FMEDA_155] Before the safety application starts, functional ADCs shall run a conversion cycle of known signals together with the supervisor ADC. The acquired values shall be compared by software. [end]

NOTE

During the self-test conversion cycle, the configuration of both functional and monitor (supervisor) ADCs shall be the same. After the self-test and during normal acquisitions, the configurations may be modified.

3.2.23 Temperature sensor (TSENS)

The MPC5777M includes a temperature sensor that monitors device temperature. The temperature sensor only has an analog output that can be used.

Assumption: [SM_FMEDA_156]Before the safety application starts, software shall configure the ADC measurement of the analog output of the temperature sensor to trigger an event if the temperature is outside of the permitted range. [end]

3.3 Runtime checks

During the execution of the safety function, application software is assumed to perform a set of tasks to support the detection of random hardware failures and transition the device to a Safe state$_{\text{MCU}}$ in case of a failure. This section collects the assumptions software has to fulfill during runtime.

3.3.1 General requirements

The safety concept does not protect against spurious subtle timing changes (for example, due to the XBAR not parking on the safety relevant master due to other accesses). Thus, such subtle timing must not be relied on.

Assumption: [SCG18.079]During the development of safety-relevant software, counting clock cycles will not be used (for example, relying on the execution time of core assembler instructions to measure time). [end]

Assumption: [SCG18.080]If independent data paths to or from any ViMos classified module exists, software shall use them redundantly to read or write safety related data. [end]

An independent data path exists to access the two PBRIDGEs and application software should use the peripheral set redundantly. In this case, failures in one of the data paths will be detected by application level checks (for example, by comparing data provided by two redundantly used peripherals when each is attached to a different PBRIDGE).

NOTE

The “Periphery allocation” figure in the *MPC5777M Reference Manual* shows the peripheral split between the two peripheral bridges (PBRIDGEA, PBRIDGEB). Section 3.3.17, I/O and Peripheral Bridge gives additional detail about using safety relevant I/Os.

Assumption: [SCG18.081]A safety mechanism will be implemented at application level to detect critical timing failures leading to violation of application timeouts. [end]

NOTE

> **Implementation Hint**: The SWT module can be used to satisfy the above requirement.

Machine check exceptions of the Safety Core are directly forwarded to the FCCU's "Safety Core Exception" input.

Recommendation: Due to the more comprehensive information available in the exception handler it is recommended to handle machine check exceptions in the exception handler and not use the FCCU mechanism.

Assumption: [SM_FMEDA_061]Other exceptions, which are not directly forwarded to the FCCU (for example, Data Storage, Alignment), must be handled by the core itself. [end] This assumption shall be considered only for exception considered safety relevant by the application.

NOTE

> *MPC5777M Reference Manual's* "Core e200z425n3Description" and "Core e200z420n3 Description" chapters and the "Exceptions" sections of each chapter for details on core exceptions.

3.3.2 CRC of configuration registers

The CRC unit offloads the core in computing a CRC checksum. There are three sets of CRC registers to allow concurrent CRC computations in the MPC5777M device. The CRC unit should be used to detect accidental modifications of data in configuration registers by calculating its CRC signature and comparing it against a pre-calculated CRC.

NOTE

> Some configuration registers, as those for clock and MCU mode configuration, are copied to the corresponding internal registers only when an event (for example, mode change) is triggered. The values of those configuration registers themselves have no effect. Additional measures are needed, along with CRCing, to ensure correct operation of the MCU.

Assumption: [SM_FMEDA_062]A periodic scan of the safety relevant configuration registers, which are not covered by other safety mechanisms, shall be executed once per FTTI to ensure that the configuration has not changed due to a bit flip. [end]

NOTE

> **Implementation hint:** The CRC checksum of the configuration registers of the modules involved with the safety function should be calculated offline.
>
> At run time, the same CRC value must be calculated by the CRC module within the FTTI. To avoid overloading a core, the DMA module can be used to support the data transfer from the registers under check to the CRC module.

The result of the runtime computation is then compared to the offline one.

CMU registers are sources of latent failures which cannot lead directly to the violation of the safety goal. The assumption below shall be considered.

Assumption: [SCG18.099]To reduce number of possible CCFs, the configuration registers of the CMU_1, used to monitor the clock source of the Safety Core, shall be included into the periodic register CRCing scheme. [end]

Assumption: [SCG18.040]The two CRC units are not specifically designed to be used redundantly (for example, to check each other). In fact, there is no dependency constraint imposed on the design. [end]

3.3.3 XBAR usage

The application software must check the XBAR configuration once after programming but it must also detect failures of the XBAR when safety-relevant functions are running.

Assumption: [SCG18.055] Application software shall check the configuration of XBAR every FTTI to detect failures affecting the register interface. [end]

Assumption: [SCG18.056]Within the FTTI, application software will detect failures of the XBAR configuration affecting system performance. [end]

The detection of failures of the XBAR configuration can be achieved as a combination of periodic read-back of the configuration registers and control flow monitoring using the SWT. The SWT is needed to cover those failure conditions leading to a complete lock-out of XBAR masters. The need for periodic configuration read-back depends on how stringent the control flow monitoring is implemented.

XBAR data and address lines are covered by E2E ECC. Some failures, particularly those affecting muxing logic, might introduce multi-bit errors on data and addresses. Though ECC coverage is limited on a single transaction the probability of detecting the fault is higher when multiple transactions are affected.

Assumption: [SM_FMEDA_063]Safety analysis assumes that at least two transactions are affected (for example, at least two accesses are made by or to the safety relevant XBAR master(s) or slave(s) within each FTTI). [end]

3.3.4 System Memory Protection Unit (SMPU)

The SMPU provides memory protection at the XBAR. A failure in the SMPU can change the behavior of the SMPU (for example, enabling or disabling the protection), resulting in unauthorized access to the protected data, or leading to unexpected access violations and data storage exceptions.

The protection against such failures is given by the read-back of the configuration registers, together with the exception handler and the SWT if the exception handler cannot execute. SWT and exception handlers are assumed to cover cases when accesses to system resources are unexpectedly prevented to authorized masters. On the other hand, SMPU failures resulting in missing memory protection are considered critical only if coupled with other failures causing the undesired access to protected data (notice that systematic failures, besides random HW failures, can lead to this scenario).

Assumption: [SM_FMEDA_064]Application SW checks the configuration of the SMPU every FTTI. In particular, it has to check the cacheability attribute of each region descriptor as transactions erroneously marked as cacheable may cause shared data to be cached, potentially leading to stale data in the cache. [end]

Safety analyses are performed under the following assumptions:

- **Assumption:** [SM_FMEDA_065]FMEDA assumes that 90% of region descriptors are usually used during the execution of safety tasks. [end]
- **Assumption:** [SM_FMEDA_066]SMPU is enabled approximately 99% of the time during the execution of safety tasks. [end]

3.3.5 Platform flash memory controller

The PFLASH controller configuration controls aspects of read wait states, port arbitration, prefetching policy, master access and flash memory remapping.

Some of these failures only cause performance reductions, so they can be covered by the SWT.

Assumption: [SM_FMEDA_067]Safety analysis assumes that at least four reads through the PFLASH controller are executed within the FTTI. [end]

Other configuration failures, such as master access and safe remapping, only cause MultiPoint Failures (MPF), so one time readback is sufficient.

Assumption: [SM_FMEDA_068]After configuring the PFLASH controller, the application shall read back the PFLASH controller registers and compare them with the expected values every FTTI. [end]

3.3.6 Flash memory

3.3.6.1 Overlay operations

Overlay SRAM is included in the MPC5777M family of devices as part of a comprehensive set of calibration and debug features. It is recommended that overlay SRAM be used only for these tasks and not for wide scale general functionality in production since the safety mechanisms have only limited CCF protection.

Assumption: [SM_FMEDA_069]Overlay RAM is used to remap data only. No instruction fetch remapping occurs during normal operation, but this can be done during debug mode. [end]

Writes to incorrect addresses are covered by reading back the data that was written. Reads from an incorrect source have different effects according to the selected source versus the targeted one:

- Overlay RAM, instead of flash memory, read errors can be detected by E2E ECC as the overlay read data buffer contains data fetched from a different address (with its specific addr/data ECC).
- Prefetch buffers, instead of overlay RAM, read errors can be detected by E2E ECC as the word has been prefetched from a different address.

- Flash memory, instead of overlay RAM, read errors are not detected by E2E ECC as the access is done with the correct (logical) address but can be detected by writing and reading back a few patterns from the overlay RAM.

Assumption: [SM_FMEDA_070]Software shall run write and read-back patterns from overlay RAM to check integrity of overlay read/write/selection path, and this test shall be executed every FTTI. [end]

When overlay, or flash memory, regions are programmed, data in the minicache can be stale (a missed hit during write operations could lead to erroneously valid prefetched data). Reading back the data after each programming operation ensures that prefetched data are invalidated.

Assumption: [SCG18.050]After write operations to overlay RAM, or flash, software shall read back the data that was written and compare it with the expected data to check the integrity of the programmed data. [end]

NOTE

These countermeasures apply only if the overlay RAM is used by the safety function.

When software reads data that was programmed in the flash memory, or written to overlay RAM (to verify contents), the minicache will be automatically refreshed.

Assumption: [SM_FMEDA_071]Overlay RAM is used only for a fraction of the time on a small number of devices (assumed 5%, averaged considering all MCUs). [end]

3.3.6.2 Flash memory program and erase

Flash memory program/erase operations are stopped in the event of a fault event (for example, no flash sector selected, or elevated current draw).

Assumption: [SM_FMEDA_072]For program operations, only the address specified by an interlock write determines the partition being written. An interlock sequence is used to prevent accidental programming of flash memory. [end]

Assumption: [SCG18.058]A software safety mechanism shall be implemented to ensure the correct termination of any program/write operation of the flash memory. [end]

Even when flash memory signals the correct termination of programming operations, there is still the chance that flash memory content is incorrect due to failures of the flash memory write path and programming logic.

Assumption: [SCG18.061]To ensure that the content of a write operation to flash memory is correct, software shall read back the data that was written and compare it with the expected data. This checks the integrity of the programmed data. This test should execute after every program or erase operation. [end]

NOTE

In addition, this test prevents the return of stale data from the PFLASH controller minicache.

3.3.6.3 Flash memory multibit error

Nonvolatile flash memory is protected with a single-bit correction/double-bit error detection (SEC/DED) ECC scheme.

Multibit errors can be caused by failures affecting common pieces of the flash memory (for example, sensing amplifier, read logic). These type of failures lead to random data reads (for example, white noise on read word). Reading random data is detected as single-bit correction (SBC) and corrected by the ECC logic[1]. A software mechanism is needed to distinguish between a real SBC and a MBE.

This test consists of executing multiple reads to be run if an SBC event occurs (for example, 4 reads is sufficient). If the multiple reads trigger additional correctable/noncorrectable errors, the flash memory contains permanent multibit errors.

Assumption: [SM_FMEDA_073]If an ECC correction occurs, the application shall force the read of a number of patterns sufficient to trigger other ECC error corrections/detections revealing the actual nature of the fault (in fact, permanent flash memory control failures typically affects multiple read operations). [end]

NOTE

> The piece of the flash memory which can cause multibit errors are shared by the Read-While-Write (RWW) partitions of each flash memory. The multiple read shall be executed out of the affected RWW flash partition (list of flash memory RWW partitions are shown in the “Memory Map” chapter’s “Flash memory and overlay RAM map” table of the *MPC5777M Reference Manual’s*).
>
> [SCG18.134] Reading 4 patterns is sufficient to reach a DC of about 99% of coverage. [end]

3.3.6.4 EEPROM emulation

The MPC5777M provides eight blocks (8 × 64 KB) of the flash memory for EEPROM emulation. ECC events detected on accesses to the EEPROM flash memory blocks are not reported to the MEMU. Single-bit corrections (SBCs) are performed, but not signaled to the MEMU. MBEs are replaced by a fixed word (for example, an illegal instruction) and are also not forwarded to the MEMU.

Assumption: [SCG18.063]Software using EEPROM for storage of information will use its own information redundancy (for example, CRCs) to detect incorrect data returned from the EEPROM emulation. [end]

3.3.7 PRAMC configuration

PRAMC provides a certain level of configurability on accessing the RAM. Faults in the PRAMC configuration registers may change PRAMC port priority and, most important, read wait states. Changes in port priorities, or more wait states, can have an impact on the overall performance, which is typically

[1] With a DC of about 70%.

covered by using the SWT. However, fewer wait states can lead to multi-bit errors that are detected by E2E ECC with only low to medium effectiveness.

Assumption: [SM_FMEDA_074]Application software shall check the configuration of the PRAMC every FTTI. [end]

The periodic check of PRAMC configuration can be avoided if the following assumption is satisfied:

- **Assumption:** [SM_FMEDA_075]Application software performs at least two accesses to the SRAM within the FTTI, or a simple test could be performed (for example, a test based on write and read-back performed every FTTI). [end]

3.3.8 RAM

RAM is protected from failures by ECC logic with various implementations discussed in the following sections. To increase the coverage against MBE certain SW measures have been assumed.

3.3.8.1 Error Correcting Code (ECC)

Some failure modes of the RAM, for example failures affecting common part of the RAM structure, cause data to be read from all location as All-0 or All-1[1].

In such a case if a data is read out of the RAM, an event should be detected by the ECC which perceives All-X code-word as invalid code. But in the MPC5777M there are some RAMs whose address is included in the ECC checksum calculation to increase the diagnostic coverage in case of addressing failures.

List of memories where ECC bits are computed including address contribution can be found in the Reference Manual (please see the *MPC5777M Reference Manual's* “ECC RAM implementation” table in the “Functional Safety” chapter).

Due to this hardware architecture there are address locations out of which reading All-X word is valid and no ECC event is triggered[2]. Approximately there is one of these addresses out of 256 ones.

Assumption: [SCG18.122] There is no special handling of All-X words for ECC that includes addresses in the ECC code-bit calculation. They can be valid, correctable or uncorrectable words depending on the address. [end]

Consider a permanent All-X failure mode:

- If there is a transaction to a “normal address”, this failure mode is detected by the ECC which perceives the All-X code-word as invalid (either single bit error or correction is triggered).
- If there is a transaction to an “All-X address”, this failures mode is not detected by the ECC or other means (All-X code-word is valid for “All-X address”).

The permanent All-X failure mode is not detected by the ECC if an application reads only All-X addresses of the RAM. This is a pure theoretical case because a real application doesn't read only such All-X addresses, but reads different parts of the RAM including (and mainly) normal addresses.

[1] All-0 and All-1 will be referenced generically as All-X.

[2] For the sake of simplicity, let us call “All-X addresses” the ones which perceive All-X as valid and “Normal addresses” the remaining ones.

[SCG18.140]Within the FTTI, application software shall read in each RAM block two addresses that are known to cause an uncorrectable error in case the memory globally shows an All-0 or an All-1 state. [end]

NOTE

> Real application continuously reads several RAM locations (both normal and All-X addresses) in different RAM blocks. Some of these transactions are directed to addresses which trigger uncorrectable error in case of All-X events.
>
> As result in most of cases the assumption above is satisfied by the application accessing RAM during the normal code execution without any additional overhead in terms of both coding and timing.

The program in Section 6, Testing All-X in RAM, calculates the list of addresses, which trigger uncorrectable errors if an All-0 (or an All-1) failure occurs, by a linear search from a start address. These locations shall be used to verify the presence of a global All-0 (or All-1) error.

The user can verify that the application software reads, once per FTTI, at least one location to detect a global All-0 errors and one location to detect for All-1. In that case additional readings of previous assumption are not necessary.

Assumption: [FMEDA_SM_169] SW shall ensure that data in Standby RAM is additionally protected (for example, with an application-level checksum) against effects occurring during standby, especially the aggregation of several Single Bit Upsets (SBUs) and the possibility of power failures. [end]

3.3.8.2 Repair logic

Memory repair faults can cause a partial shift of the word. This failure mode can affect one word or an entire column depending on the type of failure in the repaired column (single bit in array or column periphery). If a read operation is performed first, this will result in a MBE (white noise model). In the event a write operation to a specific address was executed first after this error resulted, any subsequent read of that same address will be either correct or result in a SBE.

Assumption: [SCG18.350]To guarantee coverage for MBEs it is assumed at least four reads on different addresses per RAM block and FTTI will occur. This provides sufficient Diagnostic Coverage for column repair with ECC. [end]

3.3.8.3 Error reporting

The MEMU collects and reports error events associated with ECC logic used on system RAM, peripheral RAM and flash memory. The MEMU stores the addresses where ECC errors occurred. The MEMU also reports whether the error is correctable vs. uncorrectable. Uncorrectable errors will cause a report to the FCCU.

Correctable errors include:

- Single-bit error in the data part that is detected via ECC for a system RAM, peripheral RAM or flash memory
- Single-bit error in the data part that is detected via MBIST on any RAM

Uncorrectable errors include:

- Multi-bit error that is detected via ECC for a system RAM, peripheral RAM or flash memory
- Multi-bit error that is detected via MBIST on any SRAM
- Addressing errors and unused data bit errors detected by ECC logic

Failures in RAM logic (for example, decoding, control, and so on) might lead to MBEs (white noise model). Faults can have two kinds of effects:

- Always result in a random data pattern when the content of the faulty address is read (for example, no word lines selection, clocking failure)
- Cause MBEs only on transactions targeting a subset of RAM addresses (for example, multiple word lines selection)

In both cases above, ECC logic can lead to a wrong correction. It is necessary to implement a software test to detect permanent MBE sources leading to erroneous ECC corrections, so the overall coverage (ECC + software test) is the same as that provided by a 64 / 8 EDC scheme (for example (1 - 1 / 256 × 100.0%) = 99.6%).

Assumption: [SCG18.066]In the first case (on page 38) a software test shall be implemented to detect permanent MBE sources. It will fetch the error address of corrected errors from the MEMU and assess the nature of the fault by writing and reading back a few patterns (for example, two's-complemented patterns) to the faulty location. The software test shall be executed within the FTTI after a new ECC error correction in RAM is reported. [end]

Assumption: [SM_FMEDA_077]For the second case (on page 38) a software test shall be implemented to detect permanent MBE sources caused by multiple address selections. It will fetch the error address of corrected errors from the MEMU and assess the nature of the fault by writing and reading back a (small) set of patterns to multiple locations depending on the faulty address. [end]

NOTE

This test is described in Section 5, Address decoding coverage.

Assumption: [SCG18.068]These software tests will be executed within the FTTI after a new ECC error correction in RAM is reported. [end]

Assumption: [SCG18.950] During operation, if the MEMU contains two entries for the same address of an address which is part of a memory for which ECC syndromes are reported, SW will check whether one of the two syndromes is FFh. If so, this entry should be deleted. This entry came from another ECC unit which does not report syndromes. As long as the entry with the correct syndrome is stored in the MEMU, entries for the same address without syndrome will not be stored. [end]

3.3.9 ECC Bypass using core registers and Indirect Memory Access (IMA)

During test, or development, the need for direct access to all RAM bits that is not filtered through the ECC logic may arise. Memory locations can be accessed directly either via processor core access or the IMA module (see the *MPC5777M Reference Manual's* “Indirect Memory Access (IMA)” chapter).

This mechanism provides access to all bits in the RAM arrays, therefore allows reading and manipulating of ECC check bits. In general, the core mechanism needs to be used for core accessible RAM, whereas the IMA module is responsible for granting direct access to other RAMs (typical peripheral).

Accesses via the IMA module are not controlled by the MPU, but the MPU controls access to this module. Direct accesses using the core mechanism are normally controlled by the MPU.

Assumption: [SCG18.064]Software shall ensure that no other RAM access occurs to a certain array while the IMA module is used to access the contained RAM cells directly. [end]

Assumption: [SCG18.065]Software shall check that ECC bypassing mechanisms are executed only when the ECC manipulation is really expected and not due to some software control flow problem. [end]

3.3.10 Decorated Storage Memory Controller (DSMC)

DSMC gives the hardware support to have atomic read-modify-write memory operations in the MPC5777M microcontroller. These capabilities are called decorated storage.

FMEDA assumes some limitations on the usage of the DSMC.

Assumption: [SM_FMEDA_079]Safety analysis assumes the following usage of the DSMC:

1. Safety Application (running on Safety core) can access the DSMC_SysRam and DSMC_SafetyCore for both read and write operations.
2. Safety Application (running on Safety core) can only write to Non ViMos DSMCs. It should not read decorated data unless application level safety measures are put in place to ensure accuracy of read data at the destination (point of usage).
3. NoSaMos Cores should not write to DSMC_SafetyCore and DSMC_SysRAM. They are allowed to read. The read/write restriction should be managed inside the SMPU. [end]

3.3.11 Interrupt management

No specific hardware protection is provided against spurious or missing interrupt requests (for example, caused by EMI on the interrupt lines or bit flips in the interrupt registers of the peripherals). The Interrupt Controller (INTC) can drop, delay or create interrupts.

[SCG18.951]To detect these unwanted events different software measure need to be considered: [end]

- **Assumption:** [SM_FMEDA_080]Periodically check for effects of lost interrupts (for example, buffer overflow or underflow). [end]
- **Assumption:** [SM_FMEDA_081]Periodically check that interrupt flags in peripherals are cleared. [end]
  - This works specifically well if done outside an IRQ routine or with very low IRQ priority. If a flag for an interrupt (with higher priority) is set, this is an error. No IRQs shall be blocked while this test is executed.
- **Assumption:** [SM_FMEDA_083]The ISR will check that the triggering module actually shows a requested interrupt (for example, reading the interrupt request or status register in the peripheral). [end]

- **Assumption:** [SM_FMEDA_084]The ISR shall check that it was called with the correct priority. [end]
- **Assumption:** [SM_FMEDA_085]Interrupts where a short latency is safety-relevant are assigned to two (or more) cores and one of those cores checks (for example, using a shared variable) that the other core actually executes the ISR within the expected latency after the IRQ occurred. [end]
- **Assumption:** [SM_FMEDA_086]The ISR checks that it is executed on the expected core using the relevant core register. [end]

NOTE

The application software can determine the core that is presently running software by reading the Processor ID Register (PIR) (see *e200z7xx Core Reference Manual* for details).

- **Assumption:** [SM_FMEDA_087]Unused interrupt vectors shall point, or jump, to an address which is illegal to execute, contains an illegal instruction, or in some other way causes detection of their execution. [end]

NOTE

Example implementations of this software and further information on it can be found in Application Note AN4527 “Software Routines for Functional Safety Usage of the Qorivva Interrupt Controllers”.

3.3.12 eDMA usage

The DMA provides the capability to perform data transfers with minimal intervention from the core. It supports programmable source and destination addresses and transfer size.

Since DMA is NoSaMo, no safety measure has been implemented in HW. It is the task of the application software to provide any necessary safety measures due to safety-relevant usage of the eDMA.

3.3.13 Reset Generation Module (MC_RGM)

MC_RGM can trigger interrupts or request a transition to SAFE mode, if the MC_RGM is configured to do so.

Assumption: [SM_FMEDA_089]To detect spurious interrupts or transition requests to SAFE mode, the interrupt handler, for IRQs coming from the MC_RGM, will check that the shown source is one which was configured to cause such a request from the MC_RGM (for example, compare the MC_RGM_FES register to the expected MC_RGM_FERD and MC_RGM_FEAR register contents). [end]

NOTE

If the MC_RGM triggers a transition request to SAFE mode, no interrupt is triggered by the MC_RGM. An interrupt will be triggered by the MC_ME.

3.3.14 Detection of unwanted resets

MC_RGM allows triggering individual resets for MCU modules (for example, using the Peripheral Reset Registers (RGM_PRST[*n*]). This can be prohibited by using the access control mechanisms of the MPC5777M such as the MPU or PAC. In case those are not used, and also to detect spurious resets caused by SEE, the following describes how such spurious resets can be detected.

Assumption: [SCG18.150]To detect unwanted reset of these modules, software and hardware counter measures can be applied. Table 1 summarizes these counter measures. [end]

This is a brief description of each of the column headings in Table 1:

- Receiving module – This module is reset.
- Software Control – The register (or registers) which can reset the specified “Receiving Module”.
- Detection – The effect of the unwanted reset of the specified “Receiving Module” and shows some mechanisms that can detect the module where the event occurred. If multiple mechanisms are listed, the software can choose the mechanism that better fits its need (unless explicitly specified).
- Software action required – Additional software mechanism, with respect to the application software, required to detect an unwanted reset of the specified “Receiving Module” (for example, polling coming from configuration registers).

Table 1. Effects of reset

Receiving module	Software control	Detection	Software action required?
Peripheral core_2	ME_CCTL[0]	non safety related	NO
Main core_0 (Safety Core)	ME_CCTL[1]	RCCU	NO
Main core_0s (Checker Core)	ME_CCTL[2]	RCCU	NO
Main core_1 (Computational Core)	ME_CCTL[3]	non safety related	NO
HSM	ME_CCTL[4]	non safety related	NO
dspi_0	RGM_PRST[99]	DSPI module is enabled after reset (MDISrst=0) but is kept in HALT state (HALTrst=1, stop transfers). Cfg after reset is a valid one. DSPI Transfer Count Register (DSPIx_TCR) is reset to zero.	NO, after reset no message will be sent/received
dspi_1	RGM_PRST[98]		
dspi_2	RGM_PRST[227]		
dspi_3	RGM_PRST[226]		
dspi_4	RGM_PRST[97]		
dspi_5	RGM_PRST[225]		
dspi_6	RGM_PRST[96]		
dspi_12	RGM_PRST[93]		
iic_0	RGM_PRST[101]	module disable MDISrst=1. When high, the interface is held in reset, but registers can still be accessed. IIC is kept under reset and no message will be sent/received	NO, after reset no message will be sent/received
iic_1	RGM_PRST[229]		
pit_rti_0	RGM_PRST[30]	module disable MDISrst=1. No clock for PIT timers hence no interrupt nor DMA transfer request is generated. Detection depends on how the module is used by application software	YES, application dependent
pit_rti_1	RGM_PRST[31]		
linflex_0	RGM_PRST[92]	no enable bit and after reset the LIN controller is in NORMAL state (not INIT: To enter this mode software sets the INIT bit in the LINCR1. To exit the initialization mode software should reset the INIT bit. When in initialization mode, all message transfers to and from the LIN bus are stopped and the status of LIN bus output LINTX is recessive). However, LIN baud rate after reset is set to zero (LINIBRRrst=0, LIN clock disabled) and is simple to check.	NO, after reset no message will be sent/received
linflex_1	RGM_PRST[91]		
linflex_2	RGM_PRST[220]		
linflex_14	RGM_PRST[85]		
linflex_15	RGM_PRST[213]		
linflex_16	RGM_PRST[84]		

Table 1. Effects of reset (continued)

Receiving module	Software control	Detection	Software action required?
psi5_0	RGM_PRST[111]	Disable mode is the default state after module reset is released (GCR[GLOBAL_DISABLE_REQ]rst = 1). Also, any channel is individually disabled (PSI5_CH_Enrst=0). In this mode the RX, TX, common time base counters are disabled for any operation	NO, after reset RX,TX, common time base are disabled
psi5_1	RGM_PRST[239]		
psi5_s	RGM_PRST[162]		
sent_0	RGM_PRST[104]	After reset, the SENT module comes up in the disabled state. All channel enable bits (EN_CHxrst=0) and the global enable bit (SENT_ENrst=0) are set to 0 and the user software must program the SENT module parameters correctly before enabling it	NO, no transmission after the unwanted reset
sent_1	RGM_PRST[232]		
dma_ch_mux	RGM_PRST[36]	After reset all DMA channels are in Disabled Mode and no DMA transfer is performed. SW might need to check periodically this bit as no transfer can result in stale data (depends on the usage of DMA at application level).	YES, application dependent
flexray_0	RGM_PRST[107]	module enable MENrst=0; the application requests the CC to leave the Disabled Mode by writing 1 to this bit Before leaving the Disabled Mode, the application must configure the SCM, SBFF, CHB, CHA, TMODE, BITRATE values; once enabled the module cannot be disabled by SW (i.e. write 0 not allowed)	NO, after reset no communication is performed on the bus
flexray_1	RGM_PRST[235]		
sipi_0	RGM_PRST[11]	SIPIMCR[MOEN] = 0 after reset. After reset SIPI is in disable mode and all activities on SIPI Tx and Rx ports are immediately stopped	NO, after reset all activity on SIPI ports are stopped

Table 1. Effects of reset (continued)

Receiving module	Software control	Detection	Software action required?
gtm	RGM_PRST[128]	This is the AEI (CPU interface hardware) reset. After the reset the MDIS bit becomes active removing the clocks from GTM (MDISrst=1). All outputs will stop at the present value when the clock is just removed. All GTM internal modules are halted and keep their state, including the RAM modules. Automatic detection depends on how module is used. In any case, the detection can be implemented by polling the MDIS bit. A software reset is needed in the AEI interface in order to put AEI interface in a known state. Further re-initialization through software is required in order to resume operation. Commands in the "command buffer" will be lost thus the integrity of the GTM module regarding registers/memory controlled by CPU is compromised. Software action is required: AEI software reset bit should be used. It is highly recommended to re-initialize the whole GTM module before resume operation.	YES, application dependent
adcsar_dig_b	RGM_PRST[112]	module power-down PWDNrst=1 and ADC status ADCSTATUSrst=001=power-down. ADCSAR is in power-down mode after reset and no conversion can be started (hence no end-of-conversion will be generated, not clear if an error is flagged when trying to start conversion)	NO, after reset no ADCSAR conversion can be started
adcsar_dig_0	RGM_PRST[127]		
adcsar_dig_1	RGM_PRST[254]		
adcsar_dig_2	RGM_PRST[253]		
adcsar_dig_3	RGM_PRST[252]		
adcsar_dig_4	RGM_PRST[123]		
adcsar_dig_5	RGM_PRST[250]		
adcsar_dig_6	RGM_PRST[249]		
adcsar_dig_7	RGM_PRST[248]		
adcsar_dig_8	RGM_PRST[247]		
adcsar_dig_9	RGM_PRST[246]		
adcsar_dig_10	RGM_PRST[245]		

Table 1. Effects of reset (continued)

Receiving module	Software control	Detection	Software action required?
adcsd_dig_0	RGM_PRST[60]	For SDADCDig the conversion start sequence steps are the following: 1)After System Reset Deassertion, Enable SDADC by writing MCR.EN Bit 2)Configure MCR to select the required mode, polarity, common mode voltage, input gain,decimation rate; select the required analog channel for data conversion. It is possible to select the bias for each channel for AC coupling applications; configure OSD delay according to SDADC startup time or latency from reset exit. 3)Start The Conversion: Generate a reset event by writing 0x5AF0 to RESET_KEY of RKR. If EN is not set (condition after reset), then Step2&3 has no impact i.e No EOC received and start command is ignored by SDADCDig	NO, after reset no ADCSD conversion can be started
adcsd_dig_1	RGM_PRST[188]		
adcsd_dig_2	RGM_PRST[59]		
adcsd_dig_3	RGM_PRST[187]		
adcsd_dig_4	RGM_PRST[58]		
adcsd_dig_5	RGM_PRST[186]		
adcsd_dig_6	RGM_PRST[57]		
adcsd_dig_7	RGM_PRST[185]		
adcsd_dig_8	RGM_PRST[56]		
adcsd_dig_9	RGM_PRST[184]		
crc_0	RGM_PRST[38]	no enable bit but CRC_CFG reg includes length of data, poly selection and other options. Also, it is possible to check CRC_STAT, CRC_OUTP, CRC_OUTP_CHK (all 0/1 after rst). After reset the status of the CRC unit is lost (including the possibly partial signature computed and the use poly). Failure will be detected when the signature is checked against the expected value.	NO, reset is detected by the CRC when signature is checked against the expected value
crc_1	RGM_PRST[166]		
linflex_0	RGM_PRST[92]	no enable bit and after reset the LIN controller is in NORMAL state (not INIT: To enter this mode software sets the INIT bit in the LINCR1. To exit the initialization mode software should reset the INIT bit. When in initialization mode, all message transfers to and from the LIN bus are stopped and the status of LIN bus output LINTX is recessive). However, LIN baud rate after reset is set to zero (LINIBRRrst=0, LIN clock disabled) and is simple to check LIN baud rate after reset is set to zero (LINIBRRrst=0, LIN clock disabled) and no message is sent/received	NO, after reset no message will be sent/received
linflex_1	RGM_PRST[91]		
linflex_2	RGM_PRST[220]		
linflex_14	RGM_PRST[85]		
linflex_15	RGM_PRST[213]		
linflex_16	RGM_PRST[84]		

Table 1. Effects of reset (continued)

Receiving module	Software control	Detection	Software action required?
lfast_0	RGM_PRST[9]	Module enable DRFENrst=0 After reset LFAST is immediately disabled. All current/pending requests are terminated and the Tx and Rx data FIFOs are flushed. If a reset occurs in the middle of a transmit/receive operation, then that operation is terminated immediately and nothing is transmitted/received further. Registers read/write operations can be performed through the IPS Bus.	
cansubsys (canram controller)	RGM_PRST[74]	CAN RAM CTRL is reset together with the CAN subsystem.	NO, reset is detected via CAN subsystem reset
cansubsys (can1)	RGM_PRST[70]	After reset bit 0 [INIT] of the CCCR register = `1' in the CC Control Register and enables software initialization. The M_CAN does not influence the CAN bus until the CPU resets bit 0 [INIT] of the CCCR register = `0'	NO, after reset no communication is performed on the bus
cansubsys (can2)	RGM_PRST[69]		
cansubsys (can3)	RGM_PRST[68]		
cansubsys (can4)	RGM_PRST[67]		
cansubsys (TTCAN)	RGM_PRST[72]		
EBI_0	RGM_PRST[3]		NO, after reset all activity on EBI ports are stopped
SIUL	RGM_PRST[15]		YES, application dependent
FCCU	RGM_PRST[169]		YES

3.3.15 Periodic Interrupt Timer (PIT)

If a failure in the PIT can cause the violation of a safety goal, some software mechanisms are needed to guarantee the integrity of the PIT module.

Assumption: [SM_FMEDA_090]PIT operations (for example, the number of periodic triggers) are checked and compared against the expected values every FTTI. [end]

To implement this test, the number of interrupts generated by the PIT within a given time period shall be compared with the expected number of interrupts. To avoid CCF, the reference for the time period shall be independent from the PIT (for example, SWT).

If not covered by other means, software shall read back the PIT configuration and compare it with the expected configuration (for example, check for enabled channels and compared values, and so on.).

In all cases, when timing/latency of PIT interrupts is important, software shall check that the PIT interrupts are generated within the expected time.

3.3.16 System Timer Module (STM) usage

Assumption: [SCG18.075]Since a failure in the System Timer Module (STM) can cause a violation of the safety goal, one of the two assumptions below shall be satisfied. [end]

Assumption: [SCG18.076]At every STM interrupt, the IRQ handler shall compare the elapsed time since the previous interrupt versus a free running counter to check whether the interrupt time is consistent with the STM setting, or[end]

Assumption: [SCG18.077]The STM IRQ handler shall be under SWT protection. [end]

A second timer may be used to measure STM interrupts and compare with the STM measured time.

3.3.17 I/O and Peripheral Bridge

Assumption: [SCG18.084]The integrity of safety relevant periphery will be mainly ensured by application-level measures (for example, connecting one sensor to different I/O modules, sensor validation by sensor fusion, and so on) which are enabled on the hardware level by a replication of all potentially safety-relevant I/O with appropriate freedom of interference but no hardware checkers. This replication starts at the I/O bridges (including them). [end]

Safety relevant peripherals are assumed to be used redundantly in some way. Different approaches can be used, for example by getting replicated input, (for example, connect one sensor to two DSPIs or even connect two sensors measuring the same quantity to two ADCs) or by cross-checking some I/O operations with different operations (for example, using sensor values of different quantities to check for validity).

Recommendation: The usage of different data coding (for example, inversion) is recommended for redundant communication over safety relevant peripherals (for example, DSPI or LINFlex).

Assumption: [SCG18.952] Different data coding or message transfer timing is used for redundant communication over DSPI_4 and DSPI_5. [end]

Users can choose the approach that better fits their needs.

To allow a safety application to make redundant use of all I/O peripherals, the peripherals have two instances and each instance is connected to a different peripheral bridge (PBRIDGE). The arrangement of the I/O peripherals onto two PBRIDGEs allows redundant use of peripherals while limiting CCFs.

The MPC5777M architecture allows making redundant use of the communication peripherals like LINFlexD, DSPI and PSI5. Figure 2 shows the distribution of the MPC5777M peripherals.

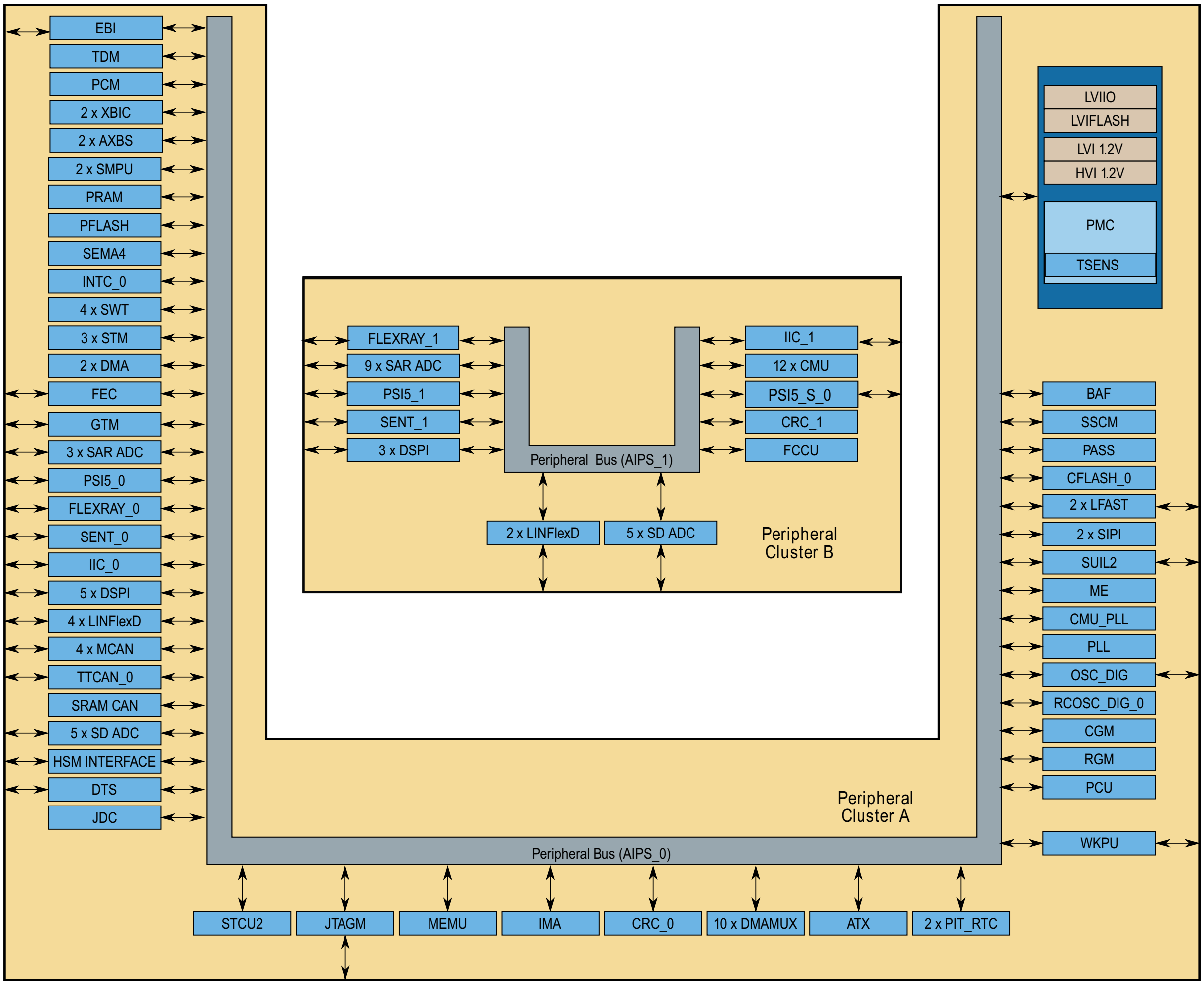

Figure 2. MPC5777M peripheral allocation

As a usage example, if an application needs to use LIN communications protocol, two different LINFlexD modules may be used; one connected to the PBRIDGEA and one the PBRIDGEB.

NOTE

> The safety concept for high bandwidth communication controllers (for example, FlexRay, FlexCAN, FEC (Ethernet)) is not based on the redundant use of multiple modules, but rather on the implementation of a fault tolerant protocol. This is the reason they are typically not split over the PBRIDGEs. Section 3.3.23, Communication peripherals discusses in more detail the usage of these types of communication controllers.

Assumption: [SCG18.085]Comparison of redundant operation is the responsibility of the application software. [end]

NOTE

> Additional details can be found in the “I/O peripherals” section in the “Functional Safety” chapter of the *MPC5777M Reference Manual*.

There are modules, particularly on-platform peripherals as INTC and eDMA, with a single peripheral interface. For these modules, the integrity of accesses to their register interface is not guaranteed by the PBRIDGE replication, and the following assumptions are required to cover failures affecting the value of data read from or written to their register interface.

Assumption: [SM_FMEDA_091]Software periodically checks the contents of configuration registers, and more than 10 registers of modules attached to PBRIDGE*n* are part of the countermeasure described in Section 3.3.2, CRC of configuration registers. [end]

Assumption: [SCG18.132] To ensure safe usage of modules which do not exist redundantly and are connected to only one PBRIDGE, one of the following shall be true for each user-visible (via the PBRIDGE*n*) register:

- The register is not relevant for the safety goal of the application.
- The register has a constant value (typically a configuration register) which is periodically checked for correct value (for example, by CRCing).
- Wrong values written into the register are detected by other safety measures.

Furthermore, for reading such registers the following is obviously true (due to the single nature of the data source):

- Values read from such registers are not guaranteed to be free of SPFs[end]

NOTE

> [SM_FMEDA_092]The FMEDA assumes that the above condition holds for at least 99% of the respective registers, but it is recommended to ensure it for 100% to reduce documentation complexities. [end]

Assumption: [SM_FMEDA_093]Software shall read back the values written to registers of non-redundant peripherals. [end]

NOTE

> Not necessary for configuration registers which are under CONF_REG_CRC_SCAN (as described in SM_FMEDA_063 (on page 50)) as that serves as a read-back on its own.

Assumption: [SM_FMEDA_094]When software reads a safety-relevant value from a peripheral, that value is read twice in a row, then the two read values are compared. This helps detect transient errors in the PBRIDGE for non-redundant peripherals. [end]

3.3.18 System Integration Unit Lite (SIUL2)

Since the SIUL2 PBRIDGE interface is unique, its failure, and particularly of its register protection module, may impact redundant I/O functionalities leading to CCF.

Assumption: [SM_FMEDA_095]When the SIUL2 is used for the implementation of safety related I/O functionality, application level redundancy is such that it covers at least 60% of failures introduced by the REG_PROT module that can result in blocked writes (lost updates) to non-locked registers (mostly GPO data registers). An additional software test shall run to detect such a failure mode. [end]

NOTE

A read-back after each write to the SIUL registers is sufficient to cover this failure mode.

Assumption: [SM_FMEDA_096]To detect wrong or multiple addressing failures, the startup read-back of SIUL configuration registers shall be executed after all SIUL2 registers have been written. [end]

Assumption: [SM_FMEDA_097]If the SIUL2 is used to perform a redundant digital input or output (read two GPIs or write two GPOs), the application will execute a periodic CRC of configuration registers that will be used to detect decoder hard faults that lead to CCF on data reads or writes. [end]

3.3.19 GTM Wrapper

Assumption: [SM_FMEDA_098]To detect if the GTM stops running due to a fault, application software shall periodically verify the GTM is running by reading the GTM status register (GTMDI_DS). [end]

Assumption: [SM_FMEDA_170] Application software shall check the configuration of the GTM Wrapper once per FTTI (for example, reading back the GTM configuration registers and compare them against the expected values). [end]

Assumption: [SM_FMEDA_099] Safety analysis assumes that failures in data registers (other than configuration failures), as well as in the GTM logic, are covered by application measures. [end]

3.3.20 External Bus Interface (EBI)

Assumption: [SM_FMEDA_100]Neither EBI nor LFAST are used in safety related applications. If used, it is the responsibility of the application software to recognize and detect failures caused by internal FIFO overflow or underflow (incorrect write or read operations), which may lead to wrong command, data or message loss. [end]

Assumption: [SM_FMEDA_101]IRQs from the LFAST module should be disabled on the Safety Core to prevent faulty LFAST communication from interfering with the execution of a safety related task. If not disabled, other measures shall be implemented to detect possible IRQ flooding. [end]

3.3.21 Reading analog inputs

Acquisition of safety related analog inputs can be performed using two independent ADCs modules redundantly.

The dual read analog input uses two analog input channels provided by two separate ADC modules to acquire a replicated analog input signal. Both ADC units acquire and digitize the two copies of a redundant analog signal connected to the inputs. In this configuration (if applied to all possible analog inputs), only half of the analog inputs are available to the applications.

Assumption: [SM_FMEDA_102] Software will read back the SIUL2 configuration once after programming to assess the correct configuration and connectivity of the two analog inputs. [end]

Assumption: [SM_FMEDA_103] Software will compare the value sampled by the two ADCs and decide on their consistency (comparison has to take into account conversion differences and tolerances). [end]

3.3.22 Software Watchdog Timer (SWT) usage

The objective of the Software Watchdog Timer (SWT) is to detect a defective program sequence when individual elements of a program are processed in the wrong sequence or period of time. Once the SWT is enabled, it requires periodic and timely execution of the watchdog servicing procedure. The service procedure must be performed within the configured time window, before the service timeout expires.

It is in general to be expected that software uses the software watchdog timer (SWT) to detect lost clocks or significantly slow clocks. Using the SWT to detect clock issues is a secondary measure since there are primary means for checking the clock integrity (for example, CMU).

MPC5777M provides the hardware support (SWT) to implement both control flow and temporal monitoring methods. If Windowed mode and Keyed Service mode (two pseudorandom key values used to service the watchdog) are enabled, it is possible to reach a high effective temporal flow monitoring.

Assumption: [SCG18.045]It is the responsibility of the application software to insert the control-flow checkpoints with the required granularity according to application needs. [end]

SWT can be configured to stop, or continue, running when the MCU is in STOP mode by configuring SWT_CR[STP]. If this SWT feature doesn't work as expected due to a fault, the safety function could be impaired (for example, SWT could trigger an unwanted reset while the device is in STOP mode).

Assumption: [SM_FMEDA_106]Current FMEDA assumes that STOP mode is not used in normal operations. [end]

3.3.23 Communication peripherals

Assumption: [SCG18.082]Communication over the following interfaces shall be protected by a fault-tolerant communication protocol (implemented by the operating system or the application):

- FlexRay
- FlexCAN
- Ethernet[end]

— Typically such a layer would contain an E2E CRC, a sequence counter, a sender ID, and an acknowledgement mechanism (if a transmission loss needs to be detected).

Assumption: [SCG18.083]If safety relevant, FlexRay and FlexCAN shall not be clocked directly by the XOSC. [end]

NOTE

> Directly using the XOSC as the source can expose the FlexRay or FlexCAN engines to glitches that would otherwise be filtered by the PLL.
>
> Customers can use the XOSC provided they implement safety mechanisms to detect the effects of glitches. These mechanisms can be part of the fault tolerant protocol.

An appropriate safety software protocol should be utilized for any communication peripheral employed to meet ASIL D application requirements

FlexRay, FlexCAN and Ethernet don’t have special safety mechanisms other than what is included into them by their protocol specs. The application software or operating system needs to provide the safety measures on top of the IP modules to meet safety requirements.

3.3.24 Temperature sensor (TSENS)

The MPC5777M includes an on-board temperature sensor that monitors device temperature and delivers an analog output signal.

The analog output signal is internally connected to an ADC input to acquire a value which is proportional to the temperature. Starting from this value, software can measure the current device temperature.

This analog path requires some software steps (for example, acquiring the value and applying a formula to obtain the temperature).

Assumption: [SM_FMEDA_039] Software shall read the analog output of the temperature sensor via the ADC and check for temperature violations at least once per FTTI. [end]

NOTE

> If only the analog output indicates undertemperature or overtemperature (but no digital indication), a TSENS failure might be indicated.

3.3.25 Analog to Digital Converters

The basic idea to verify the integrity of the functional ADCs is to implement software redundancy. This redundancy is supported by the hardware which allows acquiring analog inputs using independent ADC modules[1].

To decrease the probability of common cause of failure supervisor ADC and functional one don't share the same analog multiplexer.

[1] Simultaneous sampling of two ADCs on the same analog input is not allowed (see the *MPC5777M Reference Manual* for details).

Assumption: [SM_FMEDA_157]Analog inputs, which are safety relevant, shall be acquired redundantly by the functional and supervisor ADCs. The acquired values shall be compared by software.[1] [end]

NOTE

> Other types of redundancy can be implemented at application level. For example, information can be acquired redundantly by the MCU using analog data, i.e. via ADC, and digital data, i.e. via a communication protocol. Choosing the best strategy depends on the application.

This assumption is the main measure to be implemented. Some additional measures have been considered during the safety analysis to guarantee the integrity of all modules involved with the analog acquisition.

The SD ADC is expected to convert fast signals. The redundant acquisitions may not be effective if the frequency of the input analog signal is too high compared to conversion time and the time between the 2 redundant acquisitions. In such a case other mechanisms can be implemented, for example plausibility checks.

Assumption: [SM_FMEDA_158]In case analog input signal is expected to have certain dynamic/transient characteristics which make the redundant acquisition ineffective, the acquired data shall analyzed for such characteristics to verify the plausibility of the conversion. [end]

NOTE

> This measure mainly applies on the SDADC which is supposed to convert fast signals. User is expected to implement such a mechanism whether the redundant acquisition is not effective, for example due to the dynamic of the input signal.

An example of this mechanism is to verify if the FFT of the input signal is compatible with the expected one.

Assumption: [SM_FMEDA_159]Software periodically checks the contents of configuration registers of ADCs to ensure that the configuration has not accidentally changed. [end]

NOTE

> This counter-measure is part of the one described in Section 3.3.2, CRC of configuration registers.

ADCs embed an analog watchdog mechanism to trigger automatically DMA/interrupt request in case the converted value is outside configurable thresholds. The integrity of this hardware mechanism and the proper generation of DMA and interrupt from ADC can be verified by software.

Assumption: [SM_FMEDA_160] Once every FTTI, The ADC shall trigger a DMA/interrupt request by manipulating the thresholds of the analog watchdog with respect to a reference conversion. [end]

[1] Functional and supervisor ADCs share the same bias; a specific software mechanism to detect failures affecting the bias is presented (for example, SELFTEST_SARB_FTTI).

NOTE

> This safety mechanism doesn't cover the analog watchdog only, but it verifies the integrity of the interrupt and DMA generation by the ADC module. This procedure is required to run even if the analog watchdog is not used by the safety application.

Assumption: [SM_FMEDA_161] Every trigger (either hardware or software), which starts a conversion sequence, also initiates a timer or watchdog to monitor the conversion sequence duration. [end]

NOTE

> In case conversion time exceeds the expected value, this timer or watchdog shall abort the corresponding ADC conversion.

In case of scan mode, the conversion time is monitored for duration deviation more than the conversion time of a single channel.

Assumption: [SM_FMEDA_162] At the end of the conversion of all enabled channels (or after a CONV_TIME_MON time-out), software shall check the status of the conversion to detect any missed or spurious request. The status of the last conversion shall be cleared before starting a new one. [end]

NOTE

> In case of SAR ADC some registers which give information about the status of the conversion are showed below:
>
> - VALID and OVERW flags of the CDR registers
> - EOC/ECH flags
> - ECAWORR*x* (or ICAWOOR) and WTISR to verify any violation triggered by the analog watchdog.
>
> In case of SDADC the register showing status information is the SFR.
>
> Please check the SDADC section in the *MPC5777M Reference Manual* to have all details.

Assumption: [SM_FMEDA_163]In case the DMA is used to transfer the converted data from ADC modules to the memory, at the end of the conversion of all enabled channel VALID and OVERW flags of the CDR register and EOC status flags are verified against programmed configuration of DMA to detect any missing or spurious request. [end]

Functional and supervisor ADCs share the same reference bias. Since a failure affecting the bias can cause the violation of the safety goal, its integrity shall be verified at least per FTTI. This check can be done via software by acquiring some known analog values via the supervisor ADC.

Assumption: [SM_FMEDA_164] At least once per FTTI, the supervisor ADC shall acquire some known internal analog voltage signals and compare them with the expected values before being used to monitor the functional ADCs. [end]

NOTE

> The implementation of this software mechanism is the same than the SELFTEST_SARB one. The only difference is the execution frequency.

3.3.26 Mode Entry (MC_ME)

The MPC5777M can be configured in different functional modes. Each mode has its own unique configuration (for example, enabled peripherals and clock).

The mode configurations and the transition between different modes is controlled by the MC_ME. The correct execution of a mode transition shall be verified by application software.

Assumption: [SM_FMEDA_165] After the mode transition request, application software shall verify the status of the transition within the expected completion delay. Also, the new configuration is compared with the intended configuration. Completion delay is always monitored while the status check is performed, unless the target mode is low-power. [end]

Assumption: [SM_FMEDA_151] Mode transition process duration, from transition request to transition complete, shall be monitored. [end]

3.3.27 Semaphores (SEMA42)

Semaphores embedded in the MPC5777M is robust hardware support for implementing a simple mechanism to achieve “lock/unlock” operation of shared resources.

Assumption: [SM_FMEDA_166] To verify the integrity of the semaphores logic, application software before locking (or unlocking) a gate, shall check that the value of the gate is the expected one. [end]

NOTE

> Checking the gate state after the locking (or unlocking) request verifies if the gate has been properly locked (or unlocked).

Checking before unlocking the gate helps detect if other masters erroneously received the lock before it was released by the current master.

Checking before locking helps detect if the gate is already erroneously assigned to the requesting master.

3.4 Operational interference protection

As a multi-master system, the MPC5777M provides safety mechanisms to prevent non-safety masters from interfering with the operation of the Safety Core, as well as mechanisms to handle the concurrent operation of software tasks with different or lower ASIL.

3.4.1 Core Memory Protection Unit (CMPU)

The Core Memory Protection Unit (CMPU) ensures inter-task interference protection by providing the capability of protecting regions of memory from access by software tasks with different privilege levels. The CMPU features a 24-entry region descriptor table that defines memory regions and their associated access rights. Only accesses with the sufficient rights are allowed to complete.

Using pre-defined region descriptors that define memory spaces and their associated access rights, the CMPU concurrently monitors Core initiated memory accesses and evaluates the appropriateness of each transfer.

Assumption: [SM_FMEDA_108] The application software shall configure the CMPU (at least of the Safety Core) to define the location, size, access permissions and memory attributes for each memory region that needs to be protected. [end]

Recommendation: [SM_FMEDA_109] For ASIL D applications, the CMPU should be used to ensure that only authorized software tasks can configure modules and can access only their allocated resources according to their access rights. [end]

3.4.2 System Memory Protection Unit (SMPU)

The System MPU (SMPU) provides memory protection at the crossbar (XBAR). The SMPU splits the physical memory into 16 different regions. Each XBAR master (Core, DMA, FlexRay, SIPI) can be assigned different access rights to each region.

Assumption: [SM_FMEDA_110] The SMPU will be used to prevent non-safety masters (all except the Safety Core) from accessing restricted memory regions unless those regions are similarly protected by mechanisms shown in Section 3.4.3, AIPS protection mechanism or Section 3.4.4, Register protection (REG_PROT). [end]

Assumption: [SM_FMEDA_111] The SMPU shall only be programmed by the Safety Core. This software shall prevent write accesses to the SMPU's registers from all other masters. [end]

NOTE

> See "System Memory Protection Unit (SMPU)" chapter in the *MPC5777M Reference Manual* for details.

Assumption: [SCG18.052]After safety software takes control of the MPU it will check: [end]

- **Assumption:** [SCG18.053]That the HSM did assign itself only the expected access rights at the SMPU in the expected regions. [end]
- **Assumption:** [SCG18.054]That the configuration of SMPU/AIPS has been changed in such a way that the HSM no longer has writing access to the SMPU. [end]

3.4.3 AIPS protection mechanism

The peripheral bridges (PBRIDGE*n*) translate accesses on the switched AMBA bus (XBAR) to point-to-point accesses to the majority of peripherals on the MPC5777M. The peripherals connected to the PBRIDGEs are PBRIDGE slaves.

The PBRIDGEs implement an additional protection mechanism to support the requirement that non-safety relevant masters and safety relevant masters do not interfere with one another. The protection mechanism allows for protection of each slave from master accesses (for example, read/write or supervisor/user access).

Assumption: [SM_FMEDA_112] The application software will configure the PBRIDGEs to define the access permissions for each slave module that requires access protection, unless protected by the mechanisms in sections Section 3.4.2, System Memory Protection Unit (SMPU) or Section 3.4.4, Register protection (REG_PROT). [end]

PBRIDGE*n* should be configured to prevent any write access to the entire MC_RGM address space for all masters except the Safety Core.

Assumption: [SCG18.133]Safety software shall program the Peripheral Access Control in the PBRIDGE*n* so no write access to the MC_RGM_PRST[*n*] (individual module reset programming model) is allowed to access other cores. [end]

3.4.4 Register protection (REG_PROT)

Accidental writes to configuration registers can affect the execution of the MCU's safety function and disable the safety mechanism due to their change. Register protection offers a mechanism to protect defined memory mapped address locations in a module against writes. The address locations that can be protected are module specific.

Register protection includes these distinctive features:

- Register protection can restrict accesses for the module under protection to supervisor mode. This access restriction is in addition to any access restrictions imposed by the protected module.
- A register cannot be written once Soft Lock Protection is set. Soft Lock Protection can be cleared by software or system reset.
- A register cannot be written once Hard Lock Protection is set. Hard Lock Protection can only be cleared by system reset.

Recommendation: It is recommended that only hardware related software (OS, drivers) run in supervisor mode.

Assumption: [SM_FMEDA_114]Configuration registers are to be locked 90% of the time, either by Soft Lock or Hard Lock Protection, to prevent unwanted modifications. [end]

NOTE

> **Implementation hint:** Each peripheral register that can be protected through register protection has a Set Soft Lock bit reserved in the Register Protection address space. This bit should be asserted to enable the protection of the related peripheral registers. Moreover, the Hard Lock Bit (REG_PROT_GCR[HLB] = 1) should be set for best write protection.

Assumption: [SM_FMEDA_171] The REG_PROT configuration registers shall be read and compared against the expected values at least once after being programmed. [end]

3.4.5 Performance (Core_1) and Peripheral (Core_2) Cores

Performance (Core_1) or Peripheral (Core_2) cores are considered Non-safety modules (NoSaMo). If they execute any safety task, counter measures must be used in application software.

Some hardware resources are shared between Core_1, Core_2 and the Safety Core (Master Core and Checker Core). It is required that interference between Core_1 and Core_2 with safety relevant modules is avoided.

Assumption: [SM_FMEDA_115]No more than 20% of the entire address space contains writable safety-relevant modules or data. [end]

Assumption: [SM_FMEDA_116]To avoid excessive accesses to shared resources, the NoSaMo cores (Core_1 and Core_2) have lower XBAR priority than the Safety Core (Master Core and Checker Core). [end]

Assumption: [SM_FMEDA_123]The local memories of the NoSaMo cores must not be used to store safety-relevant data, or only if software protection against spurious changes by the NoSaMo cores exists. [end]

Assumption: [SM_FMEDA_117]To avoid unwanted software interrupts triggered by the Peripheral Core (Core_2) and Computational Core (Core_1) which are handled by the Safety Core, one of the following holds: [end]

- Accidental access to the triggering registers of these interrupts is prevented (typically by SMPU and/or AIPS_PACR)
- There exists an additional indicator (in addition to the triggering register, for example, a variable in RAM) which can be used to execute an ISR_CHECK_TRIGGER_SET (on page 39) like functionality.

Alternatively, the Safety Core could be configured to ignore software triggered interrupts.

Assumption: [SCG18.953] Safety-relevant software will enable the INTC_MPROT lock bit. [end]

4 Functions of external devices for ASIL D applications

This section describes the external components needed to use with MPC5777M in a system for ASIL D applications. It is assumed that the system reacts safely to MPC5777M being in or entering all Safe state$_{MCU}$.

It should be noted that the failure rates of external services are not included in the FMEDA of MPC5777M and have to be included in the system FMEDA by the user himself.

4.1 External reset output

MPC5777M has pin named external reset output (ESR0). The signal on this pin can be used as input to one, or more, external devices. It is possible that an unwanted or spurious assertion of ESR0 may not be detected by the MPC5777M. This could cause the external device to get reset without any automatic detection by MPC5777M. Assumption is that countermeasures against this failure mode must be considered at system level.

Assumption: [SM_FMEDA_118]System level I/O safety measures have at least 99% DC against joint spurious reset of all external devices. [end]

4.2 High impedance outputs

System-level countermeasures have to be placed in order to bring the safety-critical outputs to their safe state (for example, by pull-up or pull-down resistors) when an output high-impedance is not considered safe. Normally this requirement will be fulfilled by ensuring the error out pin(s) are pulled to the failure state. Additionally, users may drive pins (for example, CAN Tx pins) to levels that prevent interference with other parts of the system that are assumed to be independent.

Assumption: [SCG18.086]If a high impedance state on an output pin is not safe, pull-up or pull-down resistors need to be added to outputs that are safety-critical depending on application requirements for the MPC5777M during unpowered or reset conditions. [end]

4.3 External Watchdog (EXWD)

An external device, acting as supervisor of the operations, must provide a watchdog to cover common-cause failures of MPC5777M for ASIL D applications.

Assumption: [SCG18.087]An external watchdog shall exist to detect failures completely disabling the MPC5777M, including its safety mechanisms. [end]

The external watchdog will detect CCFs, such as failure of the power supply. If a failure is detected, the external watchdog should move the system to a Safe state$_{\text{system}}$ within the FTTI.

Assumption: [SCG18.088]The EXWD shall be triggered periodically, either by the software providing the safety function on the MPC5777M or by a toggling protocol on the error output pin(s). [end]

Implementation of the watchdog communication between MPC5777M and the external device is up to the user (for example, communication via serial link, ethernet, via toggling pin, or via the FCCU error out signals).

Assumption: [SM_FMEDA_119]To avoid undetected reset cycling under rare circumstances the external watchdog will not be reset by the MCU reset output. [end]

NOTE

There must be a signalling path from the safety software to the external system through which the software can confirm correct initialization. This is not automatically guaranteed by the FI[*n*] signals which communicate the status of the device independently from software. On the other hand, a different communications interface (such as a serial link) can be used to detect incorrect software initialization.

4.4 Power supply

Assumption: [SCG18.089]The device has been developed with the assumption that an external power supply of appropriate voltage shall be supplied (see the *MPC5777M Data Sheet's* for operating voltage specifications). All internal and external supplies are considered safety critical and shall be monitored for deviations beyond predefined thresholds. [end]

Assumption: [SCG18.090]External power supply shall be supervised for high and low voltage deviations as shown in Table 2. Required monitors for each power supply can be found in column “External monitor required”. [end]

NOTE

Voltage monitors are provided on the MPC5777M to monitor the internal supplies of the device. See table “POR and voltage monitors description” in the “Power management” chapter of the *MPC5777M Reference Manual* for a list of monitored supplies.

LVD/HVD are necessary to ensure logic functionality. External LVD can be removed if the failure can be detected by other means, but the external HVD is necessary to prevent physical damage.

Table 2. MPC5777M required external monitors

Name	Description	External Monitor Required
VDD_HV_ADR_D	Voltage reference of ADC sigma/delta module	LVD/HVD
VDD_HV_ADR_S	Voltage reference of ADC SAR module	LVD/HVD
VDD_HV_IO_MAIN	High voltage Power supply for the I/O’s	HVD
VDD_HV_IO_FLEX	FlexRay/Ethernet 3.3 V I/O supply	HVD
VDD_HV_IO_JTAG	Oscillator and JTAG pin supply	HVD

Assumption: [SCG18.091] External supervision shall hold the MPC5777M in a Safe state$_{\mathrm{MCU}}$ and the system in its Safe state$_{\mathrm{system}}$ if the external voltage is outside specifications. The MCU shall be protected against voltages over the maximum survivable level of the technology. [end]

Recommendation: It is recommended to protect the MCU against voltage above the maximum survivable level of the technology (for example, using a Zener diode) to prevent destruction of the MCU.

NOTE

See the *MPC5777M Data Sheet’s* “Absolute maximum ratings” and “DC electrical specifications” sections for power supplies requirements.

[SCG18.123]The MPC5777M embeds two types of voltage supervisors, Low Voltage Detect (LVD) and High Voltage Detect (HVD) monitors. Safety relevant voltages are supervised for voltages that are out of these ranges. Since safety relevant voltages have the potential to disable the failure indication mechanisms of the MPC5777M (such as FCCU, Pads, and so on) their error indication directly causes a transition into the Safe state$_{\mathrm{MCU}}$ (for example, reset assertion). [end]

Some LVDs and HVDs are configurable and enabled by default. Application should not disable safety relevant LVDs or HVDs. See the “POR and voltage monitors description” table in the “Power management” chapter of the *MPC5777M Reference Manual* for the list of configurable LVDs and HVDs.

4.5 Error Out Monitor (ERRM)

The FCCU has two external pins: FI[0] and FI[1]. An external device must be connected to the FCCU via FI[0] and optionally FI[1] to continually monitor the error output pins of the FCCU.

Assumption: [SCG18.092]The overall system needs to include measures to monitor the error output pin(s) of the MPC5777M and move the system into a Safe state$_{\mathrm{system}}$ when an error is indicated. [end]

Assumption: [SCG18.093]If the MPC5777M is signalling a failure via its error output pin(s), other output pins can not be relied on. [end]

4.5.1 Both FCCU pins connected to external device

Depending on user selection, there are two different ways to interface to the FCCU:

- Both FCCU pins connected to the external device
- Only a single FCCU pin connected to the external device

The user can choose between these two FCCU configurations, depending on which best fits the hardware and software system.

Assumption: [SM_FMEDA_120] If both error out pins are connected to the external device, the external device itself shall check both signals, taking into account the behavior of the two pins as defined in Table 3. [end]

Table 3. FCCU EOUT pin behavior[1]

2-pin protocol	FI[1]	FI[0]	Definition of faulty state
Bi-stable	1	0	Two pins are out of phase and FI[0] is low
Time switching	1	0	Two pins are out of phase and FI[0] is low
Dual rail	toggle_inv	toggle_inv	Tow pins are not out of phase
Dual rail	1	toggle_inv	Two pins are not out of phase

NOTES:

[1] See “EOUT interface” section in the “Fault Collection and Control Unit (FCCU)” chapter of the *MPC5777M Reference Manual* for details. If Error phase is accompanied by a functional reset, FI[1]/EOUT1 becomes high-z with weak pull-up, while FI[0]/EOUT0 behaves as described.

In this configuration the external device continuously monitors the output of the FCCU. Thus it can detect if the error out pins are not working properly. The advantage of the two pin configuration with respect to the single pin option is that it does not require any dedicated software.

NOTE

> **Implementation hint:** Monitoring the error output pins through a combinatorial logic (for example, XOR port) can generate some glitches. Oversampling these pins reduces the possibility that the glitches occur. A functional reset has no affect on FI[0], but it sets FI[1] to high-impedance with a pull-up. To avoid changing FI[1] during a functional reset when time-switching or bistable protocol is used, it is recommended to configure FCCU_CFG[PS] = 0.

4.5.2 Single FCCU pin connected to external device

In this configuration, only the FI[0] pin is connected to the external device. If a fault occurs, the FCCU communicates it to the external device through the FI[0] pin.

The functionality of FI[0] can be verified in two ways on a system level by testing that FI[0] can trigger the Safe state$_{system}$. If only FI[0] needs to be tested (without the rest of the shutdown path), this can be accomplished with either of the following:

- FI[0] output, and FI[0] input (loop through the IO pad).
- FI[0] output connected externally to a normal GPIO.

The customer must choose which solution best fits their requirement.

Assumption: [SM_FMEDA_121] After boot, but before executing the safety function, the functionality of FI[0] pin shall be verified[1]. [end]

As access to FI[0] is shared between the FCCU and GPIO there is a failure mode where the multiplexing fails and FI[0] becomes controlled by GPIO. To make this detectable, the respective GPIO needs to be configured to drive FI[0] into the fail state.

Assumption: [SCG18.094]If an error indication protocol is selected which makes use of only one error out pin (for example, FI[0]), then SW configures any I/O MUXed to that pin to drive low before switching the pin to FCCU control [end] (see the *MPC5777M Reference Manual's* "Signal Description" chapter and the "I/O Signal Description table" for pin MUXing specifics).

The advantage of this configuration with respect to the configuration where two error indication signals are used, is that it can use an external device that does not compare the two signals.

Assumption: [SM_FMEDA_122] If the system is using the MPC5777M in a single error output pin mode, the application software shall configure the pins and pads neighboring the FI[0] to use a lower drive strength. [end]

Using a lower drive strength on the pins near FI[0] will reduce the effects of simultaneously switching outputs on signal integrity. Software must configure the slew rate for the relevant pads in the Pad Configuration Register.

[1] Since FCCU is a monitor, it is sufficient to verify the FI[0] signal only at start-up in order to avoid latent faults.

5 Address decoding coverage

5.1 Overview

The MPC5777M embeds a hardware mechanism called Single Bit Error Correction and Dual Bit Error Detection to detect and, if possible, correct failures impacting the RAM array. This hardware measure is based on a modified Hamming code algorithm.

Faults impacting the addressing logic (for example, addressing faults) generally cause Multi Bit Errors (MBEs). The MPC5777M does not embed a specific hardware mechanism to manage this type of fault, but these MBEs can be interpreted by the modified Hamming code algorithm as Single Bit Errors (SBEs). This may cause a violation of the safety goal.

This chapter explains how, in case of an ECC hit, a software test can differentiate between an SBE and an MBE due to a permanent fault in the addressing logic.

5.2 Test implementation

The basic mechanism behind addressing fault detection is the ECC with address contribution embedded in the MPC5777M devices.

Reading from locations affected by permanent addressing faults returns a random pattern. The Diagnostic Coverage (DC) of the ECC against addressing faults on a single access is about 70%.

To improve this DC, the idea is to perform multiple memory reads in order to trigger the failure mechanism multiple times, say K, and in multiple locations in such a way that the overall DC increases up to $DC = 1 - (1 - 70\%)^K$.

This formula is valid under the assumption the K failures are somehow independent. It is necessary to:

- understand how to trigger K independent failures in case of addressing fault, and
- minimize the number of memory operations, say M, necessary to trigger the K failures.

The described algorithm is focused on the detection of failures affecting RAM address decoder considering both rows and columns of the array.

To achieve these objectives, user shall know the “hit address” and details on how the memory is implemented.

Table 4. Address decoding

							Word address predecoding bits					
							Row selection				Column selection	
Location	**Memory**	**Shall be tested?**	**Mux**	**Number of words**	**Bits per word**	**Number of address bits**	**Dec D**	**Dec C**	**Dec B**	**Dec A**	**Dec E**	**Block address**
Core_0 (Safety Core)	I-Mem	yes	8	2048	72	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
	D-Mem0[1]	yes	8	8192	40	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
	D-Mem1[1]	yes	8	8192	40	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
Core_1	I-Mem	not mandatory application dependent	8	2048	72	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
	D-Mem0[1]		8	8192	40	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
	D-Mem1[1]		8	8192	40	13	—	A<12>	A<11:9>	A<8:6>	A<5:3>	A<2:0>
FlexRay0	DRAM	not mandatory application dependent	4	128	26	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
	LRAM1,2		4	96	63	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
FlexRay1	DRAM	not mandatory application dependent	4	128	26	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
	LRAM1,2		4	96	63	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
TTCAN	TTCAN	not mandatory application dependent	16	5120	39	13	A<12:10>	A<9:8>	A<7:6>	A<5:4>	A<3:0>	—
NAR	NAR1...4		4	64	128	12	—	A<11>	A<10:8>	A<7:5>	A<4:3>	A<2:0>

Table 4. Address decoding (continued)

							Word address predecoding bits					
							Row selection				Column selection	
Location	**Memory**	**Shall be tested?**	**Mux**	**Number of words**	**Bits per word**	**Number of address bits**	**Dec D**	**Dec C**	**Dec B**	**Dec A**	**Dec E**	**Block address**
Platform	DMA0,1	not mandatory application dependent	4	256	72	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
Platform	Overlay1,2	yes	4	1024	72	12	—	A<11>	A<10:8>	A<7:5>	A<4:3>	A<2:0>
Platform	SRAM1...6	yes	16	8192	72	13	A<12:10>	A<9:8>	A<7:6>	A<5:4>	A<3:0>	—
Platform	SRAM7	yes	16	2560	72	13	A<12:10>	A<9:8>	A<7:6>	A<5:4>	A<3:0>	—
Platform	FEC/FICO	not mandatory application dependent	4	128	44	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
Platform	FEC/MIB	not mandatory application dependent	4	64	40	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—

Table 4. Address decoding (continued)

							Word address predecoding bits					
							Row selection				Column selection	
Location	Memory	Shall be tested?	Mux	Number of words	Bits per word	Number of address bits	Dec D	Dec C	Dec B	Dec A	Dec E	Block address
GTM	FIFO1,2	not mandatory application dependent	8	1024	36	12	A<11:9>	A<8:7>	A<6:5>	A<4:3>	A<2:0>	—
	(MCSi)-RAM0, i=0-2...6	not mandatory application dependent	8	1024	39	12	A<11:9>	A<8:7>	A<6:5>	A<4:3>	A<2:0>	—
	(MCSi)-RAM1, i=0-2...6	not mandatory application dependent	4	512	39	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
	DPLL-1A	not mandatory application dependent	4	128	31	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
	DPLL-1B	not mandatory application dependent	4	384	31	10	—	A<9:7>	A<6:4>	A<3:2>	A<1:0>	—
	DPLL-2	not mandatory application dependent	16	4096	31	13	A<12:10>	A<9:8>	A<7:6>	A<5:4>	A<3:0>	—

NOTES:

[1] Internal data memory of Core_0 (and Core_1) is implemented by 2 separated memory instantiations, i.e. D-Mem0 and D-Mem1. Such memories are connected in parallel. Considering a 64bit word, the first 32bit are located in D-Mem0 and the second 32bit in D-Mem1. Each memory has its own decoding logic. In case of single bit error correction, the self-test to detect failure in the addressing logic shall be executed only in the memory in which the error is detected, either D-Mem0 or D-Mem1.

Table 4 reports multiple details about the design of each RAM impacted by the described software self-test. Details below must be used to implement the testing algorithm:

- Muxing
- Number of words for the whole array
- Bits per words
- Number of address bits
- Number of bits used as address by the RAM
- Info about decoder addressing structure in terms of multiplexer
  - — testing algorithm is based on several reading of different RAM locations; list of these locations depends on the decoding structure of the RAM.

During each memory access operation, the word is selected via multiple decoders connected to the RAM cells. How the address bus is decoded for the memory array depends on the design parameters described in Table 4.

The address bus is partitioned to:

- Row decoders (for example,. DecD, DecC, DecB and DecA)
  - — these bits are used to select the row to be accessed
- Column decoders (for example, DecA)
  - — these bits are used to select the column to be accessed
- Block selection (for example, block address)
  - — these bits are used to select the block to be accessed in case the memory is internally partitioned in multiple blocks.

Let’s assume a permanent failure in the addressing logic causes an MBE. This MBE may be incorrectly interpreted as single bit error by the ECC/EDC hardware. The address of the reported single bit error is indicated as Ah[1].

To distinguish this permanent addressing fault from an SBE, some back-to-back reads from Ah and their coupled addresses shall be executed.

Considering the hit address as starting point, the self-test requires reading a list of locations correlated in some way to hit address.

This list includes different locations whose address is obtained by changing one by one the bits of each decoding group (DecD, DecC, and so on).

All these memory locations shall be read following a specific order as described below.

Table 5 (Example of back-to-back read to implement test) reports an example of list of addresses obtained starting from a specific hit address (also called victim).

This example assumes a single bit error reported at the hit address Ah of the SRAM. With reference to Table 1, the addressing logic of the system RAM consists of 13 bits which go through multiple decoders:

- Row selection

[1] Hitting address.

- — DecD – A<12:10>
- — DecC – A<9:8>
- — DecB – A<7:6>
- — DecA – A<5:4>>
- Column selection
  - — DecE – A<3:0>

Having these parameters in mind the user, starting from the victim address, shall build a list of the locations which shall be read by the self-test.

For this example the list of locations to be read is shown in Table 5 (Example of back-to-back read to implement test). All locations in grey shall be read. Some locations have an associated number; this number is the read order. Location #1 shall be read first, location #2 second, and so on. The order is not important for location without any number specified.

In such example the SRAM locations to be read are:

1. 100.01.00.11.110b
2. 011.10.11.00.110b
3. 011.10.11.00.001b
4. and so on.

Next section describes how to compile such a list.

Table 5. Example of back-to-back read to implement test

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00	▨	▨					▨	▨	DecD combination
001	10	11	00		▨	▨			▨	▨		DecD combination
010	10	11	00		▨		▨	▨		▨		DecD combination
011	10	01	00	▨	▨					▨	▨	DecB combination
011	10	11	00		▨	▨			▨	▨		DecB combination
011	00	11	00		▨		▨	▨		▨		DecC combination
011	01	11	00		▨	▨			▨	▨		DecC combination
011	10	11	00	6	4	10	14	16	12	2	7	Ah : victim address (red cell)
011	11	11	00		▨		▨	▨		▨		DecC combination
011	10	11	01	▨	▨					▨	▨	DecA combination
011	10	11	10		▨	▨			▨	▨		DecA combination
011	10	11	11		▨		▨	▨		▨		DecA combination
100	01	00	11	5	3	9	13	15	11	1	7	Complementary address

Table 5. Example of back-to-back read to implement test (continued)

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
100	10	11	00		▨					▨		DecD combination
101	10	11	00		▨	▨			▨	▨		DecD combination
110	10	11	00		▨		▨	▨		▨		DecD combination
111	10	11	00	▨	▨					▨	▨	DecD combination

5.3 Obtaining the list of locations to be read

This section describes, with an example, the different steps to get the list of location to be read. The procedure starts when a single bit error correction at certain address, i.e. victim address, is reported.

Let assume the victim address is the address 011101100001 in the SRAM.

The first step is to split the victim address in “bit grouping” depending on the decoding structure of the memory (see Table 4).

Figure 3 shows the bit grouping for the victim address of the example.

	DecD	**DecC**	**DecB**	**DecA**	**DecE**
Victim address Ah	011	10	11	00	001
	row selection				column selection

Figure 3. Bit grouping of victim address considering the SRAM

With reference to the Table 6, the first locations to be read are the victim address (in red), its complementary (in yellow) and all locations belonging to the word-line of the victim and complementary addresses (in grey).

Table 6. Victim address and complement

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
011	10	11	00	▨	🟥	▨	▨	▨	▨	▨	▨	Ah : victim address (red cell)
100	01	00	11	▨	▨	▨	▨	▨	▨	🟨	▨	Complementary address

In the next step starting from the victim address, the value of DecD, DecC and DecB is kept unchanged and all combinations of DecA are considered.

As result three additional word-lines are added to the list (in gray in Table 7).

Table 7. All combinations of DecA considered

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
011	10	11	00		🟥							Ah : victim address (red cell)
011	10	11	01	▨	▨	▨	▨	▨	▨	▨	▨	DecA combination
011	10	11	10	▨	▨	▨	▨	▨	▨	▨	▨	DecA combination
011	10	11	11	▨	▨	▨	▨	▨	▨	▨	▨	DecA combination
100	01	00	11									Complementary address

In the next step starting from the victim address, the value of DecD, DecC and DecA is kept unchanged and all combinations of DecB are considered.

As result 3 additional word-lines are added into the list (in grey in Table 7 and Table 8).

Table 8. All combinations of DecB considered

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
011	10	00	00	▨	▨	▨	▨	▨	▨	▨	▨	DecB combination
011	10	01	00	▨	▨	▨	▨	▨	▨	▨	▨	DecB combination
011	10	10	00	▨	▨	▨	▨	▨	▨	▨	▨	DecB combination
011	10	11	00		🟥							Ah : victim address (red cell)
011	10	11	01									DecA combination
011	10	11	10									DecA combination
011	10	11	11									DecA combination
100	01	00	11									Complementary address

Same procedure shall be applied for remaining address decoders, i.e. DecD and DecC, as result some additional word-lines are added to the list (in grey in Table 9).

Table 9. All combinations of DecC and DecD considered

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
001	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
010	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
011	10	01	00									DecB combination
011	10	11	00									DecB combination
011	00	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecC combination
011	01	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecC combination
011	10	11	00		🟥							Ah : victim address (red cell)
011	11	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecC combination
011	10	11	01									DecA combination
011	10	11	10									DecA combination
011	10	11	11									DecA combination
100	01	00	11									Complementary address
100	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
101	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
110	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination
111	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	DecD combination

All locations listed in Table 10 should be read to perform the self-test. To minimize the testing time, the pattern can be optimized by reducing the number of locations to be read.

Table 10. All cells should be read

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00									DecD combination
001	10	11	00									DecD combination
010	10	11	00									DecD combination
011	10	01	00									DecB combination
011	10	11	00									DecB combination
011	00	11	00									DecC combination
011	01	11	00									DecC combination
011	10	11	00		🟥							Ah : victim address (red cell)

Table 10. All cells should be read (continued)

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
011	11	11	00									DecC combination
011	10	11	01									DecA combination
011	10	11	10									DecA combination
011	10	11	11									DecA combination
100	01	00	11									Complementary address
100	10	11	00									DecD combination
101	10	11	00									DecD combination
110	10	11	00									DecD combination
111	10	11	00									DecD combination

This reduction is performed into 2 steps.

First, all words belonging to the row and column of the victim and complementary addresses shall be read (in gray in Table 11).

Table 11. All cells should be read

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00		▨					▨		DecD combination
001	10	11	00		▨					▨		DecD combination
010	10	11	00		▨					▨		DecD combination
011	10	01	00		▨					▨		DecB combination
011	10	11	00		▨					▨		DecB combination
011	00	11	00		▨					▨		DecC combination
011	01	11	00		▨					▨		DecC combination
011	10	11	00	▨	🟥	▨	▨	▨	▨	▨	▨	Ah : victim address (red cell)
011	11	11	00		▨					▨		DecC combination
011	10	11	01		▨					▨		DecA combination
011	10	11	10		▨					▨		DecA combination
011	10	11	11		▨					▨		DecA combination
100	01	00	11	▨	▨	▨	▨	▨	▨	🟨	▨	Complementary address
100	10	11	00		▨					▨		DecD combination
101	10	11	00		▨					▨		DecD combination
110	10	11	00		▨					▨		DecD combination
111	10	11	00		▨					▨		DecD combination

For the second step of the reduction all of the following rules shall be considered:

- Not all columns needs to be read from each row.
- At least 4 different columns per each row shall be read.[1]
- At least 4 different rows per each column shall be read.

An example of result for this reduction is shown in Table 12.

Table 12. The locations to be read by self-test (colored gray)

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00	▨	▨					▨	▨	DecD combination
001	10	11	00		▨	▨			▨	▨		DecD combination
010	10	11	00		▨		▨	▨		▨		DecD combination
011	10	01	00	▨	▨					▨	▨	DecB combination
011	10	11	00		▨	▨			▨	▨		DecB combination
011	00	11	00		▨		▨	▨		▨		DecC combination
011	01	11	00		▨	▨			▨	▨		DecC combination
011	10	11	00	▨	▨	▨	▨	▨	▨	▨	▨	Ah : victim address (red cell)
011	11	11	00		▨		▨	▨		▨		DecC combination
011	10	11	01	▨	▨					▨	▨	DecA combination
011	10	11	10		▨	▨			▨	▨		DecA combination
011	10	11	11		▨		▨	▨		▨		DecA combination
100	01	00	11	▨	▨	▨	▨	▨	▨	▨	▨	Complementary address
100	10	11	00		▨					▨		DecD combination
101	10	11	00		▨	▨			▨	▨		DecD combination
110	10	11	00		▨		▨	▨		▨		DecD combination
111	10	11	00	▨	▨					▨	▨	DecD combination

At this point we have the list of the locations which shall be read by the self-test (in grey in Table 1Table 10).

Last step is the order of reading these locations. The rows related to the victim and complementary addresses shall be read in a specific order. The basic idea is that starting from the complementary address the addressing logic shall be stressed by alternate reads from the 2 rows.

First 4 locations to be read are shown in Table 13.[2]

[1] This rules is not valid for the word-lines of the hit-address and its complement. All columns of these word-lines shall be read.

[2] This specific order is represented by the number in the cell of Table 13.

Table 13. First four cells read

				DecE								
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00	▨	▨					▨	▨	DecD combination
001	10	11	00		▨	▨			▨	▨		DecD combination
010	10	11	00		▨		▨	▨		▨		DecD combination
011	10	01	00	▨	▨					▨	▨	DecB combination
011	10	11	00		▨	▨			▨	▨		DecB combination
011	00	11	00		▨		▨	▨		▨		DecC combination
011	01	11	00		▨	▨			▨	▨		DecC combination
011	10	11	00	▨	4	▨	▨	▨	▨	2	▨	Ah : victim address (red cell)
011	11	11	00		▨		▨	▨		▨		DecC combination
011	10	11	01	▨	▨					▨	▨	DecA combination
011	10	11	10		▨	▨			▨	▨		DecA combination
011	10	11	11		▨		▨	▨		▨		DecA combination
100	01	00	11	▨	3	▨	▨	▨	▨	1	▨	Complementary address
100	10	11	00		▨					▨		DecD combination
101	10	11	00		▨	▨			▨	▨		DecD combination
110	10	11	00		▨		▨	▨		▨		DecD combination
111	10	11	00	▨	▨					▨	▨	DecD combination

To determine the reading order of the other locations of these 2 word-lines the following principles shall be considered:

- Alternate reads between the 2 word-lines starting from the word-line of the complementary address.
- First, read from columns close to the victim address; second, a column close to the complementary address, and so on.

Table 14 shows an example about the required reading order for victim and complementary rows. No ordering requirements for the remaining locations.

To summarize:

- All grey locations of this table shall be read
- Reading of victim and complement word-lines shall follow a specific order.[1]

[1] The number in the cell represents the reading order.

Table 14. First four cells read

				DecE							
DecD	**DecC**	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Description**
000	10	11	00	▨	▨					▨	▨	DecD combination
001	10	11	00		▨	▨			▨	▨		DecD combination
010	10	11	00		▨		▨	▨		▨		DecD combination
011	10	01	00	▨	▨					▨	▨	DecB combination
011	10	11	00		▨	▨			▨	▨		DecB combination
011	00	11	00		▨		▨	▨		▨		DecC combination
011	01	11	00		▨	▨			▨	▨		DecC combination
011	10	11	00	6	4	10	14	16	12	2	8	Ah : victim address (red cell)
011	11	11	00		▨		▨	▨		▨		DecC combination
011	10	11	01	▨	▨					▨	▨	DecA combination
011	10	11	10		▨	▨			▨	▨		DecA combination
011	10	11	11		▨		▨	▨		▨		DecA combination
100	01	00	11	5	3	9	13	15	11	1	7	Complementary address
100	10	11	00		▨					▨		DecD combination
101	10	11	00		▨	▨			▨	▨		DecD combination
110	10	11	00		▨		▨	▨		▨		DecD combination
111	10	11	00	▨	▨					▨	▨	DecD combination

5.3.1 Memories including block address decoding

Some memories (for example, D-Mem) include a block address decoder. In this case a further step shall be added to the procedure described in Section 5.3, Obtaining the list of locations to be read.

	DecC	**DecB**	**DecA**	**DecE**	**Block**
Victim address Ah	1	110	010	101	001
	row selection			column selection	block selection

Figure 4. Bit grouping of victim address considering D-Mem

To describe the needed additional steps, an example is considered. Let's assume a single bit error is reported at the hit address 1.110.010.001.001b of the D-Mem.

Following the steps described in Section 5.3, Obtaining the list of locations to be read, the list of locations to be read in the block containing the hit-address are shown in Table 13 (in gray).

Table 15. List of locations read on block 001b

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
0	001	101	13	5	3	9	11	1	7	15	001	Complementary address
0	110	010		▨	▨			▨	▨		001	DecC combination
1	000	010			▨	▨	▨	▨			001	DecB combination
1	001	010	▨		▨			▨		▨	001	DecB combination
1	010	010		▨	▨			▨	▨		001	DecB combination
1	011	010			▨	▨	▨	▨			001	DecB combination
1	100	010	▨		▨			▨			001	DecB combination
1	101	010		▨	▨			▨	▨		001	DecB combination
1	110	000			▨	▨	▨	▨			001	DecA combination
1	110	001	▨		▨			▨			001	DecA combination
1	110	010	14	6	4	10	12	2	8	16	001	Ah : victim address (red cell)
1	110	011			▨	▨	▨	▨			001	DecA combination
1	110	100		▨	▨			▨	▨	▨	001	DecA combination
1	110	101	▨		▨			▨			001	DecA combination
1	110	110			▨	▨	▨	▨			001	DecA combination
1	110	111		▨	▨			▨	▨		001	DecA combination
1	111	010	▨		▨			▨	▨	▨	001	DecB combination

Additional reads must be added considering the other memory blocks.

First step is to add in the list above some reads considering the complementary block.

The same word-lines of the victim address, but considering the complementary block shall be read in a specific order[1] as shown in Table 16 (blue cells).

Table 16. Reads related to complementary block

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
0	001	101	19	7	4	13	16	1	10	22	001	Complementary address
0	110	010		▨	▨			▨	▨		001	DecC combination
1	000	010			▨	▨	▨	▨			001	DecB combination
1	001	010	▨		▨			▨		▨	001	DecB combination
1	010	010		▨	▨			▨	▨		001	DecB combination
1	011	010			▨	▨	▨	▨			001	DecB combination

[1] The procedure to find the requested order is the same used to obtain the order for the complementary word-line in section 5.3

Table 16. Reads related to complementary block (continued)

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
1	100	010	▨		▨			▨			001	DecB combination
1	101	010		▨	▨			▨	▨		001	DecB combination
1	110	000			▨	▨	▨	▨			001	DecA combination
1	110	001	▨		▨			▨		▨	001	DecA combination
1	110	010	20	8	5	14	17	2	11	23	001	Ah : victim address (red cell)
1	110	010	21	9	6	15	18	3	12	24	110	Complementary address
1	110	011			▨	▨	▨	▨			001	DecA combination
1	110	100		▨	▨			▨	▨	▨	001	DecA combination
1	110	101	▨		▨			▨			001	DecA combination
1	110	110			▨	▨	▨	▨			001	DecA combination
1	110	111		▨	▨			▨	▨		001	DecA combination
1	111	010	▨		▨				▨	▨	001	DecB combination

The second step considers all other blocks. At least 4 reads shall be done on the same word-line of the victim address, but considering other blocks (blue cells in Table 17). No specific read order is required.

Table 17. Reading same word-line, but different blocks

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
0	001	101	19	7	4	13	16	1	10	22	001	Complementary address
0	110	010		▨	▨			▨	▨		001	DecC combination
1	000	010			▨	▨	▨	▨			001	DecB combination
1	001	010	▨		▨			▨		▨	001	DecB combination
1	010	010		▨	▨			▨	▨		001	DecB combination
1	011	010			▨	▨	▨	▨			001	DecB combination
1	100	010	▨		▨			▨			001	DecB combination
1	101	010		▨	▨			▨	▨		001	DecB combination
1	110	000			▨	▨	▨	▨			001	DecA combination
1	110	010	🟦		🟦			🟦		🟦	001	DecA combination
1	110	010		🟦		🟦	🟦		🟦		000	Block combination
1	110	010	20	8	5	14	17	2	11	23	001	Ah : victim address (red cell)
1	110	010	🟦		🟦			🟦		▨	010	Block combination
1	110	010		🟦		🟦	🟦		🟦		011	Block combination
1	110	010	🟦		🟦			🟦		🟦	100	Block combination

Table 17. Reading same word-line, but different blocks (continued)

			DecE									
DecC	DecB	DecA	000	001	010	011	100	101	110	111	Block	Description
1	110	010		🟦		🟦	🟦		🟦		101	Block combination
1	110	010	21	9	6	15	18	3	12	24	110	Complementary address
1	110	010	▨		▨			▨		▨	111	Block combination
1	110	011			▨	▨	▨	▨			001	DecA combination
1	110	100		▨	▨			▨	▨	▨	001	DecA combination
1	110	101	▨		▨			▨			001	DecA combination
1	110	110			▨	▨	▨	▨			001	DecA combination
1	110	111		▨	▨			▨	▨		001	DecA combination
1	111	010	▨		▨				▨	▨	001	DecB combination

Table 18 shows the final list of locations which are required to be read in case of memory implementing the block decoding.

Table 18. Final list of locations which shall be read including the order in case of memory with block decoding

			DecE									
DecC	DecB	DecA	000	001	010	011	100	101	110	111	Block	Description
0	001	101	19	7	4	13	16	1	10	22	001	Complementary address
0	110	010		▨	▨			▨	▨		001	DecC combination
1	000	010			▨	▨	▨	▨			001	DecB combination
1	001	010	▨		▨			▨		▨	001	DecB combination
1	010	010		▨	▨			▨	▨		001	DecB combination
1	011	010			▨	▨	▨	▨			001	DecB combination
1	100	010	▨		▨			▨			001	DecB combination
1	101	010		▨	▨			▨	▨		001	DecB combination
1	110	000			▨	▨	▨	▨			001	DecA combination
1	110	010	▨		▨			▨		▨	001	DecA combination
1	110	010		▨		▨	▨		▨		000	Block combination
1	110	010	20	8	5	14	17	2	11	23	001	Ah : victim address (red cell)
1	110	010	▨		▨			▨		▨	010	Block combination
1	110	010		▨		▨	▨		▨		011	Block combination
1	110	010	▨		▨			▨		▨	100	Block combination
1	110	010		▨		▨	▨		▨		101	Block combination
1	110	010	21	9	6	15	18	3	12	24	110	Complementary address
1	110	010	▨		▨			▨		▨	111	Block combination

Table 18. Final list of locations which shall be read including the order in case of memory with block decoding (continued)

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
1	110	011			▨	▨	▨	▨			001	DecA combination
1	110	100		▨	▨			▨	▨	▨	001	DecA combination
1	110	101	▨		▨			▨			001	DecA combination
1	110	110			▨	▨	▨	▨			001	DecA combination
1	110	111		▨	▨			▨	▨		001	DecA combination
1	111	010	▨		▨				▨	▨	001	DecB combination

5.4 Test result

Let’s recap the needed steps to perform the test and to analyze the result:

1. A single bit error correction is triggered at the address Ah.
2. Starting from this address and from the RAM architecture, the user shall gather a list of memory locations which shall be read (for example, greyed cells in Table 12 or Table 16).
3. These locations shall be read to verify if any additional single/double bit error is triggered.

This self-test detects a potential permanent RAM addressing failure if one of the following conditions appears while reading selected RAM locations:

- a not correctable error bit is detected, or
- multiple single bit errors are detected by the ECC logic and the number of these errors is bigger than the buffer depth of the MEMU, or
- more than a single bit error are detected on different words of the same word-line (more details on such a case on section 5.4.1).

As described above additional SBE can be detected by the ECC while the software test runs. In this case additional iteration of the software test shall be executed considering this new SBE as new hitting address.

5.4.1 Multiple single bit error in the same word-line

A Single Event Effect (SEE) in RAM can cause single bit upset on multiple adjacent words (for example, Multiple Cell Upset (MCU)).

MCU causes SBEs on different words of the same word-line. In this case, an additional software step is needed to distinguish between:

- a MCU event, or
- a permanent fault affecting the address decoders.

Additional memory locations shall be read to discriminate between either case above.

Table 19. Additional cells shall be read in case of multiple SBEs in same word-line

			DecE									
DecC	**DecB**	**DecA**	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**	**Block**	**Description**
0	001	010	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	001	Complementary address
0	110	101	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	001	Complementary address
0	001	101						🟨			001	Ah : complementary address
1	110	010	▨	▨	🟥	▨	▨	▨	▨	▨	001	Ah : victim address (red cell)

These locations are showed in blue in Table 19. The procedure to gather these locations is described below. Let’s assume multiple locations of the Ah word-line trigger the ECC:

1. Complementary address, i.e. Ac, shall be obtained.
2. 3-to-8 address decoders are consider, i.e. in such example DecB and DecA
3. The user shall consider the complementary of DecA and DecB from the Ac to obtain additional word-lines to be read (blue word-line in Table 19).

If multiple SEC are detected while reading these additional word-lines, there is a high probability they are all the result of addressing fault.

6 Testing All-X in RAM

6.1 Candidate address for testing All-X issue

This section describes a Perl script which can be used for finding a candidate address for testing All-X in the RAMs. Some examples of usage of the script are provided.

```
#--- start Perl script ---:
: # -*- perl -*-
eval 'exec perl -w -S $0 ${1+"$@"}'
      if 0;
use strict;
my $base = hex($ARGV[0]);
my $num_to_find = ($#ARGV > 0) ? $ARGV[1] : 1;
my $all0_found = 0;
my $all1_found = 0;
my $guesses = 0;
my $addr = $base;
my $ecc;
my $bit_count;

printf "RAM base address = 0x%08x\n", $base;
printf "  All 0s - Addresses with two bits set in the address ECC contribution:\n";

while(($guesses < 131072) && ($all0_found < $num_to_find)) {
      $ecc = get_ecc($addr, 0, 0);
      $bit_count = count_ones($ecc);
      if($bit_count == 2) {
      $all0_found++;
      printf "    (%d) addr = 0x%08x, addr_ecc = 0x%02x\n", $all0_found, $addr, $ecc;
      }
$addr += 8;
$guesses++;
}

printf "\n  All 1s - Addresses with two bits cleared in the address ECC contribution:\n";

$addr = $base;
while(($guesses < 131072) && ($all1_found < $num_to_find)) {
      $ecc = get_ecc($addr, 0xffffffff, 0xffffffff);
      $bit_count = count_zeroes($ecc);
      if($bit_count == 2) {
          $all1_found++;
          printf "    (%d) addr = 0x%08x, addr_ecc = 0x%02x\n", $all1_found, $addr, $ecc;
      }
      $addr += 8;
      $guesses++;
}

sub count_ones {
      my $string = sprintf("%08b", shift);
      my $count = 0;
      my $i;
      for($i=0; $i<8; $i++) {
          if(substr($string, $i, 1) eq "1") {
               $count++;
          }
      }
      return($count);
}

sub count_zeroes {
      my $string = sprintf("%08b", shift);
      my $count = 0;
      my $i;
      for($i=0; $i<8; $i++) {
          if(substr($string, $i, 1) eq "0") {
              $count++;
          }
      }
      return($count);
}

sub get_ecc {
      my $addr = shift;
      my $data_be0 = shift;
      my $data_be1 = shift;

      my @addrx8;
      my @data_bex8;
      my @data_lex8;
      my $i;
      my $j;
      my $bit;

      for($i=3; $i<32; $i++) {
          $bit = ($addr >> $i) & 1;
          $addrx8[$i]  = $bit;
          $addrx8[$i] |= $bit << 1;
          $addrx8[$i] |= $bit << 2;
          $addrx8[$i] |= $bit << 3;
          $addrx8[$i] |= $bit << 4;
          $addrx8[$i] |= $bit << 5;
          $addrx8[$i] |= $bit << 6;
          $addrx8[$i] |= $bit << 7;
      }

      for($i=0; $i<64; $i++) {
          if($i < 32) {
          $bit = ($data_be1 >> $i) & 1;
          } else {
              $bit = ($data_be0 >> ($i-32)) & 1;
          }

          $data_bex8[$i]  = $bit;
          $data_bex8[$i] |= $bit << 1;
          $data_bex8[$i] |= $bit << 2;
          $data_bex8[$i] |= $bit << 3;
          $data_bex8[$i] |= $bit << 4;
          $data_bex8[$i] |= $bit << 5;
          $data_bex8[$i] |= $bit << 6;
          $data_bex8[$i] |= $bit << 7;
      }
```

```
for($i=0; $i<8; $i++) {
    for($j=0; $j<8; $j++) {
        $data_lex8[$i*8+$j] = $data_bex8[(7-$i)*8+$j];
    }
}



my $addr_ecc
    = (0x1f & $addrx8[31])
    ^ (0xf4 & $addrx8[30])
    ^ (0x3b & $addrx8[29])
    ^ (0xe3 & $addrx8[28])
    ^ (0x5d & $addrx8[27])
    ^ (0xda & $addrx8[26])
    ^ (0x6e & $addrx8[25])
    ^ (0xb5 & $addrx8[24])
    ^ (0x8f & $addrx8[23])
    ^ (0xd6 & $addrx8[22])
    ^ (0x79 & $addrx8[21])
    ^ (0xba & $addrx8[20])
    ^ (0x9b & $addrx8[19])
    ^ (0xe5 & $addrx8[18])
    ^ (0x57 & $addrx8[17])
    ^ (0xec & $addrx8[16])
    ^ (0xc7 & $addrx8[15])
    ^ (0xae & $addrx8[14])
    ^ (0x67 & $addrx8[13])
    ^ (0x9d & $addrx8[12])
    ^ (0x5b & $addrx8[11])
    ^ (0xe6 & $addrx8[10])
    ^ (0x3e & $addrx8[9])
    ^ (0xf1 & $addrx8[8])
    ^ (0xdc & $addrx8[7])
    ^ (0xe9 & $addrx8[6])
    ^ (0x3d & $addrx8[5])
    ^ (0xf2 & $addrx8[4])
    ^ (0x2f & $addrx8[3]);

my $addr_ecc_tcm
    = (0x1f & $addrx8[31])
    ^ (0xf4 & $addrx8[30])
    ^ (0x3b & $addrx8[29])
    ^ (0xe3 & $addrx8[28])
    ^ (0x5d & $addrx8[27])
    ^ (0xda & $addrx8[26])
    ^ (0x6e & $addrx8[25])
    ^ (0xb5 & $addrx8[24])
    ^ (0x8f & $addrx8[23])
    ^ (0xd6 & $addrx8[22])
    ^ (0x79 & $addrx8[21])
    ^ (0xba & $addrx8[20])
    ^ (0x9b & $addrx8[19])
    ^ (0xe5 & $addrx8[18])
    ^ (0x57 & $addrx8[17])
    ^ (0xec & $addrx8[16]);
```

```
my $ecc_tcm_fix
     = (0xc7 & $addrx8[15])
     ^ (0xae & $addrx8[14])
     ^ (0x67 & $addrx8[13])
     ^ (0x9d & $addrx8[12])
     ^ (0x5b & $addrx8[11])
     ^ (0xe6 & $addrx8[10])
     ^ (0x3e & $addrx8[9])
     ^ (0xf1 & $addrx8[8])
     ^ (0xdc & $addrx8[7])
     ^ (0xe9 & $addrx8[6])
     ^ (0x3d & $addrx8[5])
     ^ (0xf2 & $addrx8[4])
     ^ (0x2f & $addrx8[3]);

my $data_ecc
     = (0xb0 & $data_lex8[63])
     ^ (0x23 & $data_lex8[62])
     ^ (0x70 & $data_lex8[61])
     ^ (0x62 & $data_lex8[60])
     ^ (0x85 & $data_lex8[59])
     ^ (0x13 & $data_lex8[58])
     ^ (0x45 & $data_lex8[57])
     ^ (0x52 & $data_lex8[56])

     ^ (0x2a & $data_lex8[55])
     ^ (0x8a & $data_lex8[54])
     ^ (0x0b & $data_lex8[53])
     ^ (0x0e & $data_lex8[52])
     ^ (0xf8 & $data_lex8[51])
     ^ (0x25 & $data_lex8[50])
     ^ (0xd9 & $data_lex8[49])
     ^ (0xa1 & $data_lex8[48])

     ^ (0x54 & $data_lex8[47])
     ^ (0xa7 & $data_lex8[46])
     ^ (0xa8 & $data_lex8[45])
     ^ (0x92 & $data_lex8[44])
     ^ (0xc8 & $data_lex8[43])
     ^ (0x07 & $data_lex8[42])
     ^ (0x34 & $data_lex8[41])
     ^ (0x32 & $data_lex8[40])

     ^ (0x68 & $data_lex8[39])
     ^ (0x89 & $data_lex8[38])
     ^ (0x98 & $data_lex8[37])
     ^ (0x49 & $data_lex8[36])
     ^ (0x61 & $data_lex8[35])
     ^ (0x86 & $data_lex8[34])
     ^ (0x91 & $data_lex8[33])
     ^ (0x46 & $data_lex8[32])

     ^ (0x58 & $data_lex8[31])
     ^ (0x4f & $data_lex8[30])
     ^ (0x38 & $data_lex8[29])
     ^ (0x75 & $data_lex8[28])
```

```
          ^ (0xc4 & $data_lex8[27])
          ^ (0x0d & $data_lex8[26])
          ^ (0xa4 & $data_lex8[25])
          ^ (0x37 & $data_lex8[24])

          ^ (0x64 & $data_lex8[23])
          ^ (0x16 & $data_lex8[22])
          ^ (0x94 & $data_lex8[21])
          ^ (0x29 & $data_lex8[20])
          ^ (0xea & $data_lex8[19])
          ^ (0x26 & $data_lex8[18])
          ^ (0x1a & $data_lex8[17])
          ^ (0x19 & $data_lex8[16])

          ^ (0xd0 & $data_lex8[15])
          ^ (0xc2 & $data_lex8[14])
          ^ (0x2c & $data_lex8[13])
          ^ (0x51 & $data_lex8[12])
          ^ (0xe0 & $data_lex8[11])
          ^ (0xa2 & $data_lex8[10])
          ^ (0x1c & $data_lex8[9])
          ^ (0x31 & $data_lex8[8])


          ^ (0x8c & $data_lex8[7])
          ^ (0x4a & $data_lex8[6])
          ^ (0x4c & $data_lex8[5])
          ^ (0x15 & $data_lex8[4])
          ^ (0x83 & $data_lex8[3])
          ^ (0x9e & $data_lex8[2])
          ^ (0x43 & $data_lex8[1])
          ^ (0xc1 & $data_lex8[0]);

      my $ecc       = $data_ecc ^ $addr_ecc;
      my $ecc_tcm   = $data_ecc ^ $addr_ecc ^ $addr_ecc_tcm ^ 0x55;
      my $ecc_flash = $data_ecc ^ 0xff;
      return($ecc);
}

##printf "addr        = 0x%08x\n", $addr;
##printf "data_be     = 0x%08x_%08x\n", $data_be0, $data_be1;
##printf "addr_ecc    = 0x%02x\n", $addr_ecc;
##printf "data_ecc    = 0x%02x\n", $data_ecc;
##printf "ecc         = 0x%02x\n", $ecc;
##printf "ecc_tcm     = 0x%02x\n", $ecc_tcm;
##printf "ecc_tcm_fix = 0x%02x\n", $ecc_tcm_fix;
##printf "ecc_flash   = 0x%02x\n", $ecc_flash;
#----- end per script -----
```

This script finds the first N addresses with 2 bits set and 2 bits cleared in the address ECC contribution. Usage is as follows:

- find_allx_addr address [number]
- address – starting address to start searching from
- number – number of addresses to find, default is 1

Example:

1. Find the first address of each type for system RAM:
   — ./find_allx_addr 40000000h

RAM base address = 40000000h

All 0s - Addresses with two bits set in the address ECC contribution:

- addr = 40000010h, addr_ecc = 06h

All 1s - Addresses with two bits cleared in the address ECC contribution:

1. addr = 40000008h, addr_ecc = DBh
2. Find the first 5 addresses of each type for system RAM:
   — ./find_allx_addr 40000000 5

RAM base address = 40000000h

All 0s - Addresses with two bits set in the address ECC contribution:

1. addr = 40000010h, addr_ecc = 06h
2. addr = 40000038h, addr_ecc = 14h
3. addr = 40000058h, addr_ecc = C0h
4. addr = 40000080h, addr_ecc = 28h
5. addr = 400000F8h, addr_ecc = 21h

All 1s - Addresses with two bits cleared in the address ECC contribution:

1. addr = 40000008h, addr_ecc = DBh
2. addr = 40000098h, addr_ecc = F5h
3. addr = 400000B0h, addr_ecc = E7h
4. addr = 400000C8h, addr_ecc = EEh
5. addr = 400000E0h, addr_ecc = FCh

6.2 ECC checkbit/syndrome coding scheme

The E2E ECC scheme implements a single-error correction, double-error detection (SECDED) code using the so-called Hsiao odd-weight column criteria. These codes are named for M.Y. Hsiao, an IBM researcher who published extensively in the early 1970s on SECDED codes better suited for implementation in protecting (mainframe) computer memories than traditional Hamming codes.

The Hsiao codes are Hamming distance 4 implementations which provide the SECDED capabilities. The minimum odd-weight constraints defined by Hsiao are relatively simple in the resulting implementation of the parity check H matrix which defines the association between the data (and address) bits and the checkbits. They are:

1. There are no all zeroes columns.
2. Every column is distinct.
3. Every column contains an odd number of ones, and hence is “odd weight”.

In defining the H-matrix for this family of devices, these requirements from Hsiao were applied. Additionally, there are a variety of ECC codeword requirements associated with specific functional requirements associated with the flash memory that further dictated the specific column definitions. In any case, the resulting ECC is organized based on 64 data bits plus 29 address bits (the upper bits of the 32-bit address field minus the 3 bits which select the byte within 64-bit (8-byte) data field.

The basic H-matrix for this (101, 93) code (93 is the total number of “data” bits, 101 is the total number of data bits (93) plus 8 checkbits) is shown in Table 20. A ‘*’ in Table 20 indicates the corresponding data or address bit is XOR’d to form the final checkbit value on the left. For 64-bit data writes, the table sections corresponding to D[63:32], D[31:0], and A[31:3] are logically summed (output of each table section is XOR’ed) together to the final value driven on the hwchkbit[7:0] outputs. Note that this table uses *the AHB bit numbering convention where bit[0] is the least significant bit*.

Table 20. E2E ECC basic H-matrix definition

Checkbits [7:0]	Data Bit[1]																															
	Byte 7								Byte 6								Byte 5								Byte 4							
	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
7	*				*					*			*		*	*		*	*	*	*					*	*			*	*	
6			*	*			*	*					*		*		*				*				*			*	*			*
5	*	*	*	*					*				*	*		*		*	*				*	*	*				*			
4	*		*			*		*					*		*		*			*			*	*			*				*	
3									*	*	*	*	*		*				*		*				*	*	*	*				
2					*		*					*		*			*	*				*	*							*		*
1		*		*		*		*	*	*	*	*						*		*		*		*						*		*
0		*			*	*	*				*			*	*	*		*				*				*		*	*		*	
	Byte 3								Byte 2								Byte 1								Byte 0							
Checkbits [7:0]	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
7					*		*				*		*				*	*			*	*			*				*	*		*
6	*	*		*	*				*				*				*	*		*	*					*	*				*	*
5			*	*			*	*	*			*	*	*					*		*	*		*								
4	*		*	*				*		*	*				*	*	*			*			*	*				*		*		
3	*	*	*			*						*	*		*	*			*				*		*	*	*			*		
2		*		*	*	*	*	*	*	*	*			*					*				*		*		*	*		*		
1		*						*		*			*	*	*			*				*				*			*	*	*	
0		*		*		*		*				*				*				*				*				*	*		*	*
Checkbits [7:0]	Address Bit[1]																															
	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3			
7		*		*		*		*	*	*		*	*	*		*	*	*		*		*		*	*	*		*				
6		*		*	*	*	*			*	*			*	*	*	*		*		*	*		*	*	*		*				
5		*	*	*			*	*			*	*		*		*		*	*			*	*	*		*	*	*	*			
4	*	*	*		*	*		*		*	*	*	*		*					*	*		*	*	*		*	*				
3	*		*		*	*	*		*		*	*	*			*		*		*	*		*		*	*	*		*			
2	*	*			*		*	*	*	*				*	*	*	*	*	*	*		*	*		*		*		*			
1	*		*	*		*	*		*	*		*	*		*		*	*	*		*	*	*					*	*			
0	*		*	*	*			*	*		*		*	*	*		*		*	*	*			*		*	*		*			

NOTES:
[1] Bit numbering is AHB convention, bit 0 is LSB. D[7:0] corresponds to byte at address 0. D[63:56] corresponds to byte at address 7.

Figure 5 shows an alternative representation of the ECC encode process, written as a C language function.

Figure 5. C Language encodeECC function description

```
encodeEcc (addr, data_a2_is_zero, data_a2_is_one)
    unsigned int        addr;                   /* 32-bit byte address */
    unsigned int        data_a2_is_zero;        /* 32-bit data lower, a[2]=0 */
    unsigned int        data_a2_is_one;         /* 32-bit data upper, a[2]=1 */

{
    unsigned int        addr_ecc;               /* 8 bits of ecc for address */
    unsigned int        ecc;                    /* 8 bits of ecc codeword */

    /* the following equation calculates the 8-bit wide ecc codeword by examining
    each addr or data bits and xor'ing the appropriate H-matrix value if the bit = 1 */

    addr_ecc
        = (((addr            >> 31) & 1) ? 0x1f : 0x0)      /* addr[31] */
        ^ (((addr            >> 30) & 1) ? 0xf4 : 0x0)      /* addr[30] */
        ^ (((addr            >> 29) & 1) ? 0x3b : 0x0)      /* addr[29] */
        ^ (((addr            >> 28) & 1) ? 0xe3 : 0x0)      /* addr[28] */
        ^ (((addr            >> 27) & 1) ? 0x5d : 0x0)      /* addr[27] */
        ^ (((addr            >> 26) & 1) ? 0xda : 0x0)      /* addr[26] */
        ^ (((addr            >> 25) & 1) ? 0x6e : 0x0)      /* addr[25] */
        ^ (((addr            >> 24) & 1) ? 0xb5 : 0x0)      /* addr[24] */

        ^ (((addr            >> 23) & 1) ? 0x8f : 0x0)      /* addr[23] */
        ^ (((addr            >> 22) & 1) ? 0xd6 : 0x0)      /* addr[22] */
        ^ (((addr            >> 21) & 1) ? 0x79 : 0x0)      /* addr[21] */
        ^ (((addr            >> 20) & 1) ? 0xba : 0x0)      /* addr[20] */
        ^ (((addr            >> 19) & 1) ? 0x9b : 0x0)      /* addr[19] */
        ^ (((addr            >> 18) & 1) ? 0xe5 : 0x0)      /* addr[18] */
        ^ (((addr            >> 17) & 1) ? 0x57 : 0x0)      /* addr[17] */
        ^ (((addr            >> 16) & 1) ? 0xec : 0x0)      /* addr[16] */

        ^ (((addr            >> 15) & 1) ? 0xc7 : 0x0)      /* addr[15] */
        ^ (((addr            >> 14) & 1) ? 0xae : 0x0)      /* addr[14] */
        ^ (((addr            >> 13) & 1) ? 0x67 : 0x0)      /* addr[13] */
        ^ (((addr            >> 12) & 1) ? 0x9d : 0x0)      /* addr[12] */
        ^ (((addr            >> 11) & 1) ? 0x5b : 0x0)      /* addr[11] */
        ^ (((addr            >> 10) & 1) ? 0xe6 : 0x0)      /* addr[10] */
        ^ (((addr            >>  9) & 1) ? 0x3e : 0x0)      /* addr[ 9] */
        ^ (((addr            >>  8) & 1) ? 0xf1 : 0x0)      /* addr[ 8] */

        ^ (((addr            >>  7) & 1) ? 0xdc : 0x0)      /* addr[ 7] */
        ^ (((addr            >>  6) & 1) ? 0xe9 : 0x0)      /* addr[ 6] */
        ^ (((addr            >>  5) & 1) ? 0x3d : 0x0)      /* addr[ 5] */
        ^ (((addr            >>  4) & 1) ? 0xf2 : 0x0)      /* addr[ 4] */
        ^ (((addr            >>  3) & 1) ? 0x2f : 0x0);     /* addr[ 3] */

    ecc = (((data_a2_is_zero >> 31) & 1) ? 0xb0 : 0x0)      /* data[63] */
        ^ (((data_a2_is_zero >> 30) & 1) ? 0x23 : 0x0)      /* data[62] */
        ^ (((data_a2_is_zero >> 29) & 1) ? 0x70 : 0x0)      /* data[61] */
        ^ (((data_a2_is_zero >> 28) & 1) ? 0x62 : 0x0)      /* data[60] */
        ^ (((data_a2_is_zero >> 27) & 1) ? 0x85 : 0x0)      /* data[59] */
        ^ (((data_a2_is_zero >> 26) & 1) ? 0x13 : 0x0)      /* data[58] */
        ^ (((data_a2_is_zero >> 25) & 1) ? 0x45 : 0x0)      /* data[57] */
        ^ (((data_a2_is_zero >> 24) & 1) ? 0x52 : 0x0)      /* data[56] */

        ^ (((data_a2_is_zero >> 23) & 1) ? 0x2a : 0x0)      /* data[55] */
        ^ (((data_a2_is_zero >> 22) & 1) ? 0x8a : 0x0)      /* data[54] */
        ^ (((data_a2_is_zero >> 21) & 1) ? 0x0b : 0x0)      /* data[53] */
        ^ (((data_a2_is_zero >> 20) & 1) ? 0x0e : 0x0)      /* data[52] */
        ^ (((data_a2_is_zero >> 19) & 1) ? 0xf8 : 0x0)      /* data[51] */
        ^ (((data_a2_is_zero >> 18) & 1) ? 0x25 : 0x0)      /* data[50] */
        ^ (((data_a2_is_zero >> 17) & 1) ? 0xd9 : 0x0)      /* data[49] */
        ^ (((data_a2_is_zero >> 16) & 1) ? 0xa1 : 0x0)      /* data[48] */

        ^ (((data_a2_is_zero >> 15) & 1) ? 0x54 : 0x0)      /* data[47] */
        ^ (((data_a2_is_zero >> 14) & 1) ? 0xa7 : 0x0)      /* data[46] */
        ^ (((data_a2_is_zero >> 13) & 1) ? 0xa8 : 0x0)      /* data[45] */
        ^ (((data_a2_is_zero >> 12) & 1) ? 0x92 : 0x0)      /* data[44] */
        ^ (((data_a2_is_zero >> 11) & 1) ? 0xc8 : 0x0)      /* data[43] */
        ^ (((data_a2_is_zero >> 10) & 1) ? 0x07 : 0x0)      /* data[42] */
        ^ (((data_a2_is_zero >>  9) & 1) ? 0x34 : 0x0)      /* data[41] */
        ^ (((data_a2_is_zero >>  8) & 1) ? 0x32 : 0x0)      /* data[40] */

        ^ (((data_a2_is_zero >>  7) & 1) ? 0x68 : 0x0)      /* data[39] */
        ^ (((data_a2_is_zero >>  6) & 1) ? 0x89 : 0x0)      /* data[38] */
        ^ (((data_a2_is_zero >>  5) & 1) ? 0x98 : 0x0)      /* data[37] */
        ^ (((data_a2_is_zero >>  4) & 1) ? 0x49 : 0x0)      /* data[36] */
        ^ (((data_a2_is_zero >>  3) & 1) ? 0x61 : 0x0)      /* data[35] */
        ^ (((data_a2_is_zero >>  2) & 1) ? 0x86 : 0x0)      /* data[34] */
        ^ (((data_a2_is_zero >>  1) & 1) ? 0x91 : 0x0)      /* data[33] */
        ^  ((data_a2_is_zero        & 1) ? 0x46 : 0x0)      /* data[32] */

        ^ (((data_a2_is_one  >> 31) & 1) ? 0x58 : 0x0)      /* data[31] */
        ^ (((data_a2_is_one  >> 30) & 1) ? 0x4f : 0x0)      /* data[30] */
        ^ (((data_a2_is_one  >> 29) & 1) ? 0x38 : 0x0)      /* data[29] */
        ^ (((data_a2_is_one  >> 28) & 1) ? 0x75 : 0x0)      /* data[28] */
        ^ (((data_a2_is_one  >> 27) & 1) ? 0xc4 : 0x0)      /* data[27] */
        ^ (((data_a2_is_one  >> 26) & 1) ? 0x0d : 0x0)      /* data[26] */
        ^ (((data_a2_is_one  >> 25) & 1) ? 0xa4 : 0x0)      /* data[25] */
        ^ (((data_a2_is_one  >> 24) & 1) ? 0x37 : 0x0)      /* data[24] */

        ^ (((data_a2_is_one  >> 23) & 1) ? 0x64 : 0x0)      /* data[23] */
        ^ (((data_a2_is_one  >> 22) & 1) ? 0x16 : 0x0)      /* data[22] */
        ^ (((data_a2_is_one  >> 21) & 1) ? 0x94 : 0x0)      /* data[21] */
        ^ (((data_a2_is_one  >> 20) & 1) ? 0x29 : 0x0)      /* data[20] */
        ^ (((data_a2_is_one  >> 19) & 1) ? 0xea : 0x0)      /* data[19] */
        ^ (((data_a2_is_one  >> 18) & 1) ? 0x26 : 0x0)      /* data[18] */
        ^ (((data_a2_is_one  >> 17) & 1) ? 0x1a : 0x0)      /* data[17] */
        ^ (((data_a2_is_one  >> 16) & 1) ? 0x19 : 0x0)      /* data[16] */

        ^ (((data_a2_is_one  >> 15) & 1) ? 0xd0 : 0x0)      /* data[15] */
        ^ (((data_a2_is_one  >> 14) & 1) ? 0xc2 : 0x0)      /* data[14] */
        ^ (((data_a2_is_one  >> 13) & 1) ? 0x2c : 0x0)      /* data[13] */
        ^ (((data_a2_is_one  >> 12) & 1) ? 0x51 : 0x0)      /* data[12] */
        ^ (((data_a2_is_one  >> 11) & 1) ? 0xe0 : 0x0)      /* data[11] */
        ^ (((data_a2_is_one  >> 10) & 1) ? 0xa2 : 0x0)      /* data[10] */
        ^ (((data_a2_is_one  >>  9) & 1) ? 0x1c : 0x0)       /* data[ 9] */
        ^ (((data_a2_is_one  >>  8) & 1) ? 0x31 : 0x0)       /* data[ 8] */

        ^ (((data_a2_is_one  >>  7) & 1) ? 0x8c : 0x0)       /* data[ 7] */
        ^ (((data_a2_is_one  >>  6) & 1) ? 0x4a : 0x0)       /* data[ 6] */
        ^ (((data_a2_is_one  >>  5) & 1) ? 0x4c : 0x0)       /* data[ 5] */
        ^ (((data_a2_is_one  >>  4) & 1) ? 0x15 : 0x0)       /* data[ 4] */
        ^ (((data_a2_is_one  >>  3) & 1) ? 0x83 : 0x0)       /* data[ 3] */
        ^ (((data_a2_is_one  >>  2) & 1) ? 0x9e : 0x0)       /* data[ 2] */
        ^ (((data_a2_is_one  >>  1) & 1) ? 0x43 : 0x0)       /* data[ 1] */
        ^  ((data_a2_is_one         & 1) ? 0xc1 : 0x0);      /* data[ 0] */

    ecc = ecc ^ addr_ecc;   /* combine data and addr ecc values */

    return(ecc);
}
```

On a memory read operation, the E2E ECC logic performs the same type of optional adjustment on the read checkbits.

As the ECC syndrome is calculated on a read operation by applying the H-matrix to the data plus the checkbits, an all zero syndrome indicates an error free operation. If the generated syndrome value is non-zero and matches one of the H-matrix values associated with the data or checkbits, it represents a single-bit error correction case and the specific bit is complemented to produce the correct data value. If the syndrome value matches one of the H-matrix values associated with the address bits, or is an even weight value, or represents an unused odd weight value, a non-correctable ECC event has been detected and the appropriate error termination response is initiated.

The preceding discussion has provided a generic overview of the end-to-end ECC strategy implemented in this family of automotive MCUs.

7 Further information

7.1 Conventions and terminology

Table 21 shows the list of conventions for this document.

Table 21. List of conventions and terminology

Convention	Description
error	Discrepancy between a computed, observed, or measured value or condition and the true, specified or theoretically correct value or condition.
fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
failure	The termination of the ability of a functional unit to perform a required function.

7.2 Acronyms and abbreviations

A short list of acronyms and abbreviations used in this document is shown in Table 22.

Table 22. Acronyms and abbreviations

Terms	Meanings
ADC	Analog to Digital Converter
BAF	Boot Assist Flash
BAR	Boot Assist ROM
CCF	Common Cause Failure
CMU	Clock Monitor Unit
CRC	Cyclic Redundancy Check
CTU	Cross-Triggering Unit
DC	Diagnostic Coverage
ECC	Error Correcting Code
DMA	Direct Memory Access
ERRM	Error Out Monitor function
EXWD	External Watchdog function
FCCU	Fault Collection and Control Unit
FMEDA	Failure Modes, Effects & Diagnostic Analysis
FMPLL	Frequency-Modulated Phase-Locked Loop
GPIO	General Purpose Input/Output
LBIST	Logic Built-In Self-test
MBIST	Memory Built-In Self-test
MC_CGM	Clock Generation Module
MC_ME	Mode Entry
MCU	Microcontroller Unit
MPU	Memory Protection Unit
NCF	Non-Critical Fault
NMI	Non-Maskable Interrupt
NVM	Non-Volatile Memory
PMU	Power Management Unit
PSM	Power Supply and Monitor function
PST	Process Safety Time
RCCU	Redundancy Control Checking Unit
MC_RGM	Reset Generation Module
SM	Safety Manual
SIL	Safety Integrity Level
SSCM	System Status and Control Module
SWG	Sine Wave Generator
SWT	Software Watchdog Timer

8 Document revision history

Table 23 summarizes revisions to this document.

Table 23. Revision history

Revision	Date	Description of changes
1	15 Jan 2015	Initial release.
1.1	10 Apr 2017	Converted the document to use NXP branding.

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customers technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, AltiVec, C-5, CodeTest, CodeWarrior, ColdFire, ColdFire+, C-Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. ARM, AMBA, ARM Powered, Artisan, Cortex, Jazelle, Keil, SecurCore, Thumb, TrustZone, and ìVision are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ARM7, ARM9, ARM11, big.LITTLE, CoreLink, CoreSight, DesignStart, Mali, mbed, NEON, POP, Sensinode, Socrates, ULINK and Versatile are trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

Document Number: MPC5777M_GMSM
Rev. 1.1
10 Apr 2017