LDRA
Software Technology

Technical Briefing

Clarifying and fulfilling test tool qualification requirements

Leveraging DO-330 and ISO 26262 tool verification techniques for developments compliant with other functional safety standards

www.ldra.com

Contents

Background

Today's complex software based safety critical systems depend on software tools for automation and efficiency. "Tool qualification" is a generic term to describe a process designed to ensure that the risk of a tool error impacting the safety of a system is acceptably low – either because the errors are few, or because they cannot impact safety. Most functional safety standards define processes to achieve tool qualification by considering the application of the tool, and the environment in which it is deployed.

Many IEC 61508 [1] derived functional safety standards demand a similar level of qualification but, particularly for the most critical applications, stop short of specifying exactly how that should be approached.

Exceptions include the ISO 26262 standard [2] written specifically for the automotive sector, and DO-330 [3] written primarily with the aerospace sector in mind. There are LDRA technical briefings available to detail the use of the tool qualification processes as used in automotive [4] and commercial aviation [5] environments, respectively. This paper suggests how the tool verification processes laid out in ISO 26262 and DO-330 might be fill the void in advice offered by other standards, particularly where applications are at their most critical and hence where TÜV certification has no bearing.

The paper references the LDRA tool suite [6] as an example. The LDRA tool suite is an integrated collection of requirements traceability tools, and static and dynamic analysis tools for verification and validation.

What constitutes a functional safety standard?

According to the IEC [7]:

"Functional safety seeks to reduce the level of risk in a device or system.

While zero risk is an unattainable goal, functional safety identifies potentially dangerous conditions that could result in harm and automatically enables corrective actions to avoid or reduce the impact of an incident. It is part of the overall safety of a system or device that depends on automatic safeguards responding to a hazardous event.

Functional safety relies on active systems that can respond to a potentially dangerous situation. Examples include the deactivation of a medical infusion pump should it malfunction or the automatic activation of an overflow valve when a certain liquid or pressure level has been reached."

The term "Functional safety standards" is frequently used to describe IEC 61508 and its derivatives.

There is a subtle difference in approach between functional safety in general and civil aviation safety in particular. The former deals with devices and systems whereas the latter deals with the aircraft and its certification such that the safety of "devices and systems" are mostly determined in the context of a particular aircraft and its type certification.

With that proviso, the IEC definition of functional safety clearly applies just as well to the scope of the commercial aerospace standards exemplified by DO-178C [8] and DO-278A [9] . For that reason, this document includes them within that collective term.

Avionics	DO-178C (First published 1992)
Industrial	IEC 61508 (First published 1998, Updated 2010)
Railway	EN 5012X (First published 2001)
Nuclear	IEC 61513 (First published 2001)
Automotive	ISO 26262 (Published 2011)
Medical	IEC 62304 (First published 2006)
Process	IEC 61511 (First published 2003)
...	

Figure 1: Most functional safety standards are direct derivatives of IEC 61508 – part of the "IEC 61058 family"

Approaches to tool qualification

There are several different approaches to tool qualification promoted by the functional safety standards.

Figure 2: TÜV certification for LDRA tools

- **Tool verification:** This represents the most thorough but most time consuming approach. It is generally applicable to all applications. Each feature of the tool is analysed using the environment in which the tool is to be deployed, and the results documented. Any potential errors in these features with the potential to impact the safety of the product are further assessed to determine the probability of them being detected or avoided within the process. If that probability is low, the tool must be qualified to ensure the absence of these errors. This is achieved by applying a validation suite in a systematic way.
- **Evaluation of the tool development process** such that evidence can be provided that a suitable software development process has been applied. TÜV certification is often cited as appropriate evidence (Figure 2). Generally, this approach is not permissible for the most critical applications but it can save considerable overhead elsewhere.
- **Proof in use:** Applicable where a software tool has been used previously for the same purpose with comparable use cases, in similar circumstances. Generally, this approach is not permissible for the most critical applications.
- **Development in accordance with a safety standard** where the development of the tool itself complies with a safety standard. Applicable to all applications.

In most cases, commercial aviation standards require tool qualification to take the form of a verification process. To some degree, that different stance can be explained by the fact that commercial aerospace standards refer throughout to aircraft safety requirements that are defined at the aircraft level, as manifested by systems, before being allocated to software (and hardware) items. There can therefore be no universal prequalification of a software tool for use in DO-178C applications, for example.

Conversely, IEC 61508 and its derivatives apply to suppliers of software (and hardware) "items" that are subsequently applied in the relevant sector. The net result is that software tools can be approved for the use of software item suppliers in general.

Despite that logical distinction, DO-330 is designed to be applied in sectors outside commercial aircraft, as discussed later.

Detailed tool verification processes in the functional safety standards

ISO 26262 Road Vehicles - Functional Safety

Despite ISO 26262 being a derivative of IEC 61508, ISO 26262-8 [10] §11 "Confidence in the use of software tools" presents a much more detailed definition of tool qualification in general and verification in particular than IEC 61508 itself, or most of its other derivatives.

ISO 26262 tool validation using Tool Qualification Support

In recognition of this need, many vendors provide Tool Qualification Support Packs (TQSPs, sometimes known as Tool Qualification Kits) which provide a defined process and associated test cases. Applied correctly, these packs can be used to show whether or not the tool has been configured appropriately to provide the correct results in the tool chain and environment in which it will be deployed.

The LDRA tool suite ISO 26262 TQSP covers three discrete functions, each of which can be specified as an "operational requirement" for the pertinent development project:

- Programming Rules Checking
- Structural Coverage Analysis
- Unit Test / Low Level Test

The TQSP includes five key documents designed to guide the user through the validation process. The process defined by these documents ensure the creation of evidential artefacts and the compilation of reports designed to summarize findings in a form appropriate to the standard:

- LDRA provides a generic **Tool Criteria Evaluation Report (TCER)** for customization by the user in accordance with the instructions in the TVP. The TCER describes the tool and its architecture, details the certification credit sought, identifies the tool qualification activities to be performed, and summarizes the tool qualification data to be produced.
- The LDRA **Tool Operational Requirements (TOR)** identify one or more of the functions described named above as they relate to the scope of qualification specified by the user in the TCER and SVR.
- The **Tool Verification Plan (TVP)** provided by LDRA is a generic document, common to all projects. It is an instructional script for the verification of the LDRA tool suite. The TVP refers to the TVCP to identify the test cases associated with each of the functions specified in the TOR as requiring qualification for the pertinent project.
- The **Tool Verification Cases and Procedures (TVCP)** provided by LDRA include source code, test cases, and expected results, for use in verifying the effectiveness of the tool on the pertinent installation environment. The user is responsible for ensuring that the test cases contained in the TVCP are sufficient to cover all of the source code constructs to be used on the project.

- **Tool Verification Results (TVR)** are generated by applying the TVCP to test source code in the installation environment. These results are compared with the expected results detailed in the TVCP to establish whether the tool is operating properly under the project's customized operating conditions.

RTCA DO-330 Software Tool Qualification Considerations

Tool qualification is a vital part of the certification process for airborne systems and equipment, as documented in the DO-330 Software Tool Qualification Considerations. Despite its clear association with other commercial aviation standards, DO-330 was specifically designed to be equally applicable to other sectors. From DO-330 §1.2 "Scope":

c. "This document provides guidance for airborne and ground-based software. It may also be used by other domains, such as automotive, space, systems, electronic hardware, aeronautical databases, and safety assessment processes."

The LDRA tool suite is therefore a criteria 3 tool. Irrespective of the application DAL, such a tool is always assigned Tool Qualification Level 5 which implies a demanding tool verification process. The responsibility for showing the suitability of any tools falls on to the organization developing the application. However, they can make use of Tool Qualification Support Packs (TQSP) provided by the vendor.

DO-330 tool validation using a Tool Qualification Support Pack

Under the terms of DO-330, tool qualification is required for every project. TÜV and similar approvals have no bearing on projects to which DO-330 applies.

As discussed previously for ISO 26262 projects, many vendors provide DO-330 Tool Qualification Kits or Tool Qualification Support Packs. The LDRA DO-330 Tool Qualification Support Pack (TQSP) consists of five sub-packs each of which can be specified as an "operational requirement" for the pertinent development project:

- Programming Rules Checking
- Structural Coverage Analysis
- Data Coupling and Control Coupling
- Assembler Coverage Analysis
- Unit Test / Low Level Test

The TQSP includes four key documents designed to guide the user through the validation process. The process defined by these documents ensure the creation of evidential artefacts and the compilation of reports designed to summarize findings in a form appropriate to the standard:

The **Tool Verification Plan (TVP)** provided by LDRA for configuration to suit the application includes source code, test cases, and expected results, for use in verifying the effectiveness of the tool on the pertinent installation environment.

LDRA provides a generic **Tool Accomplishment Summary (TAS)** for customization by the user in accordance with the instructions in the TVP. The TAS describes the tool and its architecture, details the tool chain and other environmental conditions under which it is operating, and provides the results of the exercise associated with the PRC and TVP documents (Figure 7).

For the tool to be qualified in accordance with RTCA DO-330, **Tool Operational Requirements (TOR)** need to be defined. In order to achieve compliance, the TORs must be verifiable, consistent, and include enough detail to demonstrate that the functionality and the resulting output from the tool correspond to the activities that the tool is replacing.

The **Tool Qualification Plan (TQP)** document includes project specified information as identified in the Tool Verification Plan (Figure 9). DO-330 is usually applied to aeronautical application development, in which case it also captures all the requirements specified in the Plan for Software Aspects of Certification (PSAC).

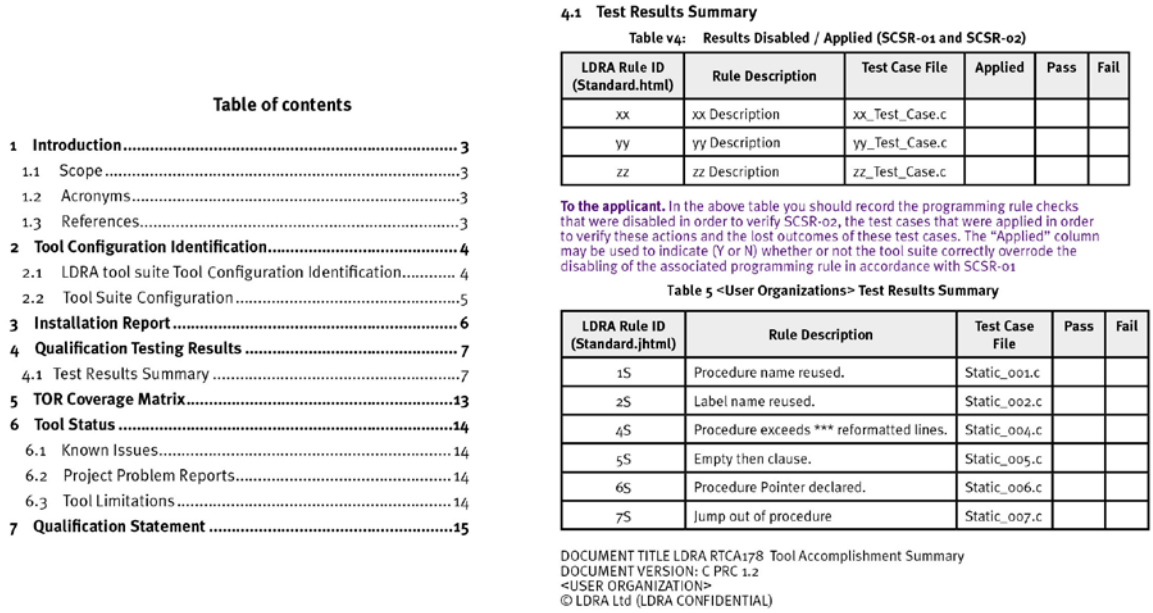

Table of contents

4.1 Test Results Summary

Table v4: Results Disabled / Applied (SCSR-01 and SCSR-02)

LDRA Rule ID (Standard.html)	Rule Description	Test Case File	Applied	Pass	Fail
xx	xx Description	xx_Test_Case.c			
yy	yy Description	yy_Test_Case.c			
zz	zz Description	zz_Test_Case.c			

To the applicant. In the above table you should record the programming rule checks that were disabled in order to verify SCSR-02, the test cases that were applied in order to verify these actions and the lost outcomes of these test cases. The "Applied" column may be used to indicate (Y or N) whether or not the tool suite correctly overrode the disabling of the associated programming rule in accordance with SCSR-01

Table 5 <User Organizations> Test Results Summary

LDRA Rule ID (Standard.jhtml)	Rule Description	Test Case File	Pass	Fail
1S	Procedure name reused.	Static_001.c		
2S	Label name reused.	Static_002.c		
4S	Procedure exceeds *** reformatted lines.	Static_004.c		
5S	Empty then clause.	Static_005.c		
6S	Procedure Pointer declared.	Static_006.c		
7S	Jump out of procedure	Static_007.c		

DOCUMENT TITLE LDRA RTCA178 Tool Accomplishment Summary
DOCUMENT VERSION: C PRC 1.2
<USER ORGANIZATION>
© LDRA Ltd (LDRA CONFIDENTIAL)

Figure 7: Extracts from LDRA Tool Accomplishment Summary as provided in the DO-330 TQSP

Tool qualification for highly critical applications compliant with other functional safety standards

Functional safety is concerned with the removing of unreasonable risk to individuals caused by the malfunctioning of electrical or electronic systems. It is regulated in most industries where individuals are in danger if the product fails to keep them safe.

It is therefore logical that almost all industry specific standards, like ISO 26262 and DO-330, require a level of tool qualification - but unlike them they do not provide precise details of how this is to be approached, particular with regards to tool validation for the most critical of applications. Consider these three examples.

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

Like its derivative ISO 26262, IEC 61508 defines a tool classification approach that does not depend on the use cases of the tools. Part 4 §3.2.11 of IEC 61508 defines three classes of tool, defined in a similar way to the ISO 26262 equivalents:

- **T1:** tools which have no impact on the executable code. The examples given in IEC 61508-4:2010 include text editors and requirements management tools.
- **T2:** tools which only impact on the verification of the executable code and can't inject an error into the code but could cause an error to be missed. Static and dynamic analysis tools typified by the LDRA tool suite tool fall into this class.
- **T3:** generates outputs which can directly or indirectly contribute to the executable code of the safety related system.

Part 3 §7.4.4.5 requires that:
"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."

The standard includes no further details of what these appropriate measures might be.

EN 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

Like ISO 26262, EN 50128 [11] is another derivative of the IEC 61508 standard and so defines tool classes in a similar way. From §3.1.42, §3.1.43, §3.1.44:

- *"tool class T1 generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software*
- *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*
- *tool class T3 generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system"*

The analysis of potential failure is required in Section 6.7.4.2: *"The selection of the tools in classes T2 and T3 shall be justified. 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."*

And again – no further details are provided.

IEC 62304 Medical device software - Software life cycle processes

Another derivative of IEC 61508, IEC 62304 [12] is also insistent that tools should be verified, but offers little specific guidance about how.

§3.3 defines VERIFICATION as *"confirmation through provision of objective evidence that specified requirements have been fulfilled";*

§5.1.10 it requires that *"The items to be controlled shall include tools, items or settings, used to develop the MEDICAL DEVICE SOFTWARE, which could impact the MEDICAL DEVICE SOFTWARE.*

§5.11 it requires that *"The MANUFACTURER shall plan to place CONFIGURATION ITEMS under configuration management control before they are VERIFIED. [Class B, C]"*

In summary, as for the other examples there is a requirement for objective evidence of tool fitness for

purpose, but no detailed instruction of what that should consist of.

Leveraging ISO 226262 and DO-330 principles elsewhere

In general, it is the responsibility of the development team to decide what constitutes adequate "assessment", "justification" or "verification". The TÜV certification discussed earlier is likely to play a large part for the less demanding classifications (SILs, Classes or whatever) but it is hard to justify that alone for the most critical applications given ISO 26262 positioning for ASIL D applications.

On that basis, there is a very good case for using either the ISO 26262 or DO-330 tool qualification process for filling the void. There is nothing about either of them that makes them sector specific, and tool qualification support is available for either from a multitude of vendors.

Indeed, the void in this regard is acknowledged by DO-330. As previously discussed, the document states that it is applicable outside the aerospace sector. The tool qualification process of ISO 26262 makes no such claims but because most other functional safety standards are also derived from IEC 61508, there is an obvious parallel. The ideal path is therefore perhaps one of preference, and so it is useful to highlight the differences.

ISO 26262 and DO-330 tool qualification: A comparison

To that end, a comparison between the tool qualification processes is useful to highlight some of the differences that exist across the different domains and the effect of those differences.

- For both DO-330 and ISO 26262, the tool confidence level is dependent on the **potential impact of errors** associated with methods and processes supported by the tool.
- Both DO-330 and ISO 26262 **differentiate between tool types**, depending on whether they can create an error (such as a code generator) or merely fail to detect one (test tools, including the LDRA tool suite).
- Both DO-330 and ISO 26262 **classify confidence requirements**. DO-330 expresses those as Criteria 1,2 and 3; ISO 26262 expresses them as Tool Confidence Levels (TCLs) 1,2 and 3.
- Although both standards use tables to map software criticality to qualification methods, the DO-330 table shows that test tools at risk of failing to detect errors (including the LDRA tool suite) must follow the qualification process detailed in the standard. ISO 26262 permits the use of **alternative qualification methods** under some circumstances.
- Whereas ISO 26262 tool qualification process is primarily one of **reviews and analyses** particularly for the less demanding ASILs, DO-330 mandates **on target testing** to demonstrate tool effectiveness and compliance for DAL A to C.

Conclusions

Most functional safety standards require some form of tool qualification. However, amongst the most popular standards only ISO 26262 and DO-330 offer a detailed explanation of how to go about it. This leaves a void where applications are so critical that TÜV certification is not applicable.

ISO 26262 demands tool verification in the context of the nominated development environment for similarly critical applications, suggesting that a similar approach would be appropriate for the most demanding SILs or Classes in other sectors.

The principles promoted by ISO 26262 (for ASIL D) and DO-330 are very similar, and tool qualification support packs for the two standards reflect that. For example, the LDRA TQSPs both include test code appropriate to the functionality being tested, expected results, and associated documentation to fulfil the objectives of the applicable standard.

Despite that associated documentation supporting the wider terminology of those standards, there is nothing implicit about either ISO 26262 or DO-330 tool qualification processes that marks them out as sector specific; indeed, the DO-330 standard states as much. It would therefore be a pragmatic approach to use one of these two qualification approaches outside the automotive or aerospace domains, with the choice between the two being down to preference and circumstance.

Works cited

[1] International Electrotechnical Commission (IEC), IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC, 2010 (Part 1).

[2] International Organization for Standardization, ISO 26262:2018 “Road vehicles - Functional safety”, International Organization for Standardization, 2018.

[3] RTCA, Inc., RTCA DO-330 Software Tool Qualification Considerations, RTCA, Inc., 2011.

[4] LDRA, “Test tool qualification for ISO 26262 compliant automotive applications,” LDRA, Liverpool, 2021.

[5] LDRA, “DO-330 test tool qualification for aerospace applications,” LDRA, Liverpool, 2021.

[6] LDRA, “Products - LDRA tool suite,” LDRA, 2021. [Online]. Available: https://ldra.com/automotive/products/. [Accessed 26 August 2021].

[7] International Electrotechnical Commission (IEC), “Safety and Functional Safety,” 2021. [Online]. Available: https://www.iec.ch/safety. [Accessed 25 August 2021].

[8] RTCA, DO-178C “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 2011.

[9] RTCA, DO-278A, “Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, RTCA, 2011.

[10] International Organization for Standardization, in ISO 26262 8:2018 “Road vehicles — Functional safety — Supporting processes” , International Organization for Standardization, 2018.

[11] European Committee for Electrotechnical Standardization (CENELEC), EN 50128 “Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems”, CENELEC, 2020.

[12] International Electrotechnical Commission, IEC 62304:2006+AMD1 Medical device software - Software life cycle processes, IEC, 2015.

LDRA UK & Worldwide
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

LDRA Technology Inc.
2540 King Arthur Blvd, 3rd Floor, 12th Main, Lewisville, Texas 75056
Tel: +1 (855) 855 5372
e-mail: info@ldra.com

LDRA Technology Pvt. Ltd.
Unit B-3, Third floor Tower B, Golden Enclave
HAL Airport Road Bengaluru 560017
Tel: +91 80 4080 8707
e-mail: india@ldra.com