車載および産業機器における機能安全認定の合理化

Miro Adzan（ミロ・アザーン）
部門責任者
産業用システム
ファクトリ・オートメーション/制御
テキサス・インスツルメンツ

Arun Vemuri（アルン・バムーリ）
部門責任者
車載用システム
車体/ライティング
テキサス・インスツルメンツ

機能安全設計では、正しい設計のために厳密性、情報管理、時間が必要となります。このホワイト・ペーパーでは、工場向けに設計しているか、高速道路向けに設計しているのかにかかわらず、集積回路 **(IC)** の設計に対する **TI** のアプローチが、機能安全設計の効率化に必要なリソースをどのように提供するかについて説明します。

オートメーションが産業分野と自動車分野の両方で機能安全の必要性を増大させています。機能安全は、産業用アプリケーション全体で必要ですが、特にファクトリ・オートメーションと制御システムで必要となります。

自動車業界では、エアバックおよびブレーキ・システムには長年にわたって機能安全が考慮されてきましたが、電動化比率や自律的運転機能の増加に伴い、バッテリ・マネージメント、センサ・フュージョン、車両操作を制御するシステムが求められ、機能安全を利用した設計の必要性が高まっています。

工場向けロボット・システム、家庭向け家電製品、将来の自動車のいずれを設計しているのかにかかわらず、設計エンジニアは、アプリケーションに関連する機能安全規格に従ったプロジェクトを提供する必要性が増しています。

基準への準拠が必要ないアプリケーションでは、安全性の高いシステムの設計が競合他社に対する重要な差別化要因となります。

機能安全規格

機能安全はシステム全体の安全性の一部であり、特定の入力や障害状態に対して予測可能な形で応答できるかどうかによって決まります。機能安全規格では、常に危険があること、そのためすべてのシステムが本質的に故障率を持つことを前提とします。

機能安全規格では、リスクを許容可能な水準に下げることができる方法でシステムを開発する方法を指定します。機能安全を考慮したシステム設計では、誤動作のリスクを下げるだけではなく、障害を検出し、その影響を抑える必要もあります。

機能安全への準拠を実現するためにエンジニアは次のことを行う必要があります。

- 危険な状況を予測し定義する。
- これらの状況に対処する安全機能を特定する。

- 安全機能によって実現されるリスク削減を評価する。
- 安全機能が設計目的に対して実施されていることを確認する。

標準化機関によって定義された機能安全規格は、関連業界の企業からの協力とともに、システム内の安全機能の定義を支援し、安全性レベルの評価に関する仕様を設定することにより、設計者をサポートします。テキサス・インスツルメンツ (TI) の標準化機関への参加は、企業が最初から機能安全を考慮して製品を開発できるようにすることに役立っています。

共通の安全基準には、産業用アプリケーションに対する国際電気標準会議 (IEC) 61508、車載アプリケーションに対する国際標準化機構 (ISO) 26262、および家電製品に対する IEC 60730 が含まれます。

安全基準には、共通のリスク削減レベルおよびセーフティー・インテグリティ・レベル (SIL) があります。たとえば、IEC 61508 で定義されるように SIL では SIL 1 から SIL 4 までの範囲があり、SIL 4 が最も厳しくなっています。SIL 1 は、安全の有効性 90% ～ 99%、機能失敗平均確率 (PFDavg) 0.1 ～ 0.01、およびリスク低減係数 (RRF) 10 ～ 100 を必要とします。SIL 4 は、安全の有効性 99.99% 超、PFDavg 0.0001 ～ 0.00001、および RRF 10,000 ～ 100,000 を要求します。

ISO 26262 では同様の ASIL A から ASIL D までの範囲があり、ASIL D が最も厳しくなっています。

機能安全プロセス

代表的な機能安全開発プロセスは、危険および機能安全の目標を決定することによって始まります。エンジニアは、通常、システム・アーキテクチャ、モジュール、IC を調査することから始めます。機能安全規格準拠システムの主要構築ブロックとなるのは IC です。

システム動作を予測するために、エンジニアはモジュールの作動を数量化して予測する必要があります。これを達成するには、さまざまな故障モード、その原因とその影響を特定するために、開発プロセスの一環として、システムに対して構造化された定性的安全性分析を実施する必要があります。

機能安全規格では、エンジニアが独自の故障モード、影響、および診断分析 (FMEDA) を実施できるように、IC についてエンジニアが必要とする情報を定義しています。IC の複雑性に応じて、システム安全性分析では、設計、ダイ、およびパッケージのそれぞれに依存した情報が必要です。

信頼性の高いサプライヤから正しい製品を選択することは、この試みにおいて重要です。TI では、機能安全規格に準拠することを目的とした設計であれ、競合的に差別化された安全性の高いシステムであれ、エンジニアが製品を見つけ出して使用することを容易にしてきました。

機能安全カテゴリによるデバイス選択の簡略化

典型的な産業用アプリケーションおよび車載アプリケーションでは、複雑性の点で非常に異なる多数の IC が必要となります。1 つまたは複数のセンサとアクチュエータ、センサからのデータを処理するマイコン (MCU) またはプロセッサ、アナログ・マルチプレクサ、オペアンプまたは計装アンプ、プロセッサと統合される場合もあればされない場合もある A/D コンバータ (ADC) と D/A コンバータ、DC/DC コンバータ、低ドロップアウト・レギュレータまたはパワー・マネージメント IC (PMIC)、さらにドライバ部品 LED ドライバ、モーター・ドライバ、ソレノイド・ドライバ、電界効果トランジスタ (FET)、絶縁型ゲート・バイポーラ・トランジスタ・ゲート・ドライバなど) およびパワー・スイッチとロード・スイッチなど広範囲にわたります。さらに、アプリケーションには、RS-485、コントローラ・エリア・ネットワーク (CAN)、イーサネット、

		機能 安全対応	機能 安全品質管理	機能 安全準拠
開発プロセス	TI の品質管理プロセス	✓	✓	✓
	TI の機能安全プロセス			✓
分析レポート	機能安全 FIT 率の計算	✓	✓	✓
	故障モード分布 (FMD) やピン FMA**	✓	FMEDA に含まれています	FMEDA に含まれています
	FMEDA		✓	✓
	フォールト・ツリー解析 (FTA)**			✓
診断の説明	機能安全マニュアル		✓	✓
認証	機能安全製品証明書***			✓

表 *1.* 機能安全設計における製品に対する *TI* カテゴリ

** アナログ電源とシグナル・チェーン製品でのみ利用できます。

*** 一部の製品で利用可能です。

FPD-Link、PCIe (Peripheral Component Interconnect Express、ペリフェラル・コンポーネント・インターコネクト・エクスプレス）などの通信インターフェイスが含まれます。

表 **1** には、機能安全設計を提供する TI の製品カテゴリが示されています。ここでは、標準ベースの IC の複雑性カテゴリの背後にあるロジックを反映しています。カテゴリは、TI 機能安全対応、TI 機能安全品質管理、および TI 機能安全準拠となっています。

機能安全準拠製品

これらの製品は、多くの場合、MCU やプロセッサまたはアナログ・モーター・ドライバなど、十分に複雑な独立したシステムであり、安全機能を内蔵している可能性があります。

TI は、これらの製品を TÜV (Technischer Überwachungsverein、技術的監査組合）SÜD などの団体によって認証された機能安全開発フローを使って開発しました。この認定により、このカテゴリの製品が機能安全規格 ISO 26262 および IEC 61508 に記述された仕様に従って開発されたことを確認できます。

たとえば、次の機能安全準拠デバイスです。

- 車載電子部品評議会 (AEC)-100 認定 Jacinto™ TDAx システム・オン・チップ（先進運転支援システム向け）は、固定 / 浮動小数点デジタル信号プロセッサ（DSP）である TMS320C66x 世代のコア、Vision AccelerationPac 組込みビジョン・エンジン (EVE)、デュアル ARM® Cortex®-M4 プロセッサ、さらに、低電圧差動信号ベースのサラウンド・ビュー・システム向けのマルチカメラ・インターフェイス、ディスプレイ、CAN、ギガビット・イーサネット・オーディオ・ビデオ・ブリッジングなどのペリフェラルを組み合わせて統合しています。これらのデバイスは、ECC（誤り訂正コード）保護 M4、ECC 保護 32 ビット DDR インターフェイス、各 CPU（中央演算装置）の専用のメモリ管理ユニット、メモリ保護ユニット、温度監視センサ、システム監視用の 8 チャネル ADC など、機能安全システム要件の包括的なリストをサポートします。

- TPS6594-Q1マルチレール電源管理集積回路（PMIC）は、自動車および産業市場でオンチップのTIのJacinto TDAxシステムをサポートします。高精度で柔軟なPMICは、機能安全を必要とする自動車および産業用アプリケーションに適しており、機能安全のドキュメントが付属しています。TPS6594-Q1は、メイン・ドメインとMCUドメインの両方にスケーラブルな電源管理ソリューションを提供し、ASIL-D / SIL-3までの機能安全をサポートします。
- Hercules™ MCU は、エンジニアが最大 SIL 3 を目指すために十分な安全性機能と診断機能を統合しています。これは、MCU が約 99% の故障検出率を達成できるということです。たとえば、MCU 上のロックステップに 2 個の Cortex-R CPU を統合すると、各サイクルの出力の比較ができ、さらに、エラーが発生した場合は、マスク不可能割り込みを生成できます。CPU セルフテストは起動時に、または産業用アプリケーション向けのタイムスライスで実行できます。
- DRV3245E-Q1 は、三相モーター・ドライブ・アプリケーション向けの FET ゲート・ドライバ IC です。その 3 個のハーフ・ブリッジ・ドライバは、それぞれがハイサイドおよびローサイドの N チャネル MOSFET を駆動できます。ISO 26262 の適切な要件に対して設計されたこのゲート・ドライバは、各内部ブロックに対する診断と保護を統合し、一般的なシステム診断チェックのサポートを提供します。各チェックの結果は、それぞれシリアル・ペリフェラル・インターフェイスを介して報告されます。この機能のフレキシビリティにより、DRV3245E-Q1 は多くの安全性アーキテクチャにシームレスに統合できます。
- TPS65381A-Q1マルチレールPMICは、TIのHercules TMS570およびC2000™をサポートしています。自動車および産業市場のMCUファミリは、デュアルコア・ロックステップまたは疎結合アーキテクチャを備えています。FET内蔵、非同期バックスイッチモード電源コンバータは、入力電源（バッテリ）電圧を6Vプリレギュレータ出力に変換します。6Vプリレギュレータは、他のレギュレーターに電源を供給します。 電圧モニタ、アナログ内蔵セルフテスト、クロック損失監視、ジャンクション温度監視、電源の電流制限、MCUエラー信号モニタなどの監視および保護ブロックにより、診断範囲が改善され、検出されない障害率が減少します。
- TI はこのカテゴリでさらに多くのデバイスを提供します。C2000 リアルタイム・コントローラおよび AWR1843 76GHz ～ 81GHz 車載レーダー・センサ（オンボードのDSP、マイコン、レーダー・アクセラレータ搭載）などがあります。これらすべての製品には、システム開発プロセスをサポートする専用の機能安全関連資料が付属しています。
  - 機能安全の時間あたりの故障回数 (FIT) 率の計算。
  - 故障モード分布 (FMD)。
  - FMEDA。
  - フォールト・ツリー解析。
  - IC の安全機能、および外部コンポーネントを使用して故障検出率と診断を実現する方法について説明する機能安全マニュアル。
  - 機能安全製品証明書。

機能安全品質管理製品

この 2 番目のカテゴリの製品は、診断機能を内部に持ち、機能安全を必要とするシステムのために特に設計された複雑な製品で構成されています。ただし、この製品カテゴリは、機能安全準拠製品カテゴリで使用される認証された機能安全開発フローに従って開発される代わりに、TI 全体での標準品質管理開発フローを使用しています。

このカテゴリの製品例：

- TCAN4550-Q1は、CAN FDコントローラとトランシーバを統合した車載システム・ベースチップ（SBC）です。高度に統合されたこのデバイスは、既存のSPIポートを利用してCAN FDバスの拡張を簡素化するため、設計者は、より広い帯域幅のCAN FDインターフェイス・プロトコルにアップグレードするときに、現在のマイコン・ベースのアーキテクチャを維持できます。
- LP87702-Q1は、デュアルウォッチ・コンバータと5Vブーストで、ウィンドウ・ウォッチドッグと、独自の出力電源と2つの外部電源を監視する独立した電圧リファレンスを含む、ASIL準拠のmmWaveレーダーシステムに必要な診断機能が統合されています。

機能安全準拠製品と同様に、機能安全システム設計に役立つ広範囲な関連資料を提供します。それらには、機能安全 FIT 率の計算、FMEDA、機能安全性マニュアルが含まれていますが、機能安全準拠製品とは異なり、フォールト・ツリー解析または製品認定は含まれません。

機能安全対応製品

製品の 3 番目のカテゴリは、機能安全品質管理製品カテゴリと同様に TI の標準品質管理開発フローを使用して開発される、より簡略な IC で構成されています。

機能安全対応製品は、通常、統合型の安全機能を持たないため、 TI の他の機能安全製品カテゴリのデバイスでは一般的である、内部監視および診断機能を持ちません。

製品に統合された包括的な安全機能を持たないため、他のカテゴリのデバイスのような内部監視および診断機能がありません。

これらは機能安全システムにとって依然として重要なビルディング・ブロックであるため、TI は設計者が安全性分析に使用できるように、機能安全性 FIT 率や FMD などの重要な情報を提供します。

このカテゴリの製品例：

- 業界最小のリニア・サーミスタTMP61-Q1は1%未満のセンサの長期ドリフトと従来のサーミスタに比べ高い精度を実現しています。高精度温度センサTMP235-Q1は較正なしで±1.5°Cを実現し、サーミスタを代替します。
- TPS3840-Q1 電圧スーパーバイザまたはリセット IC。この AEC-Q100 認定デバイスは、1.5V ～ 10V の広い電圧範囲で動作し、消費電流は標準値でわずか 350nA、最大値が 700nA となります。
- TPS7A16A-Q1 AEC-Q100 認定、60V、5μA 静止電流 100mA 低ドロップアウト電圧レギュレータは、連続または散発的（電源バックアップ）バッテリ動作のアプリケーション向けに設計されています。ここでは、超低静止電流が重要となります。このデバイスは、セル数が多いパワー・ツール・パックから車載アプリケーションまでの範囲のマルチセル・ソリューションから低電圧電源を生成するのに最適です。TPS7A16A-Q1 は安定した電圧レールを供給できるだけではなく、電圧過渡に耐えてレギュレーションを維持できます。

TI の開発プロセス

機能安全開発の複雑さにより、企業の安全文化とプロセスについて TÜV SÜD 認定以外の情報がさらに必要になる場合があります。これが、決定論的原因による障害とランダム障害の両方を管理する開発プロセスを TI が作成した理由です (p.7の表2を参照)。

TI では全製品について品質管理開発フローを遵守することにより、決定論的原因による故障の確率を低下させます。この標準的な開発プロセスでは、p.8の図1 に示すように、決定論的な故障の管理に必要とされる多くの要素を採用しています。さらに、ISO 26262-4 または IEC 61508-2 に準

評価	計画	設計	検証	維持および寿命終了
機能安全プロセスの実行が必要かどうかを判断する	部品のターゲット SIL/ASIL 機能を定義する	部品レベルの機能安全要件を策定する	SILicon の機能安全設計を検証する	すべての報告された問題を文書化する（必要な場合）
機能安全マネージャを任命する	機能安全計画を作る	機能安全要件を設計仕様に含める	機能安全設計の特性を決定する	動作の維持に関するインシデント・レポートを実施する（必要な場合）
段階終了の監査	機能安全ケースを確認する	設計仕様を確認する	機能安全設計を認証する（AEC-Q100 により）	作業成果物を更新する（必要な場合）
	機能安全ケースを開始する	機能安全設計を開始する	機能安全ケースをまとめる	
	対象アプリケーションを分析してシステム・レベルの機能安全の想定を行う	設計の定性分析（故障モード分析）を実施する	プロジェクトの評価を実施する	
	段階終了の監査	定性分析を確認する	機能安全性マニュアルをリリースする	
		機能安全設計を確認する	機能安全分析レポートをリリースする	
		設計の定量分析 (FMEDA) を実施する	機能安全レポートをリリースする	
		定量分析を確認する	段階終了の監査	
		必要に応じて機能安全設計を繰り返す		
		段階終了の監査		

表 *2.* 機能安全アクティビティは *TI* の標準開発プロセスの上位に置かれます。

拠した車載用システムや産業用システムをはじめ、最終アプリケーションで幅広い規格への準拠を支援するために、これらの製品の資料とレポートを活用できます。

このプロセスでは開発を 3 つの段階に分けます。

- 評価 。
- 計画 。
- 設計 。
- 検証 。

TI の機能安全開発フローは、ISO 26262 と IEC 61508 から派生したものです。3 つの標準ベースの IC 複雑性カテゴリを開発するために、標準的な新しい製品開発プロセスの各段階に機能安全固有のアクティビティをいくつか追加しました。

ISO 26262-2:2018 の付属書 A にあるように、TI の開発プロセスは、機能安全の効果的な達成をサポートおよび推進しています。開発プロセスは、製品開発に携わるすべてのチーム間での機能安全関連情報のやりとりを促進します。

TI チームは適切な基準に従って機能安全に関する組織固有のルールを維持し、TI のプロセスは特定された安全の異常の解決を保証します。業界標準に従うことにより、TI は機能安全をサポートする品質管理システムを維持することで顧客をサポートします。

広がる機能安全製品ラインアップ

機能安全設計では、コンセプト段階の直後から危険性、故障、低減の計画を立てることに重点を置いています。これには、故障および実装された診断計画の有効性に関する規格に準拠したシステム分析が含まれます。 システムの構築に投入されるあらゆる製品についてのデータを中心に展開します。

TI では、関連製品を継続的に開発し、これらの製品に関する必要なデータと関連資料をすべて機能安全アプリケーションで利用できるようにすることで、これらのニーズに対応できるように支援します。

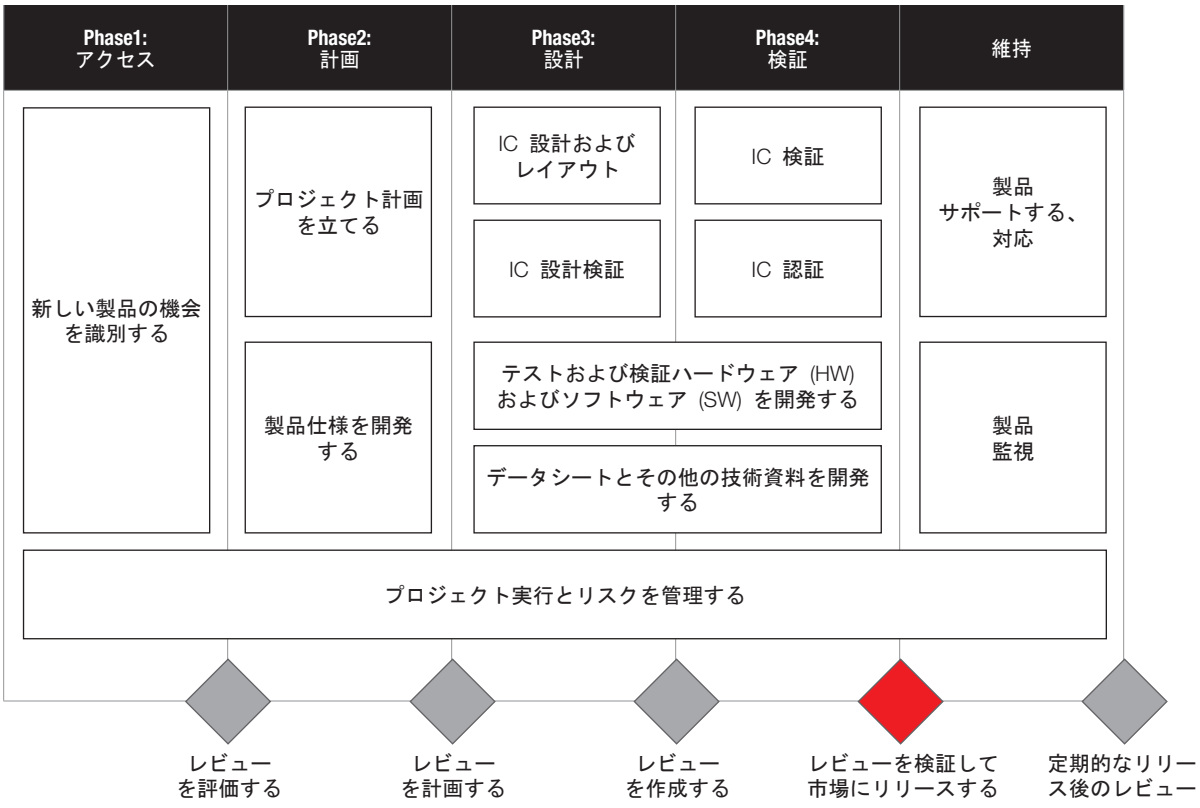

図 *1.* 追加の機能安全アクティビティが存在する場合がある標準的な品質管理開発プロセス。

TI 機能安全技術の詳細

関連資料

- Video: Understanding Functional Safety and System-Level Fault Detection of an ADC.
- Video series: Functional Safety on C2000™ MCUs.
- White paper: Actuator Design Trends for Functional Safety Systems in Electric and Autonomous Vehicles.
- White paper: Leverage Jacinto™ 7 Processors Functional Safety Features for Automotive Designs.
- White paper: C2000™ MCU SafeTI™ Control Solutions: An Introduction to ASIL Decomposition and SIL Synthesis.

重要なお知らせ：ここに記載されているテキサス・インスツルメンツ社および子会社の製品およびサービスの購入には、TI の販売に関する標準の使用許諾契約への同意が必要です。お客様には、ご注文の前に、TI 製品とサービスに関する完全な最新情報のご入手をお勧め致します。TI は、アプリケーションに対する援助、お客様のアプリケーションまたは製品の設計、ソフトウェアのパフォーマンス、または特許の侵害に対して一切責任を負いません。ここに記載されている他の会社の製品またはサービスに関する情報は、TI による同意、保証、または承認を意図するものではありません。

C2000、Hercules、JacintoおよびSafeTIは、Texas Instrumentsの商標です。 その他の商標および登録商標はそれぞれの所有者に帰属します。

© 2020 Texas Instruments Incorporated

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が適用される各種規格や、その他のあらゆる安全性、セキュリティ、またはその他の要件を満たしていることを確実にする責任を、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（www.tij.co.jp/ja-jp/legal/termsofsale.html）、または ti.com やかかる TI 製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。TI がこれらのリソースを提供することは、適用されるTI の保証または他の保証の放棄の拡大や変更を意味するものではありません。

Copyright © 2020, Texas Instruments Incorporated
日本語版 日本テキサス・インスツルメンツ株式会社