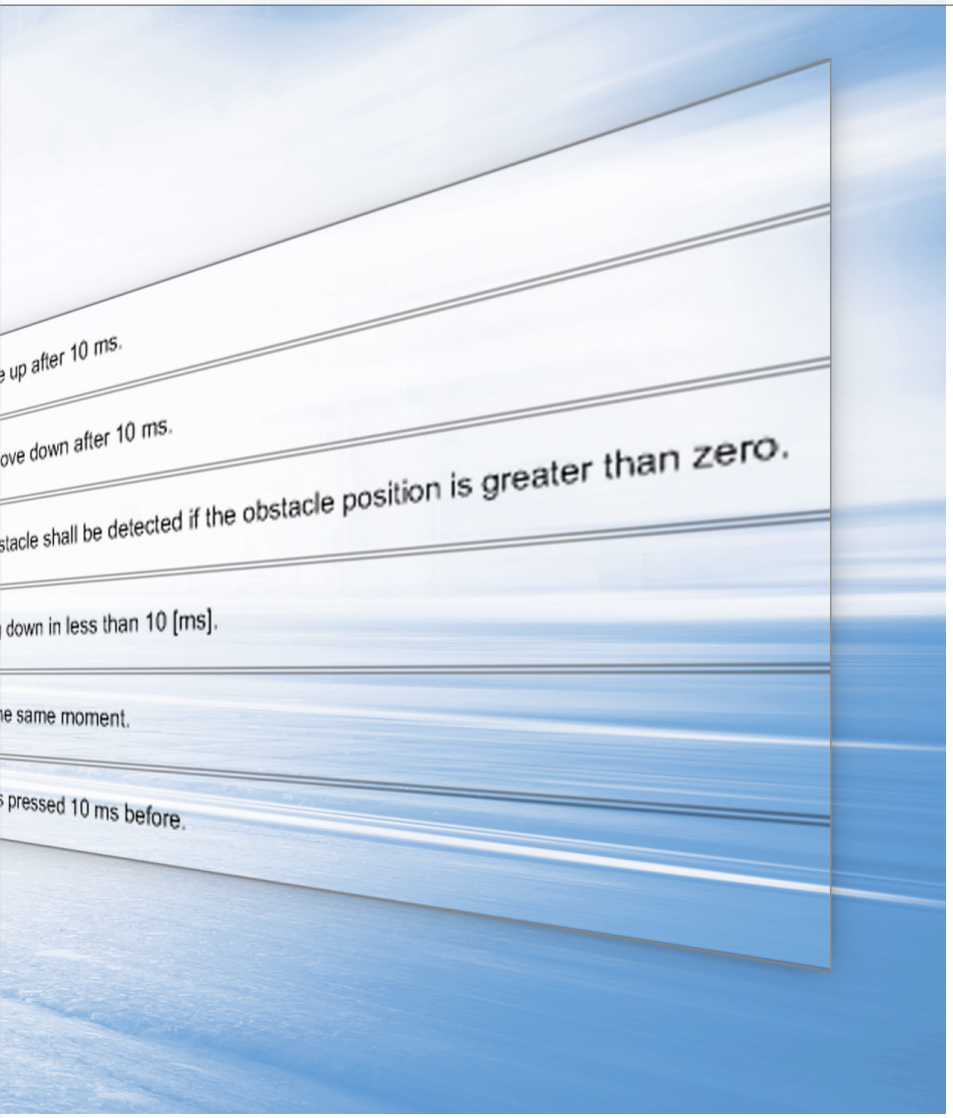
持续监控安全关键型应用程序

密切关注安全性

验证安全关键型系统需要多少测试？你如何平衡安全要求和测试工作？dSPACE 和 BTC 面向安全关键型 ECU 功能的基于仿真的形式验证的新解决方案让工作和可行性更加紧密。同时提供测试深度。

随着全球都在追求创新、用户便利和更加安全，电子安全相关系统数量日益增加。在各个领域，出于设计或成本考虑，机械后备系统的时代已经一去不复返。因此，这些电子系统的测试不可避免地面临严格要求。此类系统的示例包括线控转向和自动驾驶，其中系统故障具有灾难性的后果。这使得开发人员面临困境：尽管系统非常复杂、要求似乎永无止境，但验证所需的时间必须保持在合理限制内。开发人员还必须遵守许多重要指南。例如，ISO 26262 标准（“道路车辆 – 功能安全”）建议执行电子控制单元 (ECU) 安全关键型功能的形式验证。鉴于这些挑战，dSPACE 和 BTC 携手开发了安全关键型应用程序的基于仿真的形式验证的解决方案。它可用于在 dSPACE 平台上实时监控是否遵守安全关键型要求。



更大的测试深度

在传统测试流程中，运行每个安全关键型功能的所有必要测试用例，同时考虑所有需求和交叉参考时，会在测试工作和测试时间方面产生严重问题。毕竟，需要定义多少测试用例才能绝对覆盖所有可能性、交叉参考和并发性？即使您能够定义这么长的测试用例列表，您需要多少时间才能运行完所有这些用例来实现所需的测试深度？来自 dSPACE 和 BTC 的创新解决方案将全新 dSPACE Real-Time Testing (RTT) Observer Library 与形式化工具 BTC EmbeddedSpecifier® 相结合。这些工具通过支持实时的需求观测器完善了现有的模型在环 (MIL)、软件在环 (SIL) 和硬件在环 (HIL) 环境。运行仿真期间，观测器并行运行并且监控是否遵守所有安全关键型需求。还可以立即了解实施的测试用例覆盖的需求和未覆盖的需求。这让开发人员可高效评估测试流程的总体质量和进度。基于仿真的形式化验证是传统基于需求的测试（仍是基础）的理想补充。传统测试和基于观测器的测试的组合可大幅提高测试深度。将观测器视为可在各种 dSPACE 平台上方便使用的可执行测试标准。由于观测器与实际仿真模型解耦，现有仿真模型无需修改即可使用。现有传统测试可通过观测器轻松扩展，而无需修改。

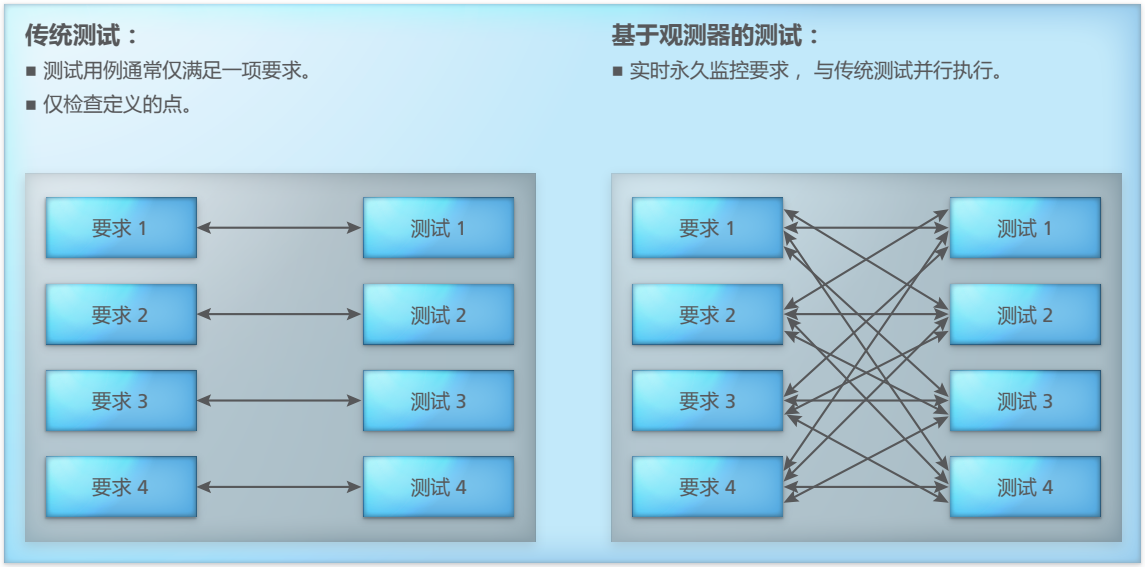
更好的质量

正是采用 BTC EmbeddedSpecifier，从中生成观测器的需求质量也随着提高。BTC EmbeddedSpecifier 提供工具支持，因此可轻松将非形式化的需求转换为形式化表示，再转换为 dSPACE 平台的可执行观测器。这样有指导性地逐步消除以前基于语言的需求和具体模型变量直接引用的歧义，可帮助用户尽可能精确地制定需求。这还将帮助遵守相关安全标准和指南。

>>

"BTC EmbeddedSystems 在需求形式化和形式化验证方面拥有长期经验，现在更是结合了来自 dSPACE 的既定强大仿真平台和系统。这铸就了完美优化的独特工具链，将测试质量和意义提升到全新水平，特别是对于安全关键型应用程序。"

Hans Jürgen Holberg，管理委员会，BTC Embedded Systems AG



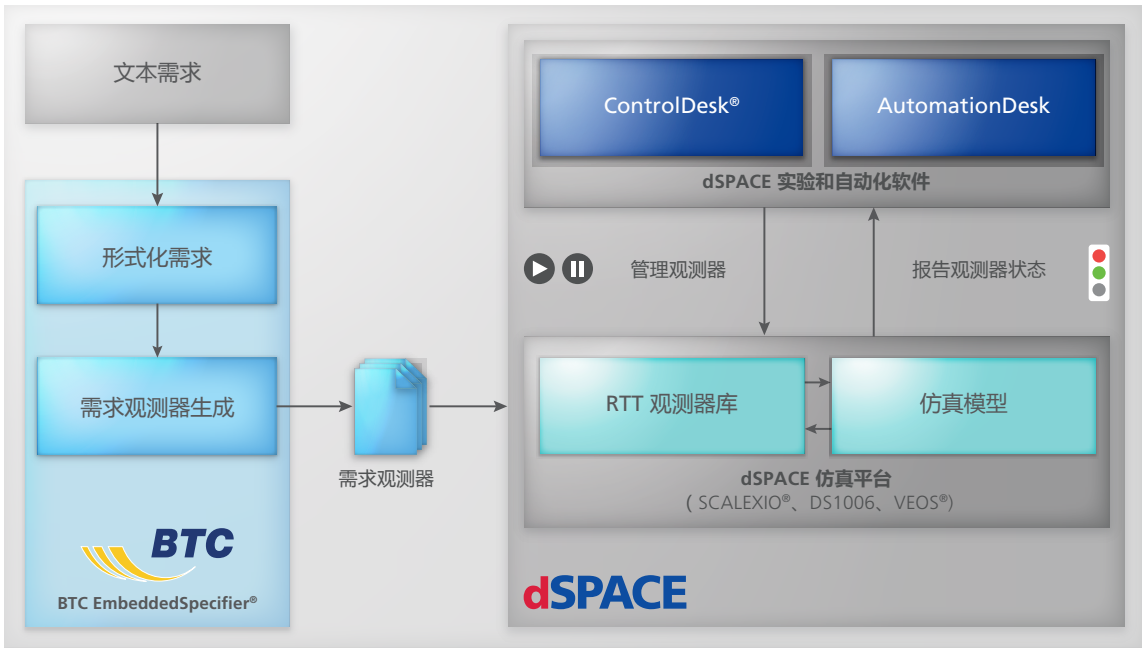


图 1（上图）：基于观测器的测试提高了测试深度。
图 2（下图）：生成具有实时功能的需求观测器，可在 dSPACE 平台上运行，监控需求的合规性。

理想的集成

为了允许用户快速使用需求观测器，dSPACE 提供测试自动化软件 AutomationDesk 的测试模板，以及实验软件 ControlDesk 的布局。该解决方案还可以集成到工具中。出于用户便利，它们可为 Control-Desk 自动生成观测器特定布局，其中在整个执行期间显示每个需求的合规性状态（图 3）。凭借 ControlDesk 布局，可以逐个且完全独立于仿真模型启动、停止和重置观测器。AutomationDesk 模板让开发人员可使用观测器永久检查需求，同时在 AutomationDesk 中执行指定测试序列。在这种情况下，生成的测试报告不仅包括各个测试用例的结果，还包括观测器的结果。触发观测器的时间可用于标识触发和错误的原因。

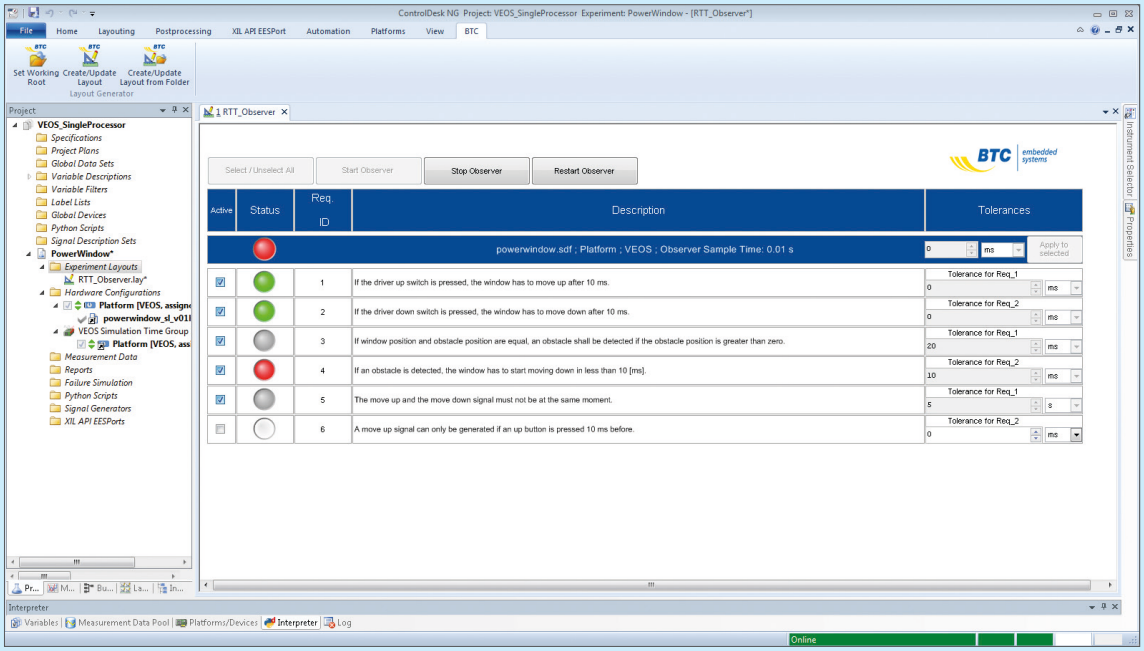


图 3：观测器可以在 ControlDesk 中启动、停止和重置。满足（绿色）和不满足（红色）的需求立即可见。因前提条件尚未得到满足而未启动的观测器显示为灰色。

在各种平台上使用

生成的需求观测器可在各种 dSPACE 仿真平台（SCALEXIO®、DS1006、VEOS®）上使用，而且在一个平台上使用的观测器可在其他平台上重复使用。这样，如果这些测试具有相同的测试级别，在 dSPACE VEOS 虚拟验证的 SIL 和 MIL 开发阶段创建的观测器可立即重复用于 HIL 测试，如 SCALEXIO 平台上。使用 VEOS 中的测试-测试运行也可以准备 HIL 测试。

总结

dSPACE Real-Time Testing (RTT) Observer Library 和 BTC EmbeddedSpecifier 的组合将带来优质解决方案，从而大幅提高测试深度，特别是对于安全关键型应用程序，而无需延长测试持续时间。要实现绝佳的测试深度，务必独立于当前测试案例和仿真情景永久监控每个需求的合规性状态。此举最大程度地降低了因无意导致未发现错误的风险。使用 BTC EmbeddedSpecifier 的工具支持的需求形式化还将提高需求的质量。新解决方案完美集成到用于 HIL 测试和虚拟验证的 dSPACE 工具链。