Technical White Paper

Functional Safety Support for Arm®-based Microcontrollers and Processors

Neelima Muralidharan, Michael Firth, Kathryn Kalouf *Catalog Processors*

ABSTRACT

This white paper provides an introduction to functional safety concepts such as the hazard analysis and risk assessment, SIL and ASIL levels, random versus systematic faults, and safety element out of context. The paper also provides examples of how the AM243x MCU and AM64x processor series support functional safety through the integration of a safety MCU and the use of safety diagnostics.

Table of Contents

List of Figures

List of Tables

1 Functional Safety Goals

A functional safety goal is a system-level objective to reduce the risk of potentially hazardous events. The key word here is *reduce*. There is always a degree of risk and the objective of the safety goal is to reduce the risk of harm to an acceptable level.

Safety goals are defined based on the end application, how the equipment is used, and how the operator interacts with the equipment. For example, the factory floor has many pieces of equipment that can harm a worker. An article of clothing can get caught on a machine and if the machine is not immediately stopped the worker can be injured. The safety goal in this example is to prevent harm to the operator by stopping the machine as soon as a person is detected within a preset distance of the machine. How the system integrator implements and supports this safety goal is called the safety concept. A common safety concept used to stop a motor or machine is called Safe Torque Off (STO) and can be implemented to support the safety goal in this example. (See the STO Concept and Evaluation report in Table 8-1 for details.)

2 Hazard Analysis and Risk Assessment

The first step in defining safety goals is for the system integrator to perform a Hazard Analysis and Risk Assessment (HARA). The HARA starts by identifying all potential hazards that can occur in the system. These hazards are then categorized based on a pre-defined set of criteria that assign a Safety Integrity Level (SIL) or Automotive Safety Integrity Level (ASIL) to each hazard. The assigned SIL or ASIL level defines the maximum acceptable occurrence rate of each hazard. Safety goals and safety concepts are then defined to mitigate the hazards and limit their occurrence to the target SIL or ASIL levels.

Figure 2-1 shows a graphical representation of the HARA and safety concept stages.

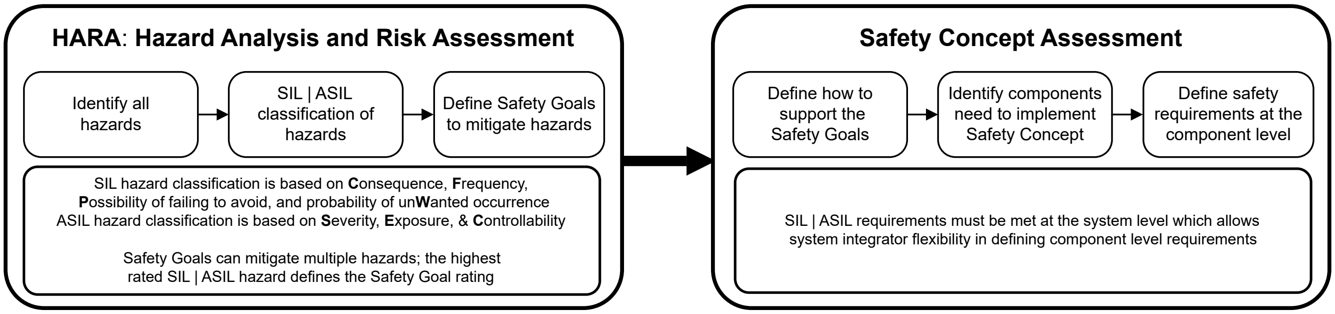

HARA: Hazard Analysis and Risk Assessment
Identify all hazards
SIL | ASIL classification of hazards
Define Safety Goals to mitigate hazards
SIL hazard classification is based on Consequence, Frequency, Possibility of failing to avoid, and probability of unWanted occurrence
ASIL hazard classification is based on Severity, Exposure, & Controllability
Safety Goals can mitigate multiple hazards; the highest rated SIL | ASIL hazard defines the Safety Goal rating
Safety Concept Assessment
Define how to support the Safety Goals
Identify components need to implement Safety Concept
Define safety requirements at the component level
SIL | ASIL requirements must be met at the system level which allows system integrator flexibility in defining component level requirements

Figure 2-1. HARA and Safety Concept Assessment Stages

3 SIL and ASIL Levels

During the HARA analysis, each of the identified hazards is categorized into one of four SIL | ASIL levels. The higher the SIL | ASIL level, the greater the risk of harm and therefore the greater the safety requirement. SIL levels are defined in IEC 61508 which is a functional safety standard applicable to many industries including industrial applications. ASIL levels are defined in the ISO 26262 standard and are automotive specific. The International Electrotechnical Commission (IEC) 61508 and ISO 26262 standards are similar in objectives, but do use different methodologies and safety metrics.

In IEC 61508, each hazard is classified in terms of **C**onsequence (4 levels), **F**requency and exposure time (2 levels), **P**ossibility of failing to avoid (2 levels) and Probability of un**W**anted occurrence (3 levels). Based on this classification, the following risk matrix in Figure 3-1 is used to rate each hazard from SIL 1 to SIL 4 (SIL 1 being the lowest risk of harm).

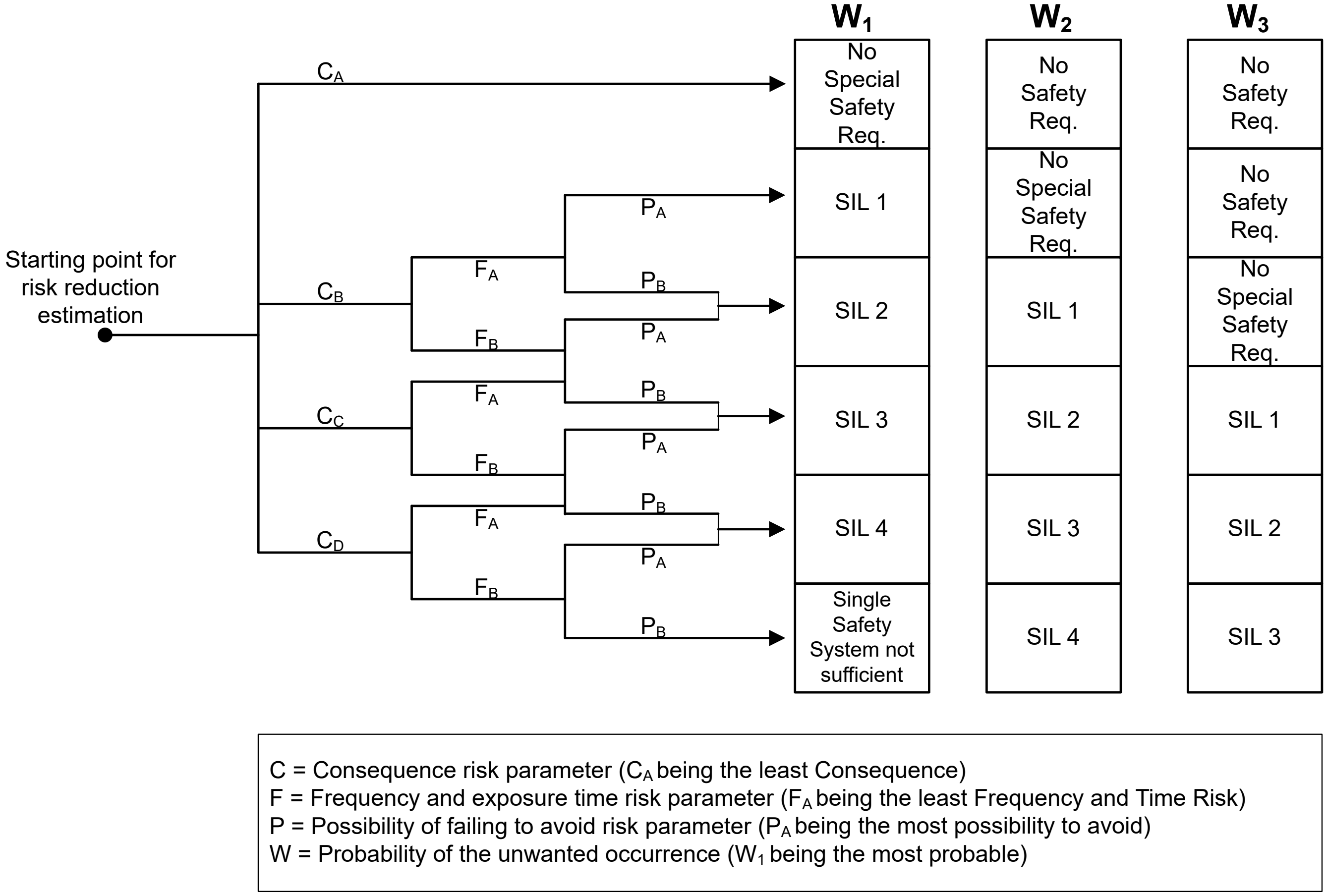
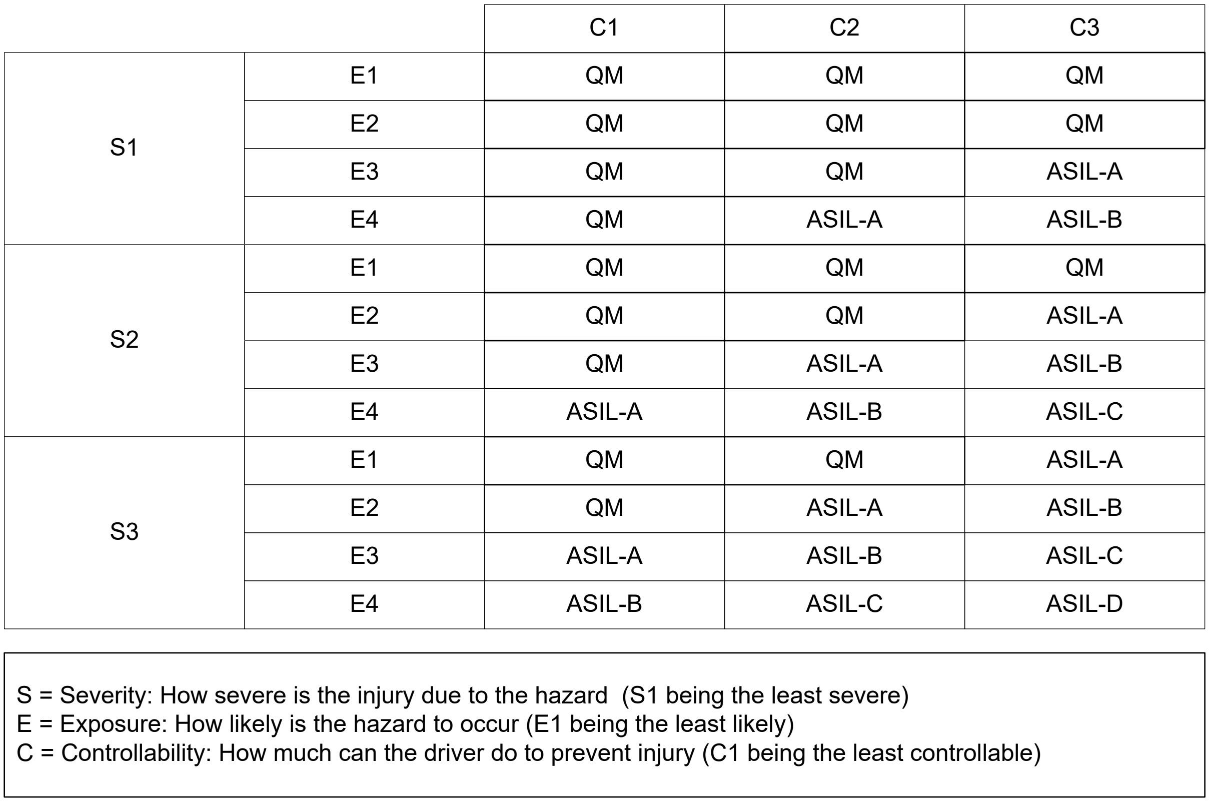

W_1
W_2
W_3
Starting point for risk reduction estimation
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B
No Special Safety Req.
SIL 1
SIL 2
SIL 3
SIL 4
Single Safety System not sufficient
No Safety Req.
No Special Safety Req.
SIL 1
SIL 2
SIL 3
SIL 4
No Safety Req.
No Safety Req.
No Special Safety Req.
SIL 1
SIL 2
SIL 3
C = Consequence risk parameter (C_A being the least Consequence)
F = Frequency and exposure time risk parameter (F_A being the least Frequency and Time Risk)
P = Possibility of failing to avoid risk parameter (P_A being the most possibility to avoid)
W = Probability of the unwanted occurrence (W_1 being the most probable)

Figure 3-1. IEC 61508 Risk Graph, Hazard Classification Matrix

ISO 26262 applications classify each hazard using **S**, **E**, **C** – severity, exposure, controllability. The **severity** of harm is evaluated in three stages. The probability of **exposure** to a potentially hazardous situation is evaluated in four stages. The **controllability** (that is, the degree to which the hazard can be avoided) is evaluated in three stages. Based on this analysis, each hazard is rated from quality management (QM) to ASIL D as shown in Figure 3-2. A QM rating indicates the risk of hazard does not require a dedicated safety goal. For integrated circuits (ICs), the standard semiconductor quality managed design and manufacturing processes are sufficient to support a QM rating.



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL-A
	E4	QM	ASIL-A	ASIL-B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL-A
	E3	QM	ASIL-A	ASIL-B
	E4	ASIL-A	ASIL-B	ASIL-C
S3	E1	QM	QM	ASIL-A
	E2	QM	ASIL-A	ASIL-B
	E3	ASIL-A	ASIL-B	ASIL-C
	E4	ASIL-B	ASIL-C	ASIL-D

S = Severity: How severe is the injury due to the hazard (S1 being the least severe)
E = Exposure: How likely is the hazard to occur (E1 being the least likely)
C = Controllability: How much can the driver do to prevent injury (C1 being the least controllable)

Figure 3-2. ISO 26262 Hazard Classification Matrix

After assigning SIL | ASIL levels to the hazards, safety goals are defined that reduce the hazards to an acceptable level as defined by the SIL | ASIL metrics. Both IEC 61508 and ISO 26262 use **FIT rate** as one of the key compliance metrics for defining acceptable risk levels. FIT is defined as the number of **F**ailures **I**n **T**ime in an interval of 10^9 hours of operation (that is, 1 billion hours of operation).

Not all failures are equal in terms of potential harm and therefore failures are classified into different categories such as non-safety related faults, detected safe faults, undetected safe faults, dangerous detected faults, and dangerous undetected faults. The most critical failure category is the dangerous undetected fault for obvious reasons. The other faults categories do not create a safety concern or can be detected via hardware diagnostics and software diagnostics and mitigated to eliminate any potential harm.

The IEC 61508 SIL and ISO 26262 ASIL metrics are listed in Table 3-1 and Table 3-2.

Table 3-1. IEC 61508 SIL Metrics

	HFT = 0		**HFT = 1**	
SIL Level (Type B Systems)	**PFH**	**SFF**	**PFH**	**SFF**
SIL 1	≤ 1000 FIT	≥60%	≤ 1000 FIT	< 60%
SIL 2	≤ 100 FIT	≥ 90%	≤ 100 FIT	≥ 60%
SIL 3	≤ 10 FIT	≥ 99%	≤ 10 FIT	≥ 90%
SIL 4	Not achievable		≤ 1 FIT	≥ 99%

Table 3-2. ISO 26262 ASIL Metrics

ASIL Level	**PMHF**	**SPFM**	**LFM**
ASIL A	≤ 1000 FIT	Not specified	Not specified
ASIL B	≤ 100 FIT	≥ 90%	≥ 60%
ASIL C	≤ 100 FIT	≥ 97%	≥ 80%
ASIL D	≤ 10 FIT	≥ 99%	≥ 90%

The IEC 61508 standard uses PFH which stands for **P**robability of **F**ailure per **H**our and is the total number of **dangerous *undetected faults*** per hour. SFF is the **S**afe **F**ailure **F**raction and represents the percentage of all fault types that are not categorized as dangerous undetected faults.

Similar to the PFH metric, ISO 26262 uses PMHF which stands for **P**robabilistic **M**etric for random **H**ardware **F**ailures and represents the total number of **dangerous *undetected* faults**. **S**ingle **P**oint **F**ault **M**etric (SPFM) is analogous to 61508 SFF from IEC. One of the key differences between IEC 61508 and ISO 26262 is the addition of the **L**atent **F**ault **M**etric (LFM) to the ISO 26262 standard. LFMs are faults associated with the diagnostic hardware and are considered latent because LFMs are not detectable during normal operation and only reveal themselves when a detectable failure is not detected. To improve the LFM metric, hardware diagnostics must be designed such that the diagnostics can be extensively tested prior to field deployment.

4 Random and Systematic Faults

There are two types of faults that can occur, random and systematic. Random fault occurrence is influenced by a number of variables, including operating temperature, power on hours, operating voltage, and neutron flux factor. Consequently, the ability to address random hardware faults is limited to detecting and possibly preventing the fault during runtime execution and putting the system into a safe state. Systematic faults result from an inadequacy in the design, development or manufacturing process and typically stem from gaps in the development process. A silicon bug is a systematic fault because the bug is detectable during the design verification phase of development.

Systematic faults in theory can be reduced to zero through tightly controlled and adhered to development and manufacturing processes. SIL | ASIL systematic ratings are not assigned a FIT rate like random faults, but rather define different levels of procedures and processes that must be adhered to, thus preventing systematic faults. To meet systematic capability requirements for both IEC 61508 and ISO 26262, TI has developed an internal safety IC development standard which has been certified by TÜV SÜD, an independent third-party assessor. TI certifications for safety hardware and software development can be found on the functional safety home page.

Unlike systematic faults, random faults can never be reduced to zero, but can be significantly reduced. Using system-level design techniques, safety diagnostics and designing the IC in a robust, low FIT rate silicon process, the number of dangerous undetected random hardware faults can be reduced to support SIL and ASIL requirements.

5 AM243x, AM64x: Safety Diagnostics and Examples

TI's AM243x MCU and AM64x processor series are examples of devices specifically designed to support functional safety in a wide range of factory automation applications including Programmable Logic Controllers (PLCs), motor control, industrial communication gateways, and robotics. The AM243x and AM64x series have device options targeting SIL-2 random fault capability (≤ 100 FIT dangerous undetected faults) and SIL-3 systematic capability. At the system level, when combined with an external safety processor, the AM243x and AM64x can assist system integrators in achieving up to SIL-3 HFT = 1. Hardware Fault Tolerance (HFT) = 1 means the system can maintain the safety concepts and safety functions even in the event of a single point hardware failure.

To meet SIL-2 random fault metrics, the AM243x and AM64x make extensive use of safety diagnostics. Device-level safety diagnostics fall into 3 categories as shown in Figure 5-1.

<table>
<tr><th colspan="3">Safety Diagnostics</th></tr>
<tr><th>Hardware Diagnostics</th><th>Software Diagnostics</th><th>Hardware + Software Diagnostics</th></tr>
<tr><td>Diagnostics supported in hardware. Software may or may not be needed for initial configuration, but not required after configuration.</td><td>Diagnostics supported by software. Require CPU support and often need to meet critical timing requirements.</td><td>Diagnostics require hardware and software support. Minimal CPU support requirements.</td></tr>
</table>

Figure 5-1. Types of Safety Diagnostics

An example of a hardware diagnostic used extensively by the AM243x and AM64x is **S**ingle-**E**rror **C**orrecting **D**ouble-**E**rror **D**etecting (SECDED) error correction which is used on all AM243x and AM64x on-chip memories. This diagnostic does exactly as the name implies, correcting single-bit memory errors and detecting 2-bit and even some 3-bit memory errors. All hardware diagnostic faults are aggregated by the AM64x, AM243x Error Signaling Module (ESM), providing a centralized fault management and reporting system. The ESM module classifies errors by severity and the response to each error can be programmed by the system integrator. Error response options include asserting the Safety Error pin (Figure 6-3), generating a high-priority or low-priority interrupt to a CPU, or both.

CRC or **C**yclic **R**eduction **C**heck is an example of a software diagnostic. CRCs are often used in digital communication networks to detect data transmission errors. A CRC value is calculated based on the data packet prior to transmission and then re-calculated on the receiving end. If the calculations do not match, the data was corrupted during transmission. Both calculations are done in software and are the responsibility of the system integrator.

Additionally, the AM243x and AM64x have hardware + software diagnostics. An example of this type of diagnostic is an internal watchdog timer. Watchdog timers are counters implemented in silicon that count down from an initial value to zero. The processor being monitored runs a program that periodically resets the watchdog timer, preventing the timer from ever reaching zero. If the watchdog is not reset and reaches zero, the assumption is the processor has locked up and needs to be reset and put into a safe sate.

The examples given above are just a few of many diagnostics TI provides to make sure that the devices meet SIL and ASIL standards. A complete list of hardware and software diagnostics supported by the AM243x and AM64x can be found in the functional safety manual. Note that the system integrator must implement the recommend software diagnostics and if not implemented, the device cannot achieve the target SIL | ASIL rating.

6 AM243x, AM64x On-Chip Safety MCU and FFI Support

Both AM243x and AM64x have a on-chip isolated Arm® Cortex®-M4F processor with dedicated memory and peripherals. When configured as a safety MCU and safety channel, this MCU can be used to monitor the main processing domain in support of the functional safety goals and target SIL rating of the system. Integrating a safety MCU versus using an external safety MCU reduces system cost and board space.

When combined with a second safety MCU, the AM243x, AM64x can help system integrators support up to SIL-3 HFT =1 rated systems. The addition of a second safety MCU is what adds a level of hardware fault tolerance to the system. The two safety MCUs perform the same functions, cross checking the results of each other. If one of the safety channels experiences a failure, the cross-check calculations are different and the other redundant safety channel detects the failure and places the system in a safe state.

Figure 6-1 shows a traditional approach to achieving SIL-3 HFT = 1 with two external safety MCUs. Figure 6-2 shows that same system, but with one of the safety MCUs integrated into the AM243x, AM64x motor controller.

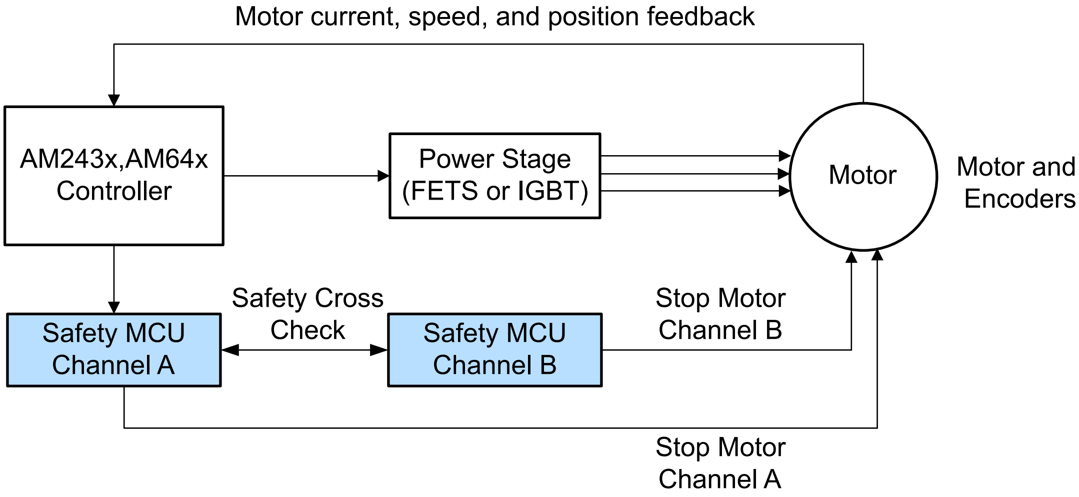


Figure 6-1. SIL-3 HFT = 1 System With Two External Safety MCUs

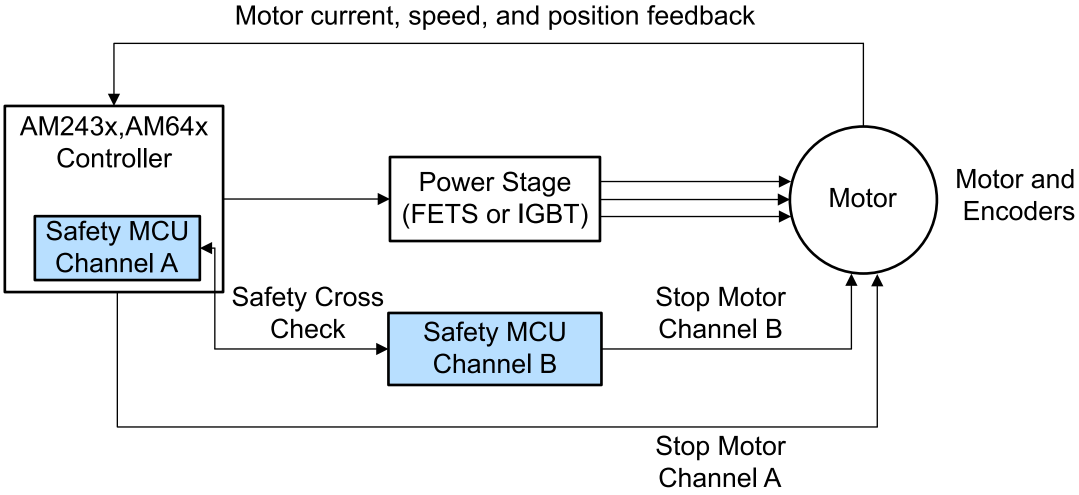


Figure 6-2. SIL-3 HFT = 1 System With Integrated and External Safety MCUs

With an external safety MCU, the safety MCU is physically separated and isolated from the processor being monitored. Integrating the safety MCU requires the use of several **F**reedom **F**rom **I**nterference (FFI) techniques to isolate the safety MCU from the main processing domain. FFI is the absence of the potential for cascading failures and cascading dependencies between two or more elements in the system; FFI is a form of isolation.

The AM243x and AM64x use a firewall to isolate the on-chip safety MCU, insuring events occurring in the main domain do not affect operation of the safety MCU. In addition to the firewall, time-out gaskets are used to protect communication channels between the safety MCU and main domain. When the safety MCU initiates a transaction with the main domain, a timer is set. If the timer expires before the transaction is complete (due to an issue in the main domain) the bus transaction is canceled, preventing the safety domain from hanging up or locking up. If the safety MCU determines that the main domain is not functioning properly, the MCU has the ability to reset the main domain while remaining active.

Figure 6-3 shows the integrated AM243x, AM64x safety MCU and associated main domain reset and safety error flag. Upon a catastrophic error, this error flag can be used to send a signal to the system Power Management IC (PMIC) or other device to initiate a full power down reset of the AM243x, AM64x device.

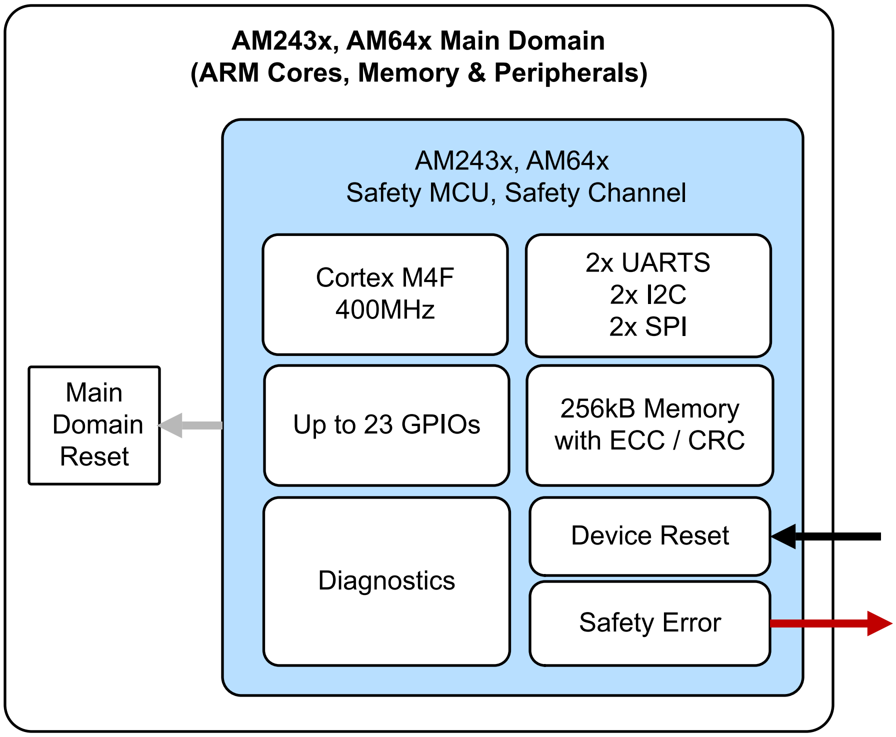


Figure 6-3. AM64x, AM243x On-Chip Safety MCU

7 Safety Element Out of Context

The AM243x and AM64x series were developed as **S**afety **E**lements **o**ut **o**f **C**ontext (SEooC). A SEooC is a device designed to support functional safety without knowledge of the end system safety goals or how the system operates. Developing a device as a SEooC is an efficient use of resources and capital as it allows a single device to support many different applications and safety goals. Since the AM243x and AM64x were designed to support functional safety independent of the end application, several system-level assumptions had to be made and must be supported at the system level to meet the rated SIL level of the device. For example, one of the AM243x and AM64x system-level assumptions is that the power supply or other external monitoring device can monitor the MCU to detect if the MCU is non-responsive. A PMIC with on-chip watchdog timer is a common method to achieve this availability monitoring.

A complete list of system assumptions is available in the AM243x, AM64x safety manual. The safety manual provides an extensive list of diagnostic recommendations. Depending on the safety goals of the system integrator, not all of the software and hardware diagnostic recommendations need be implemented and can be tailored to meet the end goal and simplify the overall development cycle.

8 Functional Safety Resources and Examples

TI provides extensive documentation and guidance to assist customers in meeting functional safety goals. Table 8-1 lists the AM243x, AM64x functional safety resources and is an example of the type of functional safety collateral that TI provides.

Table 8-1. Functional Safety Design In Collateral

Safety Manual	The functional safety manual provides a detailed listing of diagnostic capability, requirements, recommendations, and implementation guidelines. Both TI and customer responsibilities are defined as well as the SEooC system-level design assumptions and design requirements.
FMEDA	The Failure Modes Effects and Diagnostic Analysis (FMEDA) documents the SIL | ASIL calculation assumptions and allows the system integrator to model FIT rates and diagnostic coverage based on a number of variables including device life time, soft errors due to cosmic radiation, operating temperature profile, specific device functions and pins usage, and the addition of customer-defined diagnostics.
Safety Analysis Report	The Safety Analysis report defines the assumptions made in the FMEDA and variables to tailor the FMEDA to a specific application.
Functional Safety Diagnostic Library	The Safety Diagnostic Library (SDL) provides the software and API interfaces for configuring and using the safety diagnostics. Example configuration code for on-chip diagnostics is provided as well as different options for fault detection. The AM243x, AM64x SDL code has been certified SIL-3 by TÜV SÜD.
Safe Torque Off Safety Concept and Evaluation report	SIL-3, HFT = 1 Safe Torque Off Safety Concept and TÜV SÜD evaluation report

Request access to the above information using the links below. Once the AM243x, AM64x completes functional safety certification, all non-NDA materials are made available in the AM243x and AM64x product folders.

- AM243x: MySecure Functional Safety Access Request
- AM64x: MySecure Functional Safety Access Request

For a high-level view of TI's functional safety offerings and associated functional safety resources, see the functional safety home page.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265