参考資料

Technical White Paper

ロボット・モーター・ドライブの安全性評価の簡素化

Ester Vicario, Kristen Mogensen *Systems Engineering and Marketing*

概要

産業環境でのロボット・システムの使用が増加している現状で、産業安全要件と国内および国際的な安全規制を継続的に更新し、人間が機械に近接した場所で作業する際に安全な環境を確保できるようにする必要があります。機能安全性評価は、デバイスが安全要件を満たしており、責任もって市場に投入できることを実証するために必要です。

市場投入までの期間が長くなるなど、安全性評価は長期的なプロセスになる可能性があり、製品の全体的な設計コストが増加する可能性があります。この資料では、評価プロセスを簡素化する方法を説明します。自律式移動型ロボット (AMR) 向けのモーター・ドライブを例として使用し、適切なデバイスを選択し、安全要件を満たし、全体の部品表 (BOM) サイズとコストを削減するために考慮すべき要素について説明します。このホワイト・ペーパーでは、安全要件を満たすための手順を説明することで、安全性評価を迅速化し、設計コストを削減する方法を示します。

目次

図の一覧

表の一覧

商標

1 はじめに

産業界は、製造レートと全体的な効率を向上させるために、オートメーションに依存しています。生産性を高めるため、企業は工場にロボットを導入しており、人間は引き続きこれらの機械と協力して作業を進めています。その結果、従業員は新しい種類の危険にさらされ、個人の安全確保のために統制が必要になります。

ロボットが安全要件を満たしていることを示すため、市場に投入する前に、各製品に安全性評価を実施する必要があります。評価では、機械が最低限の規制された安全要件を満たしていることを示す必要があります。製品が安全性に準拠していることを確認するのは通常、長期的で複雑な手順であり、全体的な設計コスト、ロボットのサイズ、市場投入までの期間が増加します。

このホワイト・ペーパーでは、モーター・ドライブの安全性評価に必要なプロセスについて簡単に説明します。システム設計プロセスの迅速化に役立つよう、使用される主要規格、アーキテクチャの種類、デバイスの選択について説明しています。

この特定のドキュメントでは、シングル・チャネル・モーター・ドライブ設計の安全に関する新しいコンセプトをベースラインとして使用しています。この安全に関するコンセプトは、ISO 13849 または安全性インテグリティ・レベル 2 にしたがってカテゴリ 2、パフォーマンス・レベル 2 (Cat 2、PLd)、および IEC 61508 規格にしたがってハードウェア・フォルト・トレランス = 0 (SIL 2、HFT = 0) を達成するためのブロック・レベルのコンセプトを提示し、読者がコスト効率の優れた方法で安全要件を満たすことができるようにすることを目的としています。たとえば、このホワイト・ペーパーでは、自律式移動型ロボット (AMR) などの産業用トラックに焦点を当てた ISO 3691-4 規格を参照していますが、Cat 2、PLD が必要な他のどの機械でも同じ手順を使用できます。

このコンセプトは、テキサス・インスツルメンツの最新の高性能モーター制御 C2000™ リアルタイム・コントローラと PMIC を使用しており、どちらにもオンチップの安全機能が含まれています。この製品ファミリ、設計コンセプト、その他の利用可能なテキサス・インスツルメンツの安全リソースを使用することで、システム全体の BOM 実装を低減し、市場投入までの期間を短縮できます。

2 Cat 2、PLD の安全要件について

必要な製品安全規格を理解することは、製品設計プロセスの重要な最初のステップです。このホワイト・ペーパーでは、移動型ロボットのモーター・ドライブを例として使用しているため、ISO 3691-4 製品の安全規格の要件を満たす必要があります。

2.1 ISO 3691-4 に準拠した安全要件

ISO 3691-4 規格は、自律式移動型ロボット (AMR) などの産業用移動型ロボット (IMR) を含む、ドライバレス産業用トラックの安全要件と検証を定義しています。この規格は、機械全体の安全要件を規定しているため、図 2-1 に示すように、産業用トラック・モジュール内で安全機能を配置する場所を決めるのは設計者です。

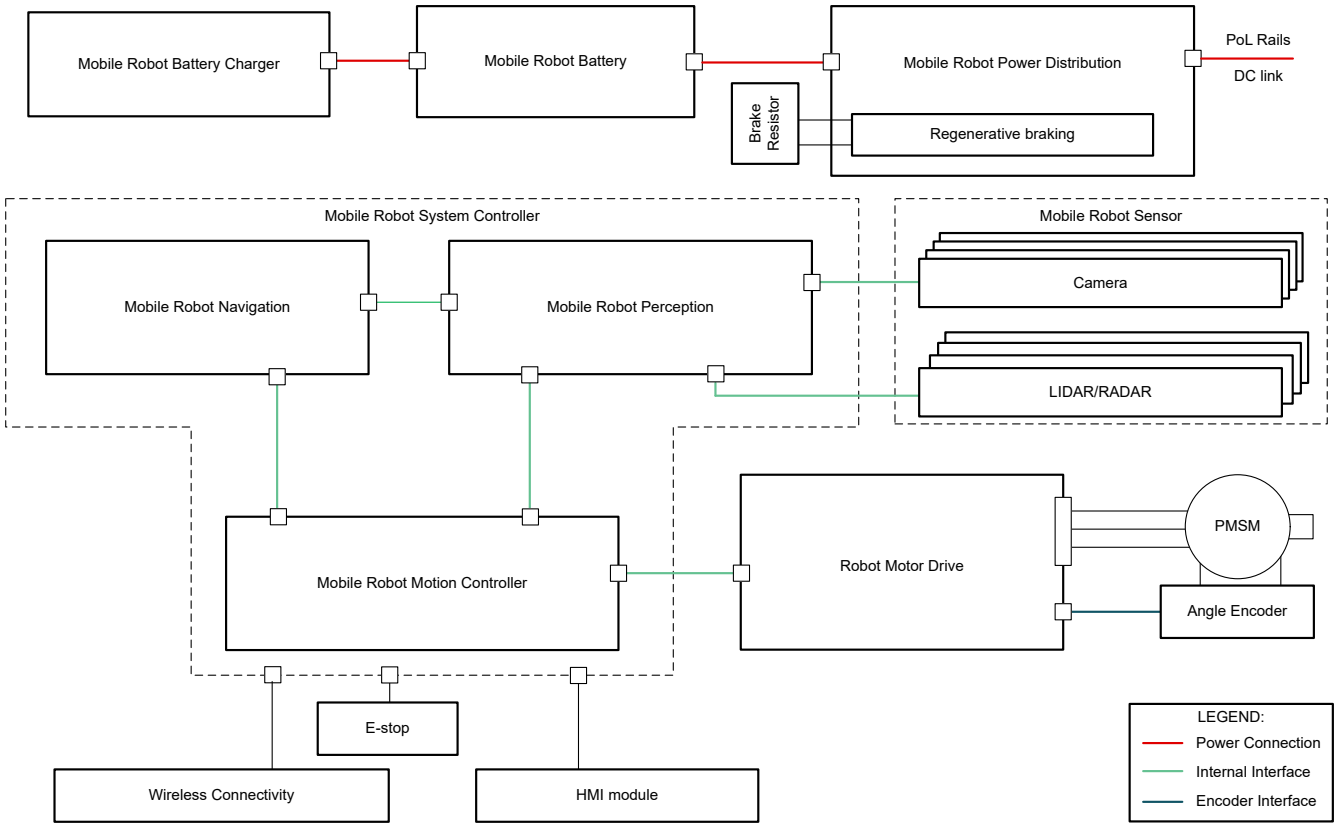


図 2-1. 簡略化した移動型ロボットのブロック図

安全規格 ISO 3691-4 には、危険な状況が存在する場合に必要なリスク低減を満たすために実装する必要のある、安全性に関する検討事項が記載されています。ここで説明した各リスク状況について、ISO 3691-4 規格は ISO 13849-1 に準拠した最小必要性能レベル (PL) を割り当てています。PL は、安全機能ごとに必要なリスク低減を実現するために一般的に使用される値であり、ISO 13849-1 機械規格で定義されています。

PL と同様に、いくつかの規格では、IEC 61508 に定義されている安全性インテグリティ・レベル (SIL) パラメータを使用して、システムの安全性能を測定します。PL レベルと SIL レベルの関係については、表 2-1 をご覧ください。

表 2-1. IEC 61508、ISO 13849 SIL、PL の関係

ハードウェア・フォルト・トレランス (HFT)								カテゴリ			
IEC 61508							ISO 13849				
0	1	2	0	1	2	SFF	DC	1	2	3	4
-	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3	60% 未満	なし				
SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4	60%～90% 未満	LOW	c	c	d	
SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4	90%～99% 未満	中程度		d	e	
	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4	99% 以下	HIGH				e
タイプ B			タイプ A								

SIL と PL はどちらも安全性能のディスクリート・レベルであり、これらのレベルは異なるパラメータを使用して診断機能を定量化します。SIL は、安全故障率 (SFF) をパラメータとして使用し、安全故障とシステムの合計故障の比率を定量化します。同様に、PL は DC パラメータを、システムに実装されている診断の有効性の尺度として参照します。ただし、SIL と PL はどちらも、反比例する 2 つの主要パラメータを通して関連しています。MTTF (Mean Time to Dangerous Failure、平均故障時間) - ISO 規格で使用され、PFH (Probability of dangerous failure per hour、1 時間あたりの危険故障率) は IEC 規格で使用されています。この関係を使用することで、システムの安全性を評価する際に PL と SIL の両方のレベルを使用できます。

表 2-2. PFH パラメータと MTTF パラメータを通した PL および SIL の関係

PL (ISO 13849)	PFH ターゲット値 [PFH = 1/MTTF]	SIL (IEC 61508、IEC 62061)
a	10^{-5} 以上 10^{-4} 未満	対応なし
b	≥ 3 x 10^{-6}～10^{-5} 未満	1
c	≥ 10^{-6}～3 x 10^{-6} 未満	1
d	10^{-7} 以上 10^{-6} 未満	2
e	10^{-8} 以上 10^{-7} 未満	3

PL または SIL は包括的な安全機能に適用されますが、通常はセンサ、データ処理、アクチュエータによって形成されます。これらの機能サブシステムのそれぞれは、最小の PL または SIL を満たす必要があります。サブシステムごとに、安全性レベルがどのように満たされているかを説明するために、さまざまな規格が存在します。たとえば、モーター・ドライブとアクチュエータの実装の場合、サブシステム固有の規格である IEC 61800-5-2 を使用して安全要件を指定します。

IEC 61800-5-2 では、モーター・ドライブの設計および開発に関する要件を定義しています。これには、安全トルク・オフ (STO)、安全制限速度 (SLS)、安全ブレーキ制御 (SBC) などの指定された安全サブ機能が含まれます。

規格内で、IEC 61800-5-2 は ISO 13849-1 を参照し、最小 PL を実現するために各サブ機能に必要な要件について説明しています。さらに、システム間の独立性、冗長性、処理時間などの要素については、前述の両方の規格で説明したとおり、システムを実装するときに考慮する必要があります。

したがって、システムの実装を開始する前に、アプリケーションごとの安全要件、実装する必要のある安全サブ機能、およびサブ機能ごとに必要なリスク低減レベル (SIL または PL) の間の主な関係を理解することが重要です。

この具体的なケースでは、ISO 3691-4 の表 1 に要約されているように、最小 PLD レベルが必要です。モーター・ドライブ・サブシステムに注目し、IEC 61800-5-2 で定義されている安全サブ機能を使用して PLD の要件を満たします。表 2-3 に、これら 3 つの規格の主な関係をまとめています。

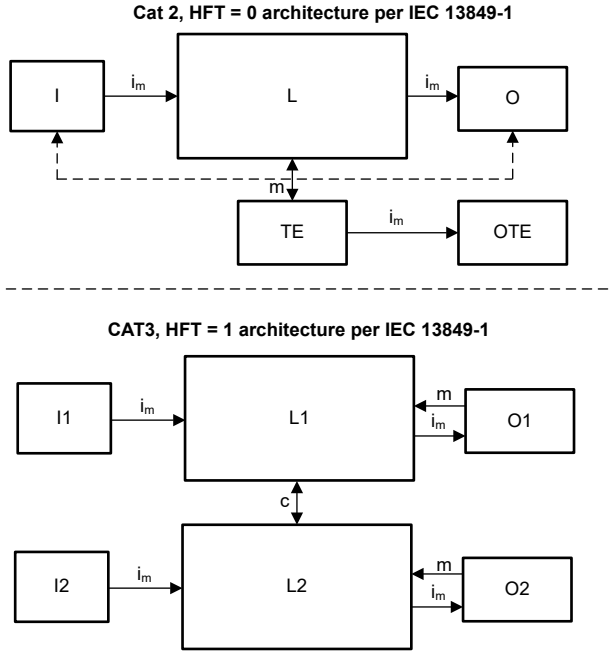
表 2-3. ISO 3691-4 に準拠した安全要件

EN ISO 3691-4 に準拠した安全機能	EN ISO 3691-4 に準拠した最小必要 PL	IEC 61800-5-2 に準拠した関連する安全サブ機能
ブレーキ・システム	d/b	SBC、SS1、STO
速度制御	d/c	SLS、SOS、STO
自動バッテリ充電	b	NR(1)
負荷処理	b	NR(1)
ステアリング	–	SLS
安定性	c	NR(1)
緊急停止機能	d	STO
人員検出システム	d/c	SLS、SOS、SS1、STO SDI
自動、手動の各メンテナンス・モード	d/c	SLS、SOS、STO
警告システム	a	NR(1)
立ち入り制限区域へのアクセス	d	SOS、STO

(1) NR: 実装は、ロボットのモーター・ドライブとは関係ありません

2.2 システム・アーキテクチャの選択

ISO 13849-1 規格では、必要な診断範囲と、システムの冗長性の量に関連するアーキテクチャのカテゴリとの関係が定義されています。すでに説明したように、ISO 3691-4 規格では、IEC 13849-1 規格で定義されているように、カテゴリ 2、HFT = 0、またはカテゴリ 3、HFT = 1 アーキテクチャを使用して達成できる最小の PLD 安全レベルが必要です。図 2-2 に示すように、この選択は、システムで必要とされる冗長性の量と診断範囲に影響を与えます。



I = 入力、L = ロジック、O = 出力、TE = テスト機器、OTE = 出力テスト機器、m = 監視、c = 比較

図 2-2. IEC 13849-1 のカテゴリ 2 と 3 の指定アーキテクチャ

表 2.1 Cat 2、HFT = 0 に示すように、90% を超える高い診断範囲 (DCavg = 90%) と引き換えに、システムの実装では必要な冗長性は少なくなります。必要な DCavg を満たすには、定義されたタイミング間隔内で診断機能を実行して、安全状態が確実にオン時間に達するようにする必要があります。一方、カテゴリ 3 アーキテクチャでは、診断範囲が低く、より緩和されたタイミング制約と引き換えに、デュアル・チャネル設計が必要です。

AMR の場合、主な制約要因の 1 つにシステム全体のなサイズと重量があります。したがって、この種のアプリケーションには、よりコンパクトな Cat 2 アーキテクチャが適しています。ただし、Cat 3 の実装が望ましい場合、テキサス・インスツルメンツは『C2000™ リアルタイム・マイコン向けの産業用機能安全』製品概要と、そのようなシステムの実装方法に関するガイダンスも提供します。

2.3 プロセスの安全時間に基づいたデバイスの選択

初期の安全要件と実装するアーキテクチャがわかったら、デバイスを選択します。一般的な出発点として、マイコンまたはプロセッサは他のデバイスよりも前に選択され、選択プロセスの際に安全機能や処理能力などの要素が重要な結果になります。

安全規格の中で、ISO 13849-1 はさまざまなタイミング要件を規定しており、システムが故障を検出し、定義されたプロセスの安全時間内に安全状態に到達できるようにしています。図 2-3 に、時間間隔の定義に使用される標準的な項目表記を示します。

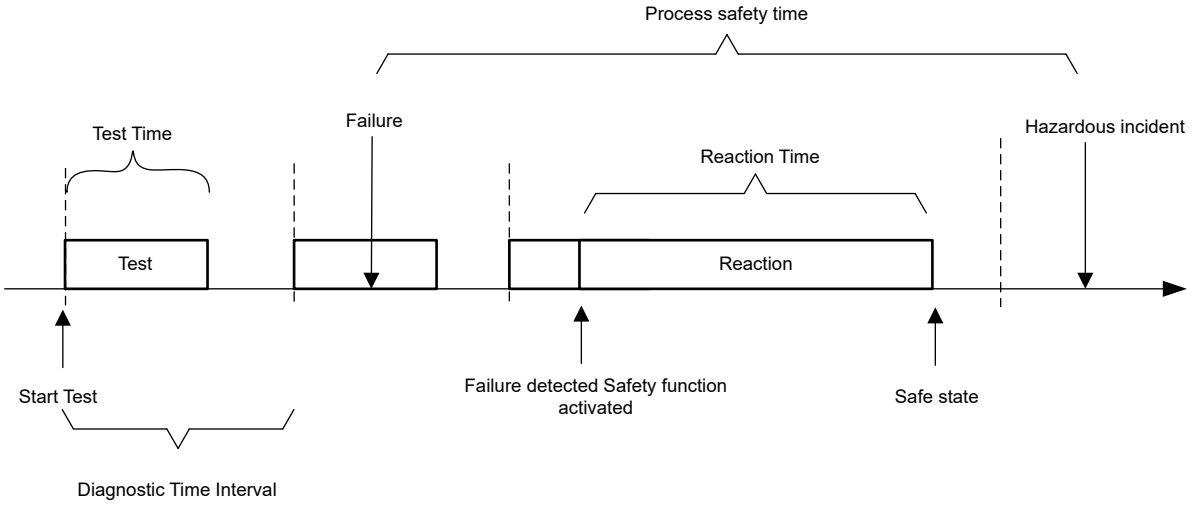


図 2-3. 機能安全関連のタイミングに関する考慮事項

診断時間間隔は、診断機能を実行し、それらから受け取った入力を処理するために利用できる時間の長さで構成されます。診断時間間隔が定義されている場合、診断範囲を拡大するとより強力なプロセッサが必要になります。

危険は予測不可能なため、AMR では診断を継続的に実行する必要があります。継続的に実行することで、故障を即座に検出し、必要なプロセス安全時間内にデバイスを安全状態に移行できます。

さらに、ISO 3691-4 では、物体との距離に応じて AMR の最大速度を定義することで、このテスト時間間隔をさらに制限しています。ワーストケースのシナリオを考慮することで、設計者はリスクを回避するために必要なプロセスの安全時間を計算し、物体の衝突前に安全状態に達していることを確認する必要があります。

ISO 3691-4 の表 A.1 に記載されている物体に対する最大速度と距離に基づき、安全プロセス時間は 415ms 未満でなければならないと推定されます。このタイミングでは、マイコンの診断機能を完了する必要があり、故障が検出された場合は、安全状態に達する必要があります。応答時間を十分に確保するには、診断時間間隔をプロセス全体の安全時間の 10% 未満にする必要があります。これは、システム機能の動作中に、完全な診断スイープに対して最大 41.5ms が許容されることを意味します。

これらのタイミング制約と Cat 2 アーキテクチャの選択により、モーター制御と安全要件の両方を満たすことができる安全性メカニズムを内蔵した強力なリアルタイム・マイコンを実現することが重要になります。テキサス・インスツルメンツの C2000 リアルタイム・コントローラと PMIC デバイスは、プロセスの安全時間と診断範囲の両方を満たし、PLD を実現するための優れた選択肢です。

3 移動型ロボット・モーター・ドライブの安全要件の実装

設計者は、システムの安全要件とアーキテクチャ・カテゴリを理解したら、残りのデバイスを選択し、モーター・ドライブ全体を実装して、安全要件が満たされていることを確認する必要があります。

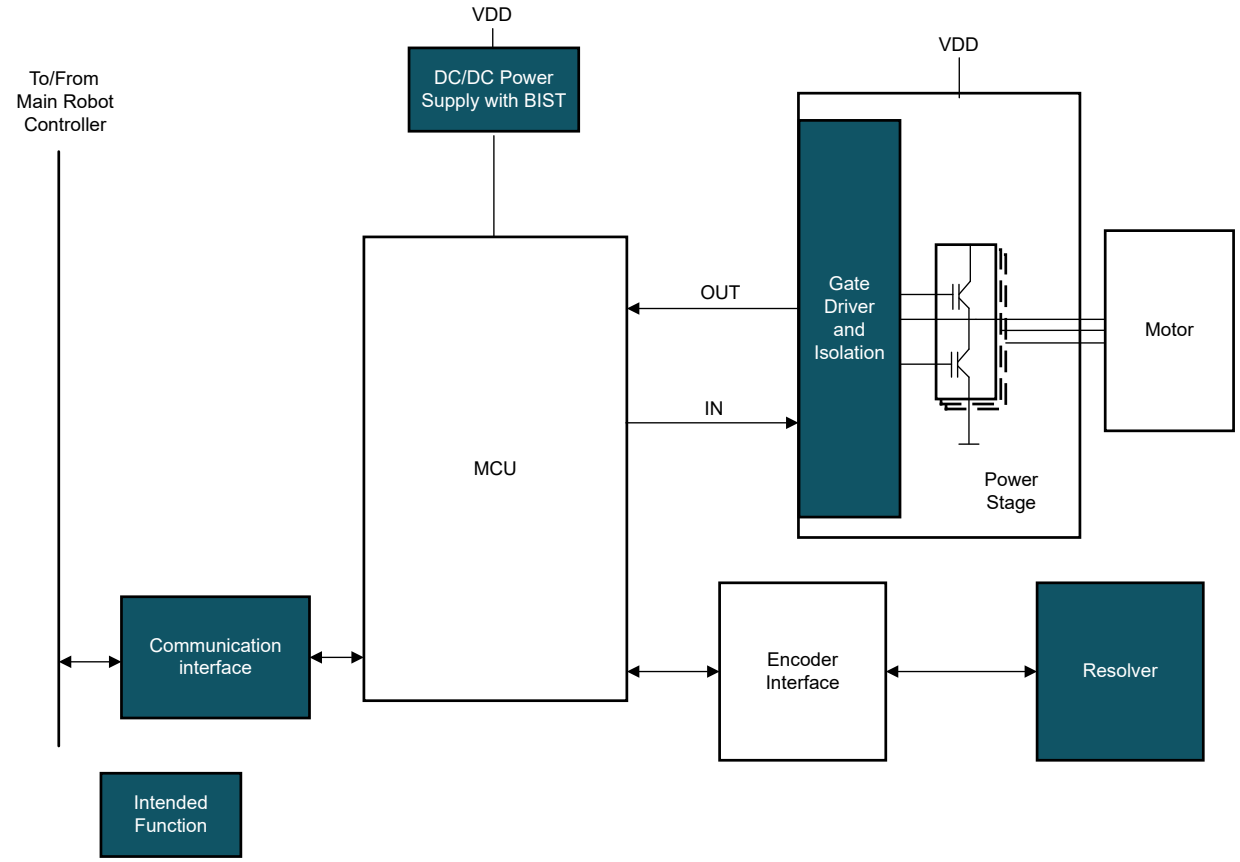


図 3-1. モーター・ドライブ・システム・ブロック図

図 3-1 に示すように、モーター・ドライブ・システムは通常、アナログ・フロント・エンド、エンコーダ、電源を統合できる電力段である MCU によって形成されます。

IEC 61508 では、必要な安全故障率 (SFF) は、デバイスのタイプがタイプ A かタイプ B によって異なります。IEC 61508 に従い、タイプ A サブシステムに故障モードが十分に定義されており、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。逆に、タイプ B サブシステムはより複雑なサブシステムであり、故障モードが完全に定義されていないため、故障条件を完全に判定できず、故障率を満たすのに十分なデータがありません。両方のタイプのサブシステムの完全な定義は、IEC61508 規格の 7.4.4 節に記載されています。

さらに、IEC61508 規格の CNB-M-11.059 改訂版では、診断サブシステムは、最小安全性レベルを達成するため、必要なシステム SIL レベルを下回る安全性レベルを達成するだけでよいと規定されています。この改訂は IEC61508 規格の一部ですが、診断サブシステムを分析するときは ISO 13849-2 機械規格と組み合わせて使用するのが最先端です。

したがって、この具体的なケースでは、SIL 2 システムが必要なため、SIL 2 システム要件を満たすには、診断関連モジュールは SIL 1 以上、最小 SFF = 0% を満たす必要があります。ただし、安全機能と非診断機能は引き続き SIL 2 を満たし、最小 SFF は 60% でなければなりません。

タイプ A とタイプ B のサブシステムを理解することで、利用可能な安全性に関する資料や診断機能などの機能に基づいてデバイス自体を簡単に選択できます。

マイコンはタイプ B デバイスであり、安全機能の実装に使用されるため、マイコンには最小 SFF = 60% が必要です。これは、必要な 60% の範囲を達成するために、デバイスが使用する各サブシステムを診断機能で監視する必要があることを意味します。

最初のステップとして、どのデバイス機能を使用する必要があるか、また各機能に必要な診断範囲を選択する必要があります。定義されたら、意図した各機能に対して十分な診断機能があるかどうか、または外部の診断デバイスが必要かどうかを示すために、安全性に関する資料が重要になります。

テキサス・インスツルメンツの最新 C2000™ リアルタイム・コントローラは、機能安全を考慮して設計されています。提供されている安全機能と資料を活用することで、安全性評価を簡素化し、迅速化できます。C2000™ の主な安全機能とデバイスの一部は、『C2000™ リアルタイム・マイコン向けの産業用機能安全』製品概要に記載されています。

さらに、さほど複雑でないデバイスについて、安全性に関する資料を入手することも重要です。すでに説明したように、デバイス・タイプ A の条件の 1 つは、デバイスの機能と故障モードを十分に定義する必要があることです。そのため、テキサス・インスツルメンツの安全性に関する資料の結果は、デバイスのタイプ、したがって必要な最小の SFF の正当性を示すのに有益です。

テキサス・インスツルメンツのマルチチャネル IC (PMIC) デバイスは、モーター制御モジュール全体の部品点数とサイズを大幅に削減すると同時に、安全要件を確実に満たすのに大いに役立ちます。内蔵 LDO、スーパーバイザ、BIST、ウォッチドッグ、DC/DC レギュレータなどの機能を搭載しているこれらの IC は設計の簡素化に役立つと同時に、マイコンと必要な電源レール両方を監視するために必要な診断機能を提供します。

ISO 13849 の節 6.1 に従い、安全機能を定期的に実行できない場合、この 60% の診断範囲を達成するために、診断機能と安全機能を同じ IC 内に配置することはできません。ISO 13849 では、IC 内の単一の故障によってこの IC の機能が完全に失われ、カテゴリ 2 では診断機能によって機能の損失を検出する必要があると考えています。したがって、機能の損失によって診断機能が失われないようにするため、同じ IC 内で電圧監視とウォッチドッグ Q/A を使用することはできません。この例では、外部電圧スーパーバイザと、PMIC デバイスの内部的な質疑応答 (Q&A) ウォッチドッグを使用します。スーパーバイザとリセット IC のパワー・マネージメント・フォルダには、機能安全をサポートする電圧スーパーバイザのテキサス・インスツルメンツの幅広い製品ラインアップが詳細に記載されています。

図 3-2 に、SIL 2 を達成するために使用できるいくつかの診断機能の非常に簡略化された例を示します。

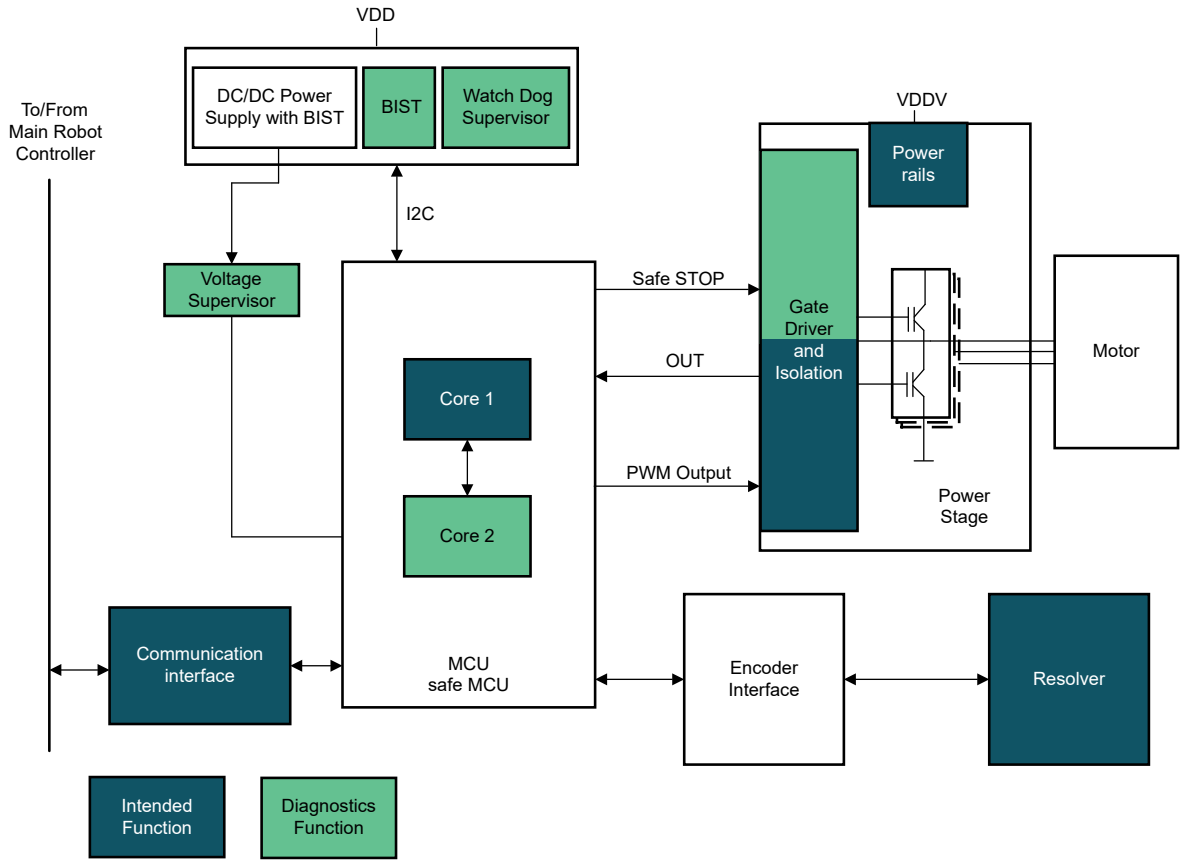


図 3-2. 安全機能を含む簡素化されたモーター・ドライブ・システム

安全機能をシステム・レベルで定義した後、各サブシステムが必要な安全要件を満たしていることを示すために、ブロック・レベルの分析が必要です。

この場合、安全サブシステムは安全機能と診断機能の間で分割されます。診断機能を使用して、安全機能がサブシステム・タイプごとに定義されている最小 SFF を確実に満たすようにします。表 3-1 に詳述します。

表 3-1. デバイス・タイプごとに必要な診断範囲の例

パラメータ	タイプ A	タイプ A	タイプ B	タイプ B
安全機能 (S)、診断機能 (D)	S	D	S	D
SIL	2	1	2	1
HFT	0	0	0	0
必要な最小 SFF|DC	60%	0%	90%	60%

目的の各機能が必要最低限の診断範囲を達成していることを適切に定義および実証することで、システムが必要な PL および SIL を達成でき、安全性認定を取得できることを実証できます。

4 まとめ

この資料では、安全認証済みシステムの実現のために従う手順を示しています。明確な製品設計および開発戦略により、市場投入までの期間をさらに短縮できます。さらに、安全性レベルを確実に満たすために必要な要件を適切に理解することで、デバイスの内部機能を最大限に活用して総 BOM を削減できます。したがって、テキサス・インスツルメンツが機能安全に関して蓄積した専門知識を活用すると、製品開発の際に大きなメリットとなります。

テキサス・インスツルメンツは、機能安全を重視したデバイスとリソースの幅広いポートフォリオを提供しています。テキサス・インスツルメンツの機能安全ページには、最適なデバイスを選択し、安全関連の知識を深めるための関連資料と製品に関する情報が掲載されています。

この資料に記載されている例の安全性コンセプト全体をテキサス・インスツルメンツの営業チームに請求します。全体的なコンセプトにより、移動型ロボットの安全認証プロセスが大幅に簡素化され、HFT = 0、PLD が必要なあらゆるタイプのモーター・ドライブにも使用できます。

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