



Tool Qualifikation – Schreckgespenst der Testautomatisierung?

HEICON Global Engineering
Kreuzweg 22, 88477 Schwendi

Internet: www.heicon-ulm.de
Blog: <http://blog.heicon-ulm.de>





HEICON ist ein auf Beratung und Entwicklungsbegleitung spezialisiertes Unternehmen, mit Fokussierung auf softwaregetriebene Embedded Systeme.

Der Einsatz von Methoden- und Prozessen bildet hierbei den Schwerpunkt des Engagements.

Gründung: 2005

Standort:

Schwendi bei Ulm

Mitarbeiter: 3

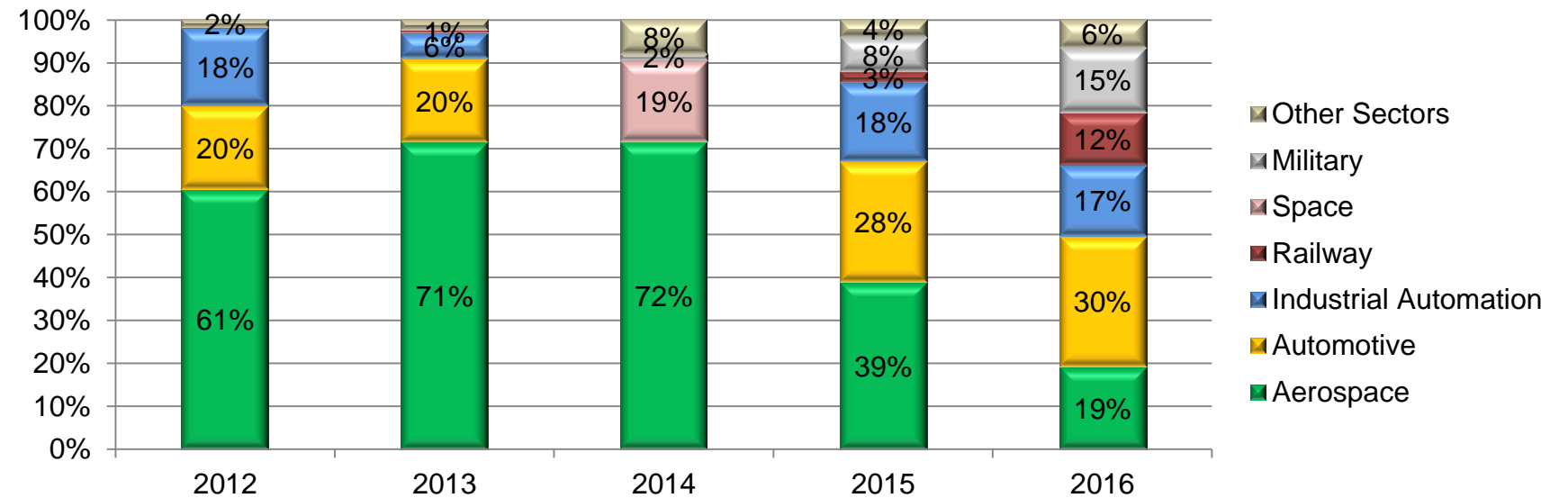
Rechtsform:

Einzelunternehmen

Mitglied:



Umsatzverteilung auf Branchen:





Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen

Was ist eine Tool Qualifikation?



Eine Toolqualifikation ist der Nachweis, durch Einsatz geeigneter Maßnahmen, das ein ausgewähltes Tool welches während der Entwicklung eines Funktionalen Sicherheitsproduktes zum Einsatz kommt korrekt funktioniert.





Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen



Wann wird eine Tool Qualifikation benötigt?

4-Augen-Prinzip

- ✓ Findet in weiten Teilen eines FuSi Entwicklungsprozesses Anwendung
- ✓ Im Bereich der Tools bedeutet dies, dass man nicht ohne weiteres davon ausgehen kann das ein Tool korrekt arbeitet.
- ✓ Eine Toolqualifikation wird benötigt, wenn ein Prozess des FuSi Standard durch ein Tool ersetzt (automatisiert) wird
(= Verletzung des 4-Augen-Prinzips)

2 denkbare Fehlerkategorien

- ✓ **Fehler** in einem sicherheitsrelevanten System werden **nicht erkannt** (Beispiel: Verifikationstools wie Prüfung der Codierrichtlinien, Unittesttools)
- ✓ **Fehler** werden in das sicherheitsrelevante System **einggebracht** (Beispiel: Compiler)





Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen



DO 178C bzw. DO 330: Bestimmung des Tool-Qualifikationslevel

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5



Criteria 1: Ein Tool dessen Output Fehler in die sicherheitsrelevante SW einbringen kann.

Criteria 2: Ein Tool welches einen Fehler in der sicherheitsrelevante SW nicht findet und dessen Ergebnisse für darüber hinausgehende Begründungen zur Korrektheit des SW-Entwicklungsprozesses verwendet werden

Criteria 3: Ein Tool welches einen Fehler in der sicherheits-relevanten SW nicht findet.

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen



TQL-5 Tools

Erstellung von Tool operational requirements und Nachweis
Deren Erfüllung durch Tests

TQL-1 bis 4 Tools

Nachweis das Tool gemäß DAL A bis D entwickelt wurde!



Kriterien zur Auswahl der Tool Qualifikation Maßnahmen



ISO 26262: Bestimmung des „tool confidence level“ (TCL)

		Tool error detection		
		TD1	TD2	TD3
Tool impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

Tabelle 3, ISO 26262-8



TI1: Toolfehlfunktion fügt keinen Fehler in ein sicherheitsrelevantes Item ein und es wird auch nicht verhindert einen Fehler in einem Item zu entdecken

TI2: Wenn TI1 nicht zutrifft

TD1: Großes Vertrauen, dass eine Fehlfunktion verhindert oder entdeckt wird

TD2: Mittleres Vertrauen, dass eine Fehlfunktion verhindert oder entdeckt wird

TD3: Wenn TD1 und TD2 nicht zutrifft

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen



ISO 26262: Qualifikation von Software tools (TCL 3)

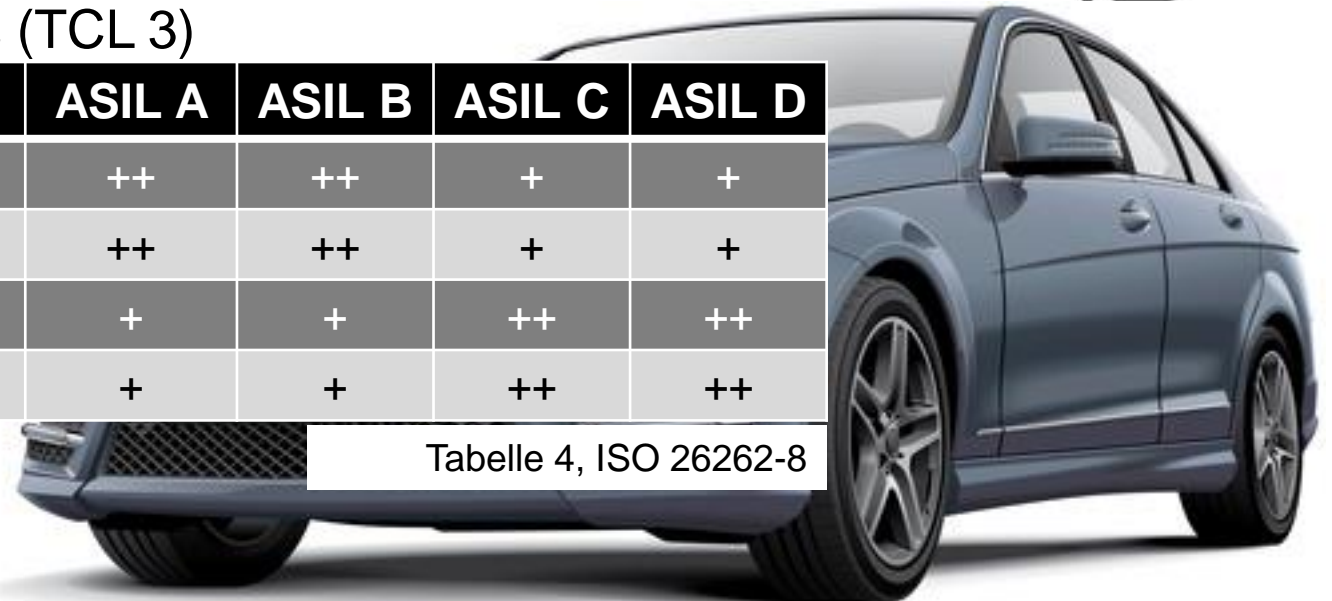
Methoden	ASIL A	ASIL B	ASIL C	ASIL D
Increased confidence from use	++	++	+	+
Evaluation of the tool development process	++	++	+	+
Validation of the software tool	+	+	++	++
Development in accordance with a safety standard	+	+	++	++

Tabelle 4, ISO 26262-8

ISO 26262: Qualifikation von Software tools (TCL 2)

Methoden	ASIL A	ASIL B	ASIL C	ASIL D
Increased confidence from use	++	++	++	+
Evaluation of the tool development process	++	++	++	+
Validation of the software tool	+	+	+	++
Development in accordance with a safety standard	+	+	+	++

Tabelle 5, ISO 26262-8





Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen



Maßnahme 1: Betriebsbewährt

Voraussetzung zur Anwendung der Maßnahme:

- ✓ Tool ist bereits langjährig auf dem Markt
- ✓ Daten über aufgetretene Fehler sind zugänglich
- ✓ Daten sind für den Anwendungsfall passend

Erfahrungen aus der Praxis mit dieser Maßnahme:

- ✓ In der Luftfahrt wird die Maßnahme sehr kritisch gesehen
- ✓ In der Vergangenheit wurde die Maßnahme schon oft angewendet ohne dass die Voraussetzungen wirklich erfüllt waren





Maßnahme 2: Assessment des Entwicklungsprozesses des Tools

Voraussetzung zur Anwendung der Maßnahme:

- ✓ Ein anerkanntes Zertifikat liegt vor

Erfahrungen aus der Praxis mit dieser Maßnahme

- ✓ Luftfahrt: Keine Anerkennung der Maßnahme
- ✓ Automobilbranche: Maßnahme wird oft kritisch gesehen
- ✓ Schwäche der Maßnahme ist, dass die Funktionsfähigkeit des Tool nicht im realen Einsatz nachgewiesen wird
- ✓ Vorteil für Industrieweit, langjährig eingesetzte Tools





Maßnahme 3: Test der Funktionalität des Tools

Erfahrungen aus der Praxis mit dieser Maßnahme

- ✓ Die bekannteste Toolqualifikationsmaßnahme
- ✓ Aufwand liegt in der Erstellung der Tests, nicht deren Durchführung
- ✓ Tests sollten immer in der Umgebung durchgeführt werden, in der auch das Tool eingesetzt wird
- ✓ Viele professionelle Toolhersteller bieten Qualifikationspakete an
- ✓ Maßnahme hat das Beste Kosten/Nutzenverhältnis



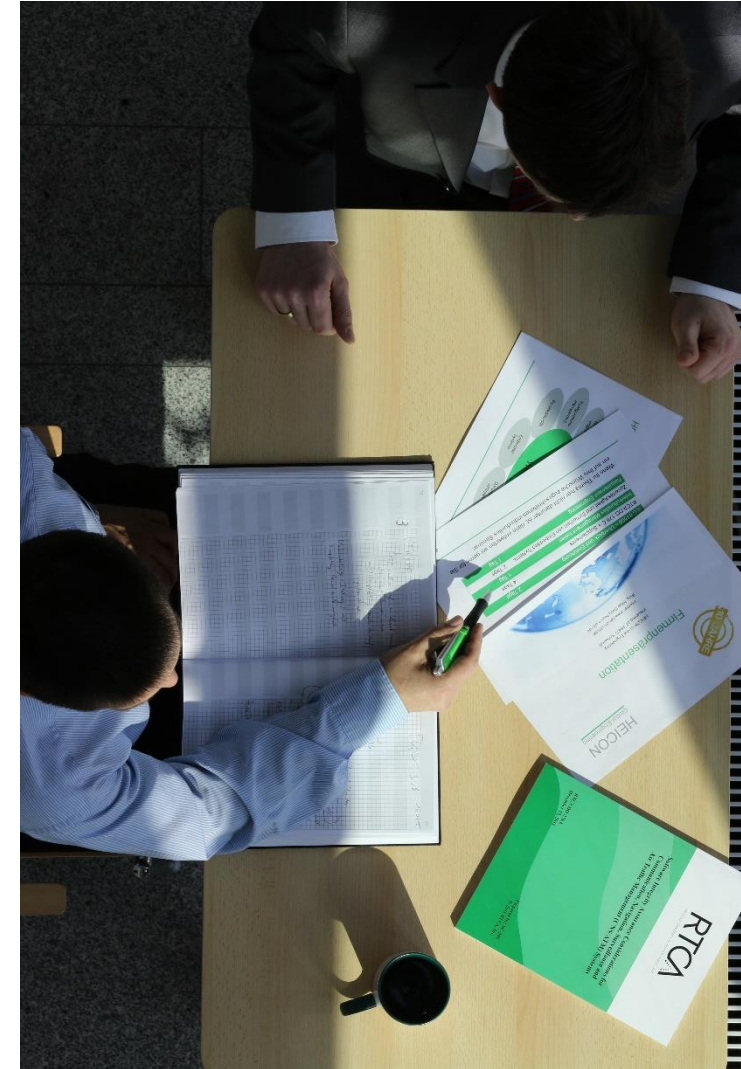
Bewertung der Tool Qualifikation Maßnahmen



Maßnahme 4: Entwicklung des Tools nach einem Standard der Funktionalen Sicherheit

Erfahrungen aus der Praxis mit dieser Maßnahme

- ✓ Maßnahme bietet aber den größten Nutzen
- ✓ Sehr aufwendig und aus Sicht der Sicherheit, beste Maßnahme
- ✓ Von kommerziellen Herstellern in nur sehr seltenen Fällen angewendet





Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen



Luftfahrt

- ✓ Häufigste Maßnahme: Test der Funktionalität
- ✓ Die Betriebsbewährtheit und das Assessment des Tool-Entwicklungsprozesses haben keine Akzeptanz
- ✓ Die Entwicklung des Tools nach DO 178 wird praktisch (fast) nur auf nicht kommerzielle Spezialanwendungen angewendet.





Auto

- ✓ Häufigste Maßnahme: Assessment des Tool-Entwicklungsprozesses
- ✓ Die Betriebsbewährtheit wird bei schlüssiger Begründung akzeptiert
- ✓ Der Test der Funktionalität stößt bei vielen immer noch auf größere Vorbehalte
- ✓ Die Entwicklung des Tools nach einem FuSi Standard findet praktisch kaum Anwendung

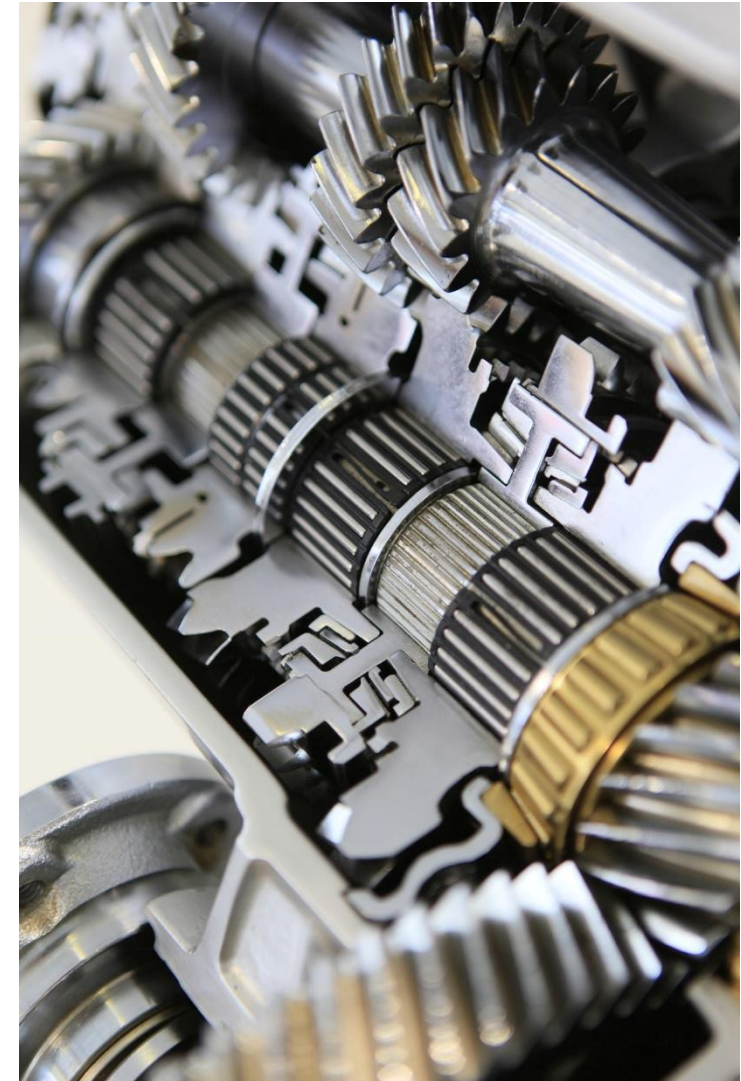


Branchen und Tool Qualifikation Maßnahmen



Industriearomatisierung

- ✓ Häufigste Maßnahmen: Assessment des Tool-Entwicklungsprozesses und Betriebsbewährtheit
- ✓ Der Test der Funktionalität kommt (nur) bei hohen SIL Leveln zum Einsatz
- ✓ Die Entwicklung des Tools nach einen FuSi Standard findet praktisch kaum Anwendung



Branchen und Tool Qualifikation Maßnahmen



Maßnahme	Luftfahrt	Auto	Industrie
Daten aus historischem Einsatz des Tools	o	+	++
Assessment des Entwicklungsprozesses des Tools	o	+	++
Test der Funktionalität des Tools	++	+	+
Entwicklung des Tools nach einem FuSi Standard	+	o	o



Was ist eine Tool Qualifikation?

Wann wird eine Tool Qualifikation benötigt?

Kriterien zur Auswahl der Tool Qualifikation Maßnahmen

Bewertung der Tool Qualifikation Maßnahmen

Branchen und Tool Qualifikation Maßnahmen

Fazit und Empfehlungen



1. Eine Toolqualifikation wird NUR benötigt, wenn ein Prozess des FuSi Standard durch ein Tool ersetzt (automatisiert) wird (= Verletzung des 4-Augen Prinzips)
2. Tools können Fehler in der sicherheitsrelevanten Software nicht entdecken
3. Tools können Fehler in die sicherheitsrelevante Software einbringen

Verständnis über die genannten Punkte ist noch nicht ausreichend in der Industrie verbreitet

- Falsches Verständnis welche Tools überhaupt qualifiziert werden müssen
- Für 60% bis 80% der in der Entwicklung eingesetzten Tools muss in der Regel gar keine Toolqualifikation durchgeführt werden
- Falsche Einschätzung der Aufwände
- Der Test der Funktionalität des Tools ist die mit Abstand beste Maßnahme im Sinne des Kosten/Nutzen Aufwandes, Allerdings sollten die Tests in der realen Umgebung durchgeführt werden
- Nur in seltenen Fällen ist es notwendig ein Tool gemäß eines FuSi Standards zu entwickeln



Die Toolqualifikation
einzelner Tools
ist kein Argument gegen die
Automatisierung von Tests

Kontakt – Veröffentlichungen



Kontaktdaten:

Martin Heininger Dipl.-Ing(FH)

Kreuzweg 22

88477 Schwendi

Tel.: 07353 / 98 17 81

Mobil: 0176 / 24 73 99 60

martin.heininger@heicon-ulm.de

<http://www.heicon-ulm.de>

Veröffentlichungen:

Leistungselektronik nach ISO26262 prüfen, ATZ 04/15

Monatlich: Blogbeiträge zu Themen der Funktionalen

Sicherheit: <http://blog.heicon-ulm.de>