連携する RTA-BSW と ISO 26262

ASIL-D:2018 のアプリケーションに準拠する ETAS AUTOSAR 基本ソフトウェア

車載ソフトウェアの機能が増えるにれ、機能安全の重要性は高まります。E/E アーキテクチャはますます複雑化し、機能安全の基準に合わせたソフトウェアの開発は非常に困難なものとなっています。これを乗り越えるための鍵の一つとなるものは、十分に試行された信頼に足る基本ソフトウェアです。TÜV SÜD は、ISO 26262 ASIL-D のアプリケーションにおいて ETAS AUTOSAR ソフトウェア製品を安全に使用するための適合性テストを実施し、結果は合格と判定されました。

ISO 26262 などの機能安全規格は、E/E システムの異常な挙動によって生じる危険な事態を防ぐ安全策の定義に重点を置いています。そのような安全策の例の一つに、ソフトウェアとハードウェアの要件適合性を検証するために用いられる「パフォーマンスインジケータ」があります。しかしそれらのインジケータは、自動車メーカーや Tier 1 サプライヤが自社システムの安全性を確認するうえで十分なものでしょうか？答は明らかに「ノー」であり、それには正当な根拠があります。

複雑性に対処して時間と費用を節約する

まずここで、平均的なプレミアムクラスの車について考えてみましょう。搭載されているソフトウェアは 1 億行ものコードを楽々と実行していますが、これは、2013 年型の F-35 ジェット戦闘機で使われているソフトウェアコードの総数の 4 倍以上にあたります。時代の趨勢は電動化と自動運転へと大きく動き、自動車メーカーは、車両 E/E アーキテクチャに対してかつて経験したことがないような無数の変更を加えることを余儀なくされてきました。しかしいくら変更を加えても、自動車ユーザーの安全要件は減りません。それどころか反対に、電子システムにはますます大きな責任が課せられ、機能安全が重要視されるようになっているのです。

すべての車載システムをカバーする安全要件を満たすには、まず明確な戦略を立て、安全を考慮したコンポーネントを設計しなければなりません。安全規格は自動車メーカーが守るべき義務を定めていますが、それを実現する手段までは示してくれません。そこでそのプロセスを容易にする助けとなるのが、認証を受けた機器コンポーネントの存在で、それらは広範囲なシステム認証に対する戦略を支える基礎になります。

自動車メーカーが直面している課題はほかにもあります。より短くなるプラットフォーム開発サイクルや、より強まるコストダウンへの圧力です。材料調達からソフトウェア開発、生産に至るまでの各工程は、絶えずチェックの目にさらされています。

安全性関連のソフトウェアの実装からレビュー、監査までには大変なコストを要しますが、どの工程も決して手抜きはできません。そこで、あらかじめ認証済みのコンポーネントを使用することが最良の解決策になるのです。

プロジェクト

ETAS は、安全志向のシステム開発を支援することを目的として、AUTOSAR 基本ソフトウェアである RTA-BSW の監査を TÜV SÜD に委託しました。TÜV SÜD は世界をリードする技術サービスプロバイダの一つであり、機能安全の分野におけるパートナーとして高い評価と信頼を得ています。TÜV SÜD Smart Software Program に基づくテストでは、機能安全要件を含めた RTA-BSW の認証適合性がチェックされました。TÜV SÜD はさらに、RTA-BSW の品質とセキュリティ機能に関して、全般的な安全管理や、ソフトウェア成果物に関する要件、ソフトウェア開発プロセスなどを分析しました。

RTA-BSW とは?

RTA-BSW は、ETAS が提供する量産対応型の AUTOSAR Classic 基本ソフトウェアのコレクションで、RTA-CAR と呼ばれる RTA Classic AUTOSAR 製品ポートフォリオの中核をなすものです。車載用ソフトウェアとして、20 年以上にわたり 20 億台近くの実車の ECU に使用された実績があり、生産後の不具合は全く発生していません。RTA-BSW は AUTOSAR R4.x の諸機能をサポートし、通信、メモリ、診断、安全性などの包括的な AUTOSAR スタック（モジュールの集まり）で構成されています。基本ソフトウェアの各モジュールは、さまざまな車両機能の開発に共通の基礎であるとされる円滑な中央 ECU との通信機能を実現します。

RTA-BSW には、機能安全基準を満たすアプリケーションに必要なすべてが揃っています。

本プロジェクトでは、乗用車やオートバイ、トラック、オフロード車など多様な車両をカバーできるよう、いくつもの安全規格を採用しました。適合性の評価では以下の安全規格が適用されました。

- ISO 26262:2018
- IEC 61508:2010
- ISO/DIS 19014:2018
- ISO 25119:2018

総合的評価において RTA-BSW は、機能安全モジュールの要件を含む TÜV SÜD Smart Software Program の要件を満たしていることが確認されました。これは英国、ドイツ、イタリアにおける ETAS の RTA チームにとって画期的な出来事となりました。RTA-BSW は ETAS のお客様に、高度な安全規格を達成するための強固な基盤を提供することができるのです。

まとめ

自動車業界は今日、無数の変化に直面し、その影響は車載ソフトウェア開発プロセスの個々のステップに及んでいます。とりわけ変化の影響が目立っているのは、安全性に関連した組み込みソフトウェアの領域です。時間とコストの削減を強いられる各企業は、差別化を重要視する一方で、AUTOSAR プラットフォームのような既成コンポーネントへの依存を余儀なくされています。ETAS は認証済みの AUTOSAR 基本ソフトウェア製品を通して、安全規格への最高レベルの適合を実現し、数々の課題を乗り越えるお手伝いをいたします。

執筆者

Luca Baldini、ETAS Ltd.（イギリス、ヨーク）
RTA-BSW プロダクトマネージャ
Daniele Garofalo、ETAS Ltd.（イギリス、ヨーク）
RTA ソリューションプロダクトマネジメント部門
グローバル統括
Jonathan Manktelow、ETAS Ltd.（イギリス、ヨーク）
安全性認証プロジェクトマネージャ