What about ISO26262?

JIRA/Confluence: How to get compliant to ISO26262-8?

Johannes Fürtler

Agenda

- ALM Disciplines in Scope
- Problem Statement
- Overview ISO26262-8:2011
- Proposed Solution / Examples
- Discussion

ALM Disciplines in Scope

- Requirements Management
- Change Management
- Test Management
- Defect Management
- Task Management
- Project Management
- Risk Management
- Configuration, Build and Release Management
- Collaboration and Communication
- Quality Management and Compliance

Problem Statement

- Standards define requirements for development of safety-related systems typically define required confidence levels for the software tools used to develop those systems
- The standards (more or less) define procedures to classify, validate and certify tools
- ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electric / electronic systems within road vehicles
  - This adaptation applies to all activities during the safety lifecycle of systems composed of electrical, electronic, and software elements that provide safety-related functions.
- Clause 11 of ISO 26262-8 provides guidance on software tool classification and qualification
- Confidence is needed that the software tool achieves the goals:
  - Minimize the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs
  - The development process is adequate with respect to compliance with ISO 26262, if activities or tasks required by ISO 26262 rely on the correct functioning of the software tool used
- ISO 26262 allows different levels of qualification, including a self -qualification by the tool user (first party qualification).
- **Users of COTS tools expect the tool vendor to provide a “tool qualification package” to reduce efforts**

Qualification Artifacts

- The ISO 26262 tool qualification process requires the creation of two tool qualification artifacts:

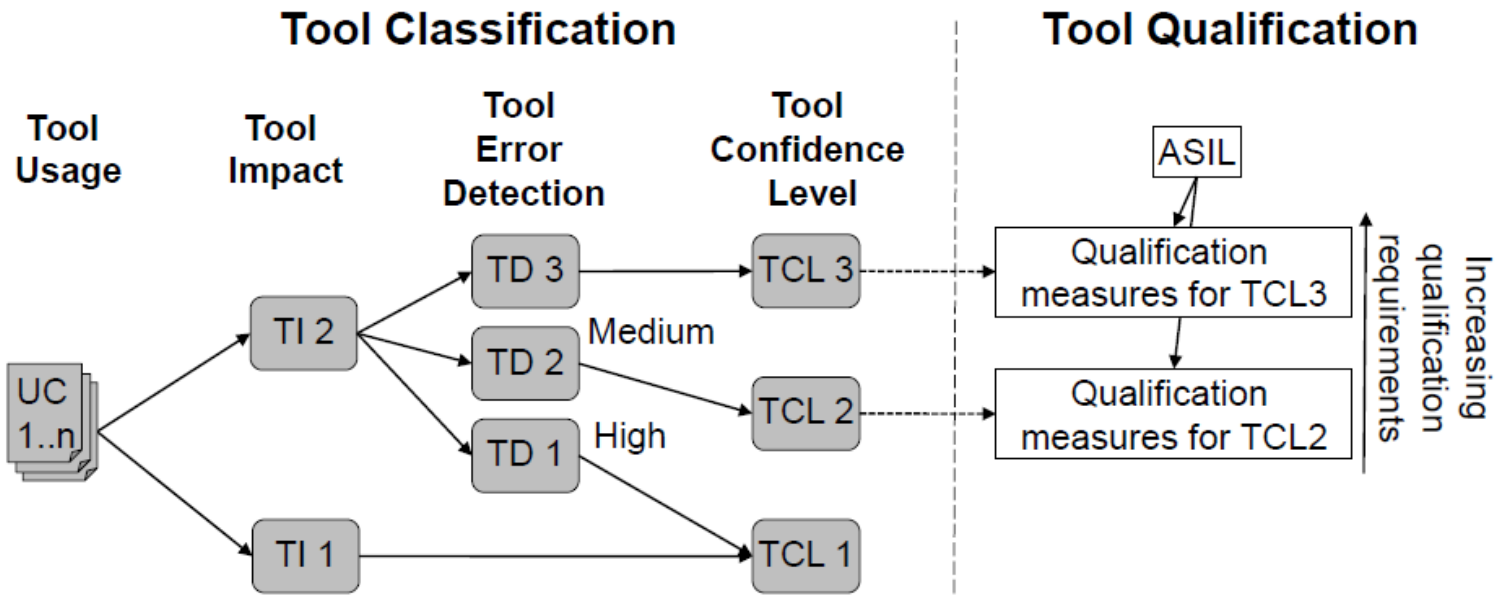
1. Tool Classification - a **Criteria Evaluation Report** documenting the tool classification
   - The intended usage of the tool (use cases)
     - The possibility that a malfunction in the software tool can introduce or fail to detect errors in the safety-related system being developed
     - Two Tool Impact classes (TI1 or TI2)
   - The confidence in measures to prevent or detect malfunctioning and corresponding erroneous output
     - Three Tool Error Detection classes (TD1, TD2 or TD3).
   - As a result of this analysis, a required Tool Confidence Level is determined.
     - Three Tool Confidence Levels TCL1, TCL2, or TCL3.
2. Tool Qualification - a **Qualification Report** documenting the tool qualification
   - Tools with the lowest possible TCL (i.e., TCL 1) do not require subsequent tool qualification
   - For all other TCLs, formalized tool qualification is required
   - The selection of appropriate tool qualification methods depends on
     - the required TCL and
     - on the Automotive Safety Integrity Level (ASIL) of the safety-related software to be developed using the software tool

Software Tool Criteria Evaluation Report

- Tool Use Cases (UC)
  - The evaluation results depend on how the tool is being used during the development of the safety-related system.
- Tool Impact (TI)
  - It shall be evaluated whether a malfunction in the software tool can introduce or fail to detect errors in the system being developed.
  - If it can be argued that malfunctions in the tool cannot introduce errors in the system or prevent those errors from being detected, Tool Impact class TI1 shall be chosen. Otherwise, the tool impact class is TI2.
- Tool Error Detection (TD)
  - The use cases for the software tool shall be analyzed to determine the confidence in measures that
    - Prevent the software tool from malfunctioning and producing erroneous output or
    - Detect that the software tool has malfunctioned and produced erroneous output
  - Both tool-internal measures (e.g., monitoring) and tool-external measures implemented as part of the software lifecycle (e.g., guidelines, tests, and reviews) to prevent or detect errors should be considered in the analysis.
  - The degree of confidence in the prevention and detection measures determines the Tool Error Detection class. Class TD1 shall be selected if there is a high degree of confidence, TD2 if there is a medium degree of confidence, and TD3 in all other cases.

Software Tool Criteria Evaluation Report

- Tool Confidence Level (TCL)
  - When TI and TD have been identified, the *tool confidence level* can be determined following the schematic provided in the left hand side of the figure. When multiple use cases for a tool exist, there can be multiple TCLs. To determine the required tool qualification measures, the maximum TCL required (TCLREQ) to support these use cases needs to be established.



Software Tool Qualification Report

- A tool classified as TCL1 does not require specific *tool qualification methods* to be carried out
- For software tools classified at TCL2 or TCL3, at least one dedicated *tool qualification method* has to be applied (see right hand side of the figure. The four permitted methods are
  1. *Increased confidence from use*,
  2. *Evaluation of the tool development process*,
  3. *Validation of the software tool*, and
  4. *Development in accordance with a safety standard*
- The selection of a method is guided by the ASIL classification of the application to be developed and the required TCL resulting from the tool classification
- The software tool qualification report documents the actual tool qualification
  - The selected tool qualification methods must be documented
  - it provides evidence that the tool qualification methods were carried out as planned
  - usage constraints and malfunctions identified during the qualification - if any - need to be documented

Proposed Solution / Examples

- ISO 26262 calls for a project-specific classification and qualification of software tools where applicable.
  - However, qualification only makes sense if it can be leveraged by several customers and on multiple projects.
- Goals
  1. Prequalification which can be applied and tailored by the tool user
  2. Tool Qualification Kit - Example Tool Qualification Kit, Press Release
     - Standard set of Use Cases
     - Inherent traceability
     - Historical data
     - Audit reporting
     - Reference Workflows
     - Templates for all tool qualification artifacts
- Is there a need? Yes → BSERV-9720, CONFSERVER-51919

Discussion

- Compliance to international standards is paramount to development of safety-critical elements, including facilitating the presentation of comprehensive and persuasive safety cases to regulators and assessors.
- What are your needs?
- What are your experiences?

References

- “Software Tool Qualification According to ISO 26262”, Mirko Conrad et al., The MathWorks Inc., 2011


kapsch
challenging limits
Thank you!
Johannes Fürtler