AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

WEFACT

ARE YOUR CERTIFICATION PROCESSES EFFICIENT AND EFFECTIVE?

PROBLEM STATEMENT

During verification, validation (V&V) and certification of safety relevant systems, the following questions typically occur:

1. According to which functional safety and security standards do you certify?
   The functional safety standards (e.g. IEC 61508) assign safety integrity levels in order to determine the level of safety relevance of the system, which leads to a series of further safety requirements for the system. The security standards (e.g. ISO 15408) assign evaluation assurance levels in order to determine the level of completion of a common criteria security evaluation of the system, which leads to the assurance requirements.

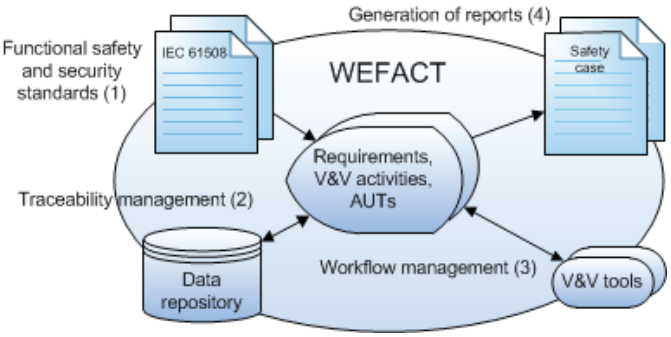
2. How do you manage the requirements?
   One of the major topics for requirements management is the traceability management, which provides guarantee that the requirement is linked to the associated artefact under test (AUT) as well as to the V&V activities in order to reproduce the changes.

3. How do you define the workflow?
   The workflow should be automated as much as possible.For example, V&V tools shall be integrated in order to efficiently execute regression tests.

4. How do you generate reports?
   It should be possible to configure various types of reports (e.g. safety case, requirement specification) and to generate them at the push of a button.

The tools for certification/generation of safety cases and security cases which are actually available on the market do not sufficiently cover the questions stated above.

AIT Austrian Institute of Technology developed a methodology-based approach for the certification of safety relevant systems. This approach is based on various industrial projects and includes the tool chain WEFACT (Workflow Engine for Analysis, Certification and Test). The numbers in the Figure refer to the associated questions.



BENEFIT

- Reduction of costs and effort for the certification of safety relevant systems
- Automated generation of safety and security cases on the basis of functional safety and security standards
- Transparent management of requirements using traceability management
- Definition of workflow for processing V&V activities

AIT SERVICES

- Tool: Licencing and deployment of WEFACT on the basis of IBM Rational DOORS®
- Service: Analysis and adaptation of existing certification processes

WEFACT

ARE YOUR CERTIFICATION PROCESSES EFFICIENT AND EFFECTIVE?

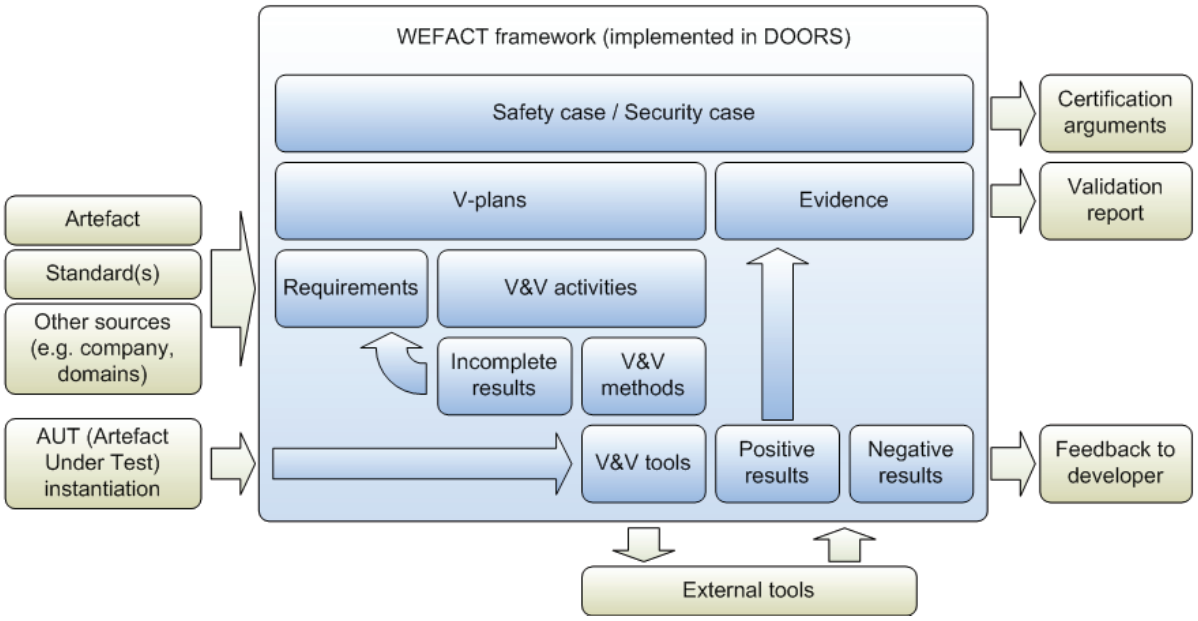
METHODOLOGY

WEFACT consists of the WEFACT framework which provides a flexible infrastructure for defining and executing V&V processes. External resources – external processes, tools and standards – are integrated into the WEFACT framework by well-defined interfaces.

The safety case or security case respectively is the central output of WEFACT. It summarizes the information of the V&V process and provides a basis for the certification of the artefact under test (AUT).

The validation plan (V-plan) consists of the requirements for the AUT as well as the V&V activities which are necessary in order to satisfy those requirements. A V&V activity is the application of a V&V method by means of an appropriate V&V tool.

It is possible to integrate various external tools. Positive results of the V&V activity are used to establish evidence for the requirements, while negative results are fed back to the developer team.



CONTACT

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

AIT Austrian Institute of Technology · v2.2 · © 29062015 · Errors excepted. Images: AIT