Technical White Paper

Functional Safety Support for Arm®-based Microcontrollers and Processors

Neelima Muralidharan, Michael Firth, Kathryn Kalouf

Catalog Processors

ABSTRACT

This white paper introduces functional safety concepts such as the hazard analysis and risk assessment, random and systematic faults, safety element out of context and IEC 61508 SIL and ISO 26262 ASIL ratings. Examples are provided of how the AM243x MCU and AM64x processor series assist system integrators in achieving functional safety goals through the use of an on-chip safety MCU and safety diagnostics.

Table of Contents

1 Functional Safety Goals and Safety Concepts....1
2 HARA and Safety Concept Assessment Stage....2
3 SIL and ASIL Classification....2
4 Random and Systematic Faults....5
5 AM243x and AM64x: Safety Diagnostics and Examples....5
6 AM243x and AM64x: Safety MCU With FFI Support....6
7 Safety Element Out of Context....8
8 Functional Safety Resources and Examples....8

List of Figures

Figure 2-1. HARA and Safety Concept Assessment Stages....2
Figure 3-1. IEC 61508 Risk Graph, Hazard Classification Matrix....3
Figure 3-2. ISO 26262 Hazard Classification Matrix....4
Figure 5-1. Safety Diagnostics Categories....5
Figure 6-1. SIL-3 HFT = 1 System With Two External Safety MCUs....6
Figure 6-2. SIL-3 HFT = 1 System With Integrated and External Safety MCUs....7
Figure 6-3. AM64x and AM243x On-Chip Safety MCU....8

List of Tables

Table 3-1. IEC 61508 SIL Metrics....4
Table 3-2. ISO 26262 ASIL Metrics....4
Table 8-1. Functional Safety Design In Collateral....8

1 Functional Safety Goals and Safety Concepts

Functional safety goals are system-level goals defined at the beginning of the design process focused on reducing the risk of potentially hazardous events. Risk of harm cannot be completely designed out of a system, but with proper design techniques, the risk of harm can be reduced to an acceptable level. Functional safety goals will vary based on the end application, degree of potential harm, and how likely the hazard is to occur. The method of achieving the safety goal at the accepted level of risk of harm is called the safety concept.

To better understand functional safety goals and safety concepts, it can be helpful to examine a modern-day manufacturing plant. On the manufacturing floor both automated and non-automated processes and machinery coexist along with a number of people operating, monitoring, and servicing the equipment. The manufacturing equipment varies from fast moving robotic arms to simple test and measurement stations all of which under the right set of conditions could result in potential harm to an individual.

To reduce the risk of harm on the manufacturing floor, safety goals were defined early in the design process for both the manufacturing equipment and factory processes. To address the potential hazard of a person getting hit by a robotic arm, a safety goal was defined to reduce the occurrence of such a hazard to < 1x per billion hours of operation. A safety concept was then defined to support this safety goal that uses a laser based light curtain to create a keep-out zone around the robotic arm, a Machine Learning (ML) based vision system that tracks the position of the operator relative to the keep-out zone, and a fail-safe method of stopping the robotic arm if an operator is detected entering the keep-out zone. The Safe Torque Off (STO) and Safe Brake Control (SBC) safety functions are used to perform the emergency stop of the robotic arm. STO removes power from the motor and SBC applies an external brake to the motor. STO and SBC (as well as other motor specific safety functions) are commonly used to support safety concepts in motor control applications. The next section (Section 2) details the process used by system integrators to define safety goals and safety concepts.

2 HARA and Safety Concept Assessment Stage

The Hazard Analysis and Risk Assessment (HARA) is a well accepted process for defining system-level safety goals. The first step in the HARA process is to identify all potential hazards in a system and then classify each of the hazards based on risk of harm. The criteria used to classify the hazards varies based on the standard used but typically includes factors such as how dangerous (severity), how likely to occur (exposure), and how controllable the hazard is (controllability). This paper focuses on the Safety Integrity Level (SIL) and Automotive Safety Integrity Level (ASIL) hazard classification techniques and levels.

After the system-level hazards are identified and assigned SIL or ASIL levels, safety goals can be defined to mitigate the hazards. To achieve the safety goals in the end system, safety concepts are required which are defined during the Safety Concept Assessment phase. It is during this phase that the individual components needed to support the safety concept are identified and assigned an appropriate SIL or ASIL level. For example in this phase the system integrator determines if the MCU or processor are critical to implementing the safety concept and if so, assign an appropriate SIL or ASIL rating. Decomposition techniques as per safety standards can be used to lower the safety integrity levels on certain components based on system architecture without lowering the final system safety-integrity levels.

Figure 2-1 shows a graphical representation of the HARA and Safety Concept stages.

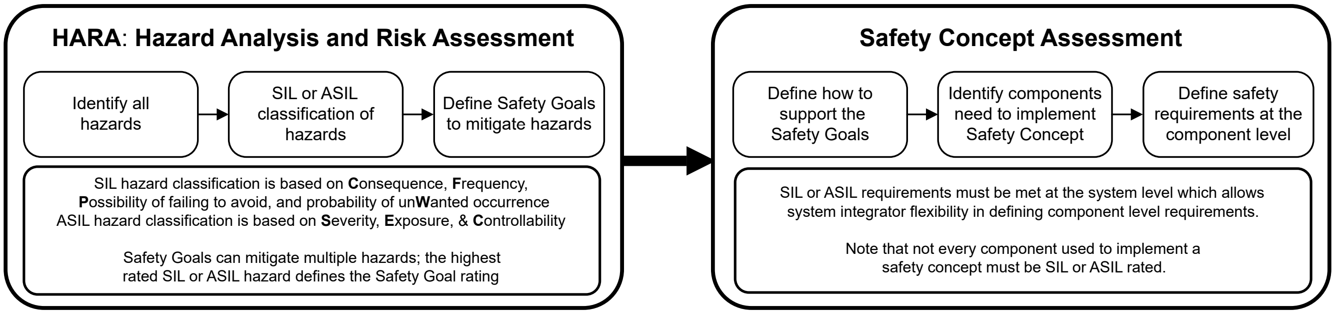

HARA: Hazard Analysis and Risk Assessment
Identify all hazards
SIL or ASIL classification of hazards
Define Safety Goals to mitigate hazards
SIL hazard classification is based on Consequence, Frequency, Possibility of failing to avoid, and probability of unWanted occurrence
ASIL hazard classification is based on Severity, Exposure, & Controllability
Safety Goals can mitigate multiple hazards; the highest rated SIL or 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 or ASIL requirements must be met at the system level which allows system integrator flexibility in defining component level requirements.
Note that not every component used to implement a safety concept must be SIL or ASIL rated.

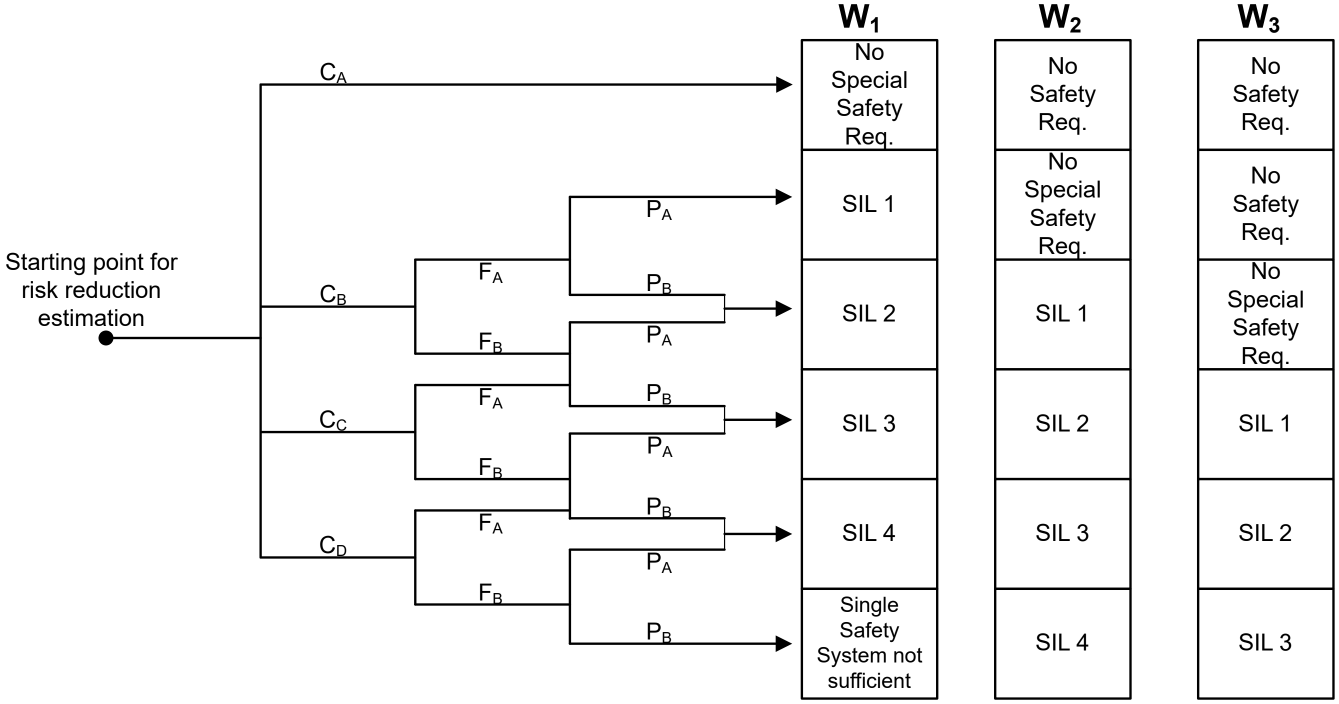
Figure 2-1. HARA and Safety Concept Assessment Stages

3 SIL and ASIL Classification

For many industrial applications, SIL levels are used to classify hazards and define the acceptable failure rates of the safety concept components. The criteria for assigning SIL levels is defined in the International Electrotechnical Commission (IEC) 61508 functional safety standard. IEC 61508 is used in many industries and covers safety-related systems that incorporate electrical, electronic, or programmable electronic devices (or any combination of these three functions).

In IEC 61508, each hazard is classified in terms of Consequence, Frequency and exposure time, Possibility of failing to avoid, and Probability of unwanted occurrence.

Figure 3-1 shows the matrix used to rate each hazard from SIL 1 to SIL 4 (SIL 1 being the lowest risk of harm).



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)

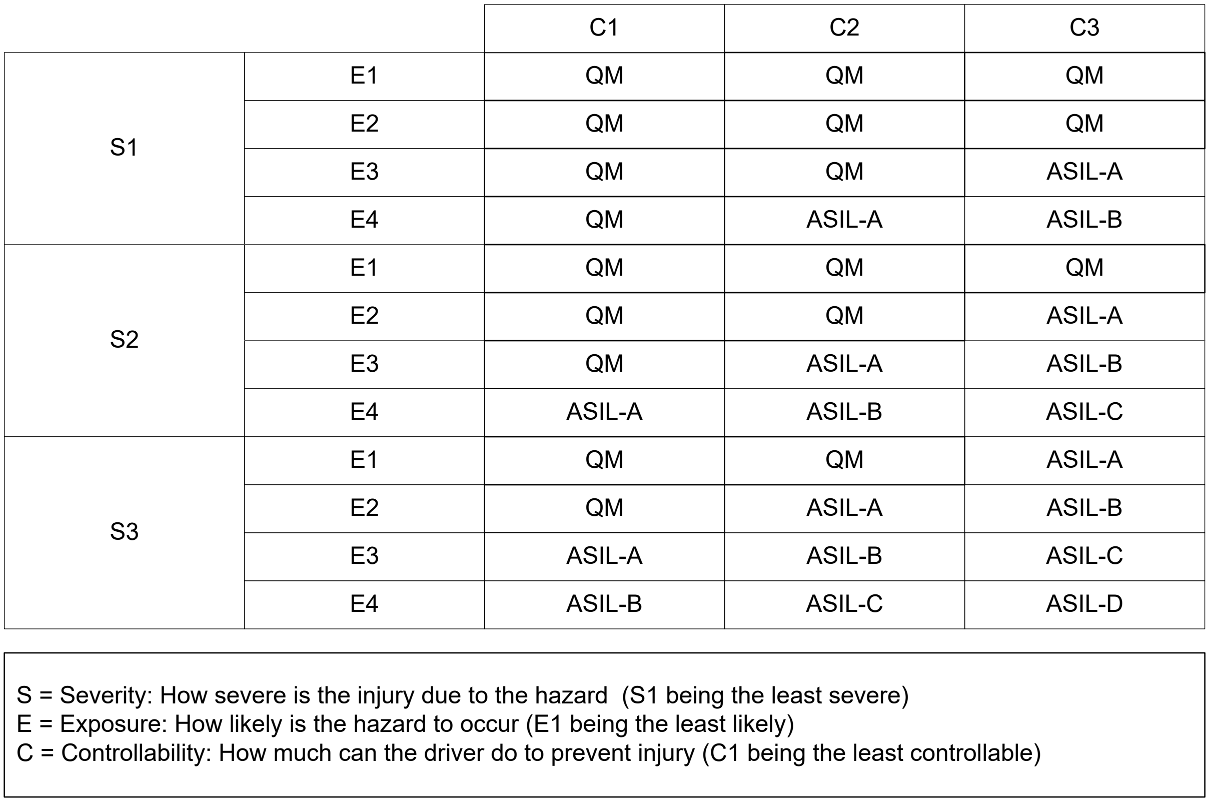
Figure 3-1. IEC 61508 Risk Graph, Hazard Classification Matrix

For automotive applications, ASIL levels are used to classify hazards and define the acceptable failure rates of the safety concept components. The criteria for assigning ASIL levels is defined in the International Organization for Standardization (ISO) 26262 standard. IEC 61508 and ISO 26262 are similar in objectives, but use different methodologies and safety metrics

ISO 26262 classifies each hazard using **S**everity or harm, probability of **E**xposure, and **C**ontrollability which is the degree to which the hazard can be avoided. Using the matrix shown Figure 3-2, each hazard is classified as quality managed (QM) or one of 4 levels from ASIL A to ASIL D. A QM rating indicates the identified hazard does not require a dedicated safety goal to reduce the risk while an ASIL D rating indicates the highest potential risk of harm.

Note

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

FIT rate is a key compliance metric for defining acceptable risk levels in both IEC 61508 and ISO 26262. 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 faults are equal in terms of potential harm and therefore faults are classified into different categories such as non-safety related faults, detected safe faults, undetected safe faults, dangerous detected faults, and dangerous undetected faults. For obvious reasons, the most critical category is the dangerous undetected fault. The other faults categories do not create a significant safety concern or can be detected through diagnostics and mitigated to eliminate any potential harm. The FIT rate at the component level defines the maximum number of dangerous undetected faults that can occur over time.

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 **P**robability of **F**ailure per **H**our (PFH) to represent the total number of **dangerous *undetected faults*** per hour. **S**afe **F**ailure **F**raction (SFF) represents the percentage of faults that are not 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 to represent the total number of dangerous undetected faults. **S**ingle **P**oint **F**ault **M**etric (SPFM) is analogous to SFF.

ISO 26262 adds an additional fault metric called the **L**atent **F**ault **M**etric (LFM) for diagnostic hardware that is not found in IEC 61508. A diagnostic hardware fault is considered latent because the fault cannot be detected during normal operation, reveling the fault only when a detectable failure is not detected. To reduce the number of LFM faults, the diagnostic hardware must be designed with a high percentage of test coverage and 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.

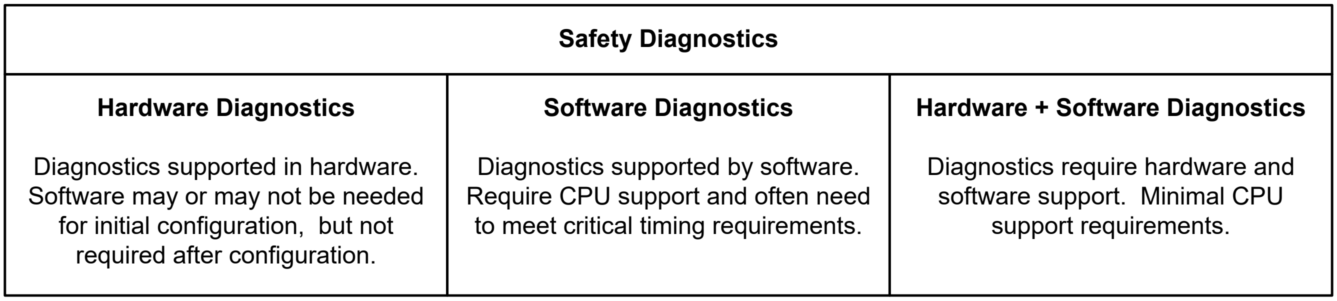
In theory, systematic faults can be reduced to zero through tightly-controlled and adhered-to development and manufacturing processes. SIL or ASIL systematic ratings are not assigned a FIT rate like random faults, but rather define different levels of procedures and processes that must be adhered to.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

Unlike systematic faults, random faults can never be reduced to zero and must be managed to an acceptable level through the use of different techniques. For ICs, the number of random hardware faults can be reduced to an acceptable SIL or ASIL level by using system-level design techniques, manufacturing in a low FIT rate silicon process, and implementing both hardware and software safety diagnostics. Section 5 describes what is meant by safety diagnostics and provides use examples in the AM243x and AM64x devices.

5 AM243x and AM64x: Safety Diagnostics and Examples

TI's AM243x microcontrollers and AM64x processors were specifically designed to support functional safety in a wide range of 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 of 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 concept 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.



Safety Diagnostics		
Hardware Diagnostics Diagnostics supported in hardware. Software may or may not be needed for initial configuration, but not required after configuration.	**Software Diagnostics** Diagnostics supported by software. Require CPU support and often need to meet critical timing requirements.	**Hardware + Software Diagnostics** Diagnostics require hardware and software support. Minimal CPU support requirements.

Figure 5-1. Safety Diagnostics Categories

Single-**E**rror **C**orrecting **D**ouble-**E**rror **D**etecting (SECDED) is a common hardware diagnostic used to detect memory errors. This diagnostic does exactly as the name implies, correcting single-bit memory errors and detecting 2-bit and even some 3-bit memory errors. Both the AM243x and AM64x have SECDED on all on-chip memories.

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

An example of a hardware + software diagnostics 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 reaches zero, the assumption is the processor has locked up and needs to be reset, put into a safe state, or be reset *and* put into a safe state.

All safety faults are routed to AM64x and AM243x Error Signaling Module (ESM), providing a centralized fault management and reporting system. The ESM module classifies errors based on severity and allows the system integrator to program the response to each error. Response options include asserting the Safety Error pin (Figure 6-3), generating a high- or low-priority interrupt, or asserting the Safety Error pin and generating an interrupt.

A complete list of hardware and software diagnostics supported by the AM243x and AM64x can be found in the functional safety manual.

6 AM243x and AM64x: Safety MCU With FFI Support

Both AM243x and AM64x have an on-chip isolated **Arm®Cortex®-M4F** processor with dedicated memory and peripherals. When configured as a safety MCU, the M4F can be used to monitor the main processing domain in support of the system SIL rating.

When combined with a second safety MCU, the AM243x and AM64x can help support up to SIL-3 HFT = 1 rated systems. The addition of a second safety MCU is what adds the hardware fault tolerance to the system. The two safety MCUs perform cross-check calculations on each other. If the results do not match, one of the two processors can be used to place the system in a safe state.

Integrating a safety MCU versus using two external safety MCUs reduces system cost and board space. Figure 6-1 shows a SIL-3 HFT = 1 system with two external safety MCUs. Figure 6-2 shows that same system, but with one of the safety MCUs integrated into the AM243x or AM64x controller.

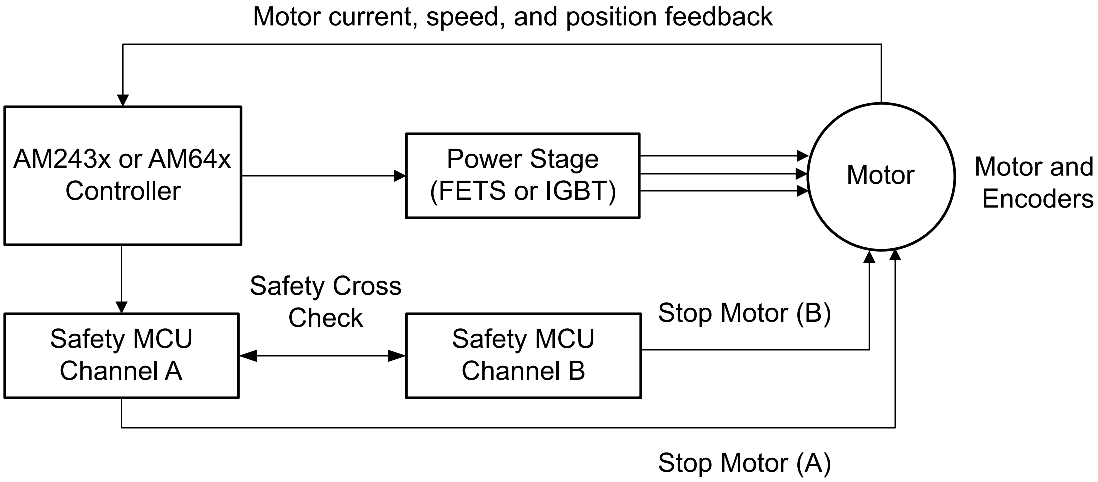


Figure 6-1. SIL-3 HFT = 1 System With Two External Safety MCUs

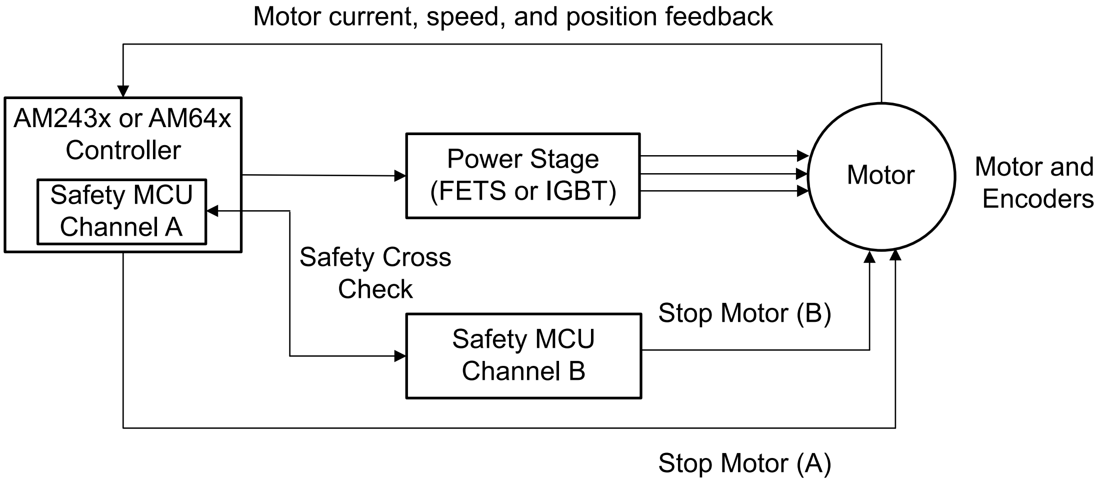


Figure 6-2. SIL-3 HFT = 1 System With Integrated and External Safety MCUs

Integrating the safety MCU requires the use of **F**reedom **F**rom **I**nterference (FFI) techniques to isolate the safety MCU domain from the main processing domain. FFI is defined as the absence of cascading failures and dependencies between two or more elements in the system; FFI is a form of isolation.

A firewall and time-out gaskets are used to isolate the AM243x and AM64x safety domains, insuring events occurring in the main domain do not affect the safety domain. Time-out gaskets protect the safety domain from faults in the main domain during inter-domain communication. When the safety domain initiates a transaction with the main domain, a watchdog 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 locking up. In the event of the main domain becoming unresponsive, the safety domain has the ability to reset the main domain while remaining active.

In addition to the firewall and safety gaskets, additional safety features in the safety domain include loss of clock detection circuitry, a dual-clock comparator to detect incorrect clock frequencies, parity on the bus transactions, dedicated I/O power rail, and built-in self-test (BIST) support.

Figure 6-3 shows the AM243x and AM64x safety domain, main domain reset, safety error flag, and device reset pin. Upon a catastrophic error, the error flag can signal the Power Management IC (PMIC) or other device to initiate a reset of the AM243x|AM64x.

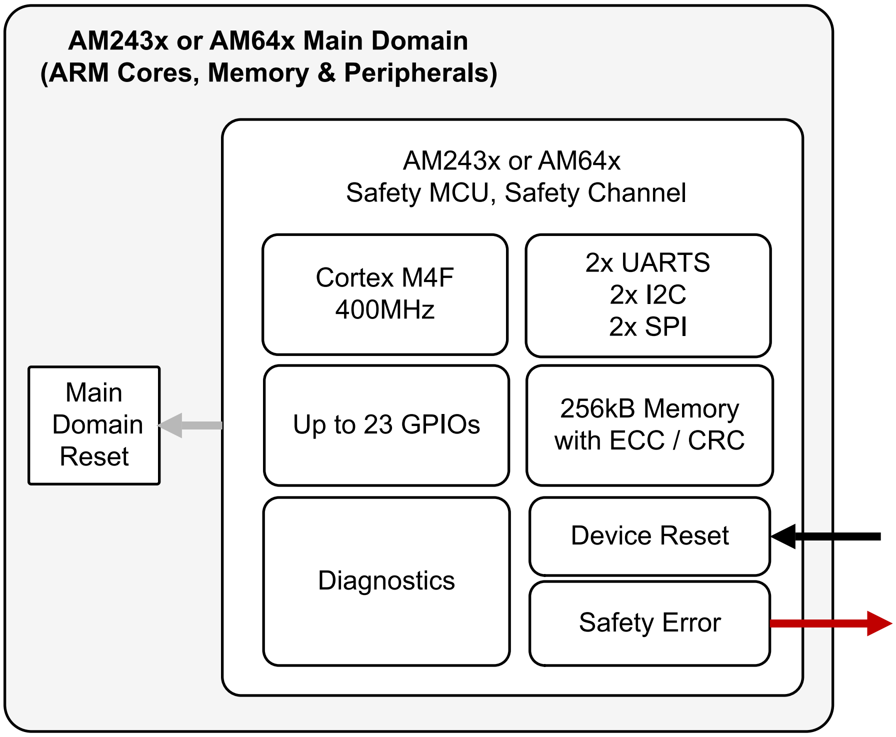


Figure 6-3. AM64x and AM243x On-Chip Safety MCU

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 beforehand 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.

To design an IC to support functional safety independent of the end application, several system-level assumptions must be made and supported at the system-level to meet the SIL level rating 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 processor and detect if it is non-responsive. A PMIC with on-chip watchdog timer is a common method to meet this requirement.

A complete list of system assumptions is available in the AM243x and AM64x safety manual. The safety manual provides an extensive list of diagnostic recommendations and details of the types of diagnostics supported. Depending on the safety goals of the system integrator, the system integrator can chose a subset of the available hardware and software diagnostics to support the functional safety goals; that is, not all of the available safety diagnostics must be used in a given system.

8 Functional Safety Resources and Examples

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

Table 8-1. Functional Safety Design In Collateral

Safety Manual	The functional safety manual provides a detailed listing of device diagnostic capability, recommendations, and implementation guidelines. TI and end-customer responsibilities are defined as well as SEooC system-level design assumptions and design requirements.
FMEDA	The Failure Modes Effects and Diagnostic Analysis (FMEDA) documents SIL or ASIL calculation assumptions. Modeling of FIT rates and diagnostic coverage based on device lifetime, soft errors due to cosmic radiation, operating temperature profile, specific device functions, and pins usage and customer-defined diagnostic is supported.
Safety Analysis Report	The Safety Analysis report defines the assumptions made in the FMEDA and defines variables that can help tailor the FMEDA to a specific application.

Table 8-1. Functional Safety Design In Collateral (continued)

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 following links. Once the AM243x, AM64x completes functional safety certification, all non-NDA material is 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, please see TI's functional safety home page.

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