

Qualification Kit for Testwell CTC++

Tools which are used for the development of safety critical software need to be classified (Tool Classification) in order to determine whether a qualification of the tool are necessary. This classification considers the impact of the software tool on the project.

Tools which can have an impact on the project, and in which a malfunction is not immediately apparent, the safety standards require proof of trustworthiness. This proof is done by a qualification of the tool (Tool Qualification).

A tool must always be qualified within the concrete development environment of the tool user.

To simplify the qualification of Testwell CTC ++ in safety-critical projects, Verifysoft Technology offers a tool Qualification Kit for Testwell CTC++. The Qualification Kit is suitable for the standards EN 50128, ISO 26262 (automotive), DO-178C (aeronautics) and IEC 61508 (railway).

Tool-Qualification Kits available



Figure 1: The Tool Qualification Kit for Testwell CTC++ covers several standards

Please note that software verification tools like Testwell CTC++ need to be qualified and not certified. Only the safety critical software which is used eg. in the aircraft or the car has to be certified.

Tool Classification

As mentioned above, the tools used in the development of safety-critical software must first be classified.

Test coverage tools like Testwell CTC++ are verification tools. Although those tools are unable to insert errors in your code, they can fail to detect errors which are already introduced in your code (for example by premature termination of the testing due to the display of a too high test coverage).

Result of the classification is to decide whether and to what extent a qualification of the tools for the specific project is required.

The classification process of software tools is slightly different for the standards DO-178C, IEC 61508/EN 50128 and ISO 26262 (c.f. figure 2).

First: Tool Classification

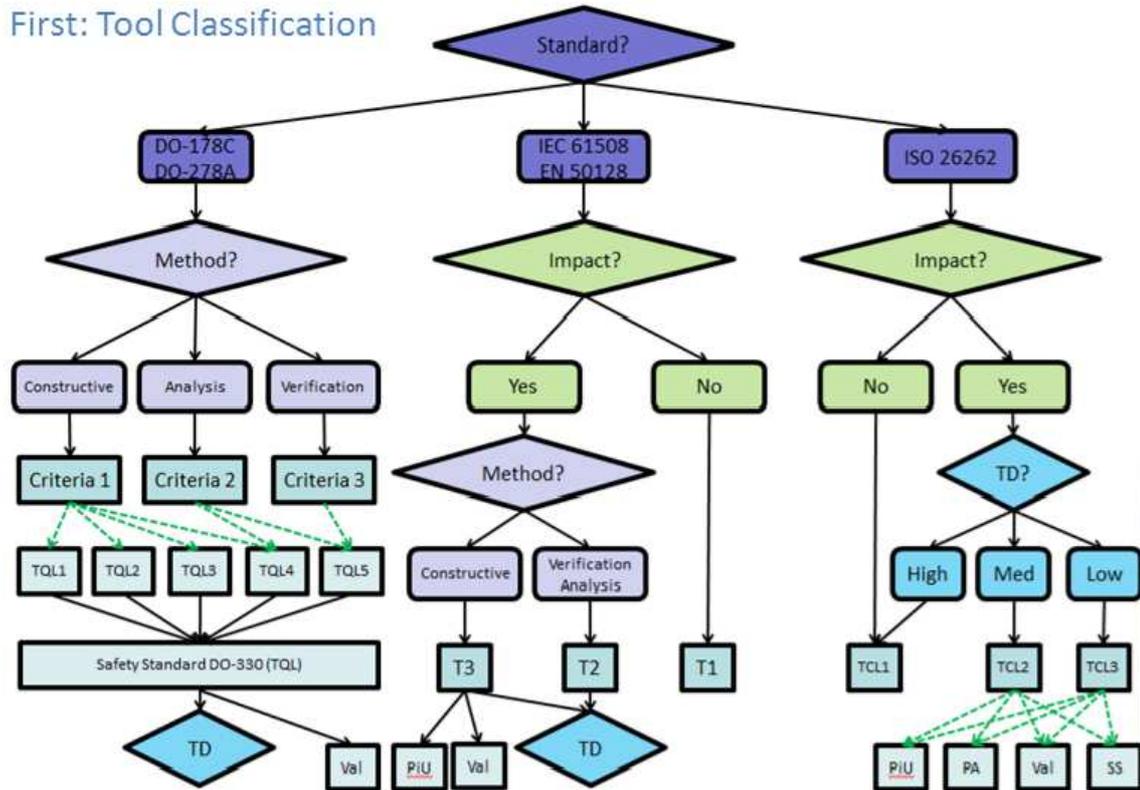


Figure 2: Tool Classification for different standards (Source: Validas AG, Munich)

The following description is about the automotive standard ISO 26262 (c.f. right part of figure 2). First is checked whether the tool has an influence (impact) on the software.

If the tool has no impact on the software, the tool is classified TCL 1 (Tool Confidence Level 1) and the qualification is not needed.

If the tool can have an impact on the software, the probability to detect such an impact need to be evaluated (TD). If the probability to detect a malfunction is high, the tool is classified TCL1 (no qualification needed). For example if you use two different coverage tools and if you compare the results, the probability to detect misfunctions is high. By this usage of redundant tools the tool qualification can be avoided .

If the probability of the detection of misfunctions is medium, the tool confidence level is 2 (TCL 2). For a low probability to detect misfunctions the tool confidence level is 3.

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

Table 1: Determination of the tool confidence level (TCL)

While for the tool confidence level 1 no tool qualification is required, the software tool must be qualified for tool confidence levels 2 according to the following table:

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance 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.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178.

Table 2: ISO 26262: Qualification of software tools classified TCL2

For tool confidence level 3 the ISO 26262 requires the following:

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance 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.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178.

Table 3: ISO 26262: Qualification of software tools classified TCL3

Tool Qualification by Validation

The qualification method is tool validation by testing the safety relevant parts of the tool. The standard ISO 26262 describes the validation of a software tool in chapter 11.4.9:

“The validation measures shall demonstrate that the software tool complies with its specified requirements (use cases of the tool). The malfunctions and their corresponding erroneous outputs of the software tool occurring during validation shall be analysed together with information on their possible consequences and with measures to avoid or detect them. In addition the reaction of the software tool to anomalous operating conditions shall be examined.”

Tool Qualification Kit for Testwell CTC++

The Tool Qualification Kit for Testwell CTC++, which have been developed by Verifysoft Technology in cooperation with Validas AG (Munich/Germany), reduces dramatically the effort for the tool qualification. The kit supports the user in the qualification of safety critical software development according to the standards ISO 26262, DO-178C, IEC 61508, and EN 50128.

The Qualification Kit for Testwell CTC++ validates that statement, decision, and MC/DC coverage is properly analysed and shown for the programming language C by Testwell CTC++ in your development and project environment.

The kit consists of a Qualification Support Tool (QST), a test suite with many test cases for the different use cases of Testwell CTC++, a Test Automation Unit (TAU) to execute the test cases, a Validation & Verification Report (V&V Report) in order to prove the quality of the qualification kit, and an user manual.

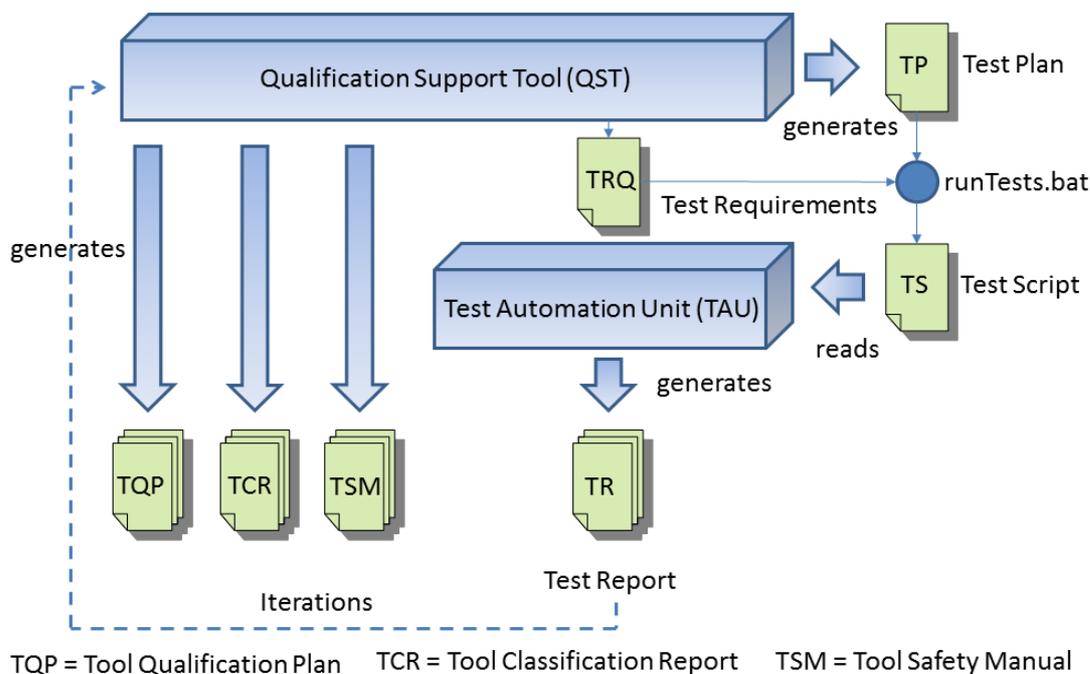


Figure 3: Tool Qualification Kit for Testwell CTC++

Application of the Tool Qualification Kit

The Qualification Support Tool guides the user through the qualification process. First the relevant standard is chosen (c.f. figure 4).



The screenshot shows a dialog box titled "Select Standard for Testwell CTC++". Below the title, there is a message: "There are more safety standards supported for qualification. Please select one". Underneath, there is a section labeled "Standard for Qualification" containing a list of five standards with checkboxes:

- ISO26262
- IEC61508
- EN50128
- DO178C
- DO330

Figure 4: Choice of standard within the Qualification Kit

In the next step the used variant of Testwell CTC++ is chosen (host only, CTC++ with host-target add-on for measuring on target code coverage, or CTC++ with bitcov-add-on for measuring code coverage on very small targets).



The screenshot shows a dialog box titled "Select Variant for Testwell CTC++". Below the title, there is a message: "There are more variants ready for qualification. Please select one". Underneath, there is a section labeled "Variant for Qualification" containing a list of three variants with checkboxes:

- HostTest
- TargetTest Bitcov
- TargetTest Hota

Figure 5: Choice of Testwell CTC++ variant

In a further step the version of Testwell CTC++ is chosen (c.f. figure 6).

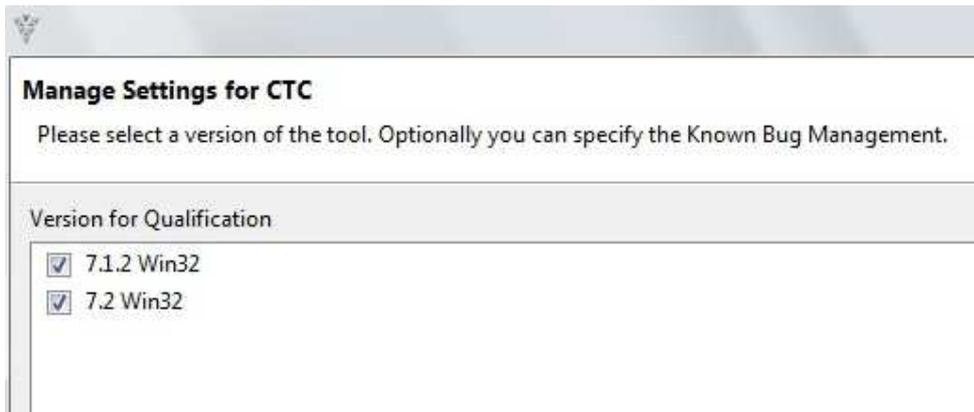


Figure 6: Choice of Testwell CTC++ version

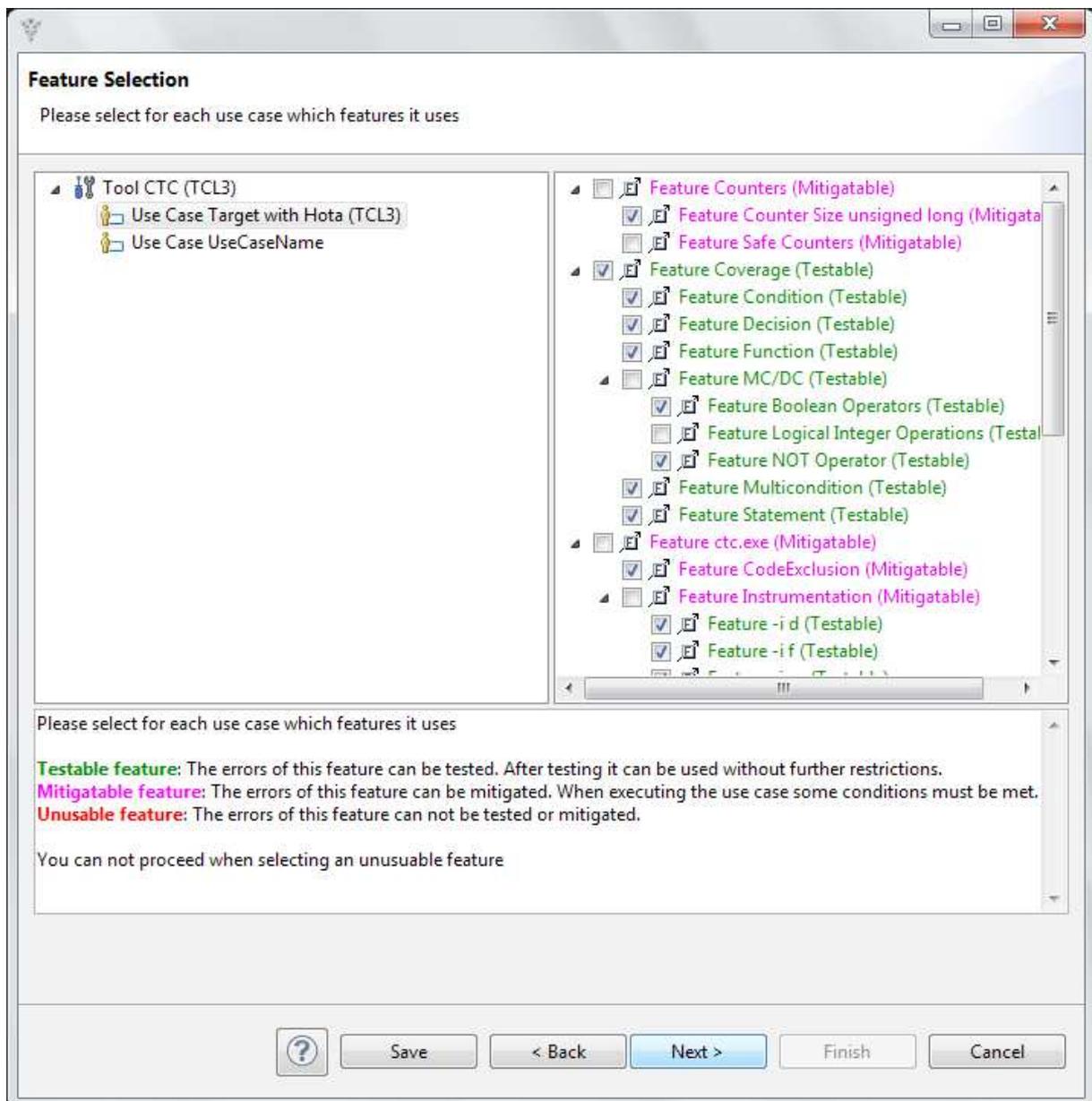


Figure 7: Choice of used features

The user then selects the used features of Testwell CTC++ (c.f. figure 7). Only the features which are used in your project need to be qualified. According to the standard and the ASIL level the used features and mitigations are already preselected.

The usage of features, which have not been validated during the tool qualification is prohibited. The Qualification Support Tool generates a notice within the Tool Safety Manual.

Features which are testable have green color. Pink colored features can be used with some constraints (mitigations).

Mitigations and test cases are preselected in the next step (c.f. figure 8). If needed other cases than the preselected ones can be chosen.

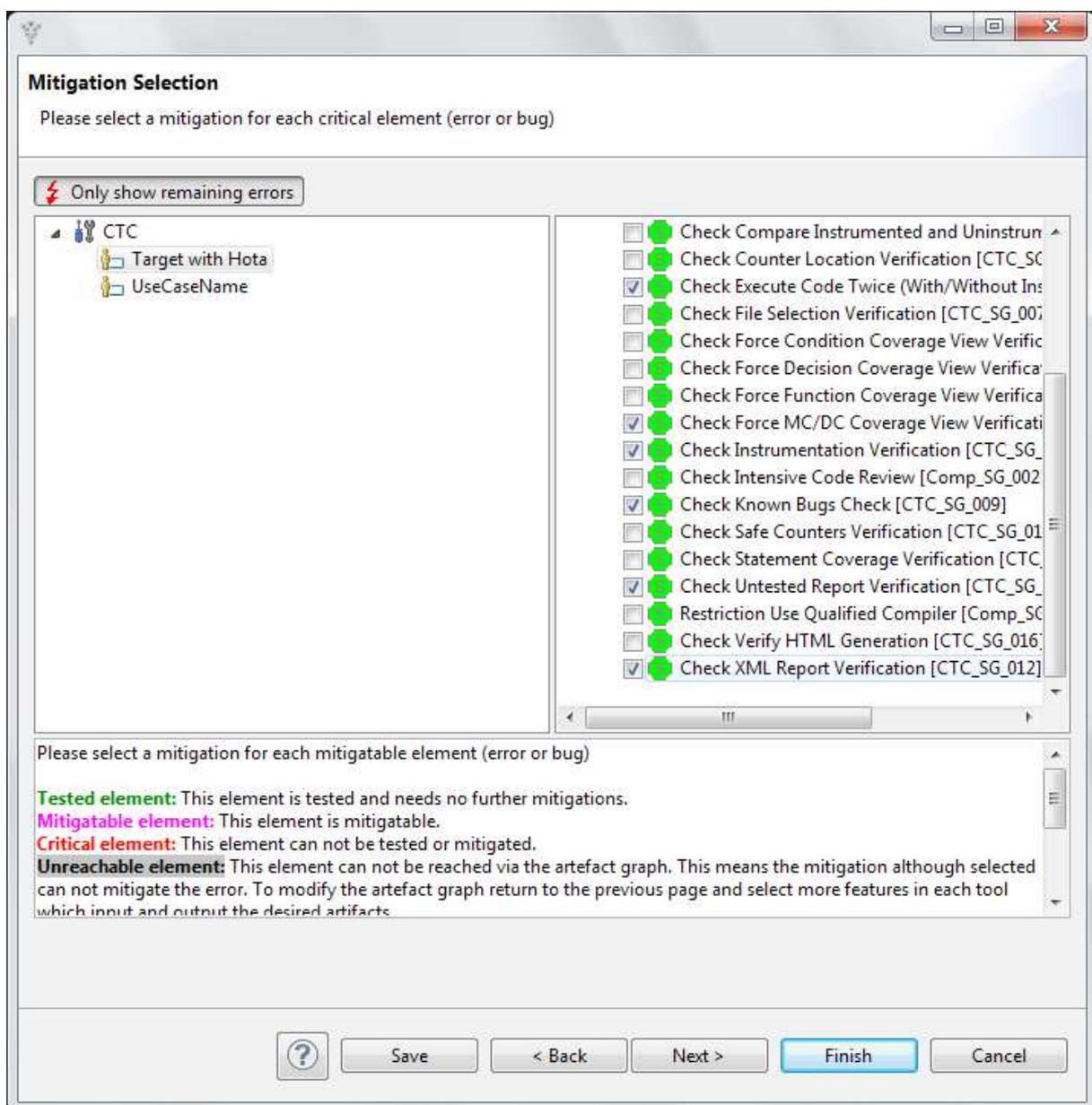


Figure 8: Choice of mitigations

The next window serves for the organisation of the qualification process (c.f. figure 9). You can determine roles (who does what and when?).

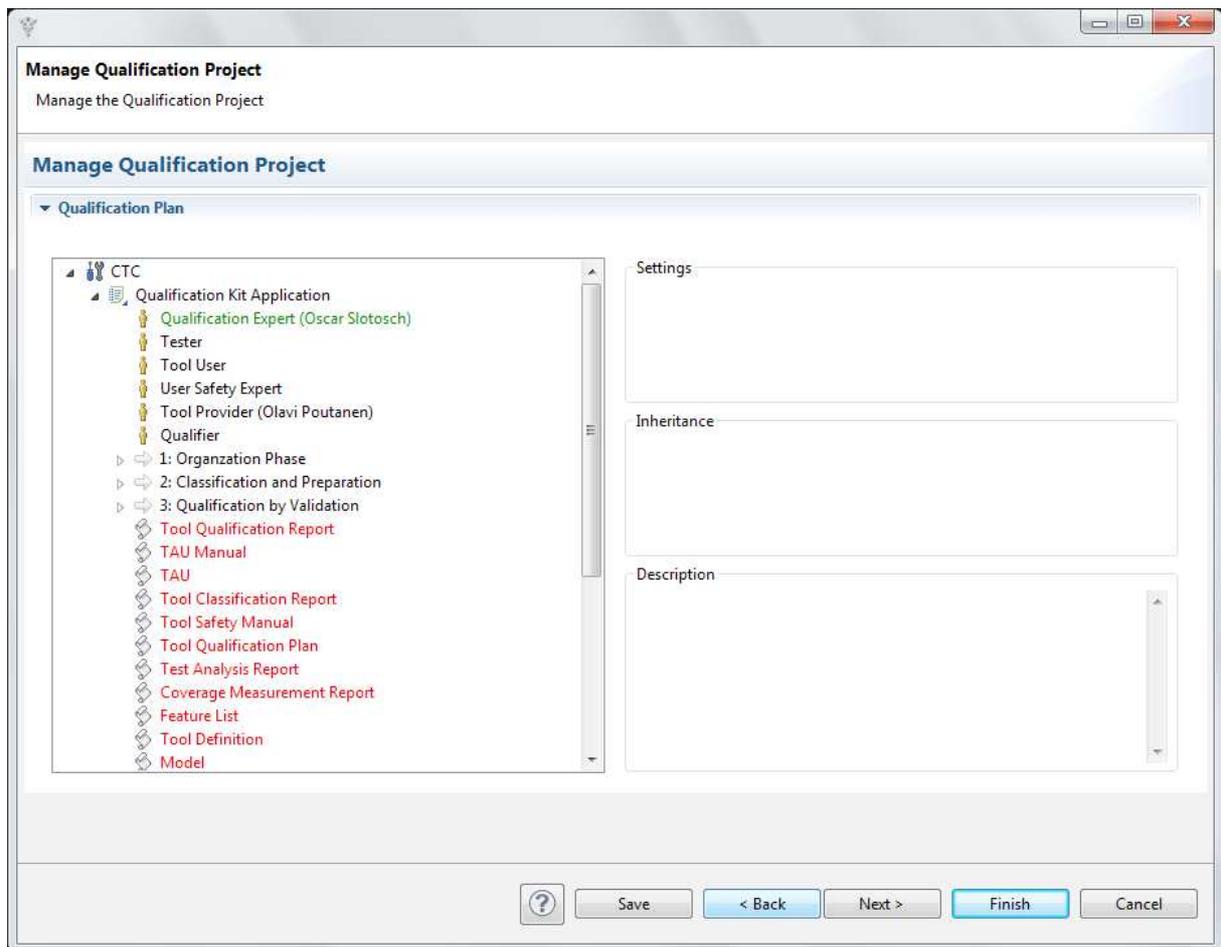


Figure 9: Planning of the qualification

The next view shows a summary with the number of features, selected checks, number of tests, and the path to the generated documents (c.f. figure 10).

After pressing the „Finish“ button, various documents like the Tool Classification Report (TCR.docx), the Tool Qualification Plan (TQP.docx), and the Tool Safety Manual (TSM.docx) are generated. Also files like Test Run Files, Test Execution.txt and tool-config-files are generated. Some of the generated documents and files are shown in figure 11.

By executing the testrun.bat, a test script is generated. This test script is read and executed by the Test Automation Unit (c.f. figure 12). The generated documents are updated. You have the proof that Testwell CTC++ works properly within your project if all tests have been passed successfully.

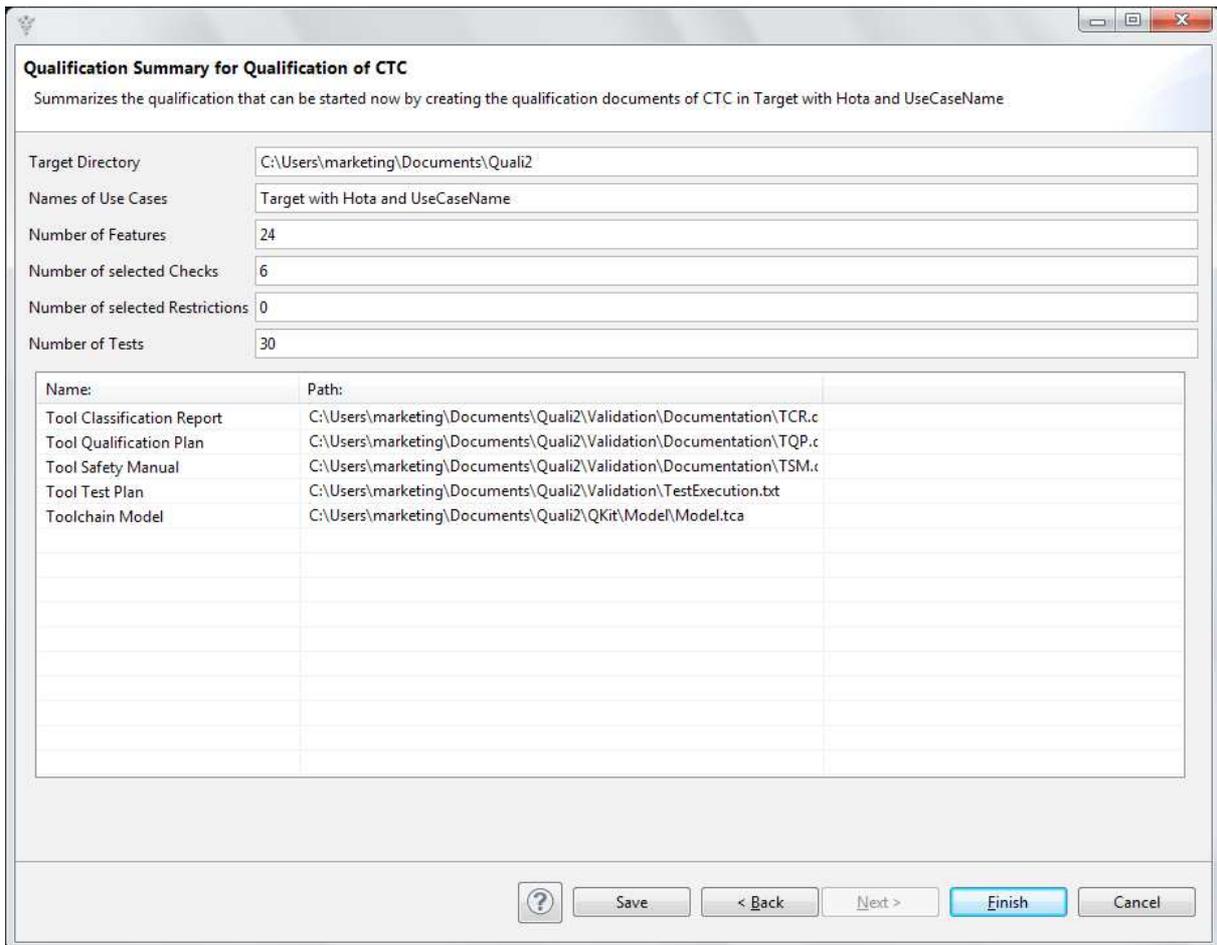


Figure 10: Summary of the qualification

Generated Documents

- Qualification Documents

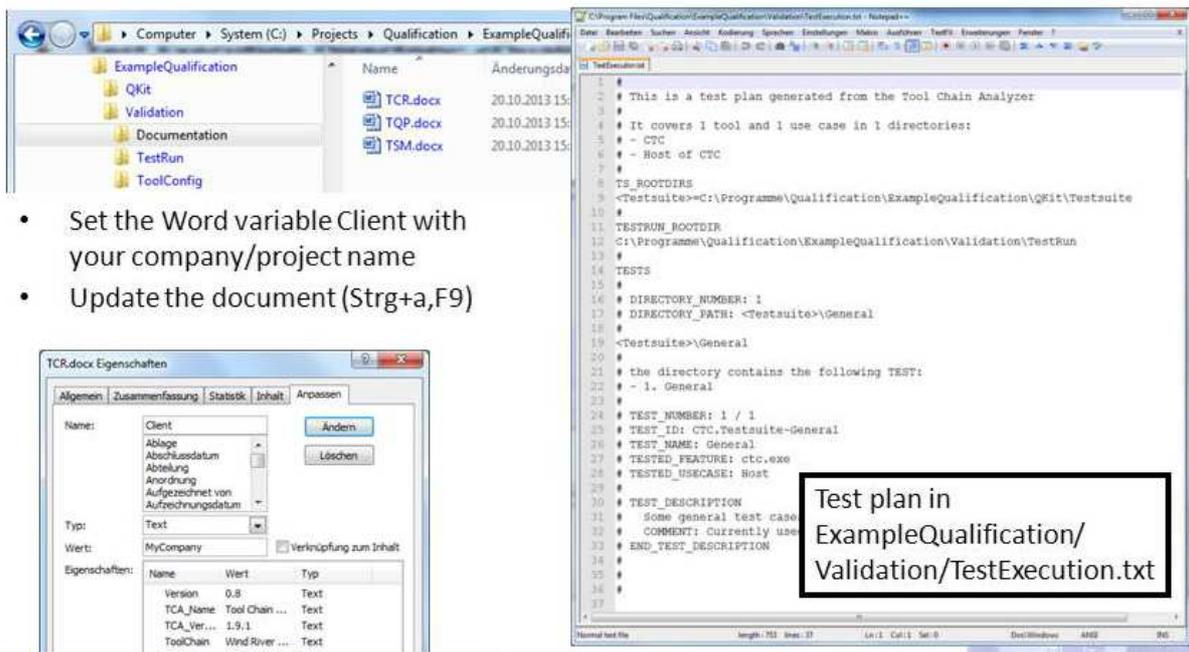


Figure 11: Documents generated by the Qualification Support Tool

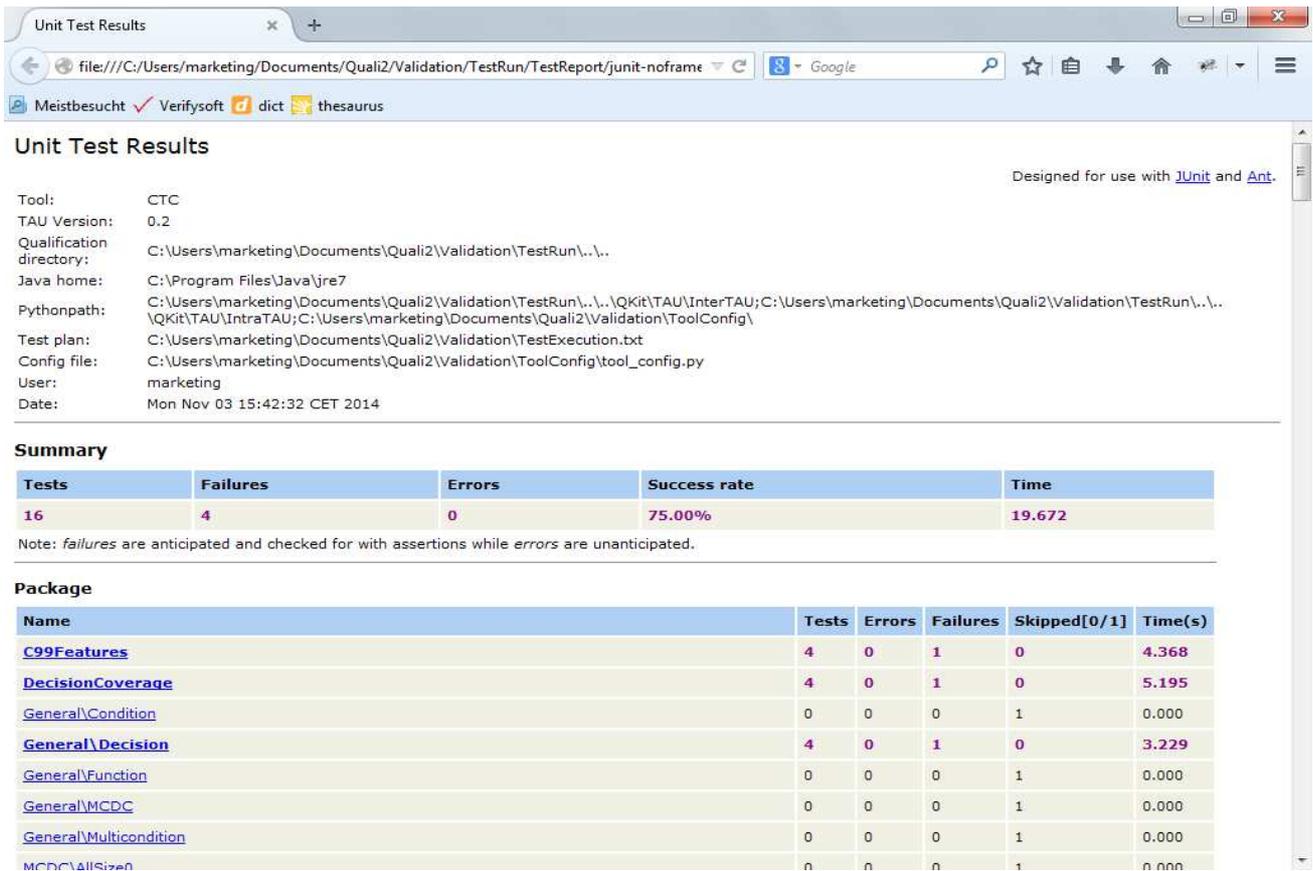


Figure 12: Results of the test run

For further information please contact:
 Verifysoft Technology GmbH
 In der Spöck 10-12
 77656 Offenburg
 Deutschland

www.verifysoft.com

Phone +49 781 127 8118-0

Last modified: 17 November 2014