車載設計の機能安全に関する Jacinto™ 7 プロセッサ機能の利用

Yashwant Dutt
Engineering Manager
Jacinto™ Processors

Sam Visalli
Functional Safety Manager
Jacinto Processors

Mahmut Cifti
Systems Architect
Jacinto Processors

Dave Maples
General Manager Automotive Gateway and Infotainment
Jacinto Processors

Krishna Gopalakrishnan
Quality Manager
Embedded Processing

Texas Instruments

概要

自律的な運転、コネクテッド・カー、電気自動車/ハイブリッド電気自動車の登場は自動車業界のパラダイムを変えています。これらのテクノロジーの中心となる機能安全はもはや従来のマイコン（MCU）に限定されておらず、アプリケーション・プロセッサでもサポートが必要になっています。エンジン制御ユニット（ECU）の計算要件が増加しているため、アプリケーションのニーズを満たすためにより高性能のプロセッサ、ハードウェア・アクセラレータ、デジタル信号プロセッサ（DSP）が必要になっています。これらのパラメータを考慮すると、既存のコアで安全関連のデータを処理すると共にミックスド・クリティカリティ機能をホストすることはさらに困難になります。ミックスド・クリティカリティ・システムでは、重要度が異なるタスクが1つの共有プラットフォームで実行されます。ミックスド・クリティカリティ・システムでは、安全性の確保が重要となるタスクのタイミングを厳密に保証する必要があります。

車載用TI Jacinto™ 7システム・オン・チップ（SoC）ファミリは、絶縁型ASIL-D安全MCUを内蔵しているだけでなく、すべてのプロセッシング・コア向けにより高いレベルのASIL機能安全も提供します。このホワイト・ペーパーでは、Jacinto 7 SoCファミリに組み込まれた安全性診断について説明します。これには、TDA4xとDRA8xデバイス、ミックスド・クリティカリティ・システムをサポートするさまざまな絶縁メカニズム、ソフトウェア・アーキテクチャ、ソフトウェア製品、包括的なソリューションを構築する方法が含まれます。

機能安全とは

機能安全とは、システムが損害を最小にする仕方でランダム障害、ハードウェア障害、環境ストレスといった誤動作に対応する能力のことです。ISO 26262では、許容できないリスクの不在を意味しています。機能安全の概念は自動車業界でかなりの期間存在していますが、アプリケーション・プロセッサでの対応は始まったばかりです。ASIL-Dに準拠したアプリケーションを念頭に置いて、Jacinto 7プロセッサではこれまでの MCUクラスのデバイスに限定されていた安全性の概念がアプリケーション・プロセッサに導入されました。これらのプロセッサでは、ミックスド・クリティカリティ・システムを実現するハードウェア支援の絶縁技法が使用されます。安全性の確保が重要となるタスクとそうでないタスクの両方を1つのデバイスでシームレスにホストする能力は、システム・コストを低減するのに役立ちます。

Jacinto 7プロセッサ・ファミリは、ハードウェアとソフトウェアの両方を扱う包括的な安全性ソリューションを提供します。ASIL-Dに対応したシステム設計では、TÜV SÜDなどの独立した安全性認証機関が認定したハードウェア開発プロセスが使用されています。ランダム障害を検出できる診断回路が備わっています。ランダム障害は次の3種類の広いカテゴリに分類できます。

- メモリ、クロック、電源、コア、相互接続の回路をテストする基本的な診断。
- 電圧/電源/リセット、ファイアウォール、メモリ管理ユニット（MMU）、マイクロプロセッサ（MPU）の分離などのハードウェア絶縁機能。ASIL-BとASIL-Dなどの重要度が異なる操作をサポートするシステムでFFI（Freedom From Interference）を簡素化します。
- 凍結フレーム検出などの特定用途向けのハードウェア診断。

Jacinto 7プロセッサ・ファミリは、ターゲットとなる最終機器で必要とされるASILレベルでもSEooC（Safety Element out of Context）として外部認定されます。ハードウェア開発プロセスと同様に、ソフトウェア開発プロセスもTÜV SÜDなどの独立した安全性認証機関によって認定されています。安全性要件のあるJacinto 7のソフトウェア・コンポーネントは、ASIL-Dまでの機能安全要件をサポートするように設計されています。ソフトウェア・コンポーネントは外部認定されていません。最終ソフトウェア/システムを認定できる認定サポート・パッケージが備わっています。ソフトウェア診断ライブラリにはオンチップ診断用のサンプルが付属しています。TIは、適合した**ハードウェア**と**ソフトウェア**に機能安全証明書を提供しています。

Jacinto 7プロセッサの重要な安全性アーキテクチャの特徴のひとつは、MCU機能の内蔵です。これにより、システム設計が簡素化され、基盤の部品点数が減り、基盤面積が小さくなります。アプリケーション・プロセッサは2つの独立したドメイン – メイン・ドメインとMCUドメイン – に分離されています。メイン・ドメインは、高性能の計算コア（MPUなど）とGPU（グラフィックス処理ユニット）、マルチメディア、DSPなどのビジョン・ハードウェア・アクセラレータのほか、必要な周辺装置を提供します。MCUドメインは高FFIの安全機能に使用する独立したドメインです。

Jacinto 7プロセッサは安全に準拠したデバイスであり、次のものを含む機能安全関連の資料が付属しています。

- セーフティー・マニュアル。サポートされているJacinto 7プロセッサ・ファミリを使用してセーフティー・クリティカル・システムを構築する方法が記載されています。この資料には、開発プロセス、機能安全アーキテクチャ、実装された機能安全メカニズムの詳細が含まれています。
- 安全性分析レポート。デバイスが機能安全に関して明示された目標を達成する能力に関する情報が記載されています。
- 定量的な機能安全分析（FMEDA[Failure Mode, Effects and Diagnostic Analysis：故障モード影響診断解析]とも呼ばれる）。安全性分析レポートの一部ですが、別個の資料になっています。部品のさまざまな部分に関する詳細が記載されています。診断機能安全メカニズムのカスタマイズ使用に基づく計算を行うのに適しており、FIT、診断範囲、SPFM/LFM、故障モードに関する情報が含まれています。

ソフトウェアの機能安全の概要

ソフトウェアは製品の安全目標全体を達成するうえで重要な要素のひとつです。Jacinto 7ソフトウェアの安全性には次の2つの面があります。

- 安全パスで使用されるソフトウェア・コンポーネントのシステム性能。
- ハードウェア診断用の包括的なソフトウェア・サポートとリファレンス・サンプル・コード。

システム性能について、TIは適切に定義された共通のソフトウェア開発プロセスとツールをさまざまなチームで使用しています。独立したソフトウェア品質組織がソフトウェア製品の承認を行っています。TIの機能安全成果物の全体には次のものが含まれます。

- **プロセスの準拠：**機能安全ソフトウェア開発プロセスは、TÜV SÜDによってISO 26262（ASIL-D）とIEC 61508の認定を受けています。
- **プロジェクトの準拠：**プロジェクトの準拠は内部監査によって保証されており、ISO 26262またはIEC 61508プロセスに照らして実施されています。違反は改善用の計画やアクションによって修正されています。
- **顧客による認証への対応：**安全プロセスを使用して開発されたすべてのソフトウェアには、CSP（Compliance Support Package：コンプライアンス・サポート・パッケージ）が付属しています。CSPに含まれるもの
  - TIの内部監査レポート。
  - 要件、テスト計画とレポート。
  - トレーサビリティ・レポート。
  - 動的コード範囲分析レポート。
  - 静的コード分析/MISRA（Motor Industry Software Reliability Association）Cレポート。
  - 機能安全診断ライブラリと資料。
  - コンパイラ認証キット。
  - ソフトウェアFMEA（Failure Mode and Effects Analysis：故障モード影響解析）レポート。

統合されたJacinto 7 SDK（Software Development Kit：ソフトウェア開発キット）も、安全ソリューションの構築に役立つソフトウェア・サポートを提供しています。システムで「現状のまま」使用されることが想定されているコンポーネントと安全ループの一部であるコンポーネントは、TIの機能安全ソフトウェア開発プロセスに従って開発されています。このプロセスには、すべての主要な安全IPとマイコン抽象化レベル・ドライバ、IPC、DMAなどの機能ソフトウェア用のソフトウェア診断ライブラリが含まれています。

TIは、これらの安全機能をアプリケーションで使用する方法を理解するのに役立つさまざまなリファレンス・サンプルも提供しています。安全機能はアプリケーションごとに異なるため、リファレンス・ソフトウェアは安全プロセスを使用する代わりにTIのベースライン・プロセスに従って開発されています。

表1は、SDKに含まれる診断ソフトウェア、機能ソフトウェア、リファレンス・ソフトウェアのさまざまな例を示しています。

安全アプリケーションのマッピング

データ・センターやモバイル・アプリケーション用に構築された標準的なSoCアーキテクチャには、自動車アプリケーションに必要な安全機能がないため、ソフトウェア・ベースの安全診断を追加するために追加の計算性能が必要になります。Jacinto 7プロセッサ・ファミリのさまざまなハードウェア/ソフトウェア安全機能をエンド・アプリケーションで使用すると、この計算性能の要件を低減できます。

次のページの**図1**に、標準的なビジョン・ベースのシステムを示します。入力カメラ・データはCSI（Camere Serial Interface：カメラ・シリアル・インターフェース）を通じてキャプチャされ、RAWからYUVへの変換用にビジョン処理ハードウェア・エンジンに送信されます。物体の分類や自由空間の検出といったさまざまな分析/ディープ・ラーニング・アルゴリズムは、プロセッサのオンチップC7x DSP、MMA、ARM® Cortex® -A72コアで実行されます。MCUドメインは各ステップのチェッカーのように機能し、処理中のデータを周期的にモニタして検証します。MCUドメインは、他のセンサ入力に基づく安全機能の最終決定を受け取り、CAN（Controller Area Network：コントローラ・エリア・ネットワーク）などの通信プロトコルによって他の自動車ECUに送信します。

ソフトウェア診断	機能ソフトウェア	リファレンス・ソフトウェア
ソフトウェア診断ライブラリ（SDL） – さまざまな安全機能用のソフトウェア機能と応答ハンドラ • さまざまなモジュール用のLBIST/PBIST • CAN、SPIを介した周辺装置 • 安全IP：CRC、ECC、RTI、DCC、ESM • エラーを注入する能力 • システム性能を持つソフトウェア	**安全パス内のコンポーネント** – システムを性能を使用して構築されたSDKコンポーネント • AUTOSAR MCAL（CAN、DIO、SPI、ETH、IPC、ADC、PWM、WDG GPT） • ECC、CRC、DCC、ESM、BIST、VTM、PGD、POK、ADCなどの安全IP用のCSL-FL • SCIクライアント、DMA • SYSFWファームウェア • TI-RTOS • 安全パス内のすべてのIP用のCSL-FL • MMA、TIDLライブラリ • CSI2、VHWA、IPC用のLLD • コンパイラ認証キット	• FFI、メイン/MCUアイランド絶縁、その他の安全機能のサンプル・コード • 使用状況コンテキストでの安全IPの使用法を示すリファレンス・ソフトウェア • セーフティ・マニュアルに記載されている診断を示すリファレンス・ソフトウェア
機能安全ソフトウェア開発プロセス **ソフトウェアCSP（コンプライアンス・サポート・パッケージ）**		標準的なソフトウェア開発プロセス

表1：*ソフトウェア機能安全製品。*

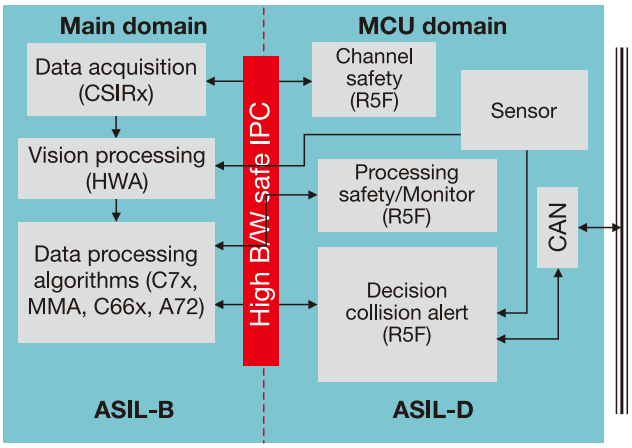

図1：標準的なビジョン処理。

図1の各ブロックはJacinto 7プロセッサのモジュールであり、CPUリソースを使用せずに全体的な安全目標を達成できるようにハードウェア診断が含まれています。**表2**は、前述のビジョン・アプリケーションをマッピングし、Jacinto 7プロセッサ・ファミリと標準的なSoCの安全機能の違いを示しています。

Jacintoプロセッサに対応したパワー・マネージメント・ソリューション

Jacintoプロセッサ・ファミリと並行して、TIは2つの高精度で柔軟なPMIC（Power Management Integrated Circuit：パワー・マネージメントIC）を開発しました。これらは機能安全が要求される自動車アプリケーションに適しており、機能安全関連の資料が付属しています。これらのPMICであるTPS6594-Q1とLP8764-Q1 PMICは、メイン・ドメインとMCUドメインの両方で使用できるスケーラブルなパワー・マネージメント・ソリューションを提供し、ASIL-Dまでの機能安全をサポートします。

安全ドメイン	特長	標準的な車載システム	Jacinto 7プロセッサ・ファミリの利点
• アーキテクチャ	• MCUアイランドの統合 • 異種安全コア	• 外部MCUの使用 • ハイパーバイザーと外部MCUの使用。ハイパーバイザー用に追加のCPU負荷が必要	• システム・コストの最適化 • スケーラブルな安全性能 • ハイパーバイザーを使わないフェイルセーフと回復
• 基本的な安全 • 過渡的な障害と永続的な障	• コア、メモリ、ハードウェア・アクセラレータ用の組み込みセルフテスト • メモリ用のエラー修正コード • ロックステップDMIPS • CRC、ウォッチドッグ、クロック・コンパレータ • 相互接続での安全	• 通常の場合、アプリケーション・プロセッサでは使用不可 • すべてのコアでソフトウェア診断用の追加負荷が発生	• すべてのハードウェアで使用可能 • 追加CPU負荷はごくわずか
• 絶縁 • FFI	• MMU、MPU、ファイアウォール、タイムアウト・ガスケット	• ハイパーバイザ – ソフトウェア・ベースの方式 – 負荷プロセッシング・コア • すべてのコアでソフトウェア診断用の追加負荷が発生	• 安全タスクと非安全タスクのハードウェア絶縁 • 追加CPU負荷はごくわずか
• 安全機能	• ブラック・フレーム • 凍結フレーム • カメラのブロック • ディープ・ラーニング・ネットワーク・パラメータの安全	• ソフトウェア・ベースの方式 – 負荷プロセッシング・コア • すべてのコアでソフトウェア診断用の追加負荷が発生	• 凍結フレーム・モニタ：ハードウェア支援の凍結フレーム検出。CPU負荷なし • ハードウェアCRCベースのディープ・ラーニング・ネットワークの安全。追加CPU負荷なし

表2：アプリケーションへの安全マッピング。

適切なアーキテクチャのシステムでは、次のような機能安全要件がサポートされます。

- SoCがセンサ・データをチェックする
- MCUがSoCをチェックする
- MCUがアクチュエータを制御する
- コントロールに対してアクチュエータが期待どおりに作用することをMCUがチェックする
- PMICがMCUハードウェアとソフトウェアの実行をモニタする
- PMICがアプリケーション・プロセッサ・ハードウェアの動作をモニタする

エラー動作を検出すると、PMICはENDRV出力ピンを強制的に低にしてシステムを安全状態にします。エラーの例には以下のものがあります。

- MCUまたはSoCへの電源電圧の障害
- PMICへの入力電源電圧の障害
- MCUソフトウェアまたはハードウェアのエラー
- SoCについてESMから報告されたSoCハードウェア・エラー

TPS6594-Q1とLP8764-Q1デバイスはスタンドアロンのPMICとして使用できますが、スケーラビリティのために複数のPMICがプロセッサやMCUと共に利用されているシステムでは、CRCプロトコルでカバーされた2線式インターフェースによってPMICが相互に通信します。このインターフェースでは、PMIC間で電源状態とエラー処理を同期できます。バスの周期的なポーリングにより、通信バスにあるすべてのPMICの健康状態がチェックされます。この実装により、システム障害条件に対する迅速な応答が保証されるため、ソリューションではエンド・システムでのより高度な機能安全目標をターゲットにできます。**図2**は、2つのPMICとJacinto 7プロセッサ・システムの接続例を示しています。ほとんどのアプリケーションではTPS6594-Q1だけを使用しますが、LP8764-Q1も使用すると追加のシステム機能がサポートされて性能が向上します。1つまたは複数のPMICを組み合わせた「仮想」PMICを使用してSoCの電源を供給するこの機能により、最高性能のシステムと同時に消費電力の低減が必要な使用状況でシステム・コストを最適化できます。

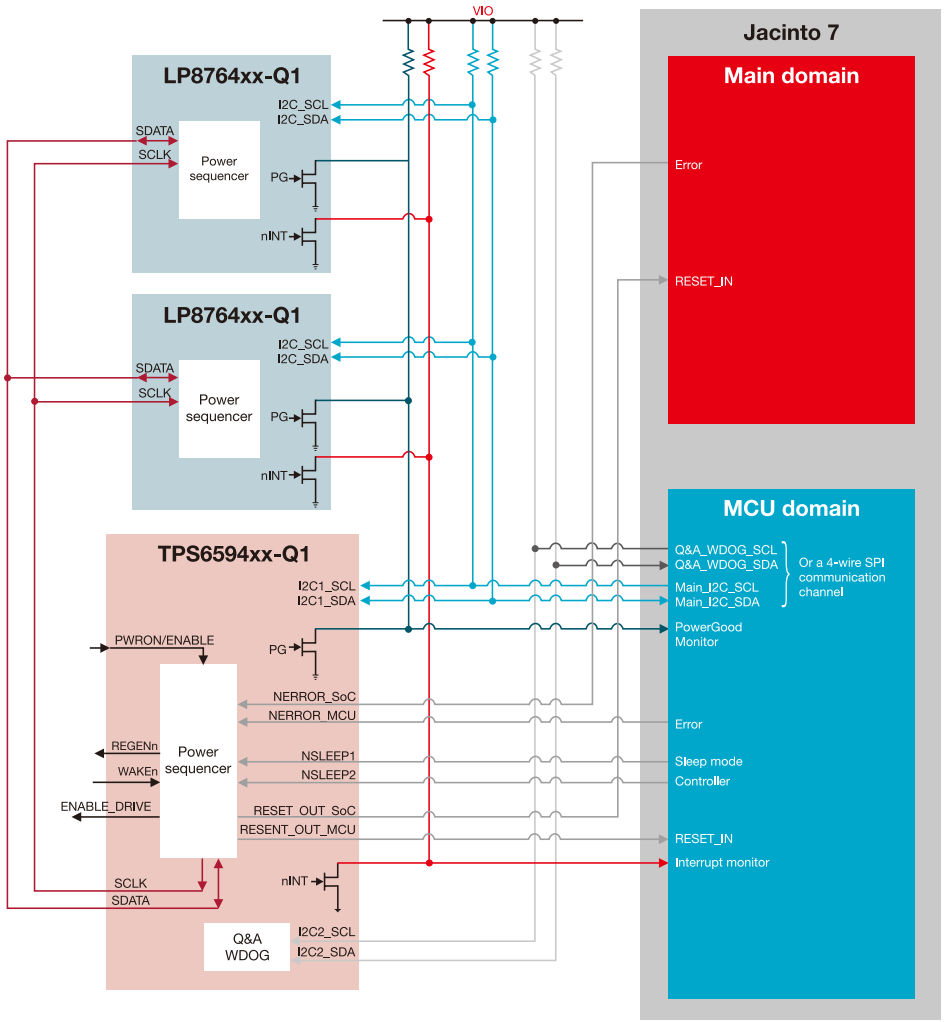

図2：TPS6594-Q1＋LP8764-Q1＋LP8764-Q1通信を「仮想」PMICとして使用。

まとめ

機能安全関連の機能をオンチップに内蔵したTIの新しいJacinto 7プロセッサ・ファミリは、顧客が安全認証を取得してエンド製品の安全目標を達成するのに役立ちます。広範囲な安全機能はシステムBOMの低減に役立ち、さまざまなコアで性能オーバーヘッドを節約できます。また、TIのソフトウェアSDKは、顧客がソフトウェア開発に関する安全目標を達成するのに役立つ安全関連のドライバと診断ライブラリを提供します。簡素化された安全アーキテクチャとソフトウェア製品は、顧客が設計と開発に使う労力を大幅に節約するのに役立ちます。

その他の技術資料

- Kumar, VC。『The state of functional safety in Industry 4.0（英語）』。Texas Instruments white paper SPRY329, 2018。
- Thomas, Jay, and Siddharth Deshpande。『Foundational Software for Functional Safety（英語）』。Texas Instruments white paper SPNY007, 2015。
- 機能安全ハードウェア証明書。
- 機能安全ソフトウェア証明書。
- Chitnis, Kedar, et al。『Enabling Functional Safety ASIL Compliance for Autonomous Driving Software Systems（英語）』。Electronic Imaging, Autonomous Vehicles and Machines 2017（英語）, Society for Imaging Science and Technology（2017年1月29日）、35～40ページ。
- Haworth, David, Tobias Jordan and Alexander Much。『Freedom from Interference from AUTOSAR-Based ECUs：A Partitioned AUTOSAR Stack（英語）』。Automotive – Safety & Security（英語）, LNI 210（2012年）、85～98ページ。

©2020日本テキサス・インスツルメンツ合同会社
Printed in Japan 2020.03

JAJY104

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