AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

WEFACT

SIND IHRE ZERTIFIZIERUNGSPROZESSE EFFIZIENT UND EFFEKTIV?

PROBLEMSTELLUNG

Bei der Verifikation, Validierung (V&V) und Zertifizierung von sicherheitsrelevanten Systemen treten typischerweise die folgenden Fragestellungen auf:

1. Nach welchen Functional-Safety-Standards bzw. Security-Standards wird zertifiziert?
   Die Functional-Safety-Standards (z.B. IEC 61508) vergeben Safety-Integrity-Levels, um den Grad der Safety-Relevanz des Systems anzugeben, was zu einer Reihe von weiteren Safety-Requirements führt, die das System erfüllen muss. Die Security-Standards (z.B. ISO 15408) vergeben Evaluation-Assurance-Levels, um den Grad der Erfüllung der Common-Criteria für die Bewertung der Security des Systems anzugeben, was zu den Assurance-Requirements führt.

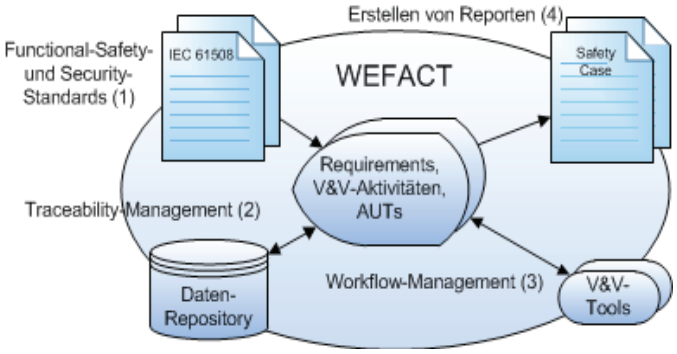
2. Wie werden die Requirements verwaltet?
   Bei der Verwaltung von Requirements ist das Traceability-Management ein wesentlicher Punkt, d.h. es muss gewährleistet sein, dass das Requirement mit den entsprechenden Artifacts-under-Test (AUT) sowie den V&V-Aktivitäten verbunden ist, sodass Änderungen nachvollzogen werden können.

3. Wie wird der Workflow definiert?
   Der Workflow sollte möglichst automatisiert sein, z.B. die Integration von V&V-Tools, um vor allem Regressionstests effizient gestalten zu können.

4. Wie werden Reporte erstellt?
   Es sollte möglich sein, verschiedene Arten von Reporten (z.B. Safety-Case, Requirement-Spezifikation) zu konfigurieren und auf Knopfdruck zu erstellen.

Die aktuell am Markt verfügbaren Tools zur Zertifizierung/Erstellung von Safety-Cases bzw. Security-Cases decken die obigen Fragestellungen nicht ausreichend ab.

Das AIT Austrian Institute of Technology hat auf Basis verschiedenster Industrieprojekte ein methodisches Vorgehen einschließlich zugehöriger Toolkette zur Zertifizierung sicherheitsrelevanter Systeme entwickelt: WEFACT (Workflow Engine for Analysis, Certification and Test). Die Nummern in der Abbildung beziehen sich auf die dazugehörigen Fragestellungen.



NUTZEN

- Reduktion der Kosten und des Aufwands bei der Zertifizierung von sicherheitsrelevanten Systemen
- Automatisierte Erstellung von Safety- und Security-Cases auf Basis der Functional-Safety- und Security-Standards
- Transparente Verwaltung der Requirements mit Traceability-Management
- Definition eines Workflows für die Durchführung von V&V-Aktivitäten

AIT LEISTUNGEN

- Tool: Lizenzierung und Betrieb von WEFACT auf Basis von IBM Rational DOORS®
- Service: Analyse und Anpassung von bestehenden Zertifizierungsprozessen

WEFACT

SIND IHRE ZERTIFIZIERUNGSPROZESSE EFFIZIENT UND EFFEKTIV?

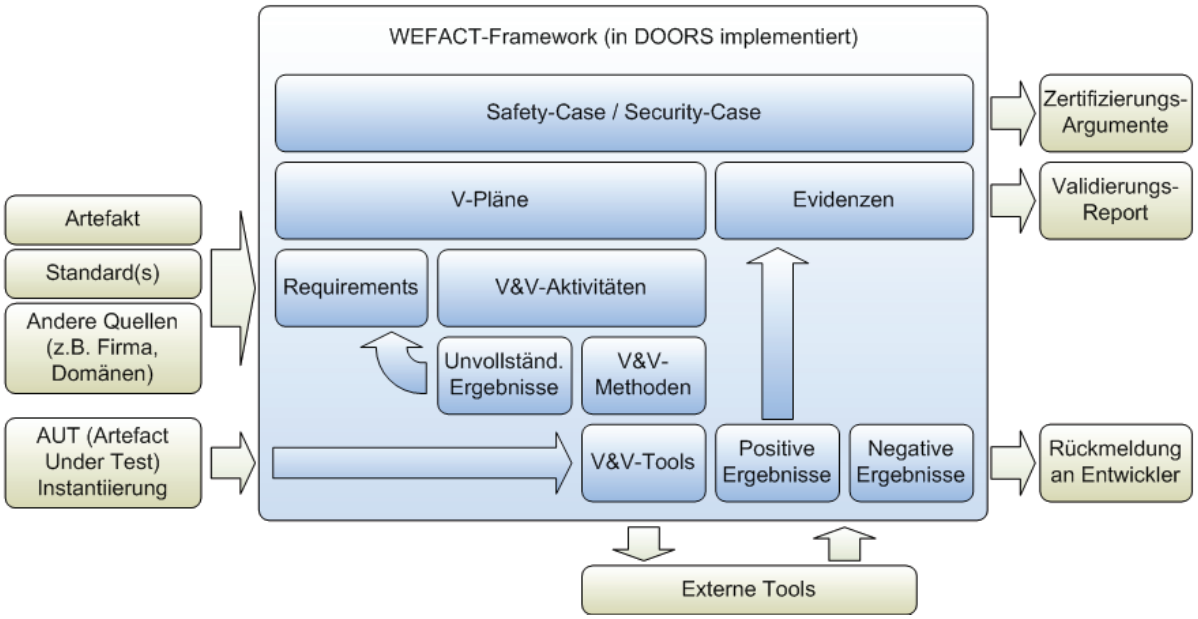
METHODIK

WEFACT besteht aus, dem WEFACT-Framework, das eine flexible Infrastruktur zur Verfügung stellt, um V&V-Prozesse zu definieren und auszuführen. Externe Ressourcen – externe Prozesse, Tools und Standards – sind über standardisierte Interfaces in das WEFACT-Framework eingebunden.

Der Safety-Case bzw. Security-Case ist der zentrale Output von WEFACT und fasst alle Informationen des V&V-Prozesses in Form von Zertifizierungs-Argumenten zusammen und dient als Basis für die Zertifizierung des Artefact-under-Test (AUT).

Der Validierungs-Plan (V-Plan) besteht aus den Requirements für das AUT sowie den V&V-Aktivitäten, die notwendig sind, um die Requirements zu erfüllen. Eine V&V-Aktivität ist die Anwendung einer V&V-Methode mittels eines passenden V&V-Tools.

Es können verschiedene externe Tools angebunden werden. Positive Resultate der V&V-Aktivität werden als Evidenz für die Requirements herangezogen, wohingegen negative Resultate dem Entwicklerteam rückgemeldet werden.



KONTAKT

AIT Austrian Institute of Technology
Center for Digital Safety & Security
Donau-City-Straße 1, 1220 Vienna

CHRISTOPH SCHMITTNER, MSC

Scientist
Phone: +43(0) 50550 - 4244
Fax: +43(0) 50550 - 4150
E-mail: christoph.schmittner@ait.ac.at
Web: www.ait.ac.at/wefact

DI JOHANNES PRIBYL

Engineer
Phone: +43(0) 50550 - 4144
Fax: +43(0) 50550 - 4102
E-mail: johannes.pribyl@ait.ac.at
Web: www.ait.ac.at/v&v