参考資料

モータ制御の設計プロセスにおける機能安全への準拠の落とし穴の回避

Texas Instruments

Bharat Rajaram
Systems Engineering Manager
Arm-Based Microcontrollers

システム設計と機能安全への準拠を順に進めるべきではありません。残念なことに、従来の設計アプローチや多くの組織は、設計プロセスにおけるこれらのステップを、個別のサイロ化された活動として扱い、多くの場合、設計コストの増加や市場投入の遅れにつながります。

概要

1 **機能安全への準拠の定義**
機能安全規格の目標は、決定論的原因による障害を管理および軽減すると同時に、偶発的なハードウェア障害が発生したときにその障害を検出して防止 (または少なくとも安全な状態に移行) できるようにすることです。

2 **機能安全システム設計の 2 つの属性**
機能安全には、意図した機能を実現し、安全性インテグリティ・レベルを満たすためのシステムの開発が含まれます。

3 **機能安全のモータ制御システムと駆動システムを設計するための推奨アプローチ**
機能安全システムを設計するシステム・エンジニアは、設計プロセスの最初に機能安全への準拠に取り組む必要があります。後から考えるのではありません。

機能安全モータ制御アプリケーションを設計する場合、最初の設計要件として、まず機能安全への準拠に取り組むべきでしょうか。それとも、機能安全をアドオン機能として扱い、設計の最終段階に組み込むべきでしょうか。

機能安全は、モータ・ドライブの意図した機能と組み合わせて、設計の初期要件の一部である必要があります。これは標準的なことではありません。従来のシステム設計ワークフローでは、安全への準拠に相乗的に取り組んでいないからです。ただし、最初に安全性インテグリティへの準拠の必要性を考慮していない場合、システムを市場に投入するときに、コストのかかる遅延が発生する可能性があります。

Industry 4.0 の開始と、自動車の電動化とコネクティビティの成長に伴い、テキサス・インスツルメンツは機能安全への準拠へのアプローチを変更する必要があります。簡単に言えば、現在では、より多くのアプリケーションでより多くのモータ・システムが使用されており、機能安全規格に準拠するための基準が高くなっています。

機能安全への準拠の定義

IEC (国際電気標準会議) 61508 や ISO (国際標準化機構) 26262 などの機能安全規格の目標は、決定論的原因による障害を管理および軽減すると同時に、偶発的なハードウェア障害が発生したときにその障害を検出して防止 (または少なくとも安全な状態に移行) できるようにすることです。

独立した検証と検証を行う厳格な開発プロセスを採用すると、決定論的原因による障害の管理に役立ちます。

以下の方法により、偶発的なハードウェア障害を検出、防止、または安全な状態に移行することができます。

- 管理対象の機器を徹底的に理解する。
- 状況的な危険の可能性がある発生源と、発生の確率、影響の重大度、インシデントの制御可能性などの属性を分析する。

安全性メカニズムを各状況の危険と組み合わせることで、設計者は IEC 61508 で要求される安全故障率 (SFF) や故障 / 時の確率 (PFH) などの定量的指標を満たすことができます。たとえば、安全性インテグリティ レベル (SIL) 2 システムは、10 億時間以上の動作時間内に、SFF≧90% かつ PFH ≦ 1000 個の故障を達成している必要があります。

機能安全システム設計の 2 つの属性

機能安全規格は、すべてのシステムが故障することを想定しており (起きることはもはや確実で問題はいつ起きるか)、ゼロ・リスクというものは存在しません。

機能安全システム設計の 2 つの属性は、意図した機能を実現するためのシステム開発と、特定の SIL または車載 SIL (ASIL) のような安全機能に対応するための同じシステムの開発です。

設計者は多くの場合、これら 2 つの側面に個別に、または順次アプローチします。設計予算要件を満たすと同時に、大量生産アプリケーション向けの機能安全システムを設計することは困難です。**表 1** に、制御 / 駆動アプリケーションで意図される機能と安全機能の例を示します。

この概念をより的確に説明できるように、**表 1** のエレベータ・モータの例をご覧ください。

エレベータが意図する機能は、ユーザーの入力に基づいて人を上下に動かすことです。5 階に行くためにボタンを押せば、エレベータで行くことができます。

エレベータの安全機能はさらに一歩先を行き、以下を含むことができます。

- 階から階までスムーズに移動する。
- 各階で踊り場と同じ高さで停止する。
- エレベータが安全速度を超えた場合に自動的にブレーキをかける。

機能安全アプリケーション	意図した機能の例	安全機能の例 (および対応する SIL または ASIL ターゲット)
産業用:エレベータ・モータ	ユーザーの要求に応じてエレベータを上下に移動	• エレベータの安全な始動 / 停止 (ガタついた動きを回避) (SIL 2) • エレベータの速度が速すぎる場合に自動ブレーキをかける (SIL 3)
車載:電気自動車 (EV) のトラクション・モータ	アクセルまたはブレーキによる運転者の命令に従って EV を前後に移動	• 加速時のトルク不足またはトルク超過を防止 (ASIL C) • 強すぎる制動力を防止 (リアエンドを回避するため) (ASIL D)
産業用:スチール・プレス	工場の生産性を低下させずにスチール・プレスを動作させる制御サーボ・ドライブ・システム	• トルク超過または速度超過が発生した場合に駆動コントローラの電源をオフにするセーフ・トルク・オフ (STO) (SIL 3) • 安全制限速度 (SLS) により、オペレータが近接している場合でもモータ速度を許容範囲内に維持 (SIL 2) • SLS が境界チェックを超えた場合に STO をトリガする (SIL-3 など、生産性と安全性のバランスを取ってより高い SIL を駆動するため)

***表 1.** 制御 / 駆動アプリケーションにおける、意図した安全機能の例。*

意図した機能と安全機能がどのように連携して動作するかをより的確に理解するために、20 階建てのビル内にあるエレベータにプッシュ・ボタン回路 (**図 1** を参照) があり、エレベータのモータ・コントローラがエレベータを 25 階または 30 階 (つまり、建物内に存在しない階) に送ると解釈している障害が発生していると想定します。境界チェックでは、エラーが発生する前、または最終的に故障が発生する前に障害が検出されます。これは、機能安全の分野で受け入れられている進歩です。「障害」は「エラー」につながり、一部のエラーは「故障」につながる可能性があります。

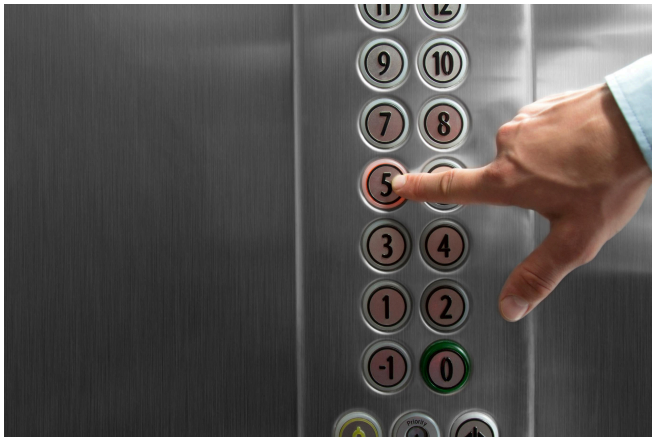

図 1. *最新のエレベータのプッシュ・ボタンの例。*

意図した機能設計と安全機能設計のプロセスを確認してみましょう。

モータ・ドライブの意図した機能設計プロセスでは、システム・エンジニアは意図した機能の要件を満たすマイクロコントローラ (MCU) を選択します。その後、回転子の位置、ライン電流、位相電圧、システム温度を監視するための内蔵 A/D コンバータ (ADC) チャネルなどのセンス機能を割り当てます。その後、システム・エンジニアはマイコンで利用できる処理機能を活用します。たとえば、マイコンの CPU にある MIPS (Million Instructions Per Second、毎秒数百万個の命令) を使用してモータ制御アルゴリズムを実行したり、PWM (パルス幅変調器) など利用可能な作動ペリフェラルを使用してモータ・ドライバ回路を駆動したりします。このプロセスには通常、数か月かかります。また、プリント基板 (PCB) の設計、モータ制御アルゴリズムの開発、すべての組み込みソフトウェアの開発とデバッグも含まれます。

独立した、ややサイロ化されたチームが安全機能設計プロセスを担当している組織では、独立した機能安全のエキスパートが同行し、システム・エンジニアが最初に選択したマイコンの機能安全マニュアルをレビューします。場合によっては、機能安全のエキスパートは、SEooC (Safety-Element-out-of-Context) 安全コンセプトで、エラー・テスト、ハードウェア冗長性、D/A コンバータ (DAC) から ADC へのループバック・チェックを含む機能の SW テストの使用、または拡張キャプチャによる拡張 PWM の監視が必要になると気付くことがあります。前述のエレベータの例を思い出すと、複数の ADC チャネルを使用して各階にあるレベル・センサを監視し、マイコンの ADC 内に存在する「固着」障害から保護する必要性が生じることがあります。

ADC と PWM のチャネル数が不十分な場合や、機能安全を実現するための CPU MIPS が不十分な場合、図面ボードに戻って、機能安全システムを実現するために別のマイコンを選択する必要性が生じることがあります。これまでにその個別のシステム設計チームが実施してきた作業が取り消される可能性があります。

設計ステップが連続的に実施されない場合でも、それらは多くの場合、別々の組織のサイロで実施されます。つまり、システム・エンジニアは通常、機能安全に関する専門知識を何も持っておらず、機能安全のエキスパートはシステム・エンジニアではありません。このサイロ化されたアプローチは、最終的には同じ問題をもたらします。つまり、システム・コストの増加と、市場投入までの数か月の遅延です。

機能安全のモータ制御システムと駆動システムを設計するための推奨アプローチ

機能安全システムを設計するシステム・エンジニアの最終的な目標は、設計プロセスの最初に機能安全への準拠に取り組むことです。

設計予算に適合する機能安全システムを設計して提供するには、安全性への準拠と意図した機能の両方について相乗的な分析を行う必要があります。個別または連続的にプロジェクトにアプローチすると、課題が発生したり、システム設計目標を達成できなくなったりする可能性があります。安全機能設計プロセスを管理するチームを対象にした前述の例を考慮すると、以前のコラボレーションでは、新しいマイコンを選択して PCB を再構成する必要が生じていた可能性が高くなります。

実際、別の例で、推奨されるアプローチを説明できる場合があります。**図 2** に示すように、人間の脳は左半分 (論理的) と右半分 (創造的) の両方を適用して、問題を全体的に解決します。

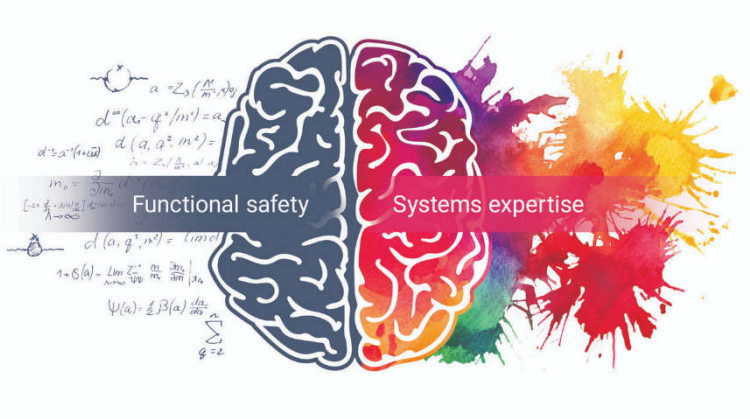

図 2. 単一の脳はシステム設計と機能安全への準拠の両方に対する統一された専門知識を備えています。

脳は、それぞれが異なるチームまたは内部の設計リソースを代表する単一の組織であり、設計プロセスにおいて特定の分野に対する視点を持ち込むことができると考えてください。一緒に設計ワークフロー内で 1 つのユニットとして機能し、明確で継続的なコミュニケーションを維持しながら、専門分野から設計にアプローチできます。

同様に、最も効果的な設計プロジェクトでは、システム設計者と機能安全のエキスパートで構成されたチームが協力して機能安全システムを実現します。

市場への投入期間を短縮できるように、システム・エンジニアは適切な設計リソースを必要としています。たとえば、テキサス・インスツルメンツはサブシステム・レベルおよびシステム・レベルの機能安全コンセプトを開発し、これらはサード・パーティーによって独立して評価されます。

機能安全システムの設計をサポートする テキサス・インスツルメンツ製品

テキサス・インスツルメンツの製品ポートフォリオは、モータドライバやゲートドライバから、AM2434BSDFHIALVR などの C2000™ や Arm® Cortex® ベースのマイコンを含む、独自の CPU アーキテクチャに基づくマイコンまで多岐にわたります。これらの製品は、高度な診断機能とオンチップ センシング ペリフェラルを搭載しており、障害を迅速に検出して対処すると同時に、システムのダウンタイムを最小限に抑えます (産業用環境では工場の生産性を向上させます)。

機能安全の設計で最も効果的なデバイスをお客様が見つけられるように、テキサス・インスツルメンツでは機能安全アプリケーションでの使用に適した 3 つのカテゴリの製品を定義しています。テキサス・インスツルメンツ機能安全対応、テキサス・インスツルメンツ機能安全品質管理、および テキサス・インスツルメンツ機能安全への準拠となっています。(当社のモータドライバ、ゲートドライバ、マイコンは通常、テキサス・インスツルメンツの機能安全への準拠製品です。)

テキサス・インスツルメンツは、IEC 61508 と ISO 26262 の決定論的能力準拠勧告に適合するようにこれらの製品を設計、製造しており、安全で信頼性の高いモータ制御 / 駆動システムの製造を可能にします。当社は、FMEDA (故障モード、影響、診断分析)、機能安全マニュアル、(該当する場合は) 安全診断ライブラリで各デバイスをサポートしており、システムとサブシステムの機能安全コンセプト レポートを TI.com で、またはご要望に応じて入手できます。テキサス・インスツルメンツのマイコンの機能安全マニュアルには、SEooC の状況に応じた考察や、アプリケーション例に対する想定される障害グループの概要が記載されています。

当社の設計リソースの例には、**産業用ドライブ向け TUEV 評価済みセーフ トルク オフ (STO) リファレンス デザイン (IEC 61800-5-2)** 内の「産業用ドライブ向け TÜV SÜD 評価済み STO モジュール」があります。当社の機能安全製品の詳細については、**www.ti.com/technologies/functional-safety.html** をご覧ください。

テキサス・インスツルメンツは ISO 26262 SEooC と IEC 61508 に準拠する部品を使用した経験があり、テキサス・インスツルメンツ製品が使用される機能安全システムの種類も理解しています。もちろん、これらの利点を実現するには、目的の機能と安全機能の両方を開発するという複雑なニーズのバランスを取る必要があります。

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