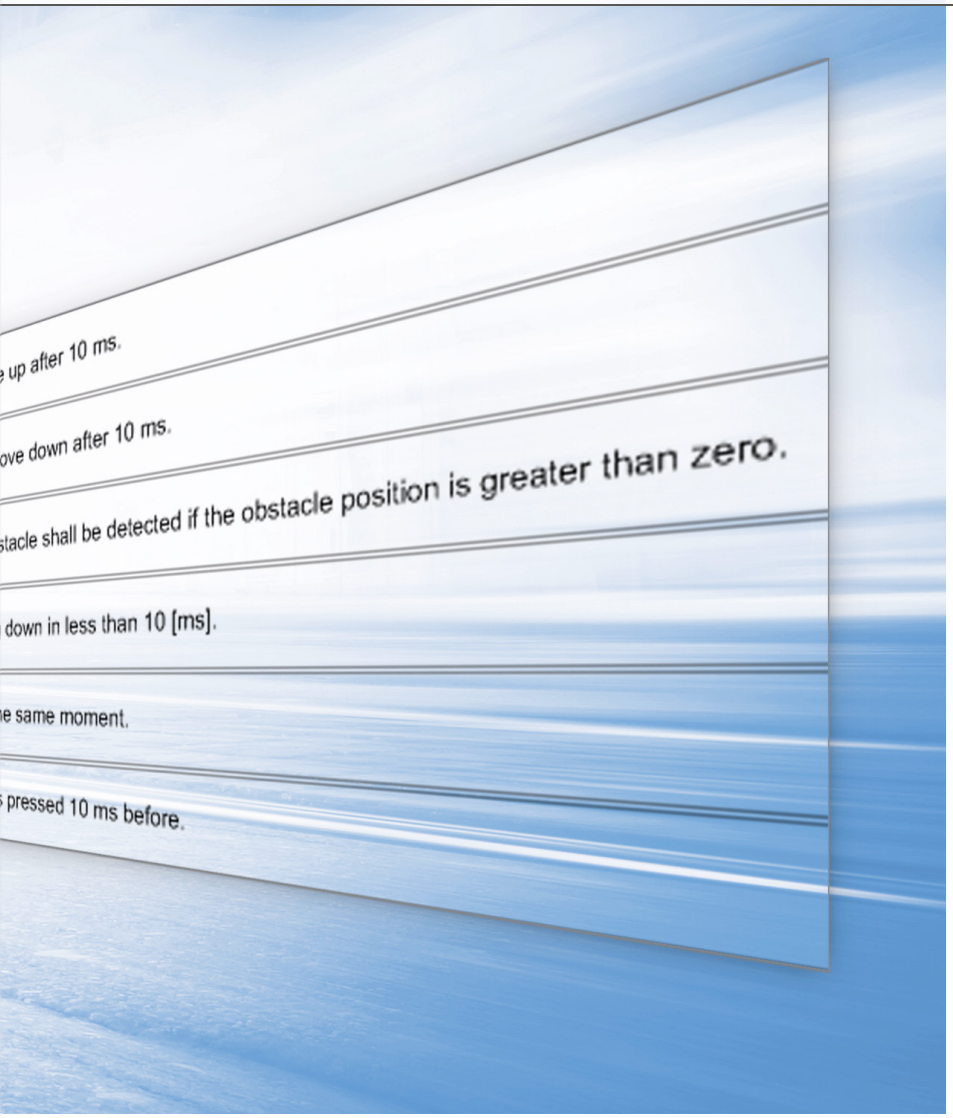
Sicherheitskritische Anforderungen permanent überwachen

Fokussiert auf Sicherheit

Welchen Testaufwand muss man für die Absicherung sicherheitskritischer Systeme treiben? Und wie lassen sich Sicherheitsanforderungen und Aufwand in Einklang bringen? Eine neue Lösung von dSPACE und BTC zur simulationsbasierten formalen Verifikation sicherheitskritischer Steuergerätefunktionen bringt Aufwände und Machbarkeit näher zusammen. Dabei wird die erzielbare Testtiefe drastisch erhöht.

Das Streben nach Innovation, Nutzerkomfort und zusätzlicher Sicherheit bringt immer mehr elektronische sicherheitsrelevante Systeme hervor. Längst sind an verschiedenen Stellen mechanische Rückfallebenen aus Design- oder Kostengründen entfallen. Enorme Anforderungen an die Tests dieser elektronischen Systeme sind somit unausweichlich. So zum Beispiel bei X-by-Wire-Steuerungen und autonomem Fahren, wo ein Systemversagen verheerende Auswirkungen haben könnte. Das Dilemma für die Testingenieure: Trotz der hohen Systemkomplexität und der fast endlos erscheinenden Liste an Anforderungen muss der Zeitaufwand für die Absicherung in vertretbaren Grenzen bleiben. Außerdem gilt es, eine Reihe wichtiger Vorgaben einzuhalten – so empfiehlt zum Beispiel die ISO-Norm 26262 („Road vehicles – Functional safety“) eine formale Verifikation sicherheitskritischer Steuergerätefunktionen. Angesichts dieser Herausforderung haben dSPACE und BTC eine gemeinsame Lösung zur simulationsbasierten formalen Verifikation sicherheitskritischer Anforderungen entwickelt. Damit kann die Einhaltung sicherheitskritischer Anforderungen permanent in Echtzeit auf dSPACE Plattformen überwacht werden.

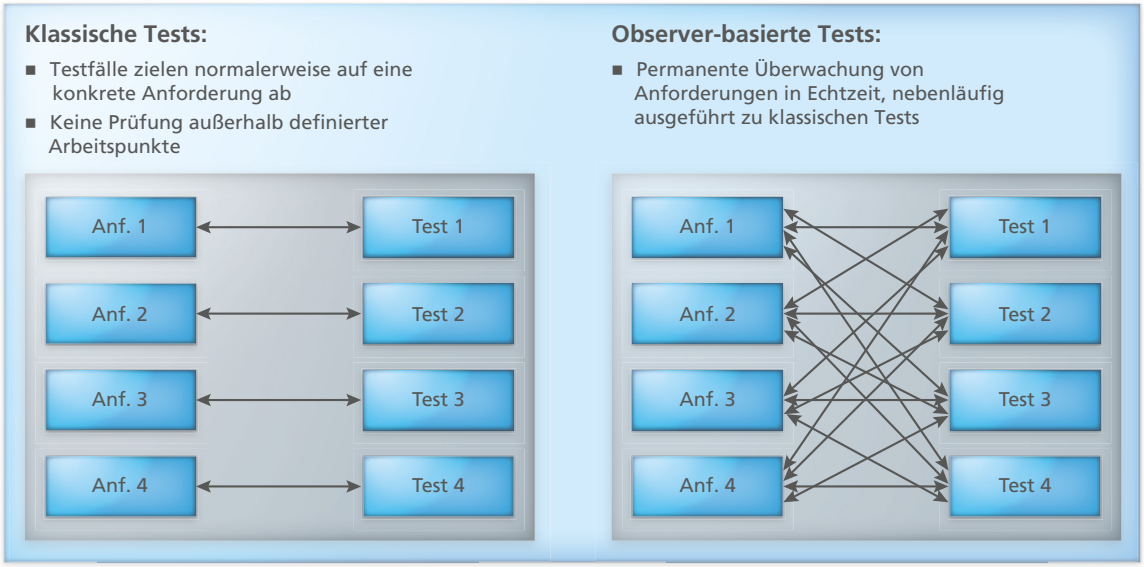


Tiefer testen

Will man für jede sicherheitskritische Funktion unter Berücksichtigung sämtlicher Anforderungen und Querbezüge alle notwendigen Testfälle durchspielen, so kann dies beim klassischen Testprozess zu ernsten Aufwands- und Zeitproblemen führen. Denn wie viele Testfälle will man überhaupt definieren, um wirklich alle Eventualitäten, Querbezüge und Nebenläufigkeiten zu erfassen? Und selbst wenn man in der Lage ist, eine solch lange Liste an Testfällen zu definieren, wie lange dauert es, sie abzuarbeiten und so die gewünschte Testtiefe zu erreichen? Die Lösung von dSPACE und BTC kombiniert auf innovative Weise die neue dSPACE Real-Time Testing (RTT) Observer Library mit dem Spezifikationswerkzeug BTC EmbeddedSpecifier®. Diese Werkzeugkombination ergänzt eine bestehende Model-in-the-Loop (MIL)-, Software-in-the-Loop (SIL)- oder Hardware-in-the-Loop (HIL)-Umgebung um echtzeitfähige „Requirement Observer". Die Observer laufen während der Simulation permanent „nebenher" mit und überwachen die Einhaltung sämtlicher sicherheitskritischer Anforderungen. Darüber hinaus lässt sich unmittelbar erkennen, welche Anforderungen durch die aufgeprägten Testfälle abgedeckt werden bzw. für welche Anforderungen noch keine Testfälle existieren. Die Gesamtgüte sowie der Fortschritt des Testprozesses kann dadurch sehr effizient beurteilt werden. Die simulationsbasierte, permanente formale Verifikation ist eine optimale Ergänzung zum klassischen anforderungsbasierten Testen, das weiterhin die Basis bildet. Die Kombination aus klassischen Tests und dem Einsatz von Observern erhöht die Testtiefe drastisch. Die Observer sind sozusagen ausführbare Prüfkriterien, die sich komfortabel auf verschiedenen dSPACE Plattformen verwenden lassen. Weil die Observer von den eigentlichen Simulationsmodellen entkoppelt sind, muss das bestehende Simulationsmodell für ihren Betrieb nicht verändert werden. Klassische bereits vorhandene Tests lassen sich ohne Änderungen um die nebenläufigen Observer ergänzen. >>

„Die langjährige Erfahrung im Bereich Formalisierung von Anforderungen und Formale Verifikation bei BTC Embedded Systems wird nun mit den bewährten und leistungsfähigen Simulationsplattformen und Testsystemen von dSPACE kombiniert. Hieraus ergibt sich eine optimal abgestimmte und neuartige Werkzeugkette, welche die Qualität und Aussagekraft des Testens gerade im Hinblick auf sicherheitskritische Anwendungen auf eine neue Stufe hebt."

Hans Jürgen Holberg, Vorstand BTC Embedded Systems AG



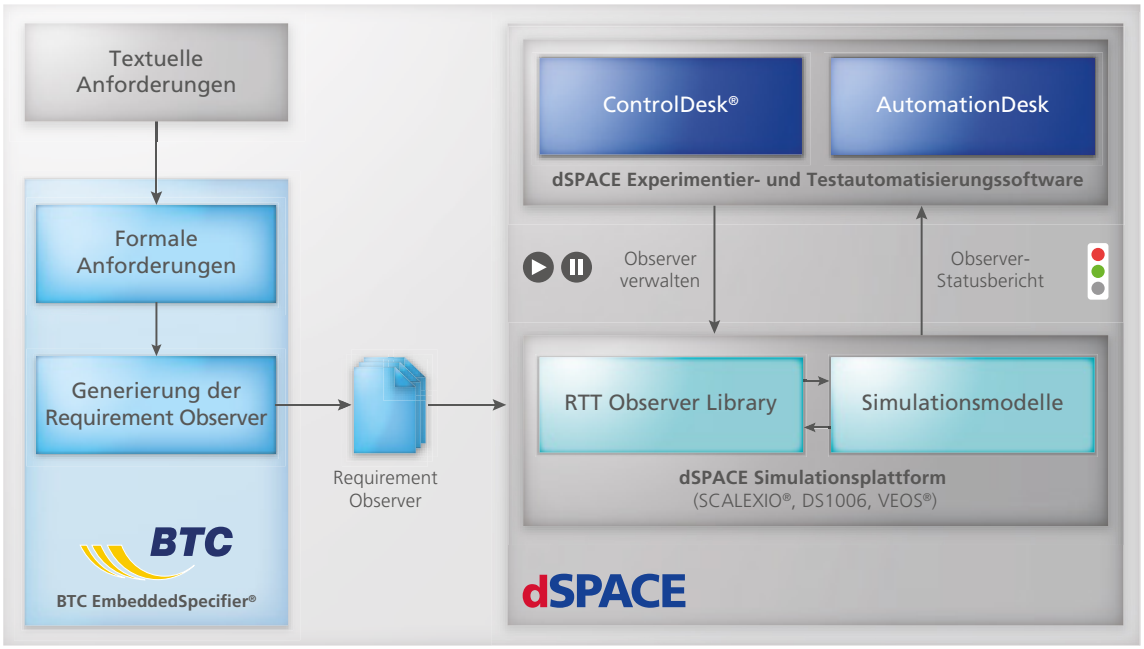


Abbildung 1 (oben): Observer-basierte Tests erhöhen die Testtiefe.
Abbildung 2 (unten): Die generierten echtzeitfähigen Observer fungieren als „ausführbare Prüfkriterien", die komfortabel auf dSPACE Plattformen verwendet werden können.

Höhere Qualität

Zusätzlich erhöht sich auch die Qualität der Anforderungen dank des BTC EmbeddedSpecifier, aus dem die Observer generiert werden. Informelle Anforderungen werden im BTC EmbeddedSpecifier intuitiv und werkzeuggestützt in eine formale Repräsentation und schließlich in ausführbare Observer für die dSPACE Plattformen überführt. Durch ein geführtes, schrittweises Eliminieren von Mehrdeutigkeiten in zuvor rein sprachlich formulierten Anforderungen sowie eine direkte Bezugnahme auf konkrete Modellvariablen wird der Anwender dabei unterstützt, seine Anforderungen so exakt wie möglich zu formulieren. Dies hilft auch dabei, den entsprechenden Sicherheitsnormen und -richtlinien gerecht zu werden.

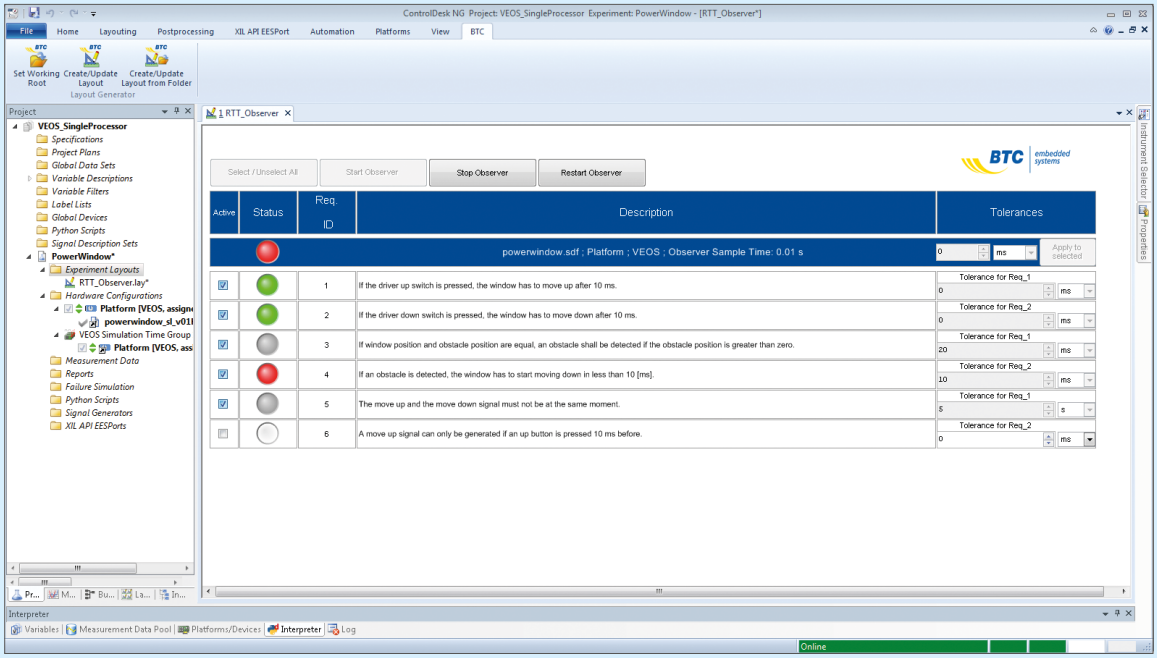


Abbildung 3: Die Observer können in ControlDesk gestartet, gestoppt oder zurückgesetzt werden. Sofort sind erfüllte (grün) und nicht erfüllte (rot) Anforderungen sichtbar. Noch nicht durchlaufene Observer (= Vorbedingung wurde noch nicht erreicht) sind grau.

Optimal integriert

Um Anwendern eine schnelle Nutzung der Requirement Observer zu ermöglichen, stehen vorbereitete Test-Templates für die Testautomatisierungssoftware AutomationDesk und Layouts für die Experimentier-Software ControlDesk® zur Verfügung. Zudem ist die Lösung auch in alternative Werkzeuge integrierbar. Zur komfortablen Bedienung kann für ControlDesk automatisch ein observer-spezifisches Layout generiert werden, das während der kompletten Ausführung den Erfüllungsstatus jeder Anforderung zeigt (Abbildung 3). Die Observer lassen sich über das ControlDesk-Layout sowohl einzeln als auch völlig unabhängig vom Simulationsmodell starten, stoppen oder zurücksetzen. AutomationDesk-Templates erlauben es außerdem, parallel zum definierten Testablauf in AutomationDesk die Anforderungen permanent mit den Observern zu prüfen. Im generierten Testbericht erscheinen dann nicht nur die Ergebnisse der einzelnen Testfälle, sondern auch die der Observer. Aus dem Zeitpunkt, zu dem ein Observer ausgelöst hat, lässt sich die Ursache des Auslösens und somit des Fehlverhaltens leicht ermitteln.

Plattformübergreifender Einsatz

Die erzeugten Requirement Observer können auf verschiedensten dSPACE Simulationsplattformen (SCALEXIO®, DS1006, VEOS®) eingesetzt werden und sind außerdem zwischen diesen Plattformen wiederverwendbar. Auf diese Weise lassen sich Observer, die in der Entwicklungsstufe SIL und MIL für die virtuelle Validierung auf dSPACE VEOS entstanden sind, auch direkt für HIL-Tests, zum Beispiel auf SCALEXIO-Plattformen, weiter nutzen, sofern sich diese Tests auf derselben Teststufe befinden. Außerdem können HIL-Tests mit Hilfe von „Test-the-Test"-Läufen in VEOS gezielt vorbereitet werden. ■

Fazit

Die Kombination aus der dSPACE Real-Time Testing (RTT) Observer Library und dem BTC EmbeddedSpecifier ergibt eine hochwertige Lösung, um die Testtiefe gerade bei sicherheitskritischen Anwendungsfällen massiv zu steigern, ohne die Testdauer zu erhöhen. Wichtig für die erzielbare Testtiefe ist es, den Erfüllungsstatus aller Anforderungen unabhängig vom konkret ausgeführten Testfall oder Simulationsszenario permanent zu überwachen. Das Risiko unentdeckter Fehler durch unbeabsichtigte Seiteneffekte lässt sich auf diese Weise minimieren. Durch die werkzeuggestützte Anforderungsformalisierung mit dem BTC EmbeddedSpecifier erhöht sich zudem die Qualität der Anforderungen. Die neue Lösung ist optimal in die dSPACE Werkzeugkette für HIL-Tests und virtuelle Absicherung integriert.