The ISO 26262 standard ("Road vehicles – Functional safety") became effective in November 2011. It describes processes and methods for ensuring functional safety during the development and production of safety-relevant vehicle electrics/electronics systems. The standard defines the state of technology and is therefore mandatory for car manufacturers. But how can manufacturers translate the generic requirements into concrete development measures? One approach is using reference workflows and tools that were qualified or certified by accredited certification authorities such as TÜV. In the end, this approach also reduces product liability risks.

ISO 26262 Requirements for Using Software Tools

ISO 26262 stipulates that a software tool used in safety-relevant projects must first be classified for the specific field of application. The classification includes analyzing the impact of the tool on fulfilling or violating functional safety requirements. The classification result is called the tool confidence level (TCL). The tool might then have to be qualified based on the TCL (see info box page 42). Usually, the qualification is performed by using a combination of suitable qualifiation methods, which depends on the Automotive Safety Integrity Level (ASIL) of the system that is being developed and tested with the software tool. For the users, however, implementing these qualification methods is very difficult and effort-intensive, because it requires sound knowledge of the processes and methods involved in the tool's development. Therefore, implementing the methods requires expert knowledge on >>

In 2014, TÜV SÜD certified dSPACE's test automation software, AutomationDesk, for testing safety-relevant systems according to ISO 26262 and IEC 61508 – making AutomationDesk the first-ever commercial test automation software for hardware-in-the-loop (HIL) simulation to receive this certificate. But what exactly does this mean for the users?

Certifiably Safe

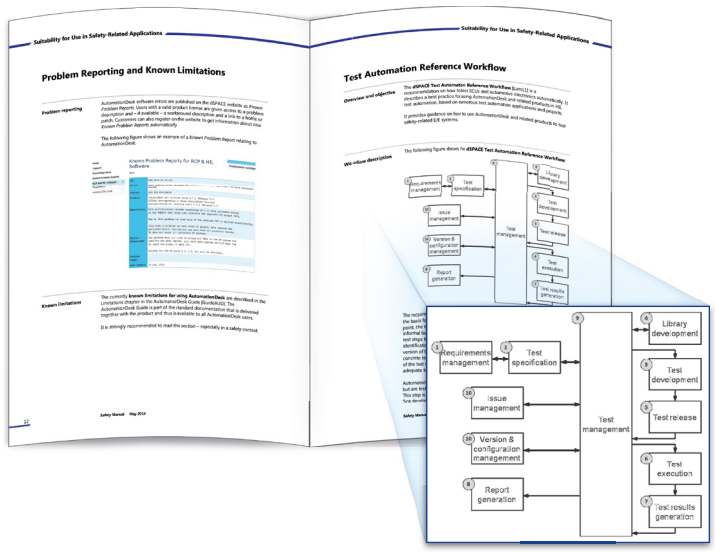
The TÜV SÜD certificate for AutomationDesk makes the classification, qualification and validation according to the ISO 26262 and IEC 61508 standards much easier

What Do ISO 26262 and IEC 61508 Define?

IEC 61508 is the internationally recognized generic standard for the development of safety-related electronic systems. In the automotive industry, ISO 26262 replaced IEC 61508 in late 2011 as the standard for the functional safety of passenger cars. ISO 26262 is a modification of IEC 61508, adjusted to the specific conditions in the automotive sector. Implementing these standards increases the functional safety of a vehicle system with electrical/electronic components. In order to adhere to these standards, the tools that are used for developing the electrical/electronic components have to be classified, qualified and/or validated.

ISO 26262 defines four methods for tool qualification. Depending on the respective ASIL, the users select a suitable combination of these methods:

a. Increased confidence from use (ISO 26262-8, 11.4.7 to 11.4.10)
b. Evaluation of the tool development process (ISO 26262-8, 11.4.8)
c. Validation of the software tool (ISO 26262-8, 11.4.9)
d. Development in accordance with a safety standard (ISO 26262-8, 11.4.10)



The AutomationDesk Safety Manual with the Test Automation Reference Workflow.

assessing tool development according to ISO 26262.

TÜV SÜD Certificate

In close cooperation with dSPACE GmbH in Paderborn, TÜV SÜD particularly analyzed dSPACE-internal processes and documentation to assess the development and quality assurance of AutomationDesk (see info box page 43). TÜV SÜD also analyzed the customer communication process and bug reporting as well as the new AutomationDesk Safety Manual. As a result, TÜV awarded AutomationDesk the "Software Tool for Safety-Related Development" certificate, which underlines that AutomationDesk is suitable for testing safety-relevant systems in the automotive, commercial vehicle, and aviation sectors, and many other areas of industry. This officially confirms that AutomationDesk is "fit for purpose" for testing safety-relevant systems according to ISO 26262 and IEC 61508, for all Automotive Safety Integrity Levels, from ASIL A to ASIL D and SIL1 to SIL3, respectively.

The AutomationDesk Safety Manual

One key component of the certification is the AutomationDesk Safety Manual, a supplemental user documentation for using AutomationDesk in safety-relevant projects. In particular, it provides

- A general overview of AutomationDesk and all available product and user documentation
- Recommendations and best practices for commissioning and using AutomationDesk, including the AutomationDesk Test Automation Reference Workflow
- An example of the Test Automation Reference Workflow in the test process defined by ISO 26262
- A tool classification for AutomationDesk
- The "fit for purpose" certificate for AutomationDesk according to ISO 26262 and IEC 61508

AutomationDesk: First certified commercial software for HIL test automation.

Valuable Support for the Development of Safety-Relevant Systems

With this certificate, TÜV SÜD, as an independent organization, confirms the high quality of the development process and the comprehensive quality assurance for AutomationDesk. And if AutomationDesk is always used as described in the AutomationDesk Safety Manual, users do not even have to go to the lengths of creating their own tool classification. The certificate also makes qualifying AutomationDesk much easier, because it attests that the software fulfills the relevant criteria of the qualification methods "Evaluation of the tool development process" and "Validation of the software tool" and most of the criteria of "Increased confidence from use".

AutomationDesk was the first commercial software product for test automation in a hardware-in-the-loop context to be awarded such a certificate. Together with the AutomationDesk Safety Manual, the certificate gives users invaluable support for using AutomationDesk to develop and test safety-related systems according to ISO 26262 and IEC 61508. The TÜV SÜD certificate for AutomationDesk facilitates the classification, qualification, and validation according to the standards.

Outlook

The certified software version is AutomationDesk 4.1. Another certification process for the new AutomationDesk version 5.0, which will be available as of summer 2015, is close at hand. Future versions will be certified as needed. For more information on the TÜV SÜD certificate for AutomationDesk, please contact your sales representative. ■

Basis of the TÜV SÜD Check

In order to certify AutomationDesk, TÜV SÜD audited the dSPACE departments responsible for AutomationDesk.

TÜV SÜD checked

- The AutomationDesk development process, e.g., requirements management, change management, release management
- The validation of AutomationDesk, e.g., traceability of test results according to the requirements
- The customer communication process
- The AutomationDesk Safety Manual

These factors were assessed on-site based on all relevant development documents for AutomationDesk, such as the Specifications Document, detailed functional and component-oriented specifications, design documents, test catalogs, test results, process documentation, company-wide development regulations and their project-specific modifications.

The cooperation with the different departments was key to the fast and positive certification result. TÜV SÜD found that the AutomationDesk processes were already very well suited. dSPACE quickly implemented the few suggestions for improvement for the audit and was consequently awarded the certificate.