Mercedes-Benz Research & Development North America 社は、dSPACE TargetLink の戦略パートナーである Model Engineering Solutions 社と協力し、TargetLink を使用した量産コードの自動生成のためのモデリングで必要となるテストを自動的に実行する適合ルールを開発しました。これらのルールは、ISO 26262 規格の主要な要件に準拠しています。

Mercedes-Benz Research & Development North America（MBRDNA）社はミシガン州のレッドフォードなどを拠点としており、インバータソフトウェア（発電機の電流変換）の開発および統合を専門に扱っています。これらのソフトウェアは dSPACE TargetLink® を使用して開発されており、Mercedes-Benz の E-Drive ポートフォリオにおけるさまざまな車載アプリケーションで使用されています。主要コンポーネントの 1 つは、関連するトルクおよび高電圧の安全コンセプトを含むモーター制御モデルであり、ISO 26262 の ASIL C 要件に従って実装することができます。このコンポーネントには革新的な技術が実装されています。

開発プロセスとモデル品質

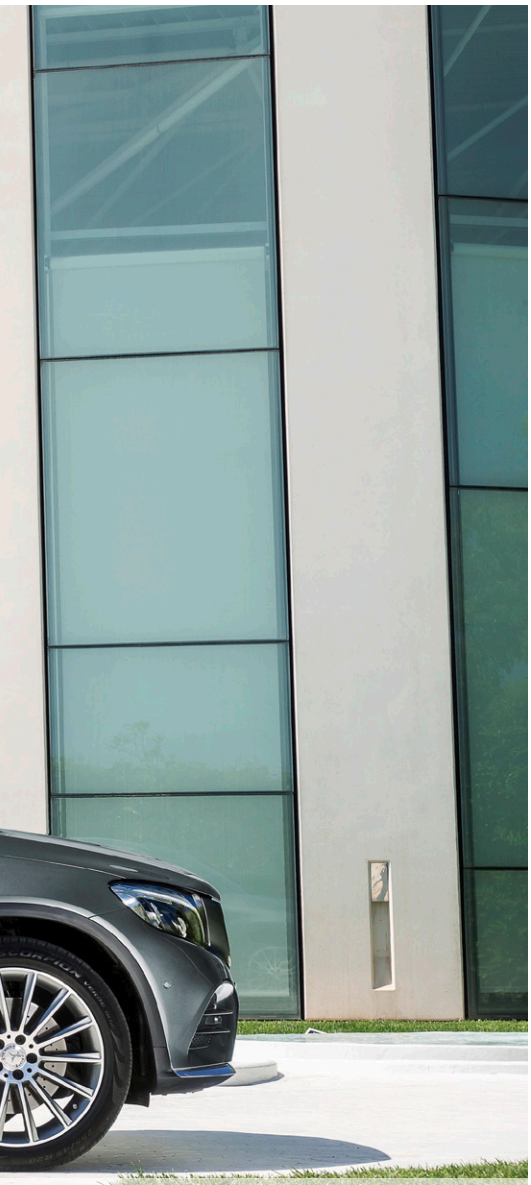
E-Drive ソフトウェアは、AUTOSAR ソフトウェアアーキテクチャベースで開発され

モデリングガイドラインを使用した
Electric Drive ソフトウェアの検証

Electric and Safe

出典：© Mercedes-Benz

ており、多くの電動ドライブトレイン用に拡張することができます。制御ソフトウェア全体は、V サイクルに従い、モデルベースの設計手法に沿って開発されます。dSPACE の量産コード生成ツールである TargetLink は、これらの開発ツールチェーンにおける中核的なコンポーネントです。TargetLink は、AUTOSAR に準拠したソフトウェアアーキテクチャのモデリングおよびコード生成をサポートしており、安全関連ソフトウェアへの適合性を示す ASIL D の認定を取得しています。Simulink® および TargetLink を使用して制御ロジックソフトウェアをモデリングすると、開発の早期段階で要件の妥当性確認を行うことができます。なぜなら、コード生成に使用されるモデルの品質は生成したソフトウェアの品質に直結するためです。Simulink/TargetLink を使用したソフトウェアのモデリングは、高品質のソフトウェアを生成する手法として業界で広く受け入れられています。また、この手法は Simulink などの準公式モデリング言語の使用を推奨する ISO 26262 規格にも準拠しています。MBRDNA 社は、妥当性確認を静的な手段と解析的な手段を組み合わせて行うことで、高いモデル品質を確保しています。また、顧客が求める機能的要件からは独立した開発手法を確立することで、最適な形でソフトウェアを目的の環境に統合できるようにしています。



ソフトウェア設計のルール

この手法の重要なポイントは、ソフトウェア設計においてモデリングルールおよび適合ルールを一貫性を保ちながら使用することです。MBRDNA 社で使用するルールは、Daimler 社のモデル開発に関する内部規定に基づいており、E-Drive ソフトウェアの開発要件に合わせて調整されています。Daimler 社のモデリングガイドラインは、MAAB、MISRA Simulink/Stateflow、MES Functional Safety Guidelines、MISRA TargetLink、dSPACE TargetLink Modeling Guidelines などのモデリング規格や個別のツールガイドラインに基づいています（図 1）。これらのガイドラインはすべて異なる対象を扱っています。そのため、安全関連ソフトウェアを ISO 26262 に準拠してモデリングする場合、必要なあらゆる側面をカバーするには、これらのガイドラインを適切に組み合わせる必要があります。MAAB（MathWorks Automotive Advisory Board）のルールでは、シミュレーションおよびコントローラモデルの設計面、ならびに可読性、保守性、ベストプラクティスにも重点を置いています。しかし、量産コード生成には重点を置いていません。一方で MISRA Simulink/Stateflow および MISRA TargetLink のガイドラインでは、生成済みのモデルやコードの安全面に重点を置いており、Simulink および Stateflow の安全な言語範囲、安全なコードパターンを実現するためのモデリングパターン、シミュレーション環境の適切な設定が定義されています。さらに、MISRA/TargetLink や dSPACE TargetLink Modeling Guidelines などの個別のツールガイドラインでは、主に TargetLink によるコード生成に重点が置かれています。これらのガイドラインに完全に適合するには、生成後のコードのプロパティに悪影響を与える可能性のあるモデリングパターンや設定が、すべてのモデルまたはコード生成ツールに含まれていないことが必要になります。また、MES Functional Safety Guidelines では、モデルや生成したコードの安全性に関する注意事項に焦点を当てています。これらのガイドラインは ISO 26262 およびその他の安全規格から派生したものであり、安全関連ソフトウェアの設計に関する既存のガイドラインを補完するものです。ここで解析の鍵となるのは、データフローおよび制御フローの検証です。

TargetLink モデルのテストを自動化

MBRDNA 社は、モデリングガイドラインを一層利用しやすくするという目標の下、TargetLink 戦略パートナーである Model Engineering Solutions GmbH（MES）と協力し、既存のドキュメントをベースとした独自の Daimler モデリングガイドラインを策定し、さらに Daimler 社固有のニーズに対応するよう適用範囲

>>

> 「ソフトウェアシステムの複雑さはますます増大しているため、従来のテスト環境では限界に達しています。当社のソフトウェア品質保証において、作成したモデルや変換したソフトウェアを自動的に解析する機能は不可欠な存在です」
>
> Alexander Dolpp 氏、Mercedes-Benz Research & Development North America, Inc. 社

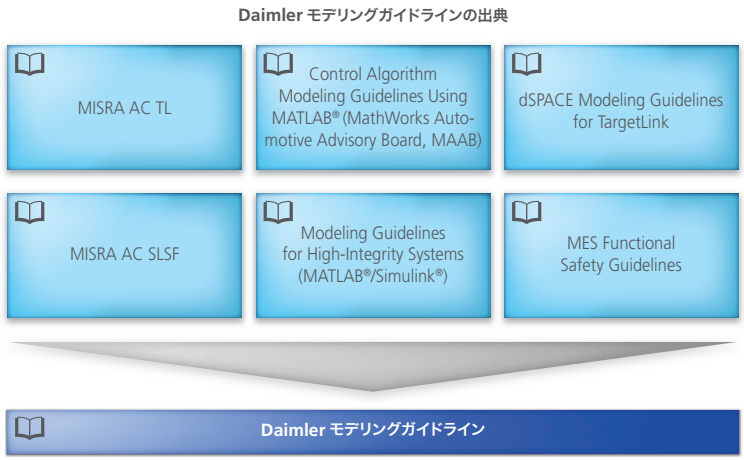


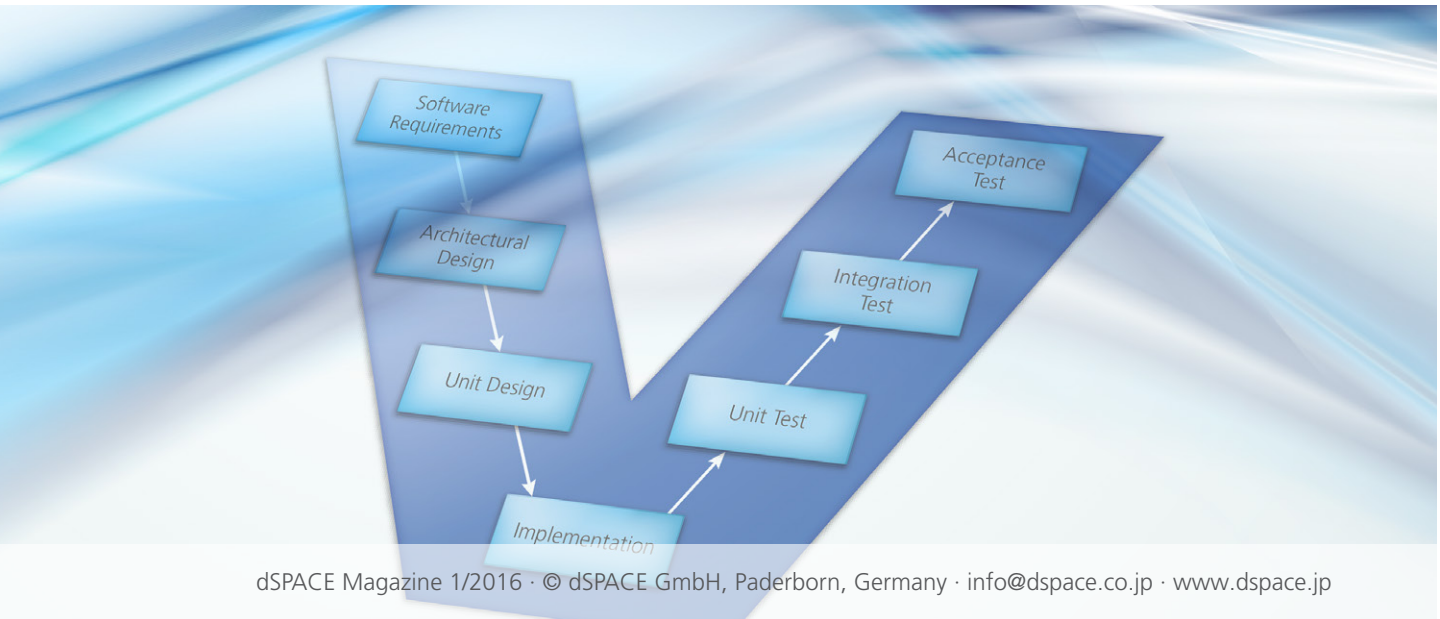
図 1：Daimler モデリングガイドラインは、確立された多数の規格およびガイドラインをベースとしています。

を拡大しました。ガイドラインの管理は MES Model Examiner (MXAM) で行われており、TargetLink モデルの自動的なテストも行われます。MBRDNA 社では、モデリングガイドラインを遵守することにより、ISO 26262 のモデリング要件への適合、ベストプラクティスの実践、モデリングエラーの回避を実現しているほか、シミュレーション環境やコード生成ツールで統一した設定を使用するなど、ツール固有の設定にも配慮しています。

きめ細かな安全性の確立

MISRA モデリングガイドラインが調整される場合の一例をご紹介します。Daimler モデリングガイドラインでは、Stateflow のセマンティクスの誤解釈を回避するため、状態や遷移のグラフィカルな配置ではなく、ユーザのみが実行順序を決定することを宣言することで Stateflow 遷移の正しい実行順序を決定していますが、この場合、Daimler モデリングガイドラインは MISRA ガイドラインと矛盾します。つまり、状態がレイアウト上の理由で移動されると (シンタックスの変更)、状態の実行動作も変更 (セマンティクスの変更) されてしまう可能性があります (図 2a を参照)。図 2b に示すように、接合点で評価される Stateflow の遷移でも同様です。誤解釈や実行動作の意図しない変更は、モデリング担当者が Stateflow の「User specified state/transition execution order」設定を使用して指定した実行順序を計算すれば、容易に回避することができます。MES Model Examiner (MXAM) のモデルチェック機能を使用すると、モデルとガイドラインとの適合性が自動的に検証され、直ちにモデルが修正されます。

> 「モデリングガイドラインや MES Model Examiner などのガイドラインチェッカーを活用すると、ISO 26262 の要件を自動的に実装できるため、モデル開発担当者の負荷を減らすことができます。当社では、彼らに制御機能の開発という本来の主要タスクに集中して欲しいと考えています」
>
> Ingo Stürmer 博士、Model Engineering Solutions 社



「AUTOSAR 規格をネイティブにサポートしながらコードの生成を行える TargetLink は、当社の開発ツールチェーンの中心的なコンポーネントです」

Alexander Dolpp 氏、Mercedes-Benz Research & Development North America, Inc. 社

明確なプロセス

すべてのモデリング担当者およびソフトウェア開発者は、モデリングガイドラインを遵守する必要があります。そのため、新しい機能が追加されるたびに、MXAM による自動モデルチェック機能を実行する必要があります。ソフトウェアをバージョン管理システムにチェックインするには、ソフトウェアがモデリングガイドラインに適合し、関連する機能的 MIL（Model-in-the-Loop）テストを実施することが条件となります。モデリング担当者の責務は、ガイドラインに基づいて特定されたすべての違反を排除することです。この静的なモデリング解析手法は、E-Drive ソフトウェアの開発および妥当性確認の V サイクルにおいて、すべての妥当性確認手段に組み込まれています。MBRDNA 社では、Daimler モデリングガイドラインに自動適合チェック機能を持つ MXAM および dSPACE の量産コード生成ツール TargetLink を組み合わせて利用することにより、業界で実績のある手法に基づいてモデルを ISO 26262 の要件に適合させつつ、モデル品質の早期の段階での改善とコード品質の大幅な向上を達成しています。

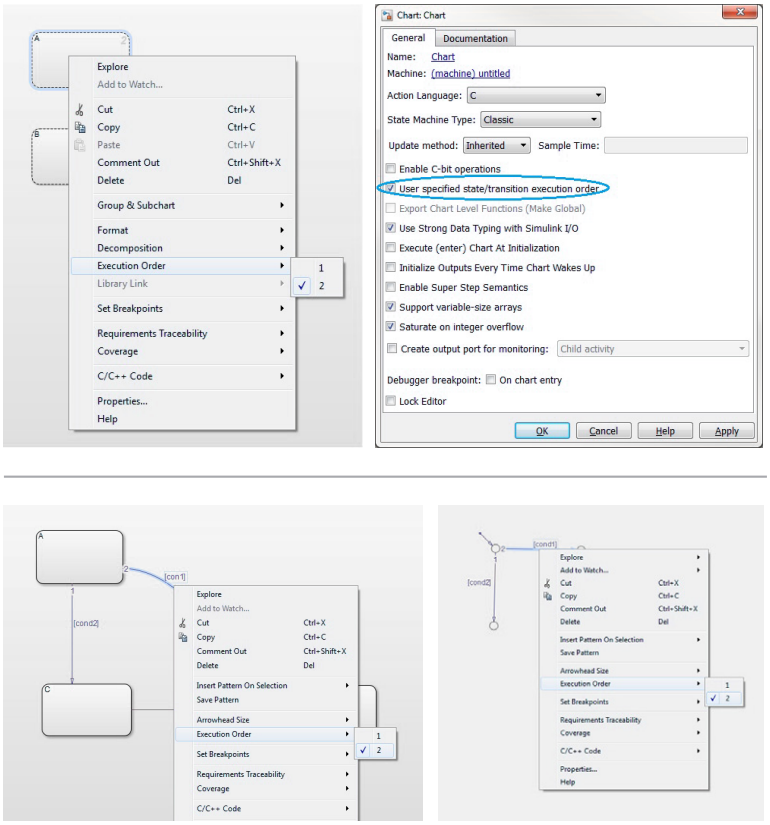


図 2a（上）：MES Model Examiner の一般的な事例 – 並列状態の実行順序（上図は Stateflow で指定）
図 2b（下）：ユーザ指定による遷移の実行順序

Alexander Dolpp 氏
E-Drive Software 部門担当者、
Mercedes-Benz Research &
Development North America, Inc.
（米国ミシガン州レッドフォード）

Ingo Stürmer 博士
Model Engineering Solutions GmbH
の創立者兼前 CEO。2016 年 1 月以降は
Model Engineering Solutions Ltd.（英国）
の責任者。