参考資料

Technical White Paper

Arm® ベースのマイクロコントローラとプロセッサ向けの機能安全サポート

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

概要

このホワイト ペーパーでは、危険分析とリスク評価、SIL レベルと ASIL レベル、ランダム故障と決定論的原因故障、コンテキスト外安全要素など、機能安全コンセプトについて紹介しています。また、AM243x マイクロコントローラと AM64x プロセッサのシリーズが、セーフティー マイクロコントローラの統合と安全診断の使用を通じて、機能安全をどのようにサポートしているかを例示しています。

目次

図の一覧

表の一覧

1 機能安全目標

機能安全目標は、潜在的に危険な事象のリスクを低減するためのシステム レベルの目標です。ここでのキーワードは、「低減」です。リスクは常にある程度存在し、安全目標における目的は、許容可能なレベルまで危害のリスクを低減することにあります。

安全目標は、最終アプリケーション、機器の使用方法、オペレータと機器との関わり方に基づいて定義されます。たとえば、工場の現場には作業者に危害を及ぼす可能性のある機器が存在しており、衣類が機械に巻き込まれた場合、機械を直ちに停止しなければ作業者が負傷する可能性があります。この例における安全目標は、機械からあらかじめ設定された距離内で人が検知されたらすぐに機械を停止させることで、作業者への危害を防止することです。システム インテグレータがこの安全目標をどのように実装し、サポートするかを安全コンセプトと呼びます。モーターや機械の停止に使用される一般的な安全コンセプトはセーフ トルク オフ (STO) と呼ばれ、この例の安全目標をサポートするために実装することができます。(詳細については、表 8-1 のセーフ トルク オフのコンセプトおよび評価レポートを参照してください。)

2 危険分析とリスク評価

安全目標を定義するための最初のステップは、システム インテグレータによる危険分析とリスク評価 (HARA) の実施です。HARA は、システムで発生の可能性があるすべての潜在的な危険を特定することから始まります。次に、これらの危険は事前に定義された基準に基づいて分類され、各危険に対してセーフティー インテグリティ レベル (SIL) または車載セーフティー インテグリティ レベル (ASIL) が割り当てられます。割り当てられた SIL または ASIL レベルによって、各危険の最大許容発生率が定義されます。続いて、危険を軽減し、その発生を目標の SIL または ASIL レベルに制限するための安全目標と安全コンセプトが定義されます。

図 2-1 に、HARA および安全コンセプトの各段階図を示します。

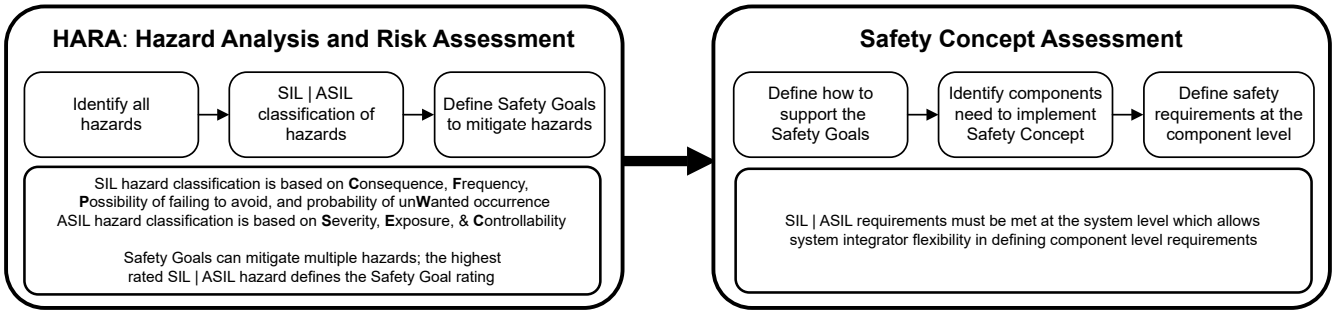

図 2-1. HARA および安全コンセプトの評価段階

3 SIL レベルと ASIL レベル

HARA 分析では、特定された危険は 4 つの SIL | ASIL レベルのいずれかに分類されます。SIL | ASIL レベルが高いほど、危害のリスクが高くなり、安全要件も高くなります。SIL レベルは、産業用アプリケーションを含む多くの業種に適用可能な機能安全規格である IEC 61508 で定義されています。ASIL レベルは ISO 26262 規格で定義されており、車載専用です。国際電気標準会議 (IEC) 61508 と ISO 26262 の各規格は、目的は似ていますが、使用する方法論や安全メトリクスが異なります。

IEC 61508 では、各危険は結果 (**C**onsequence) (4 段階)、頻度と暴露時間 (**F**requency and exposure time) (2 段階)、回避できない可能性 (**P**ossibility of failing to avoid) (2 段階)、望ましくない発生の確率 (Probability of un**W**anted occurrence) (3 段階) に分類されています。この分類に基づき、以下の 図 3-1 のリスク マトリックスを使用して、各危険を SIL 1 から SIL 4 に評価します (SIL 1 は最も低い危害リスク)。

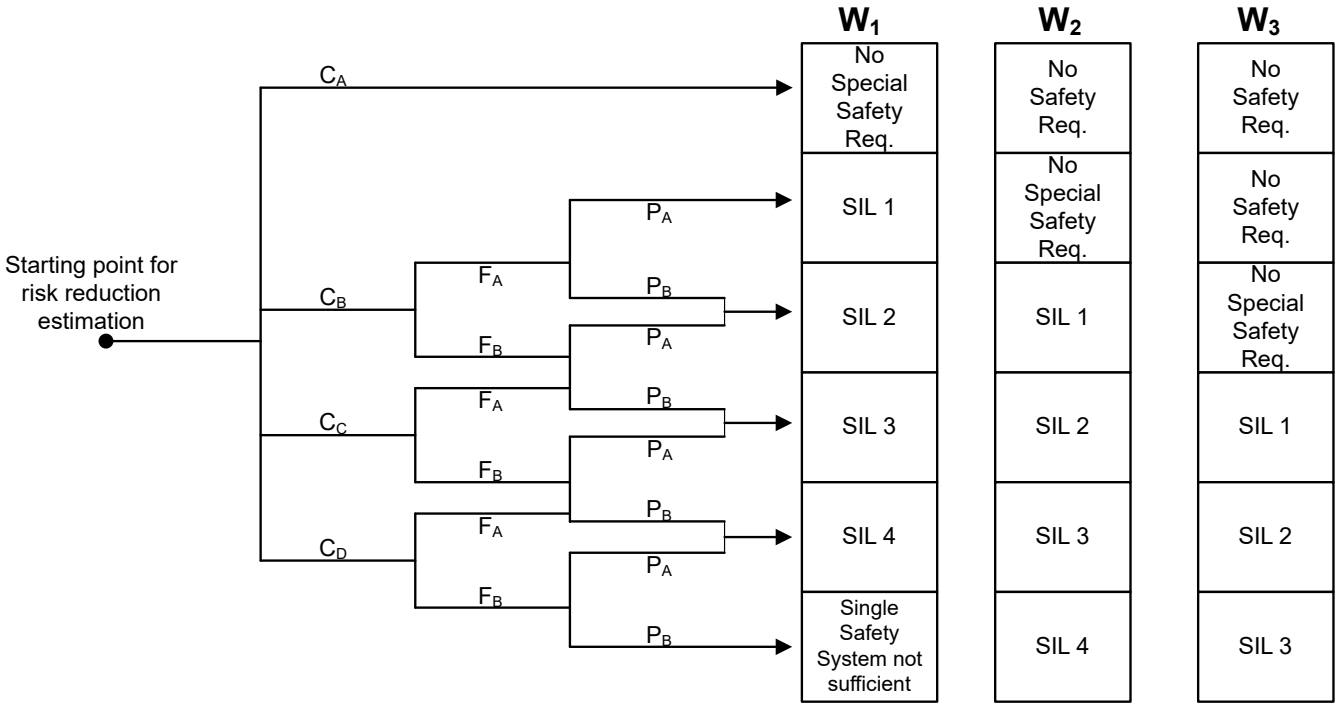

図 3-1. IEC 61508 のリスク グラフ、危険分類マトリクス

ISO 26262 のアプリケーションでは、危険を **S**、**E**、**C** (重大度、露出度、制御可能性) で分類しています。危害の**重大度**は 3 段階で評価されます。潜在的に危険な状況に**露出**される確率は、4 段階で評価されます。**制御可能性** (危険を回避できるレベル) は、3 段階で評価されます。この分析に基づき、図 3-2 に示すように、各危険を品質管理 (QM) レベルから ASIL D まで評価します。QM 評価があると、危険のリスクには専用の安全目標が必要ではありません。集積回路 (IC) の場合は、QM 評価をサポートするには、標準的な半導体の品質管理設計 / 製造プロセスで対応できます。

		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)

図 3-2. ISO 26262 の危険分類マトリクス

危険に SIL | ASIL レベルを割り当てた後、SIL | ASIL メトリクスによって定義された許容レベルまで危険を低減する安全目標が定義されます。IEC 61508 と ISO 26262 はいずれも、許容リスク レベルを定義するための主要なコンプライアンス メトリクスの 1 つとして **FIT 率** を使用しています。FIT は、10^9 時間の動作間隔 (動作時間 10 億時間) での故障回数 (**F**ailures **I**n **T**ime) として定義されます。

すべての故障が潜在的な危害という点で同じであるとは限りらないため、故障は、非安全関連の故障、検出された安全な故障、検出されない安全な故障、検出された危険な故障、検出されない危険な故障など、さまざまなカテゴリに分類されます。最も重要な故障カテゴリは、明白な理由から検出されない危険な故障です。他の故障カテゴリは、安全上の懸念をもたらさないか、ハードウェア診断やソフトウェア診断によって検出され、潜在的な危害を排除するために緩和できます。

表 3-1 と 表 3-2 に IEC 61508 SIL と ISO 26262 ASIL の各メトリクスを示します。

表 3-1. IEC 61508 SIL のメトリクス

	HFT = 0		HFT = 1	
SIL レベル (タイプ B システム)	**PFH**	**SFF**	**PFH**	**SFF**
SIL 1	≤ 1000 FIT	≥60%	≤ 1000 FIT	60% 未満
SIL 2	≤ 100 FIT	≥ 90%	≤ 100 FIT	≥ 60%
SIL 3	≤ 10 FIT	99% 以上	≤ 10 FIT	≥ 90%
SIL 4	達成不可能		≤ 1 FIT	99% 以上

表 3-2. ISO 26262 ASIL のメトリクス

ASIL レベル	PMHF	SPFM	LFM
ASIL A	≤ 1000 FIT	指定なし	指定なし
ASIL B	≤ 100 FIT	≥ 90%	≥ 60%
ASIL C	≤ 100 FIT	97% 以上	≥ 80%
ASIL D	≤ 10 FIT	99% 以上	≥ 90%

IEC 61508 規格では PFH を使用しています。PFH は、1 時間あたりの故障の確率 (**P**robability of **F**ailure per **H**our) の略で、1 時間あたりの**検出されない危険な故障**の総数になります。 SFF は安全な故障率 (**S**afe **F**ailure **F**raction) で、検出されない危険な故障に分類されないすべての故障タイプの割合を示します。

PFH メトリクスと同様に、ISO 26262 では PMHF を使用しています。PMHF はランダムなハードウェア故障の確率メトリクス (**P**robabilistic **M**etric for random **H**ardware **F**ailures) の略で、**検出されない危険な故障**の総数を示します。シングルポイント故障メトリクス (SPFM、**S**ingle **P**oint **F**ault **M**etric) は、IEC の 61508 SFF に類似しています。IEC 61508 と ISO 26262 の主な違いのうちの 1 つは、ISO 26262 規格に潜在的故障メトリクス (LFM、**L**atent **F**ault **M**etric) が追加されていることです。LFM は診断ハードウェアに関連する故障であり、通常動作中は検出できないため、検出可能な故障が検出されない場合にのみ明らかになります。そのため、潜在的な故障と見なされます。LFM メトリクスを改善するには、現場導入の前に診断を広範にテストできるようにハードウェア診断を設計する必要があります。

4 ランダム故障および決定論的原因故障

発生する可能性のある故障には、ランダム故障と決定論的原因故障の 2 種類があります。ランダム故障の発生は、動作温度、電源オン時間、動作電圧、中性子束係数など、多くの変数の影響を受けます。そのため、ランダムなハードウェア故障に対処する能力は、ランタイム実行中に故障を検出し、可能であれば防止し、システムを安全な状態にすることに限定されます。決定論的原因故障は、設計、開発、製造プロセスの不備に起因し、通常は開発プロセスのギャップから生じます。シリコン バグは、開発の設計検証段階で検出できるため、決定論的原因故障です。

理論上の決定論的原因故障は、開発および製造プロセスを厳密に管理し、遵守することによってゼロにすることができます。SIL | ASIL の決定論的評価は、ランダム故障のように FIT 率を割り当てられるのではなく、決定論的原因故障を防止するために遵守しなければならない手順やプロセスのレベルをそれぞれ定義しています。IEC 61508 と ISO 26262 の両方の決定論的能力の要件を満たすために、テキサス・インスツルメンツでは社内の安全 IC 開発標準を策定し、独立した第三者評価機関である TÜV SÜD の認証を受けています。安全なハードウェアおよびソフトウェアの開発に関するテキサス・インスツルメンツの認証については、ホーム ページの機能安全を参照してください。

決定論的原因故障とは異なり、ランダム故障はゼロにすることはできませんが、大幅に減少させることは可能です。システム レベルの設計技術、安全診断、および堅牢で低い FIT 率のシリコン プロセスで IC を設計することにより、検出されない危険なランダム ハードウェア故障の数を減らし、SIL 要件および ASIL 要件をサポートすることができます。

5 AM243x、AM64x：安全診断および例

テキサス・インスツルメンツの AM243x マイクロコントローラおよび AM64x プロセッサのシリーズは、プログラマブル ロジック コントローラ (PLC)、モーター制御、産業用通信ゲートウェイやロボットなど、幅広いファクトリ オートメーション アプリケーションで機能安全をサポートするように特別に設計されたデバイスの例です。AM243x および AM64x のシリーズにはデバイス オプションがあり、SIL-2 のランダム故障耐性 (≤ 100 FIT の検出されない危険な故障) および SIL-3 の決定論的能力に準拠することを目標としています。システム レベルでは、AM243x および AM64x を外部セーフティー プロセッサと組み合わせることで、システム インテグレータが SIL-3 および HFT = 1 まで達成できるよう支援できます。ハードウェア故障耐性 (HFT) = 1 とは、シングル ポイント ハードウェア故障が発生した場合でも、システムが安全コンセプトと安全機能を維持できることを意味します。

SIL-2 のランダム故障メトリクスに応じて、AM243x および AM64x は安全診断を広範に活用しています。デバイス レベルの安全診断は、図 5-1 に示すように、3 つのカテゴリに分類されます。

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.

図 5-1. 安全診断のタイプ

AM243x および AM64x で広範に活用されているハードウェア診断の例として、AM243x および AM64x のすべてのオンチップ メモリで使用されている SECDED (**S**ingle-**E**rror **C**orrecting **D**ouble-**E**rror **D**etecting) エラー訂正があります。この診断機能は名前が示すとおりに、1 ビットのメモリ エラーを訂正し、2 ビットさらには一部の 3 ビットのメモリ エラーを検出するというものです。すべてのハードウェア診断故障は、AM64x、AM243x のエラー シグナリング モジュール (ESM) によって集約され、中央集中型の故障管理および報告システムを実現しています。ESM モジュールは重大度によってエラーを分類し、各エラーへの応答はシステム インテグレータによってプログラムできます。エラー応答のオプションには、セーフティー エラー ピン (図 6-3) のアサート、CPU への高優先度または低優先度の割り込みの生成、またはその両方があります。

巡回冗長検査 (CRC、**C**yclic **R**eduction **C**heck) は、ソフトウェア診断の一例です。CRC は、デジタル通信ネットワークでデータ転送エラーを検出するためによく使用されます。CRC 値は、転送前にデータ パケットに基づいて計算され、受信側で再計算されます。計算値が一致しない場合は、転送中にデータが破損しています。どちらの計算もソフトウェアで行われ、その責任はシステムインテグレータにあります。

さらに、AM243x および AM64x は、ハードウェア診断とソフトウェア診断の機能を備えています。このタイプの診断の例として、内部ウォッチドッグ タイマがあります。ウォッチドッグ タイマはシリコンで実装されたカウンタで、初期値からゼロまでカウントダウンします。監視対象のプロセッサは、定期的にウォッチドッグ タイマをリセットするプログラムを実行し、タイマがゼロにならないようにします。ウォッチドッグがリセットされずにゼロになった場合、プロセッサがロックし、リセットして安全な状態にする必要があると推測されます。

上記の例は、デバイスが SIL と ASIL の各規格に準拠しているかを確認するために、テキサス・インスツルメンツが提供している多くの診断の一部にすぎません。AM243x および AM64x がサポートしているハードウェア診断とソフトウェア診断の一覧については、機能安全マニュアルを参照してください。システム インテグレータは推奨されるソフトウェア診断を実装する必要があり、実装されていない場合、デバイスは目標の SIL | ASIL 評価を達成できません。

6 AM243x、AM64x のオンチップ セーフティー マイクロコントローラおよび FFI サポート

AM243x および AM64x はどちらも、専用のメモリとペリフェラルを備えたオンチップ絶縁型 Arm® Cortex®-M4F プロセッサを搭載しています。セーフティー マイクロコントローラおよびセーフティー チャネルとして構成した場合、このマイクロコントローラを使用して、システムの機能安全目標と目標 SIL 評価をサポートするためにメイン処理ドメインを監視できます。外部のセーフティー マイクロコントローラを使用するのではなく、セーフティー マイクロコントローラを統合することで、システム コストと基板面積を抑えることができます。

AM243x、AM64x を 2 番目のセーフティー マイクロコントローラと組み合わせると、システム インテグレータは SIL-3 および HFT = 1 の評価を受けたシステムまでサポートすることができます。2 番目のセーフティー マイクロコントローラを追加することで、システムにある程度のハードウェア故障耐性が追加されます。2 つのセーフティー マイクロコントローラは同じ機能を実行し、互いの結果をクロスチェックします。セーフティー チャネルのうちの一方が故障した場合、クロスチェック計算が異なり、もう一方の冗長セーフティー チャネルが故障を検出してシステムを安全な状態に移行します。

図 6-1 は、2 つの外部セーフティー マイクロコントローラを使用して SIL-3 および HFT = 1 を達成する、従来型アプローチを示します。図 6-2 は同じシステムを示していますが、セーフティー マイクロコントローラのうちの 1 つが AM243x、AM64x のモーター コントローラに統合されています。

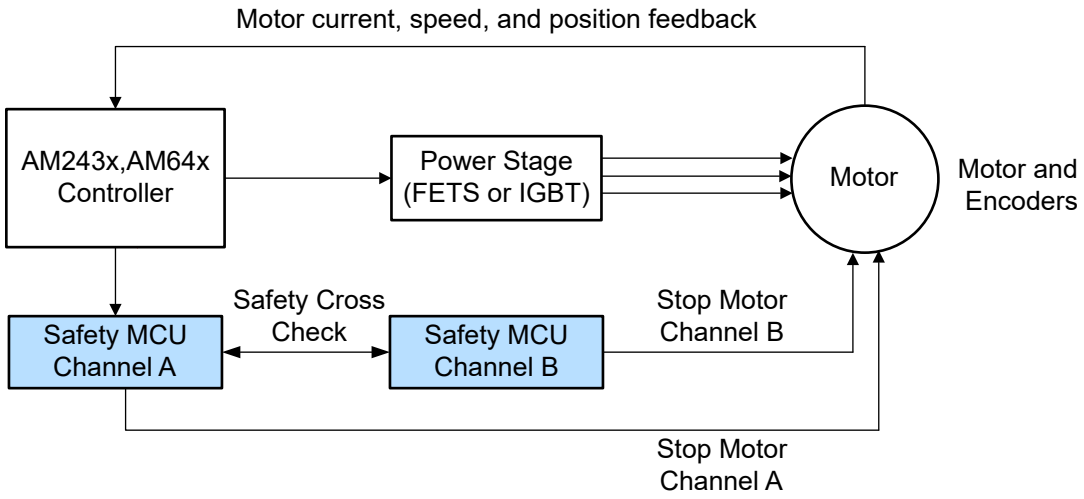

図 6-1. 2 つの外部セーフティー マイクロコントローラを搭載した SIL-3 および HFT = 1 のシステム

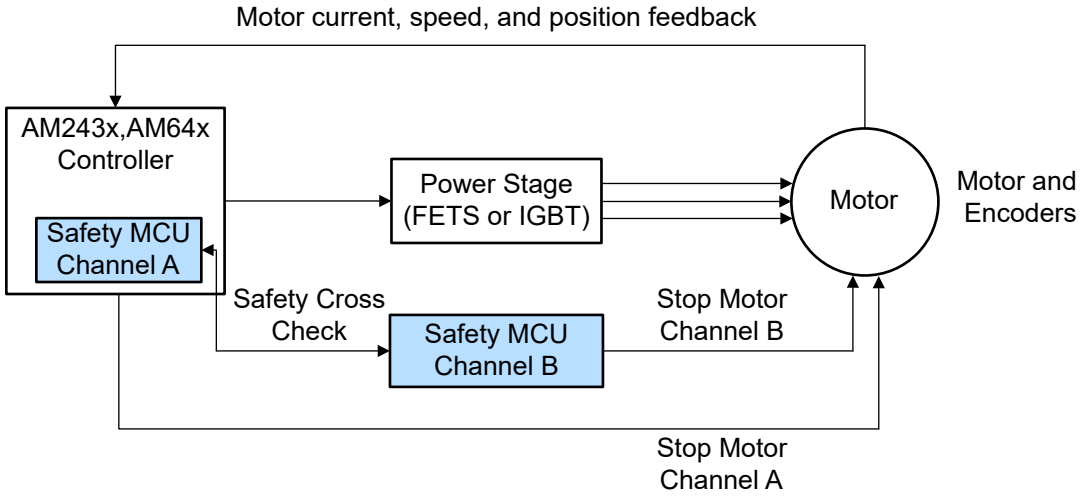

図 6-2. 統合セーフティー マイクロコントローラと外部セーフティー マイクロコントローラを搭載した SIL-3 および HFT = 1 のシステム

外部セーフティー マイクロコントローラの場合、そのセーフティー マイクロコントローラは監視対象のプロセッサから物理的に分離および隔離されています。セーフティー マイクロコントローラの統合には、いくつかの無干渉 (**F**reedom **F**rom **I**nterference、FFI) 技術を使用して、セーフティー マイクロコントローラをメイン処理ドメインから隔離する必要があります。FFI とは、システム内の 2 つ以上の要素間にカスケード故障やカスケード依存関係の可能性がないことで、FFI は隔離の一形態となります。

AM243x および AM64x はファイアウォールを使用してオンチップ セーフティー マイクロコントローラを隔離し、メイン ドメインで発生したイベントがセーフティー マイクロコントローラの動作に影響しないようにしています。ファイアウォールの他に、セーフティー マイクロコントローラとメイン ドメインの間の通信チャネルを保護するためにタイムアウト ガスケットを使用しています。セーフティー マイクロコントローラがメイン ドメインとのトランザクションを開始すると、タイマが設定されます。トランザクションが完了する前にタイマが切れた場合 (メイン ドメイン内での問題が原因の場合)、バスのトランザクションはキャンセルされ、セーフティー ドメインがハングアップまたはロックアップするのを防止します。メイン ドメインが正常に機能していないとセーフティー マイクロコントローラが判断した場合、マイクロコントローラはアクティブのままメイン ドメインをリセットできます。

図 6-3 に、統合された AM243x、AM64x のセーフティー マイクロコントローラ、および関連するメイン ドメインのリセットおよびセーフティー エラー フラグを示します。重大なエラーが発生した場合、このエラー フラグを使用してシステムのパワー マネージメント IC (PMIC) または他のデバイスに信号を送信し、AM243x、AM64x デバイスのフルパワー ダウン リセットを開始できます。

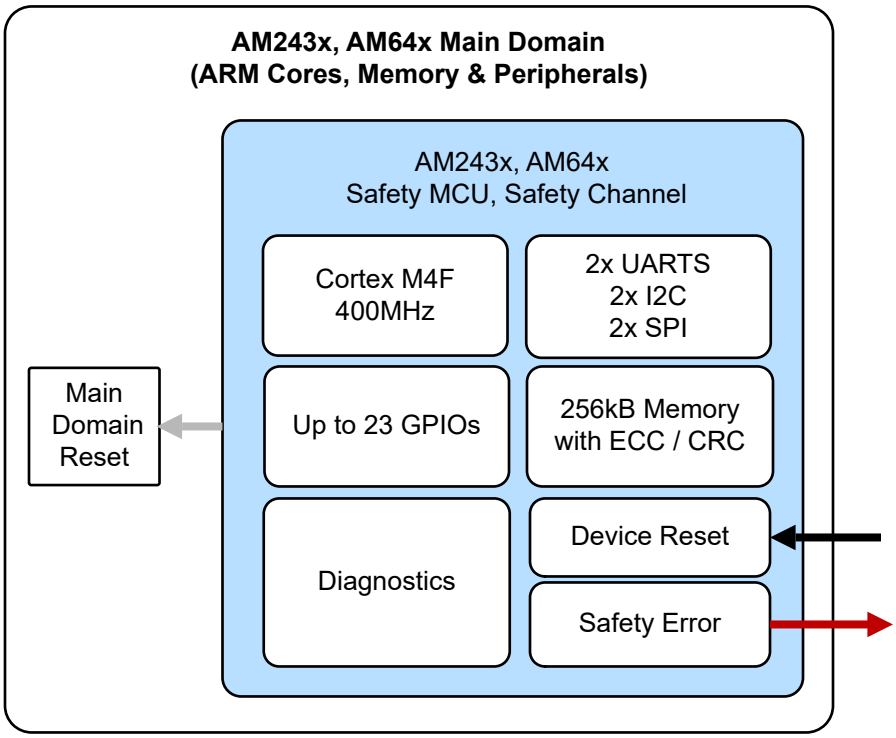

図 6-3. AM64x、AM243x のオンチップ セーフティー マイクロコントローラ

7 コンテキスト外安全要素

AM243x および AM64x のシリーズは、コンテキスト外安全要素 (SEooC、**S**afety **E**lements **o**ut **o**f **C**ontext) として開発されました。SEooC は、最終システムの安全目標やシステムの動作方法について知らなくても、機能安全をサポートできるように設計されたデバイスのことです。SEooC としてデバイスを開発すると、1 つのデバイスで多様なアプリケーションと安全目標をサポートできるため、リソースと資本を効率的に使用できます。AM243x および AM64x は最終的なアプリケーションに依存せずに機能安全をサポートするように設計されているため、デバイスの評価 SIL レベルを満たすには、システム レベルでいくつかの前提条件を設定し、それをサポートする必要があります。たとえば、AM243x および AM64x のシステム レベルの前提条件のうちの 1 つは、電源または他の外部監視デバイスがマイクロコントローラを監視して、マイクロコントローラが応答しない場合を検出できるというものです。この可用性監視を実現するには、オンチップ ウォッチドッグ タイマを搭載した PMIC が一般的な方法になります。

AM243x、AM64x のセーフティー マニュアルには、システム前提条件の詳細な一覧があり、診断に関する広範な推奨事項が記載されています。システム インテグレータの安全目標によっては、すべてのソフトウェア診断およびハードウェア診断の推奨事項を実装する必要はありませんが、最終目標を達成し、開発サイクル全体を簡素化するためのカスタマイズが可能です。

8 機能安全のリソースおよび例

テキサス・インスツルメンツは、お客様が機能安全目標を達成できるように、広範囲に及ぶ資料とガイダンスを用意しています。表 8-1 は AM243x、AM64x の機能安全リソースの一覧で、テキサス・インスツルメンツが用意している機能安全関連資料の一例です。

表 8-1. 機能安全関連資料

セーフティー マニュアル	機能安全マニュアルには、診断機能、要件、推奨事項、実装ガイドラインの詳細が記載されています。テキサス・インスツルメンツとお客様の両方の責任とともに、SEooC のシステム レベル設計の前提条件と設計要件も定義されています。
FMEDA (故障モード、影響、および診断分析)	故障モード、影響、および診断分析 (FMEDA) は、SIL | ASIL 計算の前提条件を文書化し、デバイスの寿命、宇宙放射に起因するソフト エラー、動作温度プロファイル、特定のデバイス機能とピンの使用方法、お客様によって定義された診断機能の追加などの多くの変数に基づいて、システム インテグレータが FIT 率と診断範囲をモデル化できるようにします。
安全分析レポート	安全分析レポートでは、FMEDA で仮定された前提条件と、FMEDA を特定のアプリケーションに適合させるための変数を定義します。
機能安全の診断ライブラリ	安全診断ライブラリ (SDL) は、安全診断を構成および使用するためのソフトウェア インターフェイスと API インターフェイスを提供するものです。オンチップ診断用の構成コード例と、故障検出用のさまざまなオプションが提供されています。AM243x、AM64x の SDL コードは、TÜV SÜD によって SIL-3 認証を取得しています。
セーフ トルク オフの安全コンセプトおよび評価レポート	SIL-3 および HFT = 1 のセーフ トルク オフの安全コンセプトおよび TÜV SÜD 評価レポート

上記情報へのアクセスは、以下のリンクからリクエストしてください。AM243x、AM64x の機能安全認証が完了すると、NDA を除いたすべての資料が AM243x および AM64x の製品フォルダで利用できるようになります。

- AM243x：MySecure 機能安全アクセス リクエスト
- AM64x：MySecure 機能安全アクセス リクエスト

テキサス・インスツルメンツの機能安全に関するサービスや関連する機能安全リソースの概要については、ホーム ページの機能安全を参照してください。

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス· デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、TI の販売条件、または ti.com やかかる TI 製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。

お客様がいかなる追加条項または代替条項を提案した場合でも、TI はそれらに異議を唱え、拒否します。

郵送先住所：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265