Application Note

オンボード チャージャにおける機能安全への取り組み：設計手法と部品の概要

Forest Fu, Sifan You, Harvey Chen, Mingrui Zhu

概要

車載アプリケーションにおいて機能安全 (FuSa) の重要性が高まる中、このドキュメントは、オンボード チャージャ (OBC) システムにおける FuSa 実装についての包括的な導入を提供します。セクション 1 では、背景情報、適用される規格、および TI の機能安全ツールを含む基礎知識を提供します。セクション 2 では、OBC アプリケーション向けの FuSa の一般的な設計原理を検討し、システム設計アプローチの実用的な例を紹介します。セクション 3 では、チップ レベルの安全機能およびシステム レベルの安全メカニズムに焦点を当て、OBC の FuSa 実装における主要な TI 部品を紹介します。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。

免責事項

このドキュメントで示しているシステムレベルの FuSa 解析例および安全メカニズムは、教育目的のみに使用することを意図しています。これらは、有資格のシステム設計者によって行われる適切なエンジニアリング解析や設計判断の代わりとなるものではありません。記載されているすべての安全対策は、有効性を検証するために、特定のシステム設計実装のコンテキスト内でシステム インテグレータによって再評価される必要があります。

目次

商標

すべての商標は、それぞれの所有者に帰属します。

1 はじめに

1.1 背景

電気自動車は、ゼロエミッションや化石燃料への依存低減といった環境面での利点により、近年急速な成長を遂げています。電動化および自動運転技術の進展に伴い、電気自動車における安全性への懸念は一層重要性を増しています。

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確保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。

ISO 26262:2018 は、道路車両における電気および電子 (E/E) システムの機能安全に関する国際規格です。これは、汎用的な IEC 61508:2010 の安全ライフサイクル フレームワークを自動車分野向けに適用したものです。これは、故障が危険な状況につながらないことを確認するための、構造化されたリスクベースのアプローチを提供します。

これらの故障は、系統的故障とランダム ハードウェア故障に分類されます。系統的故障は、ハードウェア設計およびソフトウェア設計の両方に存在し、厳格な開発プロセスや独立した評価によって管理および低減することが可能です。ランダム ハードウェア故障はハードウェアにのみ起因するものであり、完全に排除することはできませんが、安全メカニズムを実装することで検出および防止することが可能です。表 1-1 は、系統的故障とランダム ハードウェア故障の違いをまとめています。

表 1-1. 系統的故障とランダム ハードウェア故障の比較

要素	系統的故障	ランダム ハードウェア故障
定義	設計、仕様、実装、または運用に内在する決定論的な故障であり、特定の条件下で一貫して顕在化します	物理現象、経年劣化、ストレス、または環境要因により、ハードウェアの動作中に予測不能に発生する物理的欠陥または故障
根本原因	たとえば、設計エラー、誤った仕様、実装ミスなどです	例えば、物理的劣化、電気的ストレス、部品の経年劣化などが挙げられます
予測可能性	決定論的で再現性があり、原因を特定することで排除および恒久的な修正が可能です	確率的かつ統計的に発生する故障であり、排除することはできず、再現性もありません
目標	リリース前に欠陥を除去します。	故障が発生したときに故障を検出して軽減します。
測定値	ライフサイクル全体にわたる、機能安全マネジメント、開発、試験、検証および妥当性確認の活動。	安全メカニズムの設計と検証。
代表的な指標	未対応の安全要求事項の数、レビューの網羅率、およびツールの信頼度レベル。	故障率、診断範囲。

系統的故障は、高品質な開発プロセスを確保することで防止および排除が可能であるため、本稿ではランダム ハードウェア故障の解析に焦点を当てます。ハードウェア指標として、単一故障メトリクス (SPFM)、潜在故障メトリクス (LFM)、およびランダム ハードウェア故障の確率的メトリクス (PMHF) が定義されており、ランダム ハードウェア故障を定量的に評価し、自動車の安全度水準要件への適合性を判断するために用いられます。

自動車安全度水準 (ASIL) は ASIL A から ASIL D までの段階に分類されており、ASIL D が最も厳格な水準です。表 1-2 に、ISO 26262 に従って各 ASIL レベルに関連付けられるランダム ハードウェア故障指標の許容値を示します。

表 1-2. ISO 26262 によるハードウェア故障指標

ASIL レベル	SPFM	LFM	PMHF (単位:FIT (Failures in Time))
ASIL-A	関係ない	関係ない	関係ない
ASIL-B	90% 以上	60% 以上	≤ 100 FIT
ASIL-C	97% 以上	80% 以上	≤ 100 FIT
ASIL-D	99% 以上	90% 以上	≤ 10 FIT

1.2 HW/SW FuSa 分析プロセス

ISO26262:2018 は、初期のリスク評価から設計、実装、製造、フィールド運用に至るまで、車両のライフサイクル全体を通じて安全目標が達成され、文書化されるようにメーカーを導きます。図 1-1 は以下に準拠した一般的な HW/SW 安全分析プロセスです。ISO26262: 2018. [1]

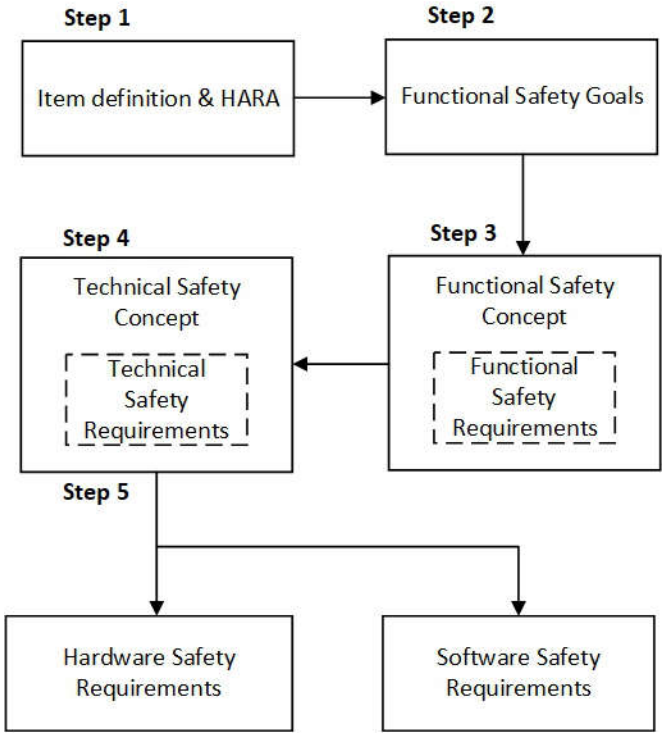

図 1-1. SW/HW 要件の開発

1.2.1 アイテムの定義

FuSa デザインの最初のステップは、アイテムの定義です。アイテムとは、機能安全解析の対象となる、車両の最上位機能またはサブシステムのことです。アイテムの定義の目的は次のとおりです:

- アイテムを定義し、その内容、環境および他のアイテムへの依存関係、ならびにそれらとの相互作用を記述します。
- 後続フェーズの活動を実施できるよう、アイテムについて十分な理解を得ることを目的とします。

このステップでは、ハザード分析およびリスク評価 (HARA) を実施しますが、これは、特定された機能ハザードを定量化された自動車安全度水準 (ASIL) およびそれに対応する安全目標へと変換する体系的な手法です。HARA プロセスは、アイテムの定義との明確なトレーサビリティを確立するとともに、その後のすべての安全活動に対するリスクベースの基盤を提供します。HARA の主な目的は次のとおりです:

- アイテムから発生する可能性のある危険なイベントをすべて特定します。
- 各ハザードの重大度、曝露確率、制御可能性の要因を詳細に分析することによって、厳密なリスク評価を行います。
- 評価結果に基づいて、適切な ASIL 分類を割り当てます。

ハザードの特定は、故障モード影響解析 (FMEA)、ハザードと運用性の分析 (HAZOP) といった手法や、過去の品質問題から得られた教訓を用いて実施できます。次に、特定された危険事象を、重大度 (S)、暴露 (E)、制御可能性 (C) の観点で評価し、ASIL を割り当てます。表 1-3 に示すマトリクスから、各イベントに適切な ASIL を求めることができます。

表 1-3. ISO 26262 に基づく ASIL 定格

重大度	露出	制御可能性		
		C1 (シンプル)	C2 (通常)	C3 (困難、制御不能)
S1 (軽傷および中程度の傷害)	E1 (非常に低い)	QM	QM	QM
	E2 (Low)	QM	QM	QM
	E3 (Medium)	QM	QM	A
	E4 (High)	QM	A	B
S2 (重度および致死的な傷害 - 生存可能性がある)	E1 (非常に低い)	QM	QM	QM
	E2 (Low)	QM	QM	A
	E3 (Medium)	QM	A	B
	E4 (High)	A	B	C
S3 (生命を脅かす傷害 - 致命傷)	E1 (非常に低い)	QM	QM	A
	E2 (Low)	QM	A	B
	E3 (Medium)	A	B	C
	E4 (High)	B	C	D

1.2.2 機能安全目標

2 番目のステップは、FuSa の目標と、危険イベントに対する対応する安全状態を策定することです。FuSa の目標は、HARA 中に特定された危険の発生を防止するために満たす必要がある高度な安全性要件です。これは、部品またはシステムに起こり得るすべての故障モードを網羅的に分析することで導き出されます。すべての FuSa の目標に対して対応する安全状態を定義する必要があり、関連するハザード事象が発生した場合には、システムは必ず安全状態へ遷移する必要があります。

表 1-3 によると、ASIL A ～ D が割り当てられた各ハザードは、少なくとも 1 つの FuSa 目標を要求します。一方、QM に分類されるハザードには安全目標は要求されません。複数のハザードが類似した安全目標に結び付くものの、それぞれ異なる ASIL を持つ場合、それらの中で最も高い ASIL を用いて、単一の安全目標に統合することができます。

1.2.3 機能安全コンセプト

3 番目のステップは、機能安全コンセプト (FSC) を開発することです。FSC は、車両機能またはサブシステムが許容可能な安全レベルをどのように達成するかを、リスクに基づいて高レベルで記述するものであり、FuSa の目標と安全メカニズムの具体的な設計とを結ぶ橋渡しの役割を果たします。FSC の目的は次のとおりです:

- 機能安全要件 (FSR) を導き出します。
- 各 FSR を、該当するサブシステム、またはアーキテクチャに追加すべき外部の安全対策へ割り当てます。

安全目標の属性である ASIL は、後続する各安全要求に継承されます。単一の FSR を直接満たすことが困難な場合、ISO 26262 では、十分に独立した設計要素に分散させた複数の冗長 FSR に ASIL を分解することが認められています。この分解では通常、要求を主機能要素と外部対策要素との間に割り当てます。外部対策要素には、冗長化の実装、監視回路、故障検出システムといった追加の安全メカニズムが含まれます。

ASIL 分解が適用された場合、この活動は、表 1-4 に示すように、ISO 26262-9 に従って許可された ASIL 分解スキーマに従うものとします。

表 1-4. ASIL 分解方式

分解し	元の要件			
	ASIL D	ASIL C	ASIL B	ASIL A
オプション 1	ASIL B (D) + ASIL B (D)	ASIL A (C) + ASIL B (C)	ASIL A (B) + ASIL A (B)	QM (A) + ASIL A (A)
オプション 2	ASIL A (D) + ASIL C (D)	QM (C) + ASIL C (C)	QM (B) + ASIL B (B)	-
オプション 3	QM (D) + ASIL D (D)	-	-	-

各 FSR について、故障許容時間間隔 (FTTI) も指定する必要があります。FTTI とは、故障が発生してから、許容できないハザードが生じる前にシステムが安全状態に到達しなければならない最大時間のことです。

1.2.4 技術的安全コンセプト

4 番目のステップは、FSC のより詳細な実装レベルの対応物である技術的安全コンセプト (TSC) を策定することです。TSC の目的は次のとおりです:

- 技術的安全要件 (TSR) を導き出します。
- TSR が対応する FSR に準拠していることを実証します。

FSC から TSC に移行するには、FSC で定義されている機能ブロックを具体的な物理アーキテクチャに割り当てる必要があります。言い換えると、TSC は上位レベルの安全目標および FSR を、製品に対する具体的なハードウェアおよびソフトウェアの開発要求へと詳細化するものです。

故障対応時間間隔 (FHTI) は、検出時間と反応時間の両方を含み、図 1-2 に示すように、安全システムが故障に対応するために使用できる合計時間を表します。[2]

- 故障検出時間間隔 (FDTI) : 故障の発生から診断手段による検出までの時間。これは、システムが故障の発生をどれだけ迅速に識別できるかを示します。
- 故障応答時間間隔 (FRTI) : 故障が検出されてから、その故障に対して規定された反応が開始されるまでの時間です。これは、故障を検出した後、システムがどの程度迅速に応答するかを示しています。

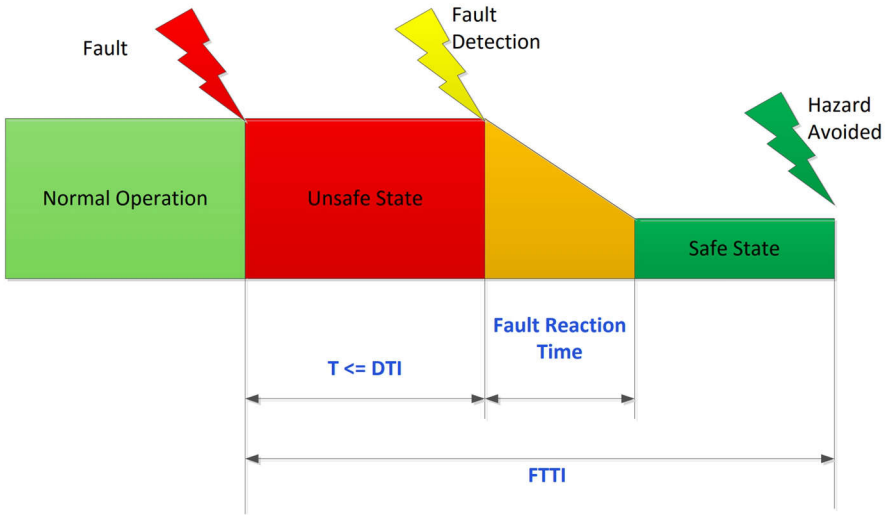

図 1-2. FDTI、FRTI、FTTI の関係

TSR は故障ツリー解析 (FTA) または故障モード効果解析 (FMEA) から取得できます。

- FTA は、望ましくないトップレベル事象から出発し、それを根本原因へと分解していくトップダウン手法であり、重要な故障パスを体系的に把握できます。このトップダウン アプローチは、重大な故障なを体系的に評価するために一般的に実装されます。
- FMEA は、個々の部品を対象に、それぞれの故障モードを特定し、それらの故障がシステム全体に与える影響を評価するボトムアップ手法です。このボトムアップ アプローチは、潜在的な k 故障を評価するために一般的に実装されます。

1.2.5 HW/SW の安全性要件

5 番目のステップは、ハードウェア安全性要件 (HSR) とソフトウェア安全性要件 (SSR) の仕様を導き出すことです。両方の要求セットは、元の機能安全要求からトレーサブルであり、同一の ASIL を引き継ぎ、合わせて具体的かつ検証可能な安全機能を構成します。

HSR は、ハードウェア要素に割り当てられた FSR を満たすためにハードウェア要素がどのように動作するかを指定する TSR です。これは、TSC において、FSR を FTA、FMEDA、または FMEA で解析することによって得られます。HSR は常に単一の FSR にトレースされ、ASIL を継承します。

SSR とは、割り当てられた FSR を満たすために、ソフトウェア ユニットが満たすべき動作、品質、および検証基準を定義する TSR のことです。これは、TSC において、各 FSR をソフトウェア機能に割り当て、その後に想定されるソフトウェア故障モードを分析することで得られます。SSR は、関連する FSR の ASIL を継承します。

ハードウェア ソフトウェア インターフェイス (HSI) は、ハードウェアとソフトウェアの境界を越えた情報を指定する、安全に重要な接続のセットです。HSI は TSC で導入され、その後 HSR および SSR に実装されます。これは、ハードウェアとソフトウェアの境界が明確で、決定論的であり、かつ独立して検証可能であることを示す上で重要です。

1.2.6 依存故障分析

依存故障分析 (DFA) は、本来独立しているはずのシステムや部品間の依存関係によって発生する故障を特定し、低減するための体系的な手法であり、カスケード故障 (CF) や共通原因故障を含みます。(CCF)。

- CF とは、ある部品の故障が別の部品の故障を引き起こし、かつ両方の故障が同一の根本原因に起因するものです。CF は故障ツリーで AND ゲートとして表されます。
- CCF は、2 つ以上の安全関連項目を同時に無効にする単一の根本原因です。

DFA は、FuSa の設計全体に適用されます。これはコンセプト フェーズで実施され、その後、システム、ハードウェア、ソフトウェアの開発を通じて段階的に洗練されていきます。DFA の目的は次のとおりです:

- 設計において、要求される独立性、または干渉からの自由が十分に達成されていることを確認します。
- 潜在的な依存故障に対する安全対策を定義します。

1.3 TI の関連資料

1.3.1 TI 部品カテゴリ

システム レベルの機能安全解析および適合プロセスを実施する最終的な責任はシステム インテグレータにありますが、成功のためには適切な部品を選定することが不可欠です。テキサス インスツルメンツは、これらの製品を明確な機能安全カテゴリに編成することで、このタスクを簡素化します。

図 1-3 に示すように、TI の製品は、機能安全対応、機能安全品質管理対応、または 機能安全適合に分類されており、安全上重要な設計に適した製品をエンジニアが容易に特定できるようになっています。

- 機能安全対応製品
  - TI の標準的な品質管理開発フローを用いて開発された、比較的シンプルな IC です。
  - 内部監視や診断のような安全機能は、必ずしも統合されているとは限りません。
  - TI では、FuSa FIT レートの計算、FMD、ピン FMA を提供しています。
- 機能安全品質管理製品:
  - 内部診断機能を備えた複雑な製品。
  - TI の標準的な品質管理開発フローを用いて開発されています。
  - 包括的な資料セット:FMEDA 分析、FuSa マニュアル。
- 機能安全準拠製品:
  - それ自体が独立したシステムとなり得る、最も複雑な製品です。
  - ISO 26262 に規定されている認証済み FuSa 開発フローに従って開発済み:2018.
  - その他の包括的な資料:故障ツリー解析、FuSa 製品証明書。

		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
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***			✓

図 1-3. FuSa 設計における TI 製品の分類

** *アナログ電源製品とシグナル チェーン製品のみで利用可能です。*

*** *選択された一部の製品で利用可能です。*

機能安全マニュアル [3] は、安全機能について説明し、必要な故障範囲と診断機能を得るために外部部品を使用する方法を示しています。前述した TI の標準的な品質管理開発フローは、体系的故障とランダム故障の両方を扱うための、当社のプロセスです。このプロセスの詳細については、[3] を参照してください。

1.3.2 安全マイコンの FuSa 関連資料

TI C2000™ リアルタイム マイコンは、TÜV SÜD により独立して評価し、認証されており、ASIL D までの体系的能力を満たすとともに、機能安全を必要とする車載アプリケーションの構築を支援します。図 1-3 に示す機能安全準拠に関する資料に加えて、FuSa の設計の効率化と迅速化を実現するためのより多くの資料とソフトウェア ライブラリを提供しています。C2000 の安全関連資料は、[4] に記載されています。

- 開発プロセス認証書。QRAS-AP00210 に対する TUV-SUD の認証書。IEC 61508-2 および ISO 26262-5 に準拠した部品向けの FuSa 開発プロセス。
- C2000 安全パッケージ。ご要望に応じて提供します (NDA が必要です)。パッケージには、ランダム HW 能力に関する技術レポート、体系的能力に関する技術レポート、FMEDA、デバイス コンセプト評価、セーフティ解析レポート、ならびにデバイス固有のセルフテスト ライブラリ パッケージが含まれます。
- ソフトウェア診断ライブラリ。安全機能および安全メカニズムを示すモジュールやサンプルのライブラリです。CPU、メモリ、クロック、ウォッチドッグ、HWBIST、など。
- FuSa フラッシュ API。ライブラリは C2000Ware で提供されています。追加のコンプライアンス サポート パッケージについては、最寄りの TI 担当者までお問い合わせください。
- コンパイラ認証キット。お客様の使用例におけるコンパイラ カバレッジを、TI コンパイラ リリース検証時のカバレッジと比較します。
- 安全認証取得済み RTOS。事前認証済みの安全対応リアルタイム オペレーティング システム。
- MathWorks のシミュレーションとコード生成。IEC 認証キットは、MathWorks のコード生成および検証ツールの適格性を確認するのに役立ち、組込みシステムの認証プロセスを効率化します。

2 OBC システムの FuSa の概念

このセクションでは、オンボード チャージャ (OBC) アプリケーションにおける全体的な FuSa 設計の概要を示し、ISO 26262: 2018 の開発プロセスをシステム レベルでどのように適用できるかを説明します。ここでは、セクション 1.2 で紹介した手順のシーケンスに従って説明します。

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、責任はシステム インテグレータにあります。ここで示す例は、あくまでトレーニング目的のものであり、完成した量産レベルのシステム設計の代替として用いてはなりません。

2.1 アイテムの定義

2.1.1 アイテム関数

アイテムとは、安全ライフ サイクルの対象となる最上位レベルのエンティティを指します。OBC を定義する際には、OBC が何であるか、OBC がどのように機能するか、そして OBC が他の項目とどのように相互作用するかを記載する必要があります。OBC は、自動車規格で定義された性能、安全性、および通信要件を満たしつつ、AC 系統から高電圧 (HV) バッテリを充電するために使用されます。

OBC のアーキテクチャは、数世代にわたって進化してきました:

- 初期の設計では、出力が 3.3kW 以下の単方向コンバータが用いられ、PFC 段としてダイオード整流器とブースト コンバータを使用し、その後に独立した DC-DC 段が配置されていました。
- 次世代では定格出力が 6.6kW に向上し、双方向機能が追加され、トーテムポール PFC 段および双方向 DC-DC コンバータ段が採用されました。図 2-1 には、現在の市場で主流となっているトポロジである、単相デュアル ステージ OBC トポロジ (左) と三相デュアル ステージ OBC トポロジ (右) を示しています。
- 最新のトレンドは単段 OBC トポロジであり、部品点数とコストを削減しつつ、より高い電力密度を実現します。このアーキテクチャでは、PFC 段と DCDC 段を 1 つの高周波変換段に統合しています。単段 OBC トポロジにも、さまざまなバリエーションがあります。図 2-2 は、代表的な 2 種類の単段 OBC トポロジを示しています。左はインターリーブ型トーテムポール単段トポロジで、右は準単段トポロジです。

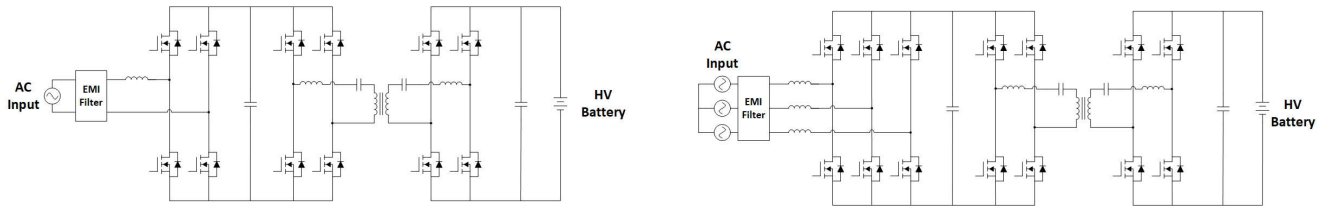

図 2-1. デュアル ステージ OBC のブロック図

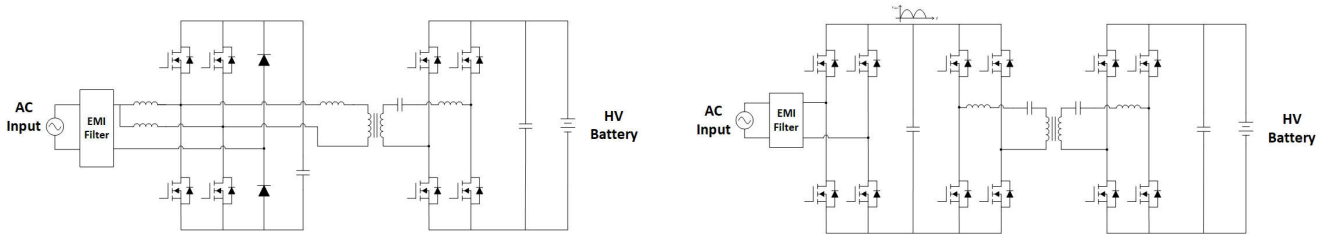

図 2-2. 単段 OBC のブロック図

図 2-2 に示す単段トポロジは市場で大きな関心を集めていますが、現在議論の中心となっている最も代表的な単段トポロジはマトリックス コンバータです。図 2-3 はマトリックス コンバータのブロック 図を示しています。このアプリケーション ノートでは、さらなる FuSa 解析の例としてマトリックス コンバータを取り上げますが、解析内容の大部分は、単相および三相のデュアルステージ トポロジや、他の単段トポロジにも適用可能です。

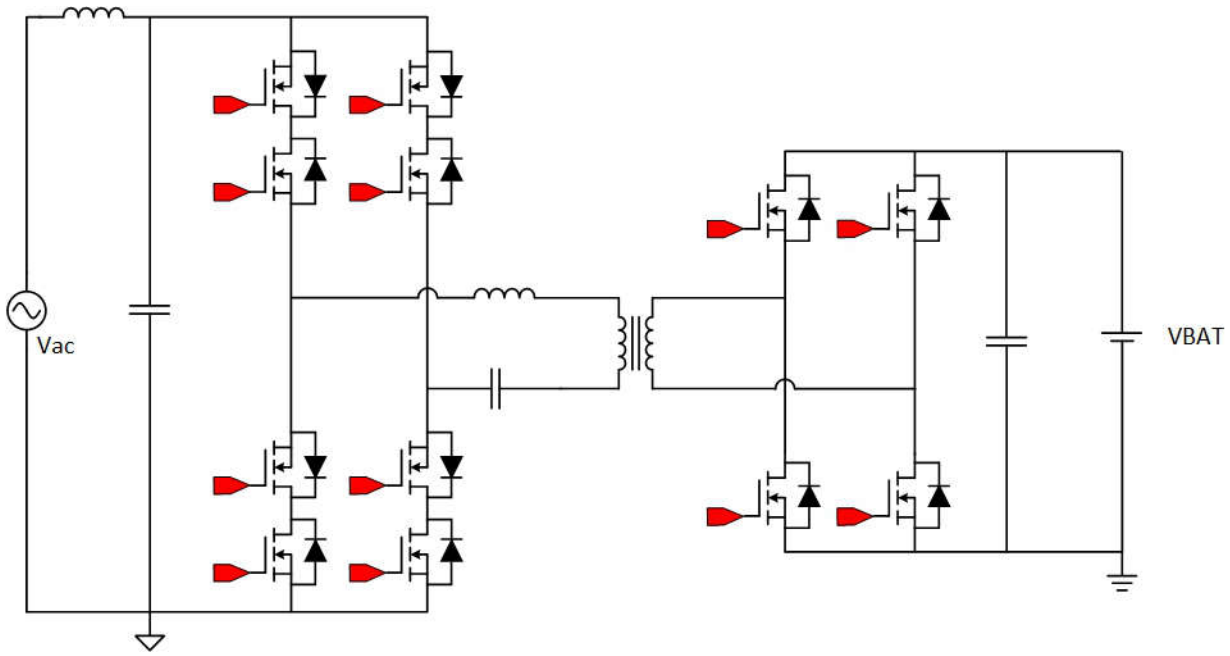

図 2-3. マトリクス コンバータのブロック図

まとめると、OBC は以下の主要な機能を実行します:

- 電力変換:OBC は、充電ステーション、ケーブル、およびバッテリの要件を満たす電力レベルで電力変換を行います。
- 力率補正:OBC は入力電流を正弦波形に整形し、入力電流を系統電圧に同期させるとともに、入力電流の高調波を最小限に抑えます。
- 出力レギュレーション:OBC は、BMS の設定値、温度制限、および充電状態制限に基づいて、バッテリ充電電圧および電流をリアルタイムで制御します。
- 車両から X への電力供給 (V2X):V2X は、OBC が逆方向動作で運転される概念を包括する用語であり、X は通信ネットワークにおけるさまざまな接続先を表します。車両から負荷への電力供給 (V2L) は、車両を移動式電源として外部負荷に電力を供給する仕組みです。自動車からグリッドへの電力供給 (V2G) により、自動車は電力をグリッドに返すことができます。車車間電力供給 (V2V) を使用すると、自動車をモバイル電源として使用して別の車両を充電できます。車両から住宅への電力供給 (V2H) により、停電や高い電力コストが発生したときに電気自動車が家庭に電力を供給できるようになります。
- ガルバニック絶縁: AC 側と HV DC バスの間の絶縁。
- 保護機能:電気的故障、熱的故障、および絶縁故障に対して包括的な保護を提供します。
- 通信:AC インレットでの CC/CP 信号。充電指示、動作モードの選択、および状態報告のために CAN 通信を行います。
- 診断機能:システムの状態を監視し、故障が発生した場合は報告します。

トポロジはマトリックス コンバータであるため、この安全目標に対する FSC には、従来の二段構成 OBC とは異なるいくつかの特徴があります。

- OBC 出力側の過電流は、すべての電力受電側を単純にオフするだけでは対処できません。フリーホイール経路が存在しないため、すべてのパワー スイッチを同時にオフすると、大きな電圧スパイクが発生し、パワー スイッチを損傷する可能性があります。そのため、電源スイッチには洗練された電源オフ シーケンスが必要です。
- AC 側の電流は妥当性チェックとして使用できます。マトリックス コンバータには DC リンク コンデンサが含まれていないため、DC 出力側の過渡電流は AC 側電流に直接反映されます。これに対し、従来の二段構成 OBC では、DC リンク コンデンサが過渡的な DC 電流を供給します。
- 短い FTTI。マトリックス トランス方式のトポロジは、はるかに高いスイッチング周波数で動作するため、一般的に SiC または GaN デバイスの使用が必要となります。従来のシリコン スイッチと比較すると、SiC/GaN トランジスタは大幅に高速な電流保護応答を必要とし、その結果、許容される故障許容時間の間隔は短くなります。

- ゲートドライバについては、バックツーバック構成のパワー スイッチを同時にオン制御する必要があるため、2 チャネル間のインターロック機能を無効化する必要があります。ゲートドライバの UVLO 機能が誤ってトリガーされてはなりません。誤動作すると、フリーホイール経路が失われる問題を引き起こす可能性があります。

2.1.2 システム境界

システム境界は、安全ライフサイクルが実行されるアイテムの正確な範囲を定義します。これにより、安全関連システムに属するすべての要素 (範囲内) と、周囲の車両、インフラ、または環境 (範囲外) とが明確に分離されます。表 2-1 に、システム境界を示します。

表 2-1. アイテム定義のシステム境界

システム境界	適用範囲内	範囲外
電力変換	Matrix Converter 主要なアナログ部品	グリッド側インフラストラクチャ 外部コネクタとヒューズ
通信	AC インレットとの通信 BMS/VCU への CAN 配線	VCU の上位レベルの車両ネットワーク。BMS、電子ロック、高電圧インターロック (HVAC、HVDC)
環境	外気温 クーラント温度	機械部品 (コールド プレート、接地) 、湿度、EMC

2.1.3 外部インターフェイス

HV バッテリ充電の一連のプロセスは、GBT 18487.1-2023 などの複数の規格で定義されています。この章では、HV バッテリ充電システムと、OBC 境界を超える他のシステムとの間のインターフェイスについて説明します。これらのシステムは HARA 分析の入力になります。

システム境界から、表 2-2、表 2-3 および表 2-4 に示すように、インターフェイスは電源インターフェイス、通信インターフェイス、環境インターフェイスにも分割できます。

表 2-2. 電源インターフェイス

電源インターフェイス	コネクタ	目的
AC 入力	ライン、中性、PE	主電源電圧。仕様:85V ～ 265V、50Hz、最大 7kW
HV DC 出力	HV+、HV-	バッテリ パックに対して、制御された DC 充電電圧 (250V ～ 460V) および電流 (標準 22A) を供給します。
電源	KL30	常時バッテリ プラス端子 / 接続。

表 2-3. 通信インターフェイス

通信インターフェイス	コネクタ	目的
AC インレット	CC、CP、充電ガン温度	CP には、プラグイン ステータス、最大電流能力、および車両準備状態を示す 1kHz PWM パイロットが搭載されています。 CC は充電器の準備ができてエラーに使用される低レベルの DC 電流を伝送します。
点火	KL15	スイッチ イグニッション電源ターミナル/接続。
BMS	CAN-H、CAN-L	バッテリ状態、充電制限、および故障コードをやり取りします。
VCU	CAN-H、CAN-L	上位レベルの充電モード コマンド、充電セットポイント コマンド、安全状態要求、診断要求。
テスト ピン	ハードワイヤード、JTAG	製造またはデバッグ時に使用されます。

表 2-4. 環境インターフェイス

環境インターフェイス	コネクタ	目的
熱インターフェイス	クーラント温度、外気温	パワー スイッチ、磁気部品、主要なアナログ部品、およびその他の受動部品に対する熱管理を提供します。クーラント温度:-40℃ ～ 85℃。周囲温度範囲:–40℃ ～ 85℃

2.1.4 動作モード

シングルステージ OBC の動作は、少数の運転モードとして整理されており、これらのモードは車両レベルのコントローラ (VCU/BMS) によって、または故障が検出された場合には内部ロジックによって選択されます。表 2-5 に、シングルステージ OBC の主な動作モードを示します。

表 2-5. シングルステージ OBC の主な動作モード

動作モード	使用事例	ステータス
スタンバイ	通常走行、車両スタンバイ	パワー コンバータが無効です。ウェークアップを待機します。
ディレーティング充電	バッテリ深放電、バッテリ低温、バッテリ高温	電圧と温度に基づいて、充電電流を安全な値に制限します。
AC 充電	標準充電。	バッテリ パックの電圧および電流を、BMS の設定値に合わせて制御します。
再生可能	V2G、V2L、V2V、V2H	パワーステージの操作を逆にします。
メンテナンス	工場出荷時診断、ファームウェア更新	事前定義されたテスト パターンを実行します
緊急	安全上重要な故障が検出され、通信が失われました	電力変換を停止します。故障コードを VCU/BMS に報告します。

これらの動作モードには、お客様ごとに大きく異なる OBC の使用プロファイルも含まれます。これには、充電頻度、一般的な充電時間、特定の充電シナリオ、平均充電電力といった要素が含まれます。サイクル ライフを評価することは、HARA にとって非常に重要です。表 2-6 に、ミッション プロファイルの説明例を示します。

表 2-6. シングルステージ OBC のミッション プロファイルの例

プロファイル	値	根拠
毎日の充電イベント	1.5	家庭での充電と職場での充電。
平均充電時間	6h	夜間充電または労働時間充電の平均値。
平均電力	7kW	単相充電器の一般的な電力
ライフタイム	8 年	車両更新の一般的な頻度
合計サイクル数	4380 サイクル	安全性評価のために 5000 サイクルを丸めました

上記の分析に基づき、図 2-4 は主要な部品およびインターフェイスを含むシステム レベルのブロック図を示しています。

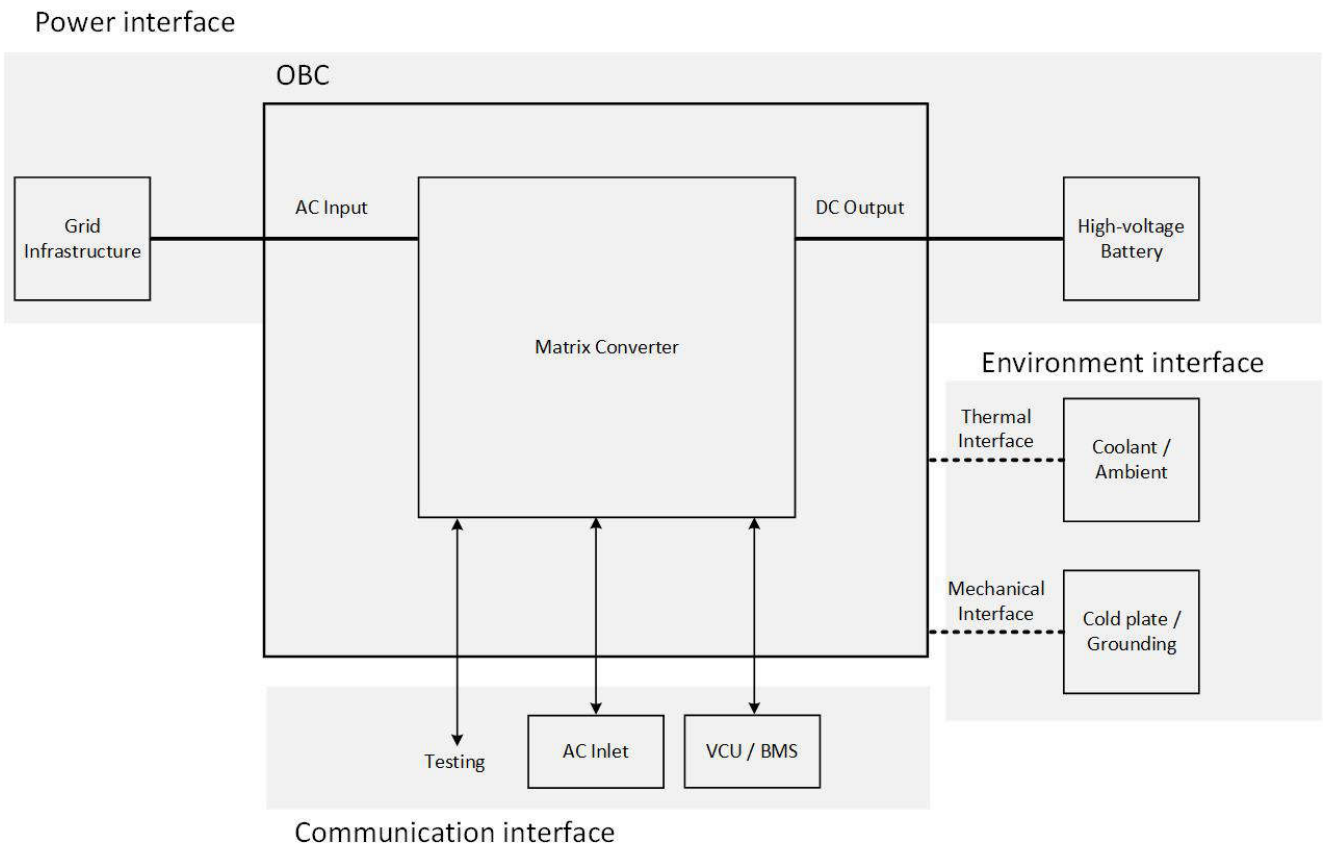

図 2-4. アイテム定義レベルのシステム ブロック図

2.2 機能安全目標

HARA を実施する前に、分析範囲を限定するため、以下の簡略化した前提条件を採用します:

- アイテムの機能 (セクション 2.1.1) :OBC は単段マトリックス コンバータトポロジを採用しており、主要なアイテム機能には、電力変換、電圧制御、ガルバニック絶縁、保護、通信、および診断が含まれます。
- システム境界 (セクション 2.1.2) :この分析の対象は OBC システムのみであり、HV-LV DC-DC コンバータ、PDU、およびその他の電子制御ユニットは対象外とします。
- 外部インターフェイス (セクション 2.1.3) :単一のマイコンが OBC を制御します。このマイコンは OBC の制御に専用で使用され、AC インレットならびに BMS/VCU と接続します。
- 動作モード (セクション 2.1.4) :主な機能は高電圧バッテリを充電することであり、この分析は急速充電動作モードのみに焦点を当てます。

各アイテムの機能、プロセス、および相互作用を定義した後、次のフェーズとして HARA を実施します。すでに設定した前提条件および実施した分析に基づくと、各サブシステムにおける誤った動作は、DC 過電圧、DC バス過電流、熱故障などの潜在的なハザード事象を引き起こす可能性があります。

各ハザードは、以下に基づいて個別に評価する必要があります。ISO 26262: 2018、重要度 (S)、露出 (E)、制御可能性 (C) の基準。例として、熱故障を考えます:

- 重大度:熱故障の最悪の結果は車両火災であり、生命を脅かす、または致命的な傷害を引き起こす可能性があります。その結果、イベントは S3 に割り当てられます。
- 露出:OBC の使用プロファイルにおいて、充電器は車両の全稼働時間のうち中程度の割合で動作します。これは、E3 の露出レーティングに対応しています。
- 制御可能性:充電中は車両が停止しているため、運転者は充電回路に迅速に割り込みができます (例:充電器を切り離す、またはコンタクタを開放する)。したがって、イベントは C2 と見なされます。

表 1-3 によると、S3 - E3 - C2 の組み合わせは ASIL-B に対応するため、熱的故障の危険性は ASIL-B に割り当てられます。

DC バス過電流については、高電圧バッテリの最大充電電流が AC 充電時の電流よりもはるかに大きいため、高電圧バッテリへの重大な影響はありません。しかし、過電流は、短絡により OBC 出力側の電力受電側を過熱させ、故障を引き起こす可能性があります。短絡故障が発生すると、高電圧バッテリによって OBC を介した低インピーダンス経路が形成され、深刻なシステム過熱を引き起こし、極端な場合には車両火災に至る可能性があります。露出レベルと制御可能性レベルは、熱故障と同じです。表 1-3 によると、S3 – E3 – C2 の組み合わせは ASIL-B に対応するため、DC バス過電流の危険性は ASIL-B に割り当てられます。

DC バス過電圧については、OBC 出力側の受電側に過電圧破壊を引き起こす可能性があります。また、過電圧は高電圧バッテリー内のリチウム イオン セルにとっても危険であり、さらにシステム過熱や、最悪の場合には車両火災につながる可能性があります。露出レベルと制御可能性レベルは、熱故障と同じです。表 1-3 によると、S3 - E3 - C2 の組み合わせは ASIL-B に対応するため、DC バス過電圧の危険は ASIL-B に割り当てられます。

すべての危険事象を分析する必要があります。この評価は通常システム インテグレータによって実施されるため、各ハザードの詳細な評価は本資料では示していません。HAZOP はシステムのハザード分析手法であり、7 つのガイド ワードを提供します。表 2-7 に HARA 分析の例を示します。HAZOP のリーディング ワードは、誤動作の挙動を記述するために使用されます。

表 2-7. 単段 OBC の HARA 分析例

ID	異常動作	車両レベルにおける潜在的ハザード	S	E	C	ASIL
H1	予想より発熱が多い	過熱による車両火災	S3	E3	C2	B
H2	要求値を超える DC バス電流	OBC 短絡による車両火災	S3	E3	C2	B
H3	要求値を超える DC バス電圧	OBC 短絡による車両火災	S3	E3	C2	B
H4	電気的干渉の増加	スプリアス制御信号	S1	E3	C2	QM

表 2-7 で ASIL A から ASIL D に危険イベントが発生した場合、少なくとも 1 つの安全目標を特定する必要があります。機能安全目標とは、安全状態の要求を満たすための、高レベルで技術に依存しない記述です。

表 2-8 は FuSa 目標の記載例です。FTTI の値は、ハザード分析と規制要件に基づいて算出する必要があります。SG1 を例に取ると、動作温度は 65°C であり、熱故障の臨界温度は 155°C です。一般的な温度上昇率を毎秒 15°C とすると、臨界温度に達するまでの時間は 6 秒となります。500ms の FTTI は、カスケード故障が発生する前に早期介入を可能とする、早期検出のための保守的な設定です。

表 2-8. 単段 OBC の FuSa 目標の例

ID	安全性の目標	ASIL	安全状態	FTTI
SG1	熱故障による車両火災を回避します。	B	OBC をシャットダウンし、非常運転モードに切り替えます。	ユーザーによって指定されます
SG2	DC バスの過電流による車両の火災を避けます。	B		
SG3	DC バス過電圧による車両火災を回避します。	B		

安全状態の要件は、ハザードが発生した際にトリガされるべきシステム全体の対応を規定します。例えば、SG1 から SG3 に対する安全状態は、OBC を非常運転モードに切り替えることであり、その際の主要な動作を以下に示します。デュアルステージ OBC とは異なり、このアーキテクチャには DC リンク コンデンサが含まれていないため、DC リンク コンデンサの放電に関する動作はありません。

- ゲートドライバを順次無効化します。
- すべてのコンタクタを開きます。
- OBC 出力バスを安全な電圧に放電します。
- 故障状態をログに記録します。

2.3 機能安全コンセプト

FuSa 目標を確立した後、次のフェーズとして FSC を策定します。図 2-5 に、システム ブロック図を示します。これは、項目定義のブロック図よりも 1 レベル深いものです。目的は、予備的なアーキテクチャ図上で、サブ機能要素およびそれらの相互接続を定義することです。

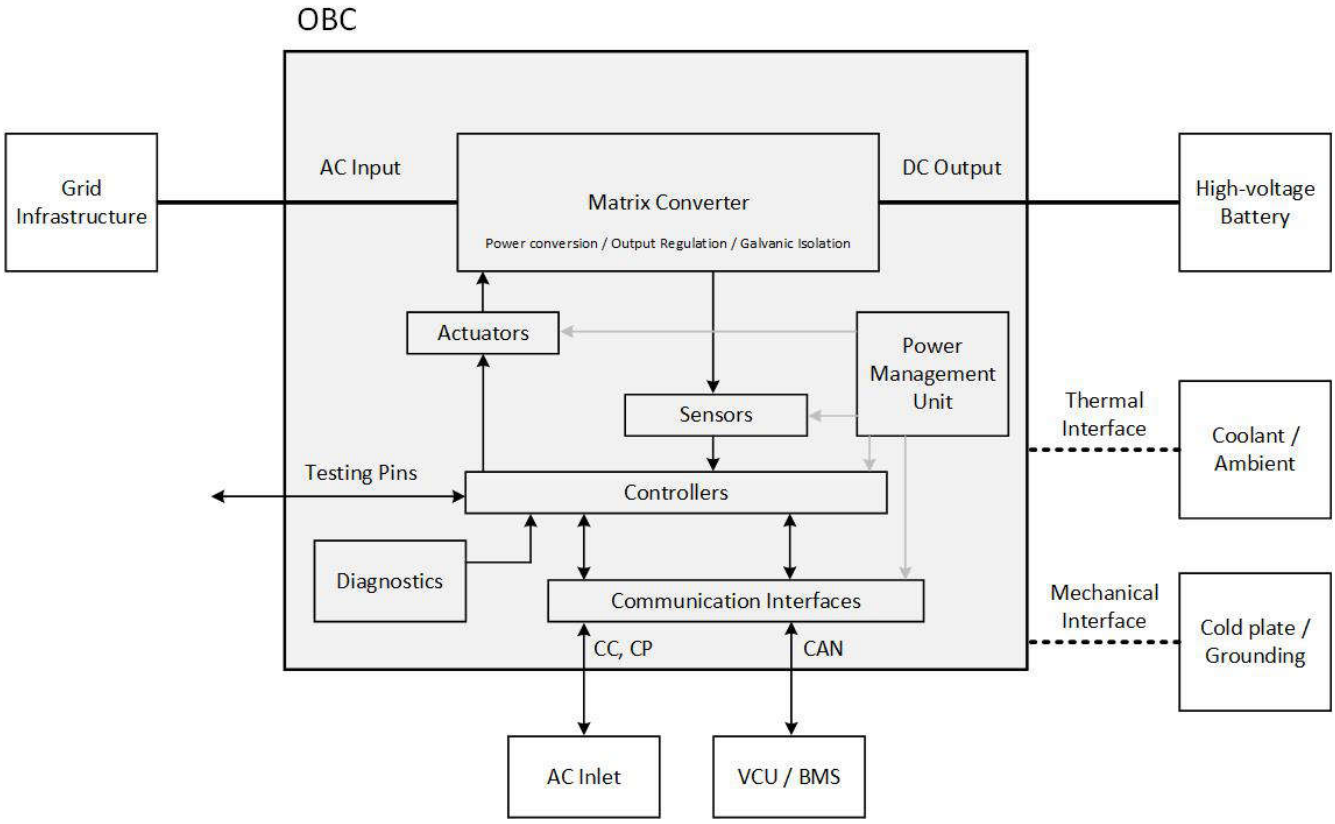

図 2-5. FSR レベルのシステム ブロック図

解析を簡単にするために、例として SG2 を選択します。図 2-6 は SG2 に関連する 1 レベル深いブロック図であり、関連するサブ機能要素と相互作用は表 2-9 で定義されています。

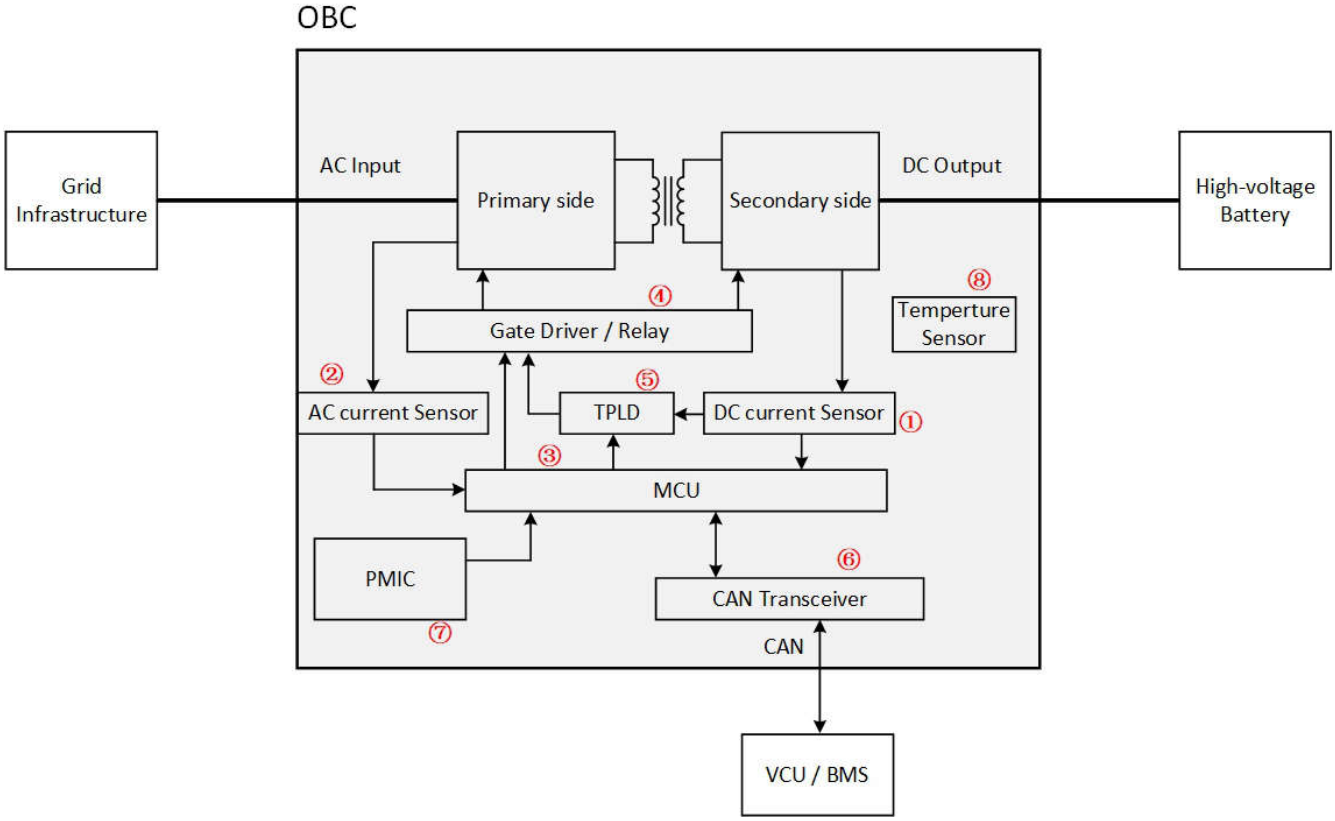

図 2-6. SG2 の FSR レベル システム ブロック図

表 2-9. SG2 のサブ機能要素および相互作用

要素 ID	要素名	説明
E1	DC 出力電流測定回路	定電流制御および過電流保護のために、OBC の出力電流を測定します。
E2	AC 入力電流測定回路	AC 電流制御および過電流保護のために、OBC の入力電流を測定します。
E3	マイコン回路	充電制御アルゴリズムを実行し、センサ データを監視し、PWM 信号を生成するとともに、車両の BMS/VCU と通信します。
E4	ゲートドライバの回路	パワー スイッチに必要な電圧および大電流の駆動信号を提供します。
E5	TPLD 回路	組合せ論理により、パワー スイッチのオフシーケンスを実現するプログラマブル ロジック デバイスです。
E6	CAN トランシーバ回路	BMS/VCU とステータスおよび診断情報を交換します。
E7	PMIC 回路	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。これにより、マイコン向けの外部ウォッチドッグおよびエラー ピン監視も提供されます。
E8	温度測定回路	パワー スイッチのジャンクション温度、トランスの温度、およびコンバータの周囲温度を監視します。

FTA は SG2 の FSR を生成するために実行されます。FTA 分析は 3 つのステップで構成されています。最初のステップでは、SG2 の違反をトップイベントとする故障ツリーを作成します。2 番目のステップでは、トップ イベントの発生につながる、定義された各サブ機能要素の潜在的な誤動作を導出します。3 番目のステップでは、イベント間の関係を表すために論理ゲートを用います。

上記の手順に従って、図 2-7 に FTA ツリーを示します。カットセット解析のために、クリティカルな故障パスを特定する必要があります。SPF が FuSa 目標を直接侵害する場合は、FSR を設計する必要があります。一方、SPF が FuSa 目標

を直接侵害しない場合は、二重点故障システムが許容可能かどうかを判断し、あわせて二重点故障の独立性を分析する必要があります。

SG に対する FTA 解析では、FSR レベルでは部品で解析を打ち切ることができますが、TSR レベルでは、より詳細な解析を実施する必要があります。図 2-7 に示すように、異常な電流検出、制御不良、または電源の問題が発生した場合、SG2 に違反します。その後、異なる成分に分解することができます。

- 電流検出の誤動作は、電流センサの故障、または過電流保護用ディスクリート コンパレータの故障に起因する可能性があります。
- 誤った制御コマンドは、複数の部品によって引き起こされる可能性があります。VCU との通信に起因する可能性があります (誤った充電コマンド、または故障状態の未報告)。マイコンからの制御信号が正しくないことが原因である可能性があります。ゲート ドライバからの不正な駆動波形によって発生する可能性があります。故障反応パス内のディスクリート ロジック部品におけるいずれかの故障によって発生する可能性があります。
- 電源の故障は、マイコン、ゲート ドライバ、センサ、電圧リファレンスなどの主要部品の誤動作を引き起こす可能性があります。

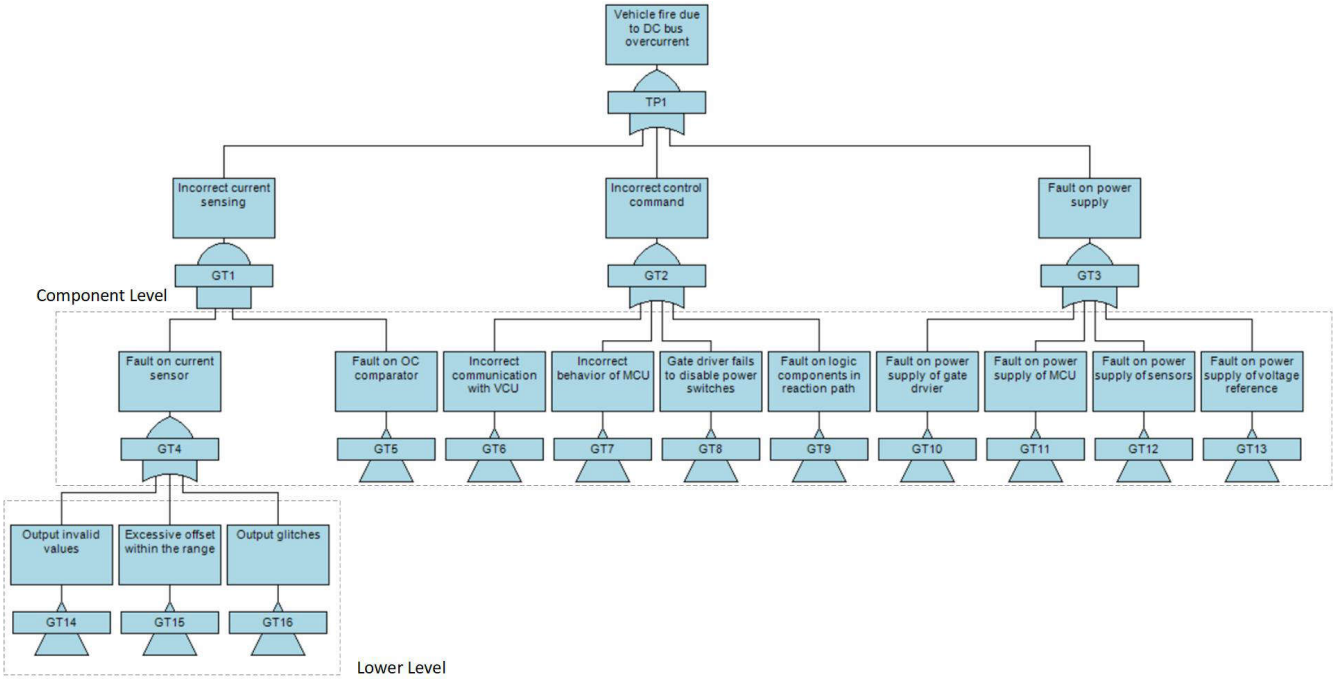

図 2-7. SG2 の FTA ツリー例

カットセットとは、トップ ゲートの条件が失敗する原因となる、ゲート/イベントの組み合わせの集合を特定するための論理解析です。

- 一次カットセット。1 つのイベントのみでトップ イベントが発生します。これらのイベントは、FTTI 要件を持つ FSR に変換されます。
- 二次カットセット。同時に 2 つのイベントが発生すると、上位のイベントが発生する可能性があります。これらのイベントは、MPFHTI 要求を含む FSR に変換されます。
- 二次を超える次数のカットセット。2 つを超えるイベントが同時に発生することで、トップ イベントが発生します。これらのイベントは FSR に変換されません。

各 FSR は、実装を担当する論理ブロックに割り当てる必要があります。FSR が複数のブロックにまたがる場合は、関連するすべてのサブシステムを列挙する必要があります。表 2-10 に、DC バスの過電流による車両の火災を防止する目標を支える FSR の簡潔なセットを示します。

表 2-10. SG2 向け FSR の例

SG2：DC バスの過電流による車両の火災を避けます。					
ID	FSR	安全状態	アロケーション	ASIL	トレース先
FSR 2.1	DC バス電流検出システムは、正確な電流測定を行うものとします。	OC フラグをマイコンにアサートします。	E1 と SW	B	GT4
FSR 2.2	TCAN は、OBC と VCU 間で正しい通信を行うものとします。	OC ステータスを VCU に送信します。	E6 と SW	B	GT6
FSR 2.3	マイコンは、正しい制御方式を実行するものとします。	緊急動作モードに切り替えます。	E3 と SW	B	GT7
FSR 2.4	ゲートドライバは、パワー スイッチを正しく駆動するものとします。	パワー スイッチを無効にします。	E4	B	GT8
FSR 2.5	バイアス電源は、主要な部品に信頼性の高い電圧を供給するものとします。	信頼性の高い電圧レールを提供します。	E7	B	GT3

2.4 技術的安全コンセプト

FSC が確立された後、次の段階として TSC を作成します。TSC は、FSC を具体的な TSR に落とし込みます。TSR を生成するため、FMEA の実施が推奨されます。重要部品については、分析により次の点が確認されています:

- 故障モードは、安全メカニズムによって検出される必要があります。
- 故障検出および安全状態への遷移に要する応答時間は十分です。
- 診断範囲は ASIL 要件を満たしています。

SG2 の TSR レベルのシステム ブロック 図は 図 2-8 に示されており、FSC アーキテクチャより 1 段階深いレベルになります。図 2-8 では、サブ機能要素の設計および相互接続が設計されています。基本的な保護パスは赤で示されています。過電流が発生すると、電流センサからの OC フラグがマイコンに入力されます。OC フラグを検出すると、マイコンは所定のシャットダウン シーケンスを実行し、確実なシャットダウンを確認するために PWM がトリップされます。

FSR ごとに、故障モード、故障の影響および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。故障パスは、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):故障は FuSa 目標を直接的に侵害します。
- デュアル ポイント故障 (DPF) :故障は、別の独立した故障と組み合わさった場合に、FuSa 目標を侵害します。
- 安全故障 (SF) :故障は、検出可能であるか、または本質的に安全であるため、FuSa 目標を侵害することはありません。

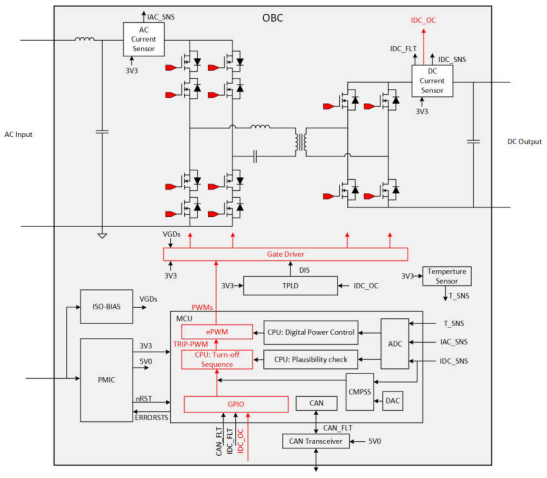

図 2-8. SG2 の TSR レベルのシステム ブロック図

SPF および DPF を含む、FuSa 目標を侵害し得る各故障に対して、安全メカニズムが設計されています。FMEA 表表 2-11 をに示します。

表 2-11. FMEA 表の例

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	故障原因	安全メカニズム
DC 出力電流測定回路 (E1)	OC 検出	OC フラグの誤ったアサート	OC 故障の検出失敗	SPF	OC スレッショルド設定または OC 信号チェーンの故障	マイコンの CMPSS モジュールからの冗長 OC フラグ。
		不適切な電流センス	OC 故障の検出失敗	DPF	VOUT 信号チェーンにおける故障。この場合、前の SM は失敗します	AC 側電流センサによる妥当性チェック
CAN トランシーバ回路 (E6)	故障ステータスの通知	通信エラー	OC 故障を報告できません	SPF	CAN バス故障またはローカル故障	TCAN インジケータフラグ
ゲートドライバ回路 (E4)	パワー スイッチの駆動	パワー スイッチ無効化失敗	DC バスの短絡	SPF	ゲートドライバまたは信号チェーンの故障	カットオフ コンタクタ
マイコン回路 (E3)	制御と保護を実行します	スイッチオフ シーケンスの不一致	電圧ストレスによるパワー スイッチの故障	SPF	CPU による ISR 実行の遅延	ゲートドライバを無効化するための独立した TLPD 回路
マイコン回路 (E3)	制御と保護を実行します	不正なデジタル出力または PWM 信号。	パワー スイッチの電源オフの失敗	DPF	PWM 出力故障	PWM 出力の冗長化、PWM ループバック チェック
マイコン回路 (E3)	制御と保護を実行します	マイコンが制御アルゴリズムを実行できません。	システム故障	SPF	CPU による ISR 実行の遅延	PMIC エラー ピンの監視およびリセット
PMIC 回路 (E7)	電圧電源	電圧誤差	システム故障	SPF	降圧 / LDO 出力エラー	過電圧と低電圧の監視

表 2-11 により、安全メカニズムは一般に、検出メカニズムと制御メカニズムに分類できます。検出メカニズムには、妥当性チェック、冗長センシング、診断テストおよび監視などが含まれますが、これらに限られるものではありません。制御メカニズムには、安全状態への遷移、故障時の反応、警告の生成、システムのシャットダウンなどが含まれますが、これらに限定されません。

SG2 (DC バス過電流による車両火災を回避する) について、システム サブ要素である DC 出力電流測定回路を例として取り上げます。電流測定回路において、電流センサは、過電流を検出した際に OC フラグをアサートする OC 出力機能を備えている必要があります。センサは、急速な故障過渡を捉えるのに十分な帯域幅または応答時間を有する必要があります。

電流センサの OC 機能における SPF の場合、OC が適切にトリガされない可能性があります。最も簡単な方法は、冗長過電流検出回路を使用することです。外付けの絶縁コンパレータを第 2 の信号チェーンとして使用できます。絶縁コンパレータの出力を電流センサの OC 出力と論理 OR することで、電流検出回路における SPF をカバーできます。

ただし、部品の追加はコストの増加につながります。マイコン内のコンパレータ サブシステム (CMPSS) モジュールを、冗長な OC 検出として活用できます。CMPSS は、デジタル フィルタ オプションを備えたアナログ比較機能を提供します。電流センサーのアナログ出力は CMPSS モジュールに入力され、マイコン内部の電圧スレッショルドと比較された後、システムが過電流状態かどうかが判定されます。この安全メカニズムは、電流測定回路における SPF に対する SM1 として定義されています。

SM1 の前提は、電流センサのアナログ出力が正確であることです。そのため、電流センサのアナログ出力の精度を監視するものとします。これは妥当性チェックによって実現できます。マトリクス コンバータの入力と出力間の過渡電力のバランスに基づき、DC 出力電流の測定値を、OBC の AC 入力側における既存の電流測定値と比較できます。AC 電圧低下やバッテリ電圧低下を考慮すると、妥当性チェックでは電流を比較するのではなく、入力電力と出力電力を比較する必要があります。妥当性チェックのスレッショルドを決定するにあたっては、無効電力および効率も考慮する必要があります。AC 側センサの測定値は、追加の DC バス センサを設けることなく、第 2 の検証経路を提供します。この安全メカニズムは、電流測定回路における DPF に対する SM2 として定義されています。

図 2-9 に、電流測定回路の安全メカニズムを示します。

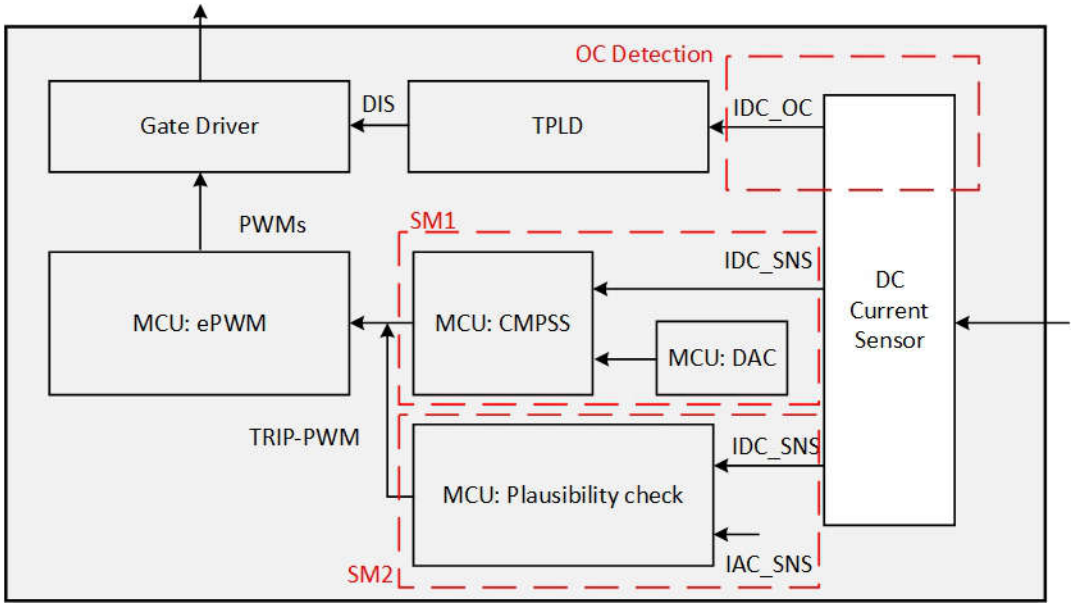

図 2-9. 電流測定回路における機能メカニズム

の表 2-11 に示すその他のシステム サブ要素については、詳細な分析は本書では割愛し、一部の機能安全機構のみを示します。

- VCU との CAN 通信。CAN トランシーバは、OBC と VCU 間の信頼性の高い双方向通信を確立および維持する必要があります。この重要なインターフェイスにより、VCU は充電パラメータおよび制御コマンドを OBC に送信でき、同時に OBC は動作状態および故障状態を VCU に報告できます。
  - SM1：CAN トランシーバの診断機能を内蔵。これにより、マイコンは CAN トランシーバの健全性およびシステム全体の完全性を継続的に評価できます。これらの統合診断機能には、低電圧検出、CAN バス故障の識別、ソフトウェア ウォッチドッグ タイマ監視、バッテリ接続検出、熱保護、ドライバ ドミナント状態タイムアウト、および包括的なバス故障保護機能が含まれます。
  - SM2：高度なエンド ツー エンド (E2E) 保護機能。これらは、潜在的な通信障害を検出するため、プロトコル レベルで実装されています。これらの手法には、CRC チェックサムによるメッセージ完全性の検証、メッセージ欠落を検出するためのシーケンス カウンタ、および通信タイミングの異常を特定するためのタイムスタンプが含まれます。この多層的なアプローチにより、ハードウェア レベルの診断では直接検出できない特定の故障条件がある場合でも、信頼性の高い情報交換が検証されます。
- ドライバ パワー スイッチ。ゲートドライバは、故障が検出された場合にパワー スイッチをオフしなければならず、システムは安全状態へ移行する必要があります。通常、OBC 用途では標準的な絶縁ゲートドライバが使用されており、自己診断機能は備えていません。パワー スイッチが同時にオフされると、単段構成の OBC にはフリーホイール経路がないため、パワー スイッチに大きな電圧スパイクが発生する可能性があります。
  - SM1：ゲートドライバを無効化するための独立した TLPD 回路。PWM シャットダウンを用いる方式では、信号チェーンまたは入力ピンに SPF が存在すると、パワー スイッチのオフ動作が規定されたシーケンスに違反することになります。TPLD は、組み合わせ論理によってパワー スイッチのオフ シーケンスを実現するプログラマブル ロジック デバイスです。このハードウェアのみのパスは、ソフトウェアの実行に依存しません。TPLD 回路の出力はゲートドライバの EN ピンに接続されているため、PWM 信号チェーンの SPF をカバーできます。
  - SM2：独立した故障反応としてコンタクタを遮断します。ドライバの 2 次側に SPF がある場合、パワースイッチを確実にオフにすることはできません。この状況では、OBC の入力側および出力側のコンタクタをオフすることで、OBC を入力および出力インターフェイスから切り離すことができます。
- 電圧電源。PMIC は、主要部品に電圧を供給します。PMIC はすでに FuSa 対応部品であるため、FuSa 機構の詳細は安全マニュアルに記載されています。以下に、電圧供給に関連する代表的な FuSa 機構を示します。
- SM1：VSYS 上の冗長 OVLO/OVP 電圧監視。

- SM2：出力電圧モニタ。
- SM3：残留電圧検出。
- SM4：パワーアップ シーケンス中の ABIST。
- SM5：VREG および VDD_1P8 に対する冗長 UV/OVP 電圧モニタ。
- SM6：レジスタ マップでの CRC。
- マイコンが制御と保護を実行します。マイコンはすでに FuSa 対応部品であるため、FuSa 機構の詳細は安全マニュアルに記載されています。関連する安全メカニズムの一部については、このアプリケーション ノートのセクション 3.2 で紹介します。マイコンの安全メカニズムに加えて、PMIC はマイコンの監視の役割も果たします。マイコン監視に関連する FuSa メカニズムのいくつかを以下に示します。
  - SM1：マイコン エラー信号モニタ。
  - SM2：デジタル出力ピン (nINT/GPIO および GPIO) の読み戻し
  - SM3：ソフトウェア実行の異常を検出するため、独立したウォッチドッグ機能を実装します。

まとめると、この安全目標が侵害されないことを確認するために、多層的な安全メカニズムが採用されています。信頼性の高い故障識別を実現するため、妥当性チェックおよび冗長化が実装されています。独立した保護経路により、あらゆる過電流事象に対して是正動作が実行されます。包括的な診断により、潜在的な故障が安全上重大な故障となる前に早期検出されることが確認されます。

SPF 用の安全メカニズムは FHTI 要件を備えた TSR へ、DPF 用の安全メカニズムは MPFHTI 要件を備えた TSR へ変換する必要があります。表 2-12 に、電流センサに関連する FSR の TSR の例を示します。複数の FSR が同一のハードウェアまたはソフトウェア機能を要求する場合、関連する要求事項は一つの TSR に統合されます。各 TSR は、元となる FSR の ASIL-B を継承し、まとめられた FSR の中で最も厳しいタイミング制約を満たすために必要な FTTI を継承します。

表 2-12. FSR 2.1 の TSR の例

FSR 2.1：DC バス電流検出システムは、正確な電流測定を実行するものとします					
ID	TSR	アロケーション	ASIL	安全状態	トレース先
TSR-CS-1	DC バス電流センサは、2% 以内の精度で電流を検出するものとします (SW OCP および妥当性チェック)	電流センサの Vout ピン。	B	ユーザー処理 SW へ遷移	FSR2.1 - 電流検出
TSR-CS-2	DC バス電流センサは自己診断を実行し、試験失敗時には故障を報告する必要があります。	電流センサ FLT ピン。	B	FLT をマイコンに通知します	FSR2.1 - 電流検出、OC 検出
TSR-CS-3	DC バス電流センサは、電流が過電流スレッショルドより 20% 高くなった場合に、OC ピンをアサートする必要があります。	電流センサ OC ピン。	B	OC をマイコンに通知します	FSR2.1 - OC 検出
TSR-CS-4	マイコンは、2 つの独立した電流センサの測定値に対して妥当性チェックを実行し、誤差が 20% を超えた場合には故障をフラグするものとします。	マイコン ADC モジュール。	B	充電の停止	FSR2.1 - 電流検出
TSR-CS-5	マイコンはソフトウェア OC 保護を実施し、OC 検出時には PWM 出力を停止する必要があります。	マイコン CMPSS モジュール。	B	充電の停止	FSR2.1 - OC 検出

すべての TSR は、元となる FSR にトレーサブルであり、同一の ASIL-B 分類を継承し、DC バス過電流による車両火災を回避するという安全目標で要求される FTTI を満たしています。

2.5 HW/SW の安全性要件

TSR が確立された後、次のフェーズではそれらを HSR および FSR へ展開します。各 HSR/SSR は、親となる TSR の ASIL-B を継承し、グループ内で最も厳しい FSR によって課される FTTI を遵守します。HSR は、電流検出フロントエンドに組み込まれるべきハードウェア特性を定義し、SSR は、タイミングおよび検出要件を満たすために、測定信号に対して実行されるべきソフトウェア処理を定義します。

表 2-12 によると、電流センサは、短絡状態を十分な帯域幅または応答時間で検出可能であり、自己診断機能を含む必要があります。これらの理由から、OBC アプリケーションの電流センサとして TMCS1133-Q1 が選定され、PFC ステージの入力側および DCDC ステージの出力側に配置されています。このピン配置図を、図 2-10 に示します。シャント抵抗を用いた代替の電流検出方式を使用することも可能ですが、その場合は HSR および FSR が異なり、本書の対象外となります。

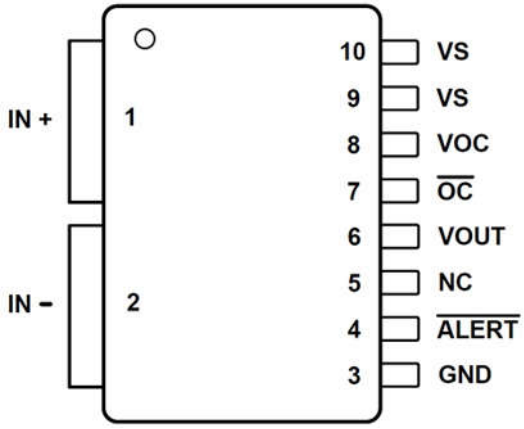

図 2-10. TMCS1133-Q1 のピン配置図

表 2-12 では、TSR-CS-1、TSR-CS-2、TSR-CS-3 が電流センサに、TSR-CS-4 および TSR-CS-5 が マイコンに割り当てられています。表 2-13 と表 2-14 は、FSR 2.1 にトレースされたこれらの TSR を実現する HSR および SSR の例です。

表 2-13. FSR 2.1 にトレースされた TSR の HSR の例

ID	HSR	ASIL	トレース先
HSR-CS-1A	ホール センサの帯域幅は 200kHz 超とし、VOUT フィルタのカットオフ周波数も 200kHz 超とする必要があります。	B	TSR-CS-1
HSR-CS-1B	ホール センサは、40A 以上のセンシング範囲を持つものとします。	B	TSR-CS-1
HSR-CS-2A	ホール センサは自己テスト用の FLT ピンを有し、故障発生時には 100ms 以内にマイコンへ通知する必要があります。	B	TSR-CS-2
HSR-CS-2B	ホール センサの FLT ピンは、故障報告のため DSP に接続する必要があります。	B	TSR-CS-2
HSR-CS-3A	ホール センサの VOC ピンは、最大電流より 20% 高い値に OC スレッショルドを設定します。	B	TSR-CS-3
HSR-CS-3B	ホール センサの OC ピンは、過電流検出時に 0.5us 以内で OC フラグをアサートする必要があります。	B	TSR-CS-3
HSR-CS-3C	ホール センサ OC フィルタは 1MHz カットオフ周波数を上回る必要があります	B	TSR-CS-3
HSR-CS-4A	AC 側電流センサの VOUT は、独立したマイコンの ADC チャネルへ接続する必要があります。	B	TSR-CS-4

表 2-14. FSR 2.1 にトレースされた TSR の SSR の例

ID	SSR	ASIL	トレース先
SSR-CS-1A	マイコンは、100kHz でホール センサ出力をサンプリングするものとします。	B	TSR-CS-1

表 2-14. FSR 2.1 にトレースされた TSR の SSR の例 (続き)

ID	SSR	ASIL	トレース先
SSR-CS-1B	マイコンは、パワーオン ホール センサのオフセット キャリブレーションを実装する必要があります。	B	TSR-CS-1
SSR-CS-2A	マイコンは、FLT のデューティ サイクルに基づいて、異なる種類のアラートを識別する必要があります。	B	TSR-CS-2
SSR-CS-2B	マイコンは、センサ アラート検出時に妥当性チェックを実行する必要があります	B	TSR-CS-2
SSR-CS-4A	マイコンは、2 系統センサの測定値の絶対差を計算する妥当性チェック アルゴリズムを 10kHz で実行する必要があります	B	TSR-CS-4
SSR-CS-4B	マイコンは、差分が 3 サンプル連続で 20% を超えた場合、2ms 以内にハードウェア故障を検出し、アサートする必要があります	B	TSR-CS-4
SSR-CS-5A	マイコンは、最大電流より 10% 高い値にソフトウェアの過電流スレッショルドを設定します	B	TSR-CS-5
SSR-CS-5B	マイコンは、ADC 値に基づいて CMPSS モジュールとの OC 検出を実行する必要があります。	B	TSR-CS-5
SSR-CS-5C	マイコンは、OC 検出時に規定されたシーケンスに従って PWM 出力を停止する必要があります。	B	TSR-CS-5

これらは、あくまで一例にすぎません。実運用の OBC プロジェクトにおいては、システム インテグレータがすべての TSR を対象に詳細な分析を実施した上で、後続の工程へ進む必要があります。

- 設計のアロケーション。各 HSR および SSR を、それぞれ該当するチームに割り当てます。
- トレーサビリティ マトリクス。FuSa 目標を FSR、TSR、さらに HSR および SSR へ関連付けるため、FTA または FMEA のブロック図を統合します。HSR および SSR は、その検証証拠に関連付ける必要があります。
- 検証計画。HSR および SSR の検証および妥当性確認。要求事項が満たされていることを示し、ASIL-B 安全目標への適合性を実証する試験報告書を提出します。

OBC システムでは、一部のアナログ部品の ASIL レベルは QM です。ASIL-B システムで QM 部品を使用することもできますが、ハードウェア素子の評価が必要です。ハードウェア要素の評価により、QM コンポーネントが安全目標に干渉しないこと、または追加の安全機構によって要求される ASIL を達成するのに十分な診断カバレッジが提供されていることが示されています。

例えば、TMCS1133-Q1 は FuSa 対応部品であり、ASIL-B 要件を満たすために選定されています。これを DC 出力側で、電流検出および過電流保護に使用するものとします。TI は、ハードウェア素子の評価を容易にするために、以下のコンテンツを提供できます。

- すべての故障モード。
- 各故障モードの確率。
- システムの安全性に及ぼす影響。

上記の情報はすべて、TMCS1133-Q1 の FuSa 文書に記載されています。お客様は、解析と試験を含む設計検証を実施するものとします。すべての故障モードには、ダイの故障モードおよびピンの故障モードが含まれます。の総 FIT 率は 62 であり、内訳はダイの FIT 率が 26、ピンの FIT 率が 36 です。すべてのダイ故障モードとダイの故障分布を表 2-15 に示します。

表 2-15. TMCS1133-Q1 ダイの故障モードと分布

ダイの故障モード	故障モード分布 (%)
VOUT オープン (ハイ インピーダンス)	5
VOUT が固着 (high または low)	30
VOUT は機能していますが、仕様外です	30
OC の誤トリップ、トリップの失敗	15
ALERT の誤トリップ、トリップの失敗	20

ピンの故障モードは、基本的に一般的なピンごとの故障シナリオを含みます:

- ピンがグランドに短絡しています。
- ピンの開路。
- ピンは隣接するピンに短絡しています。
- ピンが電源へ短絡しています。

ピンをグランドに短絡した例を取り上げます。故障による影響の可能性については表 2-16 を参照してください。故障影響クラスは、これらのピンの状態がデバイスにどのような影響を与えるかを示します:

- クラス A:機能に影響を及ぼす可能性のあるデバイス損傷。
- クラス B:デバイスに損傷はありませんが、機能は失われます。
- クラス C:デバイスの損傷はありませんが、性能は低下します。
- クラス D:デバイスに損傷はなく、機能または性能への影響もありません。

表 2-16. デバイス ピンがグラウンドに短絡した場合のピン FMA

ピン名	ピン番号。	潜在的な故障の影響の説明	故障の影響クラス
IN+	1	順方向電流の場合、ホール センサがバイパスされ、検出および増幅される信号は提供されません。IN+ ピンが GND よりも大きな電位にある場合、この状態では大量の電流がシンクされます。レイアウトや構成次第では、入力電源系、負荷デバイス、あるいはデバイス自体に損傷を与える可能性があります。	A
IN-	2	逆方向電流の場合、ホール センサがバイパスされ、検出および増幅される信号は提供されません。IN− ピンが GND よりも大きな電位にある場合、この状態では大量の電流がシンクされます。レイアウトや構成次第では、入力電源系、負荷デバイス、またはデバイス自体に損傷を与える可能性があります	A
GND	3	通常動作。	D
ALERT	4	ALERT が GND に短絡しているため、アラートはトリガされません	B
NC	5	通常動作	D
VOUT	6	出力は GND にプルされ、出力電流は短絡制限されています。この構成のまま、VS が高負荷対応の電源に接続され、かつ IN+ および IN− ピンを介して特定の高負荷条件がかかる場合、ダイ温度が 150°C に近づく、またはそれを超える可能性があります。	A
OC	7	OC が GND に短絡しているため、アラートはトリガされません。	B
VOC	8	スレッショルドが GND に設定されているため、すべての電圧でアラートがトリップします。その結果、アラートはアクティブ状態に固定されます。	B
VS	9	電源がグランドに短絡しています。	B
VS	10	電源がグランドに短絡しています。	B

安全メカニズムに基づき、90% を超える検出率を示すための診断カバレッジ計算を実装する必要があります。この評価により、このハードウェア要素は割り当てられた安全要求事項を十分に満たして支援できることが確認されました。

最終的に、開発チームは、単段 OBC に実装可能であり、ISO 26262 に基づいてレビュー可能な、完全でトレーサブルかつ検証可能な具体的安全要求事項の一式を有しています:2018 年監査。

2.6 依存故障分析

冗長性に影響を与える可能性のあるカスケード故障および共通原因故障を特定するために、DFA を実施する必要があります。独立性要求に関する追加の TSR は、DFA の分析によって特定されます。一般的に、DFA 分析では次のことを確認します:

- 物理的な分離。冗長部品は、十分な物理的分離が確保されており、冗長信号経路には異なる配線経路が用いられ、さらに重要部品間には熱的な分離が施されています。
- 多様性。冗長機能には異なる技術が用いられ、重要部品には異なるサプライヤが採用され、さらにハードウェアおよびソフトウェアの保護については異なる実装方法が用いられます。
- 独立性。冗長回路には独立した電源を用い、冗長機能には独立した処理を割り当て、さらに安全メカニズムには独立した起動経路を確保します。

例えば、マイコンのバイアス電源がグランドに短絡した場合、妥当性チェックではその故障を検出できず、ソフトウェア関連の安全メカニズムも機能を失います。この場合、OBC が安全状態に移行することを検証するための重要な安全メカニズムは、電圧監視です。

3 OBC システムの FuSa 部品

このセクションは、特定の機能安全目標を満たすための最小構成システムを設計することを目的とするのではなく、OBC システムにおけるあらゆる種類の TI 機能安全部品の概要を提供することを目的としています。したがって、以下に説明する部品のうち、同じ OBC システムですべてが同時に使用されるわけではありません。

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。以降のセクションでは、まず選定し部品たの基本機能を説明し、その後に該当する部品の安全機能を紹介します。

3.1 部品の概要

図 3-1 は、単段マトリックス コンバータの部品レベルのアーキテクチャを示しています。図は色分けされているため、さまざまなデザインの側面を簡単に認識できます。

- 赤いテキスト。詳細設計フェーズで通常選定されるハードウェア アイテムの部品番号例。これらの識別子はあくまでプレースホルダーであり、実際の部品番号は、技術要件、サイズ、およびコストに基づいて選定する必要があります。
- 青のテキスト。青色のラベルは、安全信号を伝送するピン、冗長部品 (デュアル電圧センサ)、および診断インターフェイス (セルフテスト、ウォッチドッグ、パリティチェック) を強調表示しています。この図では、これらのピンにフラグを付けることで、安全関連の信号を対応する FSR に簡単にトレースできるようになっています。

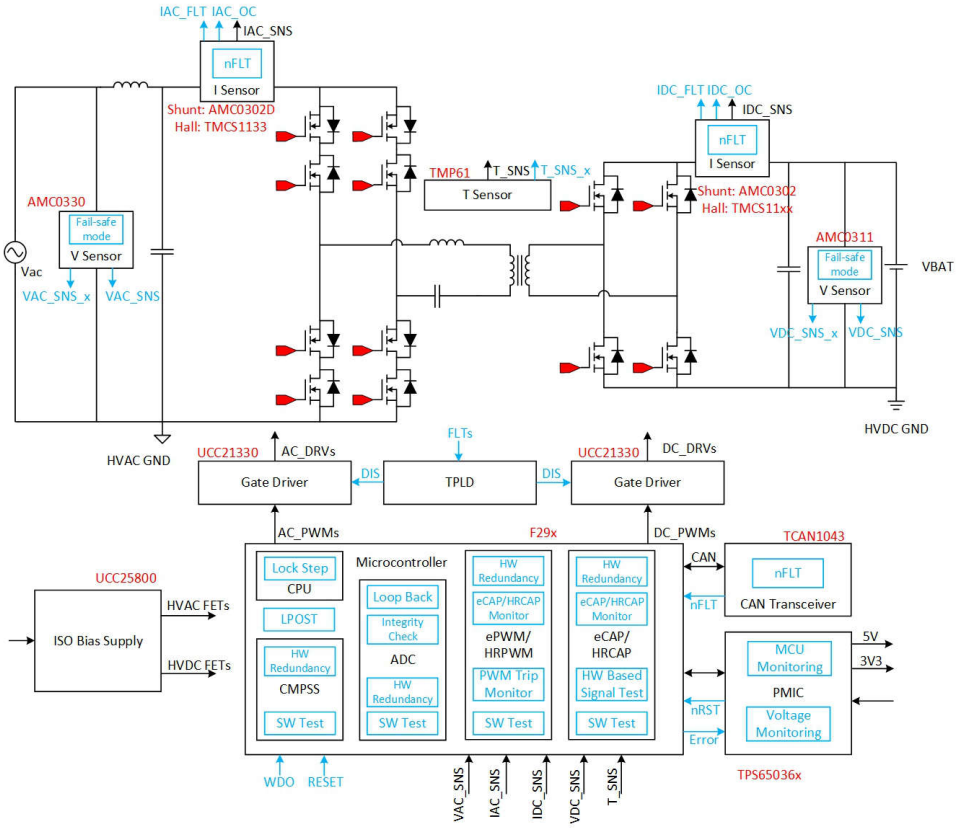

図 3-1. シングルステージ マトリックス コンバータの部品レベル アーキテクチャ

OBC アプリケーションでは、パワースイッチおよび受動部品を除くと、主な機能ブロックは、マイコン、PMIC、ゲートドライバ、電圧センサ、電流センサ、温度センサ、絶縁型および非絶縁型バイアス電源、ならびに通信機能です。

- マイコン (MCU)。充電制御アルゴリズムを実行し、センサ データを監視するとともに、車両上の BMS/VCU と通信します。安全要求の高い設計では、内部ウォッチドッグと自己診断機能を持つデュアル コア マイコンが一般的に採用されます。
- パワー マネージメント IC (PMIC)。電圧変換、電源シーケンス制御、監視、保護、および通信を含む複数の電源機能を管理および制御します。PMIC は、他のデバイスへの電源供給および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。マイコンにおいて回復不能な故障が検

出された場合、PMIC はマイコンにリセットをかけるとともに、関連する制御を遮断し、システムを安全状態へ移行させることができます。
- システム ベース チップ。BMS/VCU とステータスおよび診断情報を交換します。安全に重要なメッセージは、CRC およびメッセージ カウンタ チェックを使用して送信され、整合性が確認されます。
- 電源およびスーパーバイザ。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、センシング回路の高電圧側に電源を供給します。非絶縁型バイアス電源は、ガルバニック絶縁を必要としない低電圧部品に電力を供給します。
- ゲートドライバ。パワー スイッチに必要な電圧および大電流の駆動信号を提供します。絶縁型ゲートドライバの場合、低電圧信号側と高電圧側の間にガルバニック絶縁も提供します。ドライバの内蔵保護機能は、システムの FuSa 要件を満たすために使用されます。
- 電圧センサ。過電圧または低電圧事象を検出できる十分な分解能で、AC 入力電圧および DC バス電圧を測定します。センサ出力は、マイコンと安全監視ロジックの両方に配線できます。
- 電流センサ。AC 入力電流と DC バス電流を検出し、過電流保護機能も実装しています。一般的な実装例としては、OC 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備えたシャント方式の電流アンプが含まれます。
- 温度センサ。パワー スイッチのジャンクション温度、トランスの温度、およびコンバータの周囲温度を監視します。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。

3.2 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。このデバイスは、ロックステップ対応の C29x CPU を 3 コア搭載し、200MHz で動作します。4,000kByte のフラッシュ、452kByte の RAM を備え、5 基の SAR ADC、最大 36 チャネルの PWM 出力をサポートします。パッケージは QFP-144/ QFP-176/ BGA-256 に対応しています。ISO 2626 **2** と IEC61508 規格に適合しており、ASIL-D/SIL3 までの安全性要件に準拠しています。高度な機能と豊富な接続オプションを備え、包括的な設計を提供します。OBC アプリケーションのマイコンの主な安全機能には、以下の側面があります。

3.2.1 CPU

組込み CPU は複数の命令サイズ (16/32/48 ビット) をサポートしています。また、この CPU は、可変命令パケット サイズをサポートしており、各パケットは最大 8 個の命令を並列に実行することができます。たとえば、この CPU アーキテクチャでは、最大 8 個の 16 ビット命令を並列実行できます。これは、同時に実行可能な CPU 内の複数の機能ユニットによって実現されています。コア 1 とコア 2 は、スプリットロック モードまたはロック ステップ モードで独立して実行できます。

- ロックステップ比較モジュール (LCM) を使用したハードウェア冗長性。ロックステップ比較モジュール (LCM) は、ロックステップ比較機能を実装し、エラーを示すために使用されます。
- LCM のセルフテスト ロジック。LCM セルフテスト ロジックは、ロックステップ コンパレータ用に設計されています。コンパレータのセルフテストには、マッチ テストとミスマッチ テストの 2 つの異なるモードがあります。セルフテストが開始されると、2 つのコンパレータで次々に 2 つの異なるテスト モードが実行されます。
- 内部ウォッチドッグ (WD)。通常ウォッチドッグ (WD) とウィンドウ付きウォッチドッグ (WWD) という 2 つのモード選択でウォッチドッグ機能を実現します。
- ロジック パワーオン セルフテスト。LPOST (ロジック パワーオン セルフテスト) は、起動時およびアプリケーション時間中に、トランジスタ レベルでデバイスの高い診断範囲を提供します。LPOST は、高品質の製造試験を迅速に実行するために装置に挿入されたテスト用設計 (DFT) 構造を使用していますが、外部の自動試験装置 (ATE) ではなく内部のテスト エンジンを使用しています。LPOST テストは、SECCFG ユーザー入力に基づいて BootROM によってトリガされます。

3.2.2 ADC サンプリング

F29H859TU-Q1 マイクロコントローラには高性能のアナログ ブロックが内蔵されており、システムのさらなる統合が可能です。3 つの独立した 12 ビット SAR ADC と、2 つの独立した 16 ビット/ 12 ビット切り替え可能な SAR ADC により、複数のアナログ信号を高精度かつ効率的に管理でき、結果としてシステム スループットが向上します。4 つのアナログ コンパレータ モジュールが、トリップ条件の有無を判断するために入力電圧レベルを継続的に監視します。ADC でサポートされている主な安全メカニズムは以下のとおりです。

- DAC ～ ADC へのループバック チェック。ADC の健全性は、DAC 出力を ADC で監視することで確認できます。あらかじめ定めた電圧レベルのセットを DAC で設定し、出力することができます。これらの電圧レベルは ADC で測定でき、期待値と照合することで ADC が正しく動作していることを確認できます。
- ADC 入力信号の整合性チェック。ADC 入力信号の健全性は、ADC 変換に対するハードウェアおよびソフトウェアのランタイム診断を組み合わせて検証できます。入力信号の妥当性チェックは、内蔵ハードウェア機構とソフトウェアで設定可能なスレッショルドを用いて行うことができます。変換された結果の妥当性チェックは、ADC 後処理ブロックを使用して確認できます。
- ADC セーフティ チェッカによるハードウェアの冗長性。複数の ADC インスタンスを用いて同一の入力をサンプリングし、同時に同一の処理を実行した後、出力値をクロスチェックします。一次と冗長の両 ADC の結果がそろうと、それらを自動的に比較するハードウェア ベースの結果安全チェッカ モジュールです。
- エラー テストを含む機能のソフトウェア テスト。ADC モジュールと後処理ブロックで機能テストまたは故障注入テストをサポートします。あらかじめ定めた電圧レベルのセットは、外部回路または内蔵 DAC によって ADC 入力ピンに供給できます。変換結果を期待値と比較することで、ADC モジュールおよび後処理ブロックの機能的な正しさを確認できます。
- ロジック パワーオン セルフテスト。LPOST (ロジック パワーオン セルフテスト) は、起動時およびアプリケーション時間中に、トランジスタ レベルでデバイスの高い診断範囲を提供します。LPOST は、高品質の製造試験を迅速に実行するために装置に挿入されたテスト用設計 (DFT) 構造を使用していますが、外部の自動試験装置 (ATE) ではなく内部のテスト エンジンを使用しています。LPOST テストは、SECCFG ユーザー入力に基づいて BootROM によってトリガされます。

3.2.3 PWM 生成

F29H859TU-Q1 デバイスは、業界をリードする制御用ペリフェラルを備えており、高分解能機能 (HRPWM) を持つ 36 チャネルの拡張パルス幅変調 (ePWM) を搭載しています。拡張キャプチャ (eCAP) モジュールにより、クラス最高レベルのシステム制御が可能です。シグマ デルタ フィルタ モジュール (SDFM) が内蔵されているため、絶縁バリアを通して、オーバーサンプリング シグマ デルタ変調器をシームレスに統合できます。

- ハードウェア冗長性。PWM については、マルチチャネルを並列に構成し、内部または外部のコンパレータで出力を比較することで、ハードウェア冗長性を実装できます。eCAP や SDFM については、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、同時に同一の処理を実行したうえで、出力値を相互にクロスチェックすることで、ハードウェア冗長性を実装できます。
- eCAP/HRCAP による ePWM/HRPWM の監視。ePWM/HRPWM 出力は、eCAP/HRCAP などの入力キャプチャ ペリフェラルによって適切に動作するように監視できます。キャプチャされたパルス幅は、PWM の立ち上がりおよび立ち下がりエッジやタイムスタンプ情報を検出するために、ユーザー実装の追加診断機能として利用できます。PWM 診断として使用する場合、eCAP/HRCAP は ePWM/HRPWM のパルス幅を周期的に測定することでテストできます。
- トリップ イベントのオンライン MINMAX モニタリング。サポートは、設定された時間ウィンドウ内でトリップ イベントの発生を検出します。このウィンドウは、XMINMAX レジスタ セットに設定された MIN 値および MAX 値によって構成されます。
- 最小デッドバンド ロジックを用いた故障回避。最小デッドバンド ロジックは、2 つの PWM チャネル間、および PWM インスタンス間において、アクティブなパルス位相の間に最小の非アクティブ時間 (デッド バンド) が確保されていることを検証するように設定できます。
- ハードウェア冗長性と WADI を使用した出力の比較。波形アナライザ診断 (WADI) ペリフェラルは、多くの便利な内蔵信号分析サポートで構成されており、信号の安全メカニズムを提供します。WADI は、個々の信号に対するチェック、または 2 つの信号間のチェックを実行できます。具体的には以下のとおりです:パルス幅、周波数、位相オーバーラップ、およびデッドバンドの測定。
- エラー テストを含む機能のソフトウェア テスト。ePWM モジュールに対して、機能テストまたは故障注入テストの実行をサポートします。各サブモジュールは、PWM を用いて適切な刺激を与え、その応答をキャプチャ (タイムスタンプ) モジュール (eCAP) のいずれかで観測することでテストできます。これにより、eCAP または ePWM モジュールの機能的な正しさを確認できます。
- 信号監視を使用したエラー検出。ハードウェア ベースの信号監視ユニットは、eCAP 入力信号のエッジ、パルス幅、および周期を測定し、それらのイベントがプログラム可能な期待範囲内で発生しているかどうかを確認する機能を備えています。
- ロジック パワーオン セルフテスト。LPOST (ロジック パワーオン セルフテスト) は、起動時およびアプリケーション時間中に、トランジスタ レベルでデバイスの高い診断範囲を提供します。LPOST は、高品質の製造試験を迅速に実行するために装置に挿入されたテスト用設計 (DFT) 構造を使用していますが、外部の自動試験装置 (ATE) ではなく内部

のテスト エンジンを使用しています。LPOST テストは、SECCFG ユーザー入力に基づいて BootROM によってトリガされます。

3.2.4 CMPSS

CMPSS は、アナログ コンパレータとサポート部品で構成されており、これらの部品は、ピーク電流モード制御、スイッチモード電力、力率補正、電圧トリップ監視などの電源アプリケーションに役立ちます。アクティブ同期整流に ePWM 付きにより、アクティブ同期整流を採用することで、高い効率を実現できます。

- ハードウェア冗長性。CMPSS では、複数チャネルの並列出力や入力比較を用いることで、ハードウェア冗長性を実装できます。
- エラー テストを含む機能のソフトウェア テスト。CMPSS の重要なレジスタや重要な機能での機能テストまたは故障注入テストの実行をサポートしています。あらかじめ定められたパターンをレジスタに書き込み、その後、ユーザがレジスタ値を読み出して期待値と比較します。フィルタのスレッショルドを調整し、その変更に応じて出力が追従するかを確認することで、CMPSS の主要機能の検出を行います。
- ロジック パワーオン セルフテスト。LPOST (ロジック パワーオン セルフテスト) は、起動時およびアプリケーション時間中に、トランジスタ レベルでデバイスの高い診断範囲を提供します。LPOST は、高品質の製造試験を迅速に実行するために装置に挿入されたテスト用設計 (DFT) 構造を使用していますが、外部の自動試験装置 (ATE) ではなく内部のテスト エンジンを使用しています。LPOST テストは、SECCFG ユーザー入力に基づいて BootROM によってトリガされます。

3.2.5 データ転送

さまざまな業界標準の通信ポート (シリアル ペリフェラル インターフェイス (SPI)、シリアル通信インターフェイス (SCI)、インターインテグレーテッド サーキット (I2C)、コントローラ エリア ネットワーク (CAN) など) によりデータ送信がサポートされており、さまざまなアプリケーションにおいて最適な信号配置を行うための複数のマルチプレクシングのオプションを備えています。

- エンド ツー エンドの安全性を含む情報冗長性技術。モジュールの通信トランシーバや物理層は「ブラックボックス」として扱われ、通信トランシーバまたは物理層に関連する故障は、追加のメッセージ チェックサム、シーケンス カウンタ、タイムスタンプなどを含む通信プロトコルの E2E 保護によって間接的に検出できます。情報冗長性技術は、追加のランタイム診断としてソフトウェアを使用して適用できます。書き込んだ値の読み戻しや、同一の対象データを複数回読み出して結果を比較するなど、ソフトウェアによって適用可能な多くの手法があります。
- ロジック パワーオン セルフテスト。LPOST (ロジック パワーオン セルフテスト) は、起動時およびアプリケーション時間中に、トランジスタ レベルでデバイスの高い診断範囲を提供します。LPOST は、高品質の製造試験を迅速に実行するために装置に挿入されたテスト用設計 (DFT) 構造を使用していますが、外部の自動試験装置 (ATE) ではなく内部のテスト エンジンを使用しています。LPOST テストは、SECCFG ユーザー入力に基づいて BootROM によってトリガされます。

3.2.6 故障信号モニタと安全状態制御

安全マイコンは、リモート センサ データの完全性を確認し、バッテリ充電を制御します。異常状態が検出された場合、システムは安全な状態に入ります。

3.3 パワー マネジメント IC

TPS650365-Q1 デバイスは、高度に統合されたパワー マネジメント IC です。このデバイスは、3 つの降圧コンバータと 1 つの低ドロップアウト (LDO) レギュレータを組み合わせたものです。すべてのコンバータは、強制固定周波数 PWM モードまたは 自動 PFM モードで動作可能であり、EMI 低減のためのオプションのスペクトラム拡散変調 (SSM) をサポートしています。TPS650365-Q1 は、低電力モードにも対応しています。これらの柔軟な機能は、マイコン電源の用途に適しています。ISO 26262:2018 および IEC61508:2010 規格に準拠しており、ASIL-B/SIL2 までの安全性要件に確実に準拠しています。VQFN-24 パッケージで提供されます。OBC アプリケーションの PMIC の主な安全機能には、以下の側面があります。

3.3.1 MCU モニタ

TPS650365-Q1 は、モジュールの安全マイコンのハードウェアおよびソフトウェアの動作を監視します。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実行に関する故障モードが発生した場合、PMIC は検出された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、外部パワー ステージおよびモジュール通信インターフェイスの遮断が含まれ、さらに故障がスレッショルドを超えて継続する場合には安全マイコンを再起動します。

- ウォッチドッグ。3 つの選択可能なモードを備えた外部ウォッチドッグ機能を提供します:入力トリガ モード、ソフトウェア トリガ モード、および 質問応答 (Q&A) モード。
- エラー信号モニタ (ESM)。TPS650365-Q1 デバイスは、マイコンが ESM を設定し、スタート ビットによってこれを有効化した後、nERR 入力ピンを介してマイコンのエラー出力信号を監視できます。ESM は 2 つの動作モードをサポートします:レベル モードと PWM モード。

3.3.2 シャットダウン シーケンス

TPS650365-Q1 部品は、PMIC またはマイコンにおいて回復不能な故障を検出した場合に、シャットダウン シーケンスを実行できます。この部品はマイコンをリセット状態に遷移し、マイコンに対してリセット ピンを駆動して、安全マイコンをリセット状態に制御します。マイコンの出力制御は、それに応じて遮断されます。

3.3.3 電源

TPS650365-Q1 は、PMIC の内部電圧、入力電圧および出力電圧を監視し、内部診断機能を提供します。

- 電圧モニタ。TPS650365-Q1 の入力電源電圧および内部で生成される安定化出力電圧は、基準電圧と比較することで、低電圧および過電圧イベントを継続的に監視しています。電圧が規定範囲外になると、レギュレータはシャットオフされ、ステート マシンは故障処理状態へ遷移します。注:すべてのレギュレータには、過電流事象から内部のパワー MOSFET を保護するための電流制限回路が組み込まれています。
- ABIST。すべてのレギュレートされた電源がイネーブルの場合、電源オン時およびオンデマンドで、低電圧 / 過電圧モニタのアナログ内蔵セルフテスト (ABIST) を提供します。

パワー マネジメント IC で概要を説明しているように、PMIC は、OBC システム向けに、電源供給機能と電圧監視機能の両方を提供する完全に統合された設計を実現します。または、PMIC を使用しない場合にディスクリート アプローチを実装することもできます。ディスクリート構成では、システム ベーシス チップや個別の LDO レギュレータがマイコンへの電源供給を担い、別個のスーパバイザ回路やウォッチドッグ デバイスがシステム監視機能を担当します。セクション 3.4 ではシステムベースのチップについて、セクション 3.5 では電源ユニットと監視回路について説明します。

3.4 システム ベーシス チップ

TCAN1164-Q1 は、高速コントローラ エリア ネットワーク (CAN) 用のシステム ベーシス チップ (SBC) であり、ISO 11898-2:2016 CAN フレキシブル データ レート (FD) 仕様の物理層要件を満たしています。トランシーバは Classical CAN ネットワークと最高 8 メガビット/秒 (Mbps) の CAN FD ネットワークの両方に対応しています。TCAN1164-Q1 は、広い入力電源電圧範囲に対応しており、5V の LDO 出力を内蔵しています。5V LDO 出力 (VCCOUT) は、CAN トランシーバ電圧を内部的に供給し、さらに外部にも電流を供給できます。

TCAN1164-Q1 は、テキサス インスツルメンツ社の品質管理製品開発プロセスを使用して開発され、AEC Q100 グレード 1 に従って認定されています。このプロセスは、TI の機能安全品質管理に該当します。TI は、以下に規定されるハードウェア要素評価のアプローチに基づいて、この部品をシステムへ統合することを推奨します:(ISO 26262-8:2018、第 13 項)。

TCAN1164-Q1 は、以下に説明するようにシステムと接続します:

- TCAN1164-Q1 は、VSUP ピンを介して、非 ISO バイアス電源から 5V の電力を受け取ります。
- TCAN1164-Q1 は、内部の CAN トランシーバおよび外部デバイスに電力を供給するための 5V LDO (VCCOUT) を内蔵しています。
- TCAN1164-Q1 は、4 本の SPI ピンを経由して マイコンに接続します。ホスト マイコンは、これらのピンを使用して TCAN1164-Q1 を設定し、またウォッチドッグを定期的にサービスします。
- TCAN1164-Q1 は、CANH および CANL ピンを介して外部 CAN バスに接続され、また TXD および RXD ピンを介してマイコンと接続され、CAN バス通信を行います。

したがって、機能安全アプリケーションを満たすために、潜在的な故障点および安全メカニズムは、CAN 通信、電源電圧レールの監視、SPI/ プロセッサ間通信、ならびに内部メモリに重点が置かれています。

3.4.1 CAN 通信

CAN 通信に対応する機能安全メカニズムを以下に示します。

- CAN プロトコル:マイコンに実装された CRC チェックサム付きの CAN プロトコルにより、あらゆる通信エラーを検出し、処理します
- CAN バス故障診断:TCAN1164-Q1 は、CANH および CANL ピンを監視し、バッテリへの短絡、グランドへの短絡、相互短絡、またはオープン故障の有無を判定するための高度なバス故障検出回路を備えています。
- TSD:TCAN1164-Q1 には、CAN トランシーバを無効化するためのサーマル シャットダウン警告およびサーマル シャットダウン (TSD) 保護機能が備わっています。
- CAN バス短絡電流リミッタ:このデバイスは、CAN バス ラインが短絡した場合に短絡電流を制限します。

CAN TXD ピン ドミナント状態タイムアウト:このデバイスはドミナント状態タイムアウト (DTO) をサポートしています。TXD がハードウェアまたはソフトウェアの故障によりタイムアウト期間を超えてドミナント (LOW) に保持された場合でも、ローカル ノードがネットワーク通信を阻害するのを防止します。

3.4.2 電源電圧レールの監視

TCAN1164-Q1 では、2 つの電圧レールが監視されています:VSUP と VCCOUT。VSUP は TCAN1164-Q1 への入力電源であり、VCCOUT は CAN トランシーバおよび外部回路への電源供給に使用される LDO 出力です。電源の故障が検出されると、デバイスはスタンバイ モードまたはフェイルセーフ状態に移行します。電源電圧レールをカバーする安全性メカニズム:

- VCCOUT LDO の短絡電流保護
- VSUP 電源低電圧検出 (UVSUP)
- VCCOUT 低電圧検出 (UVCCOUT)
- VCC 過電圧検出 (OVCCOUT)

3.4.3 SPI/プロセッサ通信

TCAN1164-Q1 には、プロセッサとデバイス間の通信が正常に機能しているかどうかを判定するための複数の手段が備わっています。

- ウォッチドッグ:本デバイスは、デフォルトのウィンドウ ベース ウォッチドッグに加え、SPI インターフェイスを使用した選択可能なタイムアウト方式および質問と回答 (Q&A) 方式のウォッチドッグを提供します。
- SPI エラー インジケータ:1 回の SPI トランザクション中に、所定のクロック サイクル数およびデータが正しくシフトインされなかった場合、専用レジスタの割り込みが設定されます。
- スクラッチパッドの書き込み / 読み取り:このデバイスには、書き込みと読み戻すことができる専用のレジスタがあり、レジスタ空間への SPI インターフェイスを検証できます。

3.4.4 デバイス内蔵 EEPROM

TCAN1164-Q1 は、特定の性能調整のために内部 EEPROM を使用しています。電源投入時に、デバイスは EEPROM から内部レジスタをロードして CRC チェックを実行します。トリミングに使用される内部 EEPROM に CRC エラーが発生した場合、CRC_EEPROM 割り込みが設定されます。

3.5 電源とスーパーバイザ

このセクションでは、TI の 2 つの機能安全対応デバイスである LM5155-Q1 昇圧コントローラと TPS3850-Q1 スーパーバイザを組み合わせて、システムの ASIL-B 要件を満たす TI の設計について説明します。

LM5155-Q1 は、安全マイコン用の 3.3V 電源を出力するために使用されます。マイコンの電源電圧を推奨動作範囲内に維持することは、マイコンが危険な状態に陥るのを防ぐために不可欠です。そのため、3.3V 電源出力については、電源の低電圧や過電圧といった故障を監視する必要があります。OV または UV のいずれかが発生した場合、マイコンをリセットして停止させ、システムを安全状態へ移行させる必要があります。

3.3V 電源の OV/UV 故障モードを検出するための推奨設計は、外部スーパバイザを使用して電源出力を監視することです。スーパバイザは電源出力から独立しているため、共通原因の故障は発生しません。スーパバイザは高い性能と精度を備えているため、電源の過電圧および低電圧に対する診断カバレッジは高くなります。

この OBC システムでは、ウィンドウ ウォッチドッグを内蔵したウィンドウ電圧スーパバイザである TPS3850-Q1 を使用して、3.3V 電源レールを監視しています。これにより、電源の故障が検出された際に、安全マイコンはリセットされて安全状態へ移行します。

3.6 ゲートドライバ

一般的な OBC アプリケーションでは、ゲートドライバは、ハイサイドおよびローサイド スイッチにおける意図しないターンオンや直接的なシュートスルーを防止する必要があります。UCC21330-Q1 は、パワー MOSFET、SiC、GaN、および IGBT トランジスタを駆動するために、4A のピーク ソース電流および 6A のピーク シンク電流を備えた、絶縁型デュアル チャネル ゲートドライバです。

UCC21330-Q1 の保護機能には、抵抗で設定可能なデッドタイム、両出力を同時にシャットダウンするディスエーブル機能、および 5ns 未満の入力過渡を除去する内蔵グリッチ除去フィルタが含まれます。すべての電源が UVLO 機能を備えています。INA ピンおよび INB ピンの両方に内蔵された弱プルダウンにより、デフォルト状態で出力が low となることが確認され、安全状態が確保されます。DIS ピンが high にアサートされると両方のドライバ出力が無効化され、Low に設定されると両出力が有効になります。故障状態が検出された場合、マイコンまたは他のアナログ コンパレータによってグローバル DIS がアサートされ、すべてのドライバが一斉に無効化されます。

動的スイッチング中にハイサイドおよびローサイド FET の直接的なシュートスルーを防止するため、0Ω ～ 150Ω の抵抗を実装する、または DT ピンを GND に短絡することで、インターロック機能を有効化し、2 つの出力をインターロックさせることができます。両方の入力が同時に high になると、両方の出力は直ちに low に設定されます。図 3-2 はこの機能を示しています。

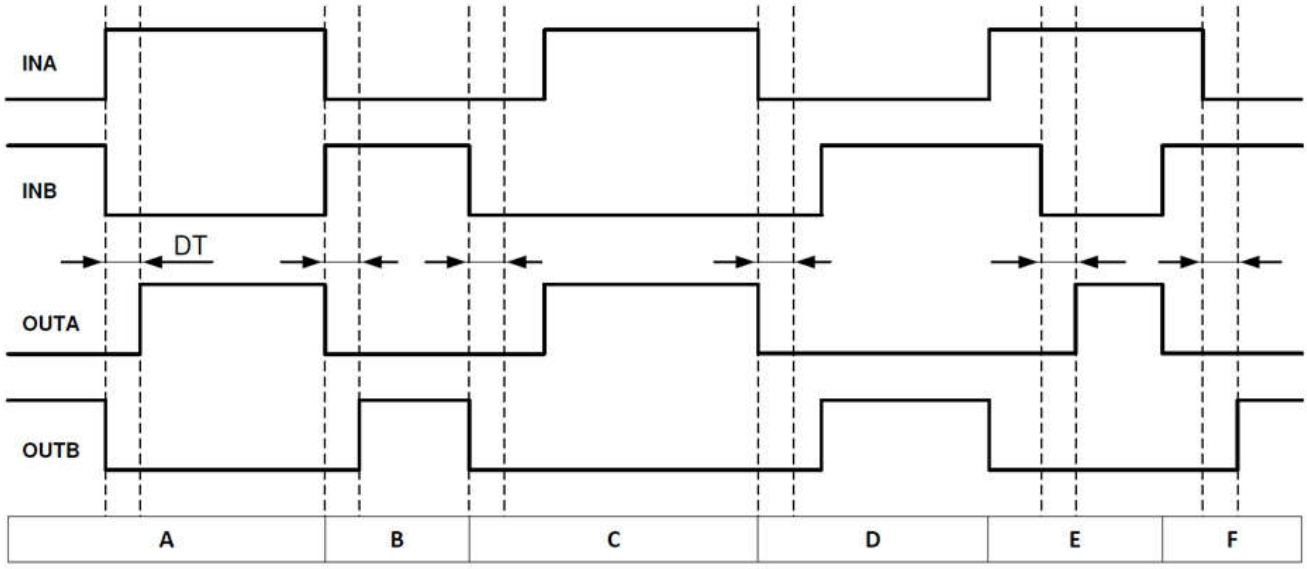

図 3-2. 入力信号と入出力ロジックの関係

条件 A：INB が Low、INA が High に遷移します。INB は OUTB を直ちに low に設定し、プログラムされたデッドタイムが OUTA に適用されます。設定済みデッド タイムの後、OUTA は HIGH に遷移できます。

条件 B：INB が High、INA が Low に遷移します。同様に、INA により OUTA は直ちに Low に設定され、OUTB には設定されたデッドタイムが適用されます。設定済みデッド タイムの後、OUTB は HIGH に遷移できます。

条件 C：INB が Low になりますが、INA はまだ Low のままです。INB は OUTB を直ちに low に設定し、プログラムされたデッドタイムが OUTA に適用されます。この場合、入力信号のデッドタイムは、プログラムされたデッドタイムよりも長くなります。したがって、INA が high になると、即座に OUTA が high に設定されます。

条件 D：INA が Low になりますが、INB はまだ Low のままです。INA は OUTA を直ちに low に設定し、プログラムされたデッド

タイムが OUTB に適用されます。INB 自体のデッド タイムは、プログラムされたデッド タイムよりも長くなります。したがって、INB が high になると

OUTB は直ちに high に設定されます。

条件 E: INB と OUTB がまだ High のうちに、INA が High に遷移します。オーバーシュートを回避するため、INA は直ちに

OUTB を low に引き下げ OUTA を low のまま維持します。その後 OUTB は low に遷移し、設定済みデッド タイムが

OUTA に割り当てられます。OUTB はすでに Low になっているため、設定済みデッド タイムの後、OUTA は HIGH に遷移できます。

条件 F: INA と OUTA がまだ High のうちに、INB が High に遷移します。オーバーシュートを回避するため、INB は直ちに

OUTA を low に引き下げ、OUTB を Low のまま維持します。その後 OUTA は low に遷移し、設定済みデッド タイムが

OUTB に割り当てられます。OUTA はすでに Low になっているため、設定済みデッド タイムの後、OUTB は HIGH に遷移できます。

ゲートドライバの堅牢で信頼性の高い動作を確認するため、最小パルス幅に特に注意を払います。最小入力パルス幅は、ドライバ IC に内蔵されたグリッチ除去フィルタによって規定され、これは無負荷状態のドライバにおいて出力に伝達される最短パルス幅を決定します。

ゲートドライバには低電圧誤動作防止 (UVLO) 機能が実装されており、ゲート電圧を監視して、指定のスレッショルドを下回ることを防止します。UVLO 定格は、Si および SiC MOSFET や IGBT を使用する高出力アプリケーションにおいて重要な検討事項です。

- UVLO は、バイアス電源の故障時にシステムが保護されていることを確認するための重要な機能です。
- デバイス特性および高出力システムの要件から、高出力アプリケーションにおける SiC MOSFET および IGBT には高い UVLO が必要です。これらのデバイスを効率的にスイッチングすることは、破壊や寿命低下を防ぐために極めて重要です。

高スイッチング周波数またはハード スイッチングのアプリケーションでは、ゲートドライバの誤動作による誤ターンオンを防止するため、システム全体の堅牢性を高める観点からミラー クランプの使用が推奨されます。UCC5350-Q1 は、典型値で 10A のピーク ソース電流および 10A のピーク シンク電流を備えた、シングル チャネルの絶縁型ゲートドライバで、ミラー クランプまたはスプリット出力を選択可能です。

- Vds の dv/dt によって、Cgd を通じた電流が発生します。このミラー電流は、ゲートに電圧を誘導します
- ミラー クランプは、低インピーダンス経路を設けてミラー電流をバイパスし、ゲートドライバが OFF のときに誤ターンオンが発生するのを防止します。

このシングルチャネル ゲートドライバには、シュートスルーを防止するための専用ロジックが内蔵されています。IN+ および IN− をそれぞれ 1 チャネル デバイスに接続するだけで、インターロックを実現できます。ハイサイドおよびローサイドの両方のゲートドライバに入力 high が与えられた場合、シュートスルーを防止するために、ドライバは出力を無効化します。論理表を表 3-1 に示します。

表 3-1. デバイスの機能状態

IN+	IN-	OUTH/OUTL	デバ機能状態
0	0	LO	システム オフ
0	1	LO	通常 low
1	0	HI	通常 high
1	1	LO	貫通電流を防止

さらに高度な保護機能が必要な場合、UCC218200-Q1 は、過電流および短絡検出、故障発生後の制御されたソフト シャットダウン、故障状態のレポート、アクティブ ミラー クランプ、SiC および IGBT のスイッチング特性と堅牢性を最適化す

る入力側および出力側電源の UVLO、ゲート出力電圧モニタリング、ならびに起動時の内蔵セルフ テスト機能を備えた絶縁型ゲートドライバです。

出力ゲート電圧モニタは、PWM が high のときにゲート電圧が VDD −3V を超えていること、および PWM が low のときにゲート電圧が VEE + 3V 未満であることを確認します。

- ゲート モニタの故障が検出されると、RDY は low にプルされます。
- LV 側の OUT_FB は、リアルタイム フィードバック出力を提供します。

初期起動時に、ドライバは以下のコンパレータが high または low に張り付いていないことを確認するため、一連のチェックを実行します:

- DESAT/OC。
- VCC、VDD、VEE UVLO。
- VDD −3V および VEE +3V のゲート モニタ。
- ミラー クランプのスレッショルド。

3.7 電圧センサ

OBC アプリケーションでは、電圧検出は閉ループ制御、故障検出、およびそれに続く保護動作のために重要です。絶縁型アンプは、絶縁バリアを使用する電圧センシングに一般的に使用される設計です。この絶縁バリアは、異なる同相電圧レベルで動作するシステム領域を分離し、電気的損傷を生じさせる可能性がある電圧またはオペレータに害を及ぼす可能性がある電圧から低電圧側を保護します。

AMC0311D-Q1 は高精度の絶縁型アンプで、磁気干渉に対して高い耐性のある容量性絶縁バリアにより、入力側と出力側の回路が分離されています。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 3-3 にブロック図を示します。

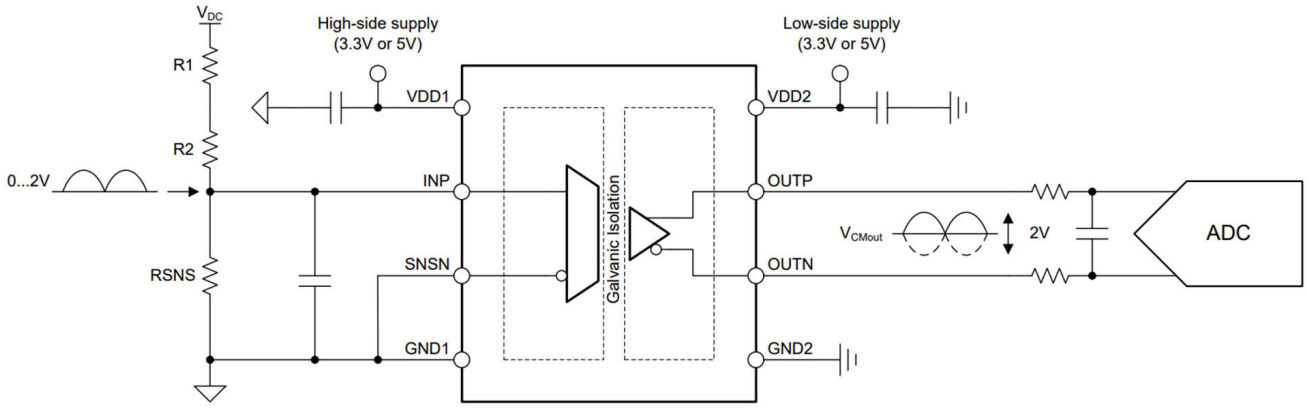

図 3-3. AMC0311D-Q1 のブロック図

ハイサイド電源喪失の検出機能が内蔵されているため、システム レベルの設計や診断が容易になります。図 3-4 はフェイルセーフ モードを示しており、このモードでは、AMC0311D-Q1 は通常動作条件では発生しない負の差動出力電圧を出力します。

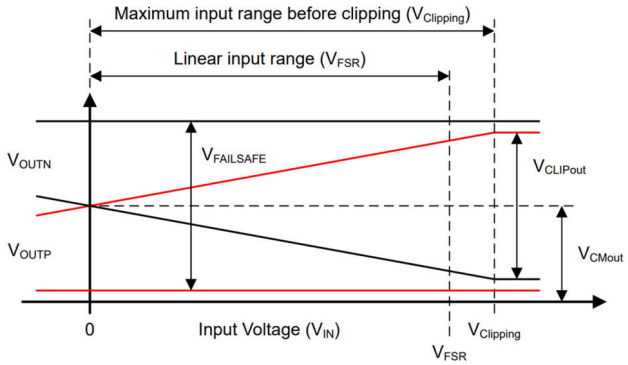

図 3-4. AMC0311D-Q1 の出力動作

システム レベルでのフェイルセーフ検出の場合、最大フェイルセーフ電圧を基準値として使用します。フェイルセーフ出力は、次の 3 つの場合でアクティブになります:

- AMC0311D-Q1 デバイスのハイサイド電源 VDD1 が欠落している場合。
- ハイサイド電源 VDD1 が VDD1 の UVLO スレッショルドを下回った場合。

実際のアプリケーションでは、マイコンが信頼性の高い電圧情報を取得していることを確認するために、冗長な電圧検出として 2 つの独立したサンプリング チャネルを使用できます。

3.8 電流センサ

代表的な OBC アプリケーションでは、閉ループ制御と過電流または短絡保護のために電流センサが必要です。ホール効果ベースの部品は選択肢の一つであり、AC および DC の両方の電流測定に使用できます。ホール効果をベースとした方式により、低抵抗のリード フレーム経路を採用して電力損失を低減しており、さらに高電圧 (HV) 側では外付けの受動部品、絶縁電源、制御信号を必要としません。

TMCS1133-Q1 は、ガルバニック絶縁型のホール効果電流センサであり、高い信頼性を持つ強化絶縁の動作電圧、優れた周囲磁界耐性、および高電流通電能力を提供します。業界トップ クラスの精度は、工場出荷時にトリミングされた感度誤差が 25°C で 0.4%、および全動作温度範囲で 0.5% に抑えられていることにより実現されています。この機能ブロック図を、図 3-5 に示します。

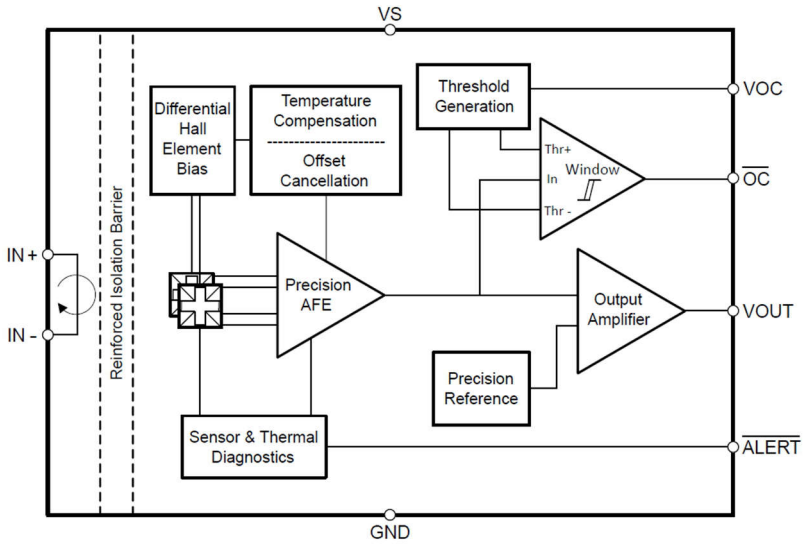

図 3-5. TMCS1133-Q1 の機能ブロック図

TMCS1133-Q1 は、高速なデジタル過電流検出応答を備えています。これは、短絡やその他の意図しないシステム状態によって生じる過大な電流から損傷を防ぐため、警告を発したりシステム シャットダウンを開始したりする用途に使用できます。OC のスレッショルドは、双方向デバイスおよび単方向デバイスの両方で設定可能で、フルスケールのアナログ測定範囲の半分から二倍超の信号に基づいてアサートされます。

過電流イベントの検出に VOUT ではなく OC 出力を使用する利点は、より高い感度を伴う広いダイナミック レンジと、アナログ信号帯域幅が低いことによる全体的な信号ノイズの低減です。ただし、マイコンの CMPSS モジュールを使用することで、VOUT ピンを冗長な過電流保護機能として用いることもできます。VOUT ピンを用いた OC 保護では、より小さい電流で発生するが継続時間の長いイベントをカバーするために、低めの OC スレッショルドを設定できます。また、OC ピン経路で SPF が発生した場合でも、OC イベントをカバーできます。

TMCS1133-Q1 には、動作条件によって電流センサの測定が無効になる場合に警告を出す内蔵セルフ診断機能が組み込まれています。監視される 2 つの重大な条件は、センサの温度と感度です。

- 高い入力電流に加え、周囲温度の上昇やプリント基板の熱設計条件が重なると、TMCS1133-Q1 は過熱し、許容される最大接合部温度を超えることで恒久的な損傷を受ける可能性があります。内部温度が最大許容接合部温度に近づくと、温度警告が発生します。
- TMCS1133-Q1 では、センサ感度およびオフセットが常時監視されています。万一イベントが発生した場合、ホール センサの感度またはオフセットが、工場出荷時の設定の制限値と比較して範囲外である場合に、センサ アラートが発生します。

アクティブ Low の ALERT 出力信号を用いることで、TMCS1133-Q1 がどの 4 種類の診断状態にあるかを判別できます。8kHz の PWM 出力信号のデューティ サイクルによって、温度およびセンサの動作条件に関する警告が、どちらか一方か、どちらもないか、または両方存在するかを示します。

電流センシングにおいては、シャント抵抗ベースの設計が代替手段としてあります。AMC0302D-Q1 は高精度の絶縁型アンプで、磁気干渉に対して高い耐性のある絶縁バリアにより、入力側と出力側の回路が分離されています。AMC0302D-Q1 の入力は、低インピーダンスのシャント抵抗またはその他の信号レベルが小さい低インピーダンス電圧源と直接接続できるよう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、OBC アプリケーションにおける正確な電流制御を実現します。図 3-6 にブロック図を示します。

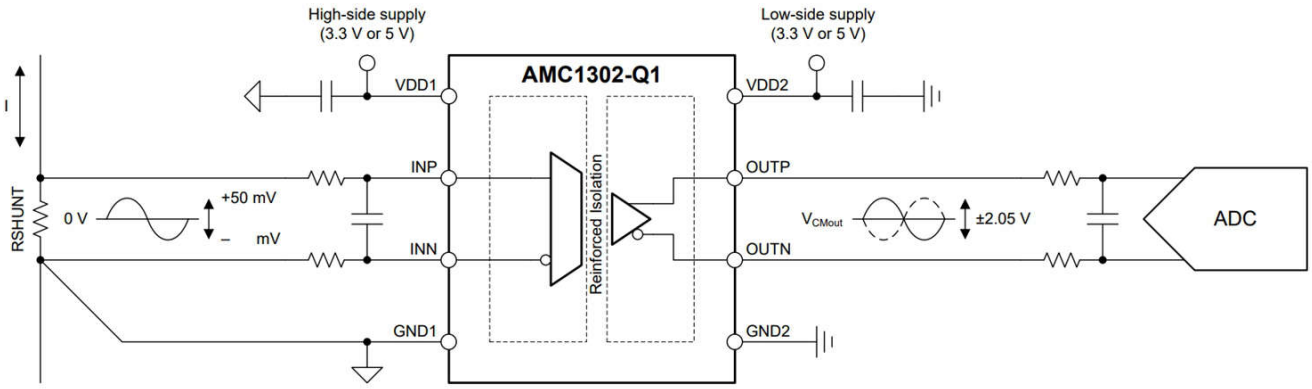

図 3-6. AMC0302D-Q1 のブロック図

シャント喪失およびハイサイド電源喪失検出機能を内蔵しているため、システム レベルの設計と診断が簡単に行えます。図 3-7 はフェイルセーフ モードを示しており、このモードでは AMC0302D-Q1 が、通常の動作条件では発生しない負の差動出力電圧を出力します。

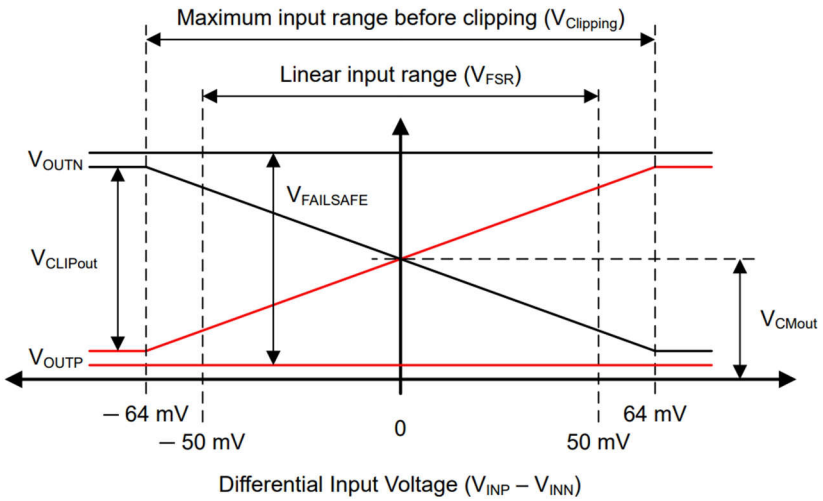

図 3-7. AMC0302D-Q1 の出力動作

システム レベルでのフェイルセーフ検出の場合、最大フェイルセーフ電圧を基準値として使用します。フェイルセーフ出力は、次の 2 つの場合にアクティブになります:

- ハイサイド電源が存在しない場合、または VDD1 の UVLO スレッショルド未満の場合。
- 同相モード入力電圧、すなわち VCM = (VINP + VINN) / 2 が、同相モード過電圧検出レベルを超えた場合。

電流センシング回路を電流制御には用いず、過電流保護のみに使用する場合、絶縁型コンパレータは非常に適したソリューションです。一般に、FuSa における冗長センシングの第 2 系統として位置付けることができます。AMC23C12-Q1 は、応答時間が短い絶縁型ウィンドウ コンパレータです。その比較ウィンドウの中心は 0V です。つまり、入力電圧の絶対値がトリップ スレッショルド値を超えると、コンパレータはトリップします。このブロック図を、図 3-8 に示します。

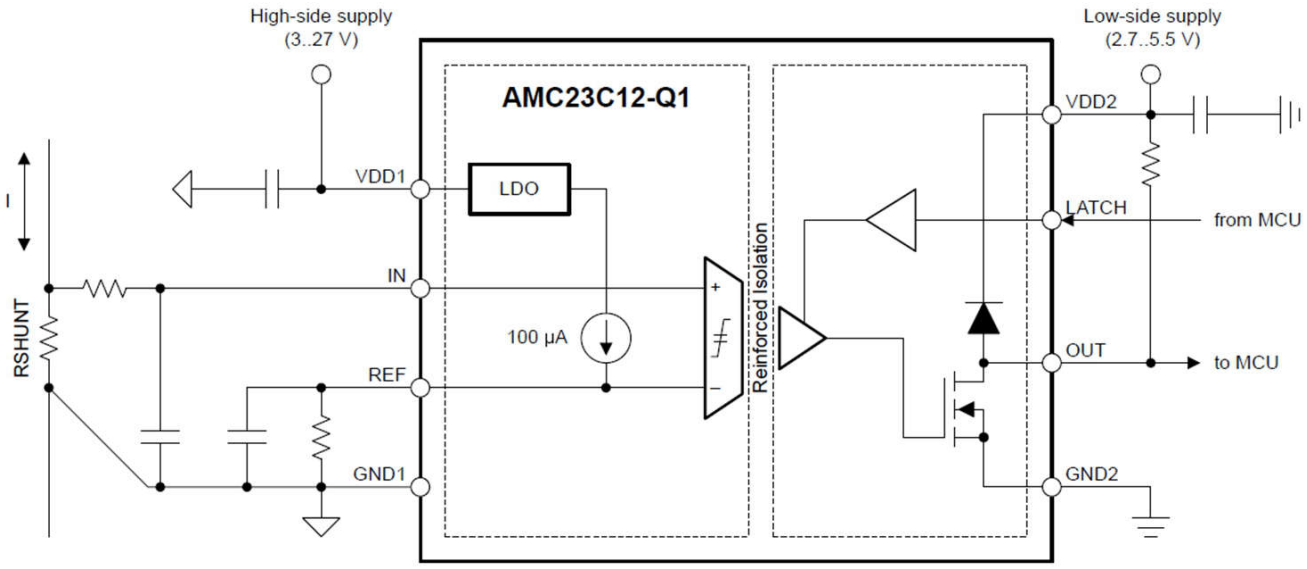

図 3-8. AMC23C12-Q1 のブロック図

3.9 温度センサ

OBC システムでは、温度センサも制御および安全監視において重要であるため、これについても慎重な検討が必要です。通常は、負の温度係数 (NTC) 抵抗などのアナログ デバイスによって実装されます。TMP61-Q1 は、正の温度係数 (PTC) を持つシリコンベースのサーミスタです。

温度センサにおいて最も重要な要素は精度です。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 3-9 に、標準抵抗と周囲温度との関係を示します。

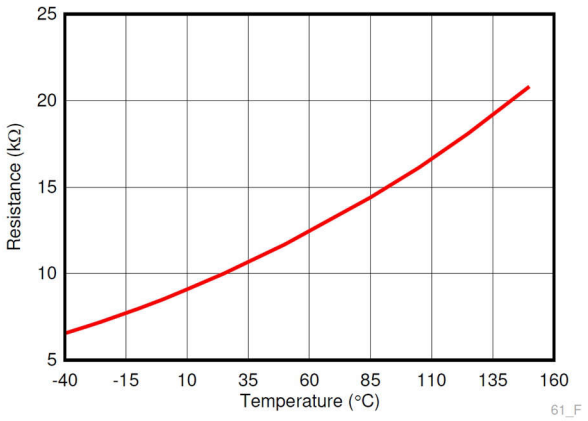

図 3-9. TMP61 -Q1 の標準抵抗と周囲温度との関係

TMP61-Q1 は、高い性能を長期間にわたって維持できるよう設計されています。高温時に短絡故障が発生した場合でも、内蔵のフェイルセーフ動作により安全性が確保されます。環境変動に対する優れた耐性により、長期的なセンサ ドリフトは典型値でわずか 0.5% に抑えられています。このデバイスは、わずか 0.6 秒という高速な熱応答時間により、温度変化に迅速に応答します。

TMP61-Q1 はコンパクトな 0402 パッケージで提供されているため、発熱源の近くに実装可能で、従来の NTC 抵抗の代替として利用できます。より高い耐熱性が求められるアプリケーション向けに、ELPG パッケージ オプションでは動作温度範囲を最大 170°C まで拡張できます。

温度検出の信頼性は、サーミスタだけでなく、プルアップ抵抗や電源にも依存します。TMP23x-Q1 デバイスは、温度に比例した出力電圧を持つ、自動車グレードの高精度 CMOS 集積回路リニア アナログ温度センサのファミリです。図 3-10 にブロック図を示します。

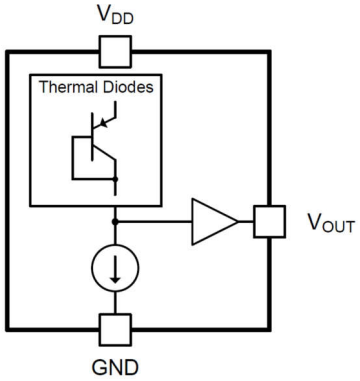

図 3-10. TMP23x-Q1 のブロック図

TMP235-Q1 は、−40°C ～ +150°C の全温度範囲において 10 mV/°C の正の傾きを持つ出力を提供し、動作電源電圧範囲は 2.3V ～ 5.5V です。一方、高ゲインの TMP236-Q1 センサは、−10°C ～ +125°C の温度範囲で 19.5mV/°C の正の傾きを持つ出力を提供し、動作電源電圧範囲は 3.1V ～ 5.5V です。また、外付けプルアップ抵抗を不要とすることで、信頼性が向上します。さらに、このデバイスは下流側コンポーネントに対する内蔵保護機能を備えており、電源過電圧状態にさらされた場合でも、異常に高い電圧がそのままバックエンドの ADC に比例して伝達されるのを防ぎ、マイコンを損傷のリスクから効果的に保護します。

サーミスタをホット スポット (例：FET、トランス、シャント抵抗) の近くに配置できない場合、測定精度および応答時間は通常低下します。OBC アプリケーションでは、電気的クリアランスおよび沿面距離を考慮する必要があるため、サーミスタの配置がトレードオフとなる場合があります。この問題を解決するため、ISOTMP35-Q1 は業界初の絶縁型温度センサ IC として、最大 3000VRMS の耐電圧を持つ内蔵絶縁バリアと、−40°C ～ 150°C の範囲で 10mV/°C の傾きを持つアナログ温度センサを統合しています。図 3-11 はブロック図を示します。

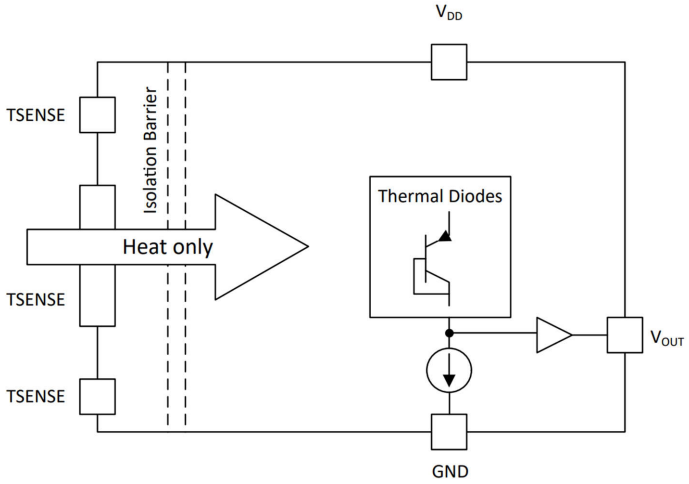

図 3-11. ISOTMP35-Q1 のブロック図

この統合により、高価な絶縁回路を追加することなく、高電圧の発熱源とセンサを同一箇所に配置することが可能になります。高電圧の発熱源と直接接触させることで、絶縁要件を満たすためにセンサを離して配置する方式と比べて、より高い測定精度と高速な熱応答が得られます。

上述のデバイス レベルの設計に加えて、冗長な温度センサの採用や妥当性チェックも、システムの機能安全性を向上させるための一般的な手法です。

4 まとめ

この資料では、OBC の FuSa 分析について説明します。セクション 1 では、FuSa の基本、ISO 26262: 2018 の一般的なワークフローと、FuSa 開発をサポートする TI の各種ツーを説明します。セクション 2 では、シングルステージ OBC を例とした FuSa 解析を順に説明します。まずアイテム定義から始め、安全目標を導出し、FSR、TSR を策定した後、最終的に HSR および SSR を開発します。セクション 3 では、マイコン、ゲートドライバ、センサ、バイアス電源などの主要な OBC 要素と安全機能の概要を説明します。この資料は、FuSa を使用した OBC の設計の作成に必要な重要な情報とリソースを設計者に紹介することを意図しています。

5 参考資料

1. *TUV SUD*、*ISO 26262 規格の理解：知っておくべきこと| TÜV SÜD PSB*
2. テキサス インスツルメンツ、IEC 623801 と SN 29500 による機能安全の FIT ベース故障率推定の理解、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機能安全認証の効率化、機能安全マニュアル。
4. テキサス インスツルメンツ、機能安全 ASIL B に適合する安全マイコン用電源の設計、テクニカル ホワイトペーパー。
5. テキサス インスツルメンツ、TMCS1123-Q1、TMCS1126-Q1、TMCS1127-Q1、TMCS1133-Q1 の機能安全に関する FIT 率、FMD およびピン FMA (Rev. A)、機能安全情報。
6. テキサス インスツルメンツ、C2000™ リアルタイム マイコン向け車載向け機能安全 (Rev. F)、機能安全マニュアル。
7. テキサス インスツルメンツ、C2000™ 安全メカニズム (Rev. B)、機能安全マニュアル。

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