電気自動車と自動運転車の機能安全システムのアクチュエータ設計動向

Anuj S. Narain
Functional Safety Engineer
Motor Drivers

Texas Instruments

機能安全アプリケーション向けに開発された各種アナログ・コンポーネントを使用すると、電動化、バイ・ワイヤ（電子制御）、故障時動作継続（フェイル・オペレーショナル）に対応した自動車アーキテクチャ向けに、洗練された電気式アクチュエータ・システムを製作できます。

「CASE」という自動車の4つのトレンド、つまりコネクテッド（ネットワーク接続型）、自動運転、共有、電動化（Connected、Autonomous、Shared、Electric）という流れは、1世紀以上前に最初のModel-T（T型フォード）が組み立てラインから登場して以来、最も魅力的な自動車開発トレンドとなっています。よりクリーン、より安全、そしてより効率的な自動車は、街をクリーンな状態に維持すると同時に、再生可能ではないエネルギー源への依存度を低減するのに役立ちます。

これらのトレンドは、パワートレインやシャーシのアーキテクチャ・レベルで、互いに興味深い関係にあります。従来はドライバーが操作していた各種機能が、より安全、そしてより効率的な方法で動作するためのインテリジェンスを備えた自動機能によって置き換えられています。このホワイト・ペーパーでは、CASEというトレンドが電気式アクチュエータ・システムに及ぼす影響に注目します。

バイ・ワイヤ（電子制御）時代の到来 – 信頼の実現

ステア・バイ・ワイヤ（電子ステアリング制御）、ブレーキ・バイ・ワイヤ、シフト・バイ・ワイヤ、および電動化パワートレインなどの技術は、これらのシステムに取り組む設計者の皆様に、従来は存在しなかった一連の魅力と課題の両方をもたらします。

自動車の各種機能を電気式アクチュエータに切り替えることは、本質的に機械系コンポーネントの数が減ることを意味します。その結果、重量を減らし、機械の一般的な故障モードを排除して、スマート機能を統合できるようになります。たとえば、ステア・バイ・ワイヤ・システムは、航空機が採用したフライ・バイ・ワイヤに似た形式であり、人間の操作を機械式で駆動系に直結する代わりに電気信号に変換して伝達する、また路面や気候など周囲の状況に応じてコンピュータがある程度の調整を自動的に加える、という特徴があります。その結果、自動車の動的特性を改善し、効率を向上させることができます。

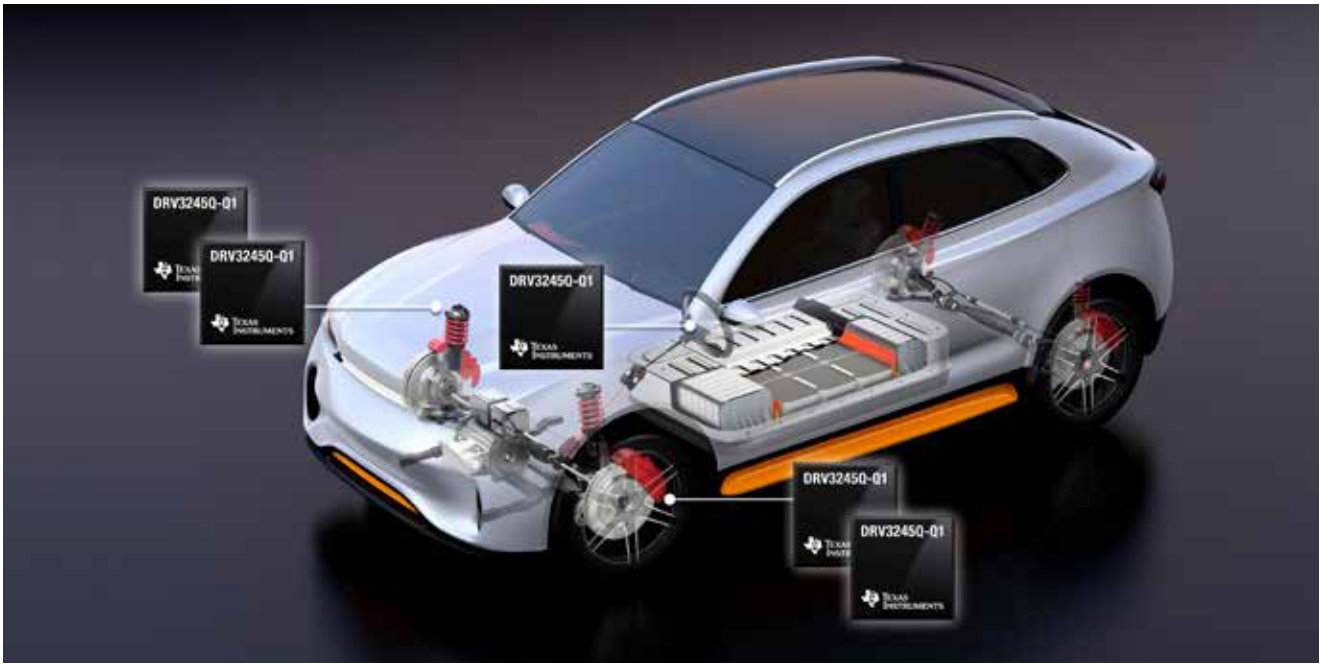

図1：ステアリング、ブレーキング、トランスミッションなどの各種車載アクチュエータをバイ・ワイヤ制御に移行することで、機能安全アプリケーションにTIのモーター・ドライバを活用できる。

別の例は、自動的なシフト（トルク・コンバータを使用する単純なATのことではなく、コンピュータのインテリジェントな判断に基づく自動的なシフト）やシフト・バイ・ワイヤ・テクノロジーです。この場合、電気式アクチュエータがトランスミッションのシフト機能を、エンジンの最も効率的な動作ポイントと組み合わせて切り替えを行います。これらのシステムには、停止状態または駐車中の自動車が前後に移動してしまう事態を防止するのに役立つ、安全性の利点もあります。

図1に、ステアリング、トランスミッション、ブレーキングを含む各種バイ・ワイヤ・システムが採用しているアクチュエータを示します。

バイ・ワイヤ・システムが必要とするハードウェアとソフトウェアの各コンポーネントは何年にもわたって利用されてきたものですが、コンシューマからどれだけの信頼を獲得しているかは明確ではありません。

「フェイル・セーフ」システムから「故障時動作継続」システムへの移行

アクチュエータを機械式から電気エネルギー使用方式に切り替えるのに応じて、安全性アーキテクチャも進化する必要があります。現在の安全性システムが採用している電気式アクチュエータの大半は、冗長性の目的で元の機械式コンポーネントを維持しています。

たとえば、電気式ブレーキング・システムについて考えると、ブレーキ・ペダルからブレーキ・シリンダーまでの機械式リンクは、電気系の故障に対する冗長性を実現しています。ただし、このような機械式リンクの残存が原因で、ブレーキ・ペダルを床まで踏み込むにはある程度強い力が必要になっています（仮に純粋な電気式であるとすると、ごく簡単に踏み込むことが可能な仕様も容易に実現できます）。電気式ブレーキング・システムは、「フェイル・セーフ」を実現するアーキテクチャを採用しています。つまり、仮にブレーキング・システムが故障した場合でも、冗長手段の動作を妨げない方法で故障する設計になっています（この場合、ドライバーがブレーキ・ペダルを床まで踏み込み、機械式リンクがそれに反応してブレーキをかける動作を妨げません）。

自律アーキテクチャが進化するにつれて、機械式冗長性への依存度は低下することになります。人間（ドライバー）は制御ループ（運転に関するインテリジェンスと指揮系統）から除外され、まったく新しいクラスの「故障時動作継続」（フェイル・オペレーショナル）システムが登場してくるからです。故障時動作継続（フェイル・オペレーショナル）システムの一例では、自動運転車が搭載しているのと同じブレーキング・システムを使用します。これは、電気式ブレーキ・アクチュエータ・システムの障害が発生した後、ドライバーがすぐには操作を行えない状況に備えるものです。システム（ここで言う「システム」とはICのことではありません）は、このような状況でも動作を継続し、自動車のブレーキをかけることが期待されています。

この種のシステムを設計する場合、安全性に関する主な検討事項は次のとおりです。

- システムの障害耐性（フォルト・トレランス）とASIL（Automotive Safety Integrity Level、車載セーフティ・インテグリティ・レベル）。
- 最初の障害が発生した後、システムで許容される機能低下の度合い。
- 緊急機能、ドライバーへの警告、緊急動作の持続時間。
- システムが安全状態（故障が発生した時のフェイルセーフ側、上記の例で言えば、電気式ブレーキによる信号伝達やインテリジェントなブレーキ機能は動作していないが、ブレーキ・ペダルから物理的リンク経由でブレーキをかけることができる状態）に移行する際、また安全状態から他の状態に移行する際に必須となるASILレベル。

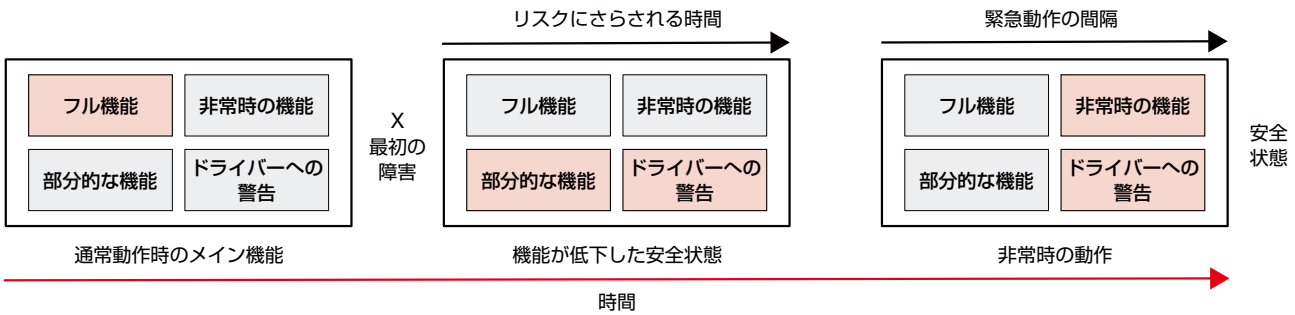

図2：ステアリング、ブレーキング、トランスミッションなどの各種車載アクチュエータをバイ・ワイヤ制御に移行することで、機能安全アプリケーションにTIのモーター・ドライバを活用できる。

（**図2**をガイダンスとして使用し）故障時動作継続システムで、安全性目標（安全性に関する目標）と安全状態に関する分析を実施するために、国際標準化機構（ISO）ISO 26262-3:2018 Clause 7の第2版を参照することができます。その中で、1つまたは複数の「安全状態」に移行する方法、または「安全状態」を維持する方法により、安全性に関する目標への違反を防止することができる、と規定されています。「安全状態」は、「故障が発生した場合でも、定義した時間にわたって機能を維持している状態」と解釈することができます。この状態は、「故障時動作継続」システムに関してすでに説明した検討事項によく当てはまります。**図2**で「機能が低下した安全状態」という説明が付いているこの状態を実現するには、ドライバーへの警告と、この状態のままリスクにさらされる時間について検討し、分析する必要があります。加えて、ある安全状態から次の安全状態に遷移した後の緊急動作と、緊急動作の持続時間を分析するときに、ISO 26262-5:2018,9.2を適用することができます。

中間の安全状態、リスクにさらされる時間、および緊急動作の間隔に関する改良を加えるために、システム設計者の皆様は複数の方式を採用してきました。これらの方式のあるものは、二重巻線モーターなど、電気機械式の冗長性コンセプトに依存しています。これらの新しいモーターは、二重固定子モーター（dual-stator motor）または二重インバータ・モーター（dual-inverter motor）と呼ばれており、個別駆動形式の2個の固定子コイルと1個の回転子で構成されています。この設計により、どちらかの固定子が故障した場合でも、冗長固定子と回転子は引き続きアクティブな状態にとどまります。この場合、故障側のパスで予期される安全性要件は事実上、「フェイルセーフを実現するように設計すること」なので、正常な固定子パスの動作を妨げないように設計することになります。**図2**の文脈で考えると、この単一固定子動作は、「機能が低下した安全状態」に相当します。

安全性目標に違反する残存リスクを1 FIT（Failure in Time、時間あたりの故障回数）レベルまで低減するための別のアプローチとして、この冗長性を拡大して個別動作の複数電源（複数バッテリ）、個別動作の複数通信チャネル、さらに独立して動作する12Vと48V、または12Vと600Vという複数の電圧系統を採用した統合システムに発展させることも考えられます。

パワートレインの電動化と機能安全に関する追加の検討事項

『Analog Components Advance Functional Safety Development for Automotive Applications』（英語）というホワイト・ペーパーは、パワー・ステアリングやブレーキングなどの各種電気式アクチュエータ・システムに注目しています。パワートレインの電動化とリチウムイオン・バッテリの導入に伴い、各種安全性規格を意識してこれらのシステムを設計する必要性が高まっています。電動化パワートレインの安全性目標は、アクチュエータに関する分析結果に似ています（ドライバーが始動を指示したときに始動し、停止を指示したときに停止し、ドライバーが意図する動作を妨げない）。加えて、リチウムイオン・バッテリには、電圧と温度に関する安全性の限界を外れる領域で、バッテリの動作を防止するという安全性目標が設定されます。

回生充電システムに付きまとう1つの懸念は、モーター発電機（回生ブレーキの使用時にモーターを使用して発電する）がバッテリを過充電してしまう可能性です。この可能性があるので、新しい革新的な安全性機能と、安全性目標に対する違反を防止するための手法が必要になります。

高温動作アプリケーション内の機能安全

アクチュエータとドライブのエレクトロニクスは多くの場合、トランスミッション・ブロックの上に直接配置することになり、周囲温度は最大150℃に達します。このような温度条件下でもエレクトロニクスが機能するように、半導体の接合部温度が最大175℃に耐える専用設計のICが必要になります。温度に対する依存性が指数関数に従うことを前提として、設計者の皆様はFITレートを評価するときに、この種の高温アプリケーション向けのミッション・プロファイルを注意深く考慮する必要があります。このような要件を満たすために、TIはAEC-Q100 グレード0の機能安全部品（型番の後に付いた「E」という記号で識別可能）を提供しています。これらの部品は、最大150℃の周囲温度、および最大175℃の接合部温度を想定して設計と認定取得を実施済みです。

人的要因

ISO TC22/SC32/WG8ワーキング・グループは、ISO/PAS（publicly available specification、公開仕様書）21448の将来の刊行向けに、SOTIF（safety of the intended function、意図した機能の安全性）という概念を導入しました。SOTIFの目的は、ハードウェアやソフトウェアの異常（故障）が発生していない状況も含め、先進運転支援システム（ADAS）と自動運転車にとっての過度のリスクを識別、検証、確認するためのフレームワークを形成することです。

ここまでで（「フェイル」または「故障」という用語を強調して）フェイルセーフ・システムと故障時動作継続システムに注目してきましたが、自律システムは故障が発生していない場合についてもさらに検討する必要があります。

自律型のバイ・ワイヤ・システムは、ハプティクス・フィードバックをシミュレートし、ドライバーが慣れている機械式フィードバックを実現します。ステア・バイ・システムの場合、ステアリング・ホイールの上にモーターを取り付け、ステアリング・コラムからの機械式フィードバックをシミュレートします。バイ・ワイヤのブレーキング・システムは多くの場合、類似のハプティクス・アクチュエータを実装しています。これらのハプティクス・メカニズムは、複数のセンサと複数の複雑なアルゴリズムの組み合わせによってハプティクス・アクチュエータを動作させ、フィードバックを実現しています。

フィードバック・アクチュエータの故障が発生した状況を分析するためにISO 26262:3:2018を適用することは適切です。ただし、フィードバック・アクチュエータは正常に動作しているが、予期しない情報をセンサが返し、アルゴリズムがこの情報を正しく解釈できないような状況に対しては、この規定を適用しても問題は解決しません。

後者のシナリオは、ドライバーに対して正しくないハプティクス・フィードバックが提示されることで、ドライバーが通常と異なる危険なステアリング操作をしてしまう結果につながる可能性があります。SOTIFは、このようなシナリオに対処するためのフレームワークを実現することを意図しています。

進化を続ける機能安全システムの課題に対処する

フェイルセーフ・システムから故障時動作継続システムまでの進化、および電動化ドライブトレインとトランスミッションの急激な進歩を踏まえて、デベロッパーの皆様は故障防止や故障検出に関する革新的な方式を実装すると同時に、複数の安全状態との間で生じる移行の可能性に対処するための戦略を計画する必要もあります。

パワー・マネージメント製品とシグナル・チェーン製品で構成されたTIの製品ラインアップを採用すると、これらの課題を満たすための包括的なシステム・ソリューションを実現できます。TPS653853-Q1のような安全性パワー・マネージメントICと、DRV3245Q-Q1（AEC-Q100 グレード1）やDRV3245E-Q1（AEC-Q100 グレード0）のようなモーター・ドライバを組み合わせることで、故障時動作継続、バイ・ワイヤ、高温動作の各種安全性システムで直面するシステム統合上の複数の課題を解決できます。

以下に、このような方法で実現できる利点を示します。

- AEC-Q100 グレード1（Ta＝125℃）とAEC-Q100 グレード0（Ta＝150℃）の各バージョンを提供しています。これらの製品はスケーラブルで、互いにピン互換でソフトウェア互換性があります。
- 単一固定子または二重固定子のモーター・システムで、ASIL-Dのシステム性能を実現します。
- 性能と部品表（BOM）を重視して最適化済みのアーキテクチャにより、ボード上での半導体の二重化によるコストの影響を軽減できます。
- ICのFITレート計算を、システム・レベルのFITレート計算と統合できます。高温動作の安全性アプリケーション向けにカスタマイズしたミッション・プロファイルも含めます。
- FITレート、故障モードの影響、診断分析の結果をICレベルで得ることができます。

加えて、TIは、ICレベルのハードウェア・メトリクスに関する想定を提示しているほか、デベロッパー固有のシステムに対応してICレベルのハードウェア・メトリクスを調整するためのサポート機能も提供しています。

モーター・システム向けの安全性開発を開始できるように、さまざまなTI安全性ペリフェラルとともに出荷されている**DRV3245Q-Q1評価基板**を、**Hercules™ TMS570LS12x LaunchPad™ 開発キット**と組み合わせることをご検討ください。次の**図3**に、開発キットと組になっているDRV3245Q-Q1評価基板を示します。

図3 : *DRV3245Q-Q1車載3相モーター・ゲート・ドライバの評価基板(BOOSTXL-DRV3245AQ1)。*

関連コンテンツ :

- **ISO 26262-2:2018規格(英語)**を表示。
- **DRV3245Q-Q1データシート**と**DRV3245E-Q1データシート**のダウンロード。
- **Hercules LaunchPad開発キット**の詳細。
- **『Driving the Green Revolution in Transportation』(英語)**ホワイト・ペーパーを読む。

Printed in Japan 2020.04

JAJY107

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265