Tool Qualification Considerations for Tools Supporting STPA
Sven Stefan Krauss, Martin Rejzek, Christian Hilbes
Zurich University of Applied Sciences, Switzerland
Agenda

Introduction ➔ Tool Qualification Overview ➔ Tool Qualification for STPA tools ➔ Conclusion Discussion
Applied Research Project

Integration of STPA as a safety analysis method in our partner’s engineering development lifecycle, by

- industrial case study how STPA can be applied for system components engineering for multiple safety domains (confidential), and
- the development and integration of an STPA tool in the partner’s engineering toolchain based on the experience gained from the case study and previous STPA projects [8], [9] and [10].
Safety Domains

Industrial & Special Applications
IEC 61508 [15]

Railway
EN 50128 [16]

Aerospace & Defense
RTCA/DO-178C [17]
RTCA/DO-330 [18]
IEC 61508 [15]
MIL-STD 882 [29]
System and Safety Engineering

System / HW / SW-Engineer
Model based development
- Design with UML/SysML
- Documentation
- Simulation, Verification
- Code Generation

Safety Engineer
Hazard & Risk Analysis
- FMEA
- FTA
- HAZOP

UML Tools
- Sparx Systems Enterprise Architect [12]
- Many others…

Software Tools supporting STPA
- SafetyHAT [5]
- MIT STPA Tool [6]
SAHRA [7] – An Integrated STPA Tool
SAHRA – STPA based Hazard and Risk Analysis

STPA integrated into UML modeling tool
- Developed as extension (plugin) for UML tool Sparx Systems Enterprise Architect [12]
- Includes UML Profile for STPA data items

SAHRA Features
1. Support for Multi Level Hierarchical Control Structures with diagram checks during modeling
2. Context sensitive element editors for STPA data items and relationship analyzer to show related data for traceability
3. Graphical safety net editor with drag’n’drop support and relationship analyzer for STPA Step 1
Integration Advantages

- Sparx System Enterprise Architect Corporate Edition provides multi user support with security permission system and configuration management integration for process control
- Requirements, Design and STPA data items are in one single repository which enables full end-to-end traceability
Research Questions

SAHRA is used for safety analysis of system components in multiple safety domains.

a) What are the tool qualification requirements in the respective safety standards?

b) What are the effects of tool errors in safety analysis tools like STPA tools?

c) Is tool qualification required or recommended and when yes to what level?
Research Questions

a) What are the tool qualification requirements in the respective safety standards?
Software Tool Qualification

- Risk assessment of whether an engineering software tool may have a negative impact on safety

- Malfunctioning engineering tools can influence the final safety-related system by
  - introducing errors or
  - failing to detect errors
Do you rely on software tools?

Software Tool Qualification
Survey about Tool Qualification according to DO-178B [20], Section J:

Development Tools
- ~44% of survey respondents with experience with tool qualification found errors in a development tool during tool qualification

Verification Tools
- 57% of survey respondents with experience with tool qualification found errors in a verification tool during tool qualification
Software Tool Qualification

Typical Tool Qualification Methods

Tool validation
- Requirements based testing of tool operational requirements which specify tool behavior

Increased confidence from use
- The software tool has a extensive history of successful use

Tool error detection means
- Built-in functionality to prevent or to detect tool errors like diverse redundant code

Tool development according to a safety standard
- Software tool was developed according to a safety standard to avoid systematic errors
Tool Qualification Overview

Industrial / Generic
- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Railway
- EN 50128 [16]

Aerospace & Defense
- DO-178C [17]
- DO-330 [18]

Automotive
- ISO 26262 Part 8 [19]

For more details: [22]
Generic Safety Standard
IEC 61508

Industrial / Generic
- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Tool classes
- T1 – Tool has no direct or indirect impact
- T2 – Tool may fail to detect errors
- T3 – Tool may introduce errors

Qualification Requirements
- Mandatory for tools of class T3
- Recommended for tools of class T2
- Specification or manual which defines tool behavior
- Safety assessment and mitigation action

Tool Qualification Methods
- Increased confidence from use
- Tool validation
Railway EN 50128

Qualification Requirements

- Mandatory for tools of class T3
- Recommended for tools of class T2
- Specification or manual which defines tool behavior
- Safety assessment and mitigation action

Tool Qualification Methods

- Increased confidence from use
- Tool validation
- Tool error detection means

Tool classes

- T1 – Tool has no direct or indirect impact
- T2 – Tool may fail to detect errors
- T3 – Tool may introduce errors

Railway

- EN 50128 [16]
Aerospace & Defense
DO-178C [17], DO-330 [18]

Aerospace & Defense

• DO-178C [17]
• DO-330 [18]

Qualification Requirements

- Depend on Tool Qualification Level (TQL)
- DO-330 provides set of objectives for each TQL

Tool Qualification Level

Tool Qualification Level TQL-1 to TQL-5 is defined by tool criteria and safety level:

- Criteria 1 – Tool may insert error
- Criteria 2 – Tool automates or eliminates verification or development process steps
- Criteria 3 – Tool may fail to detect an error
- Safety Level A (most critical) to Level D

Tool Qualification Methods

- Tool validation
- Tool development according to safety standard DO-330 (tool developers)
Automotive
ISO 26262-8 [19]

Tool Confidence Level

Tool Confidence Level TCL1 to TCL3 is defined by tool impact TI and Tool error detection TD level:
- TI – Tool impact
- TD – Confidence level if tool error can be detected or prevented

Qualification Requirements
- Depend on Tool Confidence Level (TCL) and safety level
- Recommended and highly recommended qualification methods depending on safety level

Tool Qualification Methods
- Increased confidence from use
- Tool validation
- Evaluation of tool development process
- Tool development according to a safety standard (tool developers)
Research Questions

b) What are the effects of tool errors in safety analysis tools like STPA tools?

c) Is tool qualification required or recommended and when yes to what level?
Generic Safety Standard
IEC 61508

Industrial / Generic
- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Tool classes
- T1 – Tool has no direct or indirect impact*
- T2 – Tool may fail to detect errors ❌
- T3 – Tool may introduce errors ❌

*Listed examples for T1:
- Requirement Management Tool
- Modeling tool without code generation

Really?
- Do tool errors in safety analysis tools have a direct or indirect impact on safety?
- Hypothesis: YES!
- Detailed analysis required!
Do we need to qualify STPA tools?
Effect of tool errors

Tool classification problem

IEC 61508: Tool class is selected according to tool class description and listed examples (i.e. Requirements Management Tool, Modeling tool without code generation)

1. Selected tool class is T1
2. No tool qualification is required
3. No tool risk analysis is required
4. No mitigation actions in place for risks caused by tool errors even when they would have an direct or indirect impact on safety!
Do we need to qualify STPA tools?
Effect of tool errors

Role of tool errors in safety analysis tools

To understand the effect of tool errors in safety analysis tools (here: STPA) we have to consider:

**Process Risks**
- Process risk analysis of safety analysis process (here: STPA) in the development lifecycle with STPA (Meta-Analysis)

**Tool & Integration Risks**
- Risk analysis of automating or supporting safety analysis process (here: STPA) with a tool

**Tool Operational Scenarios**
- Look at how the tool is used in the lifecycle (intended use)
Do we need to qualify STPA tools?

**Process Risks**

Simplified development lifecycle model:

- Requirements drive design
- Design is analyzed with safety analysis
- Safety analysis generates new requirements
- Requirements drive design
- ...

...until design is safe
Do we need to qualify STPA tools?

Process Risks?
Detail analysis with STPA

Controller
- Requirements Engineering (Requirements)
- STPA (Safety Analysis)
- System/Hardware/Software Engineering (Design)

Controlled Process
- Safe Design (System, Hardware, Software)

Control Actions
- Requirements (Safety, System, …)
- Safety Constraints
- Risk Control Measures
- Take Design Decisions
- Modify Existing Design
- …
Do we need to qualify STPA tools?

Process Risks?

Detail analysis with STPA Step 1.

Summary next slide.

STPA Step 1 safety nets show only a small subset of complete analysis.
## Identified Process Risks

### Analysis Summary

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Hazard</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR1</td>
<td>safety constraints and safety requirements are <strong>not provided</strong> or <strong>provided too late</strong> either to the system, hardware and software engineering when needed to make <strong>design decisions</strong></td>
<td>Unsafe Design, Incomplete Design</td>
<td>Unsafe System, Incomplete System</td>
</tr>
<tr>
<td>PR2</td>
<td>risk control measures and risk mitigation measures are <strong>not provided</strong> or <strong>provided too late</strong> to the system, hardware and software engineering when needed to make <strong>design decisions</strong></td>
<td>Unsafe Design</td>
<td>Unsafe System</td>
</tr>
<tr>
<td>PR3</td>
<td>trace data is <strong>incomplete</strong> or <strong>incorrect</strong> when needed for modification <strong>change impact analysis</strong></td>
<td>Unsafe Modification</td>
<td>Unsafe System</td>
</tr>
</tbody>
</table>
Do we need to qualify STPA tools?

Tool & Tool Integration Risks

Causal Factors [25-28]:

- Lack of Data Integrity
- Lack of Traceability for Completeness and Consistency
- ...

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR1</td>
<td>Analysis data items (i.e. safety requirements, safety constraints, risk control and mitigation measures) are incomplete or corrupt (→PR1, →PR2)</td>
</tr>
<tr>
<td>TR2</td>
<td>Trace data is incomplete or corrupt (→PR3)</td>
</tr>
<tr>
<td>TR3</td>
<td>Corrupt data items are used for verification (→PR1)</td>
</tr>
<tr>
<td>TR4</td>
<td>Corrupt data items are used for code generation (→PR1)</td>
</tr>
</tbody>
</table>
Do we need to qualify STPA tools?

Tool Operational Scenarios

TOS1 - Standalone STPA tool with manual verification
- Tool is used with manual verification of tool outputs for completeness and consistency → Manual process quality assurance is required

TOS2 - Integrated STPA tool without manual verification
- STPA data is automatically transferred to or integrated into another tool without manual verification for completeness and consistency → Tool requires tool error detection or tool error prevention

TOS3 - STPA data is used for verification
- STPA data is used for verification and may fail to detect an error.

TOS4 - STPA data is used for code generation
- STPA data is used for auto code generation may introduce an error
### Tool Qualification Overview

<table>
<thead>
<tr>
<th>TOS</th>
<th>IEC 61508</th>
<th>EN 50128</th>
<th>ISO 26262</th>
<th>Tool Class</th>
<th>Tool Class</th>
<th>Tool Impact</th>
<th>Tool error Detection</th>
<th>Tool Confidence Level</th>
<th>Tool Criterion</th>
<th>Safety Level</th>
<th>Tool Quali. Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS1</td>
<td>T1</td>
<td>T1</td>
<td>TI2</td>
<td>TD3</td>
<td>TCL1</td>
<td>---</td>
<td>---</td>
<td>(TQL-5)</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>TOS2</td>
<td>T1 (T2)</td>
<td>T1 (T2)</td>
<td>TI2</td>
<td>TD1 TD2 TD3</td>
<td>TCL1 TCL2 TCL3</td>
<td>2</td>
<td>A B C D</td>
<td>TQL-3 TQL-4 TQL-5 TQL-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS3</td>
<td>T2</td>
<td>T2</td>
<td>TI2</td>
<td>TD1 TD2 TD3</td>
<td>TCL1 TCL2 TCL3</td>
<td>2</td>
<td>A B C D</td>
<td>TQL-3 TQL-4 TQL-5 TQL-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS4</td>
<td>T3</td>
<td>T3</td>
<td>TI2</td>
<td>TD1 TD2 TD3</td>
<td>TCL1 TCL2 TCL3</td>
<td>1</td>
<td>A B C D</td>
<td>TQL-1 TQL-2 TQL-3 TQL-4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tool class depends on intended use. Tool qualification depends on many factors!
Do we need to qualify STPA tools? Example: SAHRA

### SAHRA (TOS2)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Qualification acc. Standard</th>
<th>Recommended Qualification</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>T1</td>
<td>T2</td>
<td>Indirect Impact (process risks)</td>
</tr>
<tr>
<td>EN 50128</td>
<td>T1</td>
<td>T2</td>
<td>Indirect Impact (process risks)</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>TCL1</td>
<td>TCL2</td>
<td>Tool Error Detection confidence level (TD) is high TD1, prevention of tool errors through safety tool development process (DO-330)</td>
</tr>
<tr>
<td></td>
<td>TCL2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DO-178C / DO-330</td>
<td>TQL-3</td>
<td>TQL-3</td>
<td>Automates development and verification process steps → Criteria 2</td>
</tr>
<tr>
<td></td>
<td>TQL-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TQL-5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Do we need to qualify STPA tools?

**Example: STPA Tool with Model Checker**

#### STPA Tool with verification capabilities (TOS3)

STPA data items are used for Formal Model Checking

<table>
<thead>
<tr>
<th>Standard</th>
<th>Qualification acc. Standard</th>
<th>Recommended Qualification</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>T2</td>
<td>T2</td>
<td>Indirect (process risks) Tool may fail to detect an error</td>
</tr>
<tr>
<td>EN 50128</td>
<td>T2</td>
<td>T2</td>
<td>Indirect (process risks) Tool may fail to detect an error</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>TCL1, TCL2, TCL3</td>
<td>TCL3</td>
<td>Tool Error Detection (TD) confidence level is unknown → TD3</td>
</tr>
<tr>
<td>DO-178C / DO-330</td>
<td>TQL-3, TQL-4, TQL-5</td>
<td>TQL-3</td>
<td>Eliminates verification process steps → Criteria 2</td>
</tr>
</tbody>
</table>
Agenda

Introduction

Tool Qualification Overview

Tool Qualification for STPA tools

Conclusion Discussion
Conclusion

Tool Qualification of tools supporting STPA

Tool Risk Analysis

Tool risk analysis of safety analysis tools (here: STPA) is required for proper tool classification and to determine Tool Qualification Requirements.

The tool risk analysis shall consider:

- process risks,
- tool and tool integration risks, and
- operational scenarios how the tool is used in the process.

For more details about tool and tool integration risks: [25-28]
Conclusion

Tool Qualification of tools supporting STPA

Effects of Tool Errors

- Tool errors in STPA tools (and safety analysis tools in general) might have an **negative impact** on the final safety related system and can be traced to process risks
- Tool Qualification based on **tool risk assessment** and **operational scenarios** of safety analysis tools is therefore **highly recommended**

Do we need to qualify STPA tools? **YES!**
Conclusion

Tool Qualification of tools supporting STPA

DO-330 provides detailed guidelines for multi domain tool qualification and
- can be used by tool users and tool developers as a guiding standard for tool qualification,
- can be used by tool developers as a guiding standard for safe tool development

SAHRA Development Lifecycle

- We use DO-330 as guiding safety standard for tool development of SAHRA with TQL-4 (suitable for Level B-D)

Tool Qualification Packages

- Tool developers can help tool users to qualify their tools with Tool Qualification Packages with tool operational requirements and predefined tool validation test cases and procedures.
- Tool developers should provide a safety manual including a reference workflow with operational scenarios for safe use of the tool.
Problems

Limitation to Software Development Lifecycle Support Tools
The standards have a strong focus on tools that support the software development lifecycle and do not explicitly consider other tools for system or hardware engineering.

Safety Analysis Tools?
- Safety analysis tools are not addressed in the standards. What about errors in Fault Tree Tools, FMEA tools and others?

Simulation Tools?
- What about tool errors in tools for systems or hardware engineering like simulation tools which are used for verification?

Requirements Management Tools?
- Errors in Requirements Management Tools share the same process risks, hazards and losses: Unsafe Design and Unsafe System!
Problems

Tool classification problems

- Tool classification is difficult, especially for integrated tools (like SAHRA) or combined tools (for example STPA tools with formal model checking capabilities) and depends on the operational scenarios, i.e. context and intended use.
- Wrong order of qualification steps in standards IEC 61508 and EN 50128. First demanding tool risk assessment, then tool classification would be better!

Stakeholder Scope

- Its in most reviewed standards unclear what are the requirements for tool users and what are requirements for tool developers (exception: DO-330).
- Most requirements can only be satisfied by tool developers. Example: Tool error detection confidence level TD in ISO 26262 cannot be selected correctly by tool users. When tool error detection function is used within the tool, then it should be validated by the tool developer!
Discussion & Questions

Word cloud generated with http://www.jasondavies.com/wordcloud/
Annex
## Generic Safety Standard
### IEC 61508 Part 4 [23]

<table>
<thead>
<tr>
<th>Class</th>
<th>Definition</th>
<th>Examples</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Tool that generates <strong>no outputs that can directly or indirectly contribute to the executable code (including data)</strong> of the safety related system</td>
<td>Text Editor Requirements Management Tool Modeling Tool without Code Generation Configuration Management Tool</td>
<td>3.2.11</td>
</tr>
<tr>
<td>T2</td>
<td>Tool that <strong>supports the test or verification of the design or executable code</strong>, where errors in the tool <strong>can fail to reveal defects</strong> but cannot directly create errors in the executable software</td>
<td>Test Generator Code Coverage Tool Static Code Analysis Tool</td>
<td>3.2.12</td>
</tr>
<tr>
<td>T3</td>
<td>Tool that <strong>generates outputs that can directly or indirectly contribute to the executable code</strong> of the safety related system</td>
<td>Optimizing Compiler Compiler with Runtime Package</td>
<td>3.2.13</td>
</tr>
</tbody>
</table>
## Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Ref.</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools shall be selected in accordance with all development activities</td>
<td>7.4.4.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Selection of tool shall be justified</td>
<td>7.4.4.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tools shall have documentation or specification which specifies behavior and restrictions on use</td>
<td>7.4.4.4</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Safety assessment required + mitigation actions</td>
<td>7.4.4.5</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Evidence for conformance to specification or manual required, by</td>
<td></td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>• Increased confidence from use</td>
<td>7.4.4.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tool validation</td>
<td>7.4.4.7</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Summary only, not all requirements are shown. ● Mandatory, ○ Recommended
## Class Definition Examples Ref.

### T1
- Tool that generates **no outputs that can directly or indirectly contribute to the executable code (including data)** of the safety related system

<table>
<thead>
<tr>
<th>Examples</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Editor</td>
<td></td>
</tr>
<tr>
<td>Requirements Management Tool</td>
<td></td>
</tr>
<tr>
<td>Modeling Tool without Code Generation</td>
<td></td>
</tr>
<tr>
<td>Configuration Management Tool</td>
<td></td>
</tr>
</tbody>
</table>

### T2
- Tool that **supports the test or verification of the design or executable code**, where errors in the tool **can fail to reveal defects** but cannot directly create errors in the executable software

<table>
<thead>
<tr>
<th>Examples</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Generator</td>
<td></td>
</tr>
<tr>
<td>Code Coverage Tool</td>
<td></td>
</tr>
<tr>
<td>Static Code Analysis Tool</td>
<td></td>
</tr>
</tbody>
</table>

### T3
- Tool that **generates outputs that can directly or indirectly contribute to the executable code** of the safety related system

<table>
<thead>
<tr>
<th>Examples</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimizing compiler</td>
<td></td>
</tr>
<tr>
<td>Compiler with runtime package</td>
<td></td>
</tr>
<tr>
<td>Data/Algorithm compiler</td>
<td></td>
</tr>
<tr>
<td>Tool for changing reference values during operation</td>
<td></td>
</tr>
</tbody>
</table>
### Requirements

<table>
<thead>
<tr>
<th>Tools shall be selected in accordance with all development activities</th>
<th>Ref.</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection of tool shall be justified</td>
<td>6.7.4.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tools shall have documentation or specification which specifies behavior and restrictions on use</td>
<td>6.7.4.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Safety assessment required + mitigation actions</td>
<td>6.7.4.4</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Evidence for conformance to specification or manual required by:</td>
<td>6.7.4.4</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>• Increased Confidence from use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tool validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tool detection means</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tool validation &amp; report</td>
<td>6.7.4.5</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Summary only, not all requirements are shown. ● Mandatory, ○ Recommended
<table>
<thead>
<tr>
<th>C</th>
<th>Definition</th>
<th>Level D</th>
<th>Level C</th>
<th>Level B</th>
<th>Level A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A tool whose output is part of the airborne software and thus could insert an error.</td>
<td>TQL-4</td>
<td>TQL-3</td>
<td>TQL-2</td>
<td>TQL-1</td>
</tr>
<tr>
<td>2</td>
<td>A tool that automates verification process(es) and thus could fail to detect an error, and whose output is used to justify the elimination or reduction of: 1. Verification process(es) other than that automated by the tool, or 2. Development process(es) that could have an impact on the airborne software</td>
<td>TQL-5</td>
<td>TQL-5</td>
<td>TQL-4</td>
<td>TQL-3</td>
</tr>
<tr>
<td>3</td>
<td>A tool that, within the scope of its intended use, could fail to detect an error</td>
<td>TQL-5</td>
<td>TQL-5</td>
<td>TQL-5</td>
<td>TQL-4</td>
</tr>
</tbody>
</table>
### Tool Impact

The possibility that a malfunction of a particular software tool can introduce or fail to detect errors in a safety-related item or element being developed.

<table>
<thead>
<tr>
<th>Tool Error Detection</th>
<th>High confidence to prevent/detect erroneous outputs</th>
<th>Medium confidence to prevent/detect erroneous outputs</th>
<th>Other cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD1</td>
<td></td>
<td></td>
<td>TD3</td>
</tr>
<tr>
<td>TI1 shall be selected when there is an argument that there is no such possibility</td>
<td>TI1</td>
<td>TCL1</td>
<td>TCL1</td>
</tr>
<tr>
<td>TI2 shall be selected in all other cases</td>
<td>TI2</td>
<td>TCL1</td>
<td>TCL2</td>
</tr>
</tbody>
</table>
## Automotive
ISO 26262-8 [19]

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1a</strong></td>
<td><strong>Methods</strong></td>
</tr>
<tr>
<td>Increased confidence from use in accordance with 11.4.7</td>
<td>TCL3 ++ ++ + +</td>
</tr>
<tr>
<td></td>
<td>TCL2 ++ ++ ++ +</td>
</tr>
<tr>
<td></td>
<td>TCL1</td>
</tr>
<tr>
<td><strong>1b</strong></td>
<td>Evaluation of the tool development process in accordance with 11.4.8</td>
</tr>
<tr>
<td></td>
<td>TCL2 ++ ++ ++ +</td>
</tr>
<tr>
<td></td>
<td>TCL1</td>
</tr>
<tr>
<td><strong>1c</strong></td>
<td>Validation of the software tool in accordance with 11.4.9</td>
</tr>
<tr>
<td></td>
<td>TCL2 + + + ++</td>
</tr>
<tr>
<td></td>
<td>TCL1</td>
</tr>
<tr>
<td><strong>1d</strong></td>
<td>Development in accordance with a safety standard a</td>
</tr>
<tr>
<td></td>
<td>TCL2 + + + ++</td>
</tr>
<tr>
<td></td>
<td>TCL1</td>
</tr>
</tbody>
</table>

---

**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.

Summary only, not all requirements are shown. ++ Highly recommended, + Recommended
References

8. Antoine B. Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry: Massachusetts Institute of Technology; 2013.
References

17. DO-178C - Software Considerations in Airborne Systems and Equipment Certification. 2011.