未来の輸送システムに向けた安全で堅牢な機能安全システム・ベース・チップ（SBC）

David Lopez, Marketing & Application Manager, Safety & Power Management

Maxime Clairet, Application Engineer, Safety & Power Management

2016年6月

要約

パワー・マネジメント回路上で機能堅牢性と機能安全を組み合わせると、組み込みE／E輸送システムを保護し、設計を簡素化することができます。

自動車市場は、排出ガスの削減、交通渋滞の緩和、その他の危険の低減のために、自動車の電動化と自動運転に向かって動いています。このトレンドでは、ドライバーの代わりに判断し行動することのできる電子システムが求められます。こうしたシステムは、ステアリング、ブレーキ、トランスミッションなどのセーフティ・アプリケーションに基づいて判断して行動し、操作を誤って乗員を負傷させることはありません。

運用のリスクを管理するために、これらのシステムは最高度のISO 26262自動車用安全度水準（ASIL D）に従って開発されており、受容できる確率で安全目標が侵害されたときに安全状態へ遷移化することを保証します。

すべての安全関連電子システムには、セーフティ・マイクロコントローラと、カー・バッテリに接続された信頼性の高い安全な電源が必要です。これがシステム・ベース・チップ（SBC）です。セーフティ・マイクロコントローラとセーフティ・システム・ベース・チップは、組み込みシステム・アーキテクチャのバックボーンとして独立したハードウェア・モニタリング機能を実現します。

この論文では、パワー・マネジメント・レベルにおける機能安全の最新イノベーション（SBC）について、開発フェーズからシステム設計までを、信頼性と安全対応のハードウェアを実現する方法との関連性を明らかにしながら解説します。また、ASIL D 向けに開発されたアーキテクチャを使用し、集積回路（IC）に対して破壊試験を実施して、組み込みシステムの機能堅牢性を向上させる方法についても説明します。破壊試験では、安全アーキテクチャの堅牢性と、電気的過負荷（EOS）によって破壊が発生した場合にどのように安全状態へ移行するかがわかります。

目次

ISO 26262機能安全規格について

機能安全とは、システムの機能不全によって引き起こされる危険を原因とする、不合理なリスクの発生を抑制することを意味します。機能不全によるリスクを大幅に低減するには、発生しうる故障のタイプを理解し、評価することが重要です。これらの故障は、次の2つに分類できます。

1. 決定論的原因故障：製造プロセスの設計、運用手順、文書化、またはその他の関連する要因の変更によってのみ取り除くことができます。このタイプの故障が発生する確率は、ロバストな開発プロセスと品質管理によって低くなります。
2. ランダム故障：確率分布に従ってハードウェア機器のライフタイム中に予期せず発生します。これらの故障の原因として、永続的または一時的な環境の大幅な変化や、システムのライフタイム全体における本質的な技術能力が挙げられます。ランダム故障に関連するリスクの低減には、専用のシステム・アーキテクチャやIC検出ストラテジを利用します。これは、SBCの目的の1つです。

2011年11月15日、自動車業界向けにISO 26262:2011(E)が発行されました。この規格は、特に「自動車--機能安全」を目的として修正が施され、機能安全規格のIEC 61508を車載電気／電子（E／E）システム用に適合させたものです。アプリケーションは、機能性を維持し、ディペンダビリティを保持しなければなりません。ディペンダビリティを保持するには、安全性と可用性の最適なバランスを実現しながらE／Eシステムを設計する必要があります。

可用性は保守性と信頼性の微妙なバランスの上に成り立ちますが、安全性は主にシステムの信頼性に左右されます。この関係を以下の図に示します。

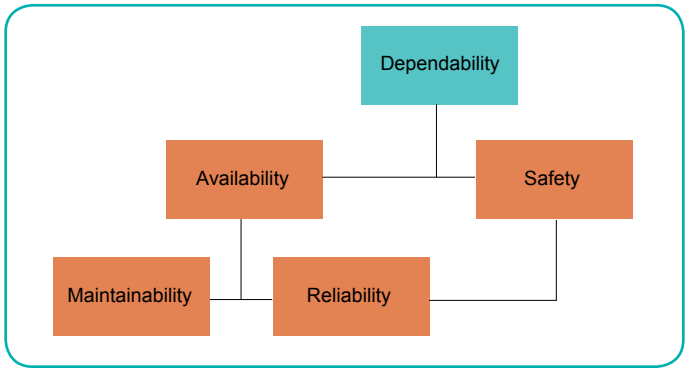

図1: 機能安全に関するディペンダビリティのトレードオフ

NXPでは、SafeAssurer®というブランドを設け、可用性、安全性、信頼性を効果的に組み合わせることでディペンダビリティを実現する各種の製品を取り揃えています。

システム要件からICアーキテクチャの定義へ

ISO 26262では、重大度、発生頻度、回避可能性によって決まる安全度水準を定義しています。以下の表に、システムに関連した自動車用安全度水準（ASIL）をまとめて示します。

Severity Extent of hard to individual(s) that can occur in hazardous situations	**Exposure** Probability of exposure regarding operational situations	**Controllability** Ability to avoid a specific hard through timely reations		
		C1 - Simple	C2 - Normal	C3 - Difficult
S1 - Light	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 - Severe	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 - Fatal	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

QM:「Quality Managed」（規格によって明示的に適用される要求事項なし）

表1: 自動車用安全度水準

この要件をICレベルの要件に置き換えるには、FIT率から算出される故障確率が必要となります。

定量的解析 – 信頼性から機能安全まで

機能安全の指標は、IEC 62380 に従って、アプリケーションのライフタイム中の故障リスクを定量的に表すFIT（Failure In Time：10億時間あたりの平均故障回数）に基づいて算出されます。FIT率は、技術、パッケージ、およびアプリケーション条件（ミッション・プロファイル）によって異なります。ハードウェアの劣化に基づいてFIT率を算出すると、次のISO 26262評価指標を決定できます。

デバイスのFIT率は、代表的なダイ・サイズに基づいてデバイスの各機能に分散され、各機能では発生しうるすべての故障モードに対して均等に分散されます。安全関連機能の故障モードがアプリケーションの安全目標に違反した場合、安全機構がそれを検出する必要があります。1 FITは、109デバイス時間（114年）に1回の故障が発生することを表します。

$$\lambda = \underbrace{\left\{\left\{\lambda_1 \times N \times e^{-0.35xa} + \lambda_2\right\} \times \left\{\frac{\sum_{i=1}^{y}(\pi_t)_i \tau_i}{\tau_{on} + \tau_{off}}\right\}\right\}}_{\lambda_{die}} + \underbrace{\left\{2.75 \times 10^{-3} \times \pi_a \times \left\{\sum_{i=1}^{z}(\pi_n)_i \times (\Delta T_i)^{0.68}\right\} \times \lambda_3\right\}}_{\lambda_{package}} + \left\{\underbrace{\pi_1 \times \lambda_{EOS}}_{\lambda_{overstress}}\right\} \times 10^{-9}\ /h$$

図2 – NXPがSafeAssureコンポーネントに使用しているFIT率の算出方法（IEC TR 62380規格に準拠

このFIT率は、NXPが開発したSafeAssureツールの入力になります。動的FMEDAにより、ASILレベルの判定に必要な3つの数値が得られます。

SPFM（Single Point Fault Metric：単一故障の評価指標）は、アプリケーションの安全目標に違反する故障の検出率を表します（ASIL Dの場合は99%以上）。安全機構の診断範囲（低-60%、中-90%、高-99%）に応じて、検出されない故障モードの残りのFITを算出します。

SPFM = 1 – [∑ (λRF) / λSR]（λSR = 安全関連機能のFIT率）

安全検出機構（モニタリング機能）のLFM（Latent Fault Metric：潜在的故障の評価指標）故障は、単一故障と同時に発生した場合にアプリケーションの安全目標の違反につながる可能性があります（ASIL Dの場合は90%以上）。BIST等で検出されない潜在的故障モードの残りのFITを使用して、同じ方法をLFMに適用します

LFM = 1 – ∑ (λMPF) / [∑ λRF) – λSR)]（λMPF = 潜在的故障の残りのFIT）

PMHF（Probability Metric of Hardware Failure：ハードウェア故障の確率的評価指標）で、安全目標の違反の残存確率に関するものです（ASIL Dの場合は10^{-8}未満）。

PMHFは、アプリケーションのライフタイム（自動車では最低15年）に対してSPFMとLFMから算出されます。ASILのIC水準の適合性は、こうして得られた3つの数値に基づいて判定することができます。以下の表に、ICレベルでASILレベルに適合する数値をまとめて示します。

	ASIL B	ASIL C	ASIL D
PMHF = Random hardware failure	$<10^{-7}$	$<10^{-7}$	$<10^{-8}$
SPFM	>90%	>97%	>99%
LFM	>60%	>80%	>90%

表2 – SPFM、LFM、PMHFの各目標とASILの目標の対応

パワー・マネジメントと機能安全ハードウェア・モニタリング機能を組み合わせる理由

マイクロコントローラには、タイミング（チャレンジ機能付きの高度なウォッチドッグ）、電圧レベル（過電圧／低電圧）、およびコンピューティング（FCCUモニタリング）を確認するために、外部の安全モニタリング手段が必要です。この重要なシステム機能を標準化してパワー・マネジメント回路に統合し、新世代のセーフティ・システム・ベース・チップ（SBC）が作り出されました。セーフティSBCは、パワー・マネジメント、コネクティビティ、およびシステムを統合したもので、組み込みシステムに対する電力供給と監視を主な目的としています。

MCUとSBCの組み合わせは、組み込みシステムの安全のバックボーンに相当するため、フェイル・セーフの質的解析も必要です。つまり、ICの安全状態をシステムの安全目標に合わせるために、故障診断後のコンポーネントの挙動を解析する必要があります。

機能安全ソリューション向けのNXPの先進的ハードウェア・システムは、ISO 26262規格の安全要求を満たすために設計された、MPC5744Pセーフティ MCUと最新世代のセーフティSBCファミリであるFS65の組み合わせから構成されています。

MPC5744Pは、安全アーキテクチャを統合したデュアルコア・ロックステップMCUです。内蔵自己診断（BIST）機構は、コア、メモリ、クロスバー、通信ブロック、およびペリフェラルに対して提供されます。

FS65デバイス・ファミリには、低消費電力モード（30 µA）に切り替え可能な効率的なDC／DCパワー・マネジメント機能が組み合わされています。FS65の安全目標は、システムへの電源供給の確保と、MCUの監視です。パワー・マネジメント機能は、システムを脅かす事象につながるアプリケーションの機能不全を防ぐため、さまざまな安全機構と関連付けられており、MPC5744Pとともに開発されました。システム内で2つのデバイスを併用すると、ASIL Dシステム・レベル・ソリューションを容易に実現することができます。

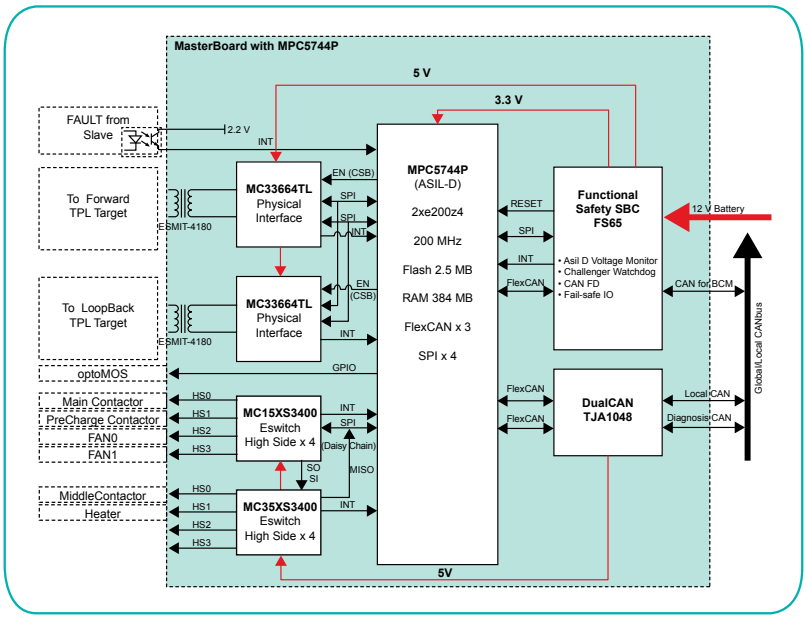

図3 – システム例 – BMS ASIL D安全アーキテクチャのMCUとSBCのバックボーン

パワー・マネジメント機能と安全ハードウェア・モニタリング機能を組み合わせると、システム・アーキテクチャを簡素化し、組み込みシステムの安全のバックボーンを標準化して、適切な量的解析を通じてASILに適合させることができます。しかしながら、定量的解析だけではシステムのディペンダビリティを実現するのに十分ではありません。故障検出後のデバイスの挙動を、重要かつ補完的な観点として検討すべきだからです。

定性的解析 – フェイル・セーフからフェイル・サイレントへ

各種のアプリケーションにはそれぞれ異なる安全状態の条件があります。リセットやフェイル・セーフ・ピンのアクティブ化などのハード・ストップがシステム・アーキテクチャにとって望ましいケースもあれば、ソフト・ストップまたは縮退モードに移行してアプリケーションを継続させた方がよいケースもあります。バッテリ・マネジメント機能は、後者の最適な例であり、フェイル・サイレント・アーキテクチャを可能にする中心的な役割を果たします。

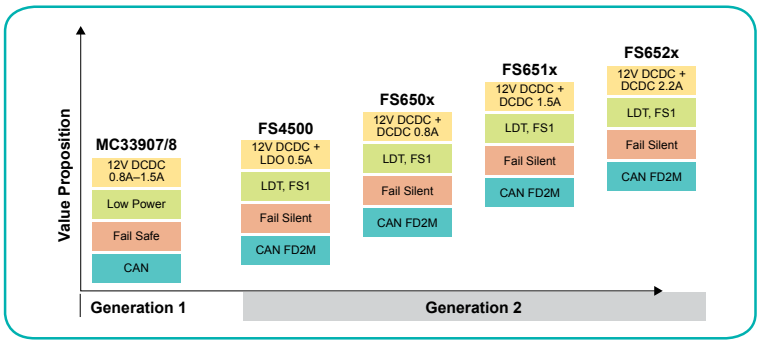

図4 – 2つの世代のセーフティSBC

上の図は、NXPのセーフティSBC製品群における機能安全動作、特にシステムに依存する安全状態条件の進化を示しています。

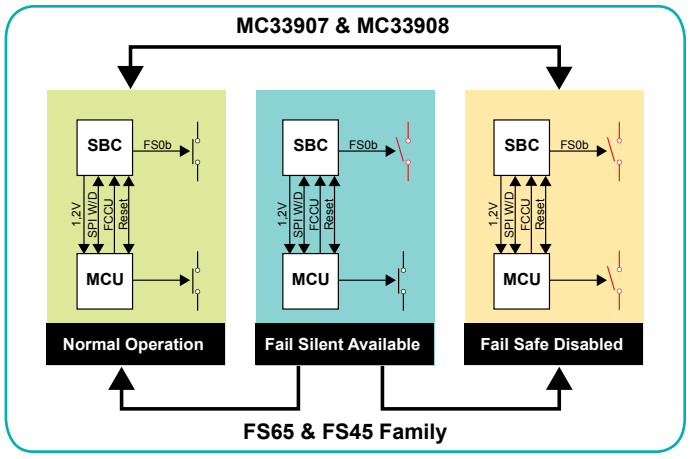

図5 – システム・アーキテクチャの進化

フェイル・サイレント・モードは、アプリケーションのさまざまな安全目標に適合するフレキシブルな安全動作を実現するために、ハードウェア・レベルで提供される新たなソフトウェア設定機能です。リセットとフェイル・セーフのアクティブ化は設定可能でかつ安全です。つまり、システム・レベルにおけるディペンダビリティの最適な水準を選択することができます。

上のBMSの例のソリューションは、故障後も、システムが適切なレベルの可用性を維持したまま縮退モードで動作することを可能にして、E／Eアーキテクチャ内で車の電源を管理し続けます。

安全な遅延 – 故障後のシステム・タイミング条件の管理

モーター制御アプリケーションには、安全状態の確保などのために、故障検出後に電源を順次切断することが必要になります。その場合、故障検出からフェイル・セーフ状態をアクティブ化するまでの期間を個別に処理する必要があります。この期間は、モーターの誘導性負荷により、消磁に起因するシステム故障の防止に役立ちます。

ISO 26262の実施をサポートし、エネルギーを安全に消磁するために、設定可能で安全な遅延が定義、実装、検証されています。このタイミング管理機能は、デジタルおよびアナログの冗長性を備えており、同じアプリケーション条件用のFS0と対照的に設定が可能な遅延信号（FS1）を生成して、システムを簡素化し、モーターのフェイル・セーフ状態を確保するのに役立ちます。

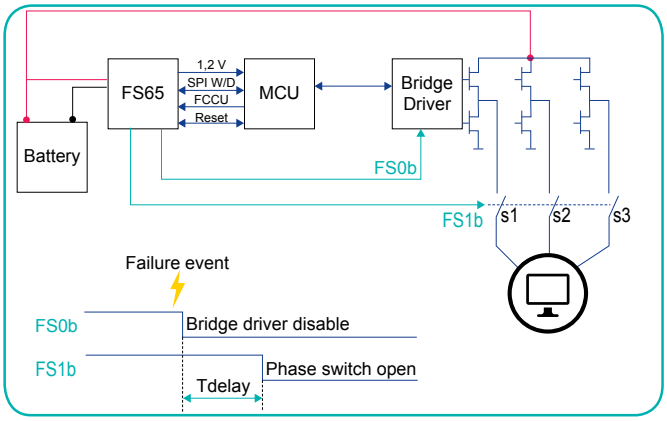

図6 – 電気モーター・アーキテクチャのシステム安全遅延の管理

この例は、ハードウェア側の機能安全が、 ASILレベルに達するための定量的解析と、SEooC (Safety Element out of Context) ICのさまざまな安全目標をサポートするための定性的解析の組み合わせであることを示しています。

ここまで、信頼性と機能安全との関連性について取り上げてきました。最後に、トランスポーテーション用ICの性能について触れておきます。機能堅牢性と、アナログICでISO 26262を満たすことを検証する目的で実施されるテストを中心に説明しますが、システムが故障する極端な条件下の技術についても説明します。

検証：システム・ソリューションのプルーフポイント

ハードウェア統合テスト

セーフティSBCの安全アーキテクチャは、 ISO 26262のハードウェア統合テスト、特に故障注入テストによって、安全目標に違反するすべてのFMEDA故障モードに対して安全状態に遷移するかが検証されています。FMEDA解析が完了し、シリコンが利用可能になったら、安全コンセプトが定義と実装の通りに機能するかどうかが検証されます。検証するには、デバイスに物理的に故障を注入して、関連する安全機構がそれを検出し、フォールト・トレラント・タイム間隔（FTTI）内に安全状態に遷移するかどうかを確認します。

例として、 SBCによる MCU Fault Collection Control Unit （FCCU）ピンのモニタリング機能の検証を挙げておきます。MCUは、通常の状態では、差動電圧で2つのFCCU 信号をSBCの安全入力IO_2とIO_3に送信します。故障状態では、FCCU信号の1つを変更してどちらも同じ電圧でSBCに送信します。 SBCは、IO_2/3の電圧が予想された差動電圧と異なることを検出し、設定可能な遅延後に安全出力FS0とFS1をアサートすることで応答します。また、SPIレジスタのフラグをセットして診断を実行することにより、安全状態に遷移された理由を、リセット後にMCUが確認できるようにします（図7）。

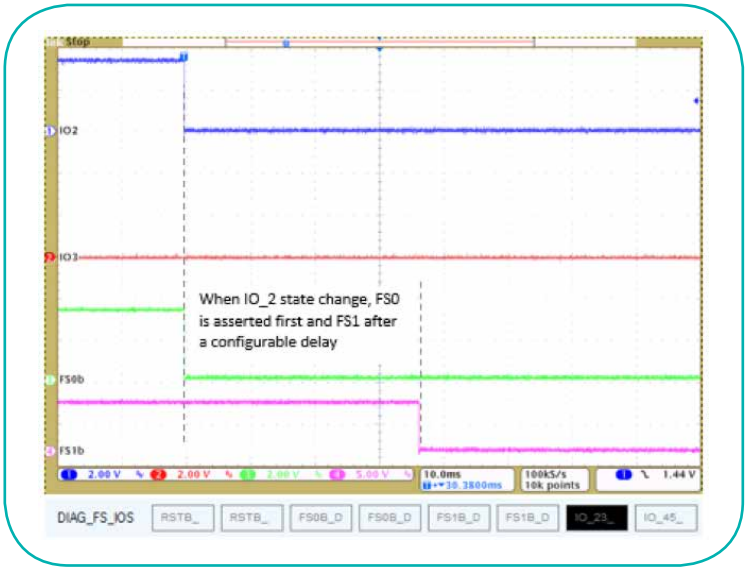

図7 – FCCU検出による安全状態のアクティブ化と関連するSPI診断

安全コンセプトで定義されている安全目標の違反としてFMEDAに含まれるすべての故障モードをデバイスに注入して、関連する安全機構を検証します。

拡張検証

NXPのセーフティSBCに実装された安全アーキテクチャの技術の限界および堅牢性を評価するため、拡張テストが実施されています。これらのテストは、デバイスが完全に破壊されるまで行いました。デバイスが破損した後でも安全状態を維持することを確認するという特殊な目標を設定して、データシートで指定された最大定格を超えました。このような極端なケースでも安全目標が達成されたことから、セーフティ・クリティカルECUの応答を制御できないことが原因でドライバーが負傷することはありません。

図8は、最大定格を8Vと指定されているプリレギュレータ（Vpre）にバッテリ電圧（18V）を印加してデバイスが破損しても、安全状態に遷移されている（FS0がアクティブLow）ことを示しています。

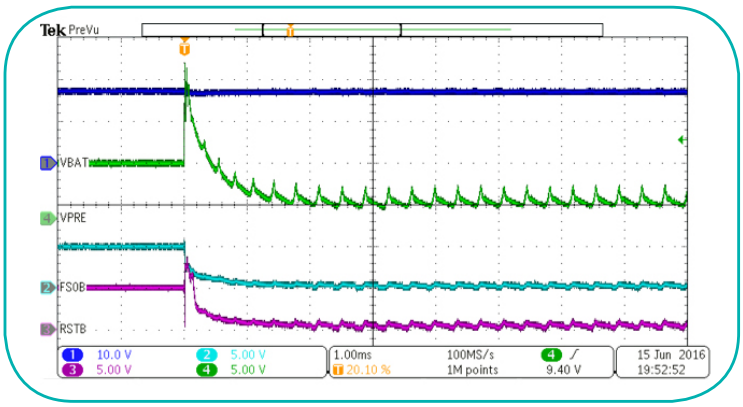

図8 – デバイス破壊（Vpreに最大定格以上を印加）後の安全状態のアクティブ化

自動システム検証

車両ネットワークにつながるすべてのパワー・マネジメント・コンポーネントは、ISO 7637規格に従って、ISOパルスの過渡現象だけではなく、自動車OEM固有のさまざまな電圧パルス変動（非ISOパルス）からの影響も受けないようにする必要があります。非ISOパルスはOEM固有であり、各OEMは経験に基づいた独自の非ISOパルス・カタログを想定しているので、非ISOパルスは無数に存在します。検証プロセスの最後に非ISOパルスの注入によってモジュール検証が失敗することがないように、ICの挙動を事前に予想しておくのが適切です。

NXPでは、そのために社内検証プラットフォームを開発しました。このプラットフォームでは、非ISOパルス・パターンを生成して自動的に注入し、パルス期間中の監視を行うだけでなく、トレーサビリティ・レポートを生成します。このレポートを結果解析後に利用すると、 ISO 26262要件に対応することができます。 このプラットフォームは、わずか数週間で、ICを非ISOパルスの数千のデータベースに照らして検証します。検証は、独自の設定に基づいており、数か月後や数年後でも再現性は100%です。

この独自プラットフォームは、アナログ・ハードウェア、MCUハードウェア、MCU組み込みソフトウェア、コンピュータのWindows®ベースのGUIで構成されています。また、NXP製MCUの接続方式の検証や、SBCのレギュレータ・レールに過渡的負荷を印加した場合のSBCの挙動の確認に使用することもできます。

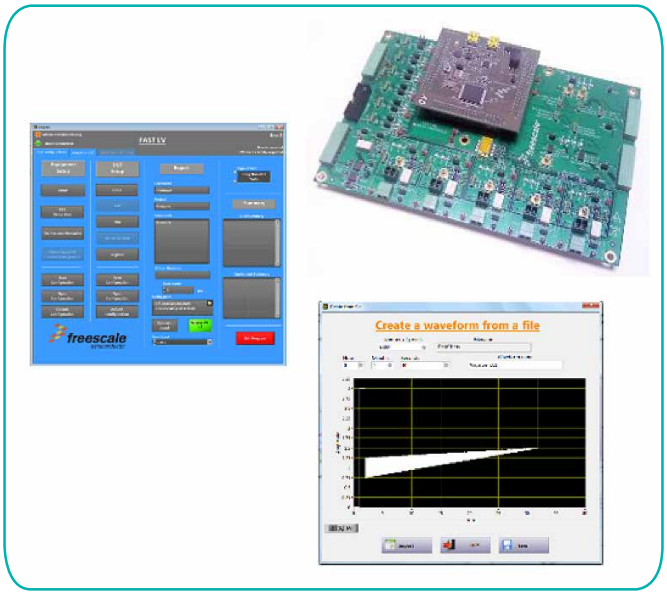

図9 – 自動化された非ISOパルス・プラットフォーム

EMCとESD

NXPが開発したセーフティSBCは、車載ネットワークを介した通信用に、CANおよびLIN物理レイヤを内蔵しています。第2世代のFS65は、最新のCAN FD 2 Mbits/sにアップグレードされており、電気特性としてはISO 11898に、EMC特性としてはIBBEおよびJ2962-2に準拠しています。したがって、最新自動車に求められる大容量データ通信に対応することができます。また、IEC 61000およびISO 10605規格に準拠して、優れたESDガン堅牢性（最大12 KVの接触放電）を備えています。

信頼性の拡張

FS65は、電気自動車のミッション・プロファイルにより要求されるONサイクルの長期化、および自動運転車用の駆動系アプリケーションにより要求される高温化の予測に基づいて設計、検証されました。

結論—簡素化された組み込みソリューションを支える主要な柱：信頼性、堅牢性、安全性

この論文では、ISO 26262の認証を取得した開発プロセスに基づいた、SBCのような外部ハードウェア・モニタリング用デバイスの定量的および定性的な安全解析という相補的な手法に焦点を当てて解説しました。これこそ、フェイル・サイレントに対応した第2世代セーフティSBCを通じてNXPが提案していることです。

品質管理とゼロ・ディフェクト手法は、機能安全解析の出発点です。FIT率の算出により、機能安全指標の解析をサポートし、フェイル・セーフのハードウェア・モニタリング・アーキテクチャとの組み合わせにより、数値目標を達成して適切なASILレベルを取得できるようにします。この論文では、品質と機能安全との関連性、特にFIT率と車両ソリューション向けのミッション・プロファイルとの関係を明らかにしました。

ところで、故障後にシステムがどのようにふるまうのかも、ICの解析と安全動作の重要な観点です。安全状態の設定可能性が進化したことで、アプリケーションのディペンダビリティをE／Eシステムの安全性と可用性との最適なバランスに決めることができるようになりました。

車載用半導体の検証も変化しており、過酷でノイズの多い環境下や故障後のコンポーネントの動作を保証するために、さらに多くのシステム・テストが求められています。この検証方法は、V&V（検証と妥当性確認）を保証するために開発されており、ドキュメントにプルーフポイントを提供します。

最後に付け加えておくと、この新世代デバイスは、アーキテクチャの冗長性を評価するために、破壊されるまでテストされており、フェイル・セーフ信号（アクティブLow）の予想動作が安全コンセプトに一致することを示しています。こうした特性の拡張は、機能堅牢性の限界を押し広げます。

結論として、この先進的な安全アーキテクチャはECUの設計を容易にし、リスクの評価に役立ち、システムの堅牢性を向上させ、設定可能なフェイル・セーフ動作やフェイル・サイレント動作によって、設計者が故障後のシステムを予想できるようにします。

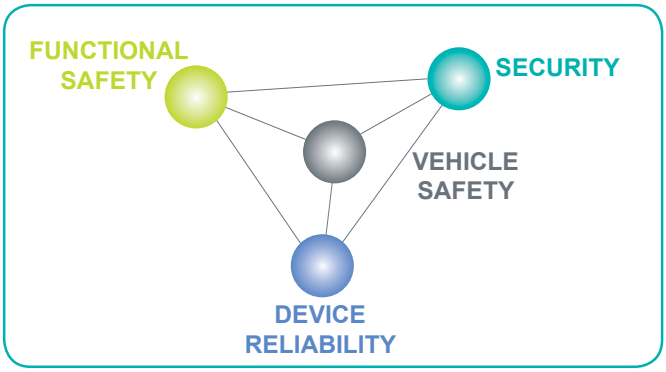

図10 自動車の電動化と自動運転を可能にするクリティカル技術

セーフティSBCは、認証取得した ISO 26262プロセスに従って定量的および定性的な安全解析に基づいて開発されます。リスク解析は、機能堅牢性を備えた設計、柔軟なフェイル・セーフ対応のシステム・アーキテクチャ、高度なセキュリティ・アーキテクチャとの組み合わせにより、フォールト・トレラントでセキュアな輸送システムを用意することで、自動運転車のために新たな地平を切り開きます。

References

[1] ISO26262:2011 - Road vehicles - Functional safety

[2] ISO10605:2008 - Road vehicles - Test methods for electrical disturbances from electrostatic discharge

[3] ISO7637-2:2011 - Road vehicles - Electrical disturbances from conduction and coupling

[4] ISO11898-5:2006 - Road vehicles - Controller area network

[5] IECTR62380:2004 - Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment

[6] IEC61000-4-2 - Electrostatic Discharge Immunity Test

[7] IEC61508 - Electrical, electronic and programmable electronic safety related systems

[8] SAEJ2962-2 - Communication Transceivers Qualification Requirements – CAN

[9] IBEE: IEC TS 62228, Hardware requirements for LIN, CAN and FlexRay interfaces in automotive application

– AUDI, BMW, Daimler, Porsche, Volkswagen – Revision 1.3/ 2012

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

NXP Japan Ltd.:
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku, Tokyo
150-6024, Japan
0120 950 032 (Domestic Toll Free)
http://www.nxp.com/jp/support/

www.nxp.com/safeassure

NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners.
© 2018 NXP B.V.

Document Number: FUNSAFETYWPA4J REV 0（原文:FUNSAFETYWPA4 REV 0）