自動車向け機能安全規格である ISO 26262（『道路用車両 – 機能安全』）は、2011 年 11 月に正式発行されました。この規格では、安全関連の車載電気／電子システムの開発および生産における機能安全を保証するためのプロセスおよび方法が規定されています。この規格は、技術の実態に関する規定であるため、自動車メーカーはその遵守を義務付けられています。ところで、自動車メーカーはこの一般的な要件を具体的な開発手順にどのように反映させれば良いのでしょうか。アプローチの 1 つとして、TÜV SÜD 社などの認証機関によって認証されたリファレンスワークフローとツールを使用することが挙げられます。このようなアプローチを採用することで、結果的に製造物責任に関するリスクを低減することもできます。

ソフトウエアツールの使用に関する ISO 26262 の要件

ISO 26262 では、安全関連プロジェクトで使用するソフトウエアを最初に特定の適用分野に分類するよう規定しています。この分類には、ツールが機能安全要件を満たしている場合と満たしていない場合の影響を分析することも含まれています。分類結果は、ツール信頼レベル（TCL）と呼ばれます。次に、TCL に基づいてツールの認証を受ける必要があります（42 ページの情報ボックスを参照）。通常、認証を行う際は、適切な認証方法を組み合わせる必要があります。どの方法を組み合わせるかは、そのソフトウエアツールで開発およびテストされるシステムの自動車安全度水準（ASIL）によって異なります。これには、ツールの開発に関連するプロセスや手法に対する十分な知識が必要となるため、これらの認証方法を実装することは非常に困難で手間がかかります。つまり、認証方法の実装には、ツールの開発環境が ISO 26262 に準拠しているかを査定するための専門的知識が要求されます。

TÜV SÜD 社の認定

TÜV SÜD 社では、パーダーボルンにある

>>

安全関連システムのテストで使用する dSPACE のテストオートメーションソフトウエア AutomationDesk は、ISO 26262 および IEC 61508 規格への準拠について、2014 年に TÜV SÜD 社の認定を取得しました。市販の HIL（Hardware-in-the-Loop）シミュレーション用テストオートメーションソフトウエアとしてこの認定を受けるのは、AutomationDesk が初めてです。これはユーザにとって一体どのような意味があるのでしょうか。

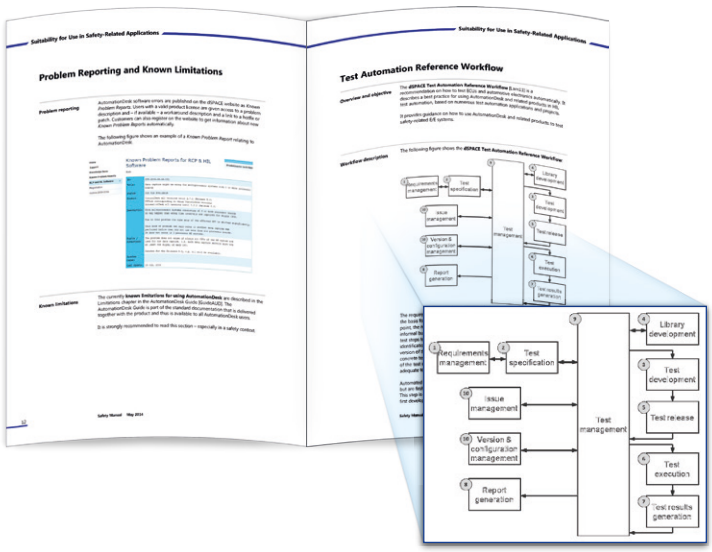
AutomationDesk が TÜV SÜD 社の認定を
取得したことにより、開発プロセスを
ISO 26262 および IEC 61508 規格に
準拠した形で非常に容易に分類、認証、
および妥当性確認できるようになります。

ISO 26262 および IEC 61508 で規定される内容

IEC 61508 は、国際的に認知された、安全関連の電子システム開発の汎用規格です。自動車業界では、2011 年末に乗用車の機能安全規格として、それまでの IEC 61508 に代わって ISO 26262 が正式発行されました。ISO 26262 は、IEC 61508 を修正した規格であり、自動車業界の特定の状況に対応できるよう調整されています。これらの規格を実装すると、電気／電子コンポーネントを搭載した車両システムの機能安全が保証されます。これらの規格を遵守するためには、電気／電子コンポーネントの開発に使用するツールの分類、認証、および妥当性確認が必要になります。

ISO 26262 では、ツールの認証のために 4 つの方法を規定しています。それぞれの ASIL に応じて、ユーザは以下の方法を適切に組み合わせて選択することができます。

a. 使用による信頼性の強化 (ISO 26262-8、11.4.7 ～ 11.4.10)
b. ツール開発プロセスの評価 (ISO 26262-8、11.4.8)
c. ソフトウエアツールの妥当性確認 (ISO 26262-8、11.4.9)
d. 安全規格に基づいた開発 (ISO 26262-8、11.4.10)



AutomationDesk 安全マニュアルとテストオートメーションリファレンスワークフロー

dSPACE GmbH との密接な協力のもと、AutomationDesk の品質や開発環境を監査するため、dSPACE 組織内のプロセスやドキュメンテーションを詳細に分析しました (43 ページの情報ボックスを参照)。また、新しい AutomationDesk 安全マニュアルについても査定し、お客様とのコミュニケーションプロセスやバグレポートも調査しました。その結果、TÜV SÜD 社 は、AutomationDesk が “Software Tool for Safety-Related Development” (「安全関連開発用ソフトウエアツール」) であることを認定しました。これにより、AutomationDesk が自動車、商用車、航空機、およびその他の多くの産業分野における安全関連システムのテストに適していることが明確に示されました。これは、AutomationDesk を使用して安全関連システムのテストを行えば、ASIL A ～ ASIL D、および SIL1 ～ SIL3 までのすべての自動車安全度水準 (ASIL) に関して、そのプロセスは ISO 26262 および IEC 61508 規格に準拠している、つまり「用途に適合する」ことを公式に確認したものでもあります。

AutomationDesk 安全マニュアル

この認定を取得できた重要な要素の 1 つに、AutomationDesk 安全マニュアルがあります。これは、AutomationDesk を安全関連プロジェクトで使用するための補足的ユーザドキュメントです。このマニュアルでは特に、下記について説明しています。

- AutomationDesk の概要、およびすべての使用可能な製品とユーザドキュメント
- AutomationDesk の使用や運用のための推奨事項およびベストプラクティス (AutomationDesk テストオートメーションリファレンスワークフローを含む)
- ISO 26262 で規定されたテストプロセスにおけるテストオートメーションリファレンスワークフローの例
- AutomationDesk に関するツール分類
- AutomationDesk が ISO 26262 および IEC 61508 に基づいて「用途に適合する」ことを認定する証明書

安全関連システムの開発を有益にサポート

独立した認証機関である TÜV SÜD 社は、AutomationDesk の開発プロセスおよび総合的な品質保証を認定しています。そのため、常に AutomationDesk 安全マニュアルの説明に従って AutomationDesk を使用すれば、ユーザは規格のために自社の

AutomationDesk：HIL テストオートメーション用の市販ソフトウエアとして初めて認定を取得しました。

ツールをわざわざ分類する必要がありません。また、AutomationDesk の認証も非常に簡単になります。AutomationDesk は、認証方法「ツール開発プロセスの評価」および「ソフトウエアツールの妥当性確認」の該当する基準、および「使用による信頼の強化」の基準のほとんどを満たすソフトウエアであることが証明されているためです。

AutomationDesk は、テストオートメーションを HIL (Hardware-in-the-Loop) 環境で行う市販ソフトウエアとしてこの認定を受けた最初の製品となりました。AutomationDesk 安全マニュアルを使用すると、ISO 26262 および IEC 61508 に準拠した安全関連システムを AutomationDesk で開発およびテストする際に必要な有益な情報を得ることができます。AutomationDesk が TÜV SÜD 社の認定を取得したことにより、規格に準拠した開発プロセスの分類、認証、および妥当性確認が非常に容易になります。

今後の展望

認定を受けた AutomationDesk のソフトウエアバージョンは 4.1 です。2015 年の夏にリリース予定の新しい AutomationDesk バージョン 5.0 に対する認定も間近に迫っています。今後のバージョンについても、必要に応じて認定を受ける予定です。TÜV SÜD 社による AutomationDesk の認定に関する詳細は、dSPACE 販売代理店にお問い合わせください。 ■

TÜV SÜD 社の監査基準

TÜV SÜD 社は、AutomationDesk の認定にあたり、dSPACE の AutomationDesk 担当部門を監査しました。TÜV SÜD 社は以下の各項について検査を行いました。

- 要件管理、変更管理、リリース管理などの AutomationDesk の開発プロセス
- 要件に基づくテスト結果のトレーサビリティといった AutomationDesk の妥当性確認
- お客様とのコミュニケーションプロセス
- AutomationDesk 安全マニュアル

上記の各項に関する査定は、仕様書、詳細な機能およびコンポーネント指向の仕様、設計ドキュメント、テストカタログ、テスト結果、プロセスドキュメンテーション、全社的開発規定、プロジェクト固有の修正など、AutomationDesk に関連するすべての開発ドキュメントに基づき現地で行われました。短期間で認定を取得するには、他部門との協力関係が鍵となりました。TÜV SÜD 社の査定では、AutomationDesk の開発プロセスは既に非常に高いレベルで基準を満たしていました。dSPACE は、監査で受けたいくつかの改善提案を直ちに実施し、その結果、認定を取得することができました。