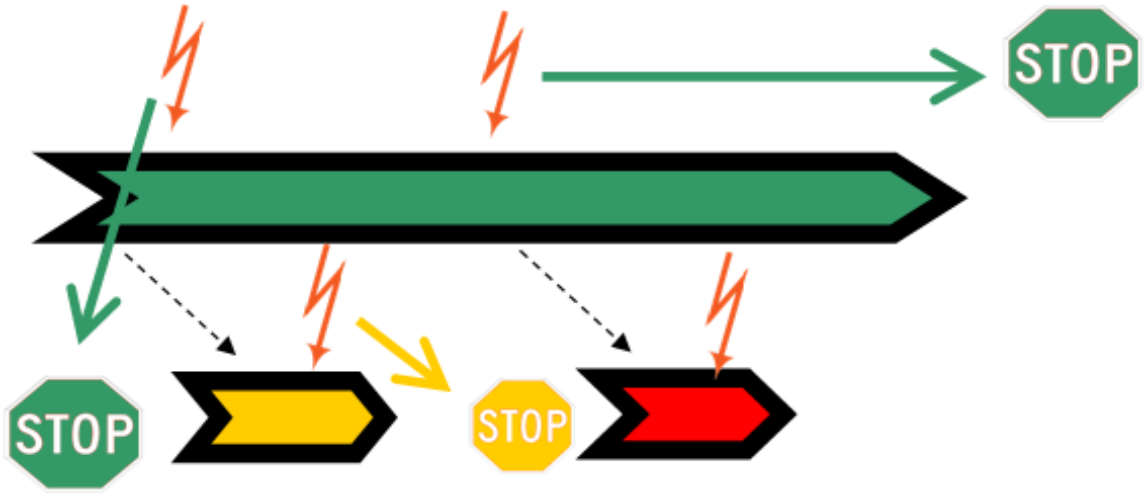
Tool Safety Manual for Testwell CTC++



Version:	0.8
Date:	2014-11-17
Status:	Generic / Adapted / **Presented** / Generated / Reviewed / Final
Author:	Dr. David Seider, Dr. Oscar Slotosch
File:	TSM_ManualPart.docx
Size:	14 Pages

Verifysoft TECHNOLOGY

History:

Version	Date	Status	Author	Change
0.1	2010-02-10	Generic	Slotosch	Template created
0.2	2013-10-10	Adapted	Slotosch	Adapted to Testwell CTC++
0.3	2014-01-23	Presented	R. Bär	Reviewed from Verifysoft
0.4	2014-01-30	Reviewed	Slotosch	Embedded fonts as review feedback
0.8	<generation date>	Generated	Generator Tool	Filled model-dependent parts
0.9	<review date>	Reviewed	<Customer>	Reviewed and updated
1.0	<finalization date>	Final	<Customer>	Finalized document

Contents

1 Scope of this Document

This document describes how the tool Testwell CTC++ shall be used such that it does not influence the safety of the developed products during its operation negatively. The main goals of the present guidelines are to ensure that

a) the requirements of the safety standards are satisfied and that
b) the assumptions and restrictions made during the tool evaluation are satisfied.

This tool safety guide is also called safety manual or tool application guideline.

The safety of tools is achieved within three steps

1. tool evaluation and possibly qualification,
2. proper tool installation and
3. proper tool operation.

The method is to show that all potential errors of the tools identified during the tool evaluation will not affect the safety of the product. The results of the tool evaluation of the Testwell CTC++ can be found in [TCR]

The completeness of this safety manual is achieved by tracing the requirements of the standards to the tool guidelines.

Therefore this document is structured as follows

- Method (see Section 3),
- Requirements derivation from Standards (see Section 0)
- Tool Guidelines (see Sections 5, 6 and 7).

2 Glossary

This section defines technical terms used within this document.

Term	Definition
Check	possibility to detect an error
Error	in this document used as "potential error"
Error (model) element	representation of an (potential) error in the model
Feature (model) element	representation of a function in the model.
Function	an elementary or composed function of the tool, that can be required in one or more use-cases, e.g. load, save, "perform" functions
Qualification environment	TAU and tests, a validation suite according to ISO 26262
Restriction	possibility to avoid an error
Safety Guideline	Guideline to mitigate some potential errors of the tool. Modeled as a *Check* or *Restriction*, either in an usual *UseCase* or *Feature* of the *Tool*, or in a separate, virtual *Feature* that can be required (added) by any use case of the same tool. Safety Guidelines are listed in the tool classification report and applied in the tool safety manual.
software off-line support tool (IEC 6108)	According to IEC61508-4-3.2.11: software tool that supports a phase of the software development lifecycle and that cannot directly influence the safety-related system during its run time.
TAU	Test Automation Unit: executes tests for the test suite
TD	Tool Error Detection (TD) probability for a potential error to be detected / avoided in a defined process TD1=high detection probability, TD2=medium detection probability, TD3=low or unknown detection probability
TCL (ISO 26262-8)	Tool Confidence Level (ISO 26262): required confidence in the tool when used in the analyzed tool chain TCL1=low confidence required , TCL2=medium confidence required, TCL3=high confidence required[1]
TCR	Tool Classification Report, also called tool criteria evaluation report in ISO 26262
Test	Single test with result PASS/FAIL/ABORT
Test Directory	A directory containing one or more test (directories)
Test (model) element	Representation of a test directory in the model including a test description that specifies it
Test Suite	structured set of single tests
Test Plan	list of test (directories) to be executed

[1] Of course once the tool with TCL>1 have been qualified, the TCL can be regarded as existing tool confidence for the qualified ASIL rather than required tool confidence.

Tool	a development tool according to ISO 26262
Tool Chain	a collection of tools, not necessarily forming an input/output chain
Tool classes (IEC 61508-4)	Software off-line support tools are classified into the following tool classes: T1: generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system T2: supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software T3: generates outputs which can directly or indirectly contribute to the executable code of the safety related system.
Tool Classification	determination of the required tool confidence level (ISO26262: TCL or IEC 61508: tool classes)
Tool Evaluation	or tool criteria evaluation: see tool classification
TQP	Tool Qualification Plan
TQR	Tool Qualification Report, extension of TQP according to [QKit_UM]
TSM	This Tool Safety Manual
Use-Case	the purpose of using the tool in development process
Use Case (model) element	representation of an use-case in the model
Virtual Feature	A *Feature* is called virtual, if it's virtual attribute is set to true. *Virtual Feature*s are modeled in a *Tool*, but are not implemented in the tool. They are used to model safety guidelines (documents) and can be added flexible as required features to use cases to denote that the use cases follow them. Virtual feature do not have errors.

Note that elements, relations and actions from the model that have a formal Semantic in the TCA are written in capital and with italic font, e.g. "*Error* element", or "*Export -> Excel Review*".

3 Method

The relevant safety standards have comparable approaches to tool qualification. In all standards the goal is to ensure that the tools can not impact the safety of the product, i.e. that all potential errors of the tool are either absent or cannot impact the safety. And all standards do this by a combination of application and installation methods. The application methods are safety guidelines that explain how to use the tool and avoid/detect the potential errors, while the installation methods ensure that the installed tool works as expected, e.g. by testing it to show the absence of the potential errors.
All standards have a classification phase to determine the required confidence into the tool and a qualification phase that provides this confidence or restricts the usage of the tools to confident scenarios. However the classification and qualification methods differ in some details. Nevertheless our qualification approach is suitable for all standards and does not require unnecessary work.

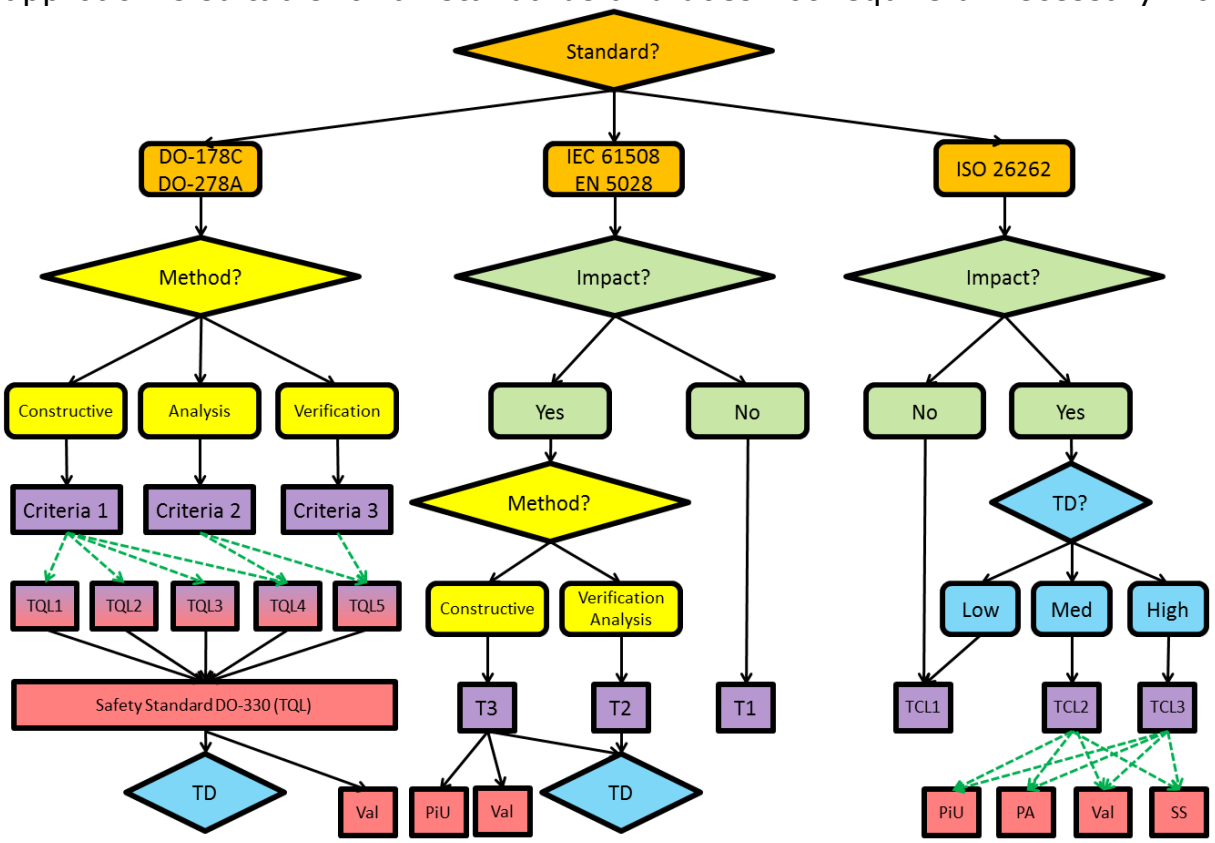


Figure 1: Comparison of Qualification Approaches

Figure 1 gives an overview on the different approaches. The main difference between ISO 26262 and the other standards is that the classification of tools depends on the analysis of the potential errors and their detection, which increases the variability of the classification. The impact and the supported methods/processes are considered in all standards as part of the classification. While the ISO does not differentiate between kinds of the tools the other standards do and classify the tools for constructive methods (e.g. code generators and compilers) as more critical than the other tools verification,

automation and analytic tools. The results of the classification is the confidence needs (represented in pink color in Figure 1). The DO expresses the tool confidence requirement by criteria 1-3 the ISO 26262 as tool confidence levels and IEC 61508 and EN 50128 as tool classes T1-T3. The next step is to derive the qualification methods from the qualification needs of the tool and the criticality of the developed software. ISO 26262 and DO 178C, DO 278A do have tables that map the software criticality to qualification methods, e.g. a validation is required from ISO 26262 for TQL 3 tool in ASIL C and D projects. In DO the qualification methods are determined by the tool qualification level (TQL) that is the interface to the DO-330 and determines the development of the tool, which is a specific qualification method. This criticality dependent selection of qualification methods is depicted in Figure 1 using green dotted lines. The qualification methods differ also. While the DO allows only the development according to the DO-330, a safety standard (SS), the other standards include also a proven in use argumentation (PiU) and a process assessment (PA). Since DO-330 requires also a validation, the validation is the only method that is applicable in every standard. Furthermore the analysis of potential tool errors and their detection (TD) is required in every approach for tools that have impact.
Therefore this classification report contains the determination of the tool confidence need and the analysis of the potential errors and their detection, that belongs to the classification in the ISO 26262.

We formalize the tool chain to determine the required confidence using the following model:

- Use case: describes an application scenario of the tool
- Feature: a tool function utilized in use cases
- Potential error: a potential error that could occur during the application of a tool
- Error mitigation: a check or restriction applied during the tool operation phase
- Qualification: a method to show that a tool or a feature satisfies its specified requirements by demonstrating the absence of potential errors.

The confidence is determined by an analysis of the use cases of the tool as used within the development process. If the tool has an impact on the safety of the product, all potential errors within the used features are analyzed for how they can be detected or avoided within the process. If there is no high probability for detecting or avoiding the errors, the tool has to be qualified to ensure the absence of these errors.

This tool safety manual contains the safety guidelines that have been found during the analysis of potential errors and cannot be excluded by validation.

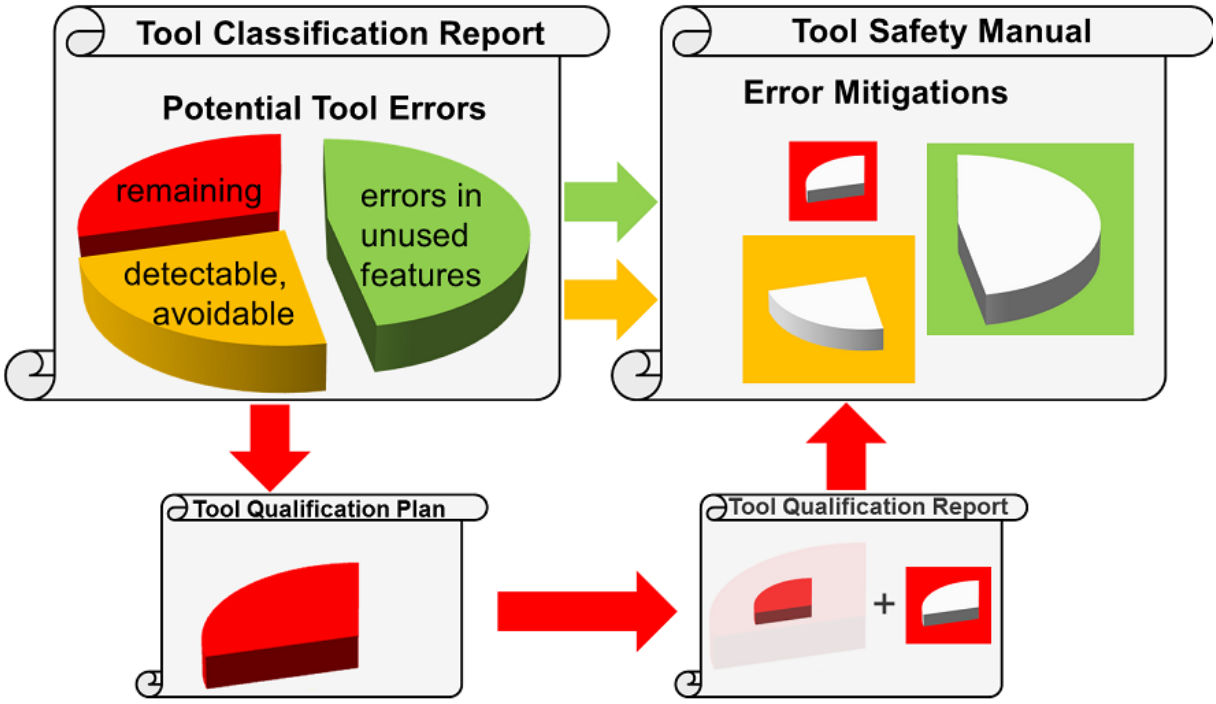


Figure 2: Derivation of Tool Safety Manual Contents

The safety manual for a tool has to contain the mitigations against all potential tool errors that are considered during tool evaluation [TCR]. The errors can be grouped into the three classes (see Figure 2):

- Potential errors in unused features (green in Figure 2)[2]: Using these features is prohibited in the safety manual.
- Potential errors with mitigations: detections and restrictions (yellow in Figure 2): These mechanisms are described in the safety manual, especially if the checks/restrictions have to be triggered by the user of that tool.
- Remaining potential errors (red in Figure 2): Demonstrating their absence has to be the goal of the tool qualification (tool qualification plan). The tool qualification report possibly shows some concrete errors that are instances of the potential error classes. The qualification report contains proposed workarounds for these concrete errors that have to be part of the safety manual (together with the workaround for other already known relevant errors.)

The safety manual / tool application guide therefore has to contain the following information:

[2] Note that the analysis of potential errors in unused functions is not required, but the features need to be identified.

- Allowed features and configurations of the tool
- For potential errors that might occur in required features and that are not excluded by tool qualification: Requirements to apply checks and restrictions to mitigate potential tool errors
- Workarounds for known errors and errors found during qualification
- Other information required by the standards to identify the tool exactly (version, configuration, etc.).

The tool qualification plan has to ensure that the identified potential errors of Testwell CTC++ that are not detectable / avoidable cannot occur. This is done by applying a validation suite in a systematic way that shows the absence of these potential errors.

Since the tool Testwell CTC++ shall be qualified using validation accruing to this qualification plan we have to provide the following documents:

- *Test Plan*: to plan the execution of tests
- *Test Report*: contains the test results
- Test Automation Unit Manual: To execute the planned tests cases correctly
- *Test suite validation and verification documents (plan and report)*: to ensure that the test suite shows the absence of the potential errors if passed successfully

The documents that depend on the model are typed using *cursive font*.

In the case that the model and the validation suite needs to be extended and new test cases need to be produced and validated, the following documents are required, or need to be extended:

- *Test specifications* including a test strategy to show the absence of the absence of the potential errors.
- *Test suite V&V plan & report*

The test specification is part of the model (descriptions). The test suite needs validation against the potential errors of the model and verification against the implementation using a review. This quality process creates the confidence into the effectiveness of the test suite. The V&V documents for the test suite are contained in the qualification kit to demonstrate the confidence to the user. If the test suite is extended these documents shall also be extended.

Figure 3 shows the relation between the documents and their variability, i.e. which are constant and which depend on the use case: It describes how to derive the safety manual by a validation suite that consist of tests that show the absence of the identified critical errors in the tool evaluation report. Depending on the used features of the tool and the applied mitigation measures this set of errors might vary. For every required test (or group of tests) that show the absence of one or more errors there needs to be a test specification (including a test strategy) that explains how the absence of the

errors is ensured if the tests pass. The tests in the test suite need to be validated to conform to the test specification. This is planned in a V&V plan of the kit and documented in the V&V report. Having a V&V report is the prerequisite for applying the validation suite to a use case. In Figure 3 the use case specific documents are in a green/inner, dashed box where the contents of the qualification kit are in the outer/blue box. Of course the sequence of creating the documents (indicated by the sequence numbers) starts with the non use-case specific documents in the qualification kit. The tool qualification is planned in the qualification plan and requires executing tests (planned in the test plan) using the test automation unit manual. The test results are documented in a test report which is than analyzed and documented in the qualification report.

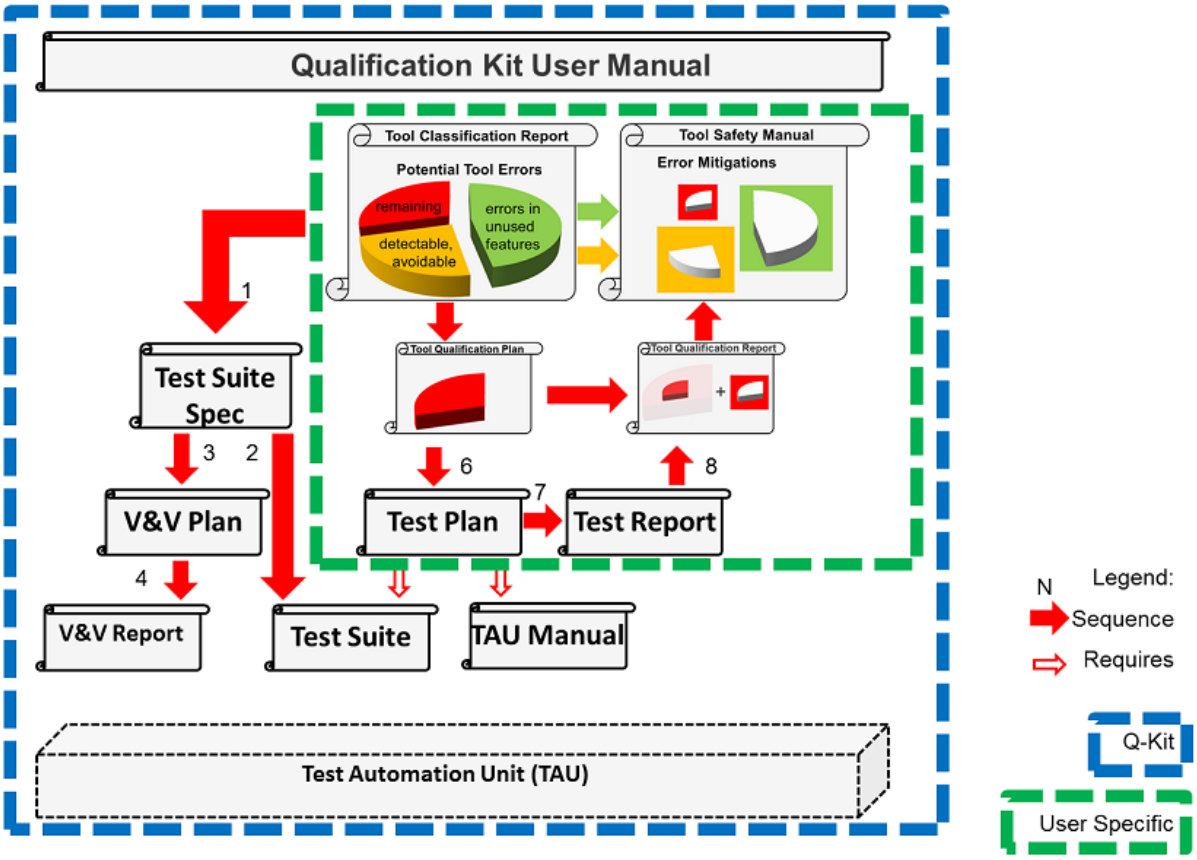


Figure 3: Documentation Plan

There are many documents in Figure 3 that are required and that need to be adapted depending on the user's process captured in the qualification model by selecting the required tool features and the executed mitigations during the process. The use case specific parts in the user specific documents are generated from the qualification model.

4 Requirements Tracing to Safety Standards

The requirements of the safety standards relevant for tool qualification and safety guidelines which are considered here mainly come from the standards

ISO 26262, IEC 61508, EN 50128 and DO-330. Many other safety standards (DO-178-C, etc.) have similar requirements.
The standards have been analyzed and the relevant requirements have been listed and linked against the guidelines in the next sections. This is documented in [QKit_UM] and in the tool qualification plans & reports.

5 [generated]

6 References

[DO330] RTCA. DO-330: Software Tool Qualification Considerations 1st Edition 2011-12-13.

[EN50128]: BS EN 50128:2011, Railway applications — Communication, signaling and processing systems — Software for railway control and protection systems, BSI Standards Publication

[IEC61508]International Electrotechnical Commission, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2.0, Apr 2010.

[QKit_UM] User Manual: Qualification Kit for Testwell CTC++

[ISO26262] International Organization for Standardization. ISO 26262 Road Vehicles –Functional safety–. 1st Edition, 2011-11-15.

[SAFECOMP12] Determining Potential Errors in Tool Chains: Strategies to Reach Tool Confidence According to ISO 26262, SAFECOMP 2012, Wildmoser, Philipps, Slotosch

[TCA] Tool Chain Analyzer, tool available on www.validas.de/TCA.html Version 1.9.1

[TCA_UM] Tool Chain Analyzer, Version 1.9.1, User Manual, (<TCAHome>/plugins/Documentation/UserManual.pdf)

[TCR] Tool Classification Report for tool chain containing Testwell CTC++

[TQP] Tool Qualification Plan for Testwell CTC++

[TQR] Tool Qualification Report for Testwell CTC++