







Continuous monitoring of
safety-critical applications

Keeping an Eye on Safety

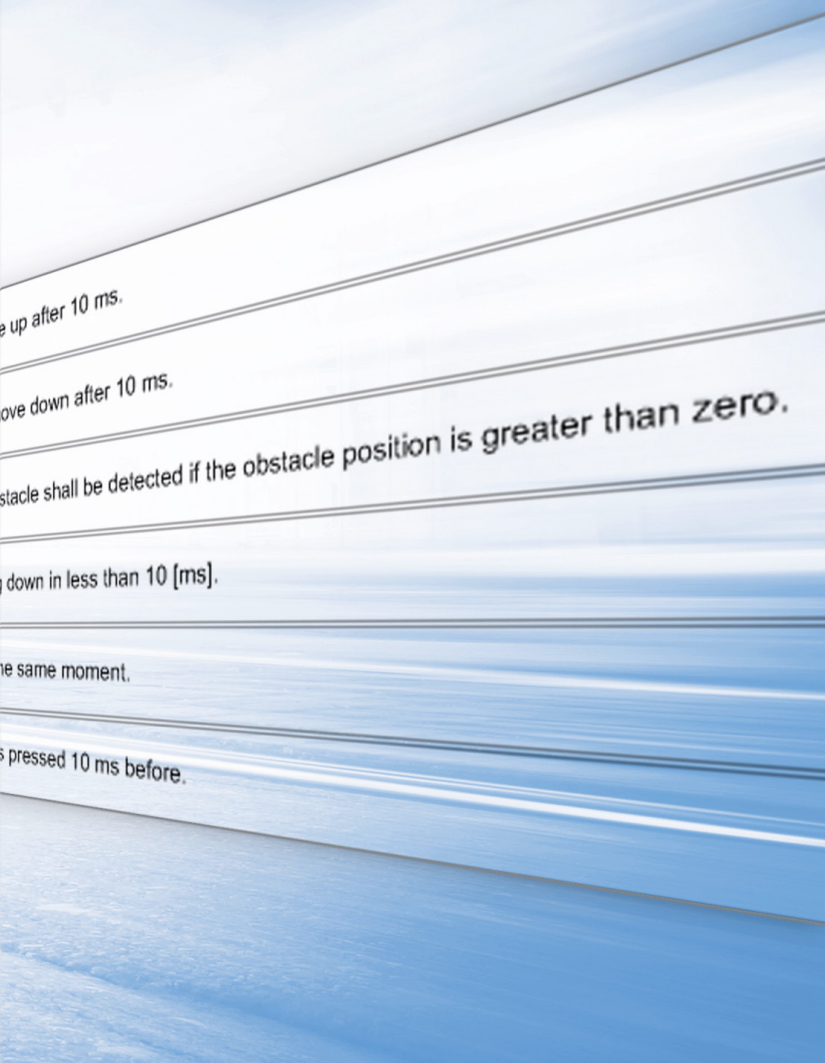
<input checked="" type="checkbox"/>		1	If the driver up switch is pressed, the window has to move
<input checked="" type="checkbox"/>		2	If the driver down switch is pressed, the window has to m
<input checked="" type="checkbox"/>		3	If window position and obstacle position are equal, an ob
<input checked="" type="checkbox"/>		4	If an obstacle is detected, the window has to start moving
<input checked="" type="checkbox"/>		5	The move up and the move down signal must not be at th
<input type="checkbox"/>		6	A move up signal can only be generated if an up button is

How much testing is necessary to validate safety-critical systems? How can you balance safety requirements and effort? A new solution by dSPACE and BTC for the simulation-based formal verification of safety-critical ECU functions brings effort and feasibility closer together. At the same time, the test depth increases.

As the world strives for innovation, user convenience and more safety, the number of electronic safety-relevant systems is growing. In various areas, the times of mechanical fallback systems are long gone due to design or cost considerations. It is therefore inevitable that the tests of these electronic systems face stringent requirements. Examples of such systems are x-by-

wire steering and autonomous driving, where system failure could have disastrous effects. This puts developers in a difficult place: Despite the high system complexity and the seemingly endless list of requirements, the time required for validation has to stay within reasonable limits. The developers also have to comply with a number of important guidelines. For example,

the ISO 26262 standard ("Road vehicles – Functional safety") recommends performing a formal verification of safety-critical functions of electronic control units (ECUs). In the light of these challenges, dSPACE and BTC together have developed a solution for the simulation-based formal verification of safety-critical applications. It can be used to monitor the compliance



all of them to achieve the desired test depth? The innovative solution from dSPACE and BTC combines the new dSPACE Real-Time Testing (RTT) Observer Library with the specification tool BTC Embedded-Specifier®. These tools complement existing model-in-the-loop (MIL), software-in-the-loop (SIL) and hardware-in-the-loop (HIL) environments with real-time-capable requirement observers. During a running simulation, the observers are running in parallel and monitor the compliance with all safety-critical requirements. It is also possible to immediately see which requirements are covered by the implemented test cases and which are not. This lets developers efficiently assess the overall quality and the progress of the test process. The simulation-based, permanent formal verification is the ideal addition to traditional requirements-based testing, which is still the basis. The combination of traditional tests and observer-based testing significantly increases the test depth. Think of the observers as executable test criteria that can be conveniently used on various dSPACE platforms. Since the observers are decoupled from the actual simulation models, existing simulation models do not have to be modified for their use. Existing traditional tests can easily be extended by observers without having to be modified. >>

with safety-critical requirements permanently and in real time on dSPACE platforms.

More Test Depth

In the traditional testing process, running all the necessary test cases for each safety-critical function while considering all the requirements and

cross-references can cause serious problems in terms of effort and time. After all, how many test cases would you have to define to cover absolutely all eventualities, cross-references, and concurrencies? And even if you were able to define such a long list of test cases, how much time would you need to run through



“The long-standing experience of BTC EmbeddedSystems in requirement formalizing and formal verification is now combined with the established and powerful simulation platforms and systems from dSPACE. This results in a perfectly fine-tuned and unique tool chain that takes the quality and meaningfulness of testing to a new level, especially for safety-critical applications.”

Hans Jürgen Holberg, Board of Management, BTC Embedded Systems AG

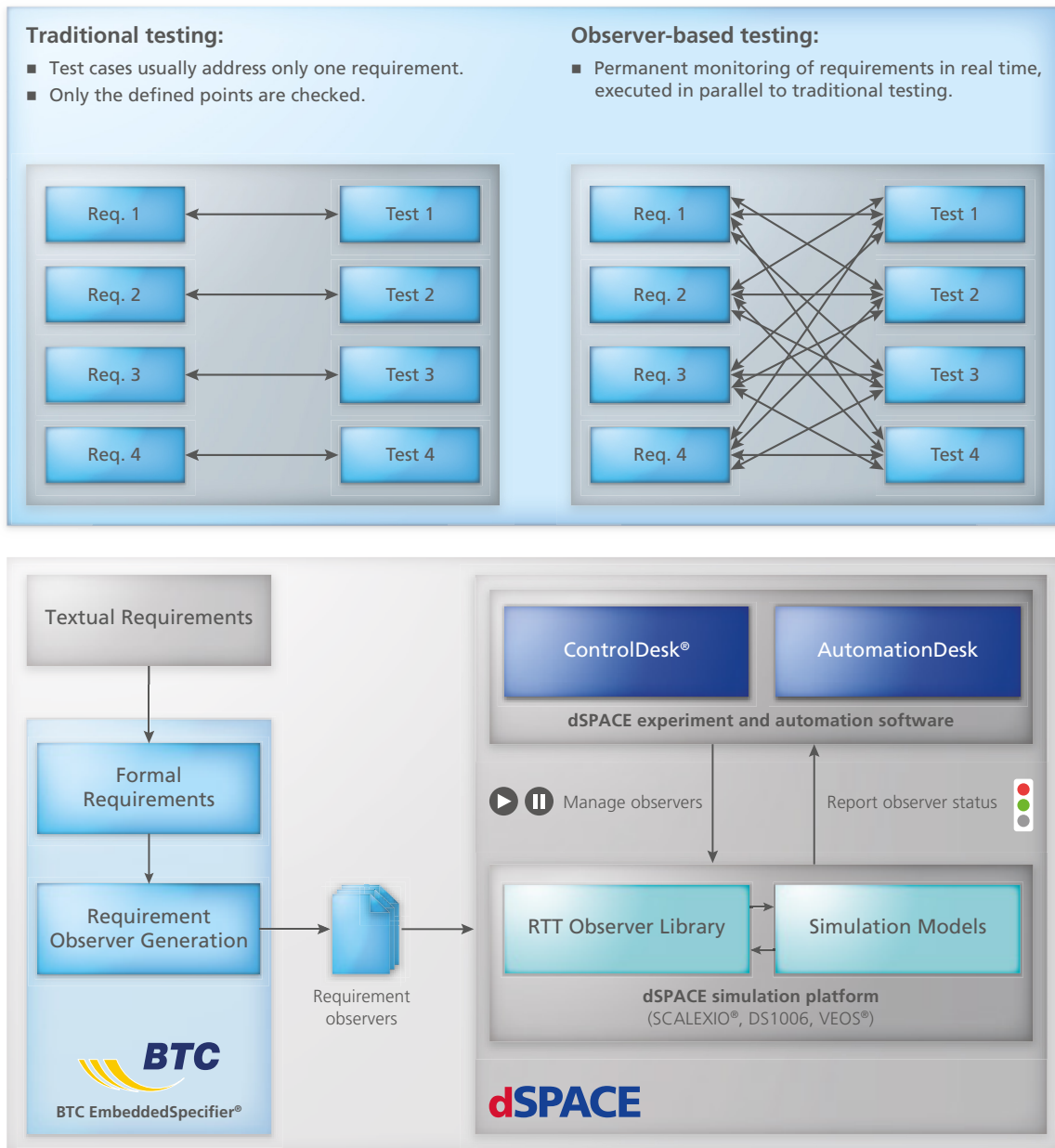


Figure 1 (above): Observer-based tests increase the test depth.

Figure 2 (below): The generated real-time-capable observers function as executable test criteria that are easy to use on dSPACE platforms.

More Quality

Thanks to BTC EmbeddedSpecifler, the quality of the requirements from which the observers are generated also increases. BTC EmbeddedSpecifler provides tool support and thus makes it easy to translate informal requirements into a formal

representation and then into executable observers for the dSPACE platform. The guided, stepwise elimination of ambiguities in the previously language-based requirements and the direct reference of concrete model variables helps the users formulate their requirements as pre-

cisely as possible. This also helps comply with the relevant safety standards and guidelines.

Ideal Integration

To allow users to quickly use the requirement observers, dSPACE provides test templates for the test auto-

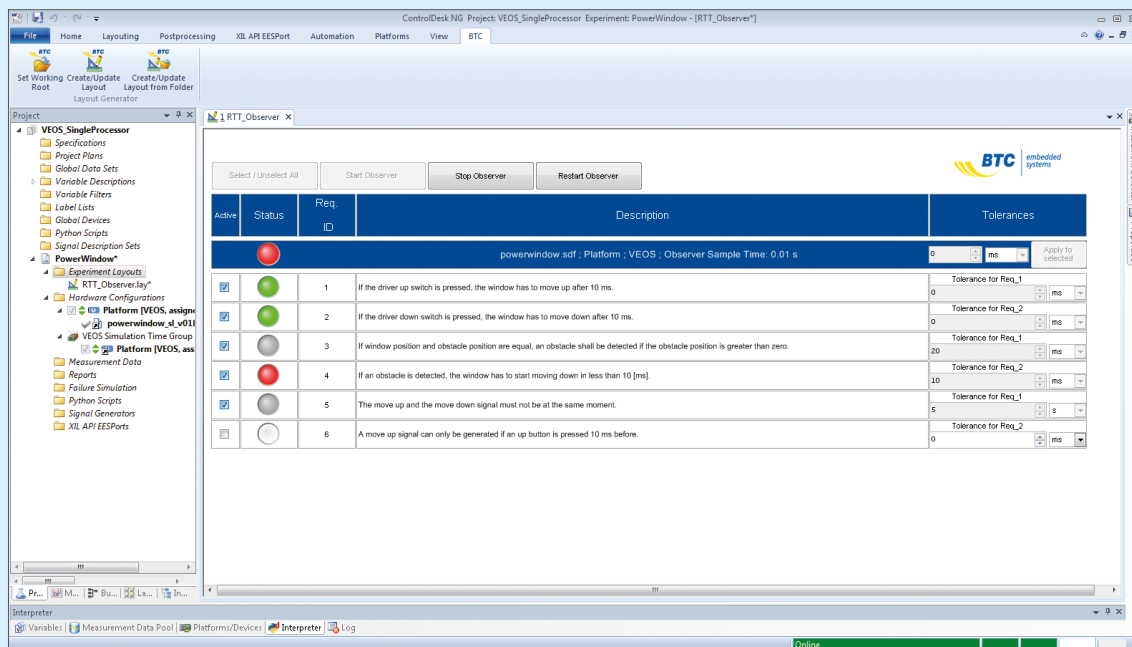


Figure 3: The observers can be started, stopped and reset in ControlDesk. Requirements that are met (green) and not met (red) are visible immediately. Observers that have not started yet because their precondition has not been fulfilled are displayed in gray.

mation software AutomationDesk and layouts for the experiment software ControlDesk. The solution can also be integrated in alternative tools. For the users' convenience, they can automatically generate observer-specific layouts for ControlDesk that display the compliance status of each requirement during the entire execution (figure 3). With the ControlDesk layout, the observers can be started, stopped and reset individually and completely independently of the simulation model. The AutomationDesk templates let developers use the observers to permanently check the requirements while a specified test sequence is being executed in AutomationDesk. In this case, the generated test report includes not only the results of the individual test cases but also those of the observers. The time when an observer was triggered can be used to identify the cause of the trigger and thus the error.

Use on Various Platforms

The generated requirement observers can be used on various dSPACE simulation platforms (SCALEXIO®, DS1006, VEOS®), and an observer that was used on one platform can be reused on another. This way, observers that were created in the SIL and MIL development stage for virtual validation on dSPACE VEOS can be reused immediately for HIL tests, e.g., on SCALEXIO platforms, if these tests have the same test level. HIL tests can also be prepared by using test-the-test runs in VEOS. ■

Conclusion

The combination of the dSPACE Real-Time Testing (RTT) Observer Library and BTC EmbeddedSpecifier creates a high-quality solution that massively improves test depth, especially for safety-critical applications, without prolonging the duration of the tests. To achieve a great test depth, it is important to permanently monitor the compliance state of each requirement independently of the current test case and simulation scenario. This minimizes the risk of undiscovered errors caused by unintentional side effects. The tool-supported requirement formalizing with BTC EmbeddedSpecifier also increases the quality of the requirements. The new solution integrates perfectly into the dSPACE tool chain for HIL tests and virtual validation.