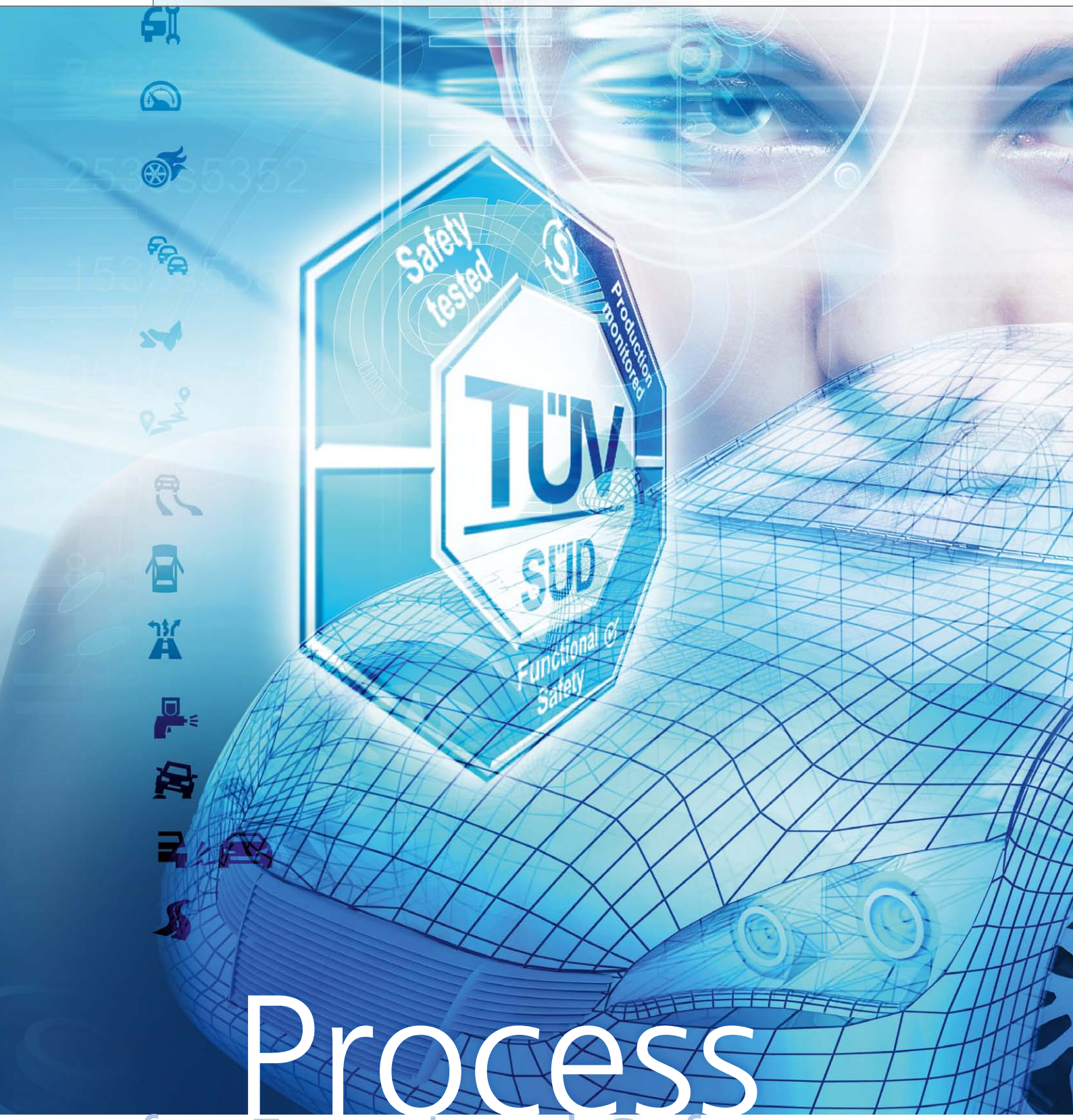


Process for Functional Safety

ISO 26262に準拠した電動ドライブトレインの
モデルベースソフトウエア開発

Siemens社のドライブテクノロジ部門は、セーフティクリティカルな車両機能の実装のために、標準的なソフトウエア開発プロセスにモデルベース開発を追加しました。dSPACEのTargetLink戦略パートナーであるModel Engineering Solutions GmbHの支援を得て、Siemens社のドライブテクノロジ部門は、dSPACE TargetLinkをベースにしたISO 26262（道路用車両の機能安全）の要求を満たすプロセスを定義しました。

自動車に使用されるセーフティクリティカルなソフトウエア

自動車業界のサプライヤの多くは、セーフティクリティカルなソフトウエアのモデルベース開発をすでに採用している、もしくは今後のソフトウエア開発プロセスにモデルベースの手法を導入する必要性に直面しています。モデルベース開発には、ソフトウエアの品質向上やソフトウエアの保守が簡単になるなど、実証済みのさまざまな利点があります。新しいISO 26262の導入にともなって、車載電気／電子システムの機能安全に関する国際規格が整備されました。ISO 26262は、IEC 61508安全規格を車両に特有の条件に適合するように改訂して制定された規格です。元のIECの規格とは異なり、ISO 26262はモデルベース開発を対象としていることは明らかです。この新しい規格には、ソフトウエアの機能安全を保証するために、それぞれの自動車安全性レベル（Automotive Safety Integrity Levels（ASIL）、レベルA～D）に対して、セーフティクリティカルな車載ソフトウエア用開発プロセスが「何を」達成しなければならないかが、はっきりと規定されています。ただ、「どのようにして」実装するかについての規定は、ほとんどありません。実際に経験してみると、この規格を適用するための広く認められているアプローチがまだ存在していないことが分かります。企業や部門の既存のプロセスとツールチェーンも考慮に入れる必要があるため、成功を収めているのは特定のプロジェクトのソリューションに限られます。

Siemens社の電気自動車用コンポーネント

Siemens社のドライブテクノロジ部門は、電気自動車用の主要コンポーネントの開発、製造、販売を行っています。それぞれのプロジェクトにおいて、自動車業界の顧客に特有の要件を常に念頭に置きながら、プロジェクトベースの視点に基づいて日常の業務を遂行しています。そのポートフォリオは、モーターとパワーエレクトロニクスからインテリジェントな車載充電テクノロジまでの広い範囲をカバーしています（図1）。Siemens社には、ソフトウエア機能の開発では広く普及しているVサイクルに沿った標準的な開発プロセスがすでに確立しています。この開発プロセスは、自動車用SPICEのガイドライン（aSPICE：国際規格ISO/IEC 15504 'SPICE'の自動車用としてのニーズに合わせて改訂されたバージョン）とCMMI-Dev（Capability Maturity Model Integration for Development（能力成熟度モデル統合））に準拠しています。事実上すべての自動車メーカーが、この2つの成熟度モデルへの準拠を要求するため、この2つの成熟度モデルに準拠していることが絶対的に必要となります。

セーフティクリティカルなソフトウエアのモデルベース開発の要件

Siemens社のドライブテクノロジ部門は、セーフティクリティカルな車両機能の大部分を、今後は、MATLAB®/Simulink®/Stateflow®およびdSPACE TargetLink®によるモデルベース開発の手法を使用して開発することを計画していたため、モデルベース開発を既存の標準的な開発プロセスに統合することを希望していました。この目標を達成するために、いくつかの条件を満たす必要がありました。

- 既存のプロセス環境に最適に統合でき、使用可能なツールを考慮し、必要なプロセス特性（aSPICEへの適合など）に違反しないモデルベース開発を行うためのISO 26262準拠プロセスを定義する。
- ISO規格のパート6（製品開発：ソフトウエアレベル）に焦点を合わせて、ASIL A～Dに対するすべての要求を満たす。
- モデルアーキテクチャを設計するための手順と設計パターンを、ISO 26262の規定に沿ってSimulinkとTargetLinkを使用して定義する。
- 生成されたコードレベルで、すべての機能要求が確実に追跡できるようにする（要求のトレーサビリティ）。
- モデルレベル、つまり、生成されたコードが使用できるようになる前の時点でも要求に対するテストができるようにする。

ISO 26262に準拠したプロジェクト固有の実装の計画

これらの要求を実装するために、Siemens社のドライブテクノロジ部門は、専門パートナーとしてModel Engineering Solutions GmbH（MES）社を選びました。MES社は、TargetLink戦略パートナーとして、車載組込みソフトウエアの品質保証に関する法人顧客を対象としたコンサルティングサービスを提供しています。MES社は、ギャップ分析（戦略および作業におけるギャップを識別）、プロセスモデリング、プロセスマニュアル、プロセス実装のサポートなどを含め、dSPACEツールを使用したISO 26262準拠の開発に関するすべてをカバーするdSPACE TargetLinkパートナーサービスを提供しています。MES社には、数多くの量産プロジェクトを通じて、セーフティクリティカルな自動車用ソフトウエアのドイツでの開発方法や、特にモデルベースのソフトウエア開発において、ISO 26262の要求を最も良く実装する方法に関して総合的なノウハウの蓄積があります。

Siemens社ドライブテクノロジ部門でのモデルベース開発プロセス

Siemens社のドライブテクノロジ部門では、自動車用電動ドライブトレインの分野におけるISO 26262準拠のソフトウエア開発を行っています。ドライブトレインは

図1：自動車用永久磁石同期モーター

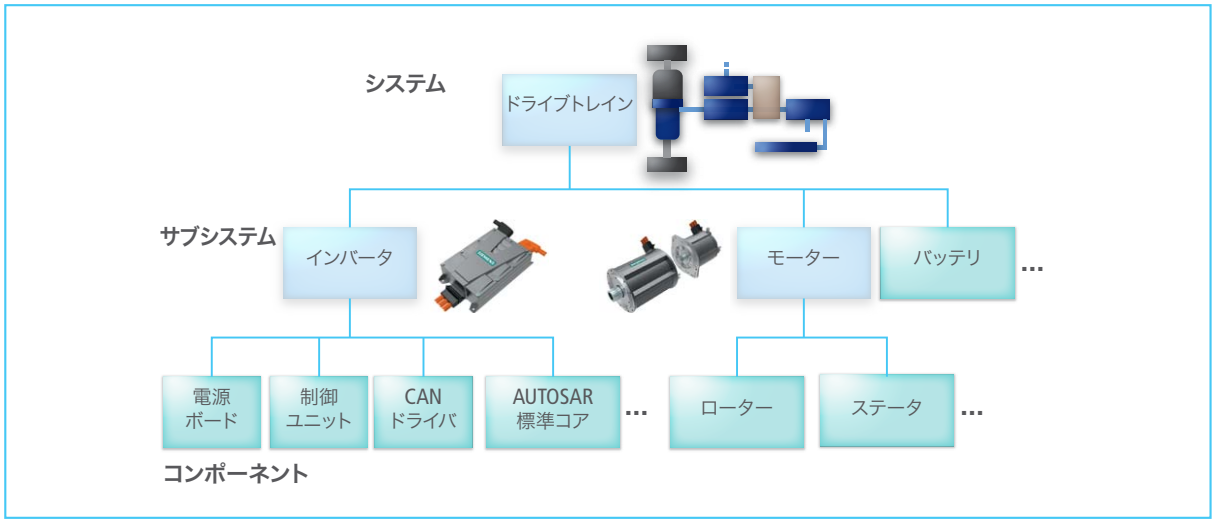


図2：電動ドライブトレインのシステム分割およびレベルの定義

複雑なシステムであり、さまざまなサブシステムとそれに関連するシステムレベルに分割することができます（図2）。サブシステムレベルに位置付けられるインバータは、バッテリ（直流）とモーター（交流）との間の電気エネルギーの流れを実装し、モーターは電気エネルギーを機械エネルギーに変換します。これらのサブシステムは、モーターステータやインバータの制御エレクトロニクスなどのコンポーネントで構成されています。これらの制御エレクトロニクス上で実行されるランタイムソフトウエアは、コンポーネントレベルの下の階層の、モジュールレベルと呼ばれるレベルに配置されます。ソフトウエア自体（この図には示されていない）も、いくつかのソフトウエアモジュールに分割され、そのそれぞれを、さらにいくつかのソフトウエア機能に分割することができます。これらの機能のあるものは、ここに示したプロセスで説明するように、今後、モデルベース手法を使用して開発されるようになります。

ソフトウエア開発プロセス

コードベースおよびモデルベースのソフトウエア開発はVサイクルに従って行われます（図3）。モジュール開発の出発点として、Electric Driveのトルク制御などのソフトウエアモジュール要求があります。システム開発プロセスでは、顧客要求の段階的詳細化を通じて、そのシステムレベル（この場合はモジュールレベル）に達するまでこれらの要求の生成が反復されます。各設計フェーズには対応するテストフェーズが存在し、機能モデルとソフトウエアの成熟度を検証する必要があります。

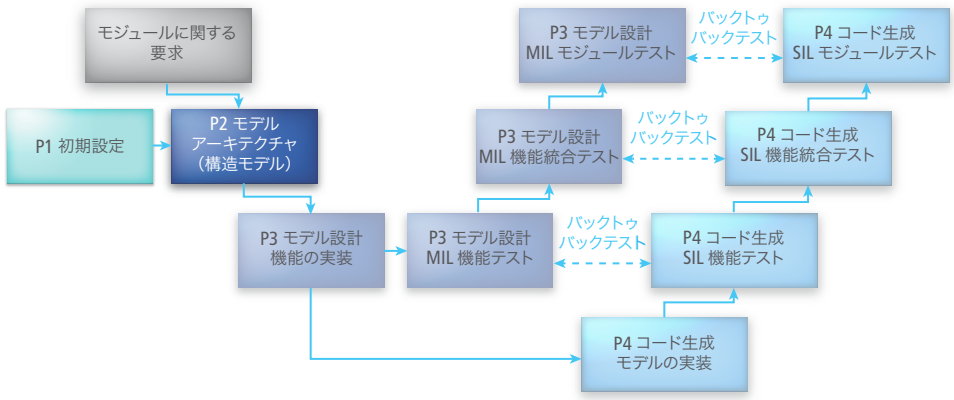
モデルベース開発プロセスの各フェーズ

ISO 26262に準拠したモデルベース開発プロセスには、4つの重要なフェーズが存在します。

フェーズ1－初期設定：

このフェーズには、第1回目のミーティング、開発環境のセットアップ、環境モデルのための要求の指定、役割りと責任の定

図3：Siemens社のドライブテクノロジ部門でのモデルベースソフトウエア開発用Vサイクル（一部）



義と割り当てなど、プロジェクトを開始する前に実行しておく必要があるすべての準備作業が含まれます。ソフトウエアエンジニアやソフトウエアアーキテクトなどの標準的なソフトウエア開発での役割りに、Simulinkでの機能モデリングを担当するモデルエンジニアなど、モデルベースのソフトウエア開発に必要な新しい役割りが追加されます。ISO規格の要求の1つは、このフェーズでModel Examiner（MXAM）を使用して自動的にテストすることができるプロジェクト関連のモデリングガイドラインを選択することです（ISO 26262-6の5.4.7章参照）。

フェーズ2－モデルアーキテクチャ：

このフェーズでは、開発するソフトウエアモジュールまたはソフトウエア関数に対する要求を機能的にまとまりのあるユニットにカプセル化し、適切な環境モデルを選択し、各コンポーネントのテストコンセプトをモデルのテストのために調整を行います。ただ、このフェーズでの重要なタスクは、モデルエンジニアおよびソフトウエアアーキテクトにモデルアーキテクチャを定義して実装させることです。完成したモデルアーキテクチャを、そのインターフェースを含めて構造モデルによって表現します。このモデルは相互接続された空のSimulinkサブシステムで構成されます。この構造モデルはソフトウエアアーキテクチャの基本的な枠組みを定義するもので、後でTargetLinkのサブシステムおよび機能ブロックを使用して実装します。ISO規格がモデルアーキテクチャおよびソフトウエアアーキテクチャに課している要求には、次のようなものがあります（ISO 26262-6の7.4章の表3参照）：

- 階層構造をもち、ソフトウエアコンポーネントが複雑でないこと
- 複雑でない小規模のインターフェース
- ソフトウエアコンポーネント内部の高い凝集性
- ソフトウエアコンポーネントの結合の制限

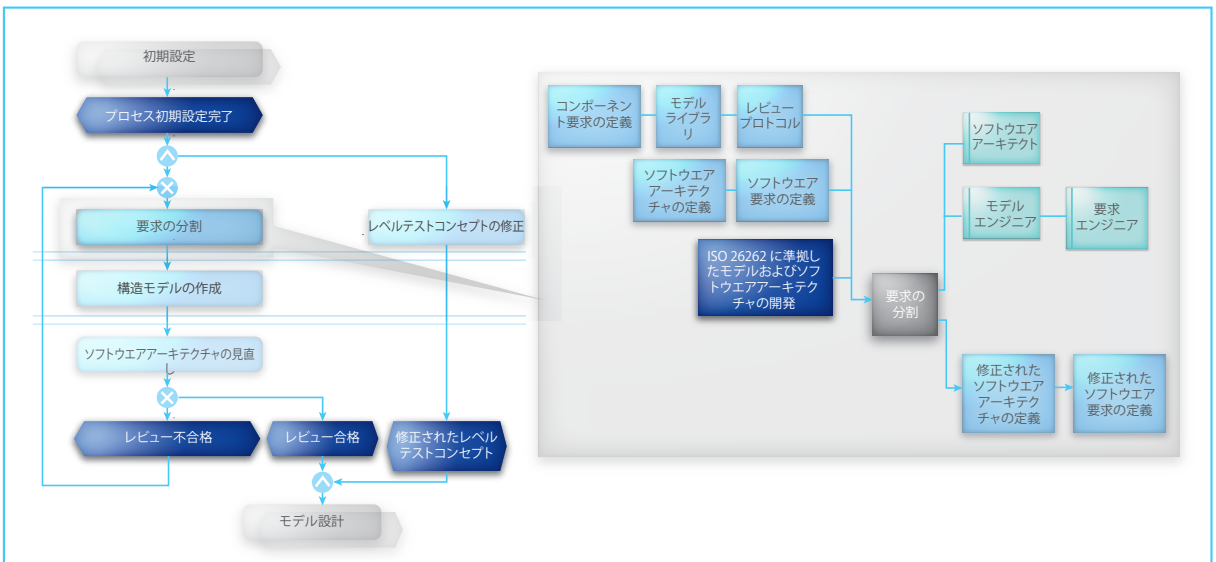
> 「開発プロセスをISO 26262に準拠させるには、専用の開発ツールで構成された統合ツールチェーンが絶対に必要となります」
>
> *Dr. Ingo Stürmer、MES社*

これらの要求を、（1）そのモデルアーキテクチャ用の設計パターンを使用する、（2）アーキテクチャを見直す、（3）M-XRAYを使用して、モデルの複雑性を測定および評価するなど、さまざまな方法によって満たします。また、ISO 26262には、要求ベースのテスト、インターフェースのテスト、モデルとコード間のバックトゥバックテストなど、ソフトウエアモジュールおよび機能のテストのための要求も定義されています（ISO 26262-6の表10および13参照）。モジュールまたは関数のテストコンセプトを、必要に応じてこのフェーズで拡張します。

フェーズ3－モデル設計：

このフェーズでは、構造モデル内に、モジュールおよび関数に対する機能要求をさらに詳細にモデル化して、機能モデルを生成します。また、関連する要求に対して倍精度のSimulinkシミュレーションであるMIL（Model-in-the-Loop）モードを使用して、テストコンセプトに従ってモジュールをテストします。この利点は、まだコードが使用できない段階であっても、モジュールが要求を満たしていることを抽象レベルで検証できることです（目的：早期の段階でのテスト）。したがって、機能モデルは機能要求の実行可能な仕様と言えます。ISO規格では適切な表記法を使用することなど、ソフトウエアモジュールおよび機能の設計に関する要求が特別に定義されています。SimulinkまたはTargetLink

図4：フェーズ2の「モデルアーキテクチャ」のサンプルモデルと「要求の分割」ステップの詳細な表示例



を使用することで、ASIL B～Dコンポーネント用の準形式的表記に対する要求が自動的に満たされます（ISO 26262-6の表7参照）。ISO規格では、これらの高度の表記要求に加え、暗黙の型変換を避けることなど、非常に具体的なエラー防止対策が要求されています（ISO 26262-6の表8参照）。

フェーズ4－コード生成：
実装フェーズでは、TargetLinkから機能モデルにコード生成に必要な情報を与えます（機能分割、数値表現、データ型、ローカル／グローバル変数など）。プロジェクトによっては、このフェーズにサブフェーズが存在することもあります。たとえば、機能モデルが純粋なSimulinkモデルの場合、まず、TargetLinkモデルに変換する必要があります。ISO 26262に準拠して生成したコードのテスト結果を、バックトゥバックテストのSIL（Software-in-the-Loop）シミュレーションとしての機能モデルのMILテストの結果と比較します。生成したコードのテストの完了後ただちに、モデルベースのソフトウエア開発タスクをコードベースのソフトウエア開発に結合します。これはたとえば、複数のモジュールまたは関数の統合テストのテスト作業が、システムテストまで、再び通常のコード検証手順に従うことを意味します。上記のテスト方法（要求ベースのテスト、インターフェーステスト、およびバックトゥバックテスト）をもう一度使用して、機能カバレッジおよび関数コールカバレッジなどの統合テストのカバレッジ評価指標に適合していることを検証する必要があります（ISO 26262-6、表15参照）。

ISO 26262に準拠したモデルベース開発のためのプロセスモデリング

Siemens社のドライブテクノロジ部門では、ARIS社のツールサポートを使用して開発プロセスがモデル化されています。これにより、プログラムコードのモデルベース開発に必要なすべてのプロセスステップがISO 26262に準拠して完全に文書化されます。相互に依存した、いくつかの連続した文書化ステージで、必要な文書が生成されます。これについて簡単に説明します。開発プロセスの「モデルアーキテクチャ」のフェーズ（図4）を、イベントドリブンプロセスチェーンとして、簡潔に表現することができます（図4の左側）。図4の右側の詳細な表現は、開発結果およびISO 26262の要求に関して、どの文書のどの役割りがそのプロセスステップ（「要求の分割」ステップなど）を実行するかを示しています。

モデルベース開発のためのプロセスマニュアル

Siemens社のドライブテクノロジ部門は、モデルベースソフトウエア開発のプロセスステップのグラフィカルな表現だけでなく、その開発プロセスを詳細に説明した、プロセスマニュアルを用意しています。このマニュアルには、定義されたすべてのプロセスステップと、すべての関係者に対する詳細な指示が含まれています。また、モデルベース開発に関連したトピックについて、モデルベーステスト、モデルアーキテクチャ設計、ソフトウエアプロセスに対するISO 26262の要求など、独立した章が立てられています。このマニュアルでは、プロセスのユーザや関心のある人が、プロセスステップの概要や必要な情報を簡単に検索することができるように、それぞれのプロセスステップを説明する情報が構造化されています。マニュアルの各章および各節の構造には、それぞれのプロセススフェーズに関する5つのポイントが含まれています（図5）。ここでは、「モデルアーキテクチャ」フェーズの例を示します：

1.目標：
このプロセスで達成すべき目標が定義されています。「モデルアーキテクチャ」フェーズでは、ソフトウエア機能の階層によって実装可能な部品への要求の機能的分解が目標になります。この際に、時間のかかる、機能モデルから実装モデルへの再構成を避けるために、後でTargetLinkモデルによって定義するソフトウエアアーキテクチャを前もって考慮しておく必要もあります。また、モジュールのテストコンセプトの微調整も目標となります（図4）。

2.前提条件および入力：
作業を開始するときに使用できるようになっていなければならない情報および作業成果を定義します。たとえば、「モデルアーキテクチャ」フェーズの目標を達成するには、より上流のシステム開発プロセスで生成される「コンポーネント要求の定義」と、「ソフトウエア要求の定義」が存在している必要があります。

3.作業の詳細：
だれが何をするか、どの作業生産物が必要か、どれを作成するかなど、プロセスステップを詳細に記述します。図4ですでに説明したように、それぞれの作業の記述は、特にISO 26262関連の要求に言及している必要があります。これらはソフトウエアアーキテクチャ、テスト方法、レビュープロセスなどにも関連します。

4.作業生産物：
テストレベルコンセプトやレビューレポートなどのISO 26262関連のものを含め、それぞれのプロセスフェーズの各ステップで得られたすべての作業生産物が含まれます。

5.成功基準：
「正常に完了」したことを示し、次のステッ

図5：Siemens社のドライブテクノロジ部門のISO 26262準拠開発プロセスの各フェーズの基本的なトピックとステップの構造

プを開始するために、各プロセスステップで満たす必要のある基準を一覧表示にします。これは、たとえばモデルアーキテクチャの例を2つ挙げれば、構造モデルに実装されている必要があること、構造モデルが統合モデルに正常に統合されている必要があること意味します。

重要なすべての用語、特にモデルベース開発に関する用語の用語集が、このマニュアルの理解を容易にしています。それぞれの章は1つのセクションとして完結していて、プロセス記述と合わせて読む必要はありません。また、このマニュアルの別の重要なセクションで、モデルベース開発のために使用するツールと推奨のメソッドを実装する方法について説明されています。

ISO 26262に準拠したプロセスおよびツールチェーン

MES社による外部サポートは、プロセスの実際的な定義とプロセスの実装に際して中心的な役割りを果たしました。MES社はプロジェクトパートナーとして、有効なものとそうでないものに関して貴重なノウハウを提供しました。Siemens社のさまざまなプロジェクトから得られた経験も、成功に貢献した要素でした。プロセスのモデリングフェーズには、Siemens社でシステム開発プロセスの全体を設計したエキスパートが参加しました。導入したプロセスが組織内で透過的であり、セーフティクリティカルな要素に対して最適化されたとき、ISO 26262準拠の手順に関する基本要件をすでに満たしていることが明らかになりました。また、使用されているソフトウエアツールも、高い製品品質とISOへの準拠を保証するために適切でなければなりません。たとえば、ドイツの認証機関であるTÜV SÜD社は、量産コード生成ツールのTargetLinkをASIL Dまでのセーフティクリティカルな機能の開発プロジェクトに使用することを承認しています。この認定は、プロセスがdSPACEのTargetLinkのリファレンスワークフローに準拠していることに基づいています。このワークフローには、TargetLinkのためのモデルおよびコード検証のためのベストプラクティスが記述されています。このワークフローが、Siemens社の開発プロセスに統合されました。MES社はModel Examiner（機能安全ソリューション）を使用して、モデルがガイドラインおよびモデルの測定およびモデルの複雑性を処理するためのM-XRAYに適合していることを保証しています。これらのツールを使用するだけで、モデルベース開発に対するISOの要求を満たすことができます（パート6、5.4.7章、表1の要求を完全にカバー）。Siemens社が使用しているツールチェーンは、この規格で定義されているプロセスをプロジェクトで実現するのに適していることが証明されました。また、Siemens社で開発されたツールチェーンも、要求からコード生成ツール／モデルおよびテストへの双方向のトレーサビリティを保証しています。

> 「TÜV SÜD社に認証されたTargetLinkリファレンスワークフローにより、dSPACE TargetLinkに基づくISO 26262準拠のモデルベース開発プロセスを簡単にセットアップできるようになりました」
>
> Dr. Heiko Zatocil、Siemens社

早期の段階でのテストと、開発プロセスの安全性の大幅な向上

新しいISO 26262は、モデルベース開発を自動車用のセーフティクリティカルなソフトウエア開発用の高品質なアプローチとして承認しています。コードベースのプロセスにモデルベース開発を付加して拡張することにより、ソフトウエアのテストを、早期の段階でより良い方法およびツールによるサポートを活用して行うことができるため、大きなメリットが得られます。これを達成するために、社内プロセスをISO規格の要求に合わせる必要があります。Siemens社のドライブテクノロジ部門は、この新しいプロセスモデルに準拠して最初のセーフティクリティカルなソフトウエアコンポーネントをすでに開発しています。モデルベース開発は、従来の開発手順に次いで今後ますます重要な役割りを果たすようになると予想されますが、ISO 26262準拠のプロセスステップに従っているため、すでに大きな広がりを見せ始めています。■

David Brothanek, Dr. Martin Jung,
Verena Jung, Michael Krell,
Reinhard Pfundt, Dr. Elke Salecker,
Dr. Ingo Stürmer, Dr. Heiko Zatocil

David Brothanek氏
ドイツのエッセンにあるHeadframe IT GmbHの上級管理職であり、プロセスのモデリング、最適化、実装のスペシャリストです。

Dr. Martin Jung
ドイツのエルランゲンにあるSoftware and System Development Consultation社の開発グループのリーダーであり、ドイツのエルランゲン=ニュルンベルクにあるフリードリヒ・アレキサンダー大学でソフトウエアアーキテクチャを教えています。

Verena Jung 氏
ドイツのエルランゲンにあるSiemens AGの統合およびテストのチームリーダーであり、ソフトウエアおよびコンポーネント開発におけるテスト作業の調整も担当しています。

Michael Krell氏
ドイツのエルランゲンにあるSiemens AGの機能安全マネージャです。プロジェクトへのISO 26262要求の実装をサポートしています。

Reinhard Pfundt氏
ドイツのエルランゲンにあるSiemens AGのソフトウエアマネージャで、周波数コンバータ、DC/DCコンバータ、車載充電装置用ソフトウエアの計画および調整を担当しています。

Dr. Elke Salecker
ドイツのベルリンにあるModel Engineering Solutions GmbHの上級ソフトウエアコンサルタントです。ISO 26262準拠のモデルベースソフトウエア開発のエキスパートとして、お客様のプロセス定義および実装をサポートしています。

Dr. Ingo Stürmer
ドイツのベルリンにあるModel Engineering Solutions GmbHの創業者でありCEOです。dSPACE TargetLinkを使用した開発プロセスに関する著名なスペシャリストであり、お客様がモデルベース開発プロセスを最適化し、その会社固有のツールチェーンをISO 26262の認証が取得できるよう支援を行っています。

Dr. Heiko Zatocil
ドイツのエルランゲンにあるSiemens AGの機能開発のリーダーであり、モデルベースソフトウエア開発の推進に大きな役割りを果たしています。本記事に紹介されているプロセスの作成を発案し、また調整役を務めました。