Die im November 2011 in Kraft getretene ISO 26262 („Road vehicles – Functional safety“) beschreibt Prozesse und Methoden für die Einhaltung der funktionalen Sicherheit bei der Entwicklung und Produktion sicherheitsrelevanter elektrischer und elektronischer Systeme in Kraftfahrzeugen. Sie definiert den Stand der Technik und ist damit von Automobilherstellern nachweisbar einzuhalten. Doch wie lassen sich die generischen Vorgaben und Anforderungen in konkrete Entwicklungsmaßnahmen umsetzen? Referenzworkflows und Werkzeuge, die durch akkreditierte Prüfstellen wie den TÜV qualifiziert oder zertifiziert wurden, bieten einen möglichen Ansatz, der letztlich auch geeignet ist, Risiken im Bereich der Produkthaftung zu reduzieren.

Anforderungen der ISO 26262 an die Verwendung von Software-Werkzeugen

ISO 26262 fordert, dass ein Software-Werkzeug, das in sicherheitsrelevanten Projekten eingesetzt wird, im konkreten Anwendungskontext zunächst klassifiziert wird. Dabei wird analysiert, welchen Einfluss das Werkzeug im Hinblick auf die Einhaltung oder Verletzung der funktionalen Sicherheit hat. Als Ergebnis der Klassifizierung ergibt sich der sogenannte Tool Confidence Level (TCL). Auf dieser Basis muss das Werkzeug gegebenenfalls qualifiziert werden (s. Infobox Seite 42). Abhängig vom ASIL (Automotive Safety Integrity Level) des Systems, das mit Hilfe des Software-Werkzeugs entwickelt und getestet wird, ist für die Qualifizierung typischerweise eine Kombination geeigneter Qualifizierungsmethoden auszuwählen. Die Umsetzung dieser Qualifizierungs- >>

2014 zertifizierte der TÜV SÜD die Testautomatisierungssoftware AutomationDesk von dSPACE für den Test sicherheitsrelevanter Systeme gemäß ISO 26262 und IEC 61508 – als erste kommerzielle Software für die Testautomatisierung im Bereich Hardware-in-the-Loop-Simulation überhaupt. Aber was bedeutet das konkret für den Anwender?

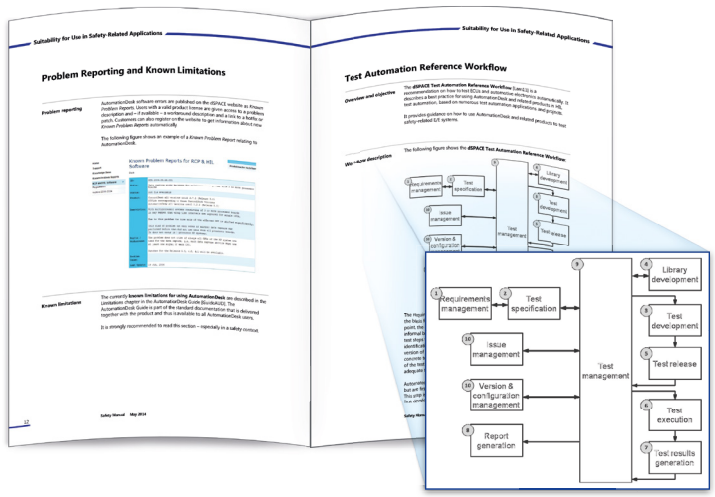
Sicher voran

Das TÜV-SÜD-Zertifikat für AutomationDesk erleichtert die Klassifizierung, Qualifizierung und Validierung gemäß den Standards ISO 26262 und IEC 61508

Was definieren ISO 26262 und IEC 61508?

Die IEC 61508 ist der weltweit anerkannte generische Standard für die Entwicklung sicherheitsrelevanter elektronischer Systeme. Im Bereich der Automobilindustrie wurde die IEC 61508 Ende 2011 durch die Einführung der ISO 26262 als Norm zur funktionalen Sicherheit von Personenkraftwagen abgelöst.
ISO 26262 ist eine Anpassung der IEC 61508 an die spezifischen Gegebenheiten im Automobilbereich. Die Umsetzung der Norm soll die funktionale Sicherheit eines Systems mit elektrischen/elektronischen Komponenten im Kraftfahrzeug gewährleisten. Zu einer normgerechten Entwicklung gemäß diesen beiden Standards gehört die Klassifizierung und Qualifizierung bzw. Validierung der Software-Werkzeuge, die für die Entwicklung der elektrischen/elektronischen Komponenten eingesetzt werden.
Die ISO 26262 definiert vier unterschiedliche Methoden für die Tool-Qualifizierung, aus denen Anwender – abhängig vom vorliegenden ASIL – typischerweise eine geeignete Kombination auswählen:

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)



Das AutomationDesk Safety Manual mit dem „Test Automation Reference Workflow".

methoden ist aus Anwendersicht jedoch extrem schwierig und aufwendig, denn sie erfordert tiefen Einblick und umfangreiche Kenntnisse der Prozesse und Methoden, nach denen das Werkzeug entwickelt wird. Hier benötigt man Experten, die sich mit der Bewertung der Tool-Entwicklung vor dem Hintergrund der ISO 26262 sehr gut auskennen.

Das TÜV-SÜD-Zertifikat

In enger Zusammenarbeit mit der dSPACE GmbH in Paderborn hat der TÜV SÜD vor allem die dSPACE-internen Prozesse und Dokumentationen für die Entwicklung und Qualitätssicherung von AutomationDesk genau unter die Lupe genommen (s. Infobox Seite 43). Weitere untersuchte Kriterien waren der Kundeninformationsprozess und das Bug Reporting sowie das neu erstellte AutomationDesk Safety Manual.
Als Ergebnis hat AutomationDesk ein TÜV-Zertifikat als „Software Tool for Safety Related Development" erhalten, das die Eignung von AutomationDesk für den Test sicherheitsrelevanter Systeme in den Bereichen Automotive, Nutzfahrzeuge, Flugzeugindustrie und vielen anderen Industriebereichen unterstreicht. Damit wird offiziell bestätigt, dass AutomationDesk „fit for purpose" für den Test sicherheitsrelevanter Systeme gemäß ISO 26262 und IEC 61508 ist, und zwar für alle Automotive Safety Integrity Level, von ASIL A bis ASIL D bzw. SIL1 bis SIL3.

Das „AutomationDesk Safety Manual"

Ein zentraler Bestandteil der Zertifizierung ist das AutomationDesk Safety Manual, eine ergänzende Benutzerdokumentation für den Einsatz von AutomationDesk in sicherheitsrelevanten Projekten. Es enthält insbesondere

- einen generellen Überblick über AutomationDesk sowie über sämtliche verfügbaren Produkt- und Benutzerdokumentationen,
- Empfehlungen und Best Practices für die Inbetriebnahme und den Einsatz von AutomationDesk, einschließlich des AutomationDesk „Test Automation Reference Workflows",
- eine Abbildung des „Test Automation Reference Workflows" auf den von der ISO 26262 vorgegebenen Testprozess,

AutomationDesk: erstes kommerzielles Software-Produkt für die Testautomatisierung im HIL-Bereich mit Zertifikat.

- eine Tool-Klassifizierung für AutomationDesk,
- den „Fit-for-purpose"-Nachweis für AutomationDesk gemäß ISO 26262 und IEC 61508.

Wertvolle Unterstützung bei der Entwicklung sicherheitsrelevanter Systeme

Mit dem Zertifikat bestätigt der TÜV SÜD als unabhängige Organisation nicht nur die hohe Qualität des Entwicklungsprozesses sowie die umfangreiche Qualitätssicherung für AutomationDesk. Wenn AutomationDesk konsequent gemäß Safety Manual eingesetzt wird, können Anwender sogar auf die aufwendige Erstellung einer eigenen Tool-Klassifizierung verzichten. Auch die Qualifizierung von AutomationDesk wird durch das Zertifikat erheblich erleichtert, bestätigt es doch die Einhaltung der relevanten Kriterien der Qualifizierungsmethoden „Evaluation of the tool development process" und "Validation of the software tool" sowie in großen Teilen die der „Increased confidence from use". AutomationDesk ist das erste kommerzielle Software-Produkt für die Testautomatisierung im Bereich Hardware-in-the-Loop-Simulation, das ein solches Zertifikat erhalten hat. Zusammen mit dem AutomationDesk Safety Manual bekommen Anwender wertvolle Unterstützung für den Einsatz von AutomationDesk bei der Entwicklung und dem Test sicherheitsrelevanter Systeme nach ISO 26262 und IEC 61508. Das TÜV-SÜD-Zertifikat erleichtert den Anwendern also erheblich die Klassifizierung, Qualifizierung und Validierung gemäß den Standards.

Ausblick

Die Zertifizierung wurde für AutomationDesk 4.1 durchgeführt. Für die neue Version, AutomationDesk 5.0, die im Sommer 2015 erscheint, steht eine Zertifizierung kurz bevor. Für zukünftige Versionen erfolgt eine Zertifizierung je nach Bedarf. Bitte wenden Sie sich an Ihren Vertriebsansprechpartner, wenn Sie weitere Informationen zum TÜV-SÜD-Zertifikat für AutomationDesk wünschen. ■

Grundlage der Prüfung durch den TÜV SÜD

Um die Zertifizierung von AutomationDesk durchzuführen, hat der TÜV SÜD die dSPACE Abteilungen einem Audit unterzogen, die für AutomationDesk verantwortlich sind. Geprüft wurden

- der Entwicklungsprozess von AutomationDesk, z.B. Requirements Management, Change Management, Release Management,
- die Validierung von AutomationDesk, z.B. Nachverfolgbarkeit von Testergebnissen entsprechend den Anforderungen,
- der Kundeninformationsprozess,
- das Safety Manual.

Basis für diese Prüfungen im mehrtägigen Vorort-Assessment waren alle relevanten Entwicklungsdokumente für AutomationDesk, z.B. das Pflichtenheft, funktionale und komponentenorientierte Detail-Spezifikationen, Design-Unterlagen, Testkataloge, Testergebnisse, Prozessdokumentationen, unternehmensweite Entwicklungsrichtlinien und deren projektspezifische Anpassungen. Für das gute und schnelle Ergebnis der Zertifizierung war die Zusammenarbeit aus unterschiedlichen Abteilungen ausschlaggebend.
Dabei hat sich gezeigt, dass die Prozesse rund um AutomationDesk schon sehr gut passten. Einige Verbesserungsvorschläge konnten zeitnah für die finale Prüfung und somit zur Erlangung des Zertifikats umgesetzt werden.