参考資料

Application Note

TI のマイコン / MPU をベースとする産業用機能安全 PLC アーキテクチャの実装

Zekun Bai, Linjun Meng, Donna Xu

概要

このアプリケーション ノートでは、テキサス インスツルメンツ (TI) の Sitara マイコン (MCU) およびマイクロプロセッサ (MPU) を使用して、IEC 61508 および ISO 13849-1 規格に準拠した機能安全プログラマブル ロジック コントローラ (PLC) システムを設計する方法を紹介します。本書では、機能安全の基本概念、システム安全目標の分解方法、TI チップの安全アーキテクチャの特性、および推奨される PLC システム設計手法について説明します。モジュール設計の原則と柔軟な冗長アーキテクチャにより、設計エンジニアはコストと複雑さを抑えながら、SIL 3/CAT 3 レベルの機能安全要件を満たすことができます。対象読者は、産業用制御システムの設計エンジニア、機能安全アーキテクト、システム インテグレータです

目次

商標

1 機能安全の基礎

1.1 機能安全とは

機能安全とは、電気、電子、プログラマブル電子安全関連システムが正しく動作することにより、危険事象を防止または軽減する能力を指します。産業用アプリケーションでは、機器やシステムが特定の故障条件の下で危険性を発生させる可能性があります。機能安全の目的は、このような危険な発生の可能性を許容可能なレベルまで下げることです。

1.2 故障から危害への因果関係チェーン

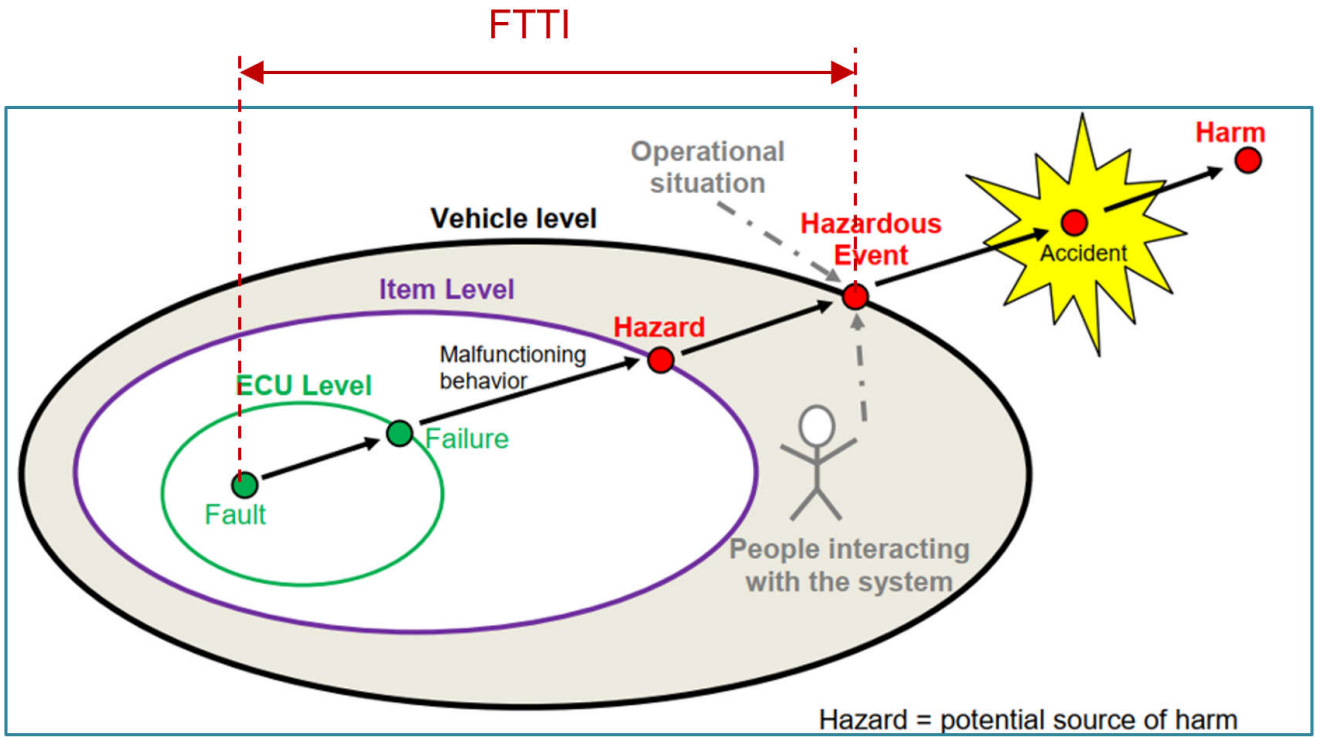

図 1-1. FTTI の可視化

- レベル 1: ハードウェア / ソフトウェア故障 (故障) → CPU 演算エラー、メモリ破損、タイミング故障など。
- レベル 2: 故障につながる故障 (故障) → 異常なシステム機能、不正確な出力、応答不能
- レベル 3: 危険事象を引き起こす故障 → 予期しない装置動作、制御不良、センサ検知不能
- レベル 4: 人身傷害 (危害) → 人身傷害、機器の損傷、生産停止

IEC 61508 規格の定義によると、故障から人身傷害に至るまでの一連のプロセスには、以下が含まれます。

故障 → 潜在的故障の指標

- ハードウェアの欠陥、製造プロセスの偏差、ソフトウェアの欠陥など、システムの欠陥
- ランダム故障:動作ストレス (温度、電圧) および累積使用時間によって発生します
- 決定論的原因故障:不適切な設計または不適切なプロセスが原因で発生します

故障 → 危険な故障と安全な故障との関係

- 故障が検出または検出されない場合は、システム機能が失われます
- 危険な故障:安全機能の損失につながる可能性のある故障
- 安全な故障:システムが安全な状態に移行する原因となる障害

危険事象 → 予見可能ではあるが避けられないものと、予見可能で回避可能なものとの比較

- 故障は最終的に、人員または機器に危害を及ぼす可能性のある事象へと発展します
- 例:予期しないロボットの動き、エレベータのブレーキの故障、予期しない産業用機器の起動

人身傷害 (危害) → 負傷の重大度の分類

- 危険な事態を時間内に防止しないと、実際の負傷につながります

1.3 機能安全が対処する主な問題

機能安全設計の目的は、この因果連鎖の中に複数の防御ラインを構築することです:

- **故障検出**:故障の存在をできるだけ迅速に検出します
- **故障分離**:故障の影響を分離し、重要な機能への伝播を防止します
- **安全応答**:故障によって故障が発生した場合に安全機能をトリガします
- **冗長設計**:単一故障が原因で安全機能が低下することはありません
- **診断機能**:故障は迅速に検出され、システムによって識別されます

2 安全基準とグレード分類

2.1 主な安全基準システム

産業分野と車載分野では、異なるものの相互に関連した安全性の考え方が採用されています。

産業用アプリケーション ベースの規格:

- **IEC 61508** - すべての電気 / 電子 / プログラマブル電子安全関連システムに適用される一般的な安全規格
- **IEC 62061** - 機械安全関連の電気 / 電子 / プログラマブル制御システムの安全性
- **ISO 13849-1** - 制御システムの機械安全関連部分の安全性 (性能レベル スキームを使用)

ドメイン固有アプリケーション規格:

- **IEC 61800-5-2** - 可変速電力駆動システム - 5-2 部:機能安全の要件
- **ISO 10218** - ロボットおよびロボット デバイス - 産業用ロボットの安全要件
- **IEC 61496** - 機械の安全性 - 電気に敏感な保護装置

産業用通信安全規格:

- **IEC 61784-3** - 産業用通信ネットワーク - 機能安全性
  - FSoE (Functional Safety over Ethernet) プロトコルを定義します
  - EtherCAT、PROFINET、EtherNet/IP などのプロトコル向けの安全拡張を規定します
  - 通信層の故障検出および回復メカニズムを定義します
  - 通信の故障の PFH バジェットは通常、システム全体 PFH の 1% を超えません

車載アプリケーション:

- **ISO 26262** - 道路車両 - 電気 / 電子 / プログラマブル電子安全関連システムの機能安全

2.2 産業用通信 (FSoE) の機能安全

産業用イーサネットの広範な採用により、新たな課題が生じています。それは、標準ネットワーク上で決定性と安全性を実現する必要性です。

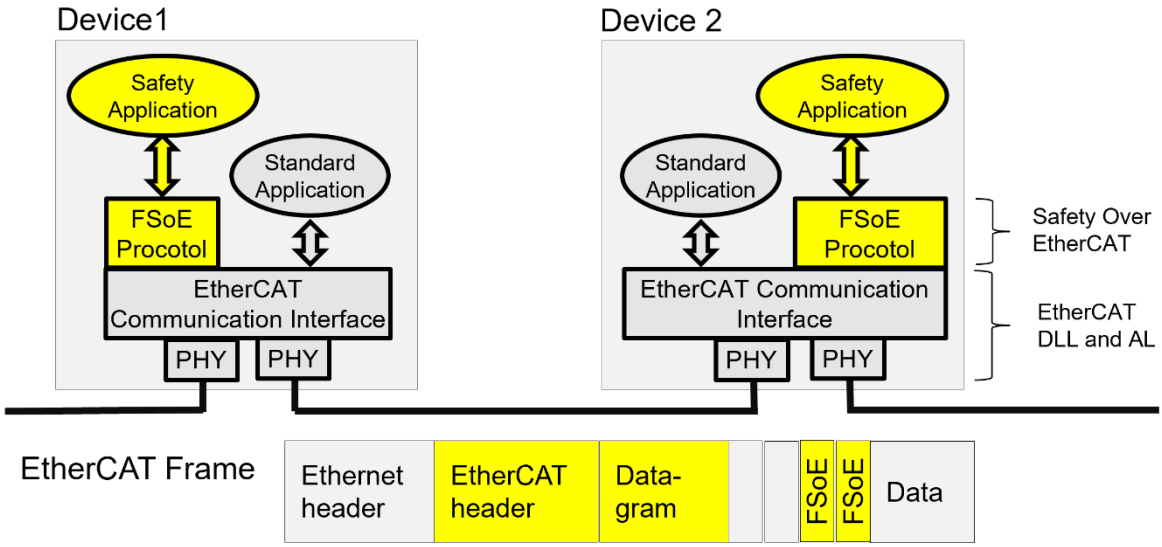

図 2-1. FSoE プロトコル階層構造

- アプリケーション層:安全関連データ (位置、速度、故障コードなど)
- FSoE プロトコル層:
  - シーケンス番号の検出 (重複、損失、異常を検出)
  - CRC 検証 (データの破損を検出)
  - 接続 ID (不適切な転送を検出)

  - ウォッチドッグ タイマ (タイムアウト遅延の検出)
- 物理層：標準的なイーサネット MAC/PHY

FSoE は基盤となる物理層を変更せず、アプリケーション層プロトコルによって機能を強化します。

図 3 FSoE と標準 PLC 通信の違い

特性	標準イーサネット / EtherCAT	FSoE の強化
ベース プロトコル	EtherCAT 規格	同一
安全データ	特別な処理はありません	CRC とシーケンス番号を含む
故障検出	パケット損失検出	FSoE 診断を完了します
遅延検出	なし	ウォッチドッグ モニタ
信頼性	メディア (ネットワーク依存)	高 (自動故障転送)
アプリケーションの複雑さ	低	中 (プロトコル スタック処理)

2.3 安全グレード インジケータ システム

2.3.1 IEC 61508 - 安全インテグリティ レベル (SIL)

IEC 61508 では、危険な故障確率インジケータに基づいて 4 つの安全性インテグリティ レベルを定義しています。

図 4 IEC 61508 のキー インジケータ

IEC61508						
ハードウェア故障耐性						SFF
0	1	2	**0**	1	2	
-	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3	**60% 未満**
SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4	60%～90% 未満
SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4	90%～99% 未満
SIL 3	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4	99% 以下
タイプ A			タイプ B			

IEC 61508 は特定の HFT を要求せず、システムは 1oo1 や 1oo2 構成になる場合があります

- タイプ A サブシステム：故障モードはよく定義されています。このモードでは、故障条件での動作が判定され、故障率が満たされていることを示す十分な故障データがあります。
- タイプ B サブシステム：より複雑であり、故障モードが完全には明確に定義されておらず、フォルト条件も完全に特定できず、さらに故障率が要件を満たしていることを裏付ける十分なデータが存在しないものです。

インジケータに関する主な説明：

- **PFH** (時間当たり故障確率)：10^9 時間の動作における故障回数 (FIT 単位)
- **SFF** (安全故障率)：危険でない故障の割合
- **HFT** (ハードウェア故障耐性)：ハードウェア故障耐性機能

通信 PFH バジェット：IEC 61784-3 によると、通信チャネル PFH はシステム全体 PFH の 1% を超えないようにする必要があります。例：

- システム目標が SIL 3 (PFH ≤ 10 FIT) の場合
- 通信が可能な PFH ≤ 0.1 FIT (10 FIT の 1%)
- このため、通信の信頼性には非常に高い要件が課されています

2.3.2 ISO 13849-1 - パフォーマンス レベル (PL) およびカテゴリ (CAT)

ISO 13849-1 では、アーキテクチャの耐故障性を重視した、異なる分類アプローチが採用されています。

図 5 性能レベルは a (最低) から e (最高) まで

ISO13849				
DC	カテゴリ			
	1	**2**	**3**	**4**
なし				
低	c	c	d	
中		d	e	
高				e

ISO13849 のカテゴリは、HFT (ハードウェア故障耐性) と同様に、故障に対する抵抗を規定しています。

- Cat.1 : シングル チャネル + 十分に試行された部品
- Cat.2 : シングル チャネル + 試験装置
- Cat.3 : デュアル チャネル + 診断、故障の蓄積なし
- Cat.4 : デュアル チャネル + 診断、故障の蓄積、診断の要求の増大

パフォーマンス レベルは、a (最低) から e (最高) までの範囲で設定できます。主な対応関係 :

- **PL e ≈ SIL 3** : 高い診断範囲を備えた HFT = 1 が必要です
- **PL d ≈ SIL 2** : 中程度の診断範囲を備えた HFT = 1 が必要です

3 システムの安全性目標の分解

3.1 HARA プロセスおよび安全目標定義

システム安全目標の分解は、HARA (ハザード分析およびリスク評価) から開始します

ステップ 1: すべての潜在的な危険を特定する

- システムが引き起こす可能性のあるすべての望ましくない事象を特定します
- 例 (産業用ロボット): ロボットの予期しない動作、ブレーキの故障、速度超過
- 例 (PLC 制御システム): 予期しない出力起動、通信中断による制御障害、センサーの読み取りミス

ステップ 2: リスク評価と分類

産業用アプリケーション (IEC 61508) では、リスク評価は以下に基づいて行われます。

- **結果 (結果)**: CA (軽微) → CB → CC → CD (致命的)
- **頻度および露光時間 (頻度)**: FA (まれ) → FB (頻繁)
- **回避可能性 (回避できる可能性)**: PA (回避可能) → PB (回避が困難)

ステップ 3: 安全性の目標の定義

安全目標には、以下を明確に記載する必要があります。

- 防止または軽減する必要があります
- 対応する安全インテグリティ レベル (SIL または ASIL)
- 許容故障率 (PFH)
- 診断範囲と故障耐性の要件

例:

安全性の目標 1:「予期しない PLC 制御信号の起動を防止」

- SIL レベル: SIL 2

- PFH ターゲット: ≤100 FIT

- 診断範囲: ≥90%

- 故障耐性要件: HFT = 1 (単一の故障では作動しない)

安全性の目標 2:「通信チャネルの信頼性を確保」

- SIL レベル: SIL 2

- PFH ターゲット: ≤ 1 FIT (通信バジェット)

- 診断範囲: ≥ 99% (FSoE メカニズム)

- 故障耐性要件: DLR リング ネットワークの冗長性

3.2 安全目標の分解と ASIL/SIL 割り当て

トップレベル: システムの安全性目標「PLC 制御システムの安全性」- SIL 3

第二階層は以下に分解されます。

- サブゴール A:「I/O モジュールの故障が危険な出力を引き起こさない」- SIL 3
- サブゴール B:「通信故障が検出され、処理されました」- SIL 2
- サブゴール C:「プロセッサの故障が絶縁されています」- SIL 2

第三レベルでは、具体的な要求事項への分解が続きます。

ASIL 分解の原理 (ISO 26262)

ASIL 分解により、上位レベルの安全目標を複数の下位レベルのサブゴールに分配できます。独立性および多様性の要求事項が満たされている場合、システムは元の ASIL レベルを引き続き達成できます。

図 6 分解規則:

正規 ASIL 製品	許容される分解の組み合わせ
ASIL-D	D(D) + QM(D) または C(D) + A(D) または B(D) + B(D)
ASIL-C	C(C) + QM(C) または B(C) + A(C)
ASIL-B	B(B) + QM(B) または A(B) + A(B)
ASIL-A	A(A) + QM(A)

主要な要件:

1. 独立 (独立性)
   - 分解されたサブゴールは、相互に独立している必要があります
   - 一つのサブゴールの失敗が、別のサブゴールの失敗を引き起こしてはなりません
   - 例:異なるハードウェア、異なる電源、異なるクロックを使用
2. 多様性 (ダイバーシティ)
   - さまざまな技術や実装方法を採用します
   - 例:異なるプロセッサ ベンダ、異なるプログラミング言語、異なるアルゴリズムを使用す
3. トレーサビリティ (追跡可能性)
   - 分解プロセスと基礎の明確な文書化
   - 各サブゴールがどのように組み合わさって元の目標を満たすかの説明
   - 完全な要求事項トレーサビリティ マトリックスを維持
4. 位置合わせ (妥当性説明)
   - 分解されたアーキテクチャが実際に元の ASIL を達成していることを証明する必要があります
   - 通常、故障ツリー解析 (FTA) またはその他の定量的手法によって証明されます

SIL 合成の原理 (IEC 61508)

ASIL 分解に対応するため、IEC 61508 には SIL 合成方法が定義されています。SIL 合成では基本的に、システマティック能力が N である二つの冗長要素を合成 (または組み合わせ) することで、N が SIL 3 以下である限り、システマティック能力 N + 1 を得ることができます。IEC 61508 に従って SIL 合成を制御するルールは次のとおりです

- SIL 2 + SIL 2 → SIL 3
- SIL 1 + SIL 1 → SIL 2

IEC 61508 では再帰的な (多層の) 合成は認められていませんが、ISO 26262 では認められています。例:SIL 合成

(IEC 61508 による) では以下のいずれも許可されていません。

- SIL 2 (SIL 3 をサポート) + [SIL 1 (SIL 2 をサポート) + SIL 1 (SIL 2 をサポート)] → SIL 3。
- SIL 2 (SIL 3 をサポート) + SIL 1 (SIL 3 をサポート) → SIL 3。

対照的に、ISO 26262 ではマルチレベルの分解が可能です。

IEC 61508 では、SIL 4 システムについて 2 チャネル実装も義務付けています

(SIL 4 機能ではハードウェア故障の許容度が 0 未満である必要があります)。それ以外の点では、ASIL 分解と SIL 合成は、

それぞれ ISO 26262 規格および IEC 61508 規格における同等の構成概念です。

3.3 システム レベル分解の具体的な応用

例:SIL 3 産業用 PLC システムの分解

システム レベルの安全性の目標:SIL 3。三つのサブシステムに分解:

サブシステム 1 - I/O 故障絶縁 (SIL 2)

- デジタル入力故障検出

- デジタル出力故障検出
- 故障発生時に出力を遮断します
- 診断範囲:≥90%

サブシステム 2 – デュアル マイコン故障検出 (SIL 2)

- ウォッチドッグのタイムアウト検出
- メモリ ECC チェック
- 内部診断セルフテスト
- 診断範囲:≥90%

サブシステム 3 - 通信安全性 (SIL 2)

- FSoE プロトコル故障検出
- ネットワークリング冗長性 (DLR)
- メッセージの検証とタイムアウト
- 診断範囲:≥99%

組み合わせ戦略:

- 独立したハードウェアおよび検出メカニズムによる三つの SIL 2 サブシステム
- システムレベルの診断範囲は 99% を超えています
- 単一点故障は安全機能の損失につながりません (HFT ≥ 1)
- 結果:システム全体が SIL 3 を達成します

3.4 役割責任部門

機能安全プロジェクトにおける関係者間の明確な役割分担の重要性:

お客様 / システム インテグレータの責任:

- HARA を実施し、システムレベルの安全性目標を定義する
- 安全コンセプトを策定し、安全性目標をサブシステムに分割する
- 適切な TI 部品を選択する
- 安全関連ソフトウェアを開発する
- システムレベルの検証とテストを実行する
- 安全ケースのドキュメントを準備する

TI の責任:

- 認証取得済みの開発プロセスを使用して、機能安全マイコン / MPU を開発する
- 部品レベルの安全性分析 (FMEDA) を提供する
- 安全マニュアルと診断ライブラリ (SDL) を提供する
- SEooC (コンテキスト外安全要素) として機能する
- システム統合、アプリケーション ソフトウェアの開発、システム評価の責任は負いません

独立評価機関 (TÜV SÜD など) の責任:

- TI コンポーネントを独立して評価し、認証する
- お客様のシステムの安全ケースを確認する
- 機能安全認証証明書を発行する

4 TI チップの安全アーキテクチャ

4.1 マイコン レベルの安全アーキテクチャ

以下に、TI の機能安全マイコンにおける三つの一般的な安全アーキテクチャを示します。

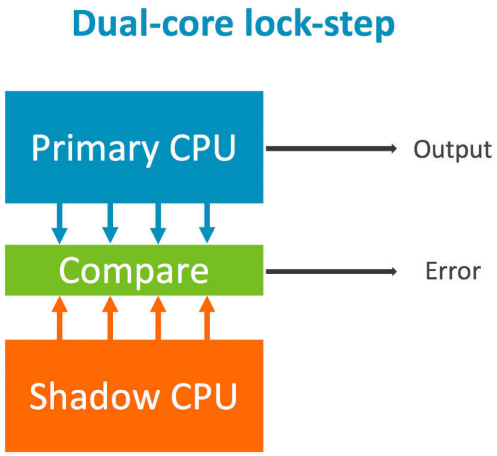

図 4-1. デュアル コア ロック ステップ

デュアル コア ロック ステップ (DCLS): 同一の二つの CPU コアが並列に動作し、ハードウェア コンパレータが不一致を検出し、検出時に即座に割り込みを発生させます。

特性:

- 二つの CPU コアが、同期したタイミングで同一の命令を実行します
- ハードウェア コンパレータが、計算結果を継続的に比較します
- 不一致が発生すると、エラー処理が直ちにトリガされ、システムが停止します
- 故障検出のレイテンシ:シングル サイクル (最小)

利点:

- 低コスト、シングル チップ実装
- 超高速の故障検出
- シンプルなアーキテクチャ

欠点:

- 共通原因故障 (共有クロック障害など) を検出できません
- 故障トレランスなし、検出能力のみ
- 一つのコアに障害が発生すると、システム全体が停止します

アプリケーション:SIL 2 HFT = 0 系

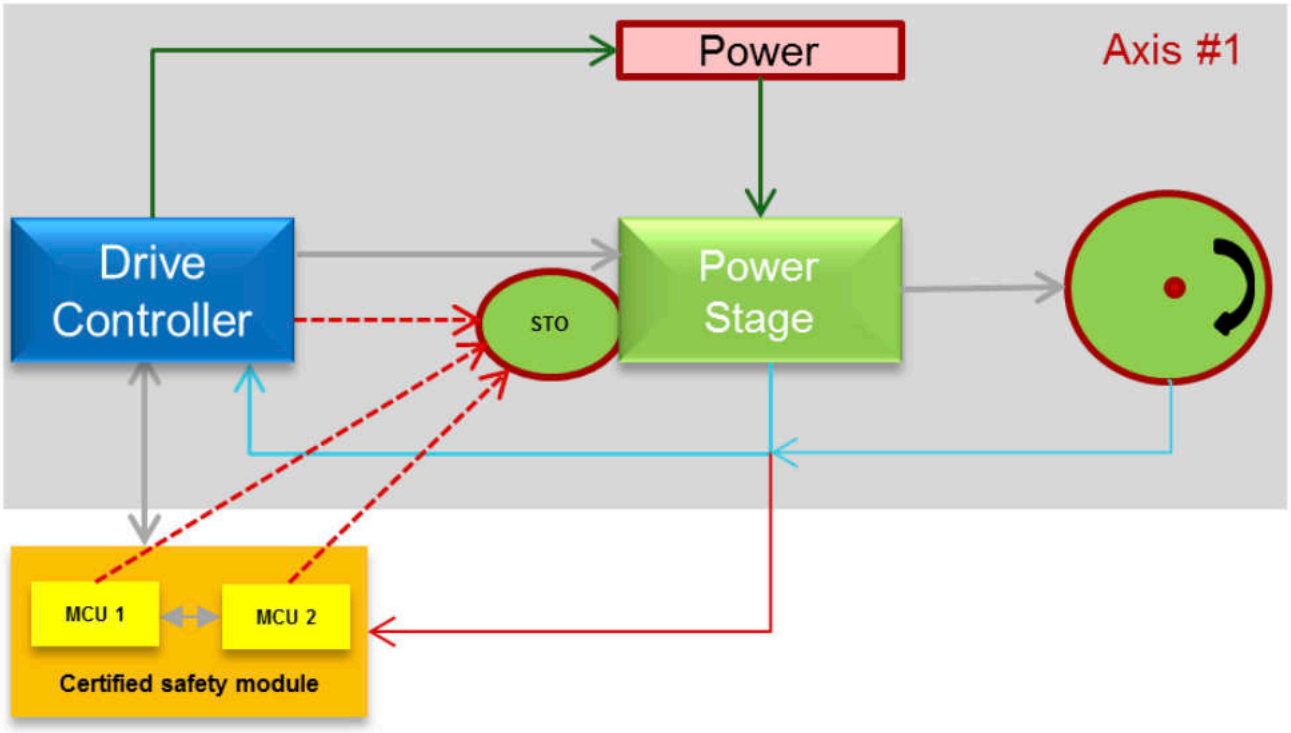

図 4-2. 同種冗長性

同種冗長性 (HFT = 1): 同一の二つのマイコンが独立したタスクを実行し、SPI/I2C 経由で相互チェックを行うことで、共通原因故障 (CCF) を排除します。

特性:

- 同一の二つのマイコンが、並列タスクをそれぞれ独立して実行します
- I2C、SPI、またはその他の絶縁インターフェイスを介して相互検証を行います
- 周期的に結果を比較し、不一致が検出されると安全アクションがトリガされます
- 故障検出のレイテンシ:10 ～ 100ms (構成可能)

利点:

- 独立した設計により、ほとんどの共通原因故障を検出できます:
- ハードウェア故障トレランス:単一のマイコンの故障が発生した後もシステムは動作を継続します
- 両方のコアを個別に監視および管理できます
- 複雑な安全性ロジックをサポートします

欠点:

- 二個のマイコンが必要で、コストが増加します
- クロスチェック通信を行うと、遅延が発生します
- 統合がより複雑になります

アプリケーション:SIL 3 HFT = 1 系

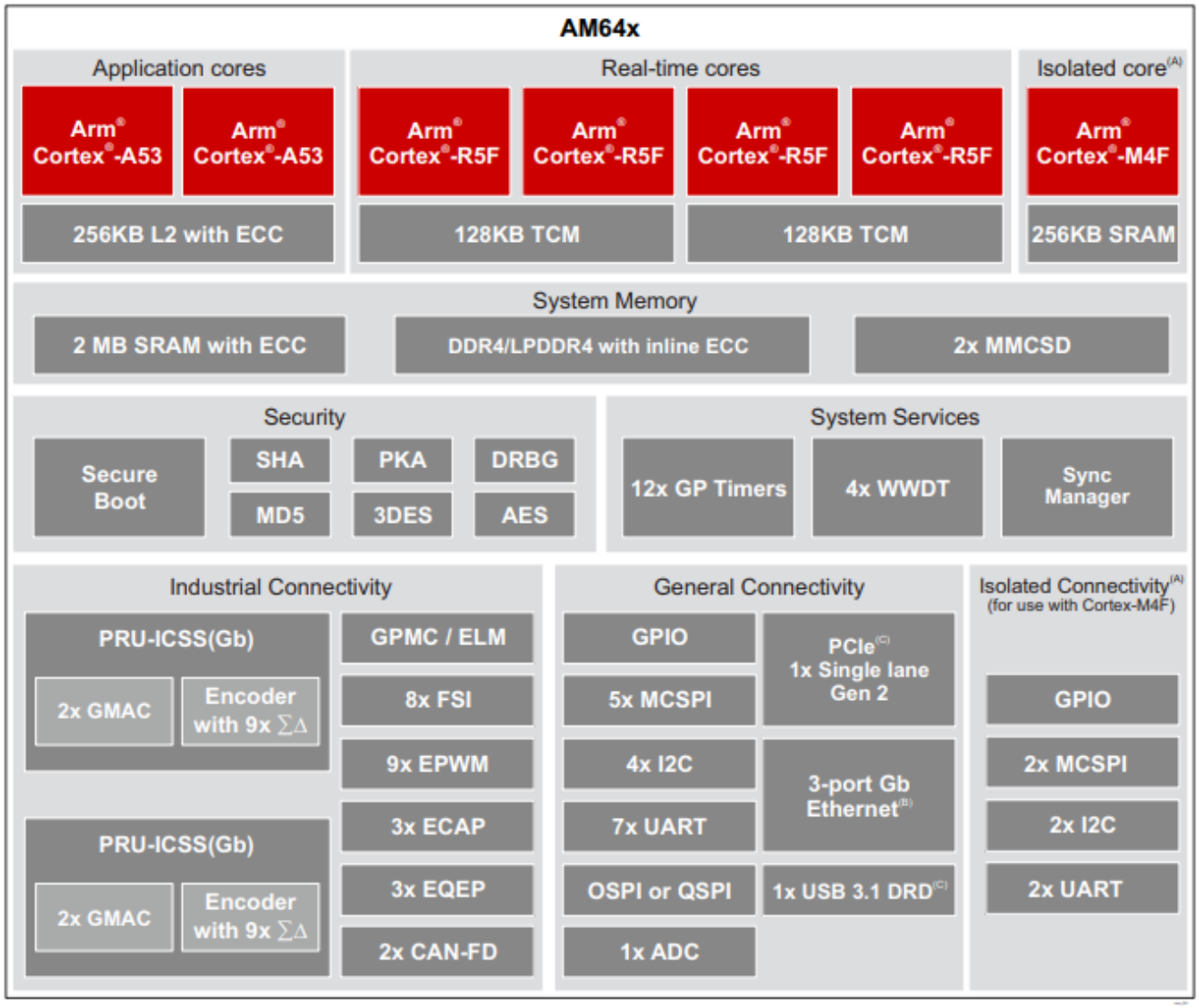

図 4-3. AM64 1 ページ

異種冗長性 (HFT = 0): 異なる種類のマイコン、または多様化されたソフトウェア実装により、システムレベルの故障を検出します。

特性:

- マイコンと MPU の組み合わせを採用したプロセッサのアーキテクチャを使用します。
- 異なるコア、さまざまな SIL 要件に異なるソフトウェアを実装します。低 SIL コアタスクを監視するには、高 SIL コアを使用します。
- ペリフェラル、電源、メモリを含むコア間のハードウェア分離。

利点:

- システムレベルの特定の設計上の欠陥を検出できます
- 最大限の冗長性と耐故障性
- あらゆるアプローチにおける低コスト

欠点:

- 開発の複雑さが高い
- 複数のプラットフォームに精通した専門知識が必要です

アプリケーション：SIL 2/3 または特別な ASIL-D 要件

4.2 TI マイコン / MPU に統合された安全機構 / 技術

TI は、各機能安全マイコン / MPU に対する認証済みソフトウェア診断ライブラリ (SDL) を提供しています。

SDL ライブラリの一般的なコンテンツ：

- CPU コアおよびバス診断ルーチン
- メモリ テスト アルゴリズム
- ペリフェラル内蔵自己テスト (P-BIST)
- ロジック内蔵自己テスト (L-BIST)
- クロック、電圧、温度の監視
- 割り込みと例外への対応

TÜV 認証に関する注記：SDL は、TÜV SÜD などの評価機関によって独立した評価を受けており、特定の SIL/ASIL レベルを満たすことができます。

また、TI マイコン / MPU はハードウェア SIL2 およびシステマティック SIL3 の能力を達成でき、以下に示す多くの安全対策を統合しています。

4.2.1 干渉からの自由 (FFI) デザイン

FFI は、単一の SoC でさまざまな安全レベル タスクを実行する際の重要な技術です。それは排除することができます

異なる ASIL/SIL レベルの部品間における連鎖故障や依存関係を排除し、低レベルの部品の故障が高レベルのセーフティ アイランドへ波及しないようにすることができます。

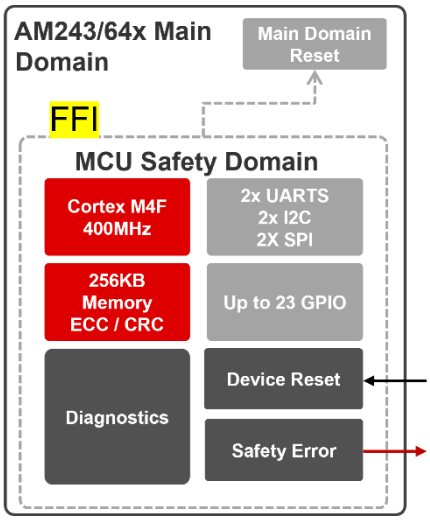

図 4-4. TI のマイコン / MPU における FFI の実装

FFI 外部側：非安全ドメイン - 標準アプリケーション、通信、重要でないタスク

FFI 内部側：セーフティ アイランド - 安全重視タスク、独立した R5F または M4F コア

FFI 分離メカニズム：

- ファイアウォール (ファイアウォール) - バス アクセスの制御
- タイムアウト ガスケット (タイムアウト ガスケット) - 通信パスを保護し
- 独立したクロック / 電源 / リセット
- 専用割り込みコントローラ

双方向矢印：必要な通信に必要な制御インターフェイス (SPI/I2C)

ステータス インジケータ：セーフティ アイランドは、非安全ドメインを独立して監視し、再起動することができます。

FFI の利点

- **コストの最適化**: 複数の安全レベルの機能を単一のマイコンに統合することで、総 BOM を削減できます
- **統合レベル**: 個別の外部安全マイコンは不要です
- **システムの複雑さ**: 統合の難易度を低減し、テストにかかる労力を低減します

4.2.2 メモリ保護と ECC 技術

マイコン / MPU 内のデータ パス: オリジナル データ → ECC エンコード → ストレージ → ECC 検証 → 訂正 / 検出

ECC は、メモリをランダム故障から保護するための中核技術です。

- シングルビット エラー (SBE) 検出と訂正のプロセス
- マルチビット エラー (DBE) 検出プロセス
- ハミング コードまたは SECDED コード パリティ ビットの生成。

AM243/AM64 を例として取り上げます。以下の ECC 範囲を参照してください。

図 11 キー メモリ内の ECC 範囲

メモリ タイプ	ECC のタイプ	範囲	注
L1 I キャッシュ	パリティ	A53 コア	検出のみ
L1 D キャッシュ	ECC SECDED	A53 コア	シングルビット訂正に対応
L2 キャッシュ	ECC SECDED	共有された 512KB	シングルビット訂正に対応
R5F SRAM	ECC SECDED	コアごとに 64KB	すべての R5F メモリをカバー
MCUSS SRAM	ECC SECDED	共有された 512KB	セーフティ アイランド メモリ
DDR EMIF	ECC オプション	メイン メモリ	お客様が設定可能

4.2.3 その他の統合型安全メカニズム

図 12 TI のマイコン / MPU 内にある他のメカニズム

安全メカニズム	説明	検出されたコンテンツ	範囲
ECC/EDAC	エラー検出および訂正	メモリ内のシングルビット反転	高
メモリ保護ユニット (MPU)	不正アクセスを防止します	スタック オーバーフロー、バッファ オーバーフロー、不正アクセス	中
ウォッチドッグ (WD)	プロセッサ ハングの検出	CPU デッド ループ、システム スタック	高
デュアル クロック コンパレータ (DCC)	クロックの異常検出	クロック周波数の偏差	高
エラー通知モジュール(ESM)	一元的な故障管理	すべての診断故障と応答をルーティングします	非常に高い
パワーオン リセット (POR/BOR)	電源監視	異常な電圧状態	中

5 機能安全 PLC アーキテクチャの設計

5.1 機能安全 PLC の必要性とアプリケーション シナリオ

機能安全 PLC が必要な理由

最新の産業用オートメーション:

1.規制安全要求事項の強化

- EU 機械指令は機能安全を義務付けています
- ISO 10218 (ロボット) には PL d/SIL 2 が必要です
- IEC 61800-5-2 (可変ドライブ) には SIL 評価が必要です

非準拠製品は市場に参入することはできません

2.人とロボットの協働が進展

- 協働ロボットは人と共存します
- 何らかの故障があると、人身傷害の原因となります
- 従来の PLC では、適切な安全保護を提供できません

3.システムの複雑性の増大

- 複数の独立したサブシステムが調整を必要とします
- 通信障害は、カスケード障害の原因となる場合があります
- 信頼性の高い故障検出および回復メカニズムが必要です

4.可用性と保守性の要件

- 生産停止によるコストが高い (1 分あたり数万単位)
- 迅速な故障検出と自動回復が必要
- 詳細な診断情報が必要です

5.2 機能安全 PLC アーキテクチャの設計

機能安全 PLC の重要な概念は、階層化、絶縁、冗長性です。

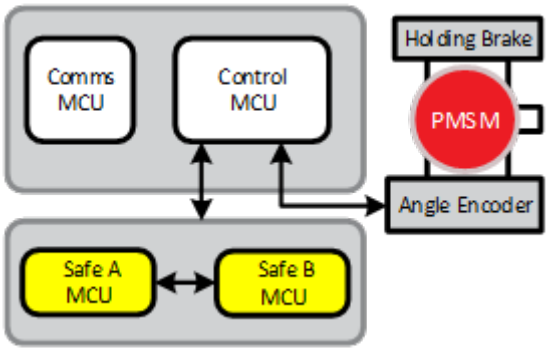

図 5-1. 標準マイコンと安全マイコンを分離したシステム コンセプト

コントロール プロセッサ (セントラル プロセッサ)

- 高性能 MPU (例:AM64x または AM243x)
- PLC スキャン サイクルとユーザー ロジックを実行します
- 複数の産業用通信プロトコルを処理します

安全サブシステム (安全サブシステム)

- 二つの独立した安全マイコン (AM243x または C2000)
- 個別の SRAM、ROM、ペリフェラル
- SPI インターフェイスを介したクロスチェック

- 出力 : 故障診断、ステータス レポート
- 絶縁型リレー ドライバまたは GPIO の直接制御

通信冗長性管理 (DLR / リング ネットワーク)

- AM243x/AM64x DLR スーパーバイザ マネージャ内蔵
- 二つの独立した通信パスを維持します
- PRU_ICSSG は、高速故障検出と転送を実行します
- イーサネット スイッチベースの冗長性
- 産業用イーサネット リンク層で処理

I/O モジュール

- モジュール形設計
- 各種 I/O タイプをサポート (DI/DO/AI/AO)
- オプションの故障検出 (ハイエンド モジュール)

5.3 設計実装事例

AM64/AM243 は、ハードウェア SIL2、システム SIL3 をサポートできます。AM243/AM64 データシートの詳細を参照してください。AM64 と AM243 はピン互換です。

さらに重要な点として、AM64/AM243 には 2 つの PRU_ICSSG サブシステムが統合されており、PRU_ICSSG に異なるファームウェアをロードすることで、産業用リアルタイム通信を実現できます。

各 PRU_ICSSG は以下を内蔵します。

- 二つの PRU コア (プログラマブル ロジック)
- ギガビット イーサネット MAC (RGMII/SGMII)
- リアルタイム データ バッファ (DPRAM)

以下に 2 * AM243 を FuSa マイコン モジュールとして使用し、別の 1 つの AM243 を通信モジュールとして使用する構成を示します。前章のシステム コンセプトと組み合わせて、TI の FuSa PLC ソリューションを示します。

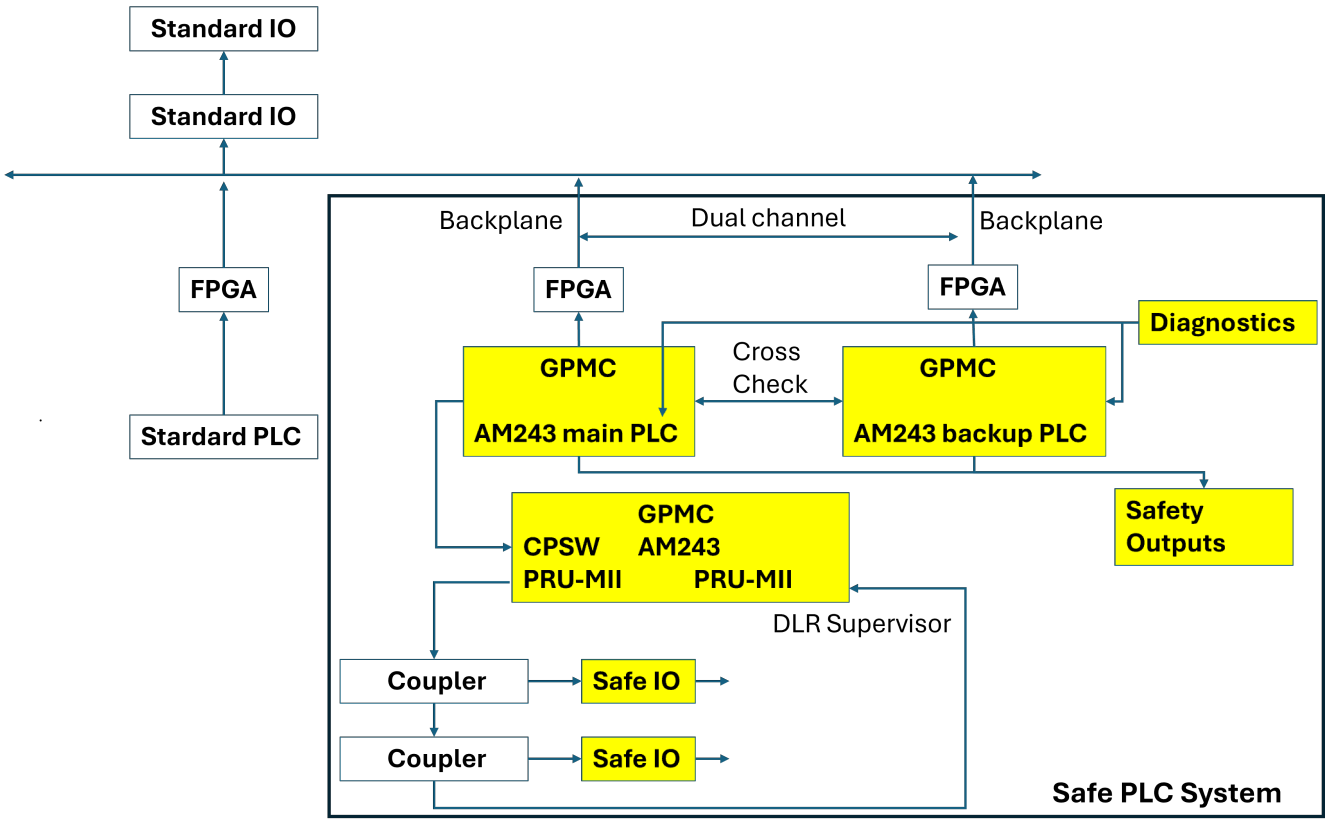

図 5-2. 機能安全 PLC アーキテクチャの例

標準 PLC と組み合わせることで、2 * AM243 が FuSa PLC システムとして機能し、SIL3、HFT = 1、CAT 3 を達成します。SPI または I2C を使用して、2 * AM243 間のクロスチェックを実装します。

もう一つの AM243 を通信モジュールとして動作させて通信を管理し、DLR スーパーバイザを実行して外部カプラと接続することで、安全 IO 点数を拡張します。

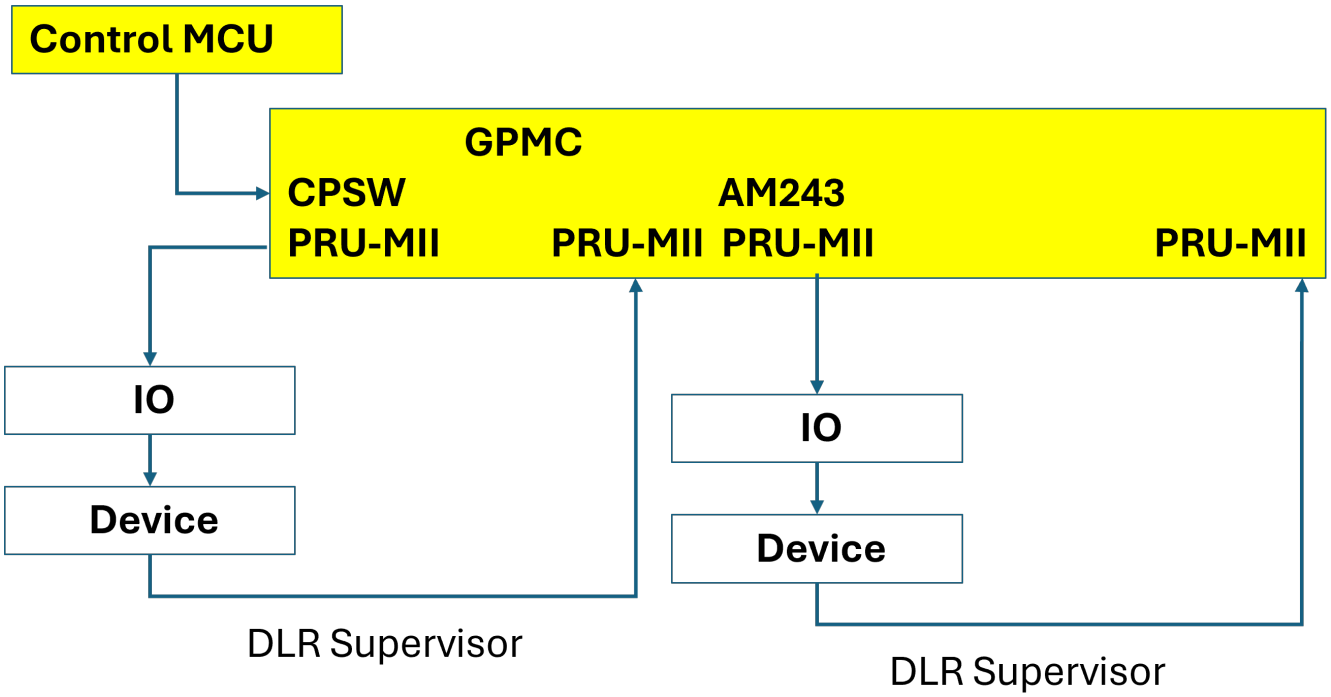

図 5-3. 冗長通信モジュールの例

AM243 には二つの PRU_ICSSG サブシステムが統合されており、最大五つの MAC ポートをサポートできます。内訳は、PRU_ICSSG の四つの MAC ポートと CPSW の一つの MAC ポートです。

- 一つの PRU_ICSSG は二つの MAC ポートをサポートし、DLR スーパーバイザは一つの R5F コア上で動作します。
- もう一つの PRU_ICSSG は 2 つの MAC ポートをサポートし、DLR スーパーバイザは一つの R5F コア上で動作します。
- CPSW 内の一つの MAC を使用し、制御マイコンに接続します。

アーキテクチャの主な特性

一般的なハードウェア インターフェイス:

- バックプレーン プロトコルはすべてのシリーズで同一
- I/O モジュールのフォーム ファクタを標準化
- 電源コネクタの標準化
- 異なるモジュールの組み合わせが可能

利点:

- お客様は複数のシステムを学習する必要はありません
- アップグレード コストが最小限 (主に CPU カード)
- 在庫管理を簡素化

実装によるメリット

1.コストの最適化

- 統合型プロセッサプラットフォームを使用
- 最下層のドライバとツールチェーンを共有し
- 顧客ニーズに応じた価格帯の提供

2.開発期間を短縮

- 部品と設計を再利用し
- 新製品ごとに開発サイクルを短縮で

- 機能安全認証の迅速化 (事前認証済みリファレンス デザイン)

3.保守性

- 統合されたコードベースとドキュメント
- テクニカル サポートと更新が容易
- 一貫性のあるユーザー トレーニング コンテンツ

4.市場対応範囲

- 小型デバイスはローエンド構成を使用
- 中規模デバイスはミッドレンジ構成を使用し
- 大規模で高リスクのアプリケーションにはハイエンド構成を使用
- 単一の製品ラインが市場全体をカバー

5.将来のアップグレード機能

- 産業規格が進化した場合 (新しいプロトコルのサポート)
- お客様は、ファームウェア アップグレードによって新機能を利用可能
- ハードウェアの交換は不要

5.4 TI の機能安全の設計リソース

システム レベルのサポート

- リファレンス デザイン
  - セーフトルク オフ (STO) リファレンス デザイン
  - 安全 I/O モジュールのリファレンス デザイン
  - DLR 冗長管理のリファレンス デザイン
  - TÜV による事前評価と認証

部品レベルのリソース

- 機能安全マニュアル (安全マニュアル)
- FMEDA 分析レポート
- 診断機能チェックリスト
- アプリケーション・ノート

ソフトウェア サポート:

- ソフトウェア診断ライブラリ (SDL)
- 事前認証済みのソース コード (TÜV 承認済み)
- 完全な API 資料
- サンプル コードと統合ガイド

ツールチェーン サポート

- SDK (ソフトウェア開発キット)
  - RTOS、ドライバ、プロトコル スタックを含みます
- SafeTI コンパイラ認定キット
  - ISO 26262/IEC 61508 コンパイラ検証に適合
- デバッグ ツール
- コード解析ツール

文書化およびガイダンス

- ホワイト ペーパーおよびアプリケーション ノート
- 機能安全に関するベスト プラクティス
- 標準マッピング ガイド
- アーキテクチャ設計ガイド]

6 まとめ

このアプリケーション ノートでは、テキサス インスツルメンツ (TI) のマイコンおよびマイクロプロセッサを使用して、機能安全規格 IEC 61508 および ISO 13849-1 に準拠した産業用プログラマブル ロジック コントローラ (PLC) を設計するための実践的な指針を提供します。基本的な概念から実装、実際のケース スタディまで、安全システムのライフ サイクル全体に対応します。

顧客にとっての価値

システム インテグレータの場合:

- 認証済みリファレンス デザインにより、開発期間を 40 ～ 60% 短縮
- 実績のあるアーキテクチャを使用して、認定サイクルを大幅に短縮
- 部品の再利用による総所有コストの削減

機器メーカーの場合:

- ISO 10218 (ロボット)、IEC 61800-5-2 (ドライブ)、各種ドメイン規格に適合する明確な経路
- 包括的な故障検出と冗長性により、賠償責任リスクを低減
- シンプルなアプリケーションから複雑なアプリケーションまで対応できる柔軟なアーキテクチャ

エンド ユーザーの場合:

- 適切な冗長性により 99.5% を超える可用性を実現したシステム
- 予防保守に役立つ包括的な診断機能
- ファームウェア変更によりアップグレード可能な将来性のある設計

重要な知見

アーキテクチャの選択:

- シンプルな安全アプリケーションでは単一の安全マイコンを使用し、複雑なシステムではマイコン + MPU による階層型アプローチを採用し、ネットワークが重要なアプリケーションでは DLR 冗長性を追加します。

診断戦略:

- すべての診断機能を実装するのではなく、ECC、ウォッチドッグ、FSoE、周期的セルフテストを戦略的に選択することで、目標 SIL/ASIL をコスト効率よく達成します。

通信の信頼性:

- FSoE プロトコルは、アプリケーション層のメカニズムにより標準イーサネット上で安全性を維持し、DLR は安全応答時間を損なうことなく、3ms 未満のネットワーク フェイルオーバーを実現します。

7 参考資料

1. AM64x Sitara™ プロセッサ データ マニュアル
2. AM243x Sitara™ マイコン データ マニュアル

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 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。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。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

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

最終更新日：2025 年 10 月