Embedded Success dSPACE

BTC Embedded Systems

Sichere Software durch qualifizierte Werkzeuge und normgerechtes Entwicklungsvorgehen

Michael Beine · dSPACE GmbH

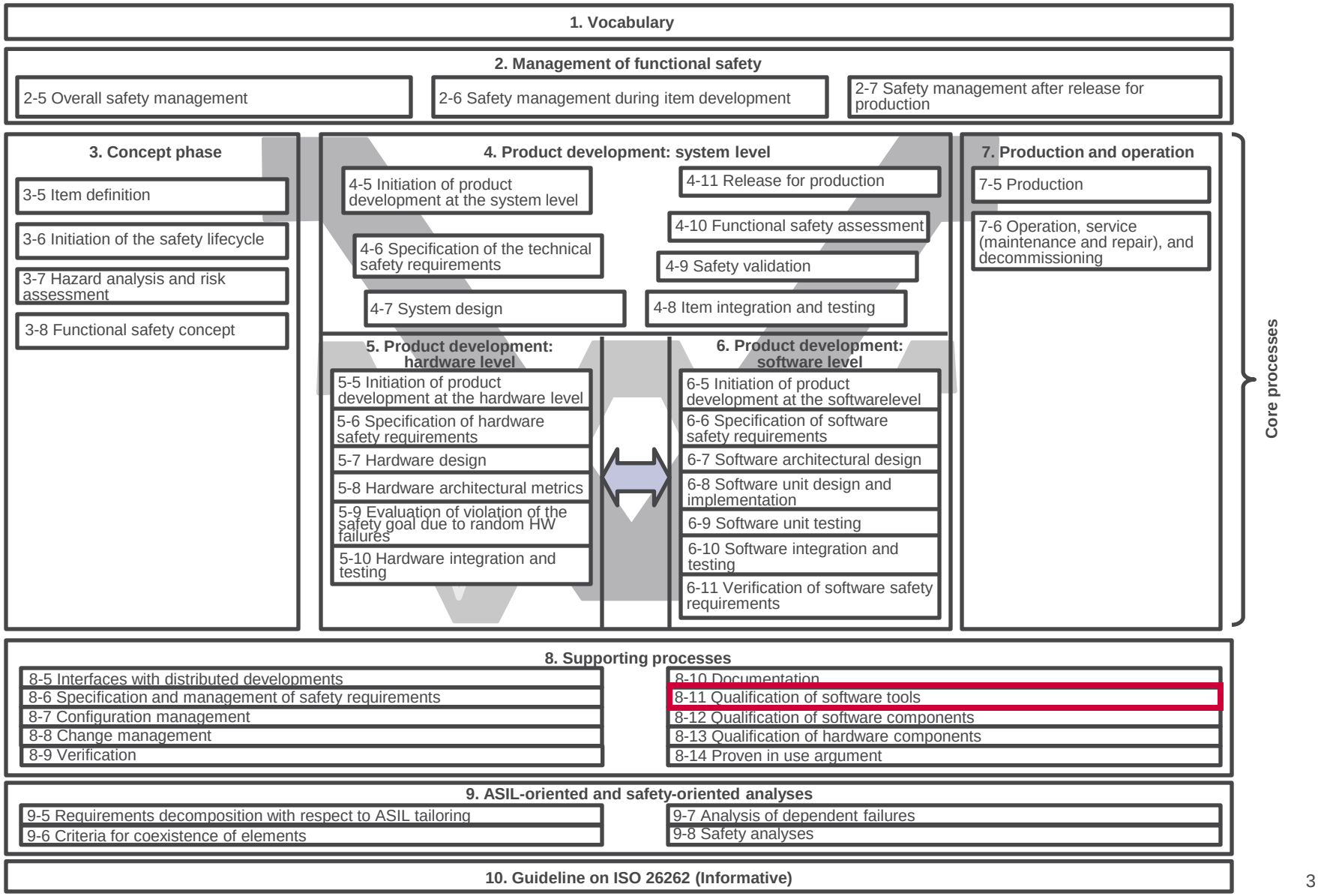
Dr. Udo Brockmeyer · BTC Embedded Systems AG

Automotive Conference · June 2010 · Stuttgart

ISO 26262 – New Automotive Safety-Standard

- New Automotive Standard addressing Functional Safety
  - Derived from IEC 61508:
    - “ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles.”
- Draft International Standard (DIS) published in July 2009
- Official release planned for 2011
- But already used by OEMs and suppliers

ISO 26262 – Überblick

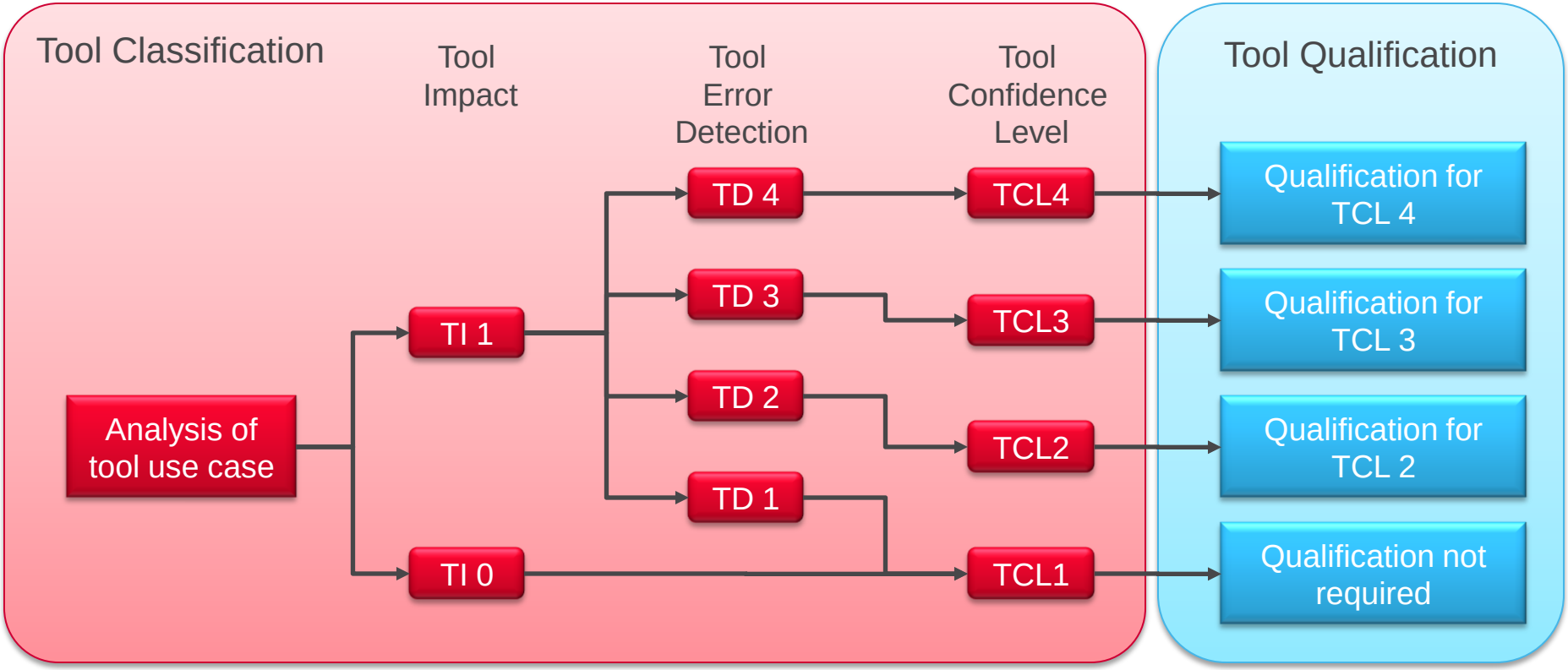


Software Tool Qualification – ISO 26262

11.4.4 Qualification of a software tool

11.4.4.1 A software tool classified at TCL1 needs no qualification measures..

11.4.4.2 To demonstrate that a software tool classified at TCL2, TCL3 or TCL4 fulfils its use cases with the required level of confidence, methods for the qualification of software tools as listed in Table 2, Table 3 and Table 4 shall be applied.



ISO 26262 – Qualification Measures and Methods

dSPACE

Table 4 — Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use	++	++	++	++
1b	Evaluation of the development process	++	++	++	++
1c	Validation of the software tool	+	+	+	+
1d	Development in compliance with a safety standard[a]	+	+	+	+

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

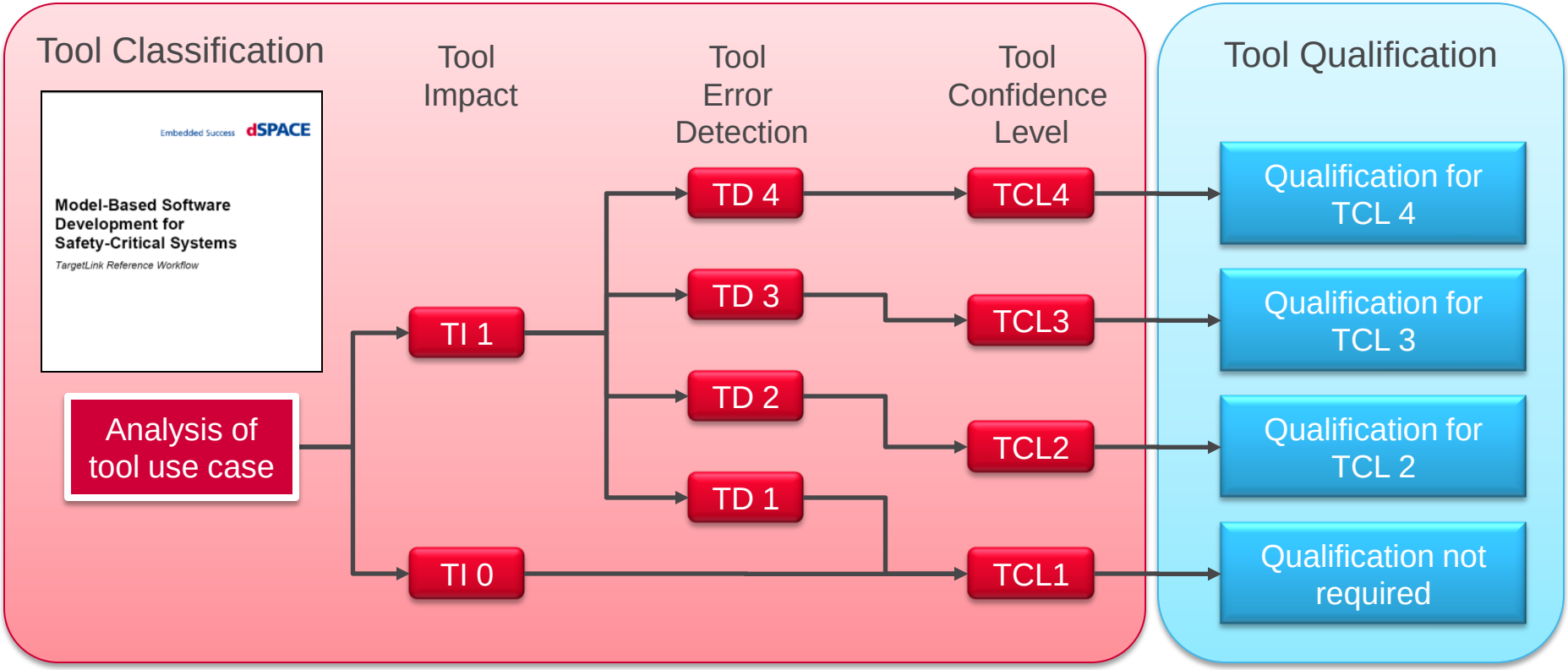
Table 3 —Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use	++	++	++	+
1b	Evaluation of the development process	++	++	++	++
1c	Validation of the software tool	+	+	+	++
1d	Development in compliance with a safety standard[a]	+	+	+	++

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

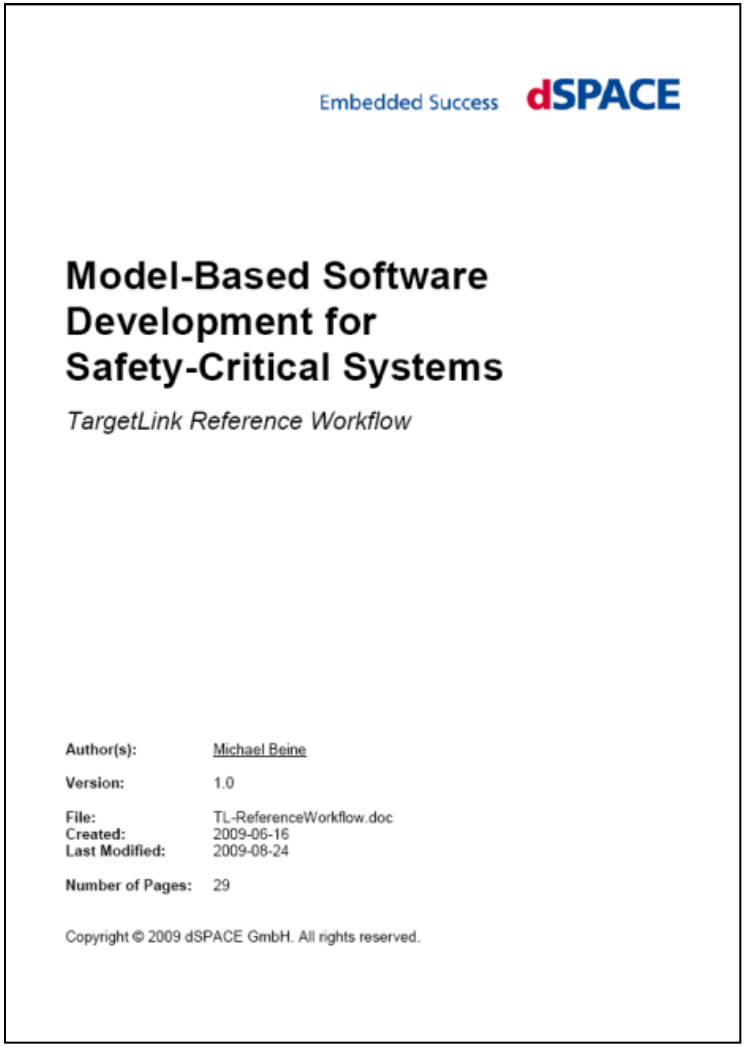
Code Generator Qualification for ISO 26262

- Tool Confidence Level (TCL): defines need for qualification and appropriate measures
  - TCL determination based on Reference Workflow



TargetLink Reference Workflow

- TargetLink Reference Workflow for the development of safety-related software
  - provides guidance on how to fulfill functional safety requirements with model-based development methods and tools
  - is based on best practices already proven in safety-related projects
  - addresses various aspects relevant for the development of safety-related software with a special focus on verification and validation
  - conforms to IEC 61508 and ISO 26262

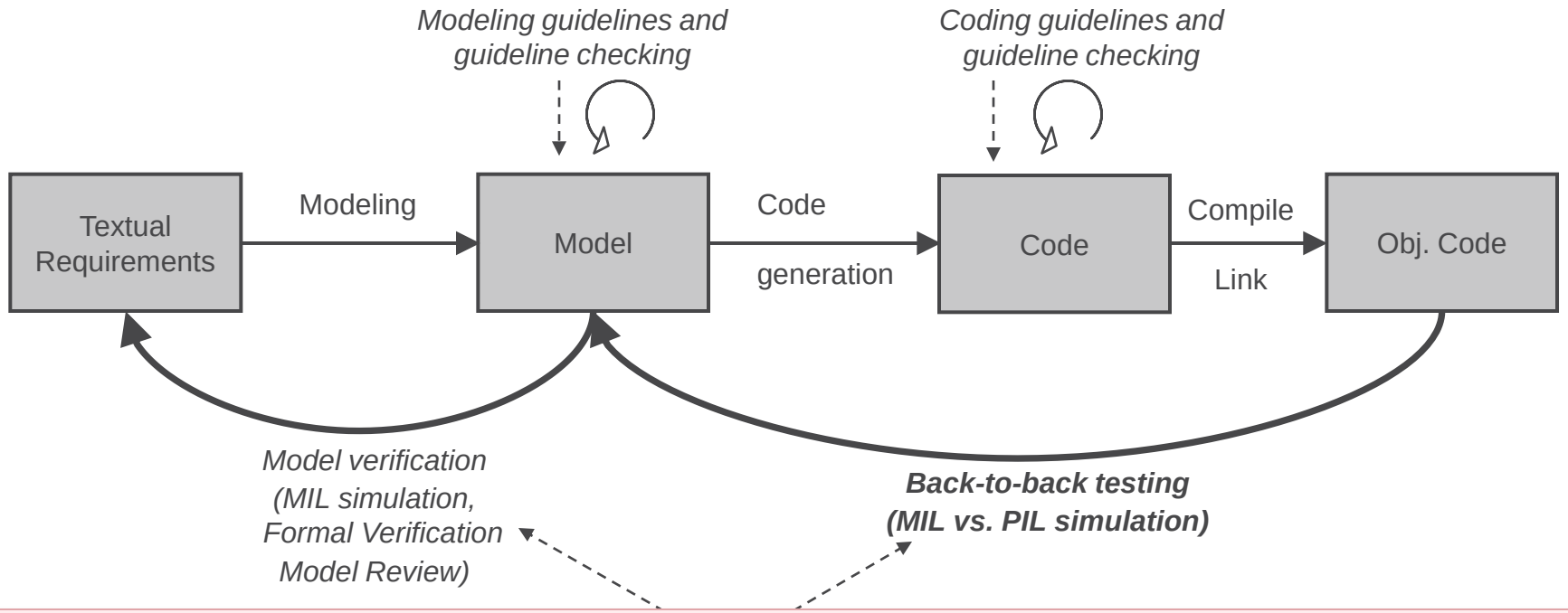

Embedded Success dSPACE

Model-Based Software Development for Safety-Critical Systems

TargetLink Reference Workflow

Author(s):	Michael Beine
Version:	1.0
File:	TL-ReferenceWorkflow.doc
Created:	2009-06-16
Last Modified:	2009-08-24
Number of Pages:	29

Model-Based Reference Workflow

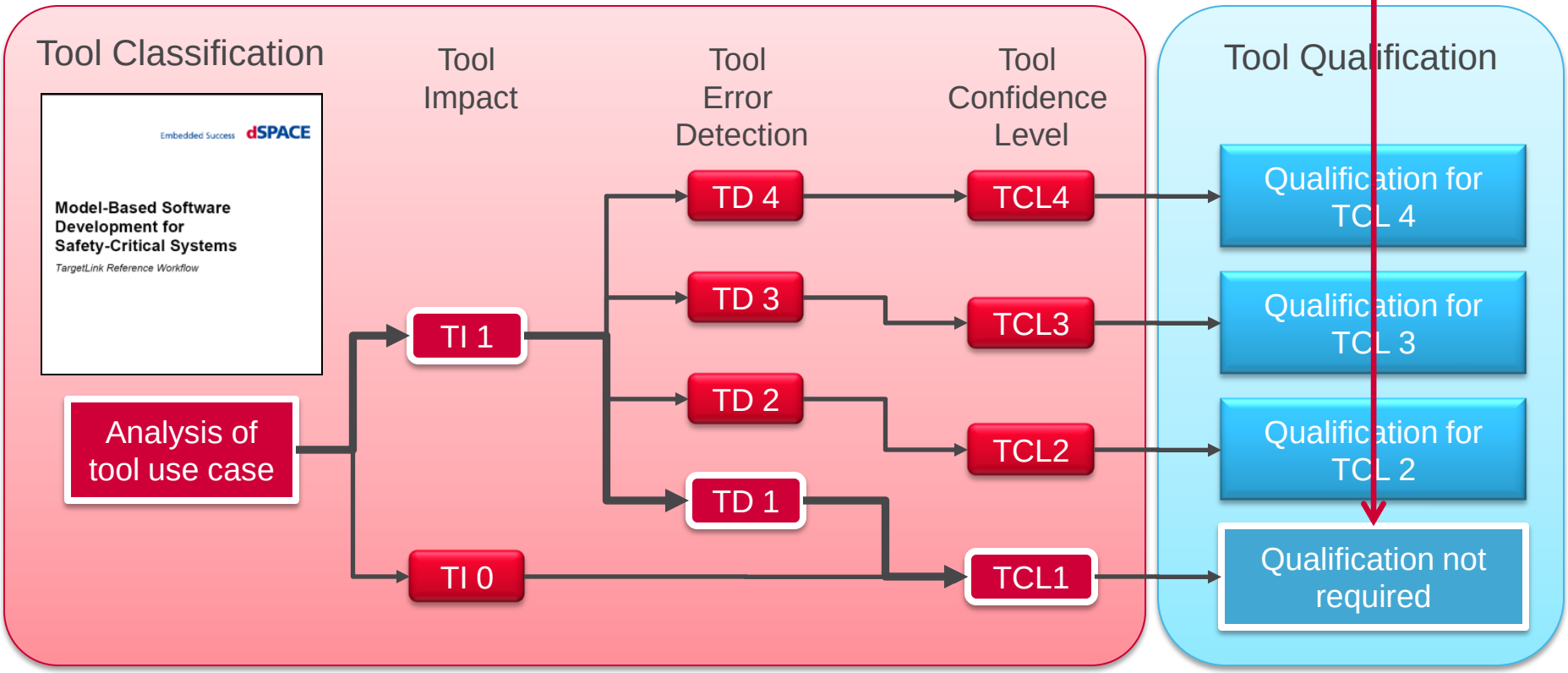


NOTE 4 For model-based development, software unit testing can be carried out at the model level followed by back-to-back tests between the model and the code. The back-to-back tests are used to ensure that the behaviour of the models with regard to the test objectives is equivalent to the automatically-generated code.

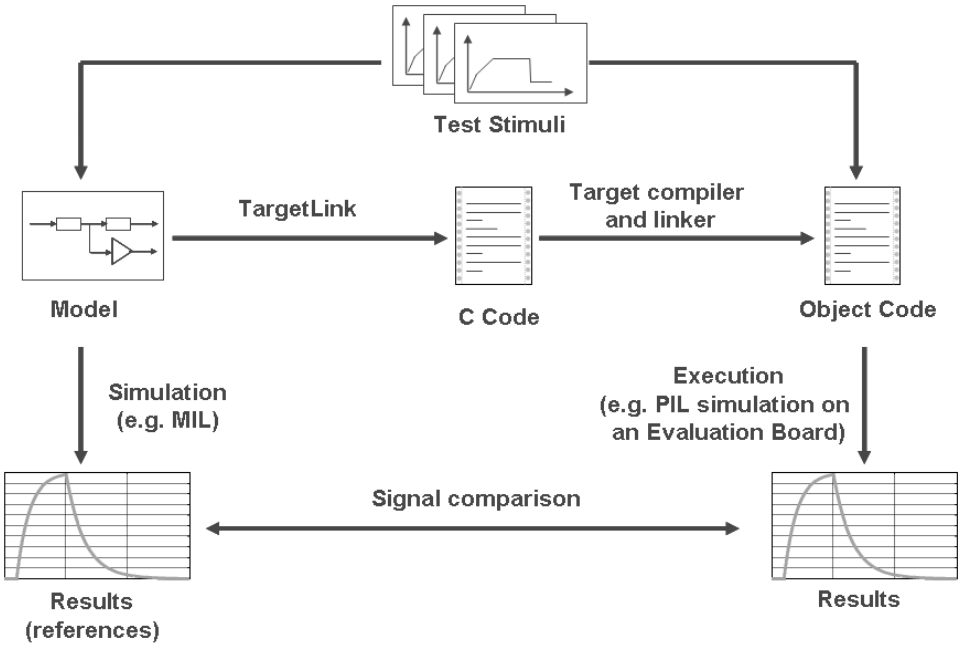
ISO/DIS 26262-6, 9.4.5

Code Generator Qualification for ISO 26262

- TargetLink
  - TCL based on Reference Workflow
  - “Fit-for-Purpose” Certification



Code Verification through Automatic Back-to-Back Testing



- Applying “identical” Test Cases both on model and code
  - Taking into account PiL specifics, timing, integer code, …
- Comparison of output signals wrt slight deviations regarding timing and values

Developing Test Cases: Manual und Automatic

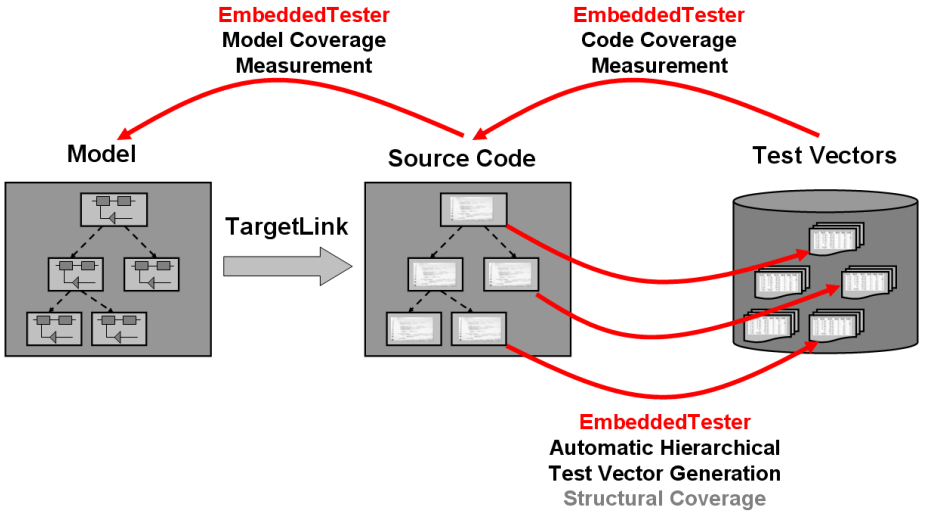
- Developing test cases is a two-stage approach
  - Manual development of test cases based on analysis of requirements
  - Automatic generation of test cases by structural analysis of model and code
- When is a test suite sufficiently powerful?
  - Metrics to determine coverage of code, model and requirements needed
  - Concept *Handling-Rate* for code level combines classical code coverage metrics (Statement, Decision, MCDC) with dead code analysis
    - 100% Handling-Rate regarding a location in the code means
      - either a test case exists contributing to the overall coverage, or
      - the code location under consideration is not executable, under no circumstances (assessment of an experienced engineer is necessary to understand reason!)
  - Leveraging from various algorithms for automatic test case generation (Monte-Carlo, Model-Checking, Bounded Model-Checking)

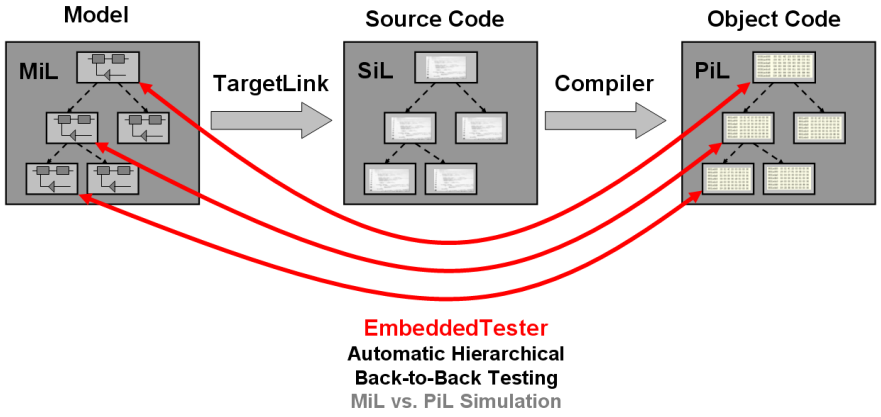
Hierarchical Approach Ensures Scalability

- Hierarchical…
  - …automatic test case generation
  - … measurement of code and model coverage

  to deal with application complexity when doing structural testing

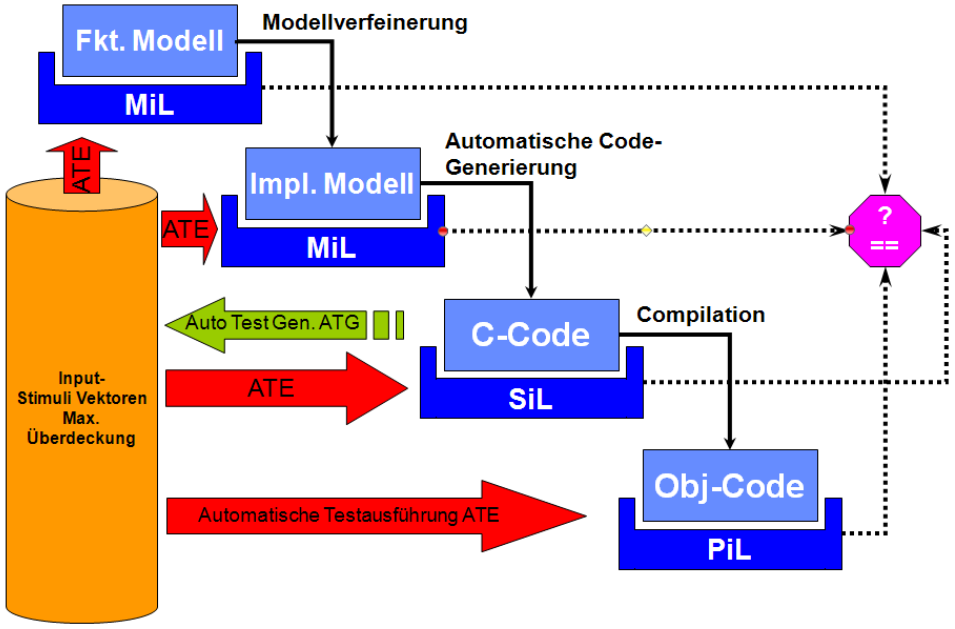
- Hierarchical Back-to-Back Testing





Approach:
Automatic Test Case Execution and Generation

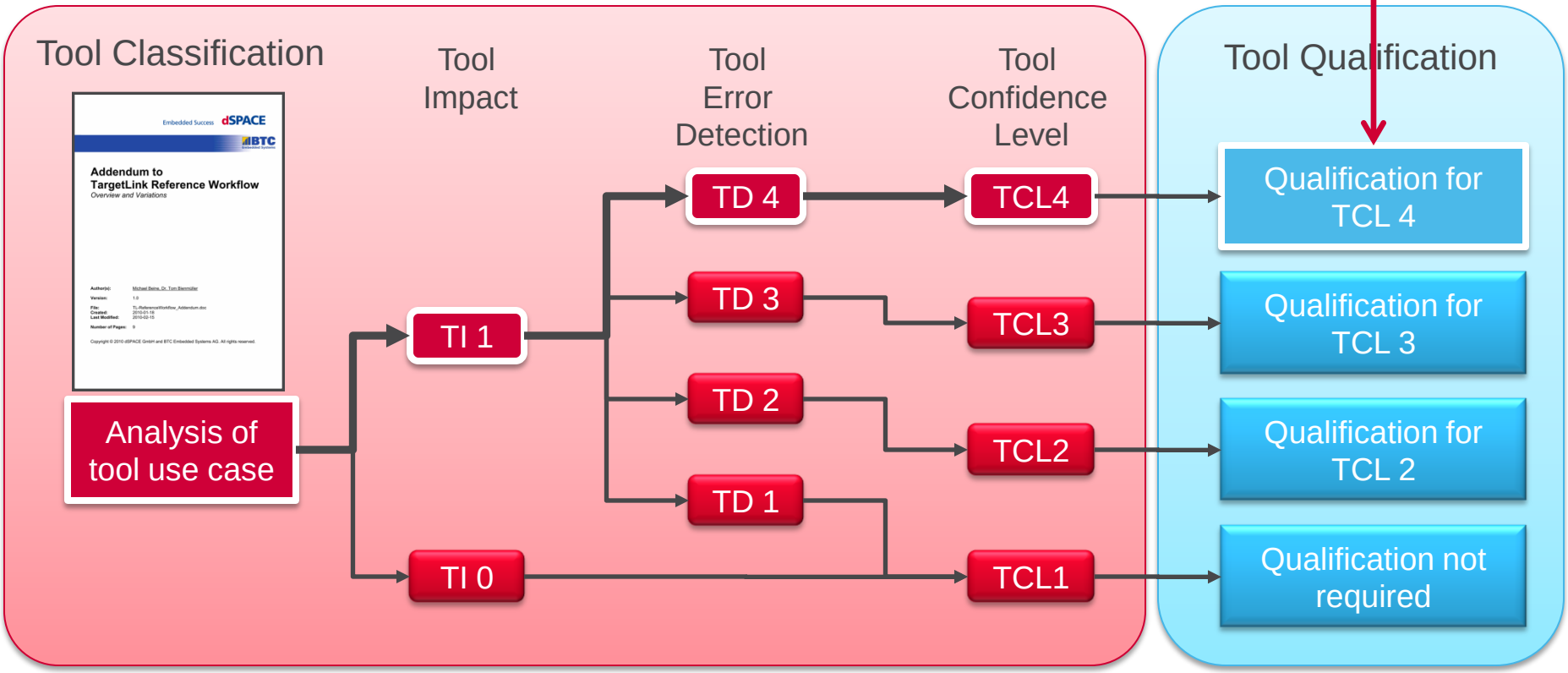
- Automatic test case generation based on the code
- Automatic test case execution on levels MiL, SiL, PiL
- Automatic comparison and reporting
- Automatic measurement of code and model coverage



- Leveraging from the hierarchical approach!
- Automate as much as possible to be efficient!

Test Tool Qualification for ISO DIS 26262

- BTC EmbeddedTester
  - TCL based on Reference Workflow (TCL4)
  - Certification: Validation of Software Tool and Evaluation of Dev. Process



TÜV Certification of BTC Embedded*Tester*®

- TÜV SÜD Automotive GmbH, German certification authority, evaluated BTC Embedded*Tester*®
- Result:
  - BTC Embedded*Tester*® is fit for purpose to verify target code by back-to-back testing including coverage criteria according to IEC 61508 and ISO DIS 26262, and derivate standards.
  - BTC Embedded*Tester*® is qualified for all ASIL-Levels according to ISO 26262
  - TÜV granted the following certificate ---->
- Certificate including certification report available on-demand

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. Z10 10 02 73219 001

Holder of Certificate: BTC Embedded Systems AG
Buschstraße 1
26127 Oldenburg
GERMANY

Factory(ies): 73219

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): BTC EmbeddedTester

Parameters: The model-based verification tool is fit for purpose to verify target code by back-to-back testing including coverage criteria according to IEC 61508, ISO 26262, and derivative standards.
The tool is qualified for all ASIL-Levels according to ISO 26262.

The report BO75961C is a mandatory part of this certificate.

Tested according to: IEC 61508-3:1998 (Fitness for purpose)
ISO/DIS 26262-8:2009

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: BO75961C

Date, 2010-02-25 (Frank Rauch)

Page 1 of 1

404584

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

Summary

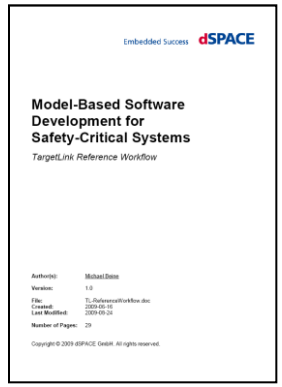
- Model-based development of safety-relevant software is applied in the industry
- TargetLink Reference Workflow based on best practice industry experiences provides guidance on the application of model-based development for safety-critical systems
- ISO 26262 defines a new approach to answer the question for software tool qualification
  - Approach has been successfully applied

TargetLink

Embedded*Tester*

International Organization for Standardization

ISO 26262



Embedded Success dSPACE

BTC Embedded Systems

Thank you for listening!

Michael Beine · dSPACE GmbH

Dr. Udo Brockmeyer · BTC Embedded Systems AG

Automotive Conference · June 2010 · Stuttgart