Qualification-Kit für Testwell CTC++

In der sicherheitskritischen Softwareentwicklung müssen die im Projekt eingesetzten Werkzeuge zunächst klassifiziert werden (Tool Classification). Diese Klassifizierung betrachtet die Auswirkungen des Software-Tools auf das Projekt und legt fest ob und in welchem Umfang eine Tool-Qualifizierung erforderlich ist.
Für die Werkzeuge, die eine Auswirkung auf das Projekt haben können und bei denen eine Fehlfunktion nicht unmittelbar erkennbar ist, verlangen die Sicherheitsnormen den Nachweis der Vertrauenswürdigkeit. Dieser Nachweis wird durch die Qualifizierung (Tool Qualification) erbracht.
Ein Tool muss immer in seiner Einbettung im konkreten Entwicklungsprozess und dem Projektumfeld des Toolanwenders qualifiziert werden.
Um die Qualifizierung von Testwell CTC++ in sicherheitskritischen Projekten zu vereinfachen, bietet Verifysoft Technology ein Tool Qualification-Kit for Testwell CTC++ an. Das Qualification-Kit kann für die Normen EN 50128, ISO 26262 (Automotive), DO-178C (Luftfahrt) und IEC 61508 (Eisenbahn) eingesetzt werden.

Abbildung 1: Tool-Qualification-Kits für Testwell CTC++ Test Coverage Analyser

Wichtig in diesem Zusammenhang ist, dass Softwareentwicklungstools wie Testwell CTC++ (Software development tools) qualifiziert und nicht zertifiziert werden müssen. Zertifiziert werden muss die sicherheitskritische Software, die beispielsweise im Flugzeug oder Auto zum Einsatz kommt.

Tool-Klassifizierung (Tool Classification)

Die bei der Entwicklung sicherheitskritischer Software eingesetzten Tools müssen (wie oben erwähnt) zunächst klassifiziert werden.
Test-Coverage-Tools wie Testwell CTC++ zählen zu den „Verification Tools". Diese Werkzeuge können zwar keine Fehler in den Produktivcode einfügen, möglicherweise das Aufdecken im Produktivcode bereits vorhandene Fehler verhindern (z. Bsp. durch verfrühtes Beenden der Test wegen Anzeige einer zu hohen Test-Coverage).
Ergebnis der Klassifizierung ist die Entscheidung ob und in welchem Maße eine Qualifizierung des Tools für das konkrete Projekt erforderlich ist.
Die Klassifizierung der Softwaretools unterscheidet sich geringfügig für die Normen DO-178C, IEC 61508/EN 50128 und ISO 26262 (siehe Abbildung 2).

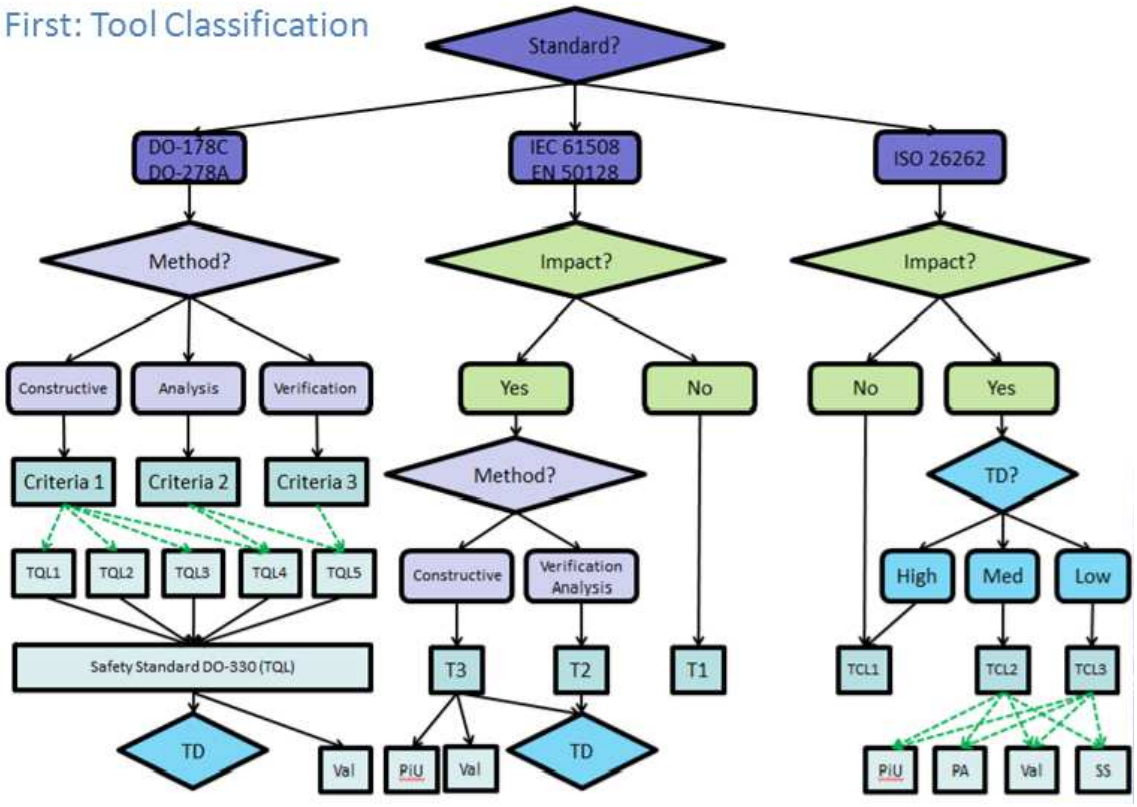

Abbildung 2: Übersicht Klassifizierung (Quelle: Validas AG, München)

Wir betrachten in der Folge die Automotive-Norm ISO 26262. Für die ISO 26262 (siehe rechter Teil der Abbildung 2) wird zunächst geprüft, ob das Tool einen Einfluss (Impact) auf die Software hat. Ist dies nicht der Fall, wird es als TCL1 (Tool Confidence Level 1) klassifiziert. Eine Qualifizierung ist bei TCL1 nicht erforderlich.
Falls das Werkzeug einen Einfluss auf das Softwareprojekt haben kann, muss geprüft werden wie hoch die Wahrscheinlichkeit (TD) ist, eine Fehlfunktion des Tools während dessen Anwendung aufzudecken. Ist die Wahrscheinlichkeit eine Fehlfunktion des Tools aufzudecken hoch, ist es damit TCL1 klassifiziert und eine Qualifizierung ist nicht erforderlich. Eine hohe Wahrscheinlichkeit Fehlfunktionen des Tools aufzudecken, ist beispielsweise dann gegeben, wenn zwei unterschiedliche Code-Coverage-Tools eingesetzt und deren Ergebnisse verglichen werden. Durch diese Redundanz kann die Tool-Qualifizierung umgangen werden.
Ist die Wahrscheinlichkeit Fehlfunktionen im Tool aufzudecken mittelgroß, liegt ein Tool Confidence Level 2 vor, bei einer niedrigen Wahrscheinlichkeit des Findens von Fehlfunktionen, dagegen ein Tool Confidence Level 3.

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

Tabelle 1: Bestimmung des Tool Confidence Levels (TCL)

Während beim Tool Confidence Level 1 (wie oben erwähnt) keine Tool Qualifizierung erforderlich ist, muss das Software Tool beim den Tool Confidence Levels 2 und 3 qualifiziert werden.

Beim Tool Confidence Level 2 erfolgt die Qualifizierung des Tools nach folgender Tabelle aus der Norm ISO 26262:

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.

Tabelle 2: Qualifizierung von Software-Tools, die TCL2 klassifiziert sind gemäß ISO 26262

Beim Tool Confidence Level 3 schreibt die ISO 26262 folgende Aktivitäten vor:

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.

Tabelle 3: Qualifizierung von Software-Tools, die TCL3 klassifiziert sind gemäß ISO 26262

Tool Qualifizierung durch Validierung (Tool Qualification by Validation)

Software-Tools werden unter anderem durch Validierung qualifiziert. Die ISO 26262 beschreibt im Punkt 11.4.9 die Validierung eines Software-Tools:
“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 für Testwell CTC++

Das von Verifysoft Technology in Zusammenarbeit mit der Münchener Validas AG erstellte Tool-Qualification-Kit for Testwell CTC++ verringert den Aufwand der Qualifizierung deutlich. Das Kit unterstützt den Nutzer bei der Qualifizierung von Testwell CTC++ für die sicherheitskritische Softwareentwicklung gemäß ISO 26262, DO-178C, IEC 61508 und EN 50128.
Das Qualification-Kit für Testwell CTC++ validiert das korrekte Ermitteln und Anzeigen von Statement-, Decision- und MC/DC-Coverage-Metriken durch Testwell CTC++ für die Programmiersprache C in Ihrer Entwicklungsumgebung.
Das Kit besteht aus dem Qualification-Support-Tool (QST), einer Vielzahl von Testfällen für die verschiedenen Use-Cases von Testwell CTC++, einer Test Automation Unit (TAU) zur Ausführung der Testfälle, einem Validation & Verification-Report (V&V-Report) zum Nachweis der Qualität des Qualification-Kits, sowie dem Benutzerhandbuch.

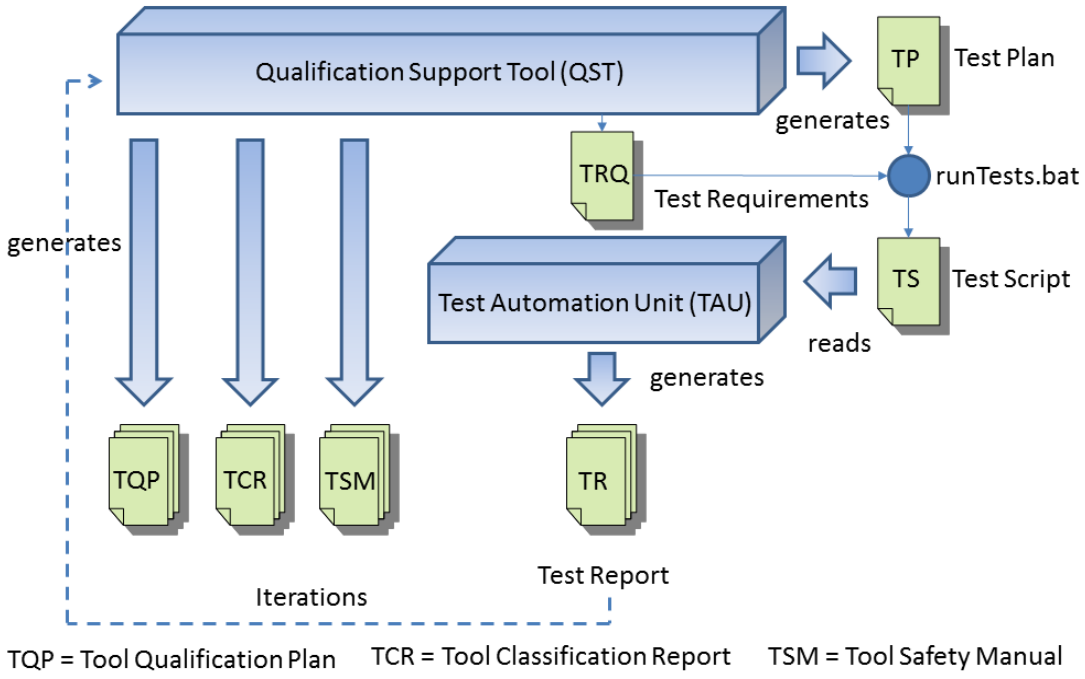

Abbildung 3: Tool-Qualification-Kit für Testwell CTC++

Anwendung des Tool-Qualification-Kits

Das Qualification-Support-Tool führt den Anwender durch den Qualifizierungsprozess. Zunächst wird die relevante Norm ausgewählt (siehe Abbildung 4).

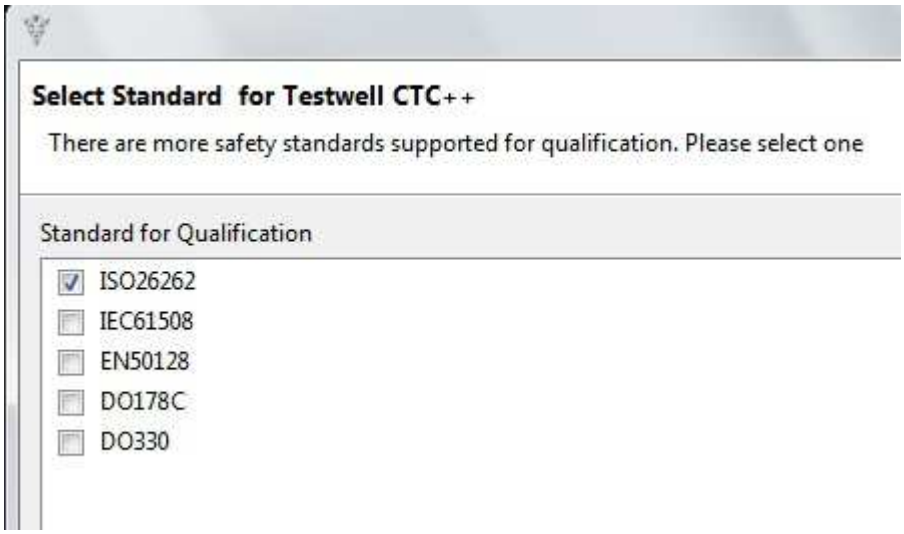

Abbildung 4: Auswahl der relevanten Norm im Qualification-Kit

Im nächsten Schritt wählt der Anwender die genutzte Variante von Testwell CTC++ (nur Host, CTC++ mit Host-Target-Add-on für die Messung der Test-Coverage auf dem Target oder CTC++ mit Bitcov-Add-on für die Messung der Testabdeckung auf Targets mit sehr geringem Speicherplatz (siehe Abbildung 5).

Abbildung 5: Auswahl der Testwell CTC++-Variante

In einem weiteren Schritt erfolgt die Auswahl der zu qualifizierenden Version von Testwell CTC++ (siehe Abbildung 6).

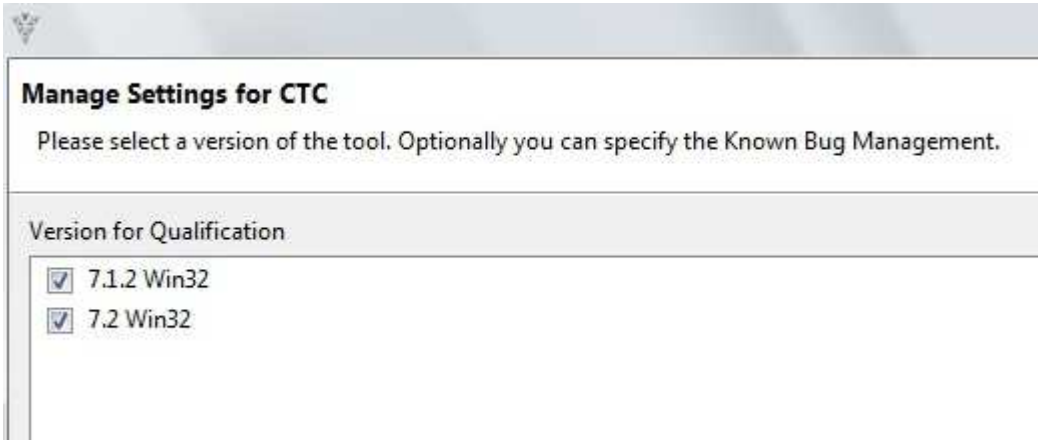

Abbildung 6: Auswahl der Testwell CTC++-Version

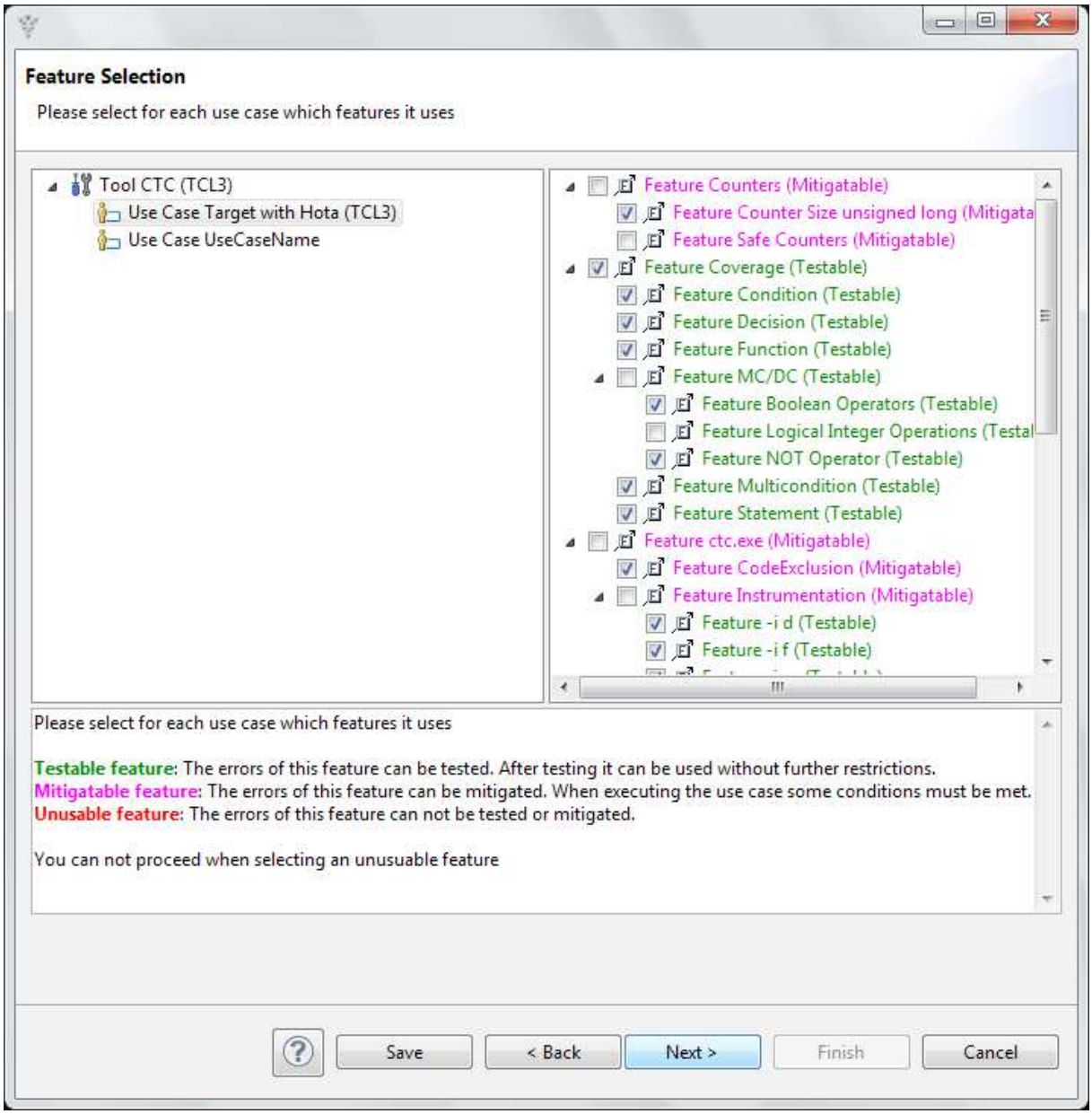

Abbildung 7: Auswahl der genutzten Features

Danach wählt der Anwender die genutzten Features des Tools Testwell CTC++ aus (siehe Abbildung 7). Es müssen nur die Features qualifiziert werden, die auch tatsächlich im Projekt genutzt werden. Je nach Standard und Sicherheitsanforderungsstufe sind die genutzten CTC++-Features bereits vorausgewählt. Ebenfalls sind die nötigen Mitigations bereits vorselektiert.
Features, die nicht überprüft worden sind, dürfen im konkreten sicherheitskritischen Projekt nicht genutzt werden. Das Qualification-Support-Tool generiert einen entsprechenden Hinweis im Tool Safety Manual.
Die Features, für welche Testfälle existieren sind im Qualification-Support-Tool grün gekennzeichnet. Für die violetten Features existieren Mitigations.
Die Mitigations und Testfälle sind im nächsten Schritt (Abbildung 8) vorausgewählt. Bei Bedarf besteht hier besteht die Möglichkeit anstatt der vorausgewählten Fälle andere geeignete Mitigations oder Testfälle auszuwählen.

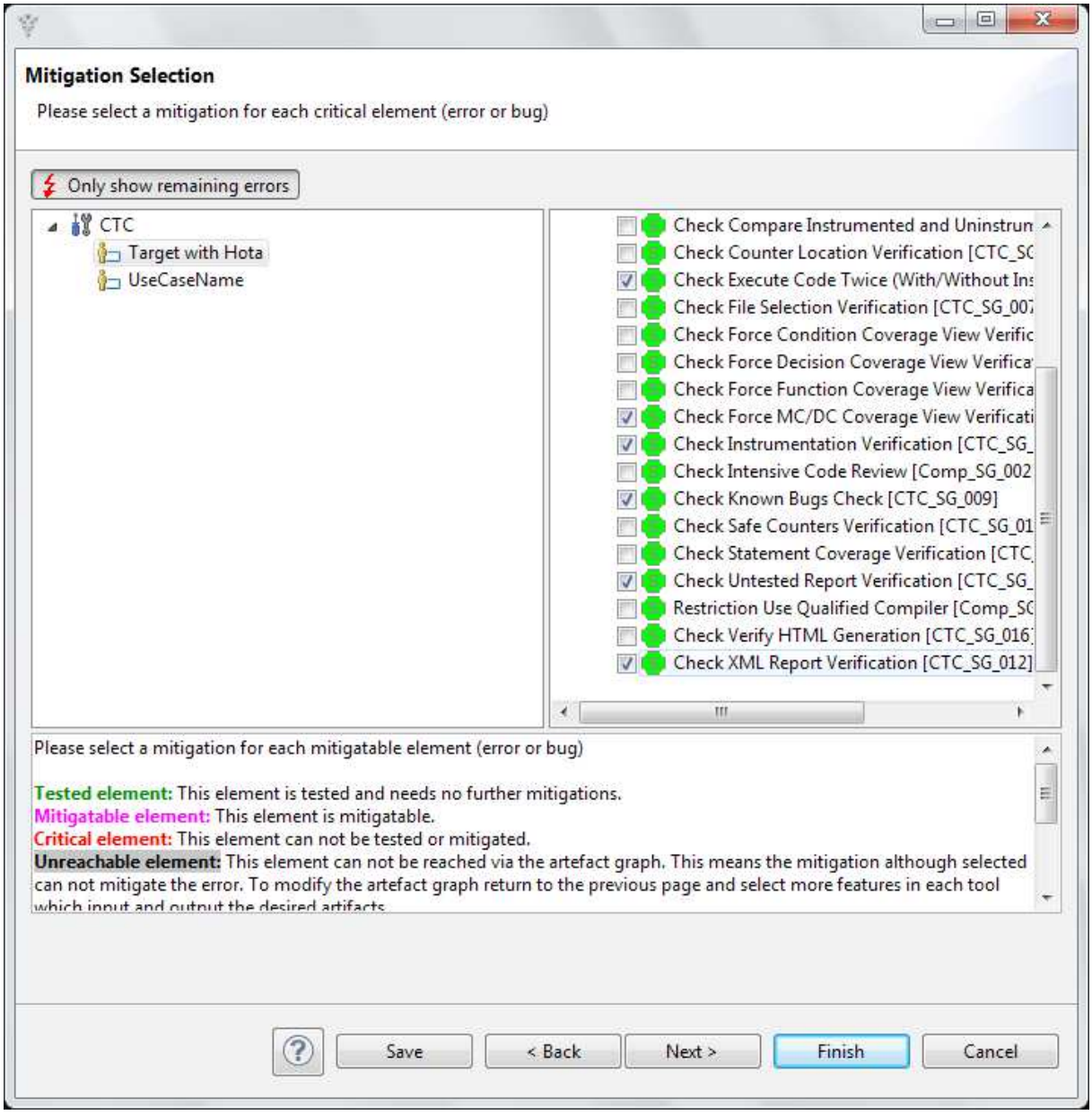

Abbildung 8: Auswahl der Mitigations

In der nächsten Auswahl kann die Qualifizierung geplant werden (siehe Abbildung 9). Hier wird festgelegt wer was wann durchzuführen hat.

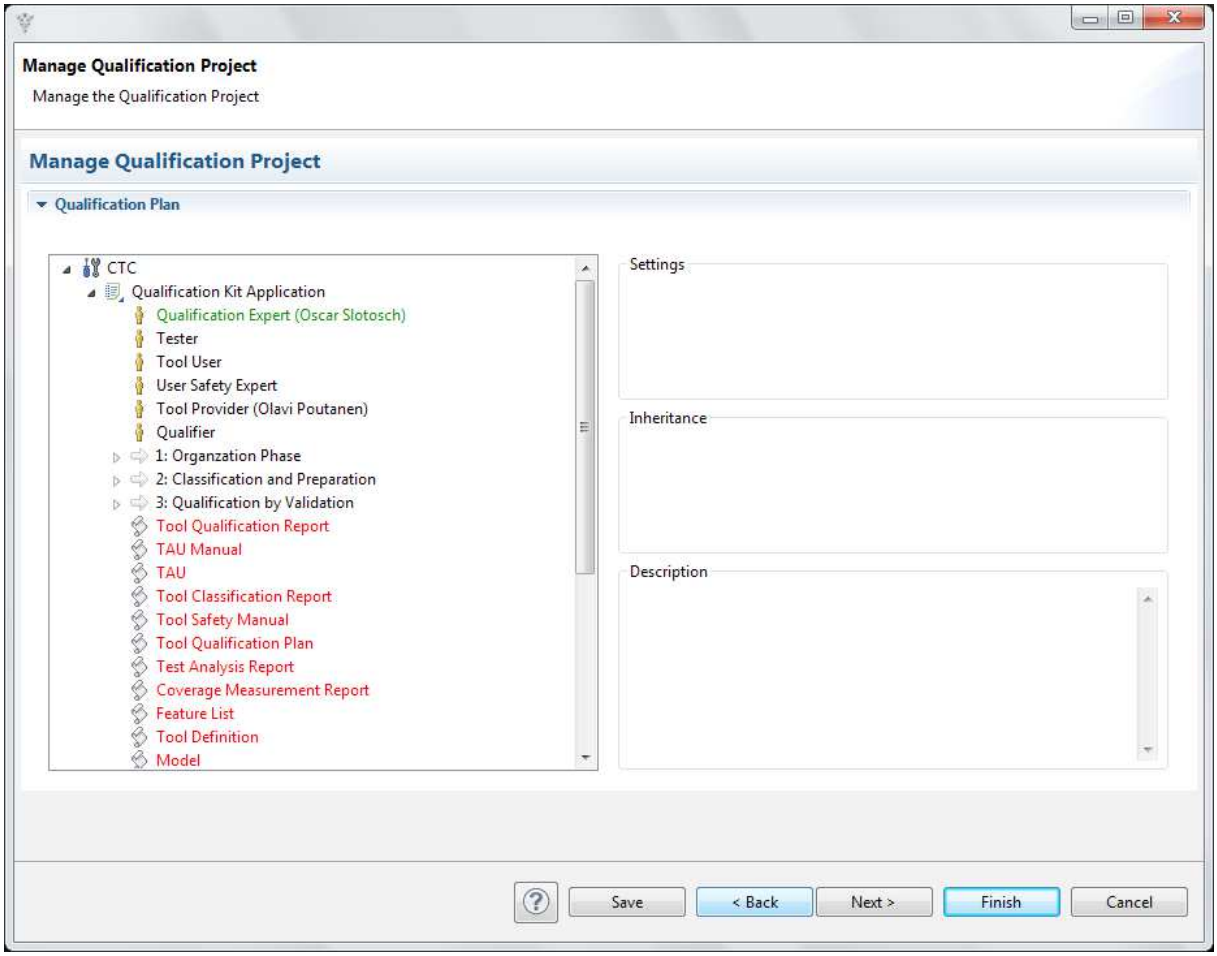

Abbildung 9: Planung der Qualifizierung

Die dann folgende Ansicht zeigt eine Zusammenfassung mit Anzeige der Anzahl der Features, der ausgewählten Checks, der Anzahl der Tests sowie den Ort an denen die generierten Dokumente hinterlegt werden (Abbildung 10).

Nach dem Drücken der „Finish“-Taste erfolgt die Generierung von verschiedenen Dokumenten wie dem Tool Classification Report (TCR.docx), dem Tool Qualification Plan (TQP.docx) und dem Tool Safety Manual (TSM.docs), sowie von verschiedenen Dateien wie den Test-Run-Dateien, der Test Execution.txt und den tool-config-Dateien. Eine Auswahl von generierten Dokumenten und Dateien wird in Abbildung 11 gezeigt.

Durch Ausführen der Testrun.bat wird ein Testskript generiert. Dieses wird durch die Test Automation Unit (TAU) eingelesen und ausgeführt (siehe Abbildung 12) und die generierten Dokumente entsprechend aktualisiert. Wenn die Tests erfolgreich ausgeführt wurden, ist damit der Nachweis erbracht, dass Testwell CTC++ fehlerfrei in Ihrer Umgebung arbeitet.

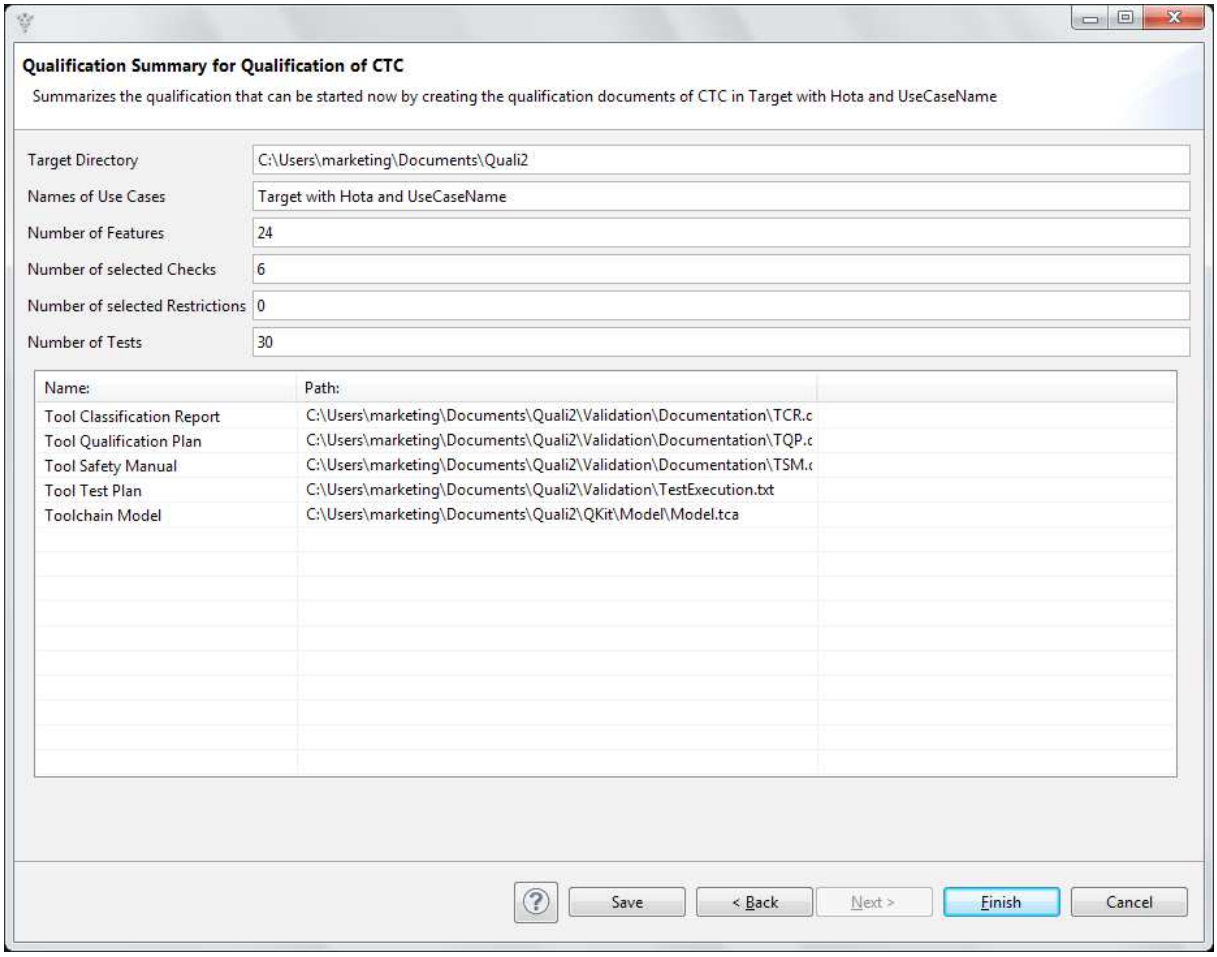

Abbildung 10: Zusammenfassung der Qualifizierung

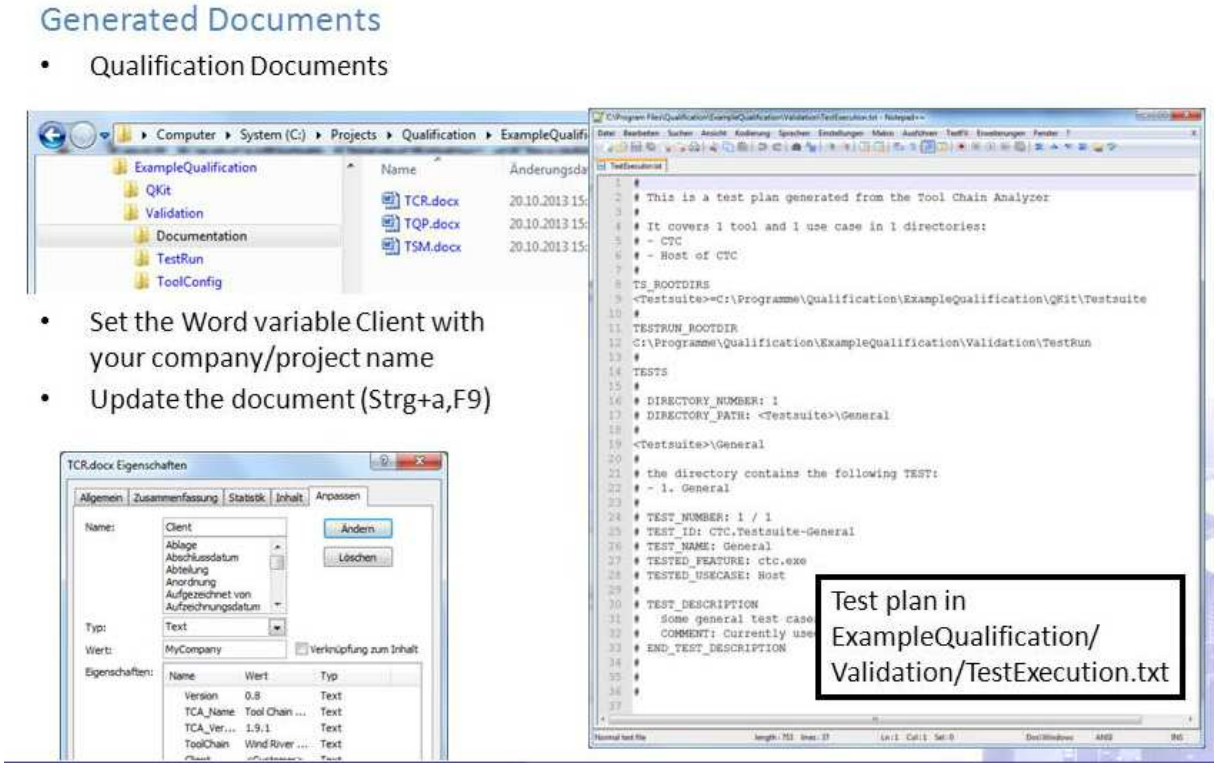

Abbildung 11: Auswahl von durch das Qualification Support Tool generierten Dokumente

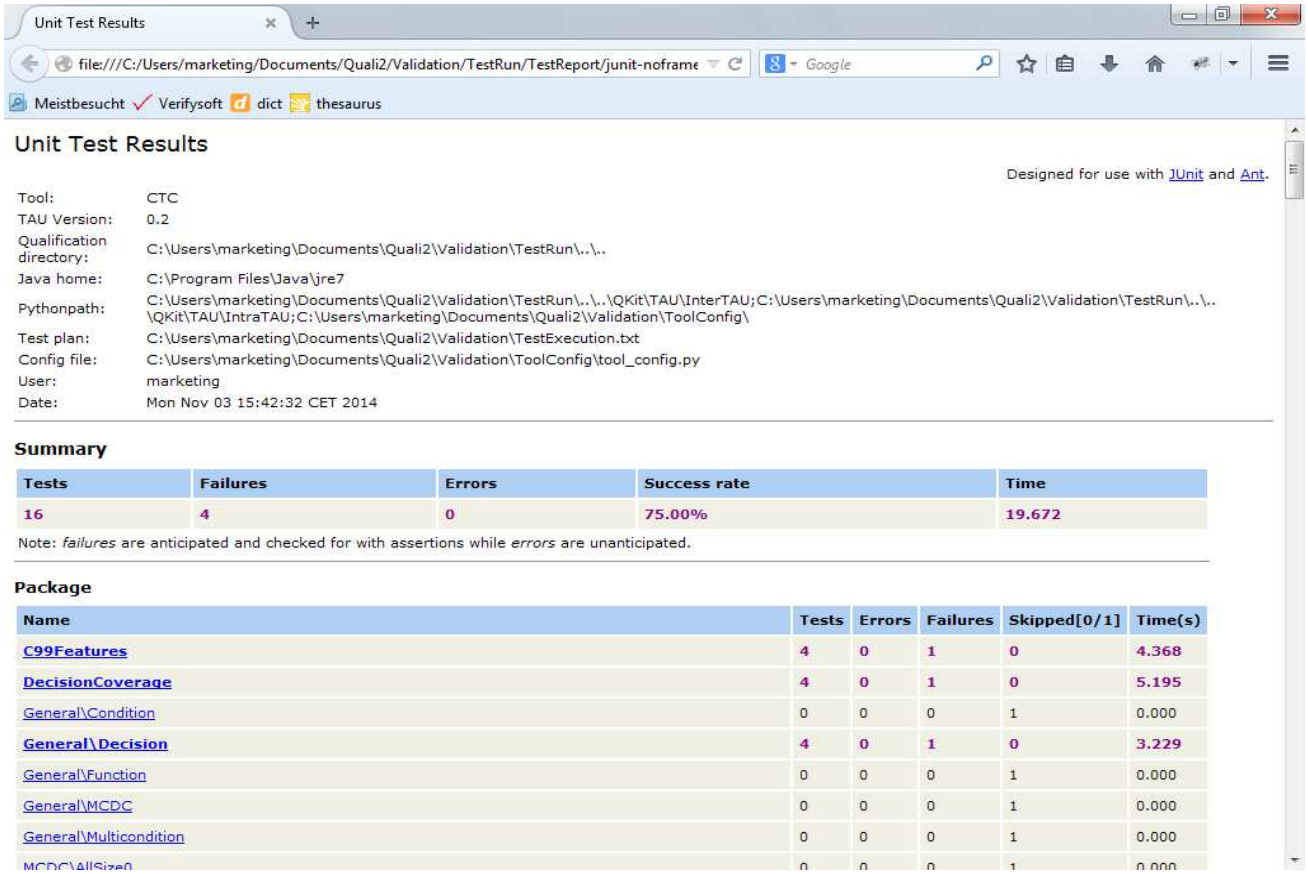

Abbildung 12: Ergebnis der Testläufe

Für weitere Informationen kontaktieren Sie bitte:
Verifysoft Technology GmbH
In der Spöck 10-12
77656 Offenburg
Deutschland

www.verifysoft.com
Telefon +49 781 127 8118-0

Stand: 17. November 2014