**通过与 TargetLink 战略合作伙伴 Model Engineering Solutions 进行合作，梅赛德斯-奔驰北美研发公司按照 ISO 26262 标准为使用 dSPACE TargetLink 制定了可自动检查一致性的建模规则。**

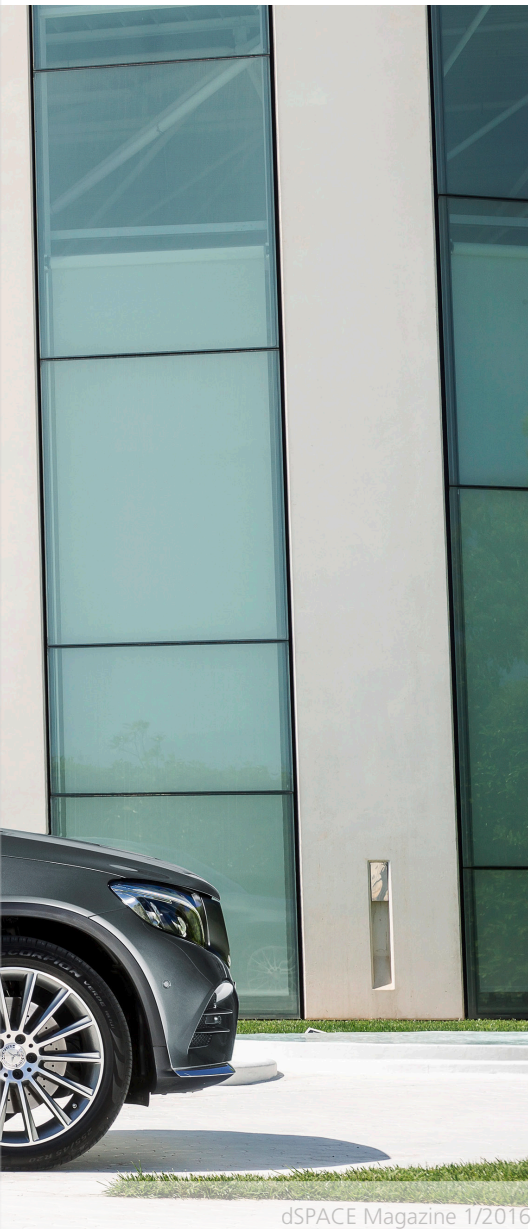
梅赛德斯-奔驰北美研发公司 (MBRDNA) 的其中一处办公地点位于密歇根州雷德福德，他们负责开发和集成逆变器软件（电机的电流转换）。利用 dSPACE TargetLink® 开发的这一软件在梅赛德斯-奔驰的电驱动产品系列中用于各种车辆的应用。其中一个主要组件（也是实际创新）是依据 ISO 26262 标准 ASIL C 级要求实施的电动机控制和相关扭矩以及高电压安全概念。

使用建模准则验证电驱动软件

# 电气与安全

### 开发流程和模型质量

电驱动软件基于 AUTOSAR 软件架构，可针对众多电气化传动系进行调整。整个控制软件根据 V-cycle 流程使用基于模型的设计方法开发而成。dSPACE 的产品级代码生成器 TargetLink 是开发工具链的核心组件。TargetLink 支持 AUTOSAR 软件架构进行建模和生成代码，并使安全相关软件最高达到 ASIL D 级标准。在 Simulink® 和 TargetLink 中对功能软件建模对于提早验证需求发挥着核心作用，因为用于生成代码的模型质量越高，所生成软件的质量也就越高。使用 Simulink/TargetLink 进行软件建模是一种广为接受且经过行业验证的方法，可生成高质量软件。此方法同样符合 ISO 26262 标准，该标准建议使用半正式建模语言，例如 Simulink。MBRDNA 将静态和分析验证措施结合在一起，以确保模型拥有高质量。MBRDNA 定义了不受客户功能性需求影响的、能以最佳方式将软件集成到目标环境的开发方法。



### 软件设计规则

此方法的一个重要环节是在软件设计中始终如一地使用建模和一致性规则。MBRDNA 采用的规则基于 Daimler 内部关于模型开发的规定，并且已按照电驱动软件的开发要求进行调整。Daimler 建模准则基于一些建模标准和特定工具准则，例如 MAAB、MISRA Simulink/Stateflow、MES 功能安全准则、MISRA TargetLink 和 dSPACE TargetLink 建模准则（图 1）。由于这些准则的关注点各自不同，因此需要明智地以根据 ISO 26262 标准涵盖安全相关软件建模的所有必要方面进行组合。MAAB（MathWorks 汽车咨询委员会）关注的是仿真和控制器模型的设计方面，重点在于可读性、服务性和最佳实践。MAAB 规则强调的并不是产品级代码生成。但是，MISRA Simulink/Stateflow 和 MISRA TargetLink 准则关注的是模型的安全以及通过模型生成的代码的安全。它们定义了 Simulink 和 Stateflow 的安全语言范围、安全代码模式的建模方式以及仿真环境的恰当配置。MISRA/TargetLink 和 dSPACE TargetLink 建模准则等特定工具准则主要针对 TargetLink 的代码生成。遵循这些准则意味着模型或代码生成器的任何建模模式或配置都不能对所生成代码的属性造成负面影响。MES 功能安全准则主要针对模型和所生成代码的安全方面。这些准则从 ISO 26262 和其他安全标准的要求中派生而来，并对现有的安全相关软件设计准则形成补充。关键的分析要素是对数据流和控制流的检查。 >>

> “软件系统不断增加的复杂性达到了传统测试方法的极限。自动分析所创建的模型和所转换的软件，是我们的软件质量保证不可分割的组成部分。”
>
> *Alexander Dolpp，梅赛德斯-奔驰北美研发公司*


*图 1：Daimler 建模准则基于各种成熟的标准和准则。*

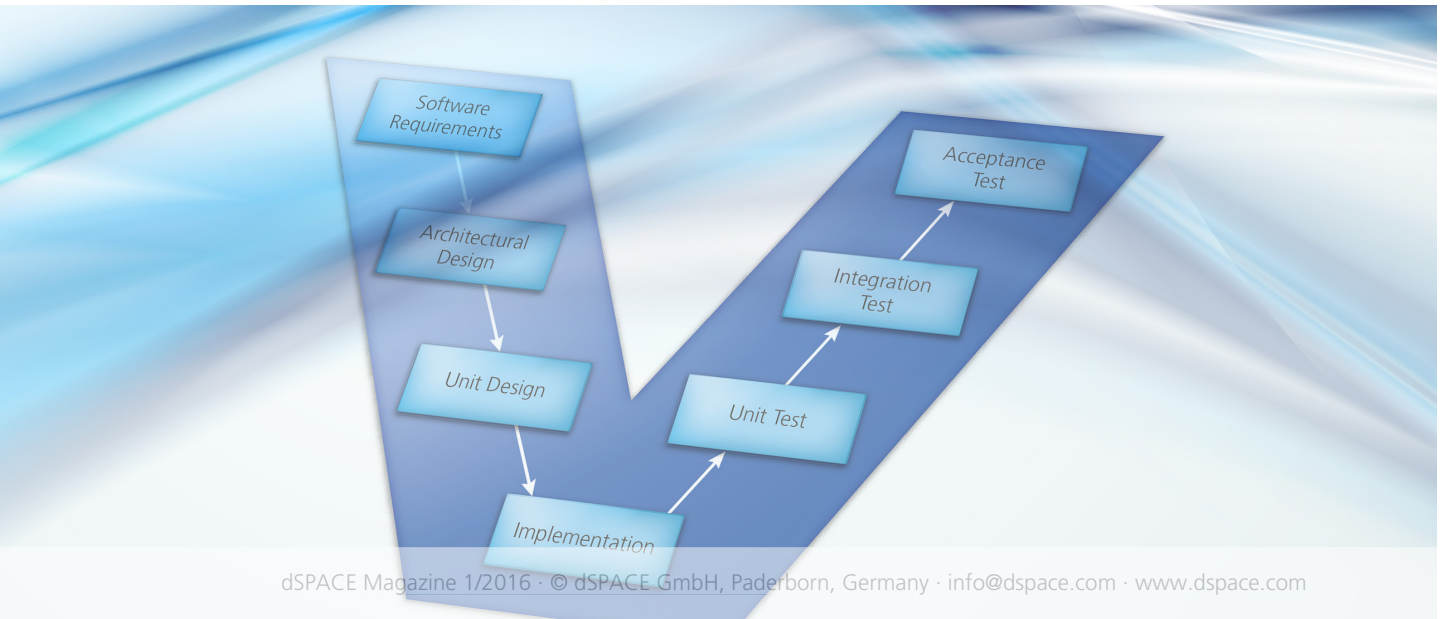
## TargetLink 模型自动化测试

为了更轻松地使用建模准则，MBRDNA 与 Model Engineering Solutions GmbH (MES)（TargetLink 战略合作伙伴）一起在现有文档的基础之上定制了 Daimler 建模准则，并将其扩展为涵盖 Daimler 特定需求。这些准则在 MES Model Examiner (MXAM) 中管理，同时提供了对 TargetLink 模型的自动化测试。通过遵循建模准则，MBRDNA 可以符合 ISO 26262 的建模要求、实施最佳实践、避免建模错误并考虑特定工具配置，例如仿真环境中或代码生成器中的统一设置。

## 安全详情

例如，作为调整后的 MISRA 建模准则，Daimler 建模准则确定了 Stateflow 跳转的正确的行顺序。此处的 Daimler 准则与 MISRA 准则相互抵触，它规定执行顺序只能由用户定义，而不是按状态和跳转的图形顺序来定义，从而避免对 Stateflow 语义的误解。例如，如果某个状态由于布局原因（语法变化）而调整，则会无意中更改状态的执行行为（语义变化），参见图 2a。在交叉点处评估的 Stateflow 跳转也是如此，如图 2b 中所示。通过使用 Stateflow 配置“用户指定的状态/跳转执行顺序”来确定建模专家指定的执行顺序，可以轻松避免这种误解或无意中改变执行行为。MES Model Examiner (MXAM) 中的模型检查用于自动验证模型是否符合这些准则，并立即修正模型。

> “使用建模准则和 MES Model Examiner 之类的准则检查器，能够自动实施 ISO 26262 标准的要求，让模型专家获得更大的自由。我们想让模型专家专注于主要任务，即开发控制功能。”
>
> *Ingo Stürmer 博士，Model Engineering Solutions*



> “在 AUTOSAR 的固有支持下，用于代码生成的 TargetLink 是我们开发工具链的核心元件。”
>
> *Alexander Dolpp，梅赛德斯-奔驰北美研发公司*

## 清晰的流程

所有建模专家和软件开发人员都必须遵循建模准则。每次添加新功能时，都必须使用 MXAM 执行模型自动检查。软件必须符合建模准则，并且已执行了相关的功能模型在环 (MIL) 测试，才能上传到版本管理系统中。建模专家负责依据准则消除所有违规情况。这种静态建模分析方法是用于开发和验证电驱动软件的 V-cycle 流程的所有验证措施的一部分。通过将 Daimler 建模准则与 MXAM 自动一致性检查及 dSPACE 产品级代码生成器 TargetLink 一起使用，梅赛德斯-奔驰北美研发公司使用了一种经行业验证的方法来遵循 ISO 26262 要求，在早期提高模型质量，并大大提高了代码质量。

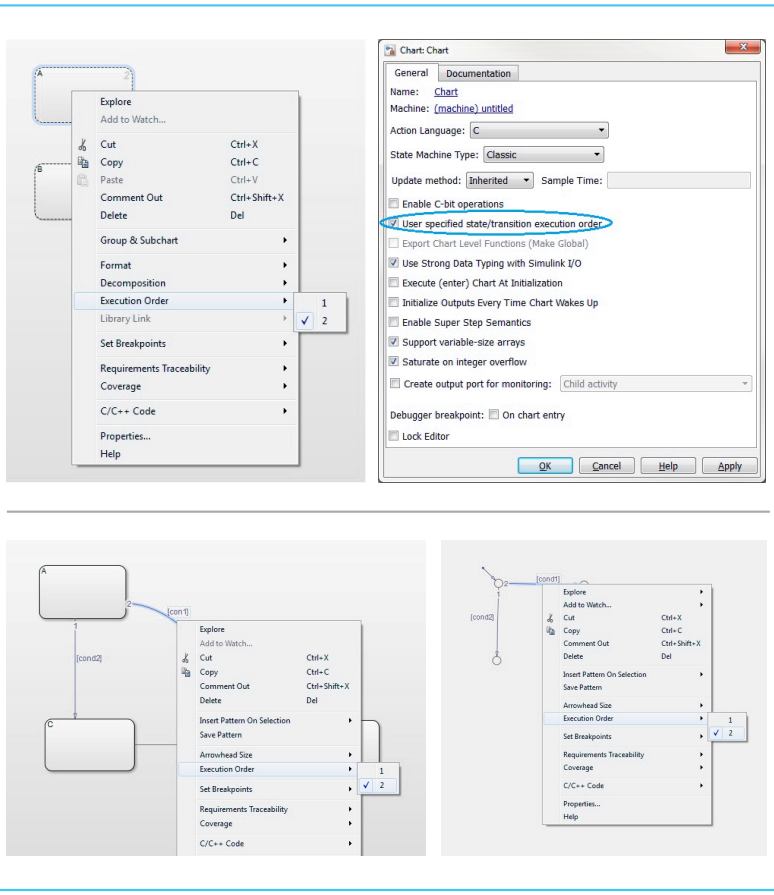



*图 2a（顶部）：MES Model Examiner 的典型案例 – 并行状态的执行顺序，此处在 Stateflow 中指定。*
*图 2b（底部）：跳转执行顺序。*

*Alexander Dolpp*
*Alexander Dolpp 是美国密歇根州雷德福德市梅赛德斯-奔驰北美研发公司的电驱动软件主管。*

*Ingo Stürmer 博士*
*Ingo Stürmer 博士是 Model Engineering Solutions GmbH 的创办人和前任 CEO。从 2016 年 1 月起，Stürmer 博士开始领导 Model Engineering Solutions Ltd.（英国）。*