

Application Note

トラクション インバータにおける機能安全の実現に向けて:設計手法と部品の概要



Yuxin Liu, Sifan You, Lars Lotzenburger

概要

自動車の電動化に伴い機能安全 (FuSa) の重要性がますます高まっていることを踏まえ、このドキュメントでは、ハイブリッド車 (HEV) および電気自動車 (EV) のトラクション インバータ システムにおける FuSa の実装について包括的に解説します。セクション 1 では、トラクション インバータにおける機能安全の重要性、適用される国際規格と地域規格、ISO 26262 V モデル開発プロセスに関する基礎的な知識を提示します。セクション 2 では、トラクション インバータ アプリケーションの体系的な FuSa 要件の導出プロセスを検討し、機能および技術的安全要件を導き出すための安全目標の定義、フォールト ツリー解析 (FTA)、故障モード影響解析 (FMEA) の実践的な例を紹介しします。セクション 3 では、トラクション インバータおよび技術的安全要件の実装に向けたテキサス インストルメンツの主要部品に焦点を当て、マイコン、ゲートドライバ、位置センサ、電流センサ、パワー マネージメント IC などの重要なサブシステムを対象としたチップ レベルの安全メカニズムやシステム レベルの安全設計戦略について解説します。このドキュメントは、FuSa 設計を開発するための重要なリソースを設計者に提供することを目的としています。

目次

1 概要.....	2
1.1 最終製品のトラクション インバータ.....	2
1.2 インバータで安全性が必要な理由.....	2
1.3 FuSa 開発フロー.....	2
2 トラクション インバータの FuSa 要件.....	5
2.1 トラクション インバータの構造と機能の概要.....	5
2.2 FuSa 要件派生プロセス.....	5
2.3 安全目標.....	6
2.4 FuSa コンセプト.....	6
2.5 技術的安全コンセプト.....	10
3 インバータの安全設計実装.....	17
3.1 TI FuSa 製品.....	17
3.2 TSR の実装方法.....	19
3.3 依存故障に関する検討事項.....	24
3.4 トラクション インバータの詳細な FuSa 設計構造.....	25
3.5 TI 安全デバイスでの FuSa 要件の達成.....	27
4 まとめ.....	42
5 参考資料.....	43

商標

すべての商標は、それぞれの所有者に帰属します。

1 概要

1.1 最終製品のトラクション インバータ

トラクション インバータは、ドライバと車両制御ユニット (VCU) からのコマンドに基づいてモータを制御してトラクショントルクを生成するハイブリッド電気自動車 (HEV) および電気自動車 (EV) に搭載される重要システムです。トラクション インバータは、回生ブレーキも管理し、高電圧バッテリーを充電します。図 1-1 に、トラクション インバータの構造を示します。

VCU からコマンドを受信し、測定された信号を処理すると、マイコン ユニット (MCU) は磁界方向制御 (FOC) アルゴリズムを実行し、パワー モジュール用の適切な PWM 信号を生成します。これにより、DC 入力を対称型の 3 相 AC 電流に変調して、モーターを駆動します。トルク コマンドは、アクセル ペダルまたはブレーキ ペダルからのドライバの入力と、自動運転または緊急ブレーキの状況での先進運転支援システム (ADAS) の 2 つのソースから発生します。

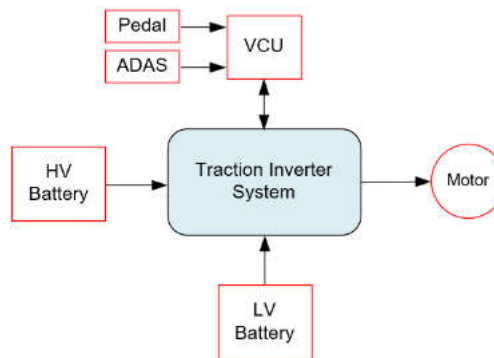


図 1-1. トラクション インバータの構造

1.2 インバータで安全性が必要な理由

電動化や自動運転技術の進展に伴い、HEV や EV の安全性に対する懸念がますます高まっています。重大な故障は危険な状態を招く恐れがあります。たとえば、回転子位置センサの不具合によって誤った信号が出力されると、FOC 変調に誤りが生じ、意図しないモータートルクが発生する可能性があります。同様に、通信インターフェースの障害が発生すると、トルク コマンドが適切に送信されなくなり、ドライバの要件と一致しないモーター動作が発生する可能性があります。このような異常動作は、車両の乗員に大きなリスクをもたらします。

機能安全 (FuSa) は、システム全体の安全性を構成する重要な要素であり、通常の入力条件および故障状態のいずれにおいても、システムが予測可能な動作を行うことを保証することに重点を置いています。FuSa の主な目的は、適切な安全メカニズムおよび設計手法を戦略的に実装することで、リスクを体系的に許容可能なレベルまで低減することです。

そのため、FuSa は世界中で国際規格や各地域の規制の枠組みに組み込まれるようになりました。道路車両の FuSa に関する国際規格である ISO26262:2018 は、車載 FuSa 分野において世界で最も権威ある指針となっています。この包括的な規格は、コンセプト設計から廃棄に至るまで、自動車の電気/電子システムを対象とした完全な FuSa 開発プロセスを規定しています。これには、安全管理、リスク評価、ASIL 分類、検証手法といった中核的な要素が含まれます。この規格は、グローバルな自動車市場で必須のコンプライアンス要件となっており、事実上すべての主流 OEM およびサプライヤは、これを厳格に遵守する必要があります。こうした基盤の上に、中国の GB/T 43254-2023、欧州の EU 2019/2144、米国の SAE J2980 など、トラクション インバータ FuSa を扱う地域ごとの規格がいくつか策定されています。これらの規格は、トラクション インバータの駆動とブレーキトルク機能に関する一般的な安全目標を提案し、安全機能に関する設計と検証の要件を公式に確立するものです。また、回生ブレーキ機能については、システム構成および安全要件が GB21670-2025 に規定されています。予想される通り、FuSa はインバータにとって徐々に必須要件となりつつあります。

1.3 FuSa 開発フロー

1.3.1 V モデル開発

従来型の FuSa 開発プロセスは V モデル と呼ばれ、多くの安全重視システムのコア フレームワークとして機能します。図 1-2 に、ISO26262:2018 の車載 FuSa V モデル を示します。この構造化されたアプローチでは、開発ライフサイクル全体が、左腕 (要件分析と設計) と右腕 (統合と検証) の 2 つの主要位相に分割されます。

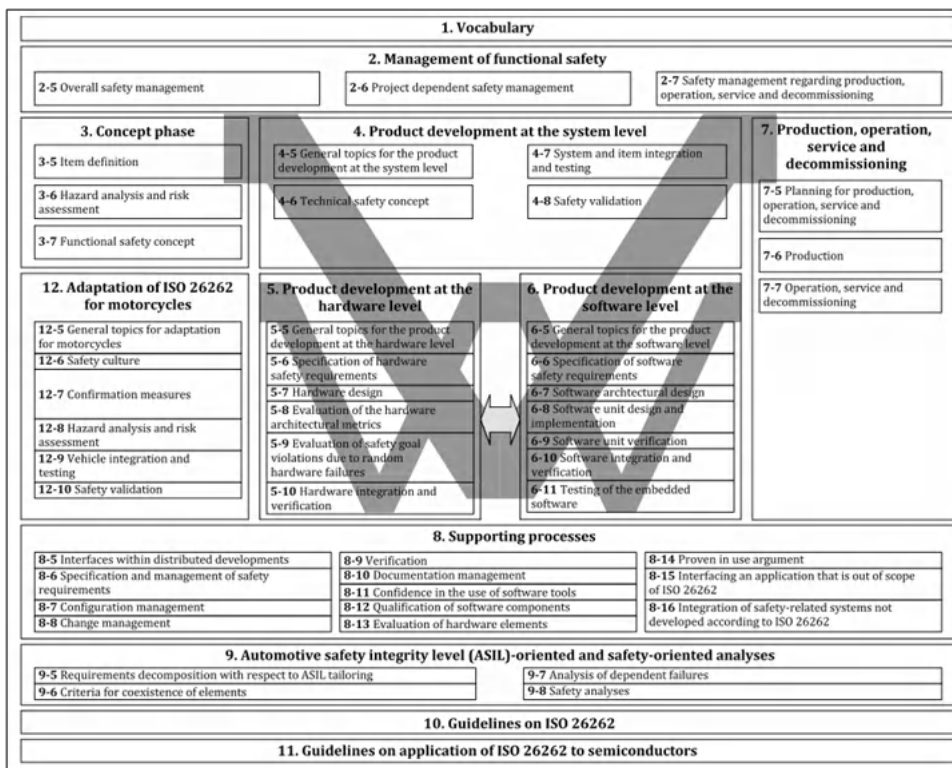


図 1-2. ISO26262:2018 の V モデル プロセス

V モデルの左腕は、FuSa 開発における分解と設計段階を示しており、以下の詳細なアクティビティが含まれています。

- **項目の定義:**プロジェクトの範囲と境界を設定します。
- **危険分析とリスク評価:**対象項目の潜在的な危険性を特定し、重大度、曝露、制御可能性の各要因に基づいて評価を行うことで、安全目標 (SG) の定義および車載安全性インテグリティレベル (ASIL) の割り当てを行います。
- **FuSa コンセプト:**システム機能全体に安全責任を割り当て、必要な安全機能を定義する FuSa 要件 (FSR) を策定する高度な安全戦略を策定します。
- **技術的安全コンセプト:**機能要件を、システムアーキテクチャにおいて安全設計をどのように実装するかを詳述した具体的な技術的安全要件 (TSR) に変換します。
- **ハードウェア/ソフトウェアの安全要件:**さらに、実際の実装をガイドするハードウェア安全要件 (HSR) およびソフトウェア安全要件 (SSR) に技術要件を絞り込みます。
- **設計の実装:**HSR と SSR に応じた特定の安全機能を実装します

V モデルの右腕は、FuSa 開発の統合と検証の段階を示しています。この段階には、次の詳細なアクティビティが含まれます。

- **ソフトウェアのテストと検証:** 最小のソフトウェア テスト可能ユニットを検証します。
- **ハードウェアのテストと検証:** 最小のハードウェア テスト可能ユニットを検証します。
- **統合テスト:** 部品間の相互作用を検証します。
- **システム テスト:** システム全体の機能を検証します。
- **車両統合テスト:** 実際の車両環境での性能を検証します。
- **安全性の確認:** 安全目標の達成を確認します。
- **FuSa 評価:** 最終的な安全確認を提供します。
- **製品リリース:** システムの量産開始を承認します。

V モデルは、各開発段階にそれに対応する検証活動が存在することを重視しています。これにより、安全要件が開発プロセス全体を通じて確実に伝達および検証されることが保証され、車載 FuSa 規格の厳しい要件を満たすことが可能となります。

1.3.2 インバータの安全ライフサイクル

機能安全のトラクション インバータシステムを実現するために、TI とシステム インテグレータは、FuSa 開発プロセスに加えて、ISO26262:2018 の安全ライフサイクルに従う必要があります。この包括的なアプローチは、コンセプトから廃止措置までの体系的なリスク削減を検証します。

このプロセスは、目的を定義するための安全計画と管理から始まります。危険分析とリスク評価を通じて、適切な車載安全性インテグリティレベル (ASIL) を特定して確立します。次に、これらの安全目標を詳細な安全要件仕様に絞り込み、その後のすべての開発作業をガイドします。

技術的安全コンセプトは設計および実装段階で実装され、統合とテストを通じて検証されます。安全要件は、特定のハードウェア安全設計およびソフトウェア安全設計に体系的に細分化され、ハードウェアおよびソフトウェア FuSa プロセスに従って個別に開発および検証されます。

最後に、生産および運用段階中の品質管理を定義します。同時に、メンテナンスおよび廃止措置メカニズムは、販売終了から寿命終了までの計画であり、トラクション インバータがライフサイクル全体にわたって FuSa を確実に維持できるようにします。

2 トラクション インバータの FuSa 要件

2.1 トラクション インバータの構造と機能の概要

トラクション システムの主な目的は、トラクション モーター (一般的には永久磁石同期モーター/PMSM) を、高い制御帯域幅で効率的に駆動することです。磁界方向制御 (FOC) アルゴリズムをマイコン (MCU) に実装して PWM 信号を生成し、その信号でゲートドライバを制御してパワー モジュールを精密に切り換えることで、高電圧 (HV) バッテリからの DC 入力電圧を 3 相対称 AC 電流に変換し、PMSM を駆動します。図 2-1 に、トラクション インバータのブロック図を示します。

FOC アルゴリズムの場合、システムでは位相電流、回転子の位置、DC リンク入力電圧をリアルタイムで測定する必要があります。そのためには、トラクション インバータ内に高精度で低レイテンシのセンサが必要です。さらに、システム内のすべての要素への電力供給には、信頼性の高いパワー マネージメント部品が不可欠です。

HV 側と低電圧 (LV) 側の間で絶縁が必要なため、信頼性の高い絶縁型電源回路を備えた絶縁型ゲートドライバが必要な要素となります。トラクション インバータは、CAN トランシーバを通して、トルク駆動コマンドを正確に受信し、潜在的な異常情報を車両制御ユニット (VCU) に報告します。ブレーキ動作中、トラクション インバータは回生モードで動作してバッテリーを充電すると同時に、ブレーキトルクを生成できます。

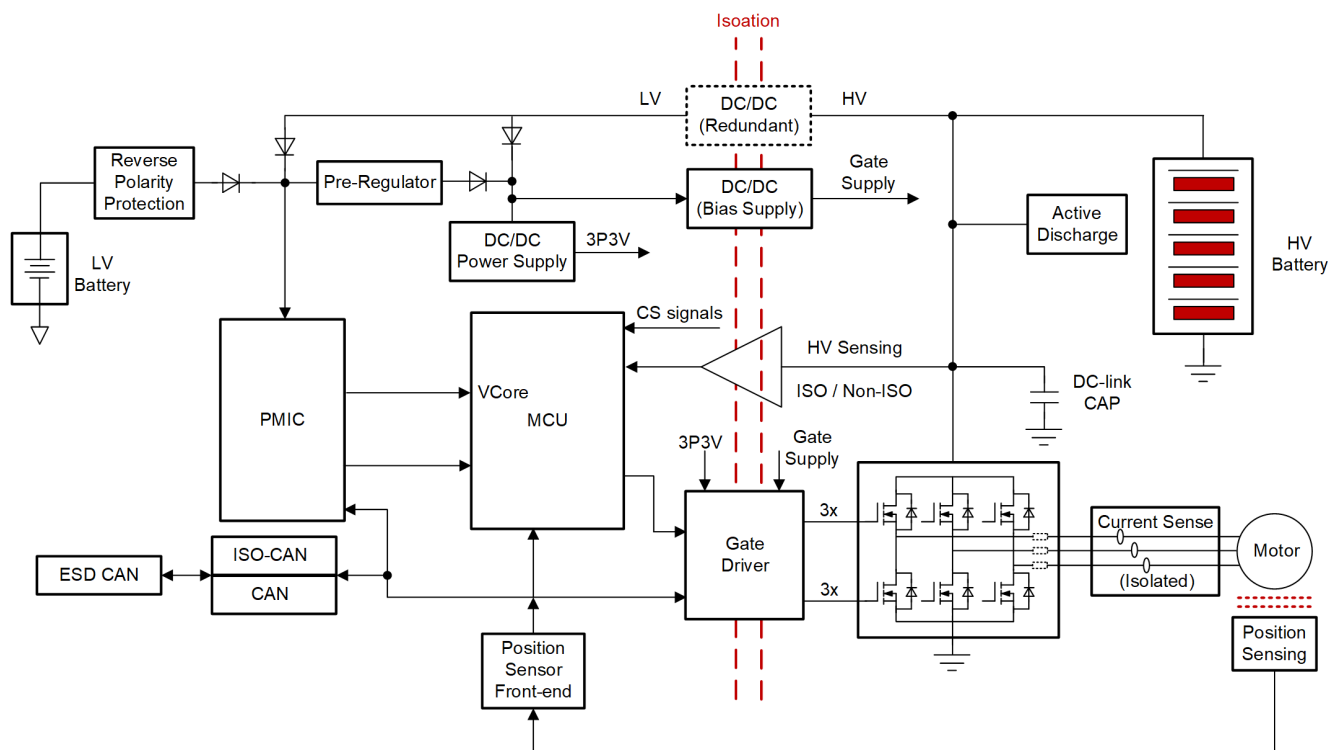


図 2-1. トラクション インバータのブロック図

2.2 FuSa 要件派生プロセス

以下のシステム安全設計は、TI の 1 つのトラクション インバータリファレンス デザインである [TIDM-02014](#) に基づいて適用され、セクション 1.3 に概説されているシーケンスに従って、すべての安全要件が導かれます。システム FuSa 要件の分析ステップの詳細については、「[オンボード チャージャの FuSa に向けて: 設計手法と部品の概要](#)」を参照してください。

以下の分析では、トラクション インバータの安全設計の安全目標として、セクション 1.2 に概説されている規格から、顧客側の一般的な安全要件と、標準ベースの安全要件を収集しています。インバータがドライブ機能とブレーキ機能の両方で提供するリソースを検討し、それに応じてシステムの安全目標を提案しています。

このドキュメントでは、安全目標 1 (SG1) を例として使用し、このトップレベルの安全目標を達成してフォールト ツリー解析 (FTA) を構築する方法を示します。その後、導出された FSR 1.6 は、故障モード影響解析 (FMEA) に対する新しい安全目標入力として機能します。位置検出システムの FMEA 解析を実施して、TSR 導出プロセスの例を示しています。

2.3 安全目標

トラクション インバータの安全目標は、システム全体の自動車レベルの安全要件です。望ましくない危険イベントと、重大な状況が発生した際の安全状態を考慮して定義します。この分析の安全目標は、表 2-1 に示すように導出されます。FTTI (フォールトトレラント時間間隔) の値は、特定のシステム動作ニーズに応じて、OEM または規制要件によって提供する必要があります。ASIL 定格は、安全プロセスに必要な厳格性のレベルを示し、ASIL D は最高の安全重視度を表します。

表 2-1. トラクション インバータの FuSa 目標の例

ID	安全目標	ASIL	安全状態	FTTI
SG1	意図しない予測以上の加速トルクの発生の回避。	ASIL C/D	1.障害のアラートを発信して報告します。 2.トルク出力をブロックします。	750ms (ユーザーが指定)
SG2	意図しない予測以上のブレーキトルクの発生の回避。	ASIL C		
SG3	駆動トルクを出力できなくなる事態の回避。	ASIL A	障害のアラートを発信して報告します。	

2.4 FuSa コンセプト

安全目標を確立した後、Fusa コンセプト (FSC) が開発されます。これには、サブ機能要素の安全要件が含まれます。ISO26262:2018 では、故障を特定して安全要件へと変換するための演繹的分析や誘導性分析などの安全性分析手法を推奨しています。この章では、一般的な演繹的分析手法である FTA を使用して、安全目標から FuSa 要件を導出します。このドキュメントでは、「SG1 - 意図しない予測以上の加速トルクの発生の回避」を例に挙げ、FSR を導出するための FTA 構築プロセスを説明します。

FTA は、論理的推論を使用して、考えられるすべての原因とシステム障害の組み合わせを特定するトップダウン式の演繹的分析手法です。この方式では、ブール論理を使用して、イベント間の原因と影響の関係を説明します。トップ イベントに直接つながる可能性のあるすべての原因は、FTA を通じて特定できます。ここで、FSR の派生プロセスを構成する基本的なイベントまたはゲートの安全要件が確立されます。

FTA 手法を使用することで、概要レベルの安全目標を、個別の故障モードに対処するより具体的な機能要件に体系的に分割できます。意図しない加速トルクを引き起こす可能性のあるイベントの論理的な組み合わせを分析することで、安全メカニズムが必要となる重要な領域を特定し、それらのリスクを低減するための適切な機能要件を確立できます。

2.4.1 FSC 設計アーキテクチャ

図 2-2 に、FSC レベルのトラクション インバータ システムのブロック図を示します。FTA は、この図に示すシステムアーキテクチャに従って実行されます。表 2-2 に、各要素の機能を示します。

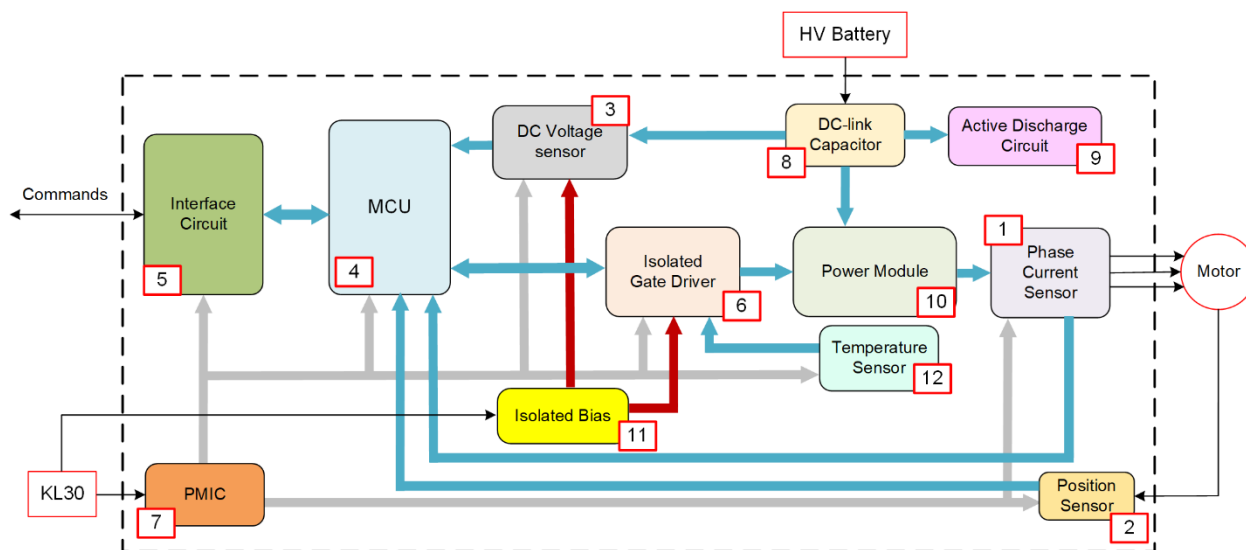


図 2-2. FSR レベルトラクション インバータ システムのブロック図

表 2-2. トラクション インバータの主な要素

要素 ID	要素名	説明
E1	モーター位相電流測定回路	出力段でインバータの位相電流を測定し、マイコンに送信して FOC と動作状態を監視します。
E2	回転子位置測定回路	FOC と動作状態の監視のために、モーターの回転子の位置を測定して、マイコンに送信します。
E3	DC 電圧センサ	FOC と動作状態の監視のために、出力段でインバータ電源を測定します。
E4	マイコン回路	FOC アルゴリズムを実行し、センサ データを監視し、PWM 信号を生成し、外部システムと通信します。
E5	インターフェイス回路	インバータと外部システム間の通信トランシーバ機能を提供します。
E6	ゲートドライバの回路	入力 PWM 信号に応じて、パワー モジュールに必要な電圧と駆動電流を提供します
E7	パワー マネージメント回路	LV 側のインバータ内にある主なデバイスに電源を供給します。また、マイコンの外部ウォッチドッグとエラー監視機能も提供します。
E8	DC リンク コンデンサ	HVDC 入力電圧を安定化および維持するための電力段用コンデンサ。
E9	アクティブ放電回路	電源オフまたは修理動作中に、DC リンク コンデンサにアクティブ放電を提供します。
E10	パワー モジュール	ゲートドライバ回路の制御下で、HV バッテリから必須の変調モーターの位相電流を生成します
E11	絶縁型バイアス電源	ゲートドライバ回路および電圧検出回路に HV (高電圧) 側絶縁型電源を供給します。
E12	温度測定回路	動作状態監視のために、電力段の温度を測定します。

2.4.2 フォールト ツリー解析

図 2-3 に、SG1 の FTA を示します。トップ イベントとは、駆動状態中にインバータに意図しない加速トルクを供給することと定義されます。次に、システム内の機能要素構造を体系的に分析し、さまざまな部品がトップ イベントの発生にどのように寄与し得るかを特定します。これらの障害イベントは、フォールト ツリー ダイアグラム内のさまざまな論理ゲートに関連付けられており、潜在的な故障モード間の AND または OR 関係を表します。

FTA の基本的なイベントまたはゲートについて、カットセット分析を実行しています。この分析の目的は、カットセットに含まれる要素または要素の組み合わせを特定し、トップ イベントが発生する可能性がある要素を特定し、各カットセット内の要素の数を決定することです。カットセット イベントの数が少ないほど、SG 違反に直接つながる可能性が高くなります。したがって、直接違反を防ぐため、1 次および 2 次のカットセットに FSR を推奨します。このアプローチは、ISO26262:2018 のシングル ポイント故障およびマルチ ポイント故障の対処に対応します。当社は、3 次以上のカットセットは安全な故障と考えています。このような故障の組み合わせは、低次のカットセットに対してすでに確立されているものよりも追加の安全要件を必要としない可能性が十分にあります。

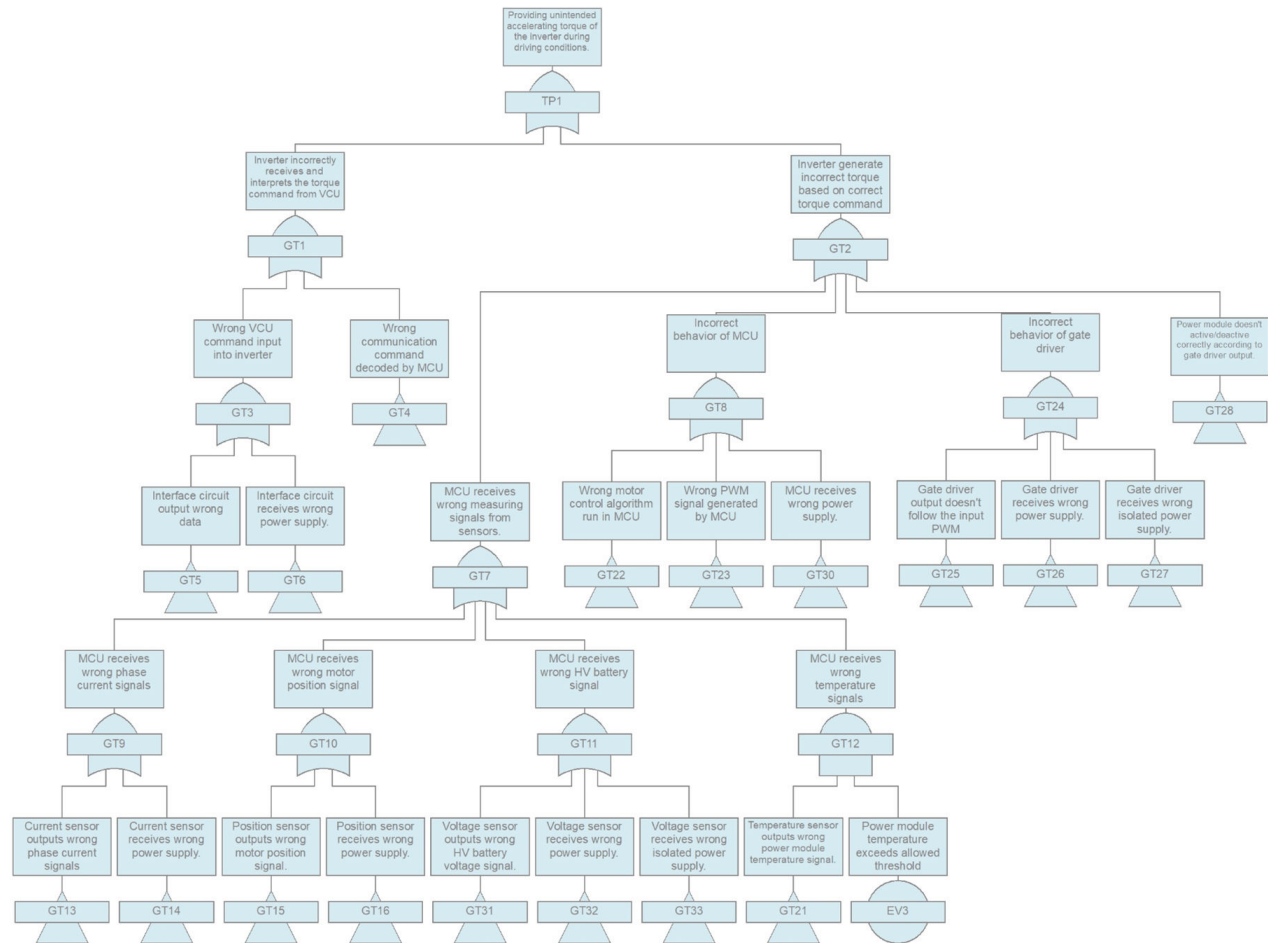


図 2-3. SG1 の FTA ツリー例

2.4.3 FuSa 要件

FTA の結果から、特定の故障はトップの安全目標に直接違反し、意図しないトルクや潜在的な損傷を引き起こす 1 次カットセットとして特定されました。たとえば、「GT15 – モーター位置センサが誤った位置信号を出力した場合」、マイコンは FOC 制御のためのセンサから誤った位置信号を受信し、イベント GT10 および GT7 をトリガします。これにより、FOC アルゴリズムは誤った PWM 信号を出力し、誤った AC 電流とトルクが生成されて、最終的にトップ イベント「TP1 - 意図しない予測以上の加速トルクを供給」します。

この分析に基づき、ユーザーは「インバーターは位置センサで回転子位置を正しく測定する必要があります」といった FSR を提案し、この要件をモータ位置センサの実装に割り当てることができます。表 2-3 に一覧されているように、この体系的な手法を用い、「意図しない予測以上の加速トルクの発生の回避」という安全目標に関連するすべての 1 次および 2 次のカットセットを FSR に導出します。

表 2-3. SG1 向け FSR の例

FSR ID	FuSa 要件	安全状態	アロケーション	ASIL	FTTI	トレース先
1.1	インバーターは、インターフェイス回路を使用して、VCU からマイコンへの通信データを正しく転送する必要があります。	マイコンへの通知を生成します。0 トルク制御を入力します。	HW、E5 SW、E4 HW&SW	D	FTTI	GT5
1.2	インバーターは、インターフェイス回路に電源を正しく供給する必要があります。	0 トルク制御を入力します。	HW、E7、E5 SW、E4 HW&SW	D	FTTI	GT6
1.3	インバーターは、マイコンによる VCU からの通信コマンドのデコードを正しく実行する必要があります。	トルク コマンドを廃棄し、0 トルク制御を入力します。	HW、E4、E5 SW、E4 HW&SW	D	FTTI	GT4

表 2-3. SG1 向け FSR の例 (続き)

FSR ID	FuSa 要件	安全状態	アロケーション	ASIL	FTTI	トレース先
1.4	インバータは、電流センサを使用してモーター一位相電流を正しく測定する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E1 SW、E4 HW&SW	D	FTTI	GT13
1.5	インバータは、電流センサに電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7 SW、E4 HW&SW	D	FTTI	GT14
1.6	インバータは、位置センサによって回転子の位置を正しく測定する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E2 SW、E4 HW&SW	D	FTTI	GT15
1.7	インバータは、位置センサに電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7 SW、E4 HW&SW	D	FTTI	GT16
1.8	インバータは、電圧センサによって HV バッテリ電圧を正しく測定する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E3 SW、E4 HW&SW	D	FTTI	GT18
1.9	インバータは、電圧センサに電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7 SW、E4 HW&SW	D	FTTI	GT19
1.10	インバータは、電圧センサに絶縁型電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7、E11 SW、E4 HW&SW	D	FTTI	GT20
1.11	インバータは、パワー モジュールの温度測定を正しく実行する必要があります。	マイコンへの通知を生成します。最大トルクを制限します。	HW、E12 SW、E4 HW&SW	D	MPFDTI	GT21
1.12	インバータは、マイコン内で動作するモーター制御ソフトウェア アルゴリズムを正しくサポートする必要があります。	マイコン出力をブロックします。 ASC またはフリーホイールを入力します。	HW、E4、E5 SW、E4 HW&SW	D	FTTI	GT22
1.13	インバータは、マイコンからの PWM 制御信号出力を正しく供給する必要があります。	マイコンの PWM 出力をブロックします。 ASC またはフリーホイールを入力します。	HW、E4、E5 SW、E4 HW&SW	D	FTTI	GT23
1.14	インバータは、マイコンに電源を正しく供給する必要があります。	マイコンをリセットします。 ASC またはフリーホイールを入力します。	HW、E7、E5 SW、E4 HW&SW	D	FTTI	GT30
1.15	インバータは、PWM 信号を正しく増幅し、ゲートドライバ内の駆動信号を生成する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E6 SW、E4 HW&SW	D	FTTI	GT25
1.16	インバータは、ゲートドライバに電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7、E6 SW、E4 HW&SW	D	FTTI	GT26
1.17	インバータは、ゲートドライバの HV 側に絶縁型電源を正しく供給する必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E7、E6 SW、E4 HW&SW	D	FTTI	GT27
1.18	インバータは、電力段による作動/解除制御を正しく行う必要があります。	マイコンへの通知を生成します。 ASC またはフリーホイールを入力します。	HW、E6、E10 SW、E4 HW&SW	D	FTTI	GT28

表 2-3 に示されているように、トップの安全目標に直接違反するいくつかの故障モードがあります。故障が発生した後、システムを強制的に安全状態にする必要があります。**PMSM** を搭載したトラクション インバータを検討してください。これは、高速時に大きな逆起電力 (**back-EMF**) を生成します。ここでは、4 つの安全状態を定義しています。

- 0 トルク モードへの低下

これは、トラクシオン インバータがモーターを完全に制御および検出機能を引き続き実現できる場合に安全状態です。アイコンは、0 トルク出力となるように $i_q = 0$ に設定し、検出信号に基づいて FOC アルゴリズムの実行を継続します。この安全状態は、誤った VCU コマンドの受信やハーネスの接続解除など、通信障害に適しています。インバータの他の部分は引き続き動作するため、障害が解決した時点で容易に通常機能を回復することができます。

• フリーホイール

これは、低速でのコマンドに続いて、トラクシオン インバータが正しい AC 電流とトルクを生成できない場合の安全状態です。この安全状態では、すべてのパワー スイッチがオフになり、3 相のすべてが接続解除されます。モーター速度が低いとき、PMSM は HV バッテリ電圧よりも低い逆起電力 (back-EMF) のみを生成します。

• アクティブ短絡 (ASC)

これは、高速でのコマンドに従って、トラクシオン インバータが正しい AC 電流とトルクを生成できない場合の安全状態です。高速では、PMSM が HV バッテリ電圧よりも大きな逆起電力 (back-EMF) を生成し、大きな回生電流、過剰なブレーキトルク、バッテリーの損傷が発生する可能性があります。したがって、3 つのハイサイド パワー スイッチすべてまたは 3 つのローサイド パワー スイッチすべてをオンにして、3 つの位相を短絡することで、インバータは高速で ASC に移行する必要があります。これにより、ブレーキトルクが小さい状態で位相電流が一定の値に制限されます。

• トルク出力の制限

これは、パワー モジュールの温度がアラート スレッショルドを超えた場合に実行される劣化フェイル オペレーショナル戦略です。この劣化モードで動作していても温度がシャットダウン スレッショルドを超え続けると、トラクシオン インバータは ASC またはフリーホイール モードに移行します。

2.5 技術的安全コンセプト

FSC が確立されたら、次の段階として、技術的安全コンセプト (TSC) を作成します。TSC は、FSC を具体的な TSR に落とし込みます。FuSa 分析を使用して、これらの技術的安全要件を FSR から導出します。

前の章では、トラクシオン インバータ システムで FTA を実行する方法を説明しました。この章では、代表的な誘導性分析手法である FMEA を使用して、安全性分析プロセスと TSR の導出方法を説明します。この章では、このデモの例として、「FSR1.6 - インバータは、位置センサによって回転子の位置を正しく測定する必要があります」を使用します。

FMEA は、製品の設計で発生する可能性のある故障モードの特定、その影響と原因の評価、特定の故障ごとに対処する適切な予防策と制御対策の開発を行う体系的な手法です。定義された危険からトップダウンで動作する FTA とは異なり、FMEA は個々の部品とその潜在的な故障モードを調べ、その結果をシステム レベルの影響までトレースすることでボトムアップを行います。

2.5.1 TSC 設計アーキテクチャ

図 2-4 に、TSC レベルのトラクシオン インバータ システムのブロック図と FSR1.6 の安全パスを示します。これは、FSC レベルのブロック図よりも 1 レベル深い部分です。重要部品については、この分析は以下を提供することを目的としています。

- 依存故障の影響を受けず、かつ安全性が損なわれる故障モードに対応する有効な安全メカニズムを提案する。
- 検出/応答時間の間隔に関する要件を満たすことができるシステム向けの安全状態への移行パスを作成する。
- 過剰設計なしで、適切な診断機能による安全メカニズムを実現する。
- TSR をハードウェア/ソフトウェア レベルの実装に転送する。

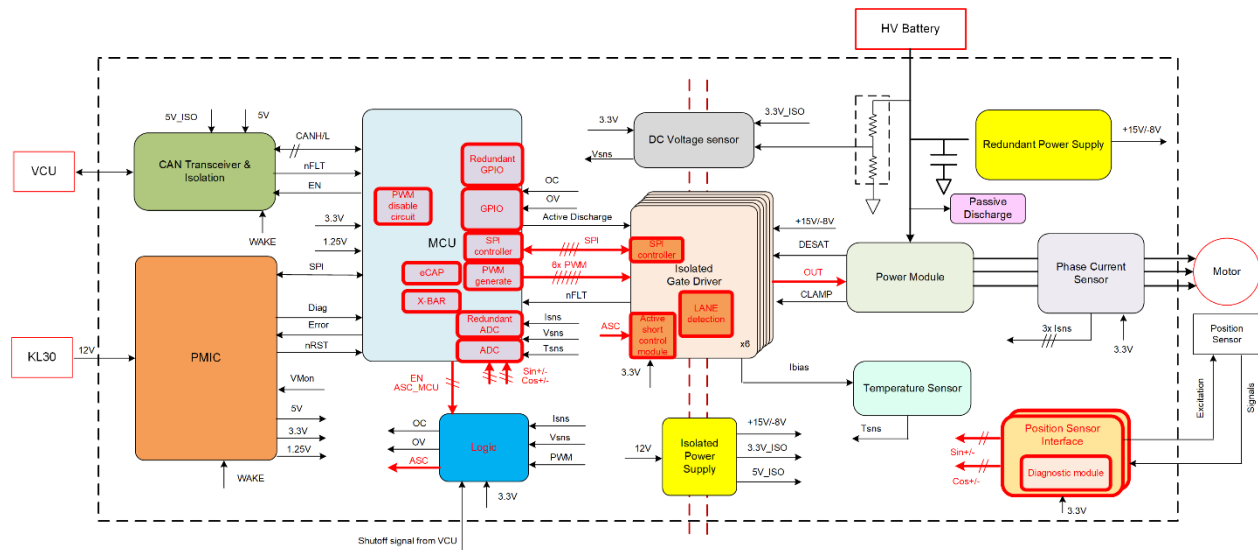


図 2-4. FSR1.6 安全パスを使用した TSR レベルのトラクション インバータシステムのブロック図

2.5.2 故障モード影響解析

FSR ごとに、故障モード、故障の影響、故障の原因を特定するため、FMEA を作成する必要があります。故障モードでは、各故障モードは安全目標違反タイプに従って分類する必要があります。これは、次の 3 つのカテゴリに分類できます。

- **シングル ポイント故障 (SPF):** FuSa 目標に直接違反する故障。
- **マルチポイント故障 (MPF) :** 別の独立した故障と組み合わせあった場合にのみ、FuSa 目標に違反する故障。
- **安全故障 (SF) :** FuSa 目標を侵害することのない故障。これらは、検出可能であるか、または本質的に安全なものです。

さらに、安全目標に影響を及ぼさない機能を持つ要素など、安全に関連しない要素も含まれる場合があります。

FSR (SPF と MPF の両方を含む) 違反となり得る各故障に対して、適切な安全機構を設計しなければなりません。こうした安全メカニズムは、以下の点で考慮されますが、これらに限定されるものではありません。

- **検出メカニズム (ISO26262 — Part5/Part11:2018 で参照):**

- 妥当性チェック: 値の範囲、変化率、信号相関性
- 冗長性の監視: 冗長チャネル間の比較
- 診断テスト: 内蔵セルフテスト、定期的な機能テスト
- ウォッチドッグ モニタ: プログラム フロー、タイミング監視

- **制御メカニズム (ISO26262 — Part5/Part11:2018 で参照):**

- 安全状態遷移: 安全な動作のための正常な劣化
- 故障時の応答: 検出された故障への即時応答
- 警告の生成: システム ステータスのユーザー通知
- システム シャットダウン: 制御されたシステムの作動停止

表 2-4 に、FSR1.6 の FMEA の一部を示します。(インバータは位置センサで回転子位置を正しく測定する必要があります)。

表 2-4. 一部の FMEA 例の表

システム要素	システム サブ要素	主な機能	故障モード	故障の影響ク	SG 違反タイプ	故障原因	安全メカニズム
回転子位置測定回路 (E2)	回転子位置測定センサ	モーター速度とトルク制御を目的として、FOC アルゴリズムの回転子の位置を測定します	モーター位置の測定ができません	モーター速度とトルクの制御ミスにつながるモーター位置の測定ができません	SPF	位置センサ出力短絡/開回路	1.トライステート出力および実行出力の範囲外チェック。 2.位置センサ出力の範囲外チェック。 3.冗長位置センサ測定回路。
					SPF	位置センサ励起回路の出力なし、または出力ドリフト。	1.励起回路出力妥当性チェック。 2.トライステート出力および実行出力の範囲外チェック。 3.冗長位置センサ測定回路。
					SPF	位置センサ入力短絡/開回路	1.入力信号妥当性チェック。 2.トライステート出力および実行出力の範囲外チェック。 3.冗長位置センサ測定回路。
			モーター位置と実際の位置が不一致です	モーターの位置が誤って測定され、モーターの回転速度とトルク制御の不具合が発生しています	SPF	位置センサ出力ドリフト	1.出力位相およびゲイン不均衡チェック。 2.トライステート出力および実行出力の範囲外チェック。 3.冗長位置センサ測定回路。
	回転子位置測定センサ冗長回路	FOC 用に、冗長回転子位置情報をマイコンに供給します	モーター位置の測定ができません	メイン回転子位置センサに異常がないにもかかわらず、マイコンへの入力値が不適切である/入力がない状態で、意図せず安全状態に移行します	MPF	位置センサ出力開回路/短絡または励起/AFE/アンプ回路からの出力がありません。	冗長位置センサ測定回路。
			モーター位置と実際の位置が不一致です	マイコンへの入力値が不正確で、メイン回転子位置センサの故障を検出できません	MPF	位置センサ出力ドリフト	1.トライステート出力および実行出力の範囲外チェック。 2.冗長位置センサ測定回路。

表 2-4. 一部の FMEA 例の表 (続き)

システム要素	システム サブ要素	主な機能	故障モード	故障の影響ク	SG 違反タイプ	故障原因	安全メカニズム
MCU (E4)	PWM ジェネレータ回路	FOC で PWM 信号を生成します。	意図しない PWM 信号を生成します	意図しない PWM が意図しないトルクを引き起こし、安全状態に移行しません。	SPF	意図しない PWM 信号を生成します。	それに応じて応答するように PWM を無効化またはプログラムするための PWMトリップ ゾーン回路。 PWM レベル検出用の eCAP。
	eCAP 回路	立ち上がりエッジまたは立ち下がりエッジをキャプチャします	エッジをキャプチャできません。	ePWM 診断用の ePWM エッジを正しくキャプチャできません	MPF	エッジをキャプチャできません。	BIST
	PWMトリップ ゾーン回路	故障発生時に、PWM を無効化またはプログラムします	所定のとおりに動作しません	PWM を無効化またはプログラムして安全状態にすることができません。	MPF	トリガ回路の故障。	BIST
			トリップ要件なしでの意図しない動作。	意図しないトリガが発生し、安全状態に移行します	SF	トリガ信号なしでの意図しないトリガ	NA
	ADC 回路	センシング用の A/D コンバータ	アナログ入力信号を正しく測定できません	正しい位置センサ出力信号を取得できません。	SPF	ADC コンバータの故障またはピンの断線	HW コンパレータ メカニズムでの冗長 ADC。
	冗長 ADC 回路	冗長 A/D コンバータ。	アナログ入力信号を正しく測定できません	正しい位置センサ出力信号を取得できません。	MPF	ADC コンバータの故障またはピンの断線	HW コンパレータ メカニズムでの冗長 ADC。
	GPIO 回路	ASC 関連信号を生成して、システムが安全状態に移行できるようにします	意図せずに GPIO 出力をトリガします。	意図せずに 安全状態に移行します。	SF	GPIO 出力が正しくありません	NA
				誤った安全状態に移行します。	SPF	GPIO 出力が正しくありません	GPIO 読み戻しおよび比較。 読み戻し比較が正しくない間、GPIO 出力をブロックし、外部ロジック回路に依存して安全状態に移行します。
	GPIO の読み戻しおよび比較	GPIO の状態を読み取って、安全状態の出力が正しいかどうかを検出します。	間違った信号の意図しないトリガ	GPIO 出力の不具合なしで意図せずに安全状態に移行します。	SF	GPIO 読み戻し回路が正しくありません	NA

表 2-4. 一部の FMEA 例の表 (続き)

システム要素	システム サブ要素	主な機能	故障モード	故障の影響ク	SG 違反タイプ	故障原因	安全メカニズム
ゲートドライバ回路 (E6)	アクティブ短絡部品	モーターが対応する安全状態に入るように、ASC を実行します。	関連する ASC コマンドで PWM 出力をブロックできません。	故障が発生している間、安全状態に移行できません。	MPF	ASC ロジック回路または伝送回路に障害が発生しています。	BIST 絶縁レーン診断
			関連する ASC コマンドで誤った安全状態が出力されます。	安全ではない間違った状態に移行します。	MPF	ASC ロジック回路または伝送回路が反転しています。	BIST 絶縁レーン診断
	絶縁レーン検出回路	絶縁レーンで誤った信号が検出されます。	絶縁レーン エラーを検出できません。	故障が発生している間、安全状態に移行できません。	MPF	絶縁レーン検出回路に障害が発生しています。	BIST
			意図せずに絶縁レーンの障害が報告されます。	意図せずに安全状態に移行します。	SF	絶縁レーン検出回路に障害が発生しています。	NA

2.5.3 技術的安全要件

FMEA の結果から、提案された安全メカニズムは TSR の形で直接提案されます。システム レベルで実用的な安全メカニズムを提案できない一部の SPF/MPF 故障では、安全要件は半導体部品内に実装できるようにハードウェア/ソフトウェア レベルに渡されます。表 2-4 に基づき、FSR1.6 に関連する TSR を表 2-5 で確認できます。

表 2-5. FSR1.6 への TSR

TSR ID	技術的安全要件	アロケーション	ASIL	安全状態	FTTI (ユーザーが指定)
1.6.1	回転子位置検出回路は、回転子の位置を正しく測定する必要があります。	位置センサ ADC	ASIL B(D)	位置センサのトライステート出力。マイコンは、位置センサ信号をブロックし、冗長位置センサ信号をルーティングします。	FTTI_PS
1.6.2	回転子位置検出回路は、入力と出力振幅および位相妥当性チェックを正しく実施する必要があります。	位置センサ ADC	ASIL B(D)	位置センサのトライステート出力。マイコンは、位置センサ信号をブロックし、冗長位置センサ信号をルーティングします。	FTTI_PS
1.6.3	回転子位置検出回路は、励起振幅および周波数妥当性チェックを正しく実行する必要があります。	位置センサ ADC	ASIL B(D)	位置センサのトライステート出力。マイコンは、位置センサ信号をブロックし、冗長位置センサ信号をルーティングします。	FTTI_PS
1.6.4	回転子位置検出回路は、センサ妥当性チェックに失敗した場合、トライステートへの出力をブロックする必要があります。	位置センサ ADC	ASIL B(D)	マイコンは、位置センサ信号をブロックし、冗長位置センサ信号をルーティングします。	FTTI_PS
1.6.5	冗長回転子位置検出回路は、妥当性チェックを実行し、故障した場合はトライステートに移行する必要があります。	位置センサ ADC	ASIL B(D)	マイコンは、冗長位置センサ信号を放棄します。	FTTI_PS
1.6.6	マイコンは、2 つの位置センサ出力が有効であるものの不一致である場合、インバータを強制的に安全状態に移行させる必要があります。	ADC SW マイコン CPU 位置センサ	ASIL D	マイコンは、ASC またはフリーホイールに移行します。	FTTI_MCU

表 2-5. FSR1.6 への TSR (続き)

TSR ID	技術的安全要件	アロケーション	ASIL	安全状態	FTTI (ユーザーが指定)
1.6.7	マイコンは、センサのトライステート出力で、センサの出力範囲妥当性チェックを正しく実行する必要があります。	ADC SW マイコン CPU 位置センサ	ASIL D	マイコンは、センサ信号を放棄し、冗長センサ信号を読み取ります	FTTI_MCU
1.6.8	マイコンは、PWM 出力が意図したロジックと一致しているかどうかを確認する必要があります。	PWM eCAP	ASIL D	マイコンは、出力をブロックし、ASC またはフリーホイールに移行します	FTTI_MCU
1.6.9	マイコンは、ADC コンパレータ出力を確認する必要があります。	ADC 冗長性 ADC ADC HW チェック	ASIL D	マイコンは、出力をブロックし、ASC またはフリーホイールに移行します	FTTI_MCU
1.6.10	ゲートドライバは、ASC 信号入力で、PWM 出力をブロックする必要があります。	PWM ディスエーブル回路 PWM レーン チェック ASC 回路 出力段 マイコン CPU	ASIL D	ゲートドライバは、出力段を遮断し、他の 5 つのゲートドライバを使用して安全状態に移行します	FTTI_GD
1.6.11	ゲートドライバは、正しい安全状態電圧レベルを出力する必要があります。	ASC 回路 絶縁レーン チェック 出力段	ASIL D	ゲートドライバは、出力段を遮断し、他の 5 つのゲートドライバを使用して安全状態に移行します	FTTI_GD
1.6.12	ゲートドライバは、絶縁レーンで転送される信号が正しいかどうかを確認する必要があります。	絶縁レーン チェック	ASIL D	ゲートドライバは、PWM 出力をブロックし、ASC またはフリーホイールに移行します。	FTTI_GD

これらの技術的安全要件は、回転子位置検出機能が適切かつ安全に動作することを保証するための具体的な措置を規定するものです。これらのデバイスは、測定精度、妥当性チェック、冗長性管理、障害検出、安全状態遷移など、さまざまな側面に対処しています。各要件は特定の部品に割り当てられ、適切な ASIL 定格を割り当てられ、定義されている安全状態およびフォールトトレラント時間間隔にリンクされます。

3 インバータの安全設計実装

3.1 TI FuSa 製品

テキサス インストルメンツは、さまざまなディスクリート デバイス オプションを提供しており、顧客固有のアプリケーション要件に合わせてカスタマイズした安全システムを構築できます。TI は、ISO26262:2018 の要件に完全に準拠した包括的かつ柔軟な FuSa ソリューションも提供しており、車載エレクトロニクスや安全性が極めて重要視されるアプリケーションにおいて、顧客が FuSa 目標を達成できるよう支援します。さらに、TI はインテグレータの設計プロセスを支援し、安全認証手順を簡素化できるように、包括的な製品 FuSa に関する資料と技術サポートを提供しています。

TI の製品は、「FuSa 対応」、「FuSa 品質管理」、「FuSa 準拠」に分類されており、さまざまな ASIL 要件を満たしています。図 3-1 に、詳細な開発プロセスと成果物を示します。

		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
		Low-complexity products that can be evaluated for use in a functionally safe system	Previously-released, complex products that have had additional documentation developed to enable their use in functional safety applications.	Products specifically developed to be compliant to functional safety standards that can be used in functional safety applications
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA*	✓	Included in FMEDA	Included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)*			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate**			✓

* May only be available for analog power and signal chain products. ** Available for select products.

図 3-1. FuSa 設計における TI 製品の分類

• FuSa 対応製品

これらの製品は FuSa には準拠していませんが、TI の品質管理プロセスに従って開発されたものです。TI は、顧客が安全アプリケーションでこれらの製品を使用する際にハードウェア要素の評価を完了できるように、「故障モード分布 (FMD)」や「ピン FMA」などの支援資料を提供しています。また、TI はシステムの FMEDA (故障モード、影響、診断分析) 向けに、FuSa 対応デバイスの故障率に関する情報も提供しています。これらの製品は、中程度から低レベルの安全性インテグリティレベルのアプリケーションや、車載環境の高安全システムの補助部品として適しています。

• FuSa 品質管理製品

これらの製品も FuSa には準拠していませんが、TI の品質管理プロセスに従って開発されたものです。TI は、故障モードの種類、分布、故障率に関する詳細情報を提供しています。この情報はデバイスの FMEDA に付属しており、顧客が安全アプリケーションでこれらの製品を使用する際に、ハードウェア要素のハードウェア評価を包括的に行うのに役立ちます。これらの製品には安全マニュアルが付属しています。システム インテグレータは、個々のニーズに応じて組み込み安全メカニズムを有効化または無効化することができます。これらは、中程度から低レベルの安全性インテグリティレベルのアプリケーションや、車載環境の高安全システムの補助部品として適しています。

• FuSa 準拠製品

これらの製品は、FuSa に適合した唯一のタイプです。これらは、TI の品質管理プロセスおよび TI FuSa プロセスの双方に従って開発されています。TI は、ハードウェアとソフトウェアの両方で FuSa 認証の FuSa 開発プロセスを提供しています。TI は、この種の製品に対応する包括的な FMEDA と安全マニュアルを提供しています。システム インテグレータは、ニーズに応じて組み込み安全メカニズムを有効化/無効化できます。これらの製品は安全関連アプリケーションでの直接使用に適しており、車載環境での安全目標を満たすことができます。また、TI は FuSa 認証レポートまたは評価レポートも提供しており、システムレベルの FuSa 認証を取得したインテグレータを支援します。

TI FuSa デバイスの情報については、www.ti.com/technologies/functional-safety/overview.html で関連情報を簡単に見つけることができます。図 3-2 に示されているように、FuSa カテゴリを選択すると、すべての安全関連デバイスが選択されます。図 3-3 に示されているデバイス詳細ページから、ユーザーは簡単なプロセスで重要な FuSa 資料にアクセスできます。技術文書セクションをクリックすると、FuSa レポートを直接ダウンロードでき、デバイスに関する重要な安全関連情報が表示されます。FMEDA などのより詳細な分析文書については、NDA (秘密保持契約) の要件により、これらを別途請求する必要があります。

Hide filters Columns Reset table 44 of 1,148 total products

Search filters...	Product number	Images	Description	Category	Subcategory	TI functional safety category	Rating
Description Category Subcategory TI functional safety category Search... OR AND ☒ Select All ☒ Functional Safety Quality-Managed ☒ Functional Safety-Capable ☒ Functional Safety-Compliant Reset filter Rating Operating temperature range (°C) Package type Pin count Package area (mm²)	LP87725-Q1 - NEW Data sheet: PDF HTML TPS65224-Q1 - NEW Data sheet: PDF HTML TPS65386-Q1 - NEW Data sheet: PDF HTML BQ79718-Q1 - NEW Data sheet: PDF HTML View alternates ADS131B24-Q1 - NEW Data sheet: PDF HTML ADS131B23-Q1 - NEW Data sheet: PDF HTML ADS131B26-Q1 - NEW Data sheet: PDF HTML BQ79731-Q1 Data sheet: PDF HTML View alternates	       	Automotive, three 3-A low-noise buck converters, IO LDO and load switch PMIC for radar MMICs 5.5-V PMIC with 4 buck converters and 3 LDOs for ADAS processors up to ASIL-B Automotive 2.3-V to 36-V, 2.8-A power management IC (PMIC) for safety-relevant applications Automotive 18-s precise battery monitor, balancer and integrated protector compliant to ASIL-D Automotive high-voltage battery-pack monitor with four ADC channels for current and voltage sensing Automotive high-voltage battery-pack monitor with three ADC channels for current and voltage sensing Automotive high-voltage battery-pack monitor with six ADC channels for current and voltage sensing Automotive battery junction box voltage monitor, current sensor and isolation interface sensor	Power management Power management Power management Power management Power management, Data converters Power management, Data converters Power management, Data converters Power management	Multi-channel ICs (PMICs) Multi-channel ICs (PMICs) Multi-channel ICs (PMICs) Battery monitors & balancers Battery monitors & balancers, Precision ADCs Battery monitors & balancers, Precision ADCs Battery monitors & balancers, Precision ADCs Battery monitors & balancers	Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant Functional Safety-Compliant	Automotive Automotive Automotive Automotive Automotive Automotive Automotive Automotive

図 3-2. TI.com の TI デバイス FuSa カテゴリ

Technical documentation

★ = Top documentation for this product selected by TI

Type	Title	Date
Data sheet	TPS3704-Q1 Automotive Quad, Triple, Dual, Single Window or Standard Voltage Supervisor datasheet (Rev. B)	14 Aug 2023
Functional safety information	TPS3704 Functional Safety Analysis Report Summary (FMEDA) (Rev. A)	26 May 2022
Functional safety information	TPS3704 Functional Safety Report Summary (Rev. A)	26 May 2022
Functional safety information	TPS3704x-Q1 Functional Safety Manual (Rev. A)	26 May 2022

Request more information

The full failure modes, effects, and diagnostic analysis (FMEDA) is available. [Request now](#)

Require FMEDA under NDA

図 3-3. TI.com 経由の FuSa 関連文書の要求

3.2 TSR の実装方法

セクション 2.5.3 の TSR を例として、このセクションでは、TI の安全位置センサ AFE LDC5072/3-Q1、安全マイコン F29H859-Q1、スマートゲートドライバ UCC5881-Q1、TI プログラマブル ロジック デバイス TPLD1201-Q1 に基づく位置センサ出力障害機能を備えた TSR 実装をご紹介します。図 3-4 に、関連デバイスによる詳細な安全パスを示します。

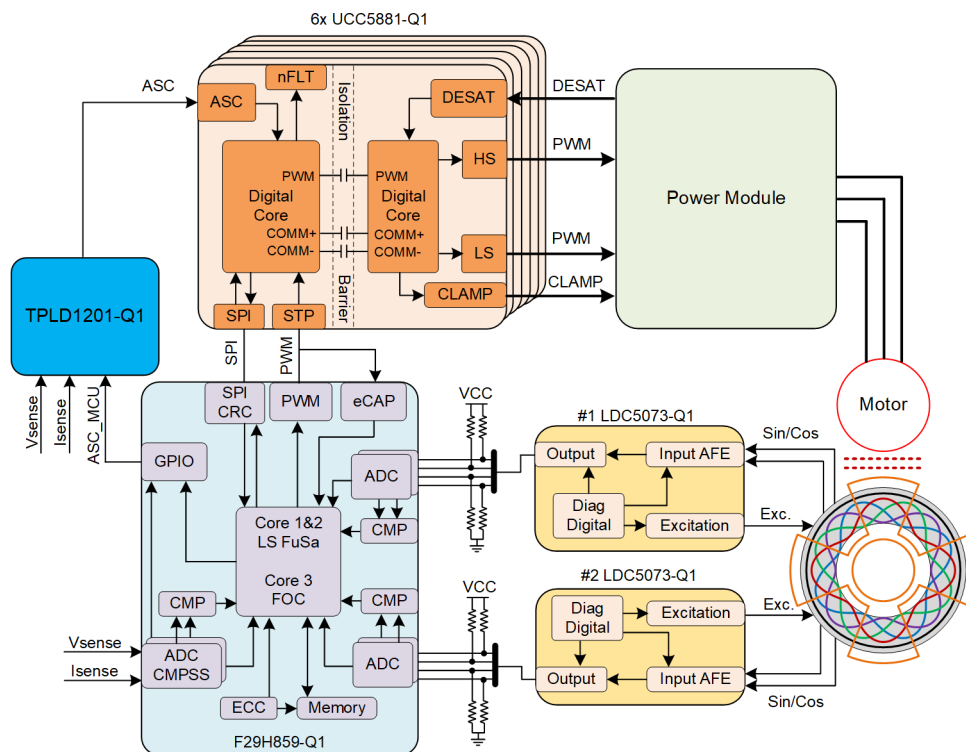


図 3-4. 位置センサ出力障害時の TSR に関する安全パス

3.2.1 位置センサ

LDC5073-Q1 は、モーター位置検出用の誘導性レゾルバ アナログ フロント エンドであり、ISO26262:2018 に準拠して開発され、最大 ASIL C のハードウェア要件を満たす能力を備えています。PCB 技術を使用して構築され、LDC5073-Q1 と同じボードを共有している誘導性センサは、固定子コイルと導電性ターゲットで構成されています。ターゲットはモーターの回転子に取り付けられ、PCB 上のトレースである固定子コイルの上に配置されます。LDC5073-Q1 は励起コイルを駆動し、ターゲット内に渦電流を生成して、固定子センスコイルに電圧を誘導します。ハーネスに取り付けられたマイコンは、これら 2 つの信号を使用して角度を推定します。LDC5073-Q1 は励起信号を生成し、COS 信号と SIN 信号のフィルタリング、復調、増幅を行います。図 3-5 に、LDC5073-Q1 を使用した誘導性センサのブロック図を示します。

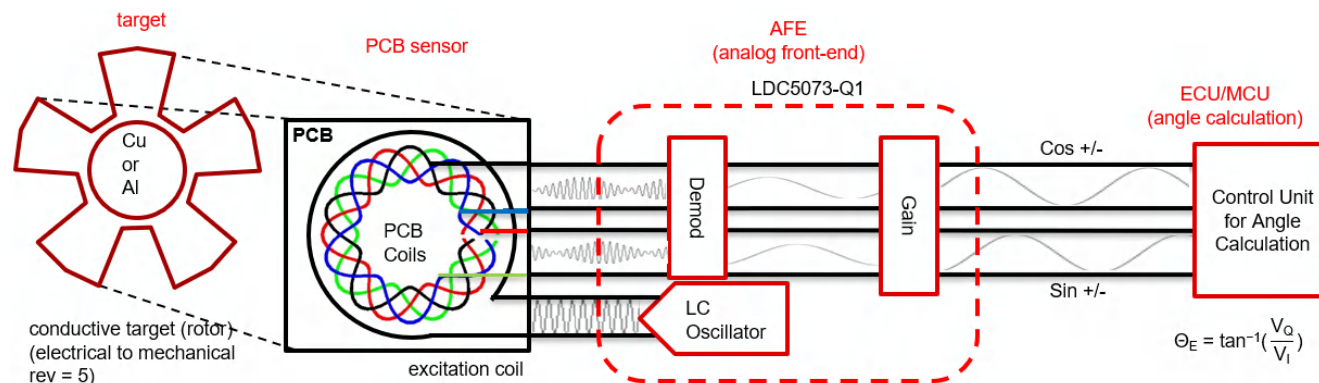


図 3-5. LDC5073-Q1 を使用した誘導性位置センサのブロック図

LDC5073-Q1 はオンボード診断 II (OBD2) を完全にサポートしており、コントローラがセンサとハーネスの障害を区別できるようになります。デバイスは、センサ ボード上の追加プルアップやプルダウンを必要とせず、出力の故障状態電圧を強制的に供給することで、故障状態をコントローラに伝達します。EOL (エンド オブ ライン) プログラミングを使用することで、故障状態電圧は、コントローラ ボードのプルアップおよびプルダウン構成に応じて設定されます。センサの故障やハーネスの故障が発生した場合、マイコン ADC はピン電圧が範囲外であることを読み取って、その故障を直接検出します。

OBD2 は、マイコンと連携して、フェイル オペレーショナル モードとフェイルセーフ モードの両方に構成できます。励起信号故障、センサ入力信号故障、LDC5073-Q1 内部ゲイン/オフセット故障、または LDC5073-Q1 出力段故障が発生した場合、LDC5073-Q1 は診断モードに移行し、マイコンは ADC の OBD2 電圧に基づいて故障モードを読み取ります。同時に、フェイル オペレーショナル モードにより、安全上の障害発生時も角度情報の報告を継続して車両の運行を維持しつつ、ユーザーに整備の必要性を通知することが可能になります。

LDC5073-Q1 は、電源投入前または通常動作中に発生する故障を検出、監視、および報告するための多数の診断機能も備えています。診断機能には、UV/OV 監視、BIST、EEPROM ECC チェック、励磁/検出入出力の整合性チェック、サーマル シャットダウンなどが含まれます。LDC5073-Q1 の構成可能な出力モードは、5.0V 電源で 3.3V の SIN/COS 出力、電源電圧 (5.0V または 3.3V) に合わせた従来型の SIN/COS をサポートしています。これにより、センサ ボードを 5V で動作させつつ、マイコン/ADC を 3.3V 対応のものへ移行させることができます。LDC5073-Q1 は、100ns 未満の遅延の不確実性と 0.05 度 (3 シグマ) の繰り返し精度を誇る市場でより予測性の高い高速角度センサです。

センサの出力角度が誤っているものの有効な値であるようなシナリオに対応し、かつ ASIL D レベルの体系的な設計要件を満たすために、冗長センシング コイルを備えた LDC507x-Q1 デバイスを 2 つ実装することが可能です。その際、PCB サイズを大幅に増大させる必要はありません。図 3-6 を参照してください。2 つのセンサ出力が一致しない場合、マイコンは両方のセンサ出力を放棄し、システムを強制的に安全状態に移行します。また、1 つのセンサ出力が範囲外になると、システムはフェイル オペレーショナル モードで動作することができます。この方式により、2 つの ASIL B 設計が分解によって ASIL D を達成できるため、各 LDC5073-Q1 について選択できる安全メカニズムの数が少なく済みます。

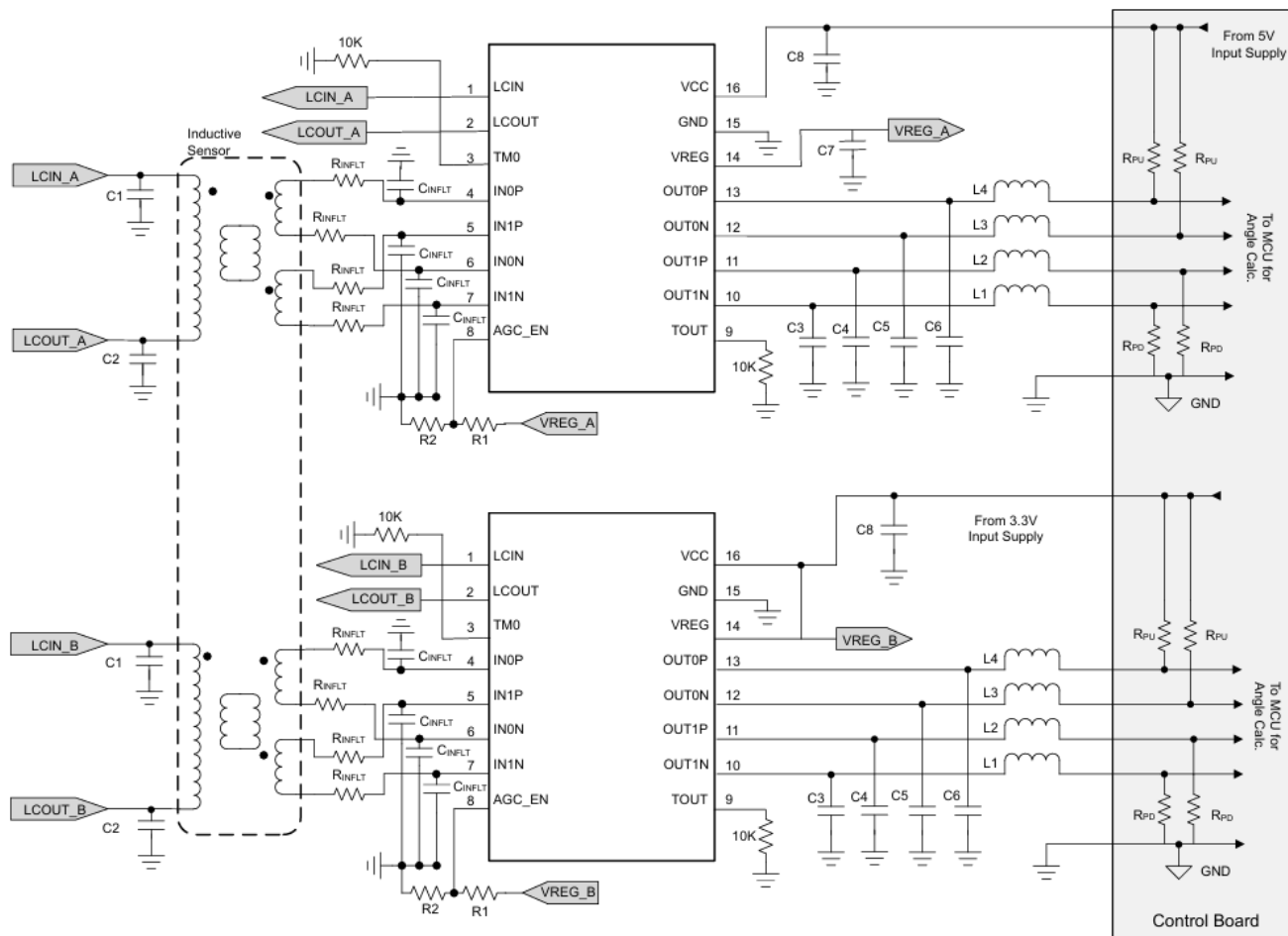


図 3-6. 2x LDC507x-Q1 パスを冗長構成として使用し、体系的な ASIL D を達成

3.2.2 マイコン

F29H859TU-Q1 マイコンは、高性能 C2000™ リアルタイム マイコン ファミリーに属します。C2000 製品ラインは、車載用および産業用アプリケーションの複数の製品に実装される、一般的な安全アーキテクチャを活用しています。200MHz で動作する 3 つの C29x CPU (ロックステップ動作対応)、4000kB のフラッシュメモリ、452kB の RAM を搭載し、5 つの SAR ADC および最大 36 チャネルの PWM 出力、QFP-144/QFP-176/BGA 256 パッケージをサポートしています。ISO26262 と IEC61508 規格を満たしており、サイバーセキュリティのため HSM もサポートする ASIL D/SIL3 までの安全要件に確実に準拠します。高度な機能と豊富な接続オプションを備え、包括的なソリューションを提供します。

トラクション インバータ アプリケーションでは、1 組のロックステップ (LS) コアを FuSa 動作専用にし、もう 1 つのコアをメイン FOC モーター制御アルゴリズムに使用できます。LS コアは同じ FuSa コードを実行し、プログラム実行またはメモリ整合性の障害を検出します。マイコンは ADC からの範囲外信号を検出すると、位置センサに故障をマークし、冗長位置センサ出力の読み取りに自動的に切り替えます。マイコンが 2 つの位置センサからの出力の不一致を検出すると、GPIO 経由で ASC コマンドを外部ロジック回路に送信し、その後、スマート絶縁型ゲートドライバ内の ASC 機能がトリガされます。また、マイコンは対応する状態情報を SPI 経由で送信し、ゲートドライバを ASC モードに正しく構成します。

ADC のハードウェア冗長性は、同一入力を複数のペリフェラル インスタンスでサンプリングし、その出力値を相互にクロスチェックすることによって実現されます。異なる ADC インスタンスにわたって ADC 変換データを同時にクロスチェックすることで、ハードウェア ADC チェック回路は ADC 変換障害を検出し、対処できます。PWM 出力は、クロスバー (XBAR) 付きの (拡張キャプチャ) eCAP で読み戻すことで、PWM 出力が正しいかどうか、または ASC コマンド後に PWM トリップゾーン (TZ) によって正常に無効化されたかどうかを検出できます。ASC (GPIO 出力) にも同様の安全メカニズムを実装し、安全状態コマンドの正しい出力を検証できます。

これらの包括的な安全機能により、マイコンはセンサの障害を確実に検出し、安全重視の信号を処理して、必要に応じて適切な安全状態を開始できるようになり、トラクション インバータ システムで FuSa の整合性を維持できます。

3.2.3 ロジック回路

TPLD1201-Q1 は、TI のプログラマブル ロジック デバイスであり、参照テーブル (LUT)、D フリップ フロップ、カウンタ、エッジ検出器、発振器などの大量のロジックリソースを統合しています。また、アナログ コンパレータや電圧リファレンスを含め、複数のアナログ マクロセルも搭載しています。図 3-7 に、TPLD1201-Q1 で利用可能な詳細なリソースを示します。

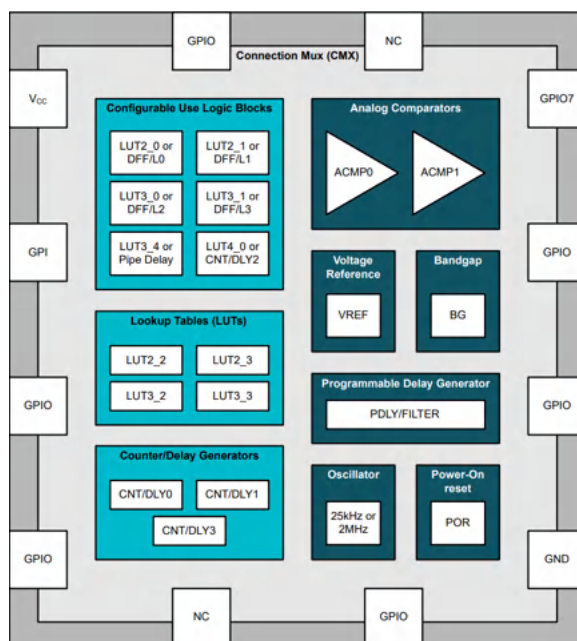


図 3-7. TPLD1201-Q1 のリソース

このデバイスは、TI の ICS GUI を使用して簡単に構成でき、固定機能デバイスとして永続的に構成できます。専用のデジタル回路設計により、TPLD1201-Q1 は冗長安全状態入力回路として機能し、マイコンに障害が発生したときにシステムが正しい安全状態に移行するのに役立ちます。図 3-8 に、この実装のブロック図を示します。

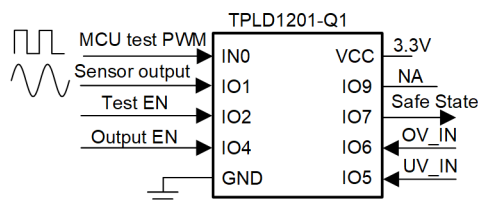


図 3-8. モーター速度検出用の TPLD1201-Q1 接続の設計

この TPLD1201-Q1 ロジック回路設計により、マイコンが故障すると、PMIC は TPLD1201-Q1 への Output_EN 信号をトリガし、安全状態出力ピンはセンサ出力信号周波数、OV_IN および UV_IN に応じて応答します。過電圧イベント中、TPLD1201-Q1 は ASC コマンドを出力しますが、低電圧イベント中はフリーホイール コマンドを出力します。電圧が通常の範囲内の場合、TPLD1201-Q1 はセンサの出力周波数に基づいて、ASC コマンドまたはフリーホイール コマンドのいずれかを出力します。スレッシュホルド周波数は、構成段階中にデバイス内でカウンタ データを変更することで柔軟に調整できます。

また、この設計は、マイコンが TEST_EN 信号を送信し PWM をテストすることで、パワーオン内蔵セルフテスト (BIST) もサポートしており、潜在的な故障指標をさらに減らすことができます。マイコンで障害が検出されないと、TPLD1201-Q1 出力はマスクされ、マイコンは対応する安全状態を送信します。TPLD1201-Q1 内のすべての機能と安全メカニズムの設計は、個々の要件に応じて ICS GUI でユーザーが柔軟に変更できます。

現在、TPLD1201-Q1 の機能安全 FIT 率、FMD、ピン FMA に関するドキュメントも提供されています。FuSa 計算要件では、このドキュメントを任意のデータの参照として使用できます。

TPLD1201-Q1 は、安全アーキテクチャにおける重要な部品として機能し、マイコン障害が発生した場合もシステムの安全性を維持できる独立監視/制御パスを提供します。この冗長性は、トラクション インバータ アプリケーションで高い安全性インテグリティレベルを実現するうえで不可欠です。

3.2.4 スマート絶縁型ゲートドライバ

UCC5881-Q1 は、大電力 SiC MOSFET および IGBT を駆動するための高度に構成可能な絶縁型かつ駆動能力の調整可能なゲートドライバです。これは、ISO26262:2018 に基づき開発され、包括的に検証された TI FuSa 準拠デバイスです。多数の安全メカニズムを組み込んだ ASIL-D までの ISO26262:2018 システム設計をサポートする資料が用意されています。

UCC5881-Q1 は、1 次側と 2 次側の両方に専用のハードウェア ASC ピンを備えています。このアクティブ短絡機能を使用することで、システムは PWM 入力に関係なく、パワー トランジスタの状態を強制的にオンにすることができます。故障またはその他の理由によりメイン マイコンが利用できない場合、2 次制御回路が ASC_EN 入力を High に駆動して、デバイスの出力を強制的に ASC ピン入力で定義された状態にします。図 3-9 に、UCC5881-Q1 を使用した代表的な ASC 実装図を示します。ASC 回路は BIST によっても検出され、正常に機能していることを確認します。

表 3-1 に、安全状態ピンの入力真理値表を示します。ここでは、入力のさまざまな組み合わせによって出力状態がどのように決定されるかを示します。これらの基本的な機能だけでなく、ASC は、他の特定の障害 (DESAT、貫通電流、SPI 障害など) を無効化する高優先度イベントとして柔軟に構成できます。2 次側 ASC は、UCC5881-Q1 の 1 次側電源の故障や、その他の PWM/通信関連の故障にかかわらず、システムを強制的に安全状態に移行させることも可能です。詳細については、UCC5881-Q1 データシートを参照してください。

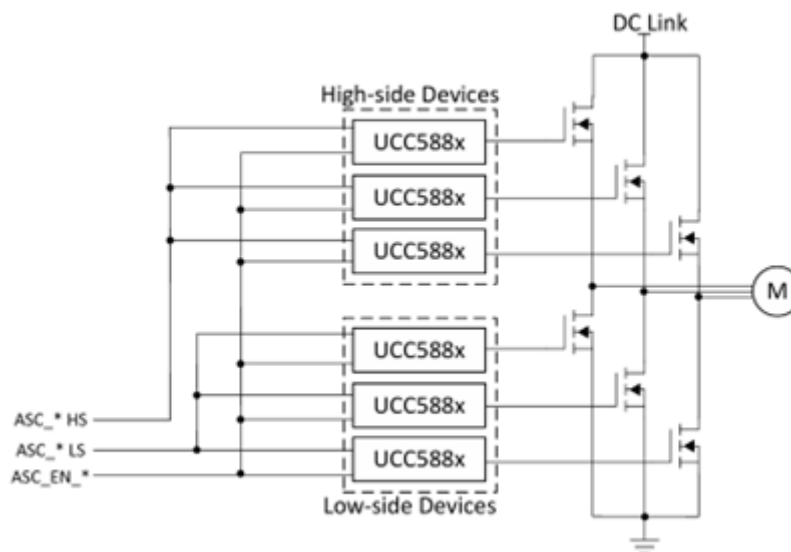


図 3-9. UCC5881-Q1 を使用した ASC の実装

表 3-1. UCC5881-Q1 の安全状態ピンの真理値表

INP	INN	ASC_EN_SEC	ASC_SEC	ASC_EN_PRI	ASC_PRI	出力状態
0	0	0	x	0	x	低
1	0	0	x	0	x	高
x	1	0	x	0	x	低
x	x	1	0	x	x	低
x	x	1	1	x	x	高
x	x	0	x	1	0	低
x	x	0	x	1	1	高

UCC5881-Q1 の貫通電流保護 (STP) 機能は、マイコンからの誤った PWM コマンドによって発生する可能性のある貫通電流状態に対する追加の保護層を提供します。この保護機能にもかかわらず、過電流またはパワー モジュールの短絡イベントが発生すると、UCC5881-Q1 は DESAT 信号によって通知します。これは BIST によっても監視されます。

トラクション インバータの安全設計アプリケーションでは、(マイコンと外部ロジック回路の両方からの) 外部 ASC 信号を UCC5881-Q1 の 1 次側 ASC ピンまたは 2 次側 ASC ピンに配線します。この構成により、ゲートドライバの出力が必要に応じて PWM 入力から独立して動作し、パワー モジュールに対して適切な安全状態出力を生成することができます。PWM 信号と ASC 信号は両方とも、絶縁レーン検出安全メカニズムで保護されており、絶縁レーンの潜在的な故障に対処できます。これらの FuSa 機能に基づき、システムは TI の安全指向デバイスを使用して、FSR 1.6 に関連する TSR を満たすことができます。

3.3 依存故障に関する検討事項

依存故障解析 (DFA) は、システム内の複数の部品の同時故障につながる可能性のある共通原因故障やカスケード故障を特定して評価するために設計された体系的な安全性分析手法です。DFA のコア原理は、システム内の相互依存性を分析して、環境要因、設計上の欠陥、製造プロセスの問題、外部干渉など、複数の安全機能が同時に故障する原因となるイニシエータを特定することです。

DFA の主なプロセスは、次の 4 つの主要なステップで実行されます。

- **ステップ 1:** アーキテクチャ要素を一覧し、依存ペアを識別します
- **ステップ 2:** 安全目標に違反する依存故障を誘発する可能性のある依存故障イニシエータ (DFI) を特定します
- **ステップ 3:** 依存故障を制御または軽減するために必要な安全対策を特定します。独立性が十分でない場合は、追加の措置を定義します
- **ステップ 4:** 依存故障を制御または回避するための対策の有効性を評価します

スペースに制限があるため、表 3-2 では、位置センサ サブシステムに焦点を当て、トラクション インバータ システムに関する DFA 解析の一部のみを示します。

表 3-2. トラクション インバータ DFA 例の表

要素	依存要素	DFI のタイプ	DFI 根本原因	DFI 効果	故障防止策	故障制御策
#1 LDC5073-Q1	#2 LDC5073-Q1	共有リソースの障害	共有電力	3.3V の共有電源により、#1 LDC5073-Q1 と #2 LDC5073-Q1 が同時に機能不全に陥る可能性があります	PMIC TPS65386x-Q1 3.3V LDO を内蔵し、UV、OV、SC イベント用の出力電圧監視機能を搭載します。	- PMIC IC レベルの検証とテスト - 顧客による統合テスト
			共有の電源要素	PMIC の障害により、#1 LDC5073-Q1 と #2 LDC5073-Q1 が同時に機能不全に陥る可能性があります	TPS65386-Q1 は、BIST、UVLO、VMON、CRC など、複数の安全メカニズムを搭載しているため、PMIC の障害に対応できます	- PMIC IC レベルの検証とテスト - 顧客による統合テスト
		単一の物理的な根本原因	クロストーク	位置センサの配置によってはクロストークの影響を受け、#1 LDC5073-Q1 と #2 LDC5073-Q1 が同時に機能不全に陥る可能性があります	NA	シミュレーションおよび妥当性試験による性能の検証。
			局所的な加熱	位置センサの配置によっては熱の影響を受け、#1 LDC5073-Q1 と #2 LDC5073-Q1 が同時に機能不全に陥る可能性があります	NA	- 周囲温度は仕様で定義されています。デバイスは、これらの条件に対して設計/シミュレーションおよびテストされています - このデバイスでは、AEC-Q100 の高温動作寿命認定を実施しています。
		環境的故障	EMI	一部のアプリケーション シナリオでは、#1 LDC5073-Q1 と #2 LDC5073-Q1 の両方が同時に影響を受け、機能不全に陥る可能性があります	NA	顧客による統合テスト
			ESD	位置センサの配置によっては ESD の影響を受け、#1 LDC5073-Q1 と #2 LDC5073-Q1 が同時に機能不全に陥る可能性があります	特定の境界に対応する ESD 保護設計。	ESD 制限は仕様で定義されており、ESD テストは、ESD 規格に従ってすべてのピンに対して実行されます

トラクション インバータ システム FuSa 設計では、DFA 解析手法が包括的に実装されています。その結果、共通原因故障に直面した場合にシステムが必要な安全機能を維持できるように、多様な冗長性、物理的な分離、独立監視、その他の保護対策が設計に実装されています。こうした対策により、FuSa レベルとトラクション インバータ システムの信頼性が大幅に向上します。

依存故障解析に対する体系的なアプローチにより、潜在的な共通原因故障を設計プロセスの早期段階で特定し、適切な対策を実施することで、トラクション インバータ システムの全体的な安全性を損なう恐れのある同時故障を防止します。

3.4 トラクション インバータの詳細な FuSa 設計構造

このセクションでは、セクション 2 で説明した手法を用いて、トラクション インバータの安全設計で使用される TI のさまざまな FuSa 部品の概要を説明します。システムレベルの FuSa 分析は、特定の使用シナリオとアーキテクチャに大きく依存します。以下のセクションでは、選定された部品の基本機能を説明し、続いて各部品の FuSa メカニズムをご紹介します。

[図 3-10](#) に、トラクション インバータの部品レベルでのアーキテクチャを示します。

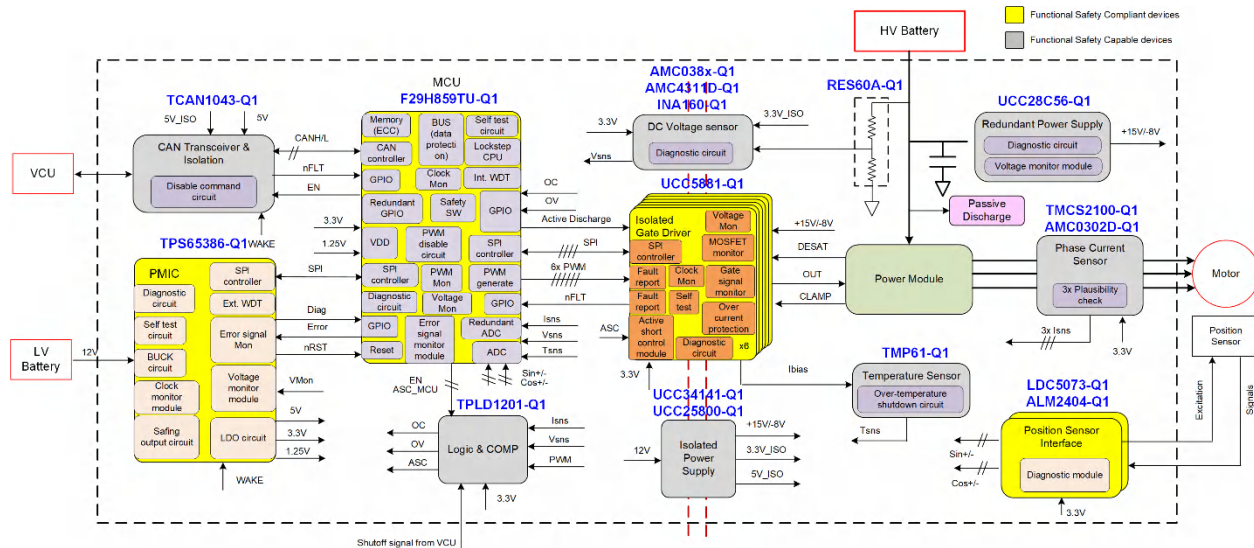


図 3-10. トラクション インバータの部品レベル アーキテクチャ

トラクション インバータには、パワー スイッチや受動部品以外に、主な機能ブロックとして、マイコン、ゲートドライバ、絶縁型バイアス電源、パワー マネージメント IC、位置センサ電流センサ、電圧センサ、温度センサ、通信インターフェイス、ロジック回路が含まれます。

- マイコン (MCU)。** モーター制御 FOC アルゴリズムの実行、センサ データの監視、システムの保護、VCU との通信を行います。安全性が極めて重要視される設計においては、ロックステップ コアに加え、マイコン専用の内部ウォッチドッグや自己診断機能が不可欠となります。
- ゲートドライバ。** パワー モジュールに必要な電圧および大電流駆動信号を供給します。絶縁型ゲートドライバは、低電圧側と高電圧側に強化されたガルバニック絶縁も提供します。システムの FuSa 要件を満たすため、絶縁型ゲートドライバには、BIST、DESAT、クランプ回路、ASC、ゲート監視、PWM レーン検出など、数多くの安全機能が組み込まれています。
- 絶縁型電源。** 絶縁型バイアス電源は、ガルバニック絶縁を維持しながら、ゲートドライバ用電圧を生成し、検出回路の高電圧側に電源を供給します。SiC と IGBT を駆動するには、正と負の両方の絶縁型バイアス電源が必要です。異なるゲートドライバに対してバイアス電源を分離することにより、FuSa レベルのより高い設計に対応できます。
- パワー マネージメント IC (PMIC)。** 保護機能を備えた電圧変換、電源シーケンス制御、電圧監視、診断、保護、ウォッチドッグ、通信など、複数の電源機能を管理および制御します。主要デバイスに電源を供給し、主要な電圧レールの電圧監視を行います。また、マイコン用の外部ウォッチドッグおよびエラー ピン監視機能も提供します。マイコンで回復不可能な故障を検出する際、PMIC はマイコン リセットをトリガし、関連する制御信号を遮断して、システムが確実に安全状態に移行できるようにします。
- 位置センサ。** FOC 制御目的で、モーターの回転子の位置と速度を測定します。トラクション インバータの一般的な位置検出ソリューションは、リゾルバと誘導性センサです。トラクション インバータは励起信号をリゾルバ/誘導性センサに生成し、センサ フィードバック信号を受信してデコードします。信号配線はメイン ボードの外部にあるセンサに接続されているため、バッテリー/GND への短絡に対する保護が必要です。
- 電流センサ。** FOC 制御用に 3 相 AC モーター電流を測定し、過電流保護を実装します。代表的な実装例としては、過電流検出用ピンを備えたホール効果方式の電流センサ、またはコンパレータを搭載したシャント抵抗式電流アンプなどが挙げられます。
- 電圧センサ。** FOC および変調目的で、HV バッテリーの DC 入力電圧を測定し、過電圧または低電圧イベントを検出して保護を行います。
- 温度センサ。** パワー モジュールの接合部温度とボードの周囲温度を監視し、マイコンに通知します。FuSa 要件を達成するために、冗長化温度センサを実装することができます。NTC または PTC をマイコンの ADC またはゲートドライバ ADC にバイアス電流で接続するだけで測定できます。
- 通信インターフェイス。** VCU からトルク コマンドおよびその他の命令を受信し、ステータスおよび故障信号を VCU に報告します。トラクション インバータでは、通常、2 つの CAN トランシーバ チャンネルが実装されます。安全上重要なメッセージは、データの完全性を検証するために、巡回冗長検査 (CRC) およびメッセージ カウンタのチェックを伴って送信されます。

- **ロジック。** FuSa 設計にはロジック回路が使用され、PWM 実行可能性チェック、安全状態入力回路、冗長モーター速度検出などの保護を実現します。

3.5 TI 安全デバイスでの FuSa 要件の達成

セクション 2.4 で説明するように、トラクション インバータ システム内で障害イベントが発生した場合はそれを検出または軽減する必要があり、障害が発生したときはシステムは適切な安全状態に移行する必要があります。このセクションでは、FuSa を目的としたトラクション インバータに TI のデバイスを効果的に実装する方法を示します。特に、必要に応じてシステムが ASC またはフリーホイール状態に移行するのに役立つ設計に重点を置きます。

3.5.1 マイコン

F29 シリーズのデバイスは、車載および産業用アプリケーションのリアルタイム制御向けに設計された C29x CPU を搭載した強力なマイコンです。C29x CPU は、完全に保護されたパイプラインを備えた VLIW (超長命令ワード) アーキテクチャであり、複数の命令サイズをサポートしています。デバイスは、オンチップのフラッシュ メモリまたは RAM 上で動作し、32 ビットおよび 64 ビットの浮動小数点および固定小数点信号処理をサポートする最大 3 つの 200MHz C29x コアで構成されています。C29x CPU は、三角関数演算命令によってさらに強化され、リアルタイム制御システムでよく使われる重要なアルゴリズムを高速化します。

セクション 3.2.2 に説明されているように、ロックステップ機能、エラー訂正コード (ECC) 保護、クロスチェック機能を備えた冗長 ADC、GPIO/PWM 読み戻し機能など、いくつかの主要機能が、トラクション インバータ FuSa 設計に特に役立ちます。前述の安全メカニズム以外にも、F29 マイコンは追加の機能、ペリフェラル、および FuSa システム設計に適した多数の安全メカニズムを提供します。

- **ロジック パワーオン セルフテスト (LPOST)。** システムの起動時に、重要なロジック回路の整合性を検証します
- **メモリ パワーオン セルフテスト (MPOST)。** システムの初期化時に、メモリの内容が有効であることを確認します
- **エラーおよび通知モジュール (ESM)。** デバイス全体のエラー検出と処理を一元化します
- **デュアル クロック コンパレータ (DCC)。** クロック周波数を監視し、クロック障害を検出します
- **安全/セキュリティユニット (SSU) による状況依存メモリおよびペリフェラルの保護。** A/B スワップおよびロールバック制御によるアプリケーション ファームウェア更新のための安全なライブ ファームウェア アップデート (LFU) および FOTA をサポートしています。
- **安全相互接続 (SIC)。** 安全性が重要な部品間で、保護された通信パスを実現します
- **サイバーセキュリティ向けに ECC 保護されたハードウェア セキュリティ モジュール (HSM)。**
- **構成可能ロジック ブロック (CLB)。** カスタム安全メカニズムに適したプログラマブル ロジック機能を実現します
- **組み込みパターン ジェネレータ (EPG)。** 診断目的のテスト パターンを生成します
- **ウィンドウ付きウォッチドッグ タイマ モジュール**
- **クロック消失検出回路。** システムのタイミングを損なう可能性のあるクロック障害を特定します
- **メモリ保護ユニット (MPU) 搭載リアルタイムダイレクトメモリアクセス (RTDMA) コントローラ。**

こうした包括的な安全機能により、F29 シリーズ マイコンは、現代のトラクション インバータ システムにおける複雑な FuSa 要件への対応に特に適しています。これにより、故障を検出し、必要に応じて適切な安全状態へ移行することが可能になります。

3.5.2 ゲートドライバ

トラクション インバータ システムにおいて、パワー モジュールにおける意図しないトルクの発生や、過電流/貫通電流状態を防ぐため、ゲートドライバには高い FuSa レベルが割り当てられています。UCC5881-Q1 は、駆動能力の調整が可能で高度に構成可能な絶縁型ゲートドライバです。これは、大電力 SiC MOSFET および IGBT を駆動するために特別に設計されています。安全状態に移行するための ASC 機能については、セクション 3.2.4 に説明が含まれています。

UCC5881-Q1 には、ASC 機能以外にも、ゲートドライバ出力状態監視、障害状態時のソフト ターンオフ、パワー モジュールのスレッシュホールド電圧検出、過電圧/低電圧誤動作防止 (OV/UVLO)、貫通電流保護など、多くの保護機能が内蔵されています。UCC5881-Q1 はアクティブ ミラー クランプ機能もサポートしており、高 dv/dt イベント時にパワー モジュールが意図せずオンになることを防止します。さらに、このデバイスには 2 つの外部 ADC チャンネルがあり、複数の DC リンク電圧とパワー モジュールの温度センシング パスをサポートします。これは、測定の冗長性を実装しながら、システム コストを最適化する上で有益です。

図 3-11 に、代表的なトラクション インバータ アプリケーションにおける UCC5881-Q1 のブロック図を示します。主な保護機能と安全メカニズムを以下に示します。

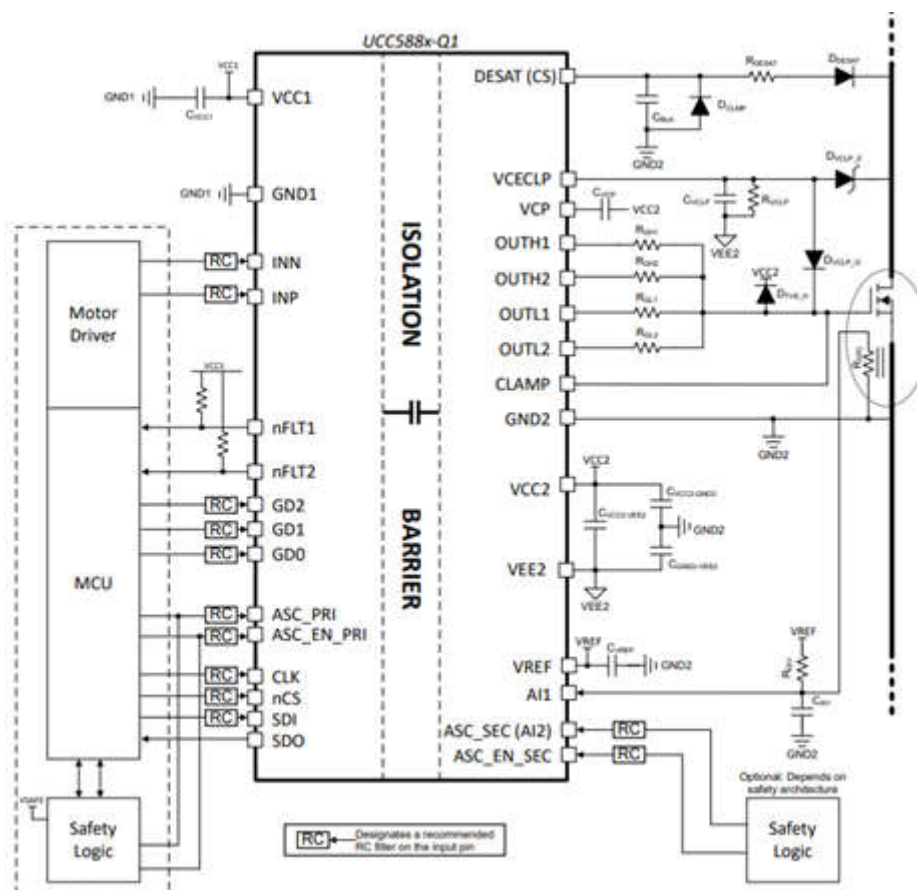


図 3-11. 一般的なトラクション インバータで使用されている UCC5881-Q1 のブロック図

3.5.2.1 ゲート監視回路と過電流保護

ASC 安全状態に適切に移行するには、トラクション インバータが 3 つのハイサイド パワー スイッチのすべてまたは 3 つのロー サイドパワー スイッチのすべてを確実にオンにしながら、反対側のレッグをオフに維持する必要があります。

UCC5881-Q1 は、ゲートドライバの出力電圧レベルがマイコンからの入力 PWM 信号と一致しているかどうかを検出するゲート監視回路を内蔵しています。この回路により、ゲートドライバ出力の障害またはパワー スイッチの短絡/断線状態を迅速に検出できます。各ゲートドライバおよびパワー スイッチの健全性状態を監視することで、マイコンは、安全状態への移行中にどの電源レッグをオンにする必要があるかを情報に基づいて決定することができます。図 3-12 に、ゲート監視回路のブロック図を示します。

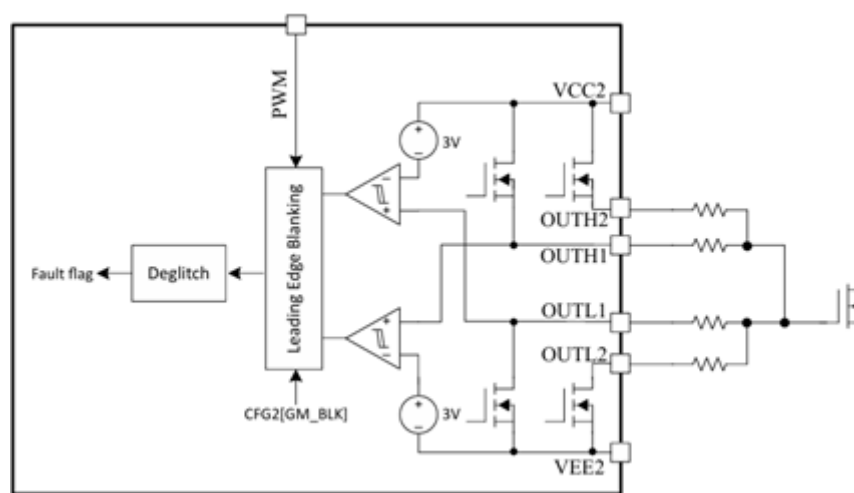


図 3-12. UCC5881-Q1 のゲート監視回路

過電流保護は、トラクション インバータにおける極めて重要な安全機能です。これは、過電流状態を放置すると、2 ～ 3 マイクロ秒以内 (SiC デバイスの標準値) に対処しなければ、深刻な損傷を招く恐れがあるためです。UCC5881-Q1 は、過電流保護のための DESAT 回路を内蔵しています。図 3-13 に示されているように、DESAT 入力、外部抵抗およびダイオード ネットワークを介して、IGBT のコレクタ/エミッタ間飽和電圧 (V_{CEsat}) または MOSFET のドレイン ソース間オン状態電圧 (V_{DSon}) を監視します。

パワー FET がオンの間、内部電流源 I_{CHG} は DESAT ダイオードを順方向バイアスし、外部パワー スwitch のコレクタ/ドレインにシンクします。DESAT 入力の電圧がスレッシュホールドまで充電されると、DESAT 故障が検出されます。UCC5881-Q1 は、故障を通知し、パワー モジュールをソフト ターンオフして、シャットダウン時の電圧スパイクを最小限に抑えます。その後、マイコンは 6 つのゲートドライバからの DESAT およびゲート監視情報に基づいて、システムを強制的に適切な安全状態に移行させます。

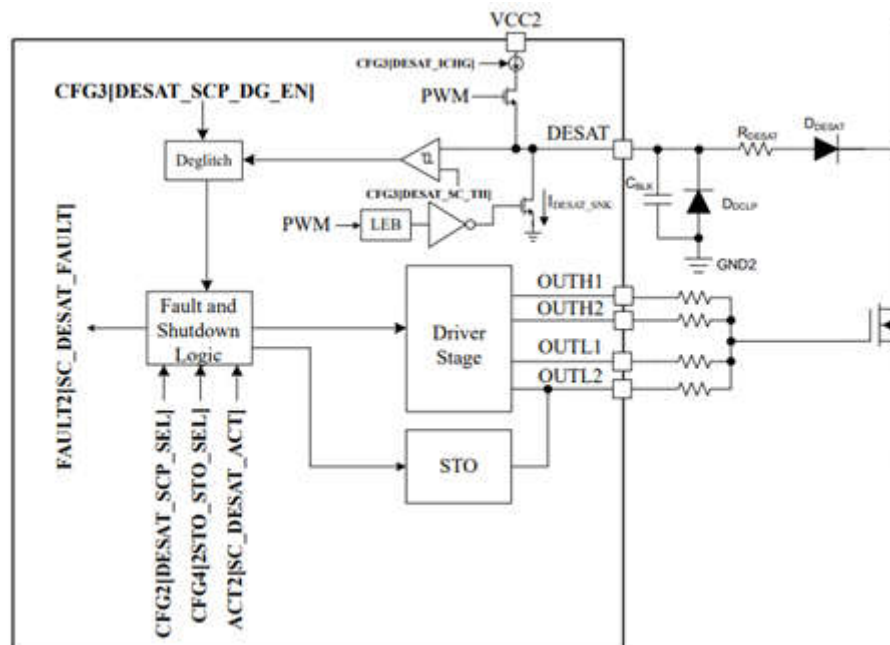


図 3-13. UCC5881-Q1 の DESAT 回路ブロック図

ゲート監視と高速な過電流保護の組み合わせにより、電源部品の損傷やモーターで意図しないトルクが発生する前に、トラクション インバータが異常動作状態を迅速に検出し、安全状態に移行できることを検証します。

3.5.2.2 UCC5881-Q1 のその他の安全メカニズム

ゲート監視および過電流保護機能以外に、UCC5881-Q1 には、トラクション インバータの保護および異常検出出力機能を強化するように設計された多数の追加安全メカニズムが組み込まれています。

- スタートアップ状態での $V_{gs(th)}$ パワー モジュールの健全性ステータス チェック。
- VCC1、VCC2、VEE2 電源の低電圧と過電圧の監視
- サポート回路に使用される内部電源の低電圧と過電圧の監視
- ロジック クロックのクロック監視
- 構成データ巡回冗長検査 (CRC)
- SPI の CRC
- 内部 NVM (不揮発性メモリ) CRC
- VCC1、VCC2、VEE2、内部レギュレータの UV/OV 監視機能、メイン クロックの内蔵セルフテスト (BIST) 診断機能
- パワー トランジスタの高電圧クランプ回路の検出と機能の診断
- アクティブ ミラー クランプ診断。

3.5.3 絶縁型バイアス電源

トラクション インバータ システムにおいて、絶縁型電源は、低電圧制御回路と高電圧電力段の間でガルバニック絶縁を維持しながら、ゲートドライバに必要な電力を供給する重要な機能を果たします。絶縁型電源にはゲートドライバを適切に動作させる役割があるため、意図しないトルク生成を防止するために、高い **FuSa** レベルを割り当てます。さまざまなアーキテクチャアプローチに基づき、トラクション インバータ システムに実装されている絶縁型電源構造には、以下の 3 つの主要な種類があります。集中型電源、完全分散型電源、半分散型電源。

3.5.3.1 集中型 LV 絶縁型電源アーキテクチャ

図 3-14 に、トラクション インバータの集中型電源アーキテクチャを示します。すべてのハイサイドおよびローサイドのゲートドライバには、単一の絶縁型バイアス電源デバイスを使用して電力を供給します。このアプローチは、部品点数の低減を通じてコスト面で大きな利点があります。しかし、集中型アーキテクチャでは、安全性に関する重要な懸念が生じます。特に、この単一電源デバイスの故障は単一の故障点を形成するものです。故障が発生した場合に、すべてのゲートドライバが同時に電力を失い、故障状態が発生したときに、トラクション インバータが必要とされる安全状態に入ることを防止する可能性があります。集中型アプローチにおけるもう 1 つの大きな課題は、すべてのゲートドライバに電力を供給するための 6 つの 2 次側巻線 (1 次と 2 次の比 = 1:6) を備えたトランスを設計する際の複雑さです。この設計には専用のトランス構造が必要で、すべてのゲートドライバに到達できるように、長い PCB パターンが存在する複雑な PCB レイアウトが可能になります。

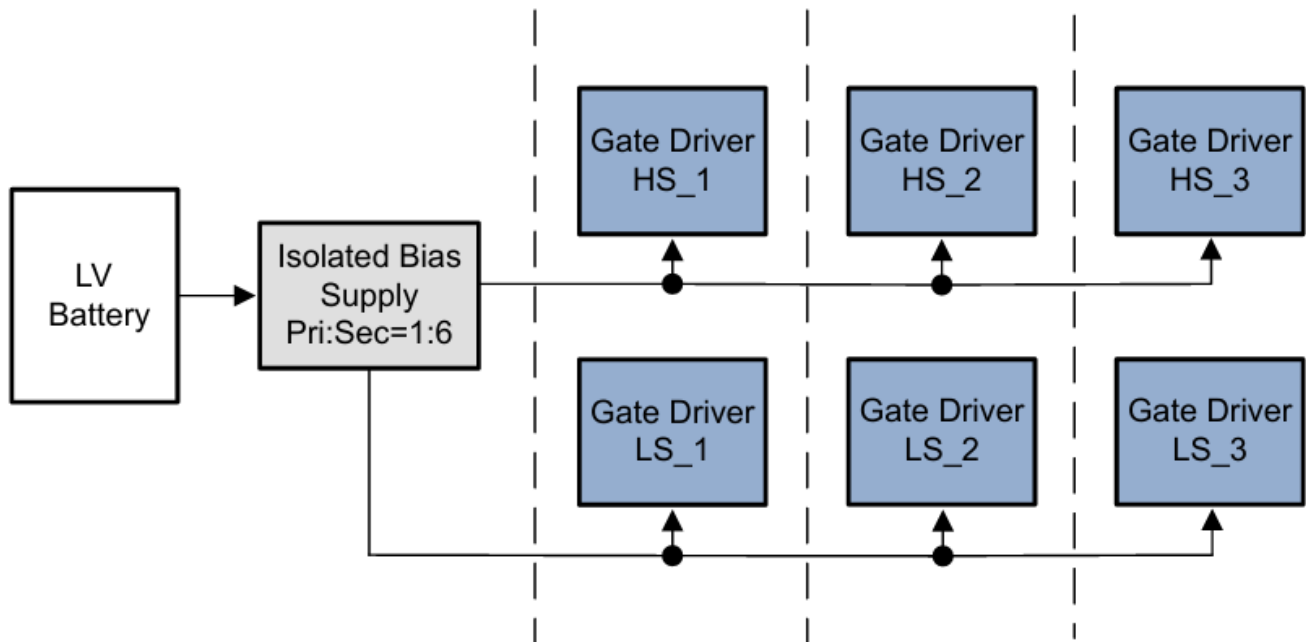


図 3-14. 集中型絶縁型電源アーキテクチャ

3.5.3.2 完全分散型 LV 絶縁型電源アーキテクチャ

図 3-15 に、トラクション インバータ内の完全分散型電源アーキテクチャを示します。この構成では、各ゲートドライバに独自の個別の絶縁型バイアス電源デバイスから電力を供給します。このアプローチでは、3 相インバータ内にある 6 つの絶縁型ゲートドライバに電力を供給するために、6 つの個別の絶縁型バイアス電源デバイスが必要です。この完全冗長ソリューションの主な利点は、耐障害性が強化されていることです。バイアス電源回路で個別に障害が発生しても、システムは引き続き適切な安全状態に移行できます。これにより、集中型アーキテクチャで発生する単一障害点の問題が解消されるため、完全分散型のアプローチは、耐障害性が重要な ASIL の高アプリケーションに特に適しています。

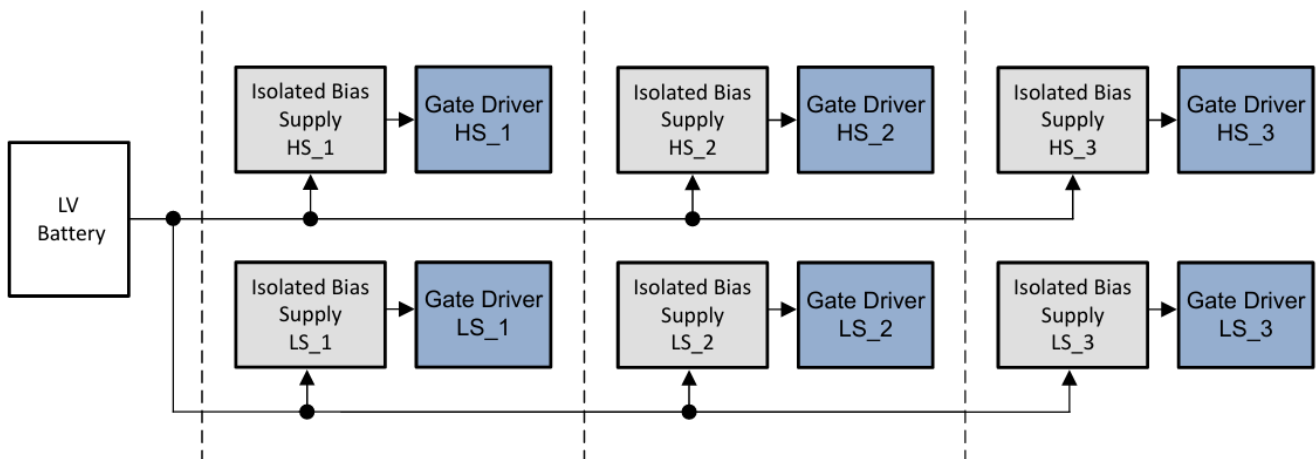


図 3-15. 完全分散型絶縁型電源アーキテクチャ

3.5.3.3 半分散型 LV 絶縁型電源アーキテクチャ

図 3-16 に、トラクション インバータの完全分散型電源アーキテクチャを示します。このアーキテクチャは、集中型アプローチと半分散型アプローチの戦略的な妥協点を表しています。この構成では、単一の絶縁型バイアス電源デバイスから複数のゲートドライバが電力を共有しますが、システムは全体として複数の電源ユニットを使用します。このハイブリッド手法により、絶縁型電源デバイスの総数が減ることで、完全分散型アーキテクチャと比べてコストを削減できます。また、集中型アプローチに固有の完全なシャットダウンの脆弱性も回避できます。1 つの電源で障害が発生した場合、ゲートドライバ

の一部のみが電力を失い、他の電源は動作状態を維持します。この部分的冗長性により、電源障害が発生した場合も、インバータが安全状態に移行する能力を確実に維持できます。

このアーキテクチャは柔軟性が高いため、システム設計者は電力分配戦略をアプリケーション固有の要件や安全目標に合わせてカスタマイズでき、最新のトラクション インバータの設計に適した多様性の高いソリューションとなります。

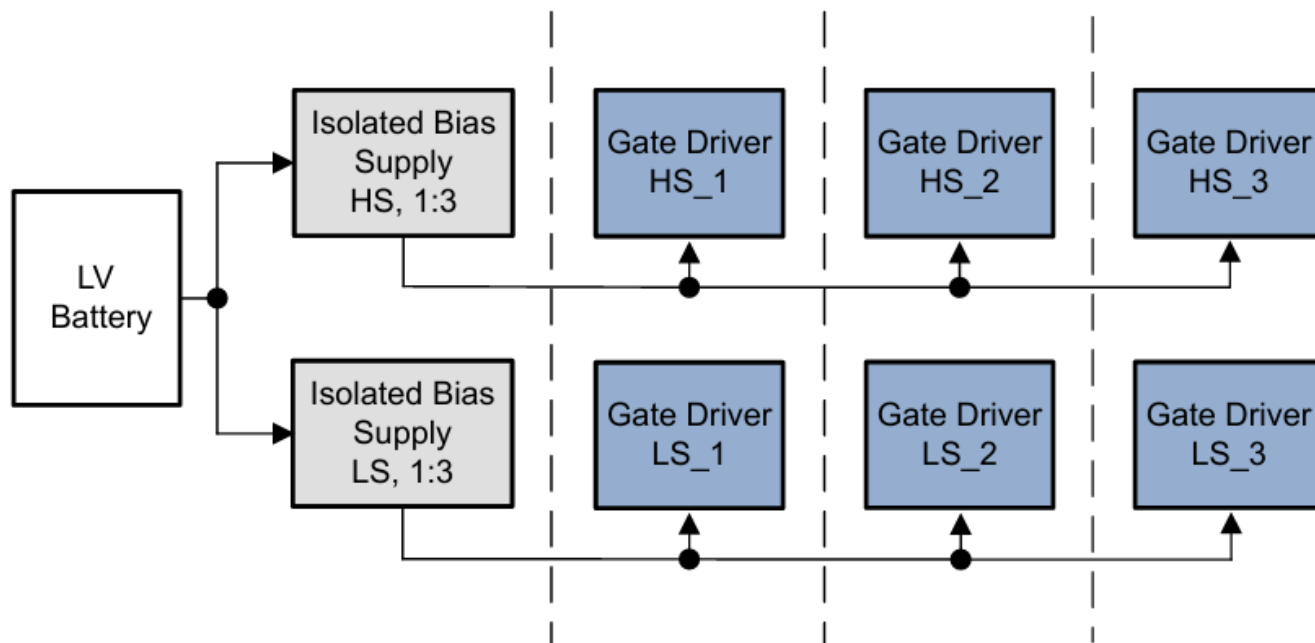


図 3-16. 半分散型絶縁型電源アーキテクチャ

3.5.3.4 HV 絶縁型バイアス電源

前述の LV 絶縁型バイアス電源アーキテクチャに加えて、HV 絶縁型バイアス電源は、より高い FuSa レベルの設計のゲートドライバ用冗長電源として実装することもできます。図 3-17 に、このハイブリッド構造の例を示します。このハイブリッド構造では、ローサイド ゲートドライバが LV システムと HV バッテリの両方から電力を受け取り、冗長パワー パスを生成します。この戦略的な構成により、LV 電源システムが完全に故障した場合でも、少なくとも 1 組のドライバ (この場合はローサイドドライバ) が電源供給を維持できることが保証され、それによってシステムは可能な安全状態のうち少なくとも 1 つを実現できるようになります。

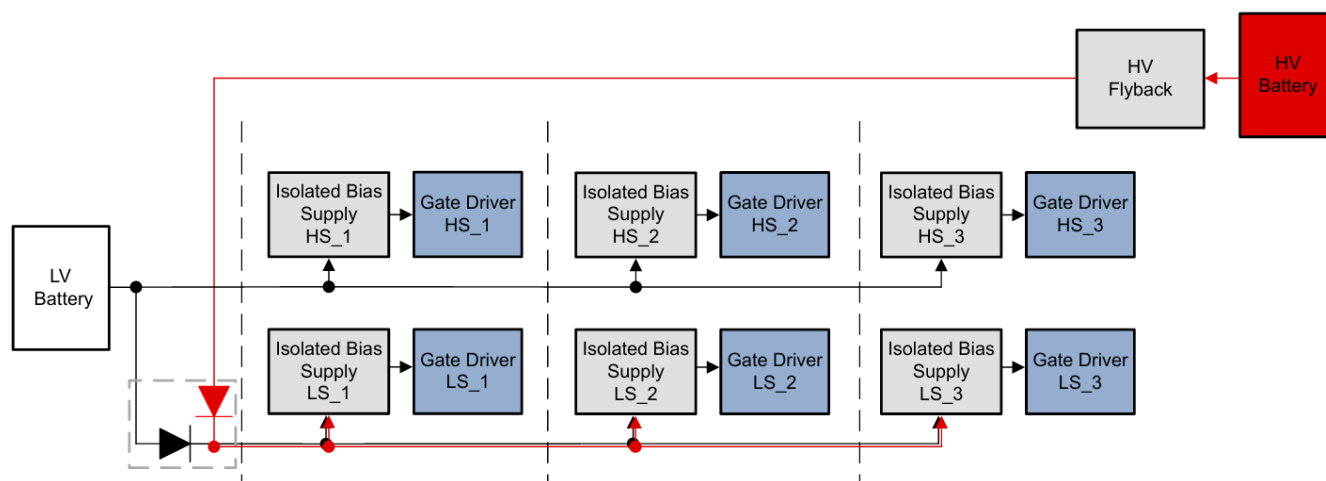


図 3-17. FuSa 設計向けの HV と LV 両方の絶縁型バイアス電源の実装

3.5.3.5 トラクション インバータ内の絶縁型バイアス電源向けの TI の設計

TI では、これまでに説明したすべての絶縁型バイアス電源アーキテクチャに対応する包括的なソリューションを提供しており、設計者は特定のアプリケーション要件に適したアプローチを柔軟に実装できます。

図 3-18 に示されているように、TI は、LV 絶縁型電源アプリケーション向けに、統合型 DC/DC モジュールの複数のバリエーション (UCC34xxx-Q1) を提供しています。これらの高度なモジュールは、10MHz を上回る周波数で動作する H ブリッジトポロジを採用した内蔵トランスを採用しています。このように高度な統合機能を採用した結果、外部トランスが不要になり、システムのサイズと高さを大幅に低減できます。これらの統合型モジュールの主な利点として、わかりやすいフィードバック設計によって出力電圧の設定が簡素化されることが挙げられます。この機能により、絶縁型電源設計に必要なエンジニアリング労力が大幅に削減されると同時に、小型サイズ、低プロファイル、コスト効率の点でのメリットが実現します。図 3-19 は、TI の統合型 DC/DC モジュールと従来型のバイアス電源方式を視覚的に比較したものであり、フォームファクタと統合性の面での明確な利点を示しています。

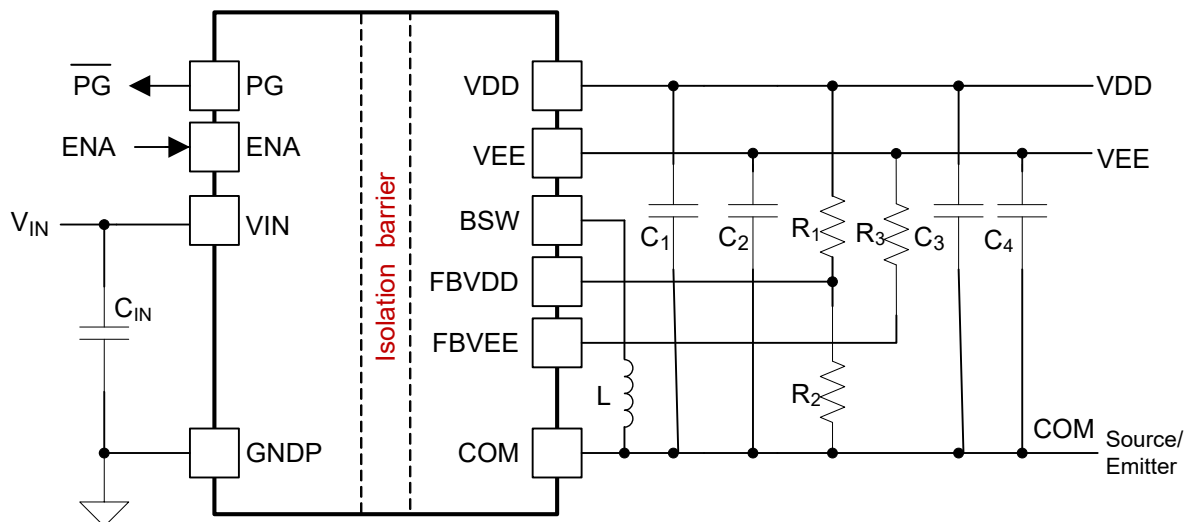


図 3-18. トランスと FET を内蔵した UCC3414x-Q1 のアプリケーション ブロック図

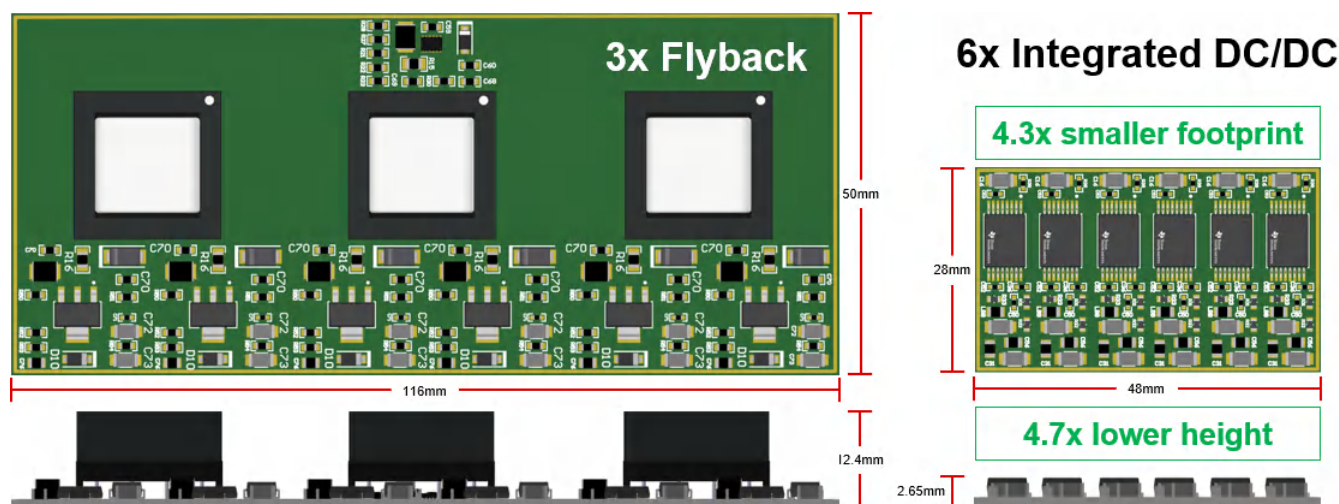


図 3-19. 統合型 DC/DC モジュール UCC3414x-Q1 とフライバックのサイズ比較

これらの統合型モジュールに加えて、TI は代替の絶縁型電源アーキテクチャと事前安定化コンバータ向けのソリューションも提供しています。これには、フライバック (LM515x-Q1、LM(2)518x-Q1)、LLC 共振コンバータ (UCC25800-Q1、UCC259xx-Q1)、プッシュプル (SN650x-Q1)、HV フライバック設計 (UCC28C5x-Q1、UCC287xx-Q1、UCG288xx)、昇降圧コンバータ (TPS55287x-Q1、UCC55289x-Q1) が含まれます。これらのオプションにより、設計者は特定の電源要件、絶縁ニーズ、システムの制約に基づいて、追加の実装を選択できます。HEV および EV トラクション インバータ向

けの絶縁型バイアス電源アーキテクチャおよび実装オプションに関する詳細情報については、以下の TI ホワイトペーパーを参照してください。『HEV および EV トラクション インバータ向けの絶縁型バイアス電源アーキテクチャ』。

3.5.4 パワー マネジメント IC

パワー マネジメント IC は、トラクション インバータ システムにおいて、マイコン、センサ、CAN トランシーバ、ゲートドライバ、ロジック回路など、事実上すべての低電圧部品に電力を供給するという極めて重要な役割を担っています。これらの要素に対して信頼性が高く十分な電力が供給されなければ、トラクション インバータは、モーターを適切に制御するために必要な FOC アルゴリズムを実行できません。図 3-20 に示されているように、TPS65386x-Q1 デバイスは、TI の車載パワー マネジメント向けの高度なソリューションを実現します。この高集積デバイスは、昇降圧コンバータを内蔵し、内部 FET を使用して、入力バッテリー電圧を構成可能な事前安定化出力電圧に変換します。この事前安定化出力は、次にデバイス内の他の内蔵リニア レギュレータに電力を供給し、追加の電源レールが必要な場合は外部レギュレータもサポートできます。

また、TPS65386x-Q1 は低消費電力モード機能を備えているため、各種の動作状態にわたって電力効率が重要なマイコン電源アプリケーションに特に適しています。このデバイスは、ISO 26262:2018 規格に準拠して開発され、車載アプリケーション向けに完全に検証された TI の FuSa 準拠製品に分類されています。多数の安全性メカニズムを搭載したデバイスで、ASIL D までの ISO 26262:2018 システム設計をサポートするための包括的な資料を提供しています。

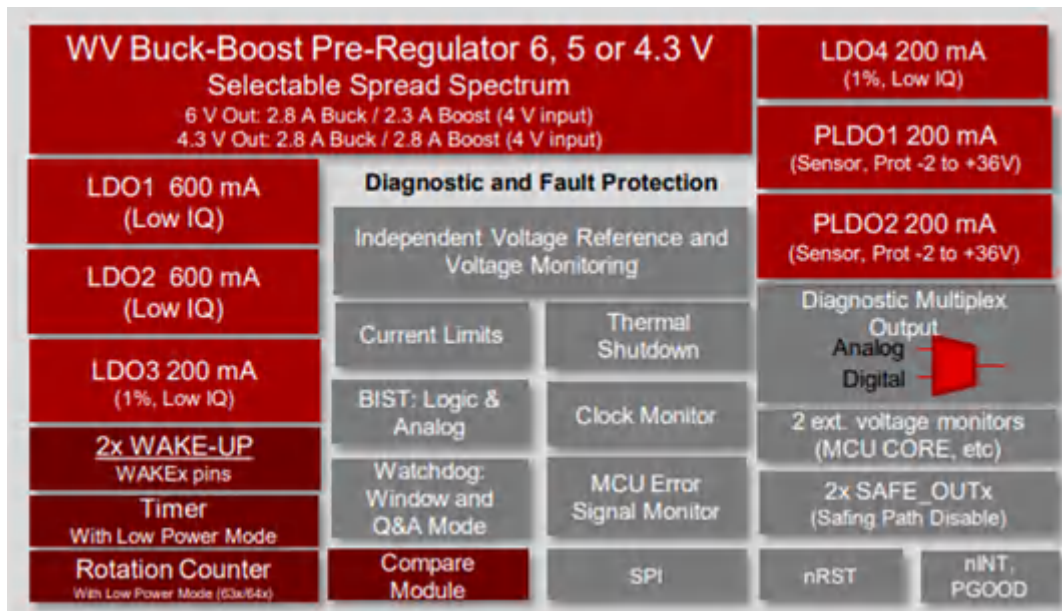


図 3-20. TPS65386x-Q1 のリソース

3.5.4.1 保護機能および独立サーマル シャットダウンを備えた複数パス電源レール

TPS65386x-Q1 は、複数の保護されたパワー パスと独立した熱管理機能を備えた精巧な電源アーキテクチャを実装しているため、部分的な障害が発生しても信頼性の高い動作が保証されます。

昇降圧レギュレータはこのアーキテクチャのコアを形成し、複数の FET 内蔵の同期 DC/DC コンバータとして機能します。この高効率設計により、デバイス内の消費電力を最小限に抑え、熱ストレスを低減できます。昇降圧コンバータは、入力電源電圧を低電圧ドメイン (VOUTBB) に変換し、LDO (低ドロップアウト) レギュレータと PLDO (保護低ドロップアウト) レギュレータの電源として機能します。コンバータは、すべての内部レギュレータにそれぞれ最大出力電流を供給すると同時に、必要に応じて、外部レギュレータに追加の電流容量を供給できるように設計されています。重要な安全機能として、パワー MOSFET における過剰な電力損失を防ぐ内臓の接合部温度監視システムが挙げられます。また、この昇降圧コンバータはデジタル スペクトラム拡散技術を採用しており、広範な周波数帯域にわたって EMI を低減し、システムの電磁適合性を向上させています。

LDOx リニア レギュレータは、1.0V ~ 1.8V (50mV 刻み) の柔軟な出力電圧オプションと、2.5V、3.0V、3.3V、5V の固定オプションを用意しています。未使用の LDOx レギュレータは電圧モニタとして転用し、システムに監視機能を追加す

ることができます。各 LDOx には独自の独立した接合部温度モニタが含まれており、いずれかの単一の LDOx レギュレータで過熱イベントが発生した場合も、その特定のレギュレータのみが無効化され、その他のレギュレータは引き続き機能します。デバイス構成によっては、その結果として低電圧イベントが発生し、必要に応じて、さらなる状態遷移がトリガされることがあります。この選択的シャットダウン機能は、マイコンのコア電源またはデジタル電源が失われたとしても、外部デバイスに電力を供給できることを意味します。図 3-8 に示す TPLD1201-Q1 回路は、この機能を活用して、マイコンが故障したときもシステムを安全状態に移行することができます。

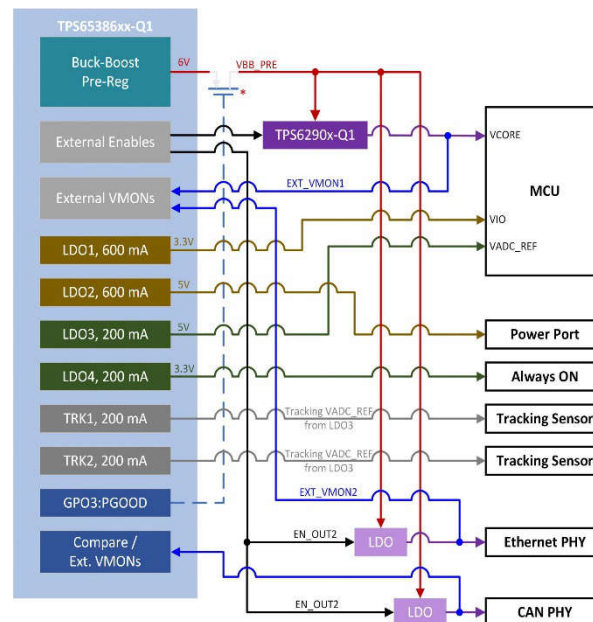
PLDOx レギュレータは、トラッキング モード、固定出力電圧 LDO モード、電圧監視モードの 3 つの動作モードをサポートし、さらに高い柔軟性を提供します。これらのレギュレータは、電源 (+36V) とシャーシ グランド (-2V) への短絡に対する堅牢な保護機能を内蔵しているため、ECU から電源が供給される可能性のあるセンサ アプリケーションや、位置センサ電源などの標準的な内部アプリケーションに最適です。PLDO は、TRACK 入力ピンを基準とするトラッキング モードでも動作できます。信頼性を高めるため、デバイスはクロスチェックと冗長性を行うための 2 つの独立したバンドギャップ電圧リファレンスソースを内蔵しており、潜在的なバンドギャップ開路モードとドリフト故障モードに対応しています。

この包括的な電源アーキテクチャは、複数の独立したパワー パスと保護メカニズムを備えており、電力システムの部分的障害が発生した場合も、トラクション インバータが重要な安全部品に対して適切な電力を維持できるようにします。

3.5.4.2 電源レール電圧監視

TPS65386x-Q1 は、トラクション インバータ アプリケーションの FuSa にとって重要となる包括的な電圧監視機能を実装しています。デバイスは、VBAT 電源電圧、すべての内部レギュレータ出力電圧、専用 EXT_VMONx ピンを介した外部レール、内部バイアス電圧など、複数の電圧レールを継続的に監視します。VMON モジュールが監視対象電圧レールでエラー イベントを検出すると、対応する VMON エラー フラグ ビットが直ちに設定され、潜在的な問題をシステムに警告すること、または障害が発生した電源レールをオフにすることができます。VMON のリファレンスの精度を確保するために、メイン バンド ギャップ電圧リファレンスは、2 番目の独立バンドギャップ リファレンスによって継続的にクロスチェックされます。さらに、内蔵アナログ セルフテスト (ABIST) は、VMON モジュールの診断チェックを定期的に行い、正常に動作していることを検証します。各電源レールで障害が発生すると、それが通知され、システムは方針に基づいて安全状態に移行することができます。

また、TPS65386x-Q1 には 2 チャネルの外部電圧モニタも搭載されており、マイコン コア入力電圧または事前安定化電圧など、重要な外部電源レールの監視に使用できます。この拡張監視機能により、システム レベルの FuSa 範囲がより高くなります。図 3-21 に、これらの外部モニタを使用して、マイコン コアおよび他の LDO に電力を供給する外部 DC/DC コンバータを監視する実装例を示します。TPS65386x-Q1 によって適切に監視されていれば、品質管理 (QM) デバイスもこの配置で DC/DC コンバータとして使用できます。この監視関係により、個別の安全定格が低い部品を使用する場合も、電源システム全体が ASIL D の安全要件を満たすことができます。また、適切な監視と故障検出による安全構成の原理を実証できます。



* If risk of VBB_PRE weak-short to VBAT is high protection switch is needed to protect external LV BUCK and LDOs

図 3-21. 外部電源レールを監視する TPS65386x-Q1 の例

3.5.4.3 マイコン故障監視および他の保護メカニズム

TPS65386x-Q1 は、モジュールの安全マイコンを監視します。安全マイコンのハードウェアおよび/またはソフトウェアの実行において故障モードが発生した場合、PMIC は故障の重大度に応じて異なる対応を行います。これには、マイコンへの割り込み通知、故障状態がスレッシュホルドを超え続けた場合の外部電源段やモジュール通信インターフェイスの遮断、安全マイコンの再起動などが含まれます。このようなマイコンの動作不能期間中、TPLD1201-Q1 ロジック デバイスは重要な安全機能を引き継ぐことができ、マイコンが制御されていなくても、システムを適切な安全状態に移行するのに役立ちます。

これらの主要な安全メカニズム以外にも、TPS65386x-Q1 には FuSa 設計を強化する多くの追加安全メカニズムが内蔵されています。

- トリガ モードと Q&A (質問・回答) モードを備えたウォッチドッグ。
- マイコンの出力ピンからマイコンの故障情報を出力するマイコン内蔵エラー診断機能によってデバイスの ESM_IN 入力へ供給されるレベル信号または PWM 信号を監視するマイコン エラー信号モニタ (MCU ESM)。
- 内部発振器のクロック監視 (システム クロックおよび低消費電力クロック)
- 不揮発性メモリ (NVM) の CRC。
- 構成レジスタの CRC。
- SPI 通信の CRC。
- マイコンからのデバイス内部のアナログ信号およびデジタル信号へのアクセスを可能にする診断出力ピン。
- マイコンおよびシステムのリセット出力 (NRST)
- パワー グッド出力 (PGOOD)。
- 割り込み出力 (NINT)。
- 検出された故障時の電力段や他のシステム機能を停止する安全出力。– 専用 SAFE_OUT1 出力 – 多重化および構成可能な SAFE_OUT2 (多重化オン)。
- 起動時にデバイスの機能をチェックし、動作中にはソフトウェアのコマンドによって実行可能な内蔵セルフテスト (BIST)。
- これらの包括的な安全メカニズムにより、電力管理システムは広範な潜在的故障を検出して対処することが可能となり、複雑な故障シナリオ下においてもシステムの安全性が維持されます。TPS65386x-Q1 は、マイコンの監視機能、独立した故障応答機能、包括的な自己診断機能を組み合わせているため、トラクション インバータ アプリケーションで高い車載安全性インテグリティレベルを実現する上で重要な構成要素となります。

3.5.5 位置センサ

誘導性センサ技術は、トラクション インバータ モーターに最適な位置検出ソリューションとして普及が進んでおり、従来型のリゾルバに比べて、コスト、重量、高速検出能力の点で大きな利点を実現します。LDC5072/3-Q1 は、トラクション モーター アプリケーション向けの誘導性リゾルバ アナログ フロント エンドであり、これらの利点を実現すると同時に、厳格な FuSa 要件を満たしています。以前は、デバイスの機能と安全メカニズムがセクション 3.2.1 にも詳細に説明されていました。

TI は、誘導性センサ以外にも、パワー オペアンプ ALM2403/4-Q1 で設計された 2 次フィルタを使用したリゾルバ励起ソリューションも提供しています。図 3-22 に、この実装のブロック図を示します。この革新的なアプローチにより、マイコンが生成した SPWM 信号を 10kHz ~ 20kHz の基本周波数で変換し、リゾルバ励起に適したクリーンな正弦波に変換でき、適切な電圧と電流をサポートできます。詳細な設計情報については、TI のアプリケーション ノート:『ALM2403-Q1 シングル チップ レゾルバ ソリューションの適用によるシステム コストの削減』を参照してください。

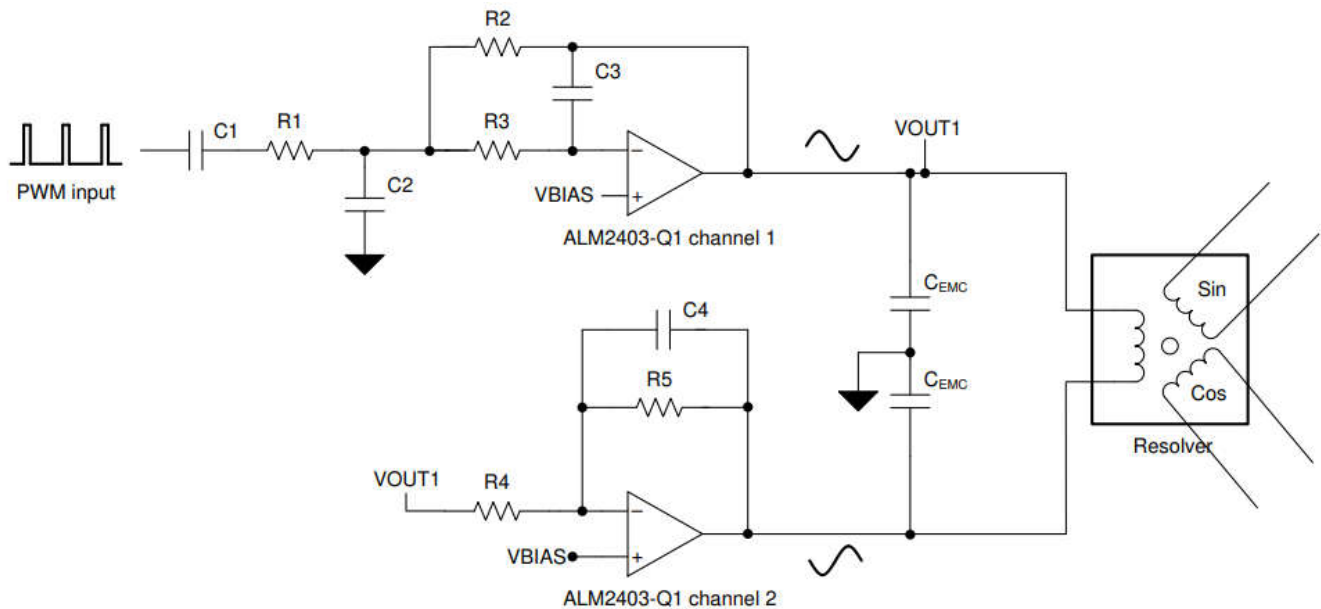


図 3-22. リゾルバ励起向けの ALM2403-Q1 をベースとする 2 次フィルタ設計

3.5.6 電流センサ

トラクション インバータ システムでは、閉ループ モータ速度およびトルク制御、過電流保護の両方にとって、モータの位相電流検出が非常に重要です。TMCS2100-Q1 は、非接触型コアレス ホール効果電流センサとしてのアプローチを表しています。フェライト材料が必要な従来型の電流センサやデバイスをバスバーに挿入するセンサとは異なり、TMCS2100-Q1 は 3 相バスバーの上に配置されたトラクション インバータ制御ボードに単純に取り付け、位相電流によって誘導される磁界を測定できます。この実装の柔軟性により、複雑な機械設計上の考慮事項が不要になり、治具や製造プロセスに関連するコストが削減されます。

TMCS2100-Q1 は、内部アルゴリズムと特性評価プロセスにより、ターゲット バスバーによって誘導される磁界を選択的に検出しながら、隣接するバスバーによって生じる影響を効果的に無視できます。この機能により、隣接するバスバー間の距離をわずか 5mm に短縮できるため、システム全体のサイズを縮小することが可能となります。図 3-23 に、この実装を図示した動作時のブロック図を示します。

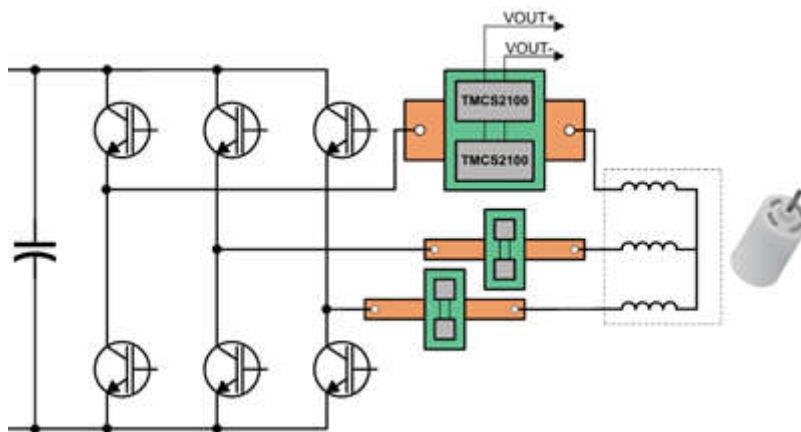


図 3-23. 3 相 AC 電流を測定する TMC52100-Q1 のブロック図

FuSa 設計では、FuSa 目標を達成するために、いくつかのシステム レベル安全メカニズムを実装できます。

- 妥当性チェック

3 相モーター制御システムでは、理論的には $I_a + I_b + I_c = 0$ という原理により、必要な電流検出信号は 2 つのみです。第 3 相の電流センサを追加することで、ソフトウェアの妥当性チェックが可能になり、効果的な安全性メカニズムとして機能します。安全分解を用いることで、各デバイスに ASIL B を割り当てつつ、システムレベルで ASIL D 準拠を達成すること、または位相 A および B に QM 定格を割り当て、位相 C に ASIL D 定格を割り当てることが可能です。

- 電流検出範囲の検出

TMC52100-Q1 の出力がフルスケール スレッショルドを超えると、これは実際の過電流状態またはセンサ出力のドリフト/誤差のいずれかを示している可能性があります。電流検出範囲の検出機能を実装することで、この故障モードに対処し、適切な安全状態遷移をトリガすることができます。これは約 60% のカバレッジを達成するのに役立ちます。

- 電流センサ出力点検のためのトルク計算

クロス検証のために、2 つの独立したトルク計算方法を実装できます。最初の手法は電力とモーター速度を使用してトルクを計算し、2 番目の手法は 3 相電流とモーターのパラメータを使用して直接トルクを計算します。これら 2 つの計算値を比較することで、電流検出精度を検証できます。

- 他の DC 電流検出を使用

インバータの DC 入力電流を測定する追加の DC 電流センサを使用して 3 相電流を再構築でき、AC 電流の測定値を検証するための別のリファレンスとして使用できます。

コアレス ホール ベースの電流検出に加えて、シャント方式の電流検出はトラクション インバータ アプリケーションでも広く使われています。このアプローチでは、各バスバーに高精度シャント抵抗を配置し、電流測定用の外部絶縁型オペアンプに接続します。AMC3302-Q1 は、絶縁型電源を内蔵した絶縁型オペアンプであり、外部の絶縁型電源は不要です。図 3-24 に、AMC3302-Q1 のブロック図を示します。また、TI は、内部電源を使用せずにシングル/差動/変調出力モードを備えたシャント ベースの電流検出用の通常絶縁型アンプ (AMC030x-Q1) も提供しています。シャント抵抗をバスバーに挿入するほか、この抵抗をパワー モジュールに統合することもでき、コスト、熱管理、設計サイズの改善を実現できます。

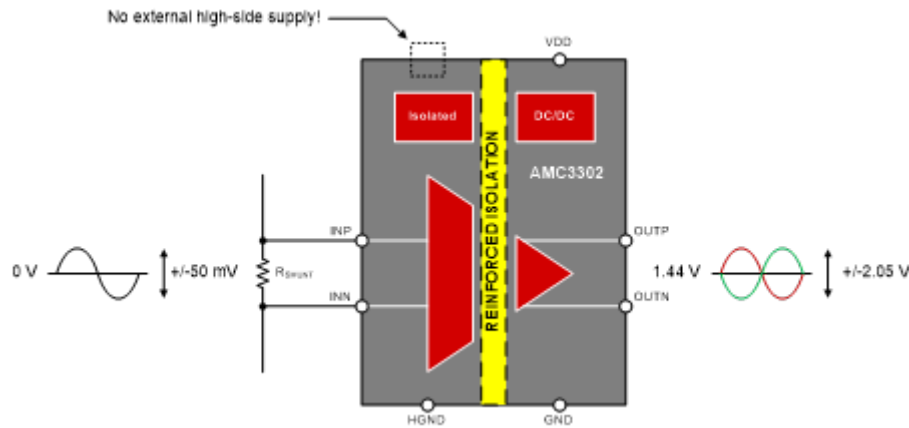


図 3-24. シャント ベース電流検出の AMC3302-Q1 のブロック図

3.5.7 電圧センサ

DC 電圧検出は、トラクション インバータシステムにとって重要な役割を果たし、弱め界磁制御や OV/UV 保護のサポートなどの制御方式を含め、複数の重要な機能を実現します。また、高精度な電圧検出は、閉ループ制御によるアクティブ放電管理および電力トルクの計算において不可欠です。絶縁型アンプの設計は、トラクション インバータ アプリケーションでの電圧検出を行うための最も一般的なアプローチを表します。これらのデバイスは、異なる同相電圧レベルで動作するシステム部品を実質的に分離する絶縁バリアを内蔵しています。この絶縁は、低電圧制御回路を高電圧 DC バスから保護し、電気的な損傷を防止し、オペレータの安全を検証するために不可欠です。絶縁型アンプは、高精度の電圧測定を行うと同時に、高電圧の車載アプリケーションで必要とされるガルバニック絶縁を維持します。または、高抵抗のパスを使用して絶縁バリアを実装することもでき、非絶縁型電圧検出設計と呼ばれるものを作成します。

3.5.7.1 絶縁型 DC 電圧検出

AMC0311-Q1 は、磁気干渉に対して高い耐性を持つ容量性絶縁バリアによって入力回路から出力が絶縁された高精度の絶縁型アンプであり、シングルエンド出力タイプと差動出力タイプの両方が用意されています。このハイインピーダンス入力は、ハイインピーダンスの抵抗分圧回路、またはその他のハイインピーダンス電圧信号源への接続に最適化されています。優れた DC 精度と低い温度ドリフトにより、閉ループシステムでの高精度の絶縁電圧検出と制御をサポートします。図 3-25 に、AMC0311-Q1 DC 電圧検出設計のブロック図を示します。

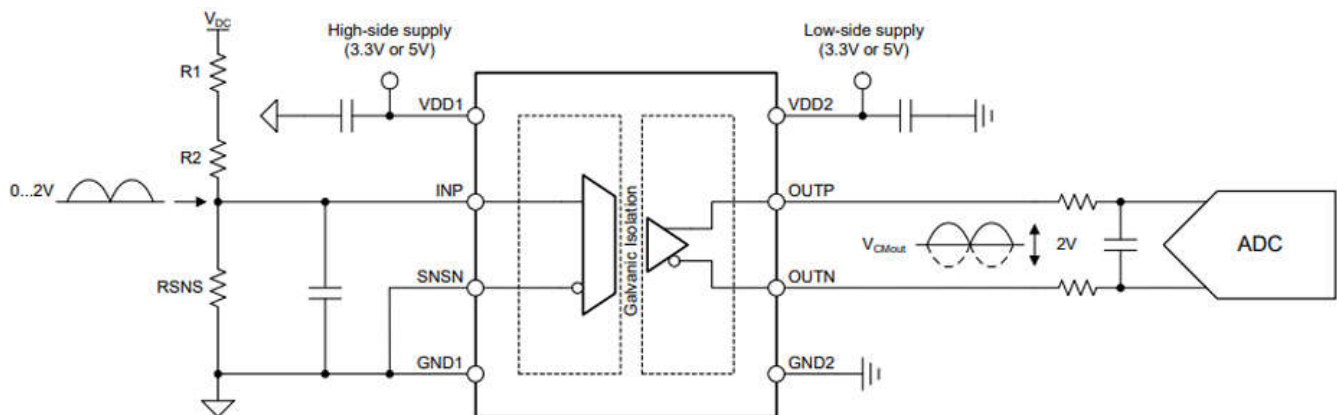


図 3-25. 絶縁型 DC 電圧検出用の AMC0311-Q1 のブロック図

FuSa の要件を満たすために、トラクション インバータの設計では、通常、発生する可能性のある共通原因故障を回避するために、さまざまな技術を使用した冗長 DC 電圧検出パスが実装されています。図 3-26 に、代表的なデュアル チャネル電圧検出の実装を示します。

- **チャンネル 1:** 抵抗ラダー、AMC0311-Q1 絶縁型アンプ、信号変換用のマイコン ADC を用いた従来型のアプローチを採用

- **チャンネル 2: RES60A-Q1** (12.5MΩ の高抵抗ラダー内蔵デバイス)、UCC5881-Q1 に内蔵された ADC、処理用に eCAP、シグマ デルタ フィルタ モジュール (SDFM) または SPI を搭載したマイコン GPIO を使用する異なる技術スタックを採用
- 2 つの電圧検出結果を互いにクロスチェックし、冗長測定検証を行い、システム全体の FuSa を向上させます。

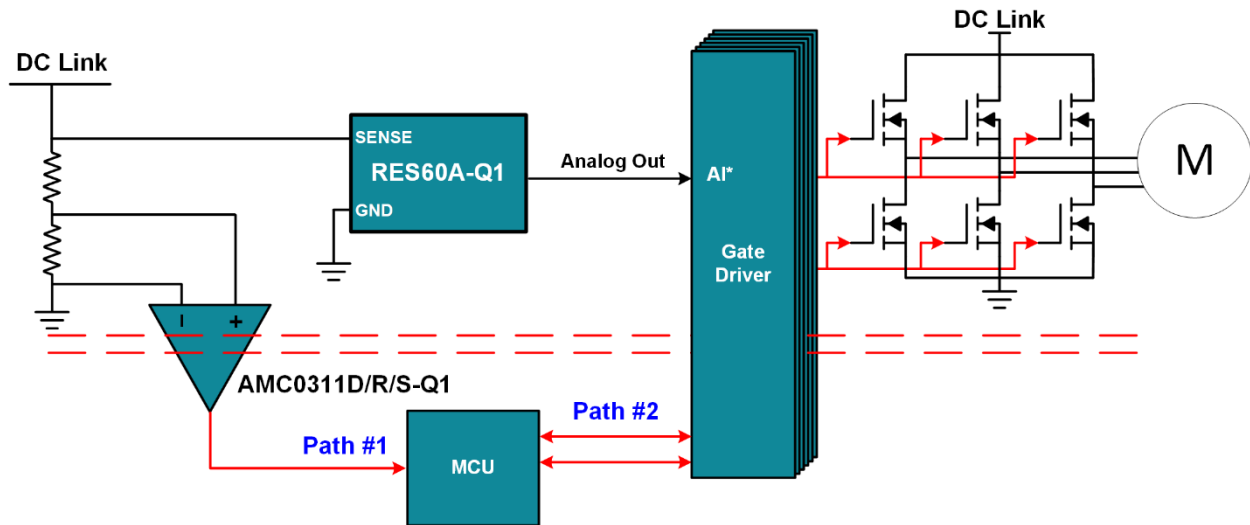


図 3-26. FuSa における技術が異なる 2 チャンネル DC 電圧検出

従来型の AMC0311-Q1 絶縁型アンプに加えて、TI は電圧検出用にいくつかの高度な統合設計も提供しています。

- **AMC038x-Q1** は、抵抗ラダーをデバイスに統合しているため、HV 検出に必要な PCB 面積を大幅に削減でき、従来型の抵抗ラダー設計よりもはるかに高い降圧精度を実現します。
- **AMC3311-Q1** は、絶縁型 DC/DC コンバータをデバイスに統合しているため、ハイスайд回路に電力を供給するための外部絶縁型電源は不要です。こうした高度な統合により、部品点数の低減、設計の簡素化、信頼性の向上を実現できます。
- **AMC23C1x-Q1** は、絶縁型コンパレータとして機能し、OV/UV 信号を高電圧側からマイコンに直接提供します。これにより、1 次側 DC 電圧検出回路から分離された独立監視パスが作成され、より高い FuSa 要件を持つ設計に対応できます。

3.5.7.2 非絶縁型 DC 電圧検出

絶縁バリアによるアプローチ以外に、DC 電圧検出アプリケーションでハイ インピーダンス パスを効果的に使用して絶縁を実現することもできます。高抵抗の入力抵抗を備えた差動オペアンプは、この非絶縁型検出手法における典型的なトポロジを表します。INA160-Q1 および TPS371K-Q1 は、CMRR 高精度 DC 電圧検出に適した非常に高い入力インピーダンスを実現する統合型差動オペアンプです。この高い入力インピーダンスにより、安全な動作を維持しながら高電圧バッテリーに直接接続できます。容量性絶縁バリアや磁気式絶縁バリアのような絶縁部品が不要になるため、これはコスト効率の優れたソリューションです。

3.5.8 温度センサ

トラクション インバータ システムでは、温度センシングは過熱保護と、低下した動作モードに関するアダプティブドライビング戦略の管理において重要な役割を果たします。TMP61-Q1 は、正の温度係数 (PTC) を持つ TI シリコン ベース サーミスタです。TMP61-Q1 は、動作範囲全体にわたって優れた直線性と一貫した感度を提供し、シンプルかつ高精度な温度変換手法を可能にします。高い直線性により、ソフトウェアで区分的な近似やルックアップ テーブルを使用することなく、温度を算出できます。本センサは、25°C において 6400ppm/°C の抵抗温度係数 (TCR) を持ち、温度範囲全体にわたって典型値でわずか 0.2% の TCR 公差により、一貫した感度を維持します。図 3-27 に、標準抵抗と周囲温度との関係を示します。

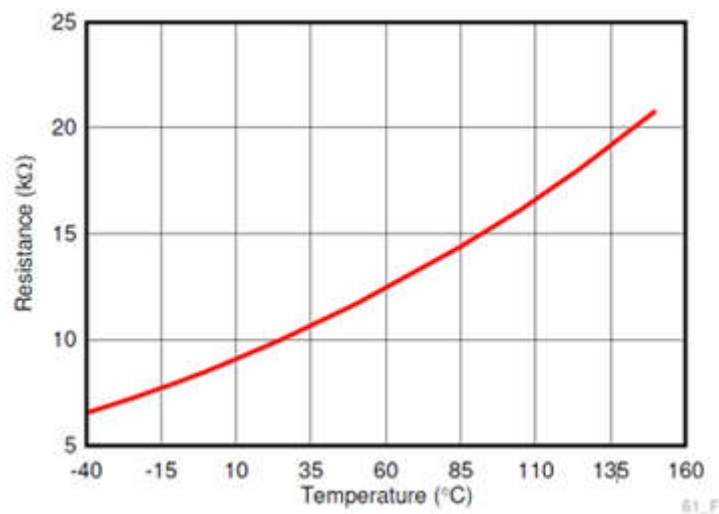


図 3-27. TMP61-Q1 PTC 抵抗と温度との関係

TMP61-Q1 は、ゲートドライバの ADC ピンに直接接続できます。前述の UCC5881-Q1 など、多くのゲートドライバは、TMP61-Q1 の両端に測定電圧を生成するために特別に設計された定電流源を内蔵しています。6 つのゲートドライバで利用可能な複数の ADC チャンネルを利用することで、システムはさまざまな場所にあるパワー モジュールの温度を監視できます。また、FuSa 要件の冗長測定としても使用できます。

4 まとめ

このホワイトペーパーでは、ISO26262:2018 規格に準拠したトラクション インバータ システムに FuSa を実装するための包括的なアプローチを提示します。[セクション 1](#) では、トラクション インバータにおける FuSa の基本的な重要性を示し、故障がどのように危険な状況につながる可能性があるかを説明するほか、安全重視の車載システムに必要な V モデル開発プロセスをご紹介します。[セクション 2](#) では、FTA と FMEA を通じた安全要件の体系的な導出方法を示し、トラクション インバータに関する具体的な安全目標と安全状態を確立すると同時に、概要レベルの安全目標から詳細な技術的安全要件に至るまでの進行状況を示します。[セクション 3](#) では、TI の FuSa 製品ラインアップを使用した実用的な実装戦略を示します。具体的には、マイコン、スマート ゲートドライバ、位置センサ、パワー マネージメント IC などの各種部品などと連携して、障害を検出し、適切な安全状態への移行を実現する堅牢な安全性アーキテクチャの構築について説明します。このドキュメントは、所定の安全指標を満たす FuSa 準拠のトラクション インバータ システムを設計・開発するために必要となる情報やリソースをシステム設計者に提供することを目的としています。

5 参考資料

1. TÜV SÜD、[ISO 26262 規格の理解: 知っておくべきこと | TÜV SÜD](#)、Web ページ。
2. テキサス・インスツルメンツ、[『IEC 62380 と SN 29500 に基づく FuSa FIT ベース故障率推定の理解 \(改訂 A\)』](#)、テクニカル ホワイトペーパー。
3. テキサス・インスツルメンツ、[『車載および産業用における FuSa 認証の効率化』](#)、機能安全マニュアル。
4. テキサス・インスツルメンツ、[『オンボード チャージャ システムの FuSa コンセプト』](#)、アプリケーション ノート
5. テキサス・インスツルメンツ、[『車載、大電力、高性能 SiC トラクション インバータのリファレンス デザイン』](#)、設計ガイド。
6. テキサス・インスツルメンツ、[『HEV および EV トラクション インバータ用の絶縁型バイアス電源アーキテクチャ』](#)、テクニカル ホワイト ペーパー。
7. テキサス・インスツルメンツ、[『車両 FuSa と、TI が高精度の位置センサで顧客を支援する方法』](#)、テクニカル ホワイトペーパー

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みいかなる保証も、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、TI は一切の責任を拒否します。

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](https://www.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。

Copyright © 2026, Texas Instruments Incorporated

最終更新日：2025 年 10 月