セーフティクリティカルな
アプリケーションの
連続モニタリング

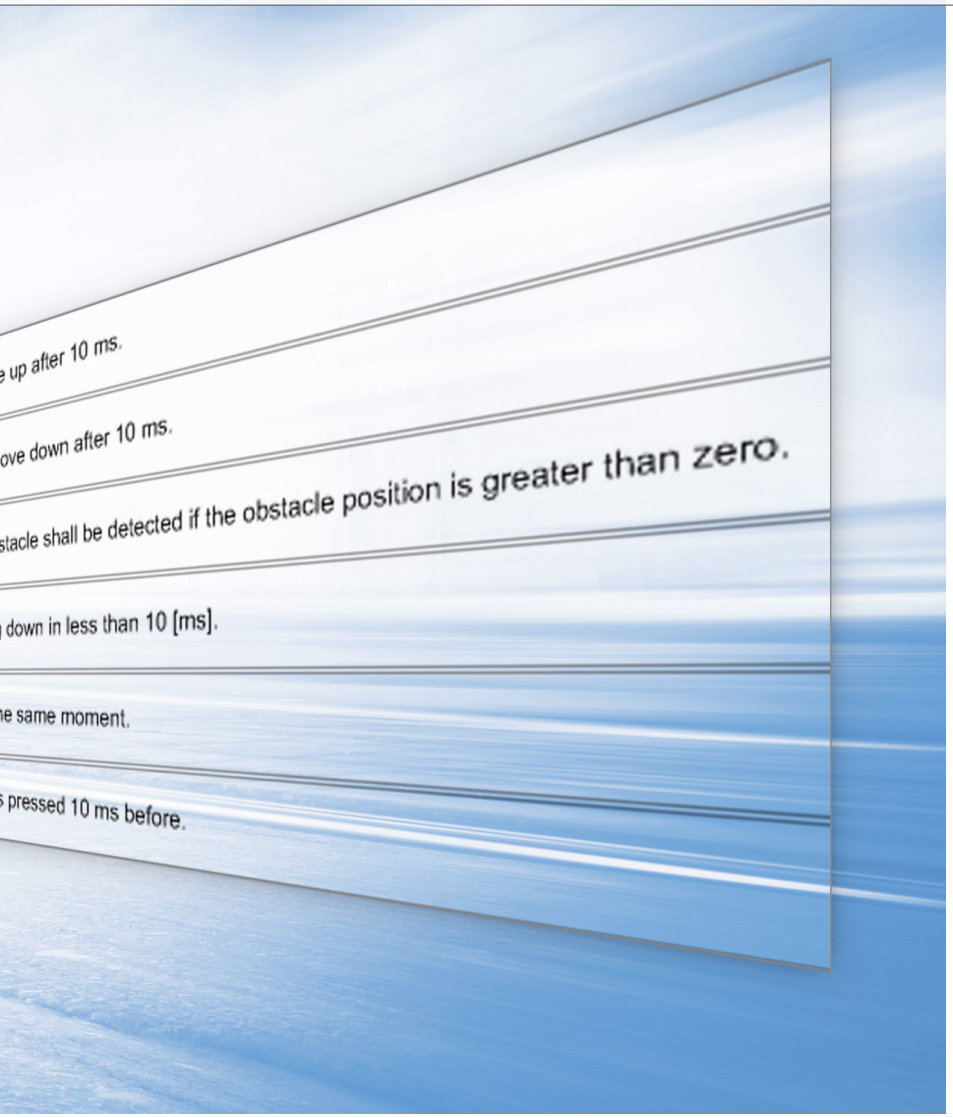
Keeping an Eye on Safety

セーフティクリティカルなシステムの妥当性を確認するには膨大なテストが必要となります。しかし、安全要件を満たしながらそれに必要な開発工数のバランスを取ることも大きな課題です。dSPACE と BTC 社は、セーフティクリティカルな ECU をシミュレーションベースで形式検証するための新しいソリューションを開発しました。これにより、開発工数を実現可能なレベルにまで近づけることができます。さらには、テスト深度の向上も可能になります。

技術革新を実現し、ユーザの利便性や安全性を向上せるための競争は世界中で繰り広げられており、それに伴い、電子的な安全関連システムの数は増え続けています。機械的なフォールバックシステムは、設計やコストの面からさまざまな領域で姿を消しています。そのため、電子的な安全関連システムを活用するうえで、それらを厳格な要件に基づいてテストすることが不可欠になっています。もし、X-by-Wire ステアリングシステムや自動運転システムに障害が発生したら、悲惨な事故の原因となってしまいます。

しかし、そのようなテストを行うことは、開発者にとって大きな課題となっています。なぜなら、システムの複雑性は極めて高く、要件リストも無限に近いほどあるにも関わらず、妥当性確認に使える時間は一定の範囲内に限られているからです。また、開発者は多数の重要なガイドラインも遵守する必要があります。たとえば、ISO 26262 規格（『道路用車両 – 機能安全』）では、電子制御ユニット（ECU）のセーフティクリティカルな機能に関して形式検証を実行することを推奨しています。

dSPACE では、このような課題を克服するため、BTC 社と連携してセーフティクリティカルなアプリケーションの形式検証をシミュレーションベースで行うことができるソリューションを開発しました。このソリューションを使用すると、セーフティクリティカルな要件への適合を dSPACE プ



ラットフォーム上で継続的かつリアルタイムで監視することができます。

テスト深度の向上

従来のテストプロセスでは、すべての要件やクロスリファレンスを考慮しながら、セーフティクリティカルな機能ごとに必要なすべてのテストケースを実行する必要があり、工数と期間が増えてしまうことがあるという深刻な問題がありました。結局、起こり得るすべての事態やクロスリファレンスを完全に網羅し、同時並行でテストを行うために定義しなければならないテストケースはどれくらいの数になるのか、そして、仮にそのように長大なテストケースのリストを定義することができたとしても、目標のテスト深度を達成するためにはすべてのテストケースに対してどれほどの実行時間が必要なのかを把握するのは困難を極めます。しかし、dSPACE と BTC 社が協力して開発した革新的なソリューションでは、新しい dSPACE Real-Time Testing (RTT) Observer Library と仕様記述ツールである BTC EmbeddedSpecifier® を組み合わせて使用することにより、開発者がテストプロセスの全体的な品質と進捗を効率的に評価できるようにしています。これらのツールでは、リアルタイム対応の要件オブザーバを使用することにより、既存 の MIL (Model-in-the-Loop)、SIL (Software-in-the-Loop)、および HIL (Hardware-in-the-Loop) 環境を補完します。また、シミュレーションの実行中にオブサーバが並行して実行され、すべてのセーフティクリティカルな要件への適合が監視されます。そのため、実装されたテストケースに応じて、どの要件がカバーされ、どの要件がカバーされていないかを直ちに表示することが可能です。形式検証をシミュレーションベースで継続的に行うこのソリューションは、未だ主流である従来の要件ベースのテストを補完するのに理想的と言えます。つまり、従来のテストとオブザーバベースのテストを組み合わせることで、テスト深度を大幅に向上させることができます。このようなオブザーバは、さまざまな dSPACE プラットフォーム上で簡単に使用できる実行形式のテスト基準と考えることができます。オブザーバは実際のシミュレーションモデルから分離されているため、既存のシミュレーションモデルをその都度変更する必要はなく、既存の従来のテストをオブザーバによって簡単に拡張することができます。

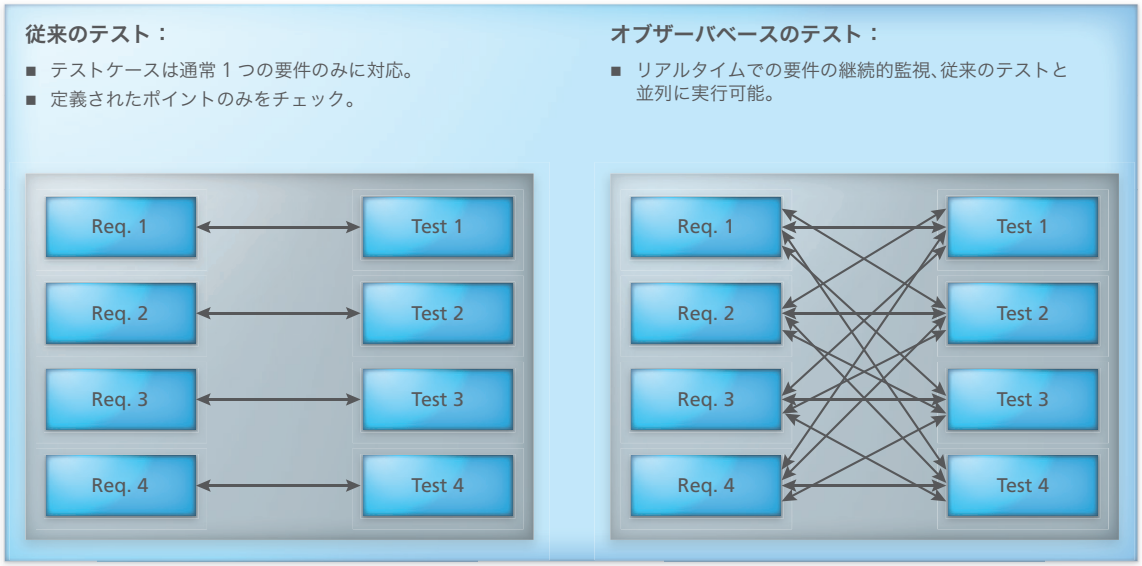
品質の向上

BTC EmbeddedSpecifier を使用すると、オブザーバの生成元となる要件の品質も

>>

「BTC EmbeddedSystems では、要件の形式化と形式検証における自社の長年の経験を組み合わせる対象として、実績のある強力な dSPACE シミュレーションプラットフォームおよびシステムを選択しました。この結果、完璧に調整された独自のツールチェーンが生まれ、特にセーフティクリティカルなアプリケーションではテストの品質と完成度が新たなレベルへと引き上げられています」

Hans Jürgen Holberg 氏、取締役会員、BTC Embedded Systems AG 社



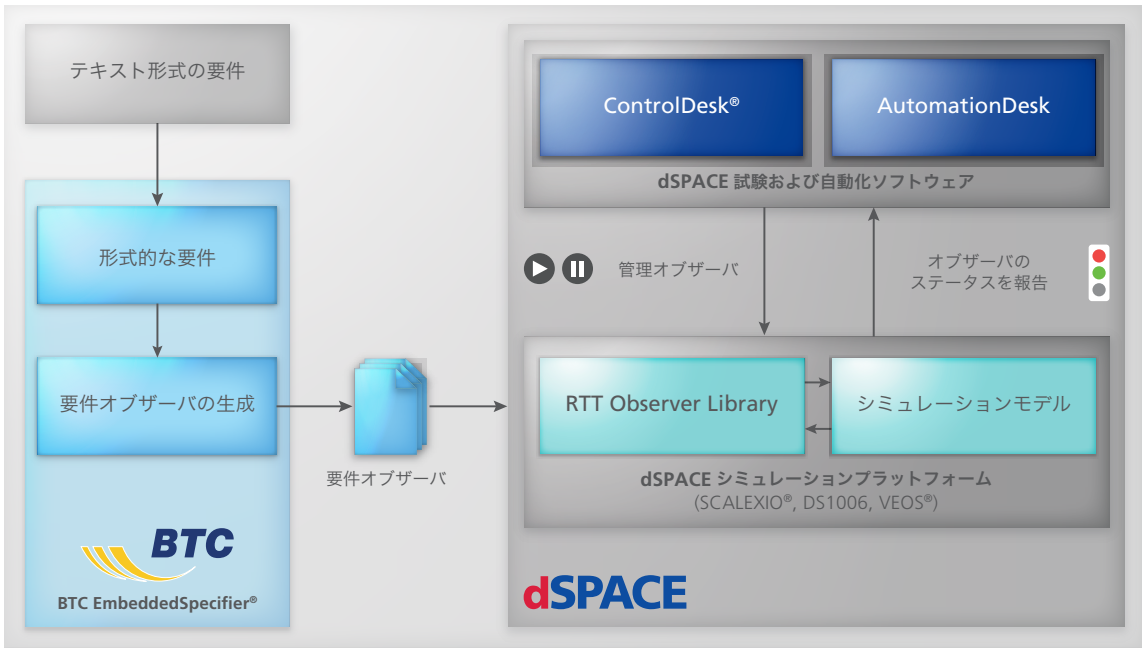


図 1 (上)：オブザーバベースのテストによりテスト深度が向上します。
図 2 (下)：生成されたリアルタイム対応のオブザーバは、dSPACE プラットフォーム上で容易に使用できる実行形式のテスト基準として機能します。

向上させることができます。BTC EmbeddedSpecifier では、ツールサポートによって非形式的要件を容易に形式表現に変換し、さらに dSPACE プラットフォーム向けの実行形式のオブザーバへと変換することができます。また、ガイド機能を利用して、従来の言語ベースでの要件定義や具体的なモデル変数の直接参照における曖昧さを段階的に排除することも可能なため、要件を可能な限り正確に記述することができます。これにより、関連する安全規格やガイドラインへの適合も可能になります。

理想的な統合

dSPACE では、ユーザが要件オブザーバをすぐに使えるようにするためのソリューションとして、テストオートメーションソフトウェア AutomationDesk で使用するテストテンプレートや試験用ソフトウエア ControlDesk で使用するレイアウトを提供しています。このソリューションは、他のツールに統合することができるだけでなく、ControlDesk で使用するためのオ

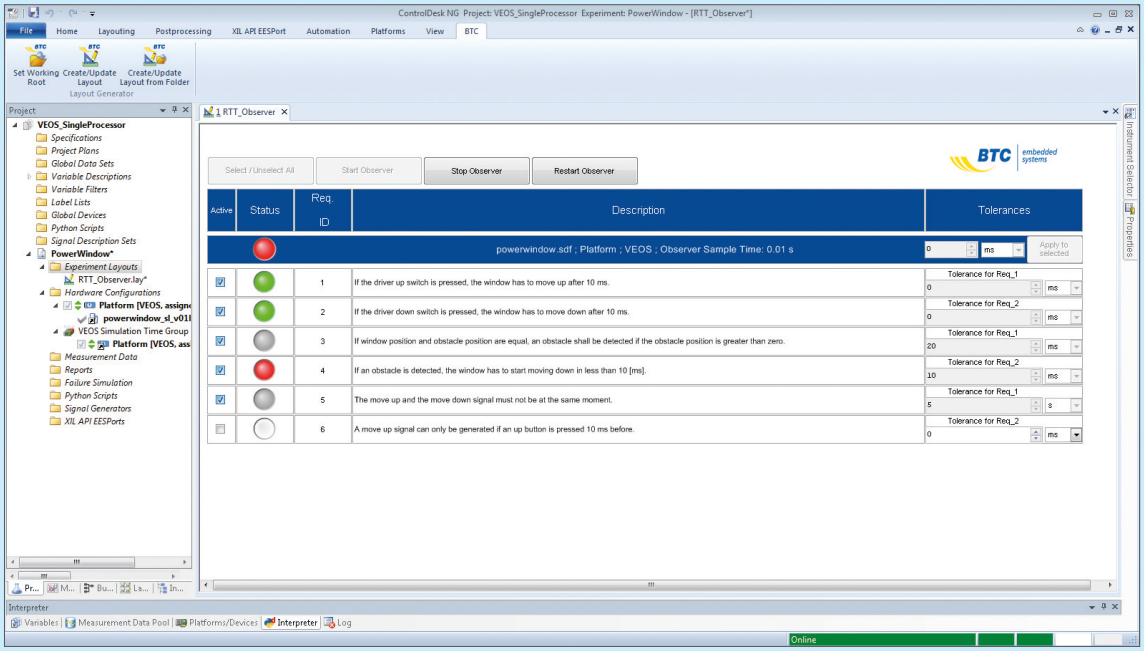


図 3:オブザーバは ControlDesk で開始、停止、およびリセットすることができます。要件が適合した場合（緑）と適合しない場合（赤）が直ちに表示されます。前提条件が満たされていないために開始していないオブザーバは、グレーで表示されます。

ブザーバ専用のレイアウトを自動的に生成し、テスト全体の実行中に各要件の適合ステータスを ControlDesk に表示することも可能なため、利便性が向上します（図 3）。

ControlDesk レイアウトを使用すると、オブザーバをシミュレーションモデルから完全に独立させ、個別に開始、停止、およびリセットすることができます。AutomationDesk テンプレートを使用すれば、指定されたテストシーケンスを AutomationDesk で実行しながら、オブザーバを使用して要件を継続的にチェックすることも可能です。

この場合、生成されるテストレポートには個々のテストケースの結果だけでなく、オブザーバの結果も表示されます。オブザーバがトリガされた時間を確認すると、トリガが発生した原因とエラーを特定することができます。

さまざまなプラットフォームでの使用

生成される要件オブザーバは、さまざまな dSPACE シミュレーションプラットフォーム（SCALEXIO®、DS1006、VEOS®）で使用でき、オブザーバを複数のプラットフォーム間で再利用することも可能です。そのため、テストレベルが同じであれば、SIL および MIL 開発段階で作成された dSPACE VEOS での仮想検証用のオブザーバを SCALEXIO プラットフォームなどでの HIL テストにおいても直ちに再利用できます。HIL テストは、VEOS 上で「テストのテスト（test-the-test）」を使用して準備することもできます。

まとめ

dSPACE Real-Time Testing（RTT）Observer Library と BTC EmbeddedSpecifier を組み合わせて使用することにより、テスト期間を延長することなく、特にセーフティクリティカルなアプリケーションにおいてテスト深度を大幅に向上させることが可能な高品質なソリューションが実現します。テスト深度を大幅に向上させるには、現在のテストケースやシミュレーションシナリオには関わりなく、各要件の適合状態を継続的に監視することが重要です。これにより、意図しない副次的な作用によってエラーが検出されないというリスクが最小限になります。BTC EmbeddedSpecifier のツールサポート機能を利用して要件を定型化すれば、要件の品質向上も可能になります。この新しいソリューションは、HIL テストおよび仮想検証用の dSPACE ツールチェーンに完全に統合することができます。