Einsatz von Modellierungsrichtlinien für die Absicherung von E-Drive-Software

# Elektrisch und sicher

Mercedes-Benz Research & Development North America hat zusammen mit dem TargetLink Strategic Partner Model Engineering Solutions automatisch prüfbare Konformitätsregeln für die Modellierung mit dSPACE TargetLink entwickelt, die wichtige Anforderungen der ISO 26262 erfüllen.

Mercedes-Benz Research & Development North America (MBRDNA), unter anderem mit Sitz in Redford, Michigan, ist für die Entwicklung und Integration der Inverter-Software (Stromwandlung für die Elektromaschine) verantwortlich. Diese mit dSPACE TargetLink® generierte Software kommt in verschiedenen Fahrzeuganwendungen innerhalb des Mercedes-Benz-E-Drive-Portfolios zum Einsatz. Ein wesentliches Element und die eigentliche Innovation ist die Steuerung der Elektromotoren sowie ein zugehöriges Momenten- und Hochvolt-Sicherheitskonzept, das nach ASIL-C-Vorgaben der ISO 26262 umgesetzt wird.

## Entwicklungsprozess und Modellqualität

Die E-Drive-Software basiert auf der AUTOSAR-Software-Architektur und ist für zahlreiche elektrifizierte Antriebsstränge skalierbar. Die komplette Steuerungssoftware wird modellbasiert nach dem V-Modell entwickelt. Der Seriencode-Generator TargetLink von dSPACE ist dabei

Quelle: © Mercedes-Benz

zentraler Bestandteil der Entwicklungswerkzeugkette. TargetLink unterstützt die Modellierung und Code-Generierung einer AUTOSAR-konformen Software-Architektur und ist für sicherheitsrelevante Software bis ASIL D zertifiziert. Die Modellierung der Funktionssoftware mit Simulink® und TargetLink nimmt eine zentrale Rolle in der frühzeitigen Absicherung der Anforderungen ein: je höher die Qualität der Modelle, die für die Code-Generierung eingesetzt werden, desto höher die Qualität der generierten Software. Die Verwendung von Simulink/TargetLink zur Modellierung von Software ist generell eine bewährte und akzeptierte Vorgehensweise, um qualitativ hochwertige Software zu entwickeln. Dies ist auch im Sinne der ISO 26262, die die Verwendung einer semi-formalen Modellierungssprache wie Simulink empfiehlt. Bei MBRDNA wird eine Kombination aus statischen und analytischen Absicherungsmaßnahmen eingesetzt, um eine hohe Modellqualität zu gewährleisten. Unabhängig von den funktionalen Anforderungen des Kunden sind Entwicklungsmethoden definiert, die sicherstellen, dass sich die Software optimal in die Zielumgebung integrieren lässt.

## Regeln für den Software-Entwurf

Ein wichtiger Bestandteil dieser Methoden ist der konsequente Einsatz von Modellierungs- bzw. Konformitätsregeln für den Software-Entwurf. Die bei MBRDNA eingesetzten Regeln basieren auf Daimler-internen Vorgaben zur Modellentwicklung und sind an die Entwicklungsanforderungen der E-Drive-Software angepasst. Die Daimler-Modellierungsrichtlinien basieren auf Modellierungsstandards und werkzeugspezifischen Richtlinien wie MAAB, MISRA Simulink/Stateflow, MES Functional Safety Guidelines, MISRA TargetLink und dSPACE TargetLink Modeling Guidelines (siehe Abbildung 1). Der Fokus der vorhandenen Richtlinienwerke ist durchaus unterschiedlich. Erst eine sinnvolle Kombination aller Regeln erlaubt eine vollständige Abdeckung aller Aspekte, die für die Modellierung sicherheitsrelevanter Software nach ISO 26262 notwendig sind. Die MAAB (MathWorks Automotive Advisory Board)-Regeln konzentrieren sich maßgeblich auf Design-Aspekte von Simulations- und Controller-Modellen im Hinblick auf Lesbarkeit, Wartbarkeit und Best Practices. Die Seriencode-Generierung steht hier nicht im Vordergrund. Die MISRA-Simulink/Stateflow- und MISRA-TargetLink-Regeln hingegen fokussieren Sicherheitsaspekte der Modelle bzw. des daraus zu generierenden Codes. So werden hier ein sicherer Sprachumfang von Simulink und Stateflow, Modellierungsmuster für sichere Code Patterns und eine geeignete Konfiguration der Simulationsumgebung definiert. Werkzeugspezifische Regeln wie die MISRA/dSPACE TargetLink Modeling Guidelines beziehen sich in großen Teilen auf die Code-Generierung mit TargetLink. Eine Einhaltung dieser Regeln schließt unter anderem Modellierungsmuster und die Konfiguration des Modells und Code-Generators aus, die sich ungünstig auf Eigenschaften des generierten Codes auswirken können. Richtlinien, die sich maßgeblich auf Sicherheitsaspekte des Modells und des generierten Codes fokussieren, sind die MES Functional Safety Guidelines. Diese wurden direkt aus Anforderungen der ISO 26262 und anderen Sicherheitsstandards abgeleitet und ergänzen die vorhandenen Richtlinienwerke, wenn der Entwurf sicherheitsrelevanter Software im Vordergrund steht. Hier kommen unter anderem Datenfluss- und Kontrollflussanalysen zum Tragen.

> „Aufgrund steigender Komplexität von Software-Systemen stößt traditionelles Testen an seine Grenzen – automatisierte Analysen der erzeugten Modelle und der übersetzten Software sind elementarer Bestandteil unserer Software-Qualitätssicherung."
>
> *Alexander Dolpp, Mercedes-Benz Research & Development North America, Inc.*

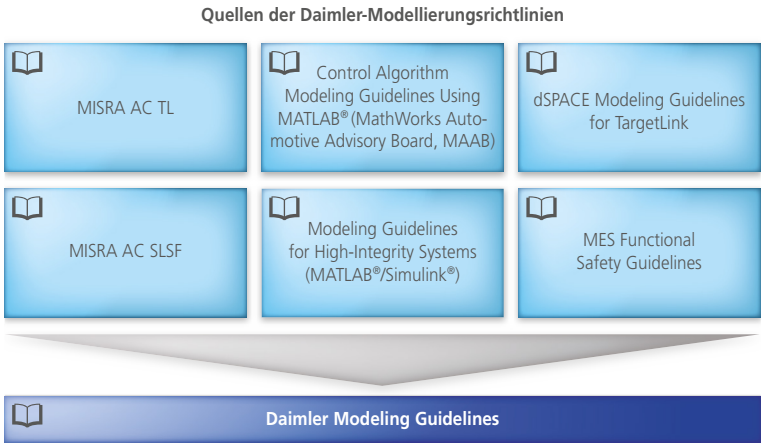



*Abbildung 1: Die Daimler-Modellierungsrichtlinien basieren auf zahlreichen etablierten Standards und Richtlinien.*

## Automatisierte Prüfungen für TargetLink-Modelle

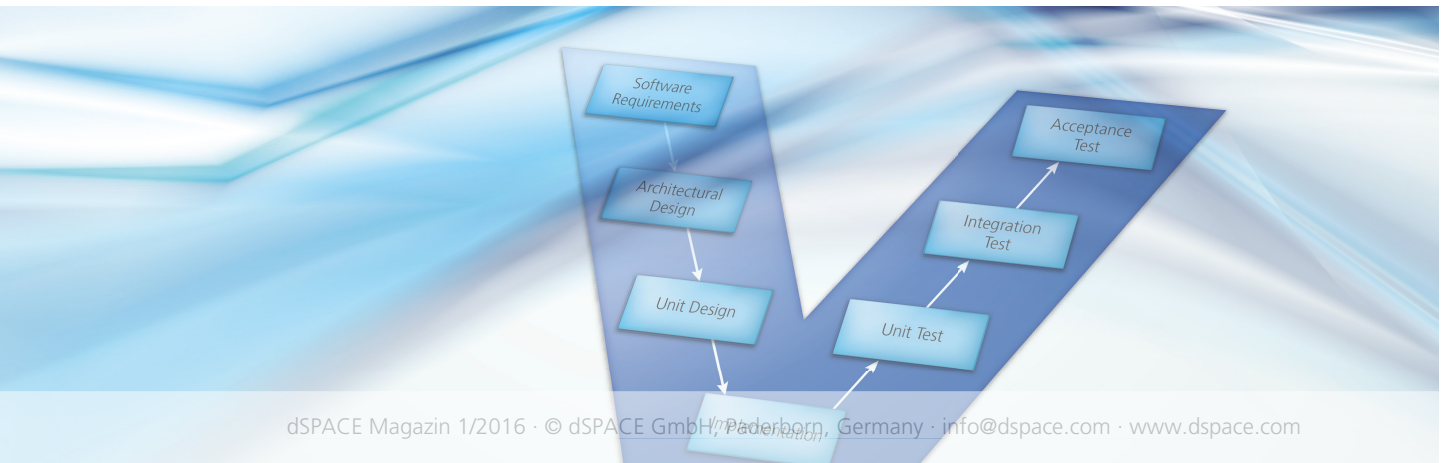
Mit dem Ziel, die Anwendung von Modellierungsrichtlinien zu vereinfachen, wurden die Daimler-Modellierungsrichtlinien zusammen mit der Model Engineering Solutions GmbH (MES), einem der TargetLink Strategic Partner, auf Basis der vorhandenen Regelwerke erstellt und um Daimler-spezifische Bedürfnisse erweitert.

Die Richtlinien werden im MES Model Examiner (MXAM) verwaltet und automatisierte Prüfungen für TargetLink-Modelle bereitgestellt. Durch den Einsatz der Modellierungsrichtlinien kann gewährleistet werden, dass Anforderungen der ISO 26262 an die Modellierung eingehalten, Best Practices umgesetzt, Modellierungsfehler vermieden und werkzeugspezifische Konfigurationen berücksichtigt werden, wie zum Beispiel einheitliche Einstellungen der Simulationsumgebung oder des Code-Generators.

## Sicherheit bis ins Detail

Als adaptierte MISRA-Modellierungsrichtlinie legen die Daimler-Modellierungsrichtlinien zum Beispiel die korrekte Ausführungsreihenfolge von Stateflow-Transitionen fest. Die Daimler-Regel sagt dabei das Gegenteil der MISRA-Regel, nämlich, dass die Ausführungsreihenfolge durch den Nutzer zu bestimmen ist und nicht durch die grafische Anordnung der Zustände (States) und Transitionen, um Fehlinterpretationen der Stateflow-Semantik zu vermeiden. Wird ein State zum Beispiel später aus Layout-Gründen verschoben (Syntax-Änderung), kann sich das Ausführungsverhalten des Zustands ungewollt ändern (Semantik-Änderung), vgl. Abbildung 2a. Ähnliches gilt für Stateflow-Transitionen, die an einem Verzweigungspunkt (Junction) ausgewertet werden, wie in Abbildung 2b gezeigt. Diese Fehlinterpretation bzw. ungewollte Än-

> „Der Einsatz von Modellierungsrichtlinien und einem Richtlinienprüfer wie dem MES Model Examiner ermöglicht es, Anforderungen der ISO 26262 automatisch umzusetzen und Freiraum für die Modellierer zu schaffen. Denn diese sollen sich auf das Wesentliche konzentrieren: die Entwicklung der Regelungsfunktionen."
>
> *Dr. Ingo Stürmer, Model Engineering Solutions*



„TargetLink zur Seriencode-Generierung ist mit seiner nativen AUTOSAR-Unterstützung ein zentrales Element unserer Entwicklungswerkzeugkette."

*Alexander Dolpp, Mercedes-Benz Research & Development North America, Inc.*

derung des Ausführungsverhaltens kann leicht vermieden werden, wenn über die Stateflow-Konfiguration „User specified state/transition execution order" die Ausführungsreihenfolge so berechnet wird, wie es der Modellierer festgelegt hat. Über den Einsatz von Modellprüfungen im MES Model Examiner (MXAM) wird die Einhaltung solcher Richtlinien automatisch geprüft und bei Bedarf sofort korrigiert.

## Klare Prozesse

Die Einhaltung der Modellierungsrichtlinien ist für alle Modellierer und Software-Entwickler verbindlich. Eine automatische Modellprüfung mit MXAM ist immer dann durchzuführen, wenn neue Funktionalitäten hinzugefügt werden. Ein Einchecken von Software ins Versionsmanagement-System ist nur möglich, wenn die Modellierungsrichtlinien eingehalten und auch die dazugehörigen funktionalen Model-in-the-Loop (MIL)-Tests durchgeführt wurden. Die Behebung möglicher Verletzungen der Richtlinien liegt im Verantwortungsbereich der Modellierer. Dieser Ansatz der statischen Modellanalyse ist ein Bestandteil aller Absicherungsmaßnahmen im V-Modell zur Entwicklung und Absicherung der E-Drive-Software. Durch den Einsatz der Daimler-Modellierungsrichtlinien im Zusammenhang mit MXAM zur automatischen Konformitätsprüfung und des dSPACE Seriencode-Generators TargetLink setzt Mercedes-Benz Research & Development auf einen bewährten Ansatz, um Anforderungen der ISO 26262 zu erfüllen, die Modellqualität früh zu verbessern und die Code-Qualität signifikant weiter zu erhöhen. ■

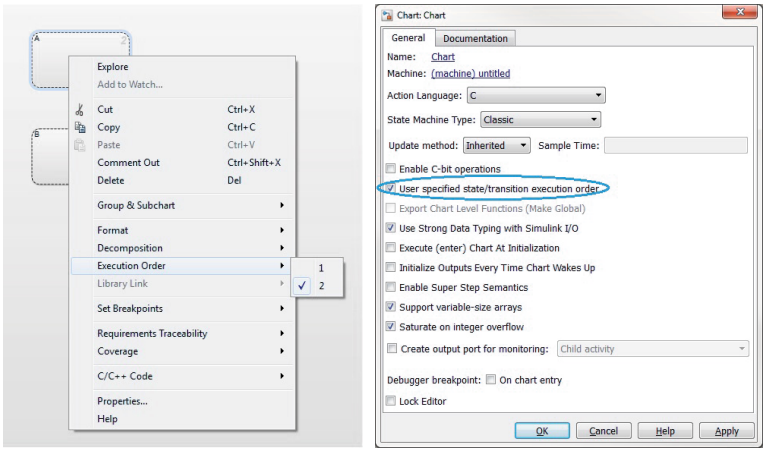



*Abbildung 2a (oben): Typischer Überprüfungsfall für den MES Model Examiner – Ausführungsreihenfolge paralleler Zustände, hier in Stateflow spezifiziert.*
*Abbildung 2b (unten): Ausführungsreihenfolge von Transitionen.*

*Alexander Dolpp*
*Alexander Dolpp ist Director E-Drive Software bei Mercedes-Benz Research & Development North America, Inc. in Redford, Michigan, USA.*

*Dr. Ingo Stürmer*
*Dr. Ingo Stürmer ist Gründer, Inhaber und ehemaliger CEO der Model Engineering Solutions GmbH. Seit Januar 2016 führt Dr. Stürmer die Model Engineering Solutions Ltd. (UK).*