参考資料

産業用固定ロボットおよび移動ロボットの安全な電力実装のために電圧監視機能を統合

Jackson Wightman
Applications Engineer
Voltage References and Supervisors

Kristen Mogensen
Systems Engineer
Robotics Systems

概要

このホワイト ペーパーでは、IEC (国際電気標準会議) 61508 規格に準拠して安全な電源を設計する方法を紹介します。ここでは、電源監視の設計慣行を説明し、安全な電源投入と円滑な障害回復のために電圧監視が不可欠である理由を示します。内蔵セルフテスト (BIST) やラッチ クリア ピンなど、電圧監視 IC の新しい機能により、正確な電圧監視を行うだけでなく、機能安全の設計慣行を大幅に改善できます。

はじめに

最新の製造施設では、産業用固定ロボットや移動ロボット用モーター ドライブは、工場の生産量、効率、安全の向上に役立っています。しかし、ますます増加する (そして強力になっている) 自動化ロボットと一緒に工場の従業員が働いている現状では、システム設計者は、より厳格な安全要件に適合する必要があります。従業員とロボットの真の協働を実現するためには、標準または最新のテクノロジーの投入および使用は、いかなる状況においても安全でなければなりません。また、故障発生時の適切な電源の切断または動作の調整は、安全の重要な要素です。システム レベルの機能安全要件を満たすには、このようなロボットやその他の電子機器のための安全な電源設計が不可欠です。

電源設計における安全に関する考慮事項および潜在的な障害

完璧な環境では、電源は、特定の設計要件を超える揺れや変動のない、一定の電圧および電流を供給します。しかし、現実の世界では、そうはなりません。電源装置には、誤動作をもたらす本質的な特性があるだけでなく、時には障害が発生する可能性もあります。これらの障害は、さまざまな形で発生します。**表 1** に、いくつかの電源障害の例とその原因を示します。

電源障害の影響	原因:
電圧が出力されない	電源入力の欠損
電源の供給電圧が高すぎる	負荷インピーダンスの急激な変化、下流側への短絡
電源の供給電圧が低すぎる	電源入力が不十分、電源入力の欠損
マイクロコントローラ (MCU) のブラウンアウト	電源入力が不十分、電源入力の欠損

表 1. *電源障害とその原因。*

人間の周囲で定常的に動作する装置や技術を設計する場合、電源の障害による危険を軽減するために、適切な手順を実行する必要があります。このことは、産業用移動ロボットや協働ロボット、または障害が致命的な事態を招く可能性のあるその他の各種技術を含めて、さまざまなアプリケーションに当てはまります。たとえば、モーター ドライブ アプリケーションでは、装置のトルクが予測できない状況は、非常に危険でリスクが高い可能性があります。

しかし、電源が仕様をはずれて変動していることを検出するにはどうすればよいでしょうか。電源の変動が問題になるのはどの時点でしょうか。産業用アプリケーションのシステム全体で、潜在的な障害はどのようにして発生しているのでしょうか。

産業用システムにおける機能安全および規格の概要

制定された機能安全規格は、システムが安全かどうかの判断に役立ちます。最も一般的な規格は、IEC 61508 および国際標準化機構 (ISO) 13849 です。どちらの規格も、故障モードの診断範囲または安全側故障割合、およびハードウェア フォールト トレランスを調べて、システムが満たす安全度水準

(SIL) またはパフォーマンス レベル (PL) を決定します。**表 2** に、これらの等級レベルをまとめます。

ハードウェア フォールト トレランス (HFT)					カテゴリ			
IEC 61508				ISO 13849				
0	1	2	SFF	DC	1	2	3	4
-	SIL1	SIL2	60% 未満	なし				
SIL1	SIL2	SIL3	60%～90% 未満	低	c	c	d	
SIL2	SIL3	SIL4	90%～99% 未満	中		d	e	
	SIL4	SIL4	≤99% (1,000 万分の 5 以下、0.5ppm 以下)	高				e
タイプ B								

表 2. *IEC 61508 と ISO 13849 安全規格の比較*

表 2 をガイドとして使用すると、IEC 61508 SIL または ISO 13849 PL それぞれを取得する方法が複数あることがわかります。適切な安全側故障割合、診断範囲、ハードウェア フォールト トレランスを備えたシステムを設計すれば、これらの等級レベルのいずれかを達成できます。特に、電源の電圧を監視すると、診断範囲を増加させることができます。電圧監視を実装することで、ハードウェア フォールト トレランスも増加させることができます。

表 3 に、これらの安全パラメータの詳細を示します。

ご覧のとおり、起こりうる故障の数だけでなく、故障が発生する確率も考慮する必要があります。診断範囲や安全側故障割合を増加させることにより、同じハードウェア フォールト トレランスでも、より高い SIL または PL を達成できます。その逆も同様です。電圧監視は、システムの診断範囲または安全側故障割合を判定し、システム ソリューションの残留 FIT (故障率) を低減するために重要な要素です。

測定時	定義
ハードウェア フォールト トレランス (HFT)	システムにおいて、安全機能を維持したままで許容可能な障害個数の最小値
SFF (Safe Failure Fraction：安全側故障割合)	$\frac{\text{Total safe failures} + \text{Total detected dangerous failures}}{\text{Total safe failures} + \text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (1)
診断範囲	$\frac{\text{Total detected dangerous failures}}{\text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (2)
SIL	機能安全の等級レベル体系

表 3. *機能安全のレベルに関する重要な用語。*

電圧スーパーバイザ IC を使用した電圧監視

電圧の監視は、多くの方法があります。さらに、監視対象の電圧もさまざまである可能性があります。産業用アプリケーションでは、過電圧または低電圧の状態として、48V までの高い電圧または 0.8V までの低い電圧を監視する必要が生じることがあります。幸いなことに、システム内で重要な電圧レールの監視に効果的な方法があり、それによっていずれかの機能安全設計のいくつかの要素を実現できます。高精度の電圧監視機能を使用すると、安全状態を実現するために、いつシステムを完全に電源オフするか、いつ MCU をリセットするか、あるいは、システム レベルの他の選択をするべきか、ということを把握できます。安全関連の電圧レールを継続的に監視しなければ、潜在的に危険な状況が発生した場合に、システムは対策を講じることができません。

ディスクリート部品を使用して電圧監視回路を設計する方法もありますが、機能安全を重視したシステムでは、電圧監視機能が 1 つのサブシステム回路に統合されていれば、診断範囲を判定するのがかなり容易になります。したがって、電圧スーパーバイザ IC は、機能安全のために特に有用であり、スレッショルドの精度、静止電流、リセット時間遅延、ラッチ機能、電圧ヒステリシス、出力タイプ、BIST について、さまざまな組み合わせが用意されています。

表 4 に、電圧スーパーバイザのパラメータおよび機能を示します。

パラメータまたは機能	概要
スレッショルド精度	公称スレッショルド電圧に関連する精度のパーセンテージ。
最小入力電圧	デバイスが監視可能な最大電圧。
静止時電流	アイドル時にデバイスが消費する電流の量。
リセット時間遅延	フォルトがなくなったときに、デバイスがフォルト状態から解除されるまでに要する時間。
電圧ヒステリシス	スレッショルドと、デアサートされるスレッショルドとの差。このパラメータは、監視対象の電圧が発振している場合に、誤ってデアサートされることを防止するのに役立ちます。
出力トポロジ	アクティブ Low またはアクティブ High 形式の電圧スーパーバイザ (オープン ドレインまたはプッシュ プル) の出力ピン。
ラッチ	フォルトが発生すると、ロジックをクリアする信号をスーパーバイザ IC が受信するまで、フォルトを表示するピンはアサートされた状態を維持します。
BIST	内部フォルトをチェックするための内部デバイス診断機能。

表 4. *電圧スーパーバイザの重要なパラメータ。*

電圧スーパーバイザ IC は、電圧を監視します。電圧が低電圧または過電圧状態になると、電圧スーパーバイザは、MCU への通知、電源スイッチの切り替え、またはゲートの駆動を行うことができます。電圧スーパーバイザは、電源に変化があったことを検出し、安全で有効かつ迅速に、電源を切断することができます。低電圧と過電圧の両方を監視するスーパーバイザは、ウィンドウ スーパーバイザとも呼ばれます。実施する電圧監視の種類も、機能安全の等級レベルに影響があります。

表 5 に、これらの等級レベルを示します。

電圧監視の種類	診断範囲または安全側故障割合の可能性
オーバーボルテージ	60%
ウィンドウ (過電圧および低電圧)	90%～99%

表 5. *電圧監視が DC (診断範囲) に及ぼす影響*

安全回路を設計する場合は、診断範囲のレベルを考慮することが重要です。さらに、電圧スーパーバイザ IC を使用すると、必要な回路部品の数が減り、設計が簡単になります。

電圧監視が機能安全レベルに与える影響

目標の SIL または PL に向けて設計する際には、ハードウェア フォールト トレランスまたは安全側故障割合を考慮することが重要です。これは、設計の冗長性と、システムへの電圧監視の実装方法に関するものです。最も一般的な 2 つの規格は、機能安全レベルを確保する、または高める方法をいくつか定義しています。電圧監視は、この決定を下すために、または機能安全を向上させるために重要な要素です。電圧モニタを使用した SIL 2 対応設計については、図 1 および 図 2 を参照してください。

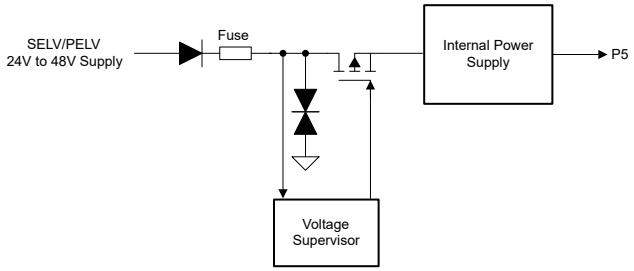

図 1. *電源および電圧監視を行うハイサイド安全電源の IEC 61800-5-2 実装。*

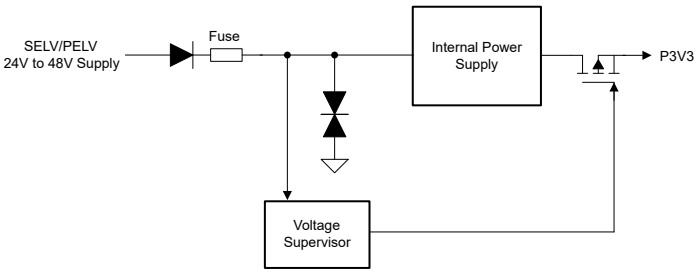

図 2. *IEC 61800-5-2 実装のもう 1 つの事例、電源および電圧監視を行うローサイド安全電源。*

図 2 では、電圧スーパーバイザは 1 つのチャネルとして機能して過電圧を監視し、必要があれば低電圧も監視できます。

電圧スーパーバイザの出力により、安全な動作範囲を超えた場合に電源を切断するか、または、MCU にフォルト状況を通知できます。図 1 および 図 2 の回路のハードウェア フォールト トレランスは 0 であり、最大 90% の安全側故障割合または診断範囲を実現できます。したがって、図 1 は、SIL 2 または PL d レベルまで対応可能です。

これと同じ論理により、回路構成のハードウェア フォールト トレランスを高めると、機能安全のレベルが向上します。図 3 に、電圧監視を使用して回路構成のハードウェア フォールト トレランスを高める方法の例を示します。

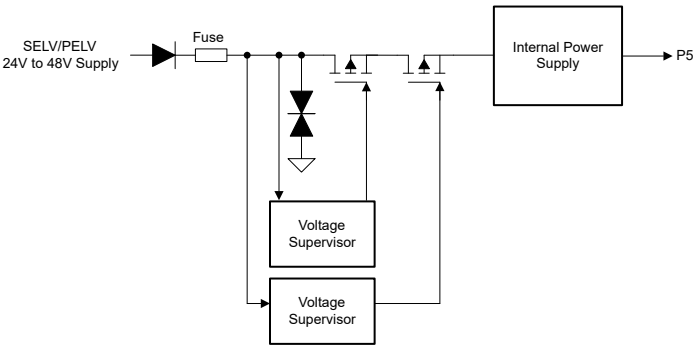

図 3. *電圧監視を使った SIL 3 対応電源のブロック図。*

2 つの電圧スーパーバイザを並列に使用することにより、過電圧または低電圧状態を監視するために 2 つのチャネルを用意できます。これらの電圧モニタは、それぞれが個別に、システムの他の部分から電源レールを切り離す手段と結合されているので、一方の電圧スーパーバイザに障害が発生した場合でも、もう一方の電圧スーパーバイザが規定された手順を正しく安全に実施でき、この設計で SIL 3 のレベルまで達成できます。

図 3 に示すような回路構成において、機能安全を高めるもう 1 つの方法は、電圧スーパーバイザの実装方式の多様性を使用することです。IEC 61508 規格の記述に従って、電圧スーパーバイザ デバイス間での共通原因故障の事例を考えてみましょう。2 つの異なる電圧スーパーバイザ技術を使って同じ電源レールを監視すると、共通モード故障の可能性を減らすことができます。

たとえば、異なる電圧スレッショルド値を持つ 2 つの電圧スーパーバイザを選択すると、多様性を高められる可能性があります。別の例として、図 3 に示すような回路構成では、電圧ス

ーパーバイザ機能ブロックの 1 つにテキサス・インスツルメンツの TPS3762 を使用し、他方にテキサス・インスツルメンツの TPS37 を使用することによっても、機能の多様性が高くなります。これは、2 つのデバイスが 2 つの異なる設計であるからです。

この時点で皆さんが疑問に思うのは、電圧監視方式が故障した場合、すなわち電圧監視回路を構成する部品が正常に機能しなくなった場合にどうするべきか、ということです。これは、電圧スーパーバイザ IC が特に有用であるもう 1 つの事例です。一部の電圧スーパーバイザ IC は、BIST 機能を備えています。このようなスーパーバイザは、ウィンドウ電圧モニタであり、デバイスがそれ自体の機能をテストするように要求できる入力ピンもあります。要求に応じて、電圧モニタは内部テストを実行し、引き続き期待どおりに動作していることを示す信号を出力します。

図 4 に、そのような実装を示します。

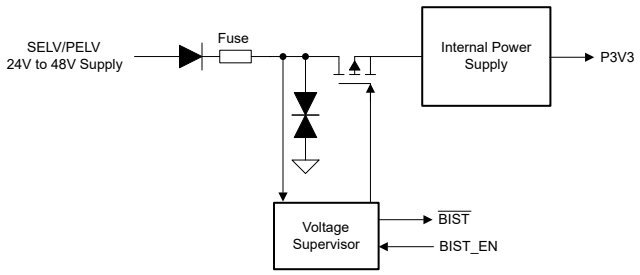

図 4. *BIST 機能付きの電圧スーパーバイザ IC を使用した電圧監視。*

電圧監視手段それ自体が診断範囲を確保する、すなわち、この場合は BIST 機能付きの電圧スーパーバイザ IC によって実施することにより、システムの診断範囲を 99% まで高められます。これは非常に高いレベルになっています。この高い診断範囲を、適切なハードウェア フォールト トレランスを備えた回路に実装すれば、システムは SIL 3 または PL e レベルの機能安全を達成できます。このような機能を統合したデバイスの例として、テキサス・インスツルメンツの TPS3762 があります。

電圧監視デバイスを使用するもう 1 つの利点は、高電圧を監視できることです。たとえば、TPS3762 は最大 65V を監視できるので、TPS3762 および入力電圧範囲の広い同様のデバイスを電源レールに直接接続し、監視やその他の診断を行うことができます。たとえば、一部の設計では、IEC 規格 60449-1 で定義されている電圧範囲である特別低電圧 (ELV) が必要となります。今では、ELV の定義を再利用して、IEC 62368 規格で SELV (安全特別低電圧) が定義されています。これは、ある電気エネルギー源レベルに対して、電源の出力が特定の電圧を超えることが許容されないというものです。たとえば、電気エネルギー源レベル ES1 では、電源の出力が 60V を超えることは許容されません。

これを念頭に置いて、安全特別低電圧電源については、安全最大電圧レベルは最大 $60V_{DC}$ に設定されています。安全な電源は、非常に短い期間だけこの値を超えることができますが、その期間を超過すると、安全特別低電圧の基準を満たしていないことになります。$60V_{DC}$ は、安全特別低電圧および保護特別低電圧など、安全規格で非常に一般的な最大電圧です。このため、TPS3762 などの入力電圧範囲の広いデバイスは、65V まで監視できる最大入力電圧を備えています。

セーフ トルクオフの設計例

モーター ドライブ段は、多くの産業用プロセスに不可欠であり、安全が最も重要な多くの環境で使用されています。多くのロボットは、人間と隣接して動作する際に、モーターを使用しています。モーター ドライブ アプリケーションでは、潜在的に危険な状態が発生した場合、システムをシャットダウンするために適切な処置を実行することが絶対に不可欠です。**表 1** に示すような状況では、モーターが突然に危険な動作をする可能性があります。

安全なモーター ドライブの重要な要素の 1 つは、セーフ トルクオフ回路の実装です。すべてのモーター ドライブには、ゲート ドライバで構成された電力段と、電力段回路の他に絶縁機能があります。電圧スーパーバイザ IC を使用してゲート ドライバおよび電力段の電源レールを監視することは、システムの機能安全のレベルを決定するために非常に有益です。**図 5** は、SIL 2 または PL d レベルのセーフ トルクオフ システム ブロック図の例です。

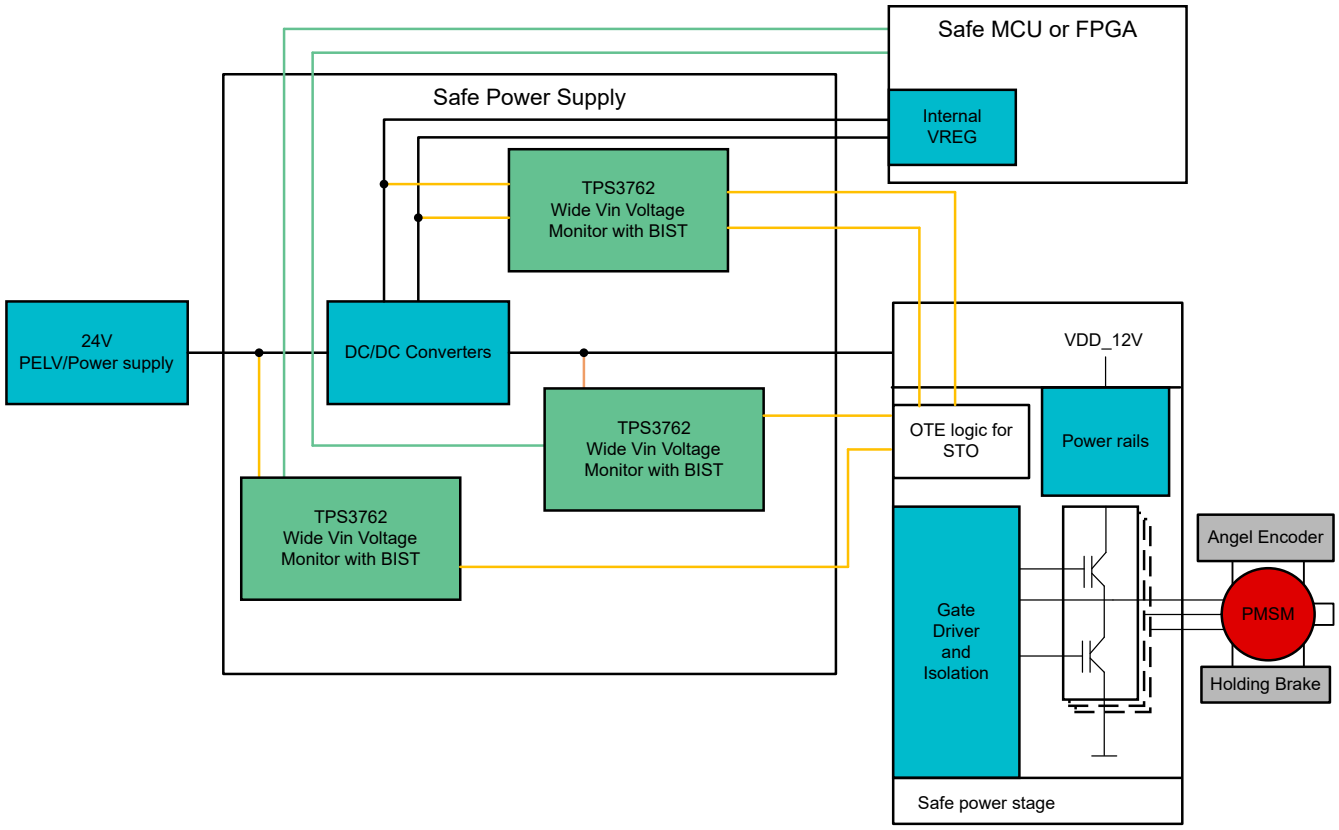

図 5. *SIL 2 または PL d レベルのセーフトルクオフ システム ブロック図。*

図 5 には、電圧監視のいくつかの対象事例があります。24V 電源と、電力段で使用される、MCU または FPGA (フィールド プログラマブル ゲート アレイ) のさまざまな絶縁型入力です。このようなの電圧監視方式のハードウェア フォールト トレランスは 0 です。しかし、TPS3762 のウィンドウ電圧監視機能とその BIST 機能によって高い診断範囲を実現しているので、SIL 2 または PL d レベルのシステムが得られます。

まとめ

技術が進歩するにつれて、私たちはその進歩が人間の生活にどのように影響するかについて、より戦略的に考える必要があります。機械、ロボット、エレクトロニクスの新しい進歩を効果的に活用するにあたっては、安全が不可欠です。電源設計における機能安全の向上は、最終的には、モーター ドライブ アプリケーションをより優れた強力なものにすることへとつながります。電圧スーパーバイザなどの高度なチップを採用すれば、システムが、安全に関する障害を検出し、安全を確保するための適切な手順を実施できるようにして、安全な設計を実現できます。

機能安全は、今後数年間でますます重要になります。電圧監視機能を利用することにより、あらゆるアプリケーションの機能安全について理解して改善できれば、より安全な世界の実現につながります。

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