

Application Note

MSPM0 マイコンのシステムレベル ASIL B 準拠



Lars Lotzenburger

概要

このアプリケーション ノートでは、テキサス インストルメンツの MSPM0 マイコン ファミリの ASIL B 派生製品に対するコア電圧監視の実装について説明します。この設計では、ISO 26262 の要件に従って、車載アプリケーションでの ASIL B 機能安全インテグリティの達成をサポートしています。

この設計は、大規模システム向けのハウスキーピングやデータ集約、さらには ASIL B 準拠のボディ エレクトロニクスや照明システムを必要とする、数多くの車載アプリケーションに適しています。機能安全エンジニア向けに設計された提案アプローチは、信頼性の高い電圧異常検出、堅牢な故障処理メカニズム、定量化可能な診断カバレッジ指標を実現します。付属の実装ガイドラインにより、エンジニアは車載安全基準に適合しつつ、MSPM0 ベースの設計にコア電圧監視機能を効率的に組み込むことができます。

目次

1 はじめに.....	2
2 詳細説明.....	3
2.1 アイテムの定義.....	3
2.2 前提.....	3
2.3 危険分析とリスク評価 (HARA).....	3
2.4 機能安全コンセプト.....	3
2.5 技術的安全コンセプト.....	4
2.6 技術的安全性要件.....	12
3 まとめ.....	15
4 参考資料.....	16

商標

Arm® and Cortex® are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.

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

MSPM0 マイコンは、コア電圧生成のための LDO を内蔵しています。ただし、LDO 出力電圧の内部監視を欠くため、車載アプリケーションで機能安全 (ASIL B) への準拠をサポートするための外部監視メカニズムが必要になります。この文書資料では、サブシステムの安全性目標の定義から始めて、外部監視を実装するためのコスト効率の優れたアプローチを説明します。この方法論では、機能安全コンセプトの開発と、機能安全と技術的安全性の要件を満たすアーキテクチャ設計について説明します。詳細な実装ガイダンスでは、電圧監視、フォルト検出、システム応答戦略の具体的な安全メカニズムについて説明しています。この文書資料では、FMEA (故障モード影響分析) と FMEDA (故障モード、影響、および診断分析) の結論として、目標とする ASIL B 要件への準拠を実証するための定量的な安全指標を示します。

2 詳細説明

2.1 アイテムの定義

このアイテムは、センサ サブシステム、処理サブシステム、アクチュエーション サブシステムという 3 つの主要な機能要素で構成される、ASIL B に適合した完全な安全関連システムです。このアーキテクチャは、ASIL B の整合性レベルを必要とする各種車載アプリケーションに適用可能な、汎用安全機能の実装を表しています。特定のシステムに関する ASIL B への適合は、システム全体の設計に依存します。

2.2 前提

次の条件が想定されています。

1. 公称 3.3V の電源レール V_{IN} が供給されます
 - a. 低電圧 (UV) および過電圧 (OV) フォルトに対する保護はありません
 - b. マイコンと直接接続されるセンサやアクチュエータ回路にも使用します
2. レールに接続されているすべての回路の推奨最大電源電圧は 3.6V 以上です
3. V_{IN} が 42V を超えません

2.3 危険分析とリスク評価 (HARA)

この文書は、危険分析やリスク評価には焦点を当てていません。HARA の結果として、安全目標の要件は以下の説明のとおり想定されています。

2.3.1 安全目標の定義

安全目標 ID	安全目標	ASIL	安全状態	FTTI
SG_01	マイコンの誤ったプログラム実行の防止	B	マイコンのパワー サイクル	10ms

ASIL B アプリケーションは、以下の ISO 26262 要件を満たす必要があります。

- SPFM $\geq 90\%$
- LFM $\geq 60\%$
- PMHF ≤ 100 FIT。

この安全メカニズムには 10ms の FTTI が割り当てられています。システム レベルのタイミング要件でより小さい値が必要な場合は、この値を下げるすることができます。ただし、ウィンドウ付きウォッチドッグ リフレッシュ時間により、実用的な最小 FTTI が定義されます。

2.3.2 安全状態「マイコンのパワーサイクル」

障害への対応としてマイコンのパワーサイクルを実行すると、上位の監視システム層との通信が一時的に途絶するなど、システム全体において連鎖的な安全状態への移行が誘発される可能性があります。原因となった障害が解消されると、マイコンは自己復旧を行うことができ、上位レベルのインスタンスは、通常の動作を再開させる前に、その復旧を独自に検知および確認できます。

2.4 機能安全コンセプト

過電圧イベントは、EMI、ロード ダンプや誘導性スイッチングに対する不十分な過渡応答、グラウンド シフト、または配線障害によって発生する可能性があります。

電圧が動作限界を超えると、一時的な誤動作から恒久的な損傷まで、さまざまな影響が生じます。マイコンの I/O ピンが絶対最大定格を超えるリスクがあり、回復不能なデバイス破壊につながる可能性があります。入出力間の電位差が過大になると、内蔵 LDO で熱ストレスや電圧調整の機能不全が発生し、 V_{CORE} の制御不能および動作の不安定化を招く恐れがあります。コア レベルでは、過電圧はラッチアップ、フラッシュ / EEPROM のデータ破損、メモリの早期劣化、シリコンの完全破壊を引き起こす可能性があります。過電圧が検出されない場合、システムの制御不能を引き起こし、機能上および安全上のリスクが生じます。

2.4.1 システム アーキテクチャ

マイコンは、システムの中央演算装置として機能します。すべてのセンサ回路とアクチュエータ回路は、マイコンに直接接続されています。車両のバッテリーがシステムに電力を供給します。DC/DC コンバータは、バッテリー電圧を安定化 3.3V レベル (V_{IN}) に降圧します。この統合電源は、マイコンへの電力と、接続されているすべてのセンサとアクチュエータ用のロジック電源を供給します。

1 つの統合電源レールを使用することは、すべての部品が常に同じ電圧レベルで動作することを意味します。同じ電圧レベルで動作することで、部品間のロジックレベルの不整合が排除され、システムの電源素子と電源オフ素子の間のリーク電流が防止されます。

図 2-1 に点線で、本書の範囲内のアプリケーション サブシステムを示します。

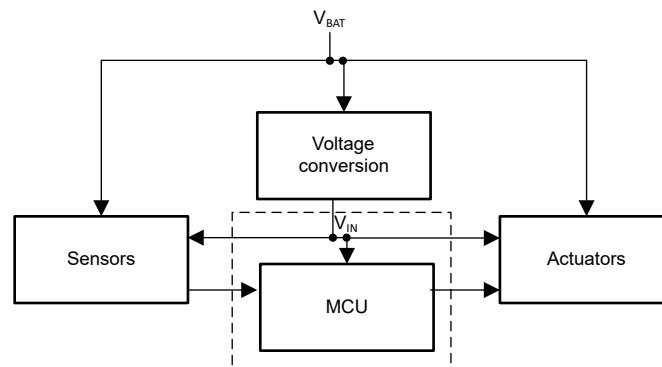


図 2-1. システム アーキテクチャ設計

2.4.2 安全アーキテクチャ

安全性目標 SG_01 を満たすために、マイコンは潜在的な危険を軽減する適切な条件が整った環境内で動作する必要があります。このシステムは、ハードウェアの損傷や誤った動作を防止するために、 V_{BAT} までの危険な電圧状態から保護すると同時に、適切にレギュレートされた V_{DD} を維持して、信頼性の高いマイコン動作を実現する必要があります。さらに、マイコンの正確な初期化および復帰動作を実現するため、適切に制御および監視されたリセット信号を供給します。さらに、ウィンドウ付きウォッチドッグ メカニズムを使用して、プログラムの誤った実行を検出します。これは、さまざまな根本的障害に起因して発生する可能性があります。

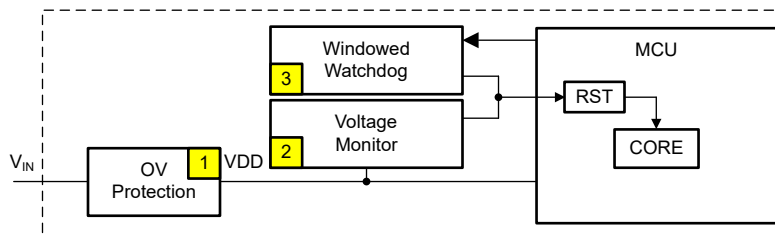


図 2-2. 安全アーキテクチャ設計

2.5 技術的安全コンセプト

ここで示す概念は、考えられるいくつかのアプローチのうちの一つに過ぎません。シャントリファレンス、抵抗ラダー、コンパレータを活用したディスクリート代替品については、『[ASIL B 要件のための MSPM0 外部 VCore 監視](#)』アプリケーションノートで詳しく説明しています。

2.5.1 製品概要

この設計の主要な構成要素はマイコンであり、MSPM0G3107-Q1 を使用して実装されています。このデバイスと、ASIL B 準拠を達成するために必要なすべてのサポート部品について、以下のセクションで紹介します。

2.5.1.1 MSPM0G3107-Q1

MSPM0G3107-Q1 は、テキサス インスツルメンツの MSPM0G ファミリの AEC-Q100 グレード 1 認定済み車載用マイコンで、車載機能安全アプリケーション向けに設計されています。このデバイスは、ASIL B までの ISO 26262 の系統のおよびハードウェアのコンプライアンス認証を取得済みです。このデバイスは、最大 80MHz で動作する 32 ビット Arm® Cortex®-M0+ コアと、ECC 保護されたフラッシュおよびパリティ保護された SRAM を組み合わせており、メモリ整合性を確保できます。接続機能には、内蔵の CAN-FD コントローラと、ハードウェア フロー制御機能を備えた UART 4 系統が含まれます。同時サンプリングを備えた 4MSPS のデュアル 12 ビット ADC と、1MSPS の 12 ビット DAC により、高精度アナログ機能を実現します。障害処理、デッドバンド挿入、QEI / ホール センサ サポート機能を備えた高度なタイマにより、堅牢なモーターおよびライティングドライブ制御を実現できます。ハードウェア AES-128/256、TRNG、CRC エンジンと 2 つのウォッチドッグにより、セーフティ クリティカルな完全性が強化されています。このデバイスは、5V 許容オープンドレイン I/O を備えた 64 ピン LQFP パッケージで供給されます。

機能安全 Web ページで、ISO26262 に準拠したすべての MSPM0 製品のリストを参照してください。

2.5.1.2 TPS388R0x-Q1

TPS388R0x-Q1 デバイス ファミリーには、2、4、6 チャネルのウィンドウ スーパーバイザ IC が搭載されており、16 ピンの 3 × 3mm WQFN パッケージで供給され、電源許容誤差が狭い低電圧電源レールで動作するシステム向けに設計されています。各チャネルは OV、UV、またはその両方によるウィンドウ監視を行うよう設定可能であり、フォルト出力は NRST/NIRQ に選択的に割り当てることができます。このデバイスは AEC-Q100 認定済みで、ASIL B (ハードウェア) および ASIL D (系統的) までの機能安全に準拠し、起動時にセルフテストが内蔵されています。このデバイスは、±6mV のスレッシュホールド精度、および 0.2V ~ 5.5V のセンシング入力電圧範囲を提供し、外付け抵抗は不要です。すべてのパラメータは I2C 経由で構成可能、または工場出荷時にプログラム可能です。追加機能には、内部グリッチ フィルタリング、CRC、パケット エラー チェック (PEC)、シーケンス ロギングが含まれます。

もう 1 つのバリエーションである TPS388C0x-Q1 ファミリーにはウィンドウ付きウォッチドッグを内蔵しています。

2.5.1.3 TPS3842C011-Q1

TPS3842C011-Q1 は、TPS3842-Q1 ファミリーに属する車載グレードの電圧スーパーバイザで、過酷な車載環境での使用に適した AEC-Q100 認定済みです。このデバイスは、電源レールの過電圧 (OV) 状態を監視し、SENSE ピンの電圧が定義されたスレッシュホールドを超えたとリセット信号をアサートします。このデバイスは 1.9V ~ 42V の広い入力電圧範囲に対応し、12V の車載用バッテリーと直接接続できます。850nA の超低静止電流と、高いスレッシュホールド精度により、安全重視のアプリケーションに対応できます。この製品は機能安全に定格付けされており、基本的な FIT 率、故障モード、分布が提供されることを意味します。

2.5.1.4 TPS22919-Q1

TPS22919-Q1 は、低損失のパワー ディストリビューションを必要とする車載用アプリケーション向けに設計された高性能ロード スイッチです。このデバイスは 5.5V の電源で動作し、最大 1.5A の連続電流を処理でき、100mΩ のオン抵抗を実現します。これらの仕様により、スイッチ両端の消費電力と電圧降下が最小限に抑えられます。このデバイスは、堅牢な動作を実現するようにパッケージされており、電流制限機能とサーマル シャットダウン保護機能が内蔵されているため、障害状態で安全な動作が可能です。

2.5.2 実装の詳細

アプリケーションは、MSPM0G3107-Q1 マイコンを中心に構築されています。このデバイスは、ISO 26262 に準拠し、ASIL B までのシステムティックおよびランダム ハードウェア安全性能力の両方をサポートしています。

このクラスのマイコンの一般的な機能は、コア電圧 (V_{CORE}) レールを生成する低ドロップアウトレギュレータ (LDO) が内蔵されていることです。この電圧は通常、内部では監視されないため、外部対策をシステム レベルで実装する必要があります。 V_{CORE} レールで UV または OV フォルトが検出された場合、リセット ロジックはこのレールに依存するため、マイコン全体の電源サイクルが必要です。

UV と OV の両方の条件について、 V_{DD} 継続的に監視する必要もあります。このマイコンには、内部リセットをトリガすることにより UV フォルトに応答する低電圧誤動作防止 (UVLO) が内蔵されています。マイコンと接続素子で V_{DD} が 4.1V (マイコンの絶対最大定格) を超えないようにするために、電力消費のために大型の受動部品を必要とする電圧クランプか、あるいは電源切断が必要になります。この設計は、電源切断アプローチを採用しています。

MSPM0G3107-Q1 は、ウィンドウ付きウォッチドッグと独立したウォッチドッグという 2 つの内部ウォッチドッグ タイマを内蔵しており、プログラム フローを監視できます。独立したウォッチドッグは、メインのシステムクロックから十分に独立した別のクロック ソースで動作します。

図 2-3 に、これらの点を考慮した実装ブロック図を示します。

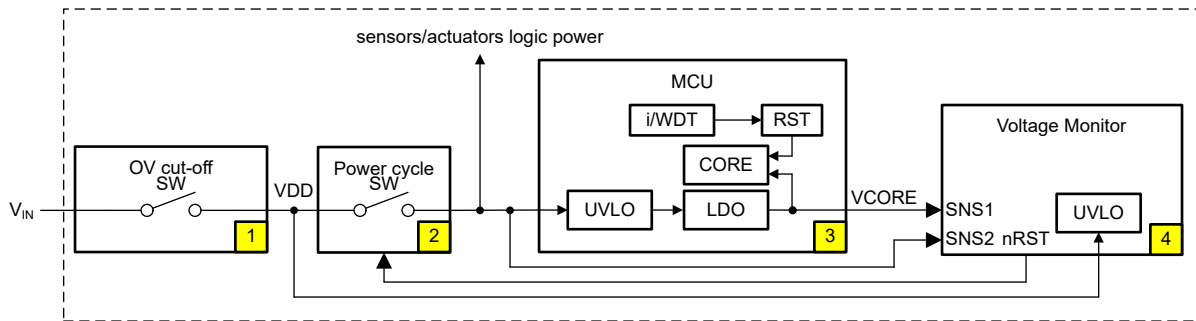


図 2-3. 実装ブロック図

次の表に、アーキテクチャ設計要素の説明を示します。

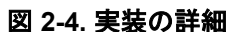
要素 ID	要素名	説明
1	OVP 遮断	電源の遮断機能を備えた過電圧モニタ
2	パワー サイクル遮断	V _{CORE} UV/OV フォルトに対処するためのマイコンのパワー サイクル
3	マイコン	プログラム コードを実行するマイコン
4	電圧モニタ	マイコンのコア電圧の監視

2.5.2.1 設計パラメータ

表 2-1 に、アプリケーション サブシステムの設計パラメータを示します。

表 2-1. パラメータ

設計パラメータ	パラメータ値
電圧入力範囲 (V _{IN})	3.3V ± 約 3%
入力電流	10mA + センサまたはアクチュエータ回路
過電圧保護回路	
過電圧保護の電圧スレッショルド	3.9V ± 約 5%
故障入力電圧、最大	42V
故障対応時間、最大	7μs
リセット時間遅延、標準	250μs
マイコン電圧監視 (V _{DD} および V _{CORE})	
故障応答時間 (V _{CORE} および V _{DD})、最大	750ns
V _{CORE} OV スレッショルド	1.40V ± 7.5mV
V _{CORE} UV スレッショルド	1.29V ± 7.5mV
V _{DD} OV スレッショルド	3.50V ± 0.5%
V _{DD} UV スレッショルド	2.65V ± 0.5%
マイクロプロセッサ	
統合 LDO 出力電圧範囲 (最大)	1.30V ~ 1.39V
V _{CORE} 動作範囲 (最大)	1.27V ~ 1.42V



TPS388R02-Q1 モニタは $\pm 7.5\text{mV}$ の精度を実現し、UV または OV フォルトを検出するとマイコン パワーダウン イベント (NRST low) をトリガして、 V_{CORE} が有効範囲に戻るまでこの状態を保持します。デバイスは 2 つの動作モードをサポートします。全動作温度範囲において最大入力リーク電流 75nA で $0.2\text{V} \sim 1.475\text{V}$ の範囲を 5mV 刻みで微調整できるモード 1X と、全動作温度範囲において 1.35V 時に最大リーク電流 $4.3\mu\text{A}$ で $0.8\text{V} \sim 5.5\text{V}$ の範囲を 20mV 刻みで微調整できるモード 4X。

V_{CORE} の測定にはモード 1X を使用してください。このモードではスレッショルドの粒度が細かく、UV 設定として 1.28V 、 1.285V 、 1.29V 、OV 設定として 1.40V 、 1.405V 、 1.41V を選択できるためです。さらに、モード 1X はリーク電流が少ないため、製品のライフサイクル全体にわたり、バイパスコンデンサや PCB に起因する他のリーク電流要因に対して、十分な許容マージンを確保できます。一方、モード 4X におけるスレッショルドは、UV が 1.28V 、OV が 1.40V となります。

V_{CORE} バイパス コンデンサの標準値は 470nF です (MSPM0G310x-Q1 データシートを参照)。コンデンサの容量を大きくするとノイズ耐性が向上しますが、下の表に示すように、 V_{DD} バイパス要件、ブート時間、UV/OV 検出時間に影響します。

V_{CORE} ピンコンデンサ (C4)	ブート時間	V_{DD} ピンコンデンサ (C3)	UV および OV 検出時間
470nF	$300\mu\text{s}$	$10\mu\text{F}$	$1\mu\text{s}$
$2.34\mu\text{F}$	$450\mu\text{s}$	$50\mu\text{F}$	$5\mu\text{s}$
$4.7\mu\text{F}$	$600\mu\text{s}$	$100\mu\text{F}$	$10\mu\text{s}$

より大きいバイパス コンデンサと、LDO の出力電圧範囲 (UV が 1.29V 、OV が 1.40V) に近い監視スレッショルドを組み合わせることは、UV と OV の障害検出時間を短縮し、監視対象のレールの電圧異常に対してより迅速な応答を可能にします。

V_{CORE} が許容範囲を外れた場合、MSPM0G3107-Q1 のフル パワー サイクルが必要となります。このイベント中、NRST がアサート (low) され、TPS22919-Q1 はマイコンへの電源供給を遮断します。NRST と ACT は接続されているため、NRST が Low になると TPS388R02-Q1 も非アクティブになります。

その後、TPS388R02-Q1 はプリセットされた NRST 遅延時間を待ってから、NRST (high) をデアサートします。この遷移により、TPS388R02-Q1 (ACT high) が再度アクティブになります。TOUT_SEQ 時間が経過した後 (TPS38800-Q1 および TPS388R0-Q1 データシートを参照)、デバイスは通常動作に復帰します。

有効なマイコンのパワー サイクルを成立させるには、 V_{DD} が 0.9V 未満の状態を少なくとも $100\mu\text{s}$ 維持する必要があります。 V_{CORE} (C5) と V_{DD} (C4) に対して選択した容量値に応じて、TPS388R02-Q1 のリセット遅延時間と放電抵抗 R6 のサイズを決定し、それに応じて適切なパワー サイクル動作を実現します。

この回路には、パワー サイクル イベント中に V_{DD} が Low に低下したことを検出するための専用測定方法は組み込まれていません。この機能が必要な場合は、TPS22919-Q1 の出力が上昇し続ける間に NRST ノードが HIGH に遷移しないようにすることで、マルチポイントフォルトに対処します。

2.5.3 監視メカニズム

2.5.3.1 保護機能を備えた VIN 電源レールの OV フォルトの監視

V_{IN} 電源レールを監視するため、OVP 回路が実装されています。入力電圧がスレッショルドである 3.9V を超えると、OVP 回路が作動してアプリケーションを電源から自動的に切断し、過電圧による損傷を防ぎます。

2.5.3.2 マイコン電源電圧の UV または OV フォルトの監視

TPS388R02-Q1 デバイスは、マイコン V_{DD} と V_{CORE} の両方の電源レールに対して、UV/OV を継続的に監視します。デバイスがいずれかのレールで UV または OV フォルトを検出すると、デバイスは安全状態に遷移して、異常な電圧状態でシステムの整合性を維持します。

2.5.3.3 CPU 処理ユニット プログラム フローの監視

プログラム フロー監視は、ウィンドウ付きウォッチドッグ タイマ (WWDT) と独立ウォッチドッグ タイマ (IWDG) という 2 つの内蔵ウォッチドッグ タイマによって行われます。IWDG は専用の独立したクロックソースで動作するため、メイン CPU クロックから独立したクロック供給が可能となり、障害検出範囲が向上します。マイコンとウォッチドッグ タイマの物理的な分離

が必要な場合は、TPS388C02-Q1 バリエーションを使用してください。このデバイスにはウィンドウ付きウォッチドッグが外部デバイスに内蔵されています。

2.5.4 FMEA

要素	サブ要素	サブ要素の機能	故障モード	故障の影響	SGV	故障原因	故障の制御または検出手段
マイコン	CPU	SW の実行	命令フローの未実行 意図しない命令フロー 命令フローのタイミング異常	意図しないプログラムの実行	SPF	アルファ粒子または内部故障	(独立した) 内蔵または外部ウィンドウ付きウォッチドッグ タイマ
マイコン	CPU	SW の実行	命令フロー実行結果の誤り	演算の誤り、プログラム シーケンスの誤り、SP の誤りなど。	SPF	アルファ粒子または内部故障	妥当性チェック、ソフトウェア テスト機能、組み込みのチェック機能
マイコン	ウォッチドッグ	マイコンのプログラム シーケンスの監視	タイミング異常時にウォッチドッグがリセットされない	誤ったプログラムの実行	MPF	ウォッチドッグ フォルト	なし
マイコン	ウォッチドッグ	マイコンのプログラム シーケンスの監視	タイミング正常時にウォッチドッグがリセットされる	安全状態への遷移	SF	ウォッチドッグ フォルト	-
マイコン	LDO	コア電圧の生成	仕様外の電圧 (UV または OV)	コア電圧の範囲外	SPF	リファレンスドリフト、PFET 短絡/オープン	外部電圧モニタ
マイコン	UV ロックアウト回路	V _{DD} が UVLO 電圧を下回った場合にマイコンをリセット	マイコンのリセットなし	マイコンが無効な V _{DD} (および V _{CORE}) で動作	MPF	内部故障	電圧モニタでの冗長な UVLO 回路と V _{DD} センシング
OV 遮断	電圧モニタ	VIN の過電圧を監視	モニタが過電圧を検出しない /RST がアサートされない	ダウンストリームのデバイスでの過電圧	MPF	抵抗またはリファレンスドリフト/オープン/短絡	なし
OV 遮断	電圧モニタ	VIN の過電圧を監視	モニタが過電圧を誤って検出 / RST が誤ってアサートされる	安全状態への遷移	SF	抵抗またはリファレンスドリフト/オープン/短絡	-
OV 遮断	スイッチング素子	アプリケーションから電源を切り離す	スイッチがオープンにならない	ダウンストリームのデバイスでの過電圧	MPF	抵抗ドリフト/オープン/短絡、BJT 短絡故障	なし
OV 遮断	スイッチング素子	アプリケーションから電源を切り離す	スイッチがクローズにならない	安全状態への遷移	SF	抵抗ドリフト/オープン/短絡、BJT オープン故障	-
電圧モニタ	VMON チャンネル	V _{CORE} の電源モニタ	モニタが UV または OV フォルト時に NRST をアサートしない	V _{CORE} の範囲外:	MPF	内部障害、リファレンスドリフト	BIST
電圧モニタ	VMON チャンネル	V _{CORE} の電源モニタ	モニタが誤って UV または OV を検出	MCU パワー サイクル	SF	内部障害、リファレンスドリフト	-
電圧モニタ	VMON チャンネル	V _{DD} の電源モニタ	モニタが UV または OV フォルト時に NRST をアサートしない	V _{DD} の範囲外:	MPF	内部障害、リファレンスドリフト	BIST
電圧モニタ	VMON チャンネル	V _{DD} の電源モニタ	モニタが誤って UV または OV を検出	MCU パワー サイクル	SF	内部障害、リファレンスドリフト	-
電圧モニタ	UV ロックアウト回路	V _{DD} が UVLO 電圧を下回った場合にマイコンをリセット	NRST がアサートされない	V _{CORE} 監視なしでマイコンが動作	MPF	内部故障	マイコンでの冗長 UVLO 回路と V _{DD} センシング
電圧モニタ	I/O 回路	NRST のアサート、回路の有効化	NRST 未アサート、ACT オープン	デバイスが監視しない (バイパス)	MPF	内部故障、ACT ピン オープン	なし
ロード スイッチ	スイッチング素子	V _{DD} をマイコンに接続	コマンド実行時にスイッチがオープンしない	マイコンがパワーダウンしない	MPF	Stuck-at 故障、制御ピンのオープン	なし
ロード スイッチ	スイッチング素子	V _{DD} をマイコンに接続	コマンド実行時にスイッチがクローズしない	マイコンがパワーアップしない	SF	Stuck-at 故障、制御ピンのオープン	-

2.5.4.1 安全メカニズム

システム内には、ランダム ハードウェア障害を検出して対処するための複数の安全メカニズムが実装されます。以下のサブセクションでは、各メカニズムについて詳しく説明します。

2.5.4.1.1 SM1:MSPM0G3107-Q1 の BIST およびソフトウェア テスト

MSPM0G3107-Q1 には、巡回冗長検査 (CRC)、誤り訂正コード (ECC)、ウィンドウ付きウォッチドッグ タイマ (WWDT)、独立ウィンドウ付きウォッチドッグ タイマ (IWDT) などの安全メカニズムが組み込まれています。さらに、安全関連アプリケーション コンポーネントをテストし、追加の内部故障を検出するために、フォルトトレラント時間間隔 (FTTI) 内でソフトウェア ルーチンを定期的に行います。詳細については、『MSPM0G3x0x-Q1 機能安全マニュアル』を参照してください。

2.5.4.1.2 SM2:TPS388R02-Q1 の BIST および内部フォルト検出

起動時に、TPS388R02-Q1 は自動的に BIST を実行し、内部の機能の整合性を検証します。診断機能は、BIST メカニズムに応じて、連続的、周期的、または単発的に実行できます。故障を検出すると、TPS388R02-Q1 は NRST 信号をアサートしてマイコンをリセットし、安全状態に移行させます。詳細については、『TPS388 機能安全情報』(ご請求に応じて利用可能) を参照してください。

2.5.4.1.3 SM3:MSPM0G3107-Q1 の V_{CORE} 監視

MSPM0G3107-Q1 の V_{CORE} 電源レールは、マイコン コア電圧が規定の安全動作範囲内に維持されるよう、TPS388R02-Q1 によって UV/OV 状態が常時監視されています。この安全メカニズムは、TPS22919-Q1 によってパワー サイクルを開始します。

2.5.4.1.4 SM4:MSPM0G3107-Q1 の V_{DD} 監視

MSPM0G3107-Q1 の V_{DD} 電源レールは、TPS388R02-Q1 によって UV/OV フォルトを継続的に監視されます。この安全メカニズムは、TPS22919-Q1 によってパワー サイクルを開始します。

さらに、MSPM0G3107-Q1 の内蔵電圧低下リセット (BOR) 回路は、 V_{DD} 電圧が規定のスレッシュホールドを下回った際にマイコンをリセット状態に移行させることで、二次保護層として機能します。

2.5.4.1.5 SM5:過電圧保護

VIN 電源レールの過電圧保護は、次の 2 つの動作範囲にわたって実装されています。

3.5V より上: TPS388R02-Q1 は、TPS22919-Q1 ロード スイッチと組み合わせて、MSPM0G3107-Q1 をオフにして、定義された安全電圧ウィンドウの外側での動作を防止します。

3.9V より上: TPS3842C011-Q1 は V_{IN} レールを監視し、入力電圧が公称 3.9V に達するかそれを上回ると、電源をアプリケーションから自動的に切断します。

2.6 技術的安全性要件

2.6.1 安全目標 SG_01 に対する FMEDA

部品名	故障率 / FIT	安全関連部品であるか。	故障モード (FM)	FM 分布	FM は、安全メカニズム (SM) なしで SG に違反する可能性があるか。	SM が FM による SG 違反を阻止しているか？	SG 違反に関する FM カバレッジ	残留故障率および SPF 故障率 / FIT	FM が SG に違反する事象と、別の構成要素の独立した故障が組み合わさったものですか？	検出手段は何か。SM は潜在 FM を防いでいるか。	潜在故障に関する FM カバレッジ	潜在的なマルチポイントフォールの故障率 / FIT
M0G3107QRGZRQ1	制限	はい	永久的	100%	X	SM1、SM3-5	>90%	制限	X	SM1	> 90%	制限
	制限		過渡	100%	X	SM1、SM3-5	> 99%	制限	X	SM1	100%	0
TPS388R02001RTERQ1	制限	はい	永久的	100%					X	SM2	99.71%	制限
	制限		過渡	100%					X	SM2	100%	0
TPS3842C011-Q1	3	はい	リセットが作動しない	35%					X	-	0%	1.05
			リセットの誤作動	25%								
			仕様外のリセット作動	30%					X	-	50%	0.45
			仕様外のリセット遅延	10%						-		
TPS22919-Q1	3	はい	VOOUT がオンに固定	25%					X	-	0%	0.75
			VOOUT オープンまたはハイインピーダンス	25%								
			仕様外の VOOUT	35%	X	SM4	99%	0.011				
			QOD がオンに固定	5%								
			QOD がオフに固定	5%					X	-	0%	0.15
			ピン間短絡	5%					X	SM2	100%	0
Q1	4	はい	短絡	80%					X	-	0%	3.2
			オープン	20%								
R1	0.2	はい	オープン	40%					X	-	0%	0.08
			ドリフト	60%					X	-	50%	0.06
R2	0.2	はい	オープン	40%								
			ドリフト	60%					X	-	50%	0.06
R3	0.2	はい	オープン	40%					X	-	0%	0.08
			ドリフト	60%								
R4	0.2	はい	オープン	40%								
			ドリフト	60%								
R5	0.2	はい	オープン	40%								
			ドリフト	60%								
R6	0.2	はい	オープン	40%					X	-	0%	0.08
			ドリフト	60%								

部品名	故障率 / FIT	安全関連部品であるか。	故障モード (FM)	FM 分布	FM は、安全メカニズム (SM) なしで SG に違反する可能性があるか。	SM が FM による SG 違反を阻止しているか？	SG 違反に関する FM カバレッジ	残留故障率および SPF 故障率 / FIT	FM が SG に違反する事象と、別の構成要素の独立した故障が組み合わさったものですか？	検出手段は何か。SM は潜在 FM を防いでいるか。	潜在故障に関する FM カバレッジ	潜在的なマルチポイントフォルトの故障率 / FIT
C1	2	はい	短絡	65%								
			オープン	10%					X	SM4	99%	0.002
			ドリフト	25%								
C2	2	はい	短絡	65%								
			オープン	10%					X	SM4	99%	0.002
			ドリフト	25%								
C3	2	はい	短絡	65%								
			オープン	10%								
			ドリフト	25%								
C4	2	はい	短絡	65%								
			オープン	10%	X	SM4	99%	0.002	X	SM4	100%	0
			ドリフト	25%								
C5	2	はい	短絡	65%								
			オープン	10%	X	SM4	99%	0.002	X	SM4	100%	0
			ドリフト	25%								

2.6.1.1 備考

FMEDA の表の構成は、ISO 26262-5:2018 付録 E に示されている計算例に基づいています。

MSPM0G3107-Q1 および TPS388R02-Q1 は、ISO 26262 適合デバイスであり、必要に応じて完全な FMEDA を入手可能です。両デバイスのダイの FMEDA の結果は、上に示されたシステムレベルの FMEDA に統合されています。

TPS3842C011-Q1 は、機能安全対応デバイスに分類されています。詳細な機能安全資料については、『TPS3842-Q1 機能安全平均故障率 (FIT)、故障モード分布 (FMD)、およびピンの故障モード解析 (FMA)』を参照してください。

抵抗、コンデンサ、トランジスタの FIT 発生率および故障モード分布は Birolini (2017) の『信頼性工学』から引用しています。

OVP 回路の作動は、接続された電源が過電圧イベントを発生させることが条件となりますが、2 重故障シナリオにおける最初の故障となります。OVP 回路はこのような故障条件下でのみ動作するため、テスト回路が実装されていない場合、通常のシステム動作中の正常な動作を検証することはできません。この挙動は、ISO 26262 機能安全規格にある潜在故障の定義を満たしています。

特定の検出メカニズムが存在しないパラメータドリフトなど、一般的な故障モードに対しては、50% の診断カバレッジが適用されます。これらの故障モードについては、安全側故障 50%、危険側故障 50% の均等配分が想定されています。

FMEDA の適用範囲は、ダイの FMEDA にのみ限定されます。ピンの FMEDA は、特定のシステム実装に応じて、デバイスごとに個別に実施する必要があります。

2.6.2 定量的な結果

上記の FMEDA の表は、サブシステムに関する以下の機能安全の結果を示しています。

IEC/TR 62380 に基づく	ダイ	
	永久的	過渡
単一点障害指標 - SPFM	>99%	>99%
潜在故障指標 - LFM	>70%	NA

3 まとめ

提案された設計は、MSPM0G3107-Q1 を使用して ISO 26262 の ASIL B までの適合を達成するために必要な、システムレベルの機能安全要件を満たしています。このシステム設計により、特定のシステムが ASIL B に適合しているかどうか判断されます。ここに記載した FMEDA の結果は、最終製品の機能安全アセスメントをサポートするために上位システムの FMEDA に組み込んで使用することを前提としています。

4 参考資料

1. テキサス インスツルメンツ、『[車載アプリケーションにおける MSPM0 マイコンの利点](#)』、技術白書
2. テキサス インスツルメンツ、『[MSPM0G3x0x-Q1 機能安全マニュアル](#)』、機能安全マニュアル
3. テキサス インスツルメンツ、『[MSPM0 G シリーズ 80MHz マイコン テクニカル リファレンス マニュアル](#)』、ユーザー ガイド
4. テキサス インスツルメンツ、『[TPS388 機能安全情報](#)』(ご請求に応じて利用可能)
5. テキサス インスツルメンツ、『[TPS3842-Q1 機能安全平均故障率 \(FIT\)、故障モード分布 \(FMD\)、およびピンの故障モード解析 \(FMA\)](#)』、機能安全情報
6. Alessandro Birolini, 信頼性の高いエンジニアリング、第 8 版、ISBN 978-3-662-54208-8
7. テキサス インスツルメンツ、『[CAN-FD インターフェイスを搭載した MSPM0G310x-Q1 車載混合信号マイコン](#)』、データシート
8. テキサス インスツルメンツ、『[TPS38800-Q1/TPS388R0-Q1 マルチチャネル過電圧および低電圧 I2C プログラマブルな電圧スーパーバイザ](#)』、データシート
9. テキサス インスツルメンツ、『[ISO26262 準拠の MSPM0x デバイスの事前フィルタリング済みリスト](#)』、Web ページ
10. テキサス インスツルメンツ、『[ASIL B 要件に対する MSPM0 外部 VCore 監視](#)』、アプリケーションノート

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](#) 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