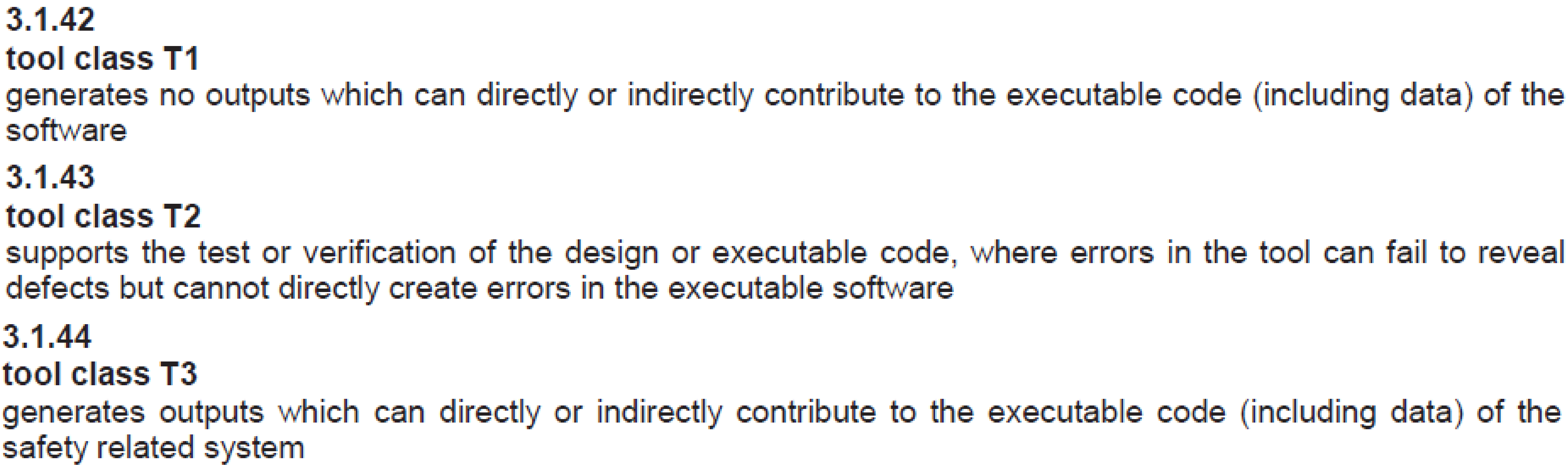
Oscar Slotosch

Comparisson of Tool Qualification EN 50128, ISO 26262, IEC 61508, DO-330

EN 50128 Requirements: Classification

- **Tool Classification:**



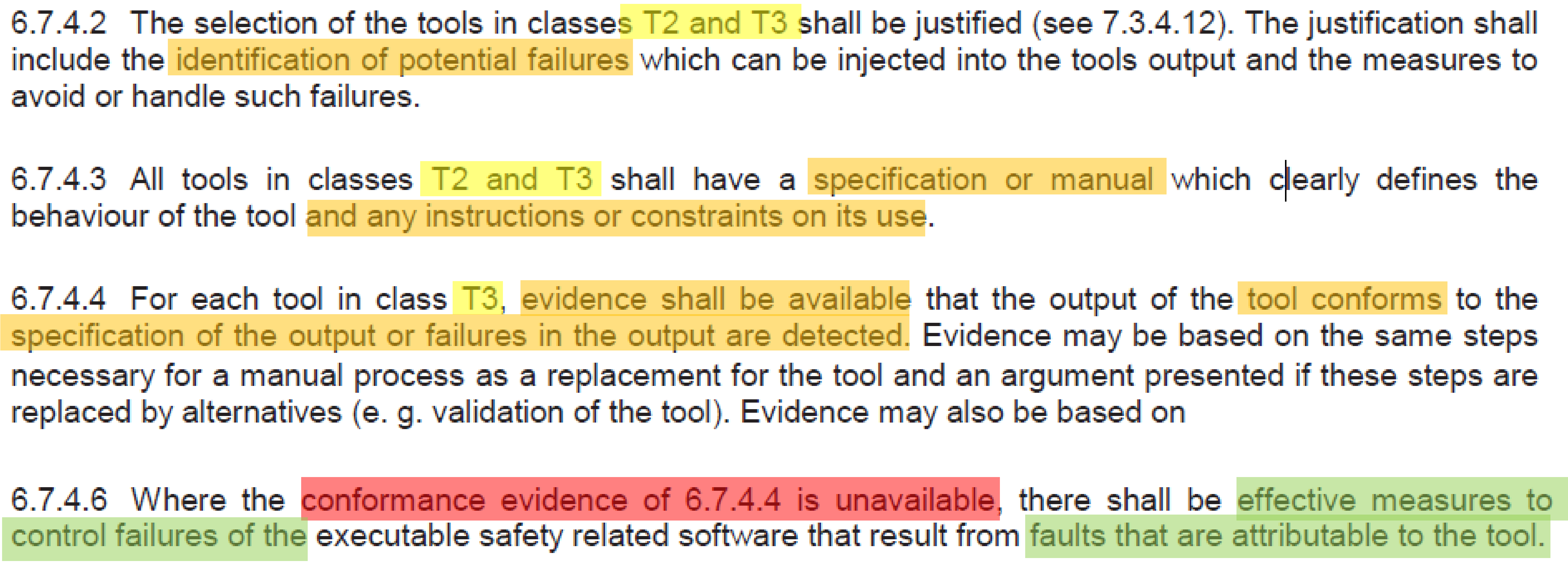
3.1.42
tool class T1
generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software

3.1.43
tool class T2
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

3.1.44
tool class T3
generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system

- **Tool Qualification depends on classification results**

EN 50128 Requirements: Qualification



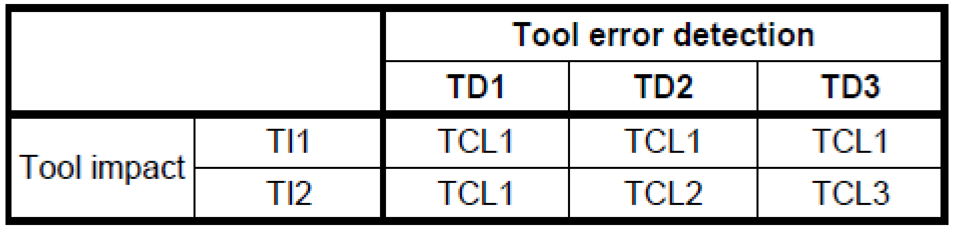
6.7.4.2 The selection of the tools in classes T2 and T3 shall be justified (see 7.3.4.12). The justification shall include the identification of potential failures which can be injected into the tools output and the measures to avoid or handle such failures.

6.7.4.3 All tools in classes T2 and T3 shall have a specification or manual which clearly defines the behaviour of the tool and any instructions or constraints on its use.

6.7.4.4 For each tool in class T3, evidence shall be available that the output of the tool conforms to the specification of the output or failures in the output are detected. Evidence may be based on the same steps necessary for a manual process as a replacement for the tool and an argument presented if these steps are replaced by alternatives (e. g. validation of the tool). Evidence may also be based on

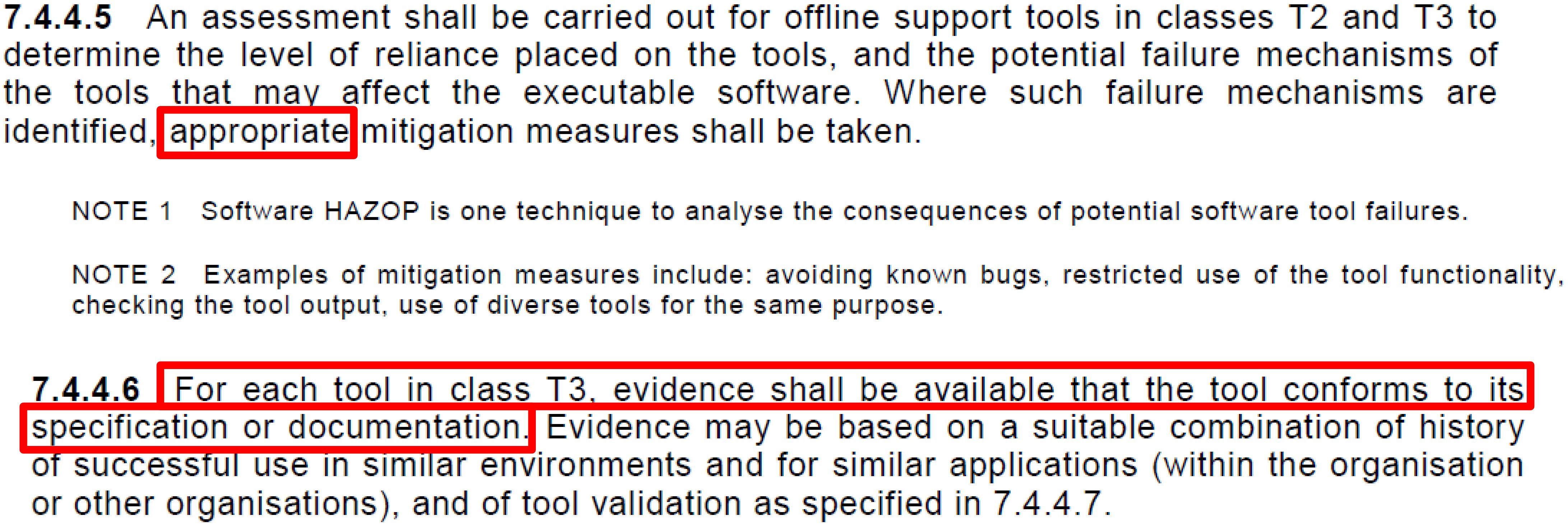
6.7.4.6 Where the conformance evidence of 6.7.4.4 is unavailable, there shall be effective measures to control failures of the executable safety related software that result from faults that are attributable to the tool.

Other Standard Requirements



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

- **ISO 26262:**
  - Classification of tools (TCL 1, TCL 2, TCL 3)
  - using errors & detection/prevention with probabilities
  - in use cases of the tools
- **IEC 61508 (3:2010 7.7.4 and 4:2012 3.2.11)**
  - Classification of tools (T1: „no impact“, T2: „test, V&V“, T3: „executing“)



7.4.4.5 An assessment shall be carried out for offline support tools in classes T2 and T3 to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures shall be taken.

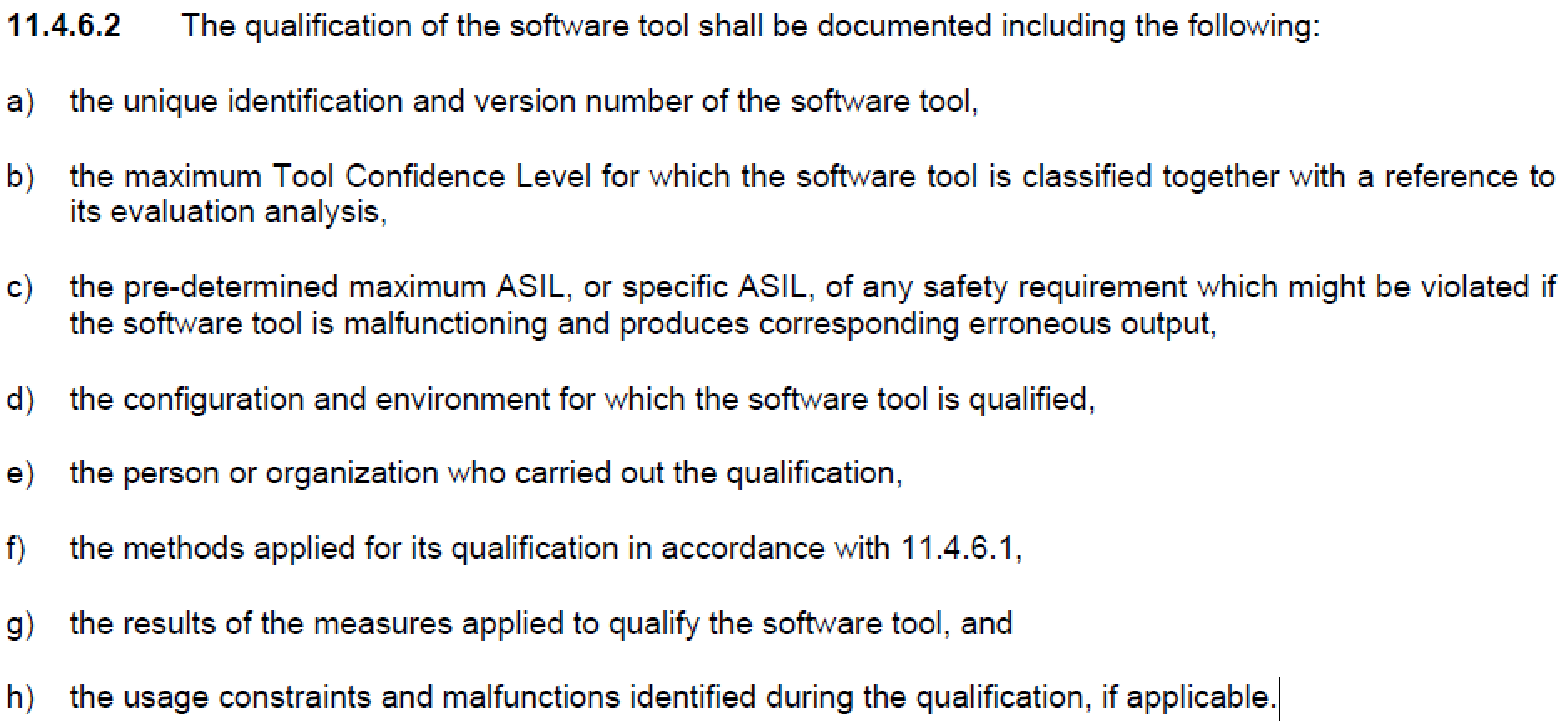
NOTE 1 Software HAZOP is one technique to analyse the consequences of potential software tool failures.

NOTE 2 Examples of mitigation measures include: avoiding known bugs, restricted use of the tool functionality, checking the tool output, use of diverse tools for the same purpose.

7.4.4.6 For each tool in class T3, evidence shall be available that the tool conforms to its specification or documentation. Evidence may be based on a suitable combination of history of successful use in similar environments and for similar applications (within the organisation or other organisations), and of tool validation as specified in 7.4.4.7.

- **DO: Split into two part DO-178C classification and D0-330: qualification**

ISO 26262 Tool Qualification



11.4.6.2 The qualification of the software tool shall be documented including the following:

a) the unique identification and version number of the software tool,

b) the maximum Tool Confidence Level for which the software tool is classified together with a reference to its evaluation analysis,

c) the pre-determined maximum ASIL, or specific ASIL, of any safety requirement which might be violated if the software tool is malfunctioning and produces corresponding erroneous output,

d) the configuration and environment for which the software tool is qualified,

e) the person or organization who carried out the qualification,

f) the methods applied for its qualification in accordance with 11.4.6.1,

g) the results of the measures applied to qualify the software tool, and

h) the usage constraints and malfunctions identified during the qualification, if applicable.

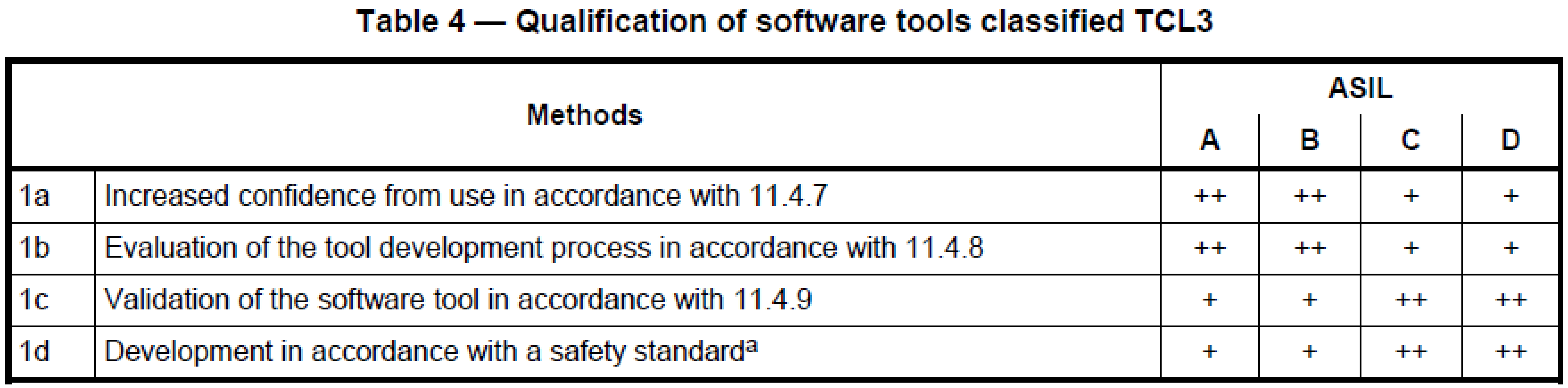
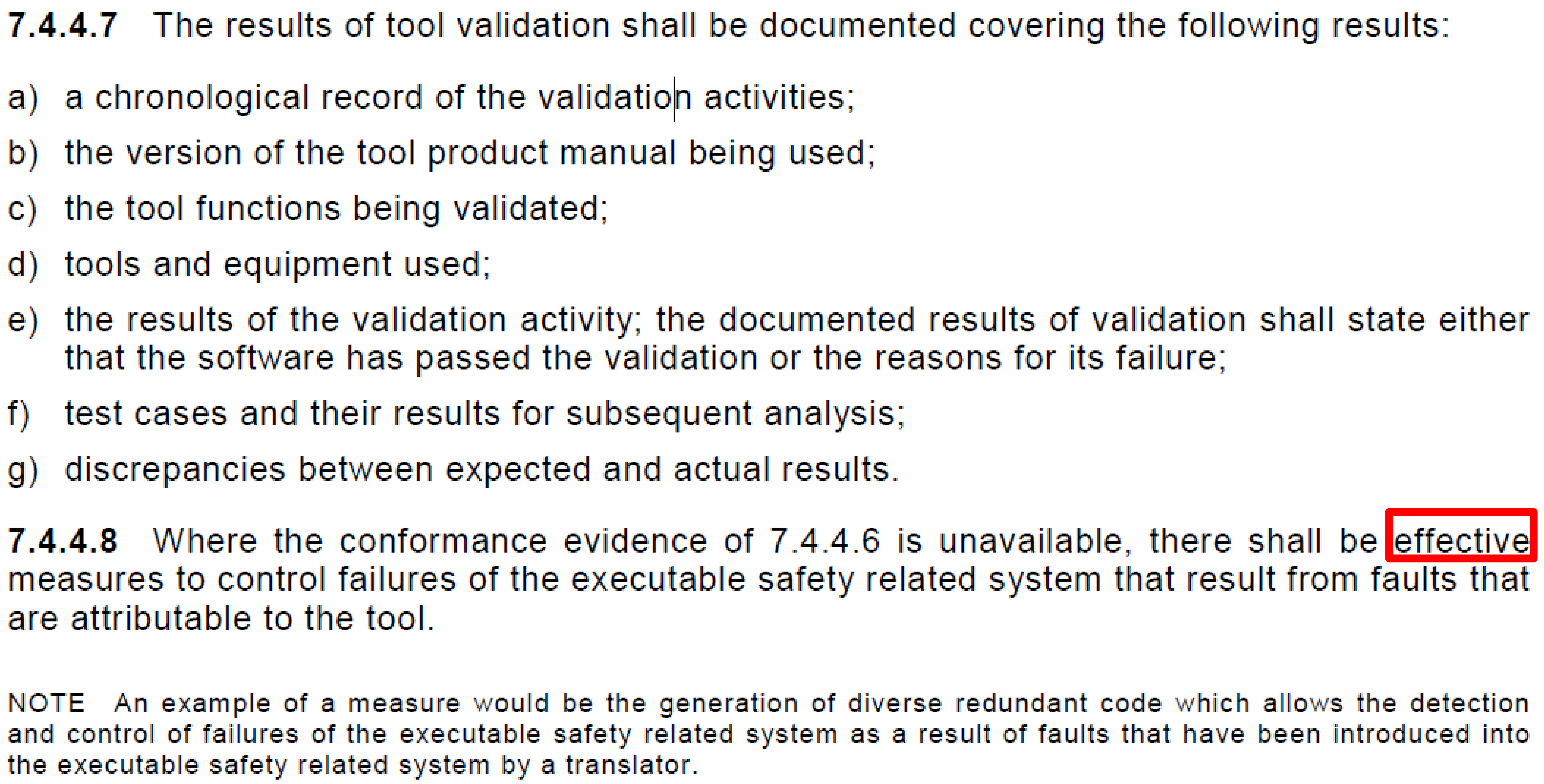


Table 4 — Qualification of software tools classified TCL3

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]	+	+	++	++

IEC 61508 Tool Qualification



7.4.4.7 The results of tool validation shall be documented covering the following results:

a) a chronological record of the validation activities;

b) the version of the tool product manual being used;

c) the tool functions being validated;

d) tools and equipment used;

e) the results of the validation activity; the documented results of validation shall state either that the software has passed the validation or the reasons for its failure;

f) test cases and their results for subsequent analysis;

g) discrepancies between expected and actual results.

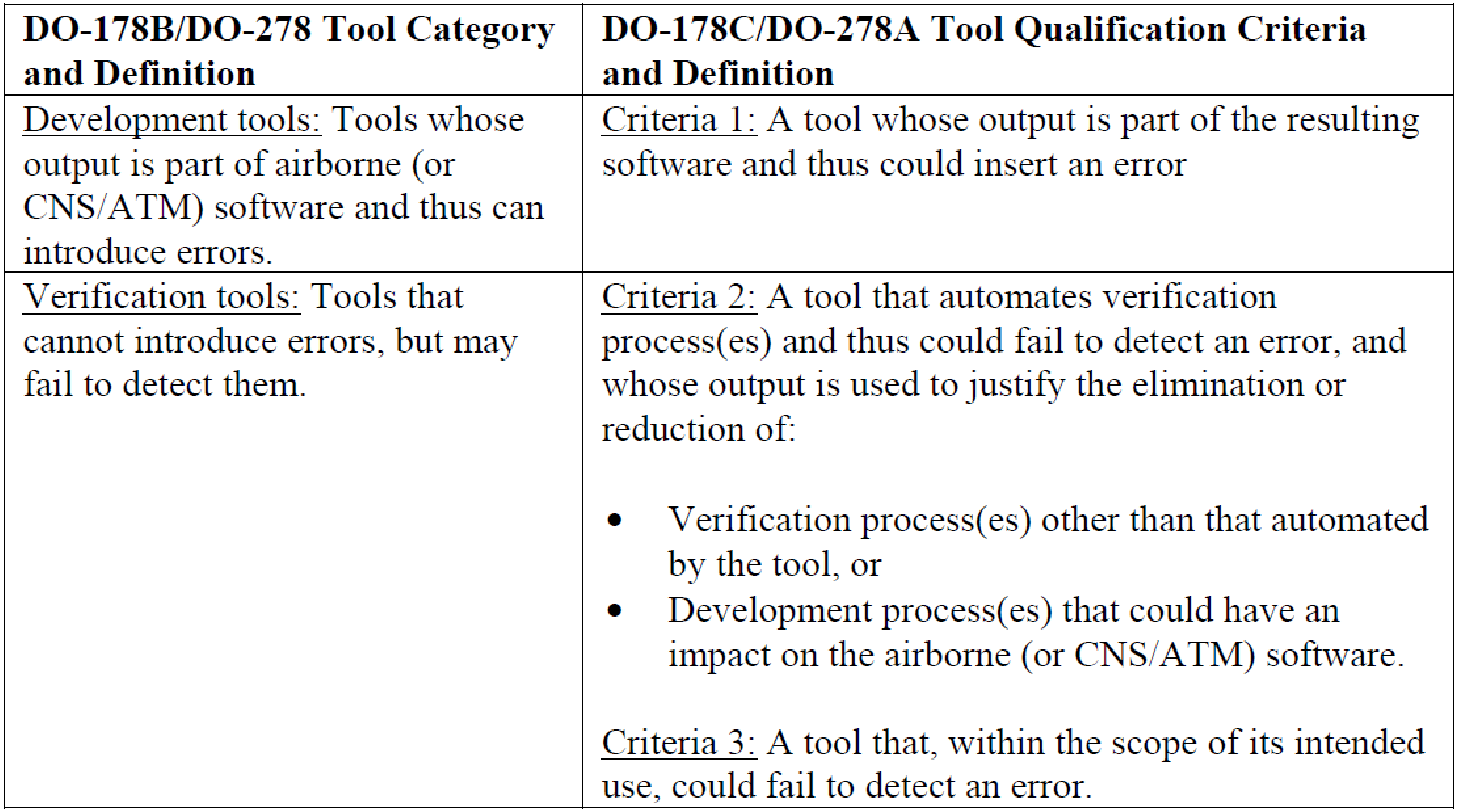
7.4.4.8 Where the conformance evidence of 7.4.4.6 is unavailable, there shall be effective measures to control failures of the executable safety related system that result from faults that are attributable to the tool.

NOTE An example of a measure would be the generation of diverse redundant code which allows the detection and control of failures of the executable safety related system as a result of faults that have been introduced into the executable safety related system by a translator.

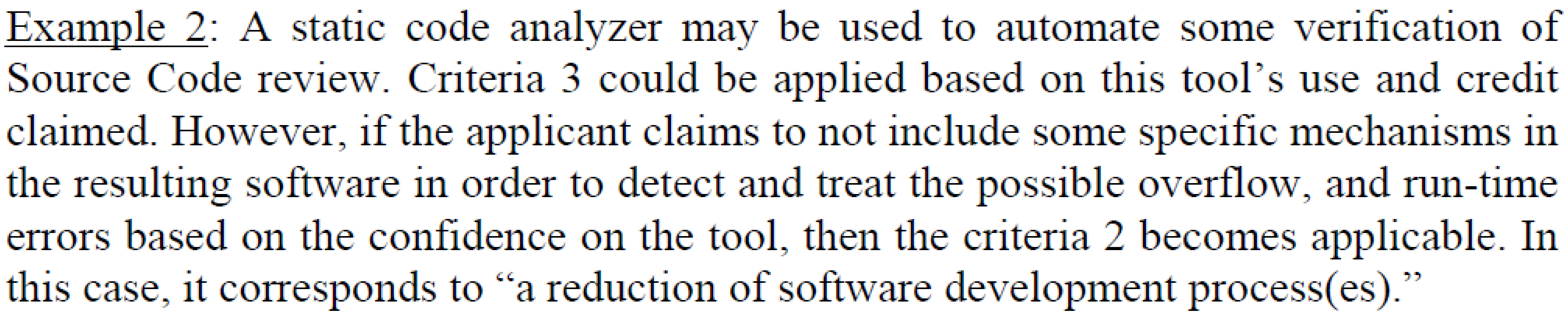
DO-330 Software Tool Qualification

- Describes tool qualification for DO-178C, DO-278A,..
- Contains classification of criteria for criticality
- Mapping to five tool qualification levels (TQLs)
- No method to determine the Criteria (part of domain standards?)

DO-330: Classification: Criteria

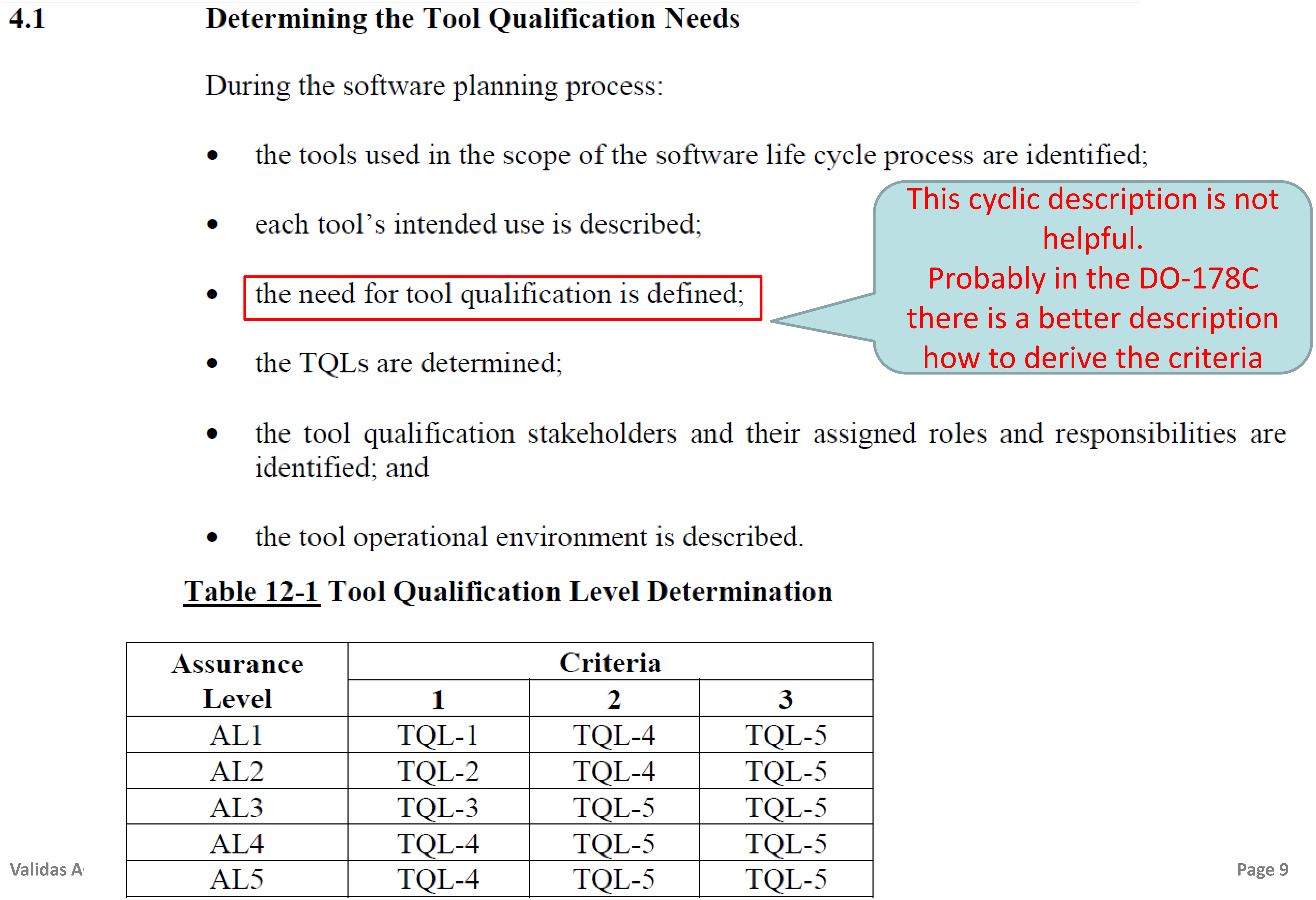


DO-178B/DO-278 Tool Category and Definition	DO-178C/DO-278A Tool Qualification Criteria and Definition
Development tools: Tools whose output is part of airborne (or CNS/ATM) software and thus can introduce errors.	Criteria 1: A tool whose output is part of the resulting software and thus could insert an error
Verification tools: Tools that cannot introduce errors, but may fail to detect them.	Criteria 2: 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: • Verification process(es) other than that automated by the tool, or • Development process(es) that could have an impact on the airborne (or CNS/ATM) software. Criteria 3: A tool that, within the scope of its intended use, could fail to detect an error.



Example 2: A static code analyzer may be used to automate some verification of Source Code review. Criteria 3 could be applied based on this tool's use and credit claimed. However, if the applicant claims to not include some specific mechanisms in the resulting software in order to detect and treat the possible overflow, and run-time errors based on the confidence on the tool, then the criteria 2 becomes applicable. In this case, it corresponds to "a reduction of software development process(es)."

Qualification Need (Criteria,TQLs)



4.1 Determining the Tool Qualification Needs

During the software planning process:

- the tools used in the scope of the software life cycle process are identified;
- each tool's intended use is described;
- the need for tool qualification is defined;
- the TQLs are determined;
- the tool qualification stakeholders and their assigned roles and responsibilities are identified; and
- the tool operational environment is described.

Table 12-1 Tool Qualification Level Determination

Assurance Level	Criteria		
	1	2	3
AL1	TQL-1	TQL-4	TQL-5
AL2	TQL-2	TQL-4	TQL-5
AL3	TQL-3	TQL-5	TQL-5
AL4	TQL-4	TQL-5	TQL-5
AL5	TQL-4	TQL-5	TQL-5

This cyclic description is not helpful.
Probably in the DO-178C there is a better description how to derive the criteria

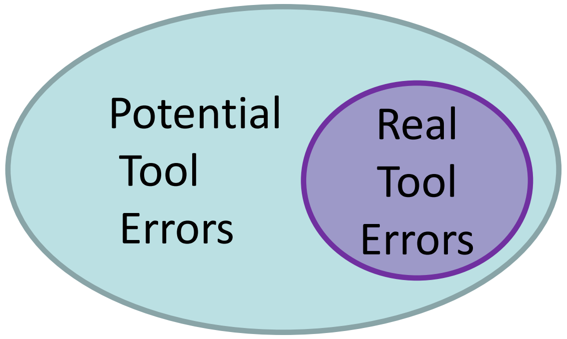
Comparison ISO, IEC/EN, DO

- **Similar Process: Classification, Qualification, Usage**
- **ISO-IEC: Similar Levels**
  - Level
    - T1 / TCL 1:
    - no impact / high detection probability (from HAZOP)
    - nothing to qualify
  - Level 2
    - T2: Error analysis required (e.g. HAZOP)
    - T2: Appropriate error mitigation in Process required (redundancy,…)
    - T2: no tool qualification
    - TCL2: medium detection probability (from HAZOP):
    - TCL2: Simple tool qualification needs according to ASIL (process, proven in use, or more)
  - Level 3
    - T3: Error analysis required (e.g. HAZOP)
    - T3: Appropriate error mitigation in Process required (redundancy,…)
    - T3: Qualification using appropriate method combination or “effective mitigation”
    - TCL3: advanced tool qualification needs according to HAZOP and ASIL (validation, safety standard but also process, proven in use for lower ASIL)

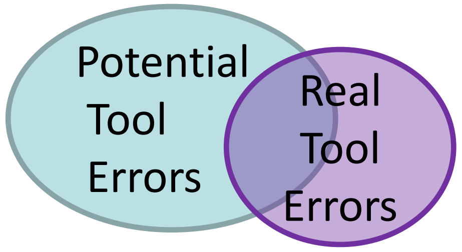
Summary Tool Qualification

- **Surrounding Process**
  - Planning
  - Classification
  - Opt. Qualification
  - Usage
- **Requirements**
  - Classification: Analysis of potential Failures
  - Qualification: Evidence for the absence of pot. Failures
- **Important: potential Tool Failures & Errors determination**

safe case:



unsafe case:



Thank You!

VALIDAS

Arnulfstraße 27
80335 München
www.validas.de
info@validas.de