ISO 26262 -
Exemplary Tool Classification of Model-Based Design Tools

30.06.2011

Mirko Conrad The MathWorks, Inc., Natick, USA
mirko.conrad@mathworks.com

Ines Fey samoconsult GmbH, Berlin, Germany
ines.fey@samoconsult.de

- **Software-Toolqualifizierung nach ISO 26262**
- **Qualifizierung von COTS Tools**
- **Tool Klassifizierung am Beispiel des Model Advisor**
  - **Applikationsunabhängige Klassifizierung und Pre-Qualifizierung**
  - **Applikationsspezifische Klassifizierung und Qualifizierung**

- ISO 26262-1
- ISO 26262-2
- ISO 26262-3
- ISO 26262-4
- ISO 26262-5
- ISO 26262-6
- ISO 26262-7
- ISO 26262-8
- ISO 26262-9
- ISO 26262-10

DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-8

ISO/TC 22/SC 3 Secretariat: DIN

Voting begins on: 2009-01-08 Voting terminates on: 2009-12-08

Road vehicles — Functional safety —
Part 8:
Supporting processes

Véhicules routiers — Sécurité fonctionnelle —
Partie 8: Processus d'appui

ICS: 43.080.10

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Copyright notice
This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.
Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

© International Organization for Standardization 2009

Chapter 11: Confidence in the use of software tools

Software-Toolqualifizierung nach ISO 26262
Safety · Modeling · Consulting

A software tool can support or enable tailoring of the safety-lifecycle, through tailoring of activities and tasks required by ISO 26262.

In such cases **confidence** is needed, **that the software tool effectively achieves the following goals**:

- To minimize the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs
- To ensure adequateness of the development process w.r.t. compliance with ISO 26262, if activities or tasks required by ISO 26262 rely on the correct functioning of the software tool.

ISO 26262-8, BL16, June 2010

Objectives

To provide

- **Criteria to determine the required level of confidence** in a software tool
- **Means for the qualification of a software tool** (when applicable), in order to create evidence that the tool is suitable to be used to tailor activities or tasks required by ISO 26262 (i.e. the user can rely on the correct functioning of a software tool for those activities or tasks required by ISO 26262).

ISO 26262-8, BL16, June 2010

Software-Toolqualifizierung nach ISO 26262
Safety · Modeling · Consulting

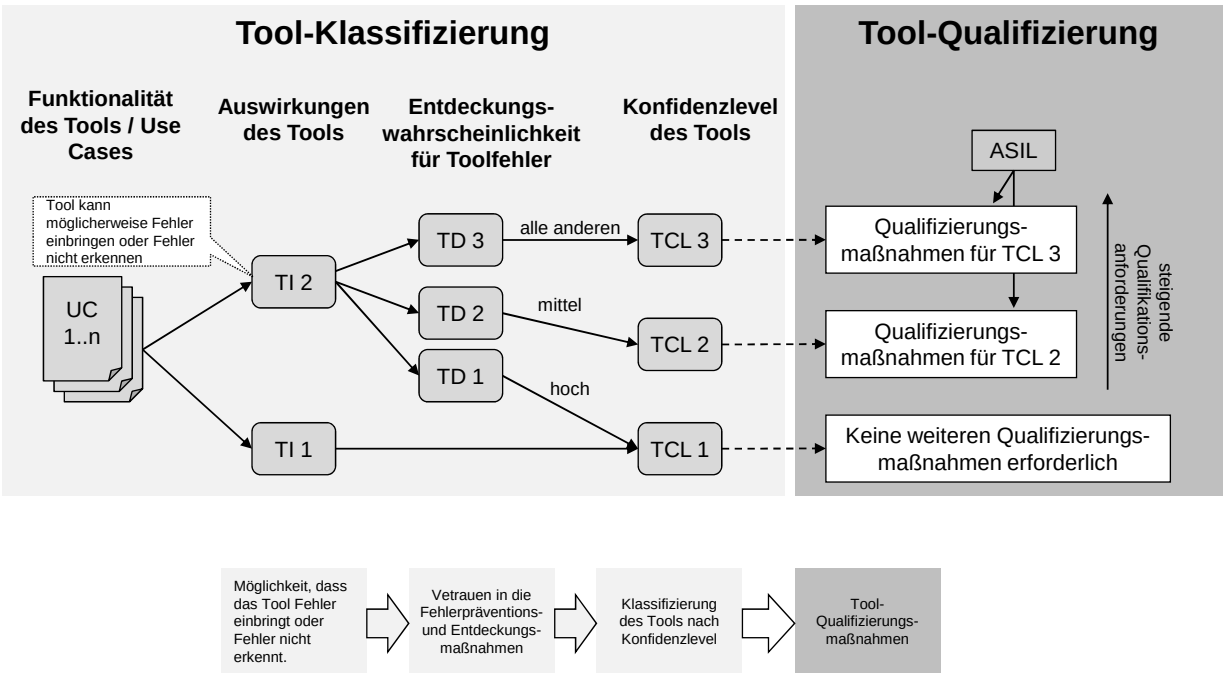
Criteria to determine the required level of confidence in a software tool

- The **possibility that the malfunctioning** software **tool and its** corresponding erroneous **output can introduce or fail to detect errors** in a safety-related item / element being developed
- The **confidence in preventing or detecting such errors** in its corresponding output

To evaluate the confidence in prevention or detection measures, **measures internal to the software tool** (e.g. monitoring) as well as **measures external to the software tool** (e.g. guidelines, tests, reviews) implemented in the development process may be considered and can be assessed.

ISO 26262-8, BL16, June 2010

Software-Toolqualifizierung nach ISO 26262



Qualifizierung von COTS-Software-Tools

- ISO 26262-8 legt fest, dass Software-Tools durch den Tool-Benutzer zu klassifizieren und ggf. zu qualifizieren sind.
- Die Aufteilung der Arbeit zwischen Tool-Lieferant und Tool-Benutzer unterstützt eine **angemessene** und **effiziente Qualifizierung** von COTS-Tools.

Effiziente Tool-Qualifizierung durch Vorarbeit des Tool-Lieferanten

- Tool-Lieferant
  - vorläufige Qualifizierung (bezogen auf die Referenz-Anwendungsfälle und -Workflows)
  - Artefakte der vorläufigen Qualifizierung
  - vorbefüllte Templates von Artefakten
- Tool-Benutzer
  - verantwortlich für die Tool-Abschlussqualifizierung im Kontext der Applikation

⇨ **Zweistufiges Vorgehen**

Software-Toolqualifizierung von COTS Tools
Safety · Modeling · Consulting

I. Applikationsunabhängige vorläufige Qualifizierung

A. Allgemeine Tool-Klassifizierung [Tool-Lieferant]

B. Allgemeine vorläufige Qualifizierung bis zum maximal erforderlichen TCL [Tool-Lieferant]

C. Unabhängige Bewertung der Tool-Klassifizierung und vorläufigen Qualifizierung [Externe Organisation]

⇨ **ISO 26262-Tool-Qualifizierungskit**

- Allgemeine Tool-Qualifizierungsartefakte (vorausgefüllte Vorlagen)
- Bewertungsreport, Zerifikat (optional)

II. Applikationsspezifische Anpassung

A. Review / Anpassung des Tool-Qualifizierungskits [Tool-Benutzer]

⇨ **ISO 26262-Tool-Qualifizierungsdokumentation**

- Tool-Qualifizierungartefakte
- Bewertungsreport, Zerifikat (optional)

Eine Voraussetzung der Tool-Klassifizierung ist die Beschreibung der Ein- und Ausgaben des Tools.

Beispiel:

Der Model Advisor benutzt die Inputs und erzeugt die Outputs, wie hier aufgelistet:

- Tool Input
  - das zu analysierende Simulink Modell
  - Konfiguration und Auswahl der Prüfkriterien/Checks
  - Eingabeparameter [nur bestimmte Checks]
- Tool Output
  - Ergebnis der Analyse mit Hyperlinks in das Simulink Modell (Model Advisor check report)
  - Korrigiertes Modell [nur bestimmte Checks]

Model Advisor: Applikationsunabhängige Klassifizierung
Safety · Modeling · Consulting

Der zweite Schritt der Tool-Klassifizierung ist die Bestimmung der Use Cases.

[UC1]	Untersuchung von Simulink Modellen auf Korrektheit der Einhaltung spezifizierter Modellierungsrichtlinien
[UC2]	Automatische Korrektur der im Report gemeldeten Fehler

Der nächste Schritt der Tool-Klassifizierung ist die Bestimmung potentieller Fehlfunktionen oder fehlerhafter Ausgaben.

(E1) *False negative:* Prüfungsergebnis der Modellierungsrichtlinien wird irrtümlich als korrekt statt inkorrekt gekennzeichnet.

(E2) *False positiv:* Prüfungsergebnis der Modellierungsrichtlinien wird irrtümlich als inkorrekt statt korrekt gekennzeichnet.

(E3) *Einflussfreiheit:* Prüfung der Modellierungsrichtlinien beinhaltet Fehler, aber die fehlerhafte Funktionalität wird durch das Modell nicht aktiviert.

(E4) *Inkorrekte Hyperlinks:* Hyperlinks im erzeugten Report beinhalten Fehler.

(E5) *Fehlerhafte Auto-Korrektur:* Automatische Korrekturfunktion des Checks arbeitet fehlerhaft.

Model Advisor: Applikationsunabhängige Klassifizierung
Safety · Modeling · Consulting

ID	Potential malfunction or erroneous output	Use case	TI	Justification for TI	Measure(s) to prevent or detect error in tool output	TD	Justification for TD	TCL
E5	Incorrect fixing of reported issues: Automatic fixing of reported issues does not work correctly	UC2	TI2	Incorrect fixing could introduce error in the model	Re –checking of the model after automatic fixing of reported issues	TD2	Re –checking of the model will detect modeling standard violations introduced by the automatic fixing but might miss other errors introduced	TCL2
					[illegible]	[illegible]	[illegible]	[illegible]2
					Simulink models and subsequent manual review of the comparison results		changes resulted did not introduce un-intended changes	[illegible]1

Die folgenden Schritte der Tool-Klassifizierung

- Bestimmung der Entdeckungswahrscheinlichkeit für Toolfehler (TD)
- Bestimmung des Konfidenzlevel des Tools (TCL)

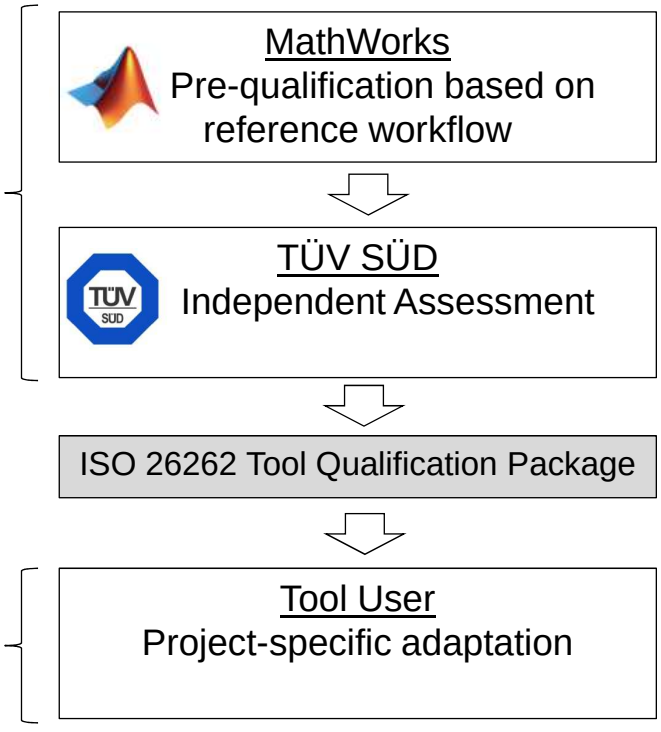
ergeben eine Tabelle mit applikationsunabhängiger Toolklassifizierung.

ID	Potential malfunction or erroneous output	Use case	TI	Justification for TI	Measure(s) to prevent or detect error in tool output	TD	Justification for TD	TCL
E5	Incorrect fixing of reported issues: Automatic fixing of reported issues does not work correctly	UC2	TI2	Incorrect fixing could introduce error in the model	Re –checking of the model after automatic fixing of reported issues	TD2	Re –checking of the model will detect modeling standard violations introduced by the automatic fixing but might miss other errors introduced	TCL2
								TCL2
					comparison results			TCL1

Die applikationsunabhängige Tool-Klassifizierung ergibt einen maximalen TCL von TCL2.

- Der ModelAdvisor muss entsprechend nach TCL2 qualifiziert werden.
- Eine Möglichkeit der Qualifizierung bietet eine Validierungs-Testsuite, mit der die Standard-Checks für Modellierungsrichtlinien validiert werden können.

Applikationsunabhängige Klassifizierung und Pre-Qualifizierung



Applikationsspezifische Klassifizierung und Qualifizierung

cf. M. Conrad, J. Sauler, P. Munier: EXPERIENCE REPORT: TWO-STAGE QUALIFICATION OF SOFTWARE TOOLS 2. EUROFORUM Conference ISO 26262, Stuttgart, Germany, 2010

ID	Potential malfunction or erroneous output	Use case	TI	Justification for TI	Measure(s) to prevent or detect error in tool output	TD	Justification for TD	TCL
E5	Incorrect fixing of reported issues: Automatic fixing of reported issues does not work correctly	UC2	TI2	Incorrect fixing could introduce error in the model	Re –checking of the model after automatic fixing of reported issues	TD2	Re –checking of the model will detect modeling standard violations introduced by the automatic fixing but might miss other errors introduced	TCL2

Die Dokumente des Toolherstellers zur Toolklassifizierung und Pre-Qualifizierung sind die Basis für die Klassifizierung und Qualifizierung durch den Benutzer.

- Review der Dokumente
- Identifizierung der im Kontext der Applikation relevanten Use Cases, potentieller Fehler und Fehleraufdeckungsmöglichkeiten
- Entfernen der nicht-relevanten Teile

Model Advisor: Applikationsspezifische Klassifizierung

Safety · Modeling · Consulting

ID	Potential malfunction or erroneous output	Use case	TI	Justification for TI	Measure(s) to prevent or detect error in tool output	TD	Justification for TD	TCL
E5	Incorrect fixing of reported issues: Automatic fixing of reported issues does not work correctly	UC2	TI2	Incorrect fixing could introduce error in the model	Re –checking of the model after automatic fixing of reported issues	TD2	Re –checking of the model will detect modeling standard violations introduced by the automatic fixing but might miss other errors introduced	TCL2
					Subsequent dynamic verification (testing) of the model	TD2	Functional or structural testing help detect real errors in the model. The likelihood of detecting these errors by testing is considered to be ‚medium'.	TCL2
					Automatic comparison of XML files exported from the original and fixed Simulink models and subsequent manual review of the comparison results	TD1	Manual review of the comparison results can verify that fixing of changes resulted did not introduce un-intended changes	TCL1

ID	Potential malfunction or erroneous output	Use case	TI	Justification for TI	Measure(s) to prevent or detect error in tool output	TD	Justification for TD	TCL
E5	Incorrect fixing of reported issues: Automatic fixing of reported issues does not work correctly	UC2	TI2	Incorrect fixing could introduce error in the model	Re –checking of the model after automatic fixing of reported issues	TD2	Re –checking of the model will detect modeling standard violations introduced by the automatic fixing but might miss other errors introduced	TCL2

Die applikationsabhängige Tool-Klassifizierung ergibt einen maximalen TCL von TCL2.

- Unter Nutzung der Pre-Qualifizierung des ModelAdvisor muss der Benutzer keine weiteren Maßnahmen definieren, da der maximale TCL der Pre-Qualifizierung entspricht.
- Werden zusätzlich selbstdefinierte ModelAdvisor Checks verwendet, müssen diese jedoch separat betrachtet werden und ggf. die Validierungs-Suite ergänzt werden.

- ISO 26262 stellt eine Framework zur Klassifizierung von Software-Tools bereit
- Die Klassifizierung muss für jedes zu betrachtende Software-Tool durchgeführt werden
- Klassifizierung und Pre-Qualifizierung für COTS-Tools kann vom Tool-Hersteller durchgeführt werden
- Der Aufwand für den Tool-Nutzer bei der Qualifizierung von COTS-Tools kann dadurch signifikant verringert werden