Software Verifikation – Testsystem oder Software-Tool?

Oktober 2014

SGS TÜV SAAR

WHEN YOU NEED TO BE SURE

SGS

Vorstellung SGS-TÜV Saar GmbH

- SGS-TÜV Saar GmbH / Funktionale Sicherheit
  - Joint-Venture zwischen SGS-Gruppe und TÜV Saarland
  - Global Competence Center - Funktionale Sicherheit
    - Zentrale in München, Zweigstelle in Dortmund
    - Lokale Expertenteams in Japan, China, Taiwan und Korea
    - Gem. ISO/IEC 17025 akkreditierte Prüfstelle für Funktionale Sicherheit
    - Mitglied bei den relevanten Standardisierungsgremien, wie z.B. IEC 61508, ISO 26262 und E-Mobilität

Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
- Fazit

Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
- Fazit

Motivation

- Immer wieder stellen sich bei der Planung der Software-Verifikation und System-Validierung folgende Fragen:
  - Werden an Testsysteme besondere Anforderungen gestellt?
  - Ist Software, die in Zusammenhang mit einer speziellen Test-Hardware benutzt wird,
    - ein Software Tool?
    - Muss diese Software den Standardanforderungen für Software Tools genügen?

Beispiel Testaufbau - Tool

Cantata Test Results Summary

Project: *AutoTest Demo* **Overall Result: Pass**

Summary Information

Hostname	MATT	Cantata version	v6.2
Summary generated	6 Dec 2013 11:52	Time elapsed during test run	12 seconds

Build Summary

Total tests	4
Compile attempted (files)	8
Link attempted (tests)	4
Execute attempted (tests)	4

Results Summary

PASSED	4
FAILED	0
Total checks	241
Total checks failed	0
Total script errors/call failures	0

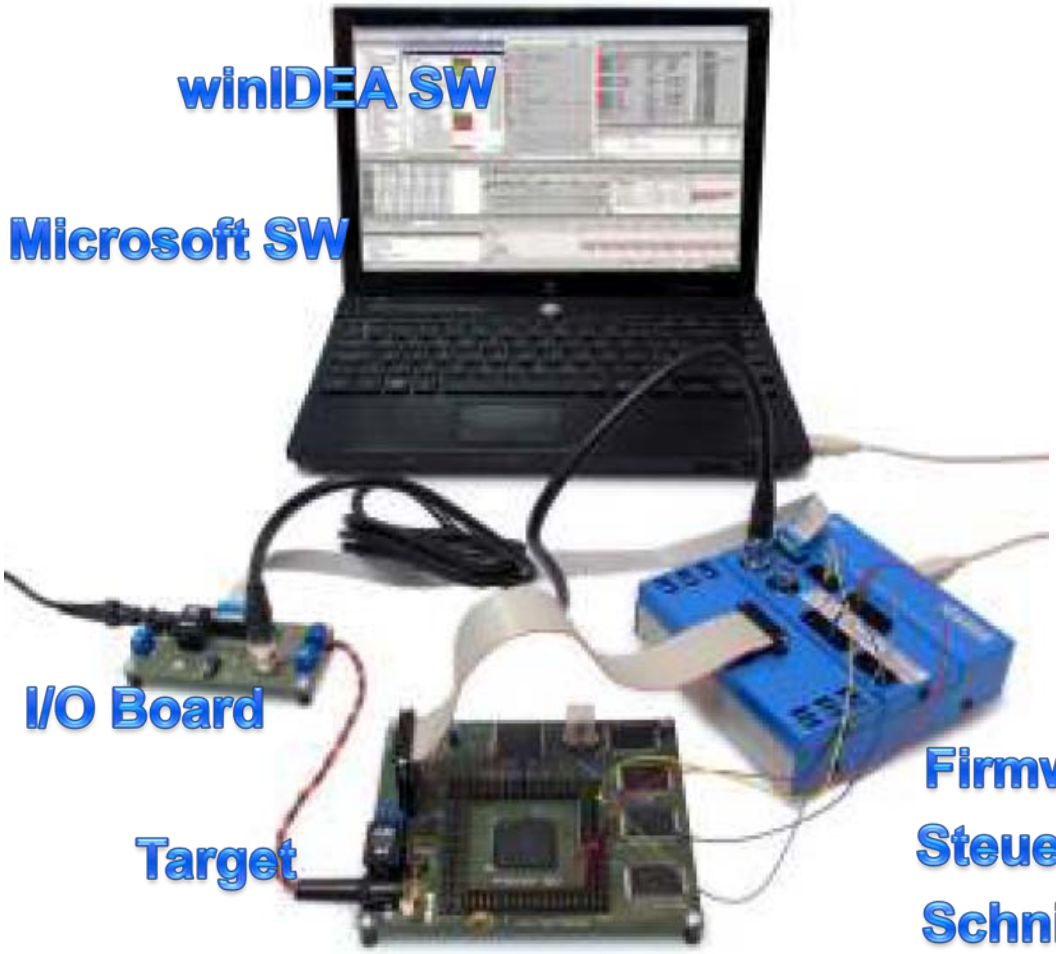
Coverage Summary

Entry point (E)	100%
Statement (S)	100%
Decision (D)	100%
Call-return (C)	-
MC/DC - masking (M)	100%
MC/DC - unique cause (U)	100%

Testaufbau besteht aus:

- Laptop, mit üblicher Microsoft SW
- Cantata, Codeanalyse Tool (Screen Shot)

Beispiel Testaufbau - Testsystem



Testaufbau besteht aus:

- „iC5000 On-Chip Analyzer“, blaue Box
- “winIDEA”, iSYSTEM's Entwicklungsumgebung
- Laptop, mit üblicher Microsoft SW
- Evaluation / Target Board
- I/O Board

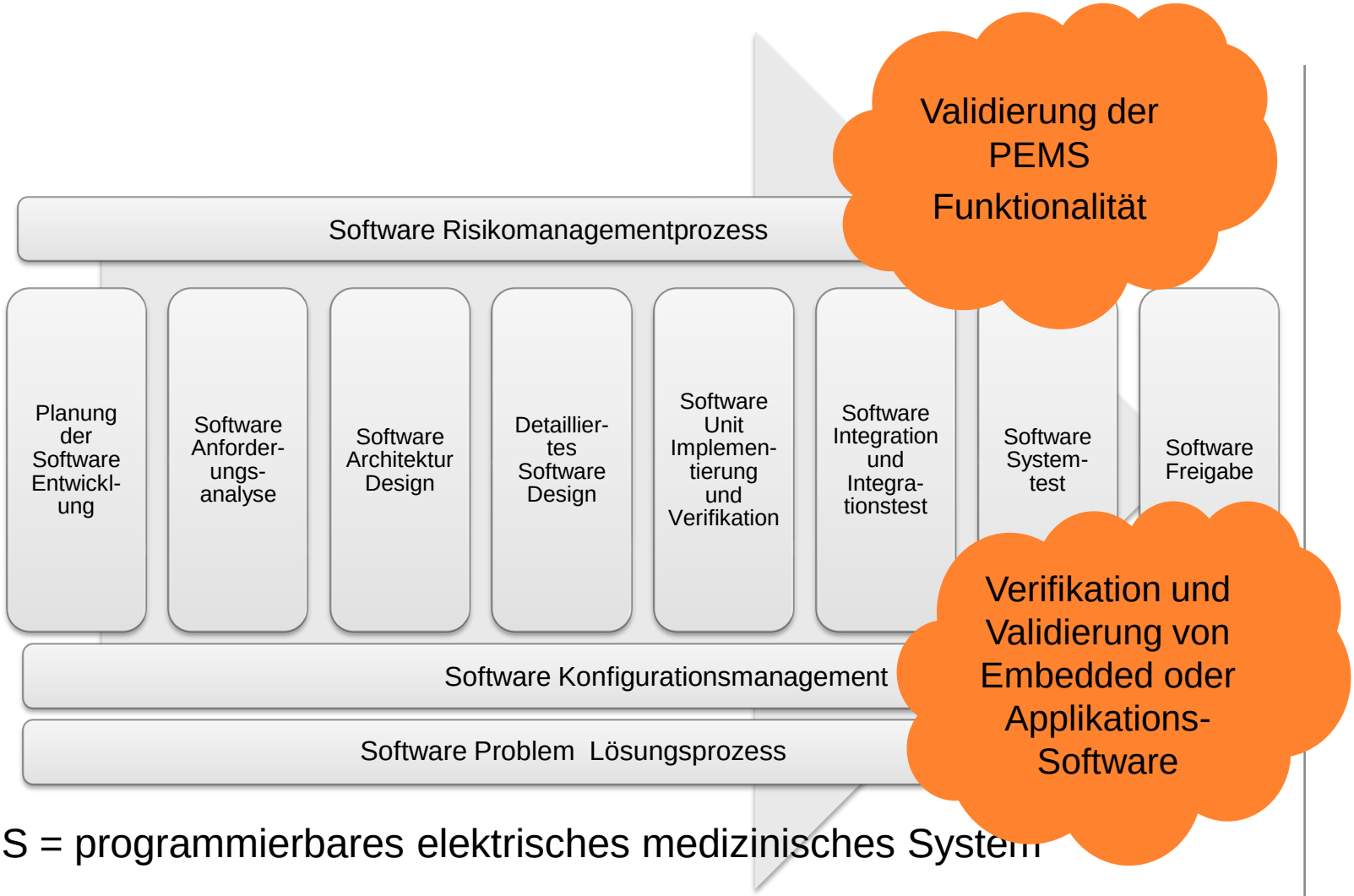
Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
- Fazit

Welche Tätigkeiten und Aufgaben werden von SW-Tools unterstützt?

Der gesamte Entwicklungsprozess kann toolunterstützt durchgeführt werden.

Welche Tätigkeiten und Aufgaben werden von Testsystemen unterstützt?



PEMS = programmierbares elektrisches medizinisches System

Software Tool / Testsystem

- Software Tools:
  - bestehen nur aus Software-Komponenten
  - Ablauffähig auf Standard-Hardware wie, z.B. PC oder Laptop
  - Verwendet in der Entwicklung von Hardware und Software, z.B. *MetaWare Developer Compiler*
- Testsysteme:
  - bestehen aus Hardware und Software Komponenten, z.B. *iC5000 On-Chip Analyzer + winIDEA*
  - können mit Software Tools kombiniert werden, aber unterscheiden sich von ihnen z.B. *GCC ARM Compiler*
- Standards zur Funktionalen Sicherheit stellen verschiedene Anforderungen an Testsysteme und Software Tools

Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
  - Testsysteme
  - Software-Tools
- Fazit

Allgemeine Anforderungen an Tools und Testsysteme

- Verhalten bzw. Ergebnis entspricht der Spezifikation
- Ergebnisse sind zuverlässig reproduzierbar
- Einfache verständliche Bedienoberfläche
- Einweisung in die Bedienung, falls notwendig
- Verständliches Handbuch
- Serviceverfügbarkeit
- Problem Management
- Dokumentation von Version, Konfigurationen, Anwendungsfällen und Ansprechpartnern

Testsysteme – Anforderungen aus dem Basis-Standard

- DIN EN IEC 61508-1:2011, Kapitel 7.14 Validierung der Gesamtsicherheit
  - 7.14.2.2 Alle für quantitative Messungen im Rahmen der Validierungstätigkeiten verwendeten Betriebsmittel müssen nach einer Spezifikation, die auf eine nationale Norm oder die Spezifikation des Herstellers rückführbar ist, kalibriert sein.
- DIN EN IEC 61508-2:2011, Kapitel 7.7 Validierung der Sicherheit des E/E/PE*-Systems
  - 7.7.2.2 Alle Prüfmesseinrichtungen, die für die Validierung verwendeten werden, müssen gegen eine Norm, die, falls vorhanden, auf eine nationale Norm rückführbar ist, oder nach einem weithin anerkannten Verfahren kalibriert werden. **Die gesamten Prüfeinrichtungen müssen in Bezug auf korrekten Betrieb verifiziert werden.**

* E/E/PE = elektrischen/elektronischen/programmierbar elektronischen

Testsysteme – Anforderungen aus dem Basis-Standard

- DIN EN IEC 61508-3:2011, Kapitel 7.7 Softwareaspekte bezüglich der Validierung der Sicherheit des Systems
  - 7.7.2.5 **Für jede Sicherheitsfunktion** muss die Validierung der Sicherheit der Software folgende Ergebnisse **dokumentieren**:
    …
    d) die verwendeten Werkzeuge und Ressourcen mit den Daten der Kalibrierung;
- DIN EN IEC 61508-3:2011, Kapitel 7.4.4 Anforderungen an Werkzeuge einschließlich Programmiersprachen
  - Folgende Eigenschaften der Werkzeuge sollten berücksichtigt werden:
    - der Umfang, in welchem die Werkzeuge die Erstellung der Software mit den notwendigen Softwareeigenschaften, unterstützen;
    - die Übersichtlichkeit der Bedienung und Funktionalität des Werkzeugs;
    - die Korrektheit und Wiederholbarkeit der Ergebnisse.

Testsysteme – Anforderungen aus ISO 13485:2003

- 7.6 Control of monitoring and measuring devices (see EN ISO 9001:2008) ...
  - Where necessary to ensure valid results, measuring equipment shall
    - a) be **calibrated or verified at specified intervals**, or prior to use, against measurement standards traceable to international or national measurement standards; where no such standards exist, the basis used for calibration or verification shall be recorded;

    ...
  - When used in the monitoring and measurement of specified requirements, **the ability of computer software to satisfy the intended application shall be confirmed. This shall be undertaken prior to initial use and reconfirmed as necessary.**

Testsysteme – Anforderungen aus ISO/TR 14969:2004

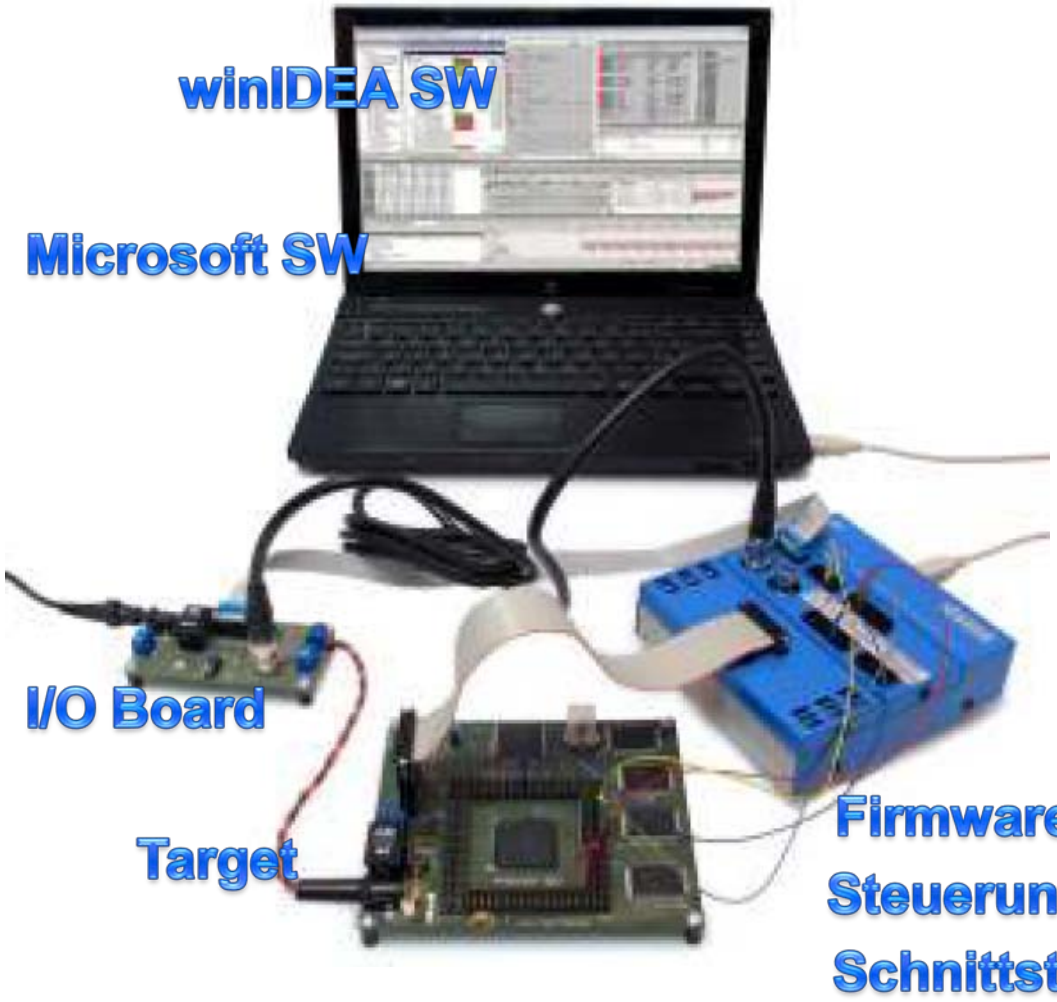
- 7.6.4 Software applications related to the control and/or calibration of monitoring and measuring devices should be validated. Examples include software used for
  - controlling the instrument calibration process,
  - determining the control or calibration status of instruments based on the data generated during the process, and
  - scheduling the calibration of equipment, if the scheduling is not backed up by a manual (e.g. calibration label or other system).
- NOTE Additional information regarding the management of monitoring and measuring equipment is available in ISO 10012.

Testsysteme – Anforderungen aus DIN EN ISO 10012:2004

6.2.2 Software

- Die in den Messprozessen und **bei der Berechnung der Ergebnisse eingesetzte Software muss**
  - **dokumentiert, gekennzeichnet und überwacht werden**, um ihre Eignung für den fortgesetzten Einsatz sicherzustellen.
- Die Software und sämtliche aktualisierten Versionen müssen
  - **vor dem ersten Einsatz geprüft und/oder validiert,**
  - **für den Einsatz freigegeben und archiviert** werden.
  - Die Prüfungen müssen in dem Umfang erfolgen, der für die Sicherstellung gültiger Messergebnisse erforderlich ist.

Beispiel Testaufbau - Testsystem „To Do List“



- Testsystem
  - Dokumentieren
  - Verifizieren, ggf. kalibrieren
  - Nachweisen, dass die SW für den Einsatz geeignet
  - Archivieren (Konfiguration Management)
- Und die weitere Entwicklungsumgebung, wie z.B. *GCC ARM Compiler ?* (Siehe Nächste Folien)

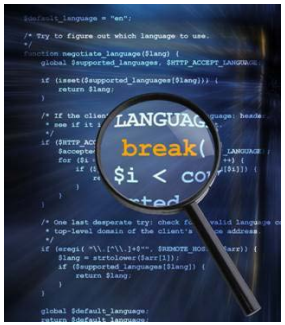
Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
  - Testsysteme
  - Software-Tools
- Fazit

Software Tools – Anforderungen aus DIN EN 60601-1:2013

- 14.10 Verifikation
  - Ein Verifizierungsplan muss erstellt werden. Der Plan muss unter anderem enthalten:
    - die Auswahl und die Anwendung von Verifizierungs-Werkzeugen
  - Die Ergebnisse der Aktivitäten müssen dokumentiert werden.
- 14.6.2 Risikobeherrschung
  - Für die Implementierung jeder Maßnahme der Risikobeherrschung müssen angemessen validierte Werkzeuge und Verfahren ausgewählt und festgelegt werden.

Software Tools – Anforderungen aus DIN EN 62304:2007



- 5.1.4 Planung von Normen, Methoden und Werkzeugen der Software-Entwicklung, ab Klasse C:
  - Werkzeuge in den Entwicklungsplan einschließen oder referenzieren
- 5.1.10 Zu kontrollierende unterstützende Komponenten:
  - Werkzeuge, Elemente oder Einstellungen, die zur Entwicklung benötigt werden und die das Endprodukt beeinflussen könnten. (Klasse B, C)
  - Beispiel: Version und Konfiguration des *GCC ARM Compilers*
- C.7 Beziehung zu IEC 61508:
  - Empfehlung: Für Techniken, Werkzeugen und Methoden für die Entwicklung von SW ist der IEC 61508 zu folgen.

Klassifizierung
Off- / ON-line Werkzeug

- IEC 61508-4:2010, 3.2.10 Online-Software-Werkzeug :
  - Softwarewerkzeug, das das sicherheitsbezogene System während seiner Laufzeit direkt beeinflussen kann.
- IEC 61508-3:2010, 7.4.4.1:
  - Ein Online-Software-Werkzeug muss als ein Softwareelement des sicherheitsbezogenen Systems angesehen werden.
- IEC 61508-4:2010, 3.2.11 Offline-Software-Werkzeug :
  - Softwarewerkzeug, das eine Phase des Software-Entwicklungslebenszyklus unterstützt und nicht das sicherheitsbezogene System während seiner Laufzeit direkt beeinflussen kann.

Klassifizierung
Off-line Tool Klassen
nach IEC 61508:2010

- Klasse T1 Tools tragen nicht zum ausführbaren Code bei und unterstützen nicht bei der Verifikation, z.B. Texteditoren.
- Klasse T2 Tools unterstützen die Prüfung oder Verifikation des Entwurfs oder ausführbaren Codes, z.B. Tool zur statischen Codeanalyse.
- Klasse T3 Tools erzeugen Ausgaben, die direkt oder indirekt zum ausführbaren Code beitragen, z.B. optimierender Compiler.

Tool Qualifikation Schritt 1

- Tool Klassifizierung ergab T2 oder T3
- Tool hat bekannte Fehler „ List of known issues”
  - Maßnahme: In den Tool-Anwendungsrichtlinien diese gefährlichen “Funktionen” verbieten.
- Tool Fehler, die während des Betriebs auftreten dokumentieren, einschließlich deren Sicherheitsrelevanz
  - Maßnahme: Sammeln dieser Felddaten erlaubt den Aufbau einer „Proven-In-Use“ Argumentation

Tool Qualifikation Schritt 2

- Tool Klassifizierung ergab (T2 oder)T3
- Neue Tool Version soll eingesetzt werden
  - Maßnahme: Validierung der spezifizierten Funktionen gegenüber der vorhandenen Implementierung (d.h. Abnahmetest)
  - Maßnahme: Sammeln der bisherigen Anwendungsfälle (firmen intern / extern), um eine „Proven-In-Use“ Argumentation aufzubauen.
- Eine Tool Validierung muss, wie in IEC 61508-3:2010, 7.4.4.7, gefordert, dokumentiert werden.

Tool Qualifikation Schritt 3

- Tool Klassifizierung ergab (T2 oder)T3
- Im Fall, dass die Validierung, den Anwendern nicht ausreichend erscheint:
  - <u>Maßnahme:</u>
  - Im Entwicklungsprozess das Ergebnis der Tool Anwendung nochmals überprüfen oder
  - parallel dazu ein zweites vom ersten verschiedenes Tool verwenden.

Agenda

- Motivation
- Unterschiede Testsysteme und Software Tools
- Anforderungen
- Fazit

Fazit

- Eine Unterscheidung von reinem Software-Tool und Testsystem ist sinnvoll.
- Ein Testsystem benötigt keine Toolqualifikation, aber eine Verifikation / Validierung vor der Verwendung ist notwendig. Bei messenden Testsystemen ist zusätzlich eine Kalibrierung durchzuführen.
- Eine Toolklassifikation bzw. -qualifikation ist in anderen Branchen Stand der Technik.
- Software – Tools müssen dokumentiert und validiert werden.

Danke für Ihre Aufmerksamkeit!

Ihr Dienstleister im Bereich Funktionale Sicherheit

SGS-TÜV Saar GmbH

Funktionale Sicherheit

Hofmannstrasse 50

D-81379 Muenchen

Germany

www.sgs-tuev-saar.com/fs

Gudrun Neumann

Product Manager Functional Safety Software

Industrial Functional Safety Expert IFSE

Automotive Functional Safety Expert AFSE

E-Mail: gudrun.neumann@sgs.com

Telefon: +49 89 787 475 -216

Fax: +49 89 787 475 -217