全方位の安全性

360° Safety

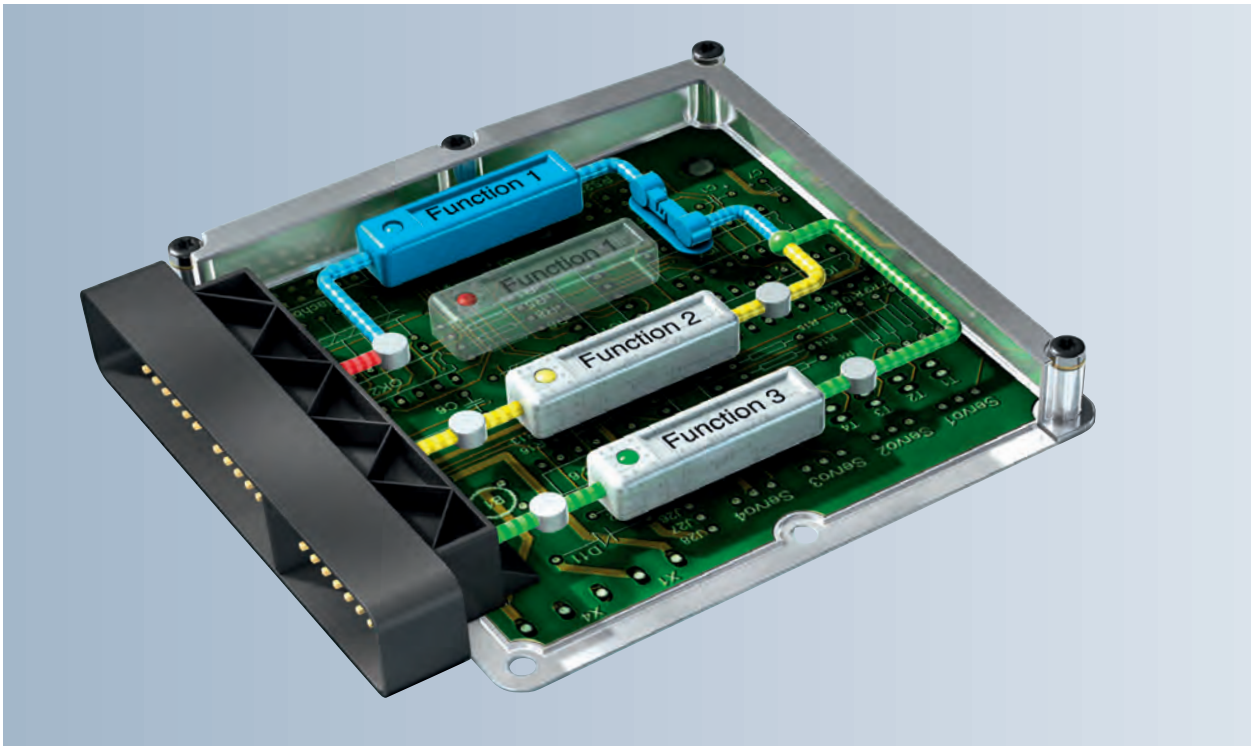


図 1:
たとえば ETAS EHOOKS などのバイパスフックツールを使用すると、エラーを故意に導入してシステムのロバスト性をテストすることができます。

図 2（ダイアグラム）:
安全コンセプトについては開発サイクル全体の至る所で詳細に調べる必要があります。テストだけでは不十分です。

機能的で安全な ECU を生み出す厳密な開発プロセス

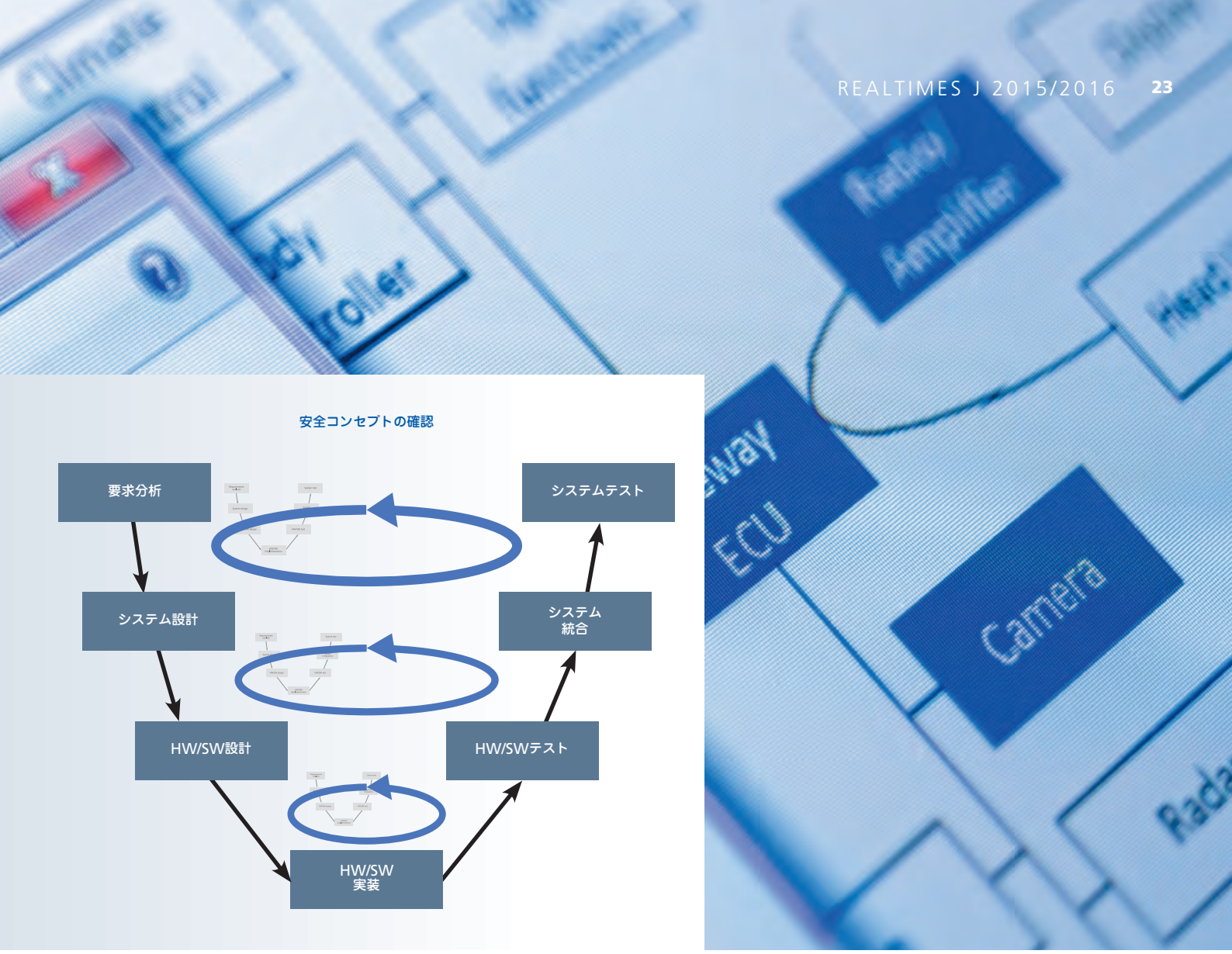
複数社の開発者チームが同じ制御装置について分散開発を行う場合、機能安全は組織化の問題にもなります。これには方法論的なノウハウ、実績のある開発ツール、および技術知見を、ひとつの厳密なプロセスに統合することが要求されます。

執筆者

Dr. Simon Burton
ETAS GmbH
グローバルエンベデッドソフトウェアサービスディレクタ

車の**ますます多くの**機能が電子制御装置（ECU）内のソフトウェアにより遂行されるようになってきました。そして複数の ECU に接続されるソフトウェア機能も増えています。中には、100 個を超える ECU が搭載されていて、車両全体に分布するセンサとデータバスで接続されて通信しているハイエンドモデルもあります。車とその周囲の環境とのコネクティビティも急速に拡大しているので、車は複雑なモビリティのコネクテッドワールドにおけるネットワークノードとなりつつあります。

このコネクティビティにより、さらに安全で効率的な運転が期待できますが、危険がまったく無いというわけではありません。それは、コネクテッド ECU の開発プロセスが複雑化の傾向にあり、世界各地に分散したチームが関与することが多くなっているからでもあります。ECU ソフトウェアの開発とプレキャリブレーションには、ECU メーカーの開発者と適合エンジニアだけでなく、ECU のサプライヤと自動車メーカーの開発者も関与します。エンジン ECU に取り組むさまざまなチームが燃料噴射、給気、点火、およびその他の多くのパラメータを扱います。しかも、プロセス全体が何度も行われる可能性があります。なぜなら OEM は多くの場合、確実に納車するために複数のサプライヤに同じ ECU を注文し、当然ながらどのサプライヤの ECU も車の購入者に違和感を与えることがあってはならないからです。ECU の出所とは無関係に、これらの ECU および ECU ソフトウェアは確実に機能しなければならず、機能安全が保証されなければなりません。



共同開発プロセスにおける安全性

このような状況の下、特に、特定のソフトウェア機能が複数個の ECU に分散されていてそのソフトウェアの一部分だけを置き換えようとしている場合には、どのようにすれば機能安全を保証できるでしょうか。成功の鍵の一つには、ソフトウェアを現実的なプラント、環境、およびドライバーのモデルで開発初期段階に評価できるようにする、仮想化のような革新的な手法およびツールを利用することです。ETAS の ISOLAR-EVE ソフトウェアのようなツールを PC シミュレーションと組み合わせれば、開発者はこのようなテストを ECU プロトタイプがまだ存在しないうちに開始することができます。エラーや不完全な前提は損害が発生する前に発見されます。また、開発者は危険の全く無いバーチャル環境で境界線領域を探ることもでき、これはセーフティ・クリティカルな支援システムを設計する場合に特に役立ちます。

しかし、仮想化はさらに完全な全体のアーキテクチャの中の 1 個の構成要素に過ぎません。開発プロセス全体を前もって構築し（図 2）、明確に定義されたソフトウェアアーキテクチャ、および各チームがどのような形で貢献するかということを、開発プロセスに明記する必要があります。さらに、緻密なプロセス監視がきわめて重要です。定期的な評価および監査を行うことにより、同意済みの安全哲学をチームが自分たちのものにしていること、および参加者全員が同じ解釈を共有していることを確認する必要があります。ISO 26262 などの規格がその基礎になります。

ソフトウェアおよび開発プロセスに関するルールの確立

ソフトウェア開発準備の第 1 ステップは、開発するアイテムのスコープを定義することです。トップダウン式のアプローチは、全体的なシステムとコンテキストを考慮して他のシステムとのインターフェースと連携の機能スコープの限界を設定することから始まります。これが完了したら、ハザードとリスクの構造化分析が実行されます。この分析では、起こりうるエラーの可能性と可制御性が予期される損害の恐れと同等に重きを置かれます。この分析の目的は、拘束力のある安全目標を定義することです。この時点から、定義された目標は開発で従うべき指針となり、まずはこの指針を作業グループ別の具体的な作業パッケージに分解する必要があります。

プログラミングは、たとえば成功事例に重点を置くこと、スタイルガイドの順守、構造化されたドキュメント、ひたむきな定期レビューとコード解析など、明確なルールと試験済みの方法にサポートされて行われなければなりません。もちろんテスト計画も必要です。ソフトウェアはいつどのように、またどのような前後関係でテストされるのでしょうか。故障注入テスト（故意に導入したエラーに対するソフトウェアの反応を調べるテスト）は必須です。そのようなテストを実行するためには、開発者はたとえば ETAS の EHOOKS などのようなバイパスフックツールを利用して不良データを送り込みます。これより早い段階で ISOLAR-EVE を用いて行うテストとは異なり、故障注入テストは実ハードウェアを使用して行います（図 1）。EHOOKS を使用すると、テストエンジニアは ECU の適合・診断インターフェースをアクセスポイントにして、ECU の内部信号の代わりに用意したエラーまたは故障データを仕掛けて ECU を操作することができます。その場合、故障データは ETAS INCA 計測・適合・診断ソフトウェアで生成されます。

AUTOSAR で安全に機能を制限

例外的な状況を引き起こすことによって、開発者はこれらの安全目標およびコンセプトが本当に守られているかどうかを知ることができます。ロバストなソフトウェアは故障を認識し、ECU を動作状態に保つか、安全な状態に移行させるかのいずれかを行う必要があります。また、予防策を講じてエラーが広がらないようにすることもできます。ここで、メモリ保護仕様を含む AUTOSAR 規格が役立ちます。開発者はソフトウェアが他のソフトウェア機能のメモリにアクセスするのを防ぐために、ハードウェアのサポートを利用することができます。これにより、エラーを局所的に封じ込めたままにして、安全に関連するソフトウェアアプリケーションを危険にさらさないようにすることができます。

また一方、AUTOSAR のメモリ保護またはタイミング保護のメカニズムを統合するためには、プロジェクトの参加者全員がソフトウェアコンポーネントのソースコードまたはオブジェクトコードを公表する必要があります。この透明性の度合いが足りないことや望ましくないことが往々にしてあるため、ETAS は RTA-HVR Hypervisor を開発しました。これは 1 個の ECU を複数個の厳密に分割されたバーチャル ECU に区画化するので、安全に関連する機能同士は互いから完全に守られます。区画間の通信は各種 ECU 間の通信と同じく、定義されているインターフェースおよび所定のルールを用いて行われます。

技術的および組織的な区画化

区画化により得られる重要なメリットがもう一つあります。さまざまな会社から参加しているチームが、後に分離して遮られた、自身の区画内で実行されることになるソフトウェアを、それぞれ他のソフトウェアとは無関係に開発できます。つまり、ソフトウェア開発早期にはコードへの相互アクセスは必要ないのです。それでも、並行開発を行うためには ECU メーカーがプロセスを調整して導く必要があります。参加者全員が利己主義から抜け出し、同じ安全目標および拘束力のあるスケジュールに従って尽力しなければなりません。これは開発パートナーが機能安全の証拠をいつ、どのような形で提供しなければならないかについての概要を示すものです。統合についての責任は依然として ECU メーカーが負い、サプライヤから供給されたテスト済みのソフトウェアコンポーネントとそのドキュメントを結合し、ECU の安全性を示す完全な証拠を提供することになります。

賢明なプロジェクト管理

絶えず検証し、正当性を示し、そして、必要な場合には（プロジェクトの）前提条件を調整することは、プロジェクト管理の一環であり一部です。パートナーも最新情報を取り入れ続ける必要があります。しかし、その努力は報われます。開発が共同安全哲学に導かれれば、テストの工数を減らすことができ、開発の最終段階で費用がかかり神経がいら立つような補正を行わなくて済むようになります。プロジェクト管理に厳密さが足りないと、往々にして問題に苦しめられることになります。監査および評価により、安全目標、前提、および作業目標についての解釈の違いが表面化されることは頻繁にあります。目標の定まった対策がないと、すぐに深刻なエラーチェーンが生じる可能性があります。このため、これらのチェックは ISO 26262 安全規格にしっかりと定められています。

まとめ

複雑な共同開発プロセスにおいても、ECU ソフトウェアの機能安全を確保することは可能です。ただし、そのためには単なる ECU 開発の知見以上のものが要求されます。たとえばバーチャル環境における評価など、標準化された開発と最新の手法を、入念に管理されている開発プロセスに徹底的に組み込むことの方がはるかに重要です。ETAS はツール、サービス、およびコンサルティングを通じて、プロジェクトの各フェーズに的確なソリューションを提案します。