

DO-330 Test tool qualification for aerospace applications

www.ldra.com

© LDRA Ltd. This document is property of LDRA Ltd. Its contents cannot be reproduced, disclosed or utilized without company approval.

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.

The application considerations are designed to ensure that the tool is used in such a way that potential errors are either avoided or detected. The environmental perspective looks to ensure that the installed tool works as part of the broader tool chain to which it contributes, building confidence and trust in the tool and its use.

This paper discusses the RTCA DO-330 "Software Tool Qualification Considerations" standard [1] as it relates to the aviation industry. It references the LDRA tool suite [2] 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.

Note, however, that the standard explicitly states that "It may also be used by other domains, such as automotive, space, systems, electronic hardware, aeronautical databases, and safety assessment processes." The LDRA paper "Test tool qualification for functional safety" discusses that perspective in more detail.

RTCA DO-330 Software Tool Qualification Considerations

RTCA DO-330 requires that tool qualification is achieved by means of a tool verification process. This dictates that each feature of the tool to be applied during the development process must be analysed 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 to prove the absence of these potential errors.

Typically, but not uniquely, RTCA DO-330 is used for commercial aviation applications – for example, in conjunction with the guidance document "Software Considerations in Airborne Systems and Equipment Certification." The first edition of that document, known retrospectively as DO-178A [3], was published in 1982. It was re-written in 1992 as DO-178B [4] and updated again in 2011 as DO-178C [5] to reflect the experience accrued to meet the needs of today's aviation industry.

If software tools are to automate significant numbers of DO-178C activities while producing evidential artefacts showing that objectives have been met, it is essential to ensure that those tools can be relied upon. DO-178C states that:

"the purpose of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of the processes of this document are eliminated, reduced, or automated."

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. DO 330 introduces the concept of Tool Qualification level (TQL) on the basis of three criteria:

- 1) A tool whose output is part of the airborne software and thus could insert an error.
- 2) A tool that automates verification processes and thus could fail to detect an error, and whose output is use to justify the elimination or reduction of:
 - a) Verification processes other than that automated by the tool, or
 - b) Development processes that could have an impact on the airborne software.
- 3) A tool that, within the scope of its intended use, could fail to detect an error.

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 (Figure 1).

Software level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

Figure 1: DO-330 Tool Qualification Level Matrix

Certification authorities such as the FAA, CAA, JAA, and ENAC undertake tool qualification on a project by project basis, so 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.

Tool Qualification documentation must be referenced in other planning documents, and it plays a key role in the compliance process.

DO-330 qualification 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.

Many vendors provide a collection of documentation including test cases with expected results and reporting processes. Usually known as Tool Qualification Kits or Tool Qualification Support Packs, these artefacts can be used to show whether or not a tool has been configured appropriately to provide the correct results in the tool chain in which it will be deployed.

Referencing the LDRA tool suite as an example, the 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.

These four documents are as follows:

Tool Verification Plan (TVP)

The Tool Verification Plan 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.

Tool Accomplishment Summary (TAS)

LDRA provides a generic Tool Accomplishment Summary 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 2).

Table of contents	
1	Introduction..... 3
1.1	Scope.....3
1.2	Acronyms.....3
1.3	References.....3
2	Tool Configuration Identification..... 4
2.1	LDRA tool suite Tool Configuration Identification..... 4
2.2	Tool Suite Configuration5
3	Installation Report 6
4	Qualification Testing Results 7
4.1	Test Results Summary7
5	TOR Coverage Matrix.....13
6	Tool Status14
6.1	Known Issues..... 14
6.2	Project Problem Reports..... 14
6.3	Tool Limitations 14
7	Qualification Statement15

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

Tool Operational Requirement (TOR)

For the tool to be qualified in accordance with RTCA DO-330, tool operational requirements (TORs) 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. An extract from the template TOR document provided as part of the TQSP is presented in Figure 3.

3 Tool Operational Requirements

3.1 Application of specified Coding Standards and Rules

[SCSR-02] If the coding standard model is selected to be applied as a whole, LDRA tool suite *shall* only apply, and report against, the subset of the available programming rules checks indicated in section 3.1.1 of this TOR

[SCSR-02] LDRA tool suite *shall* apply all of the programming standard rule checks indicated as applicable in section 3.1.1 of this TOR irrespective of whether any of these checks have been disabled in the CPEN.DAT file that is being applied at the time of the analysis

The selection of additional rules, external to the selected coding standard, is addressed in section 3.1.2 of this TOR.

3.1.1 Coding Standard Rules

[CSR-0.1] LDRA tool suite *shall* apply each <User Organization> rule below.

LDRA Rule ID (Standard.html)	Rule Description	Test Case File
1 S	Procedure name reused.	Static_001.c
2 S	Label name reused.	Static_002.c
4 S	Procedure exceeds *** reformatted lines.	Static_004.c
5 S	Empty then clause.	Static_005.c
6 S	Procedure pointer declared.	Static_006.c
7 S	Jump out of procedure.	Static_007.c
8 S	Empty else clause	Static_008.c
9 S	Assignment operation in expression	Static_009.c
11 S	No brackets to loop body (added by LDRA tool suite).	Static_011.c
12 S	No brackets to then/else (added by LDRA tool suite).	Static_012.c
13 S	goto detected.	Static_013.c
20 S	Parameter not declared explicitly.	Static_020.c

Figure 3: Extracts from LDRA Tool Operational Requirements document as provided in the DO-330 TQSP

Tool Qualification Plan (TQP)

The Tool Qualification Plan document includes project specified information as identified in the Tool Verification Plan (Figure 4). 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).

7 Tool Qualification Data to be Produced					
The following tool qualification data will be produced or otherwise used under this TQP					
Item	ID	Source	Description	CC	Submit
1	PSAC	Project	The Plan for Software Aspects of Certification is the primary means used by the certification authority for determining whether an applicant is proposing a software life cycle that is commensurate with the rigour required for the level of software being developed. The PSAC is required to contain specific information regarding the intent to qualify the LDRA tool suite, and should reference this TQP. The PSAC should identify the specific certification credit sought, which may be identified by reference to specific sections in the TQP.	CC1	Yes
2	TQP	LDRA①	This LDRA provided Tool Qualification Plan is customised by the applicant in accordance with the instructions in the TVP for the LDRA tool suite. This TQP contains a description of the tool and its architecture, details of the certification credit sought, identifies the tool qualification activities to be performed, and summarises the tool qualification data to be produced.	CC1	Yes
3	TOR	LDRA	The LDRA Tool Operational Requirements identifies the operational requirements eligible for qualification under this TQP. The applicant should identify the specific requirements being qualified in the TAS and SAS. As the TOR is referenced by submitted data, it should be controlled as CC1 data by the applicant.	CC1	Avail
4	TVP	LDRA	The Tool Verification Plan is an LDRA provided instructional script for verification of the LDRA tool suite. The TVP refers to the TVCP to identify the test cases associated with each TOR. The applicant should be prepared to provide this document to the certification authority upon request.	CC2	Avail

Figure 4: Extracts from LDRA Tool Qualification Plan as provided in the DO-330 TQSP

Summary

“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.

Typically, but not uniquely, RTCA DO-330 is used for commercial aviation applications – for example, in conjunction with the guidance document DO-178C “Software Considerations in Airborne Systems and Equipment Certification.” RTCA DO-330 requires that tool qualification is achieved by means of a tool verification process. This dictates that each feature of the tool to be applied during the development process must be analysed and the results documented.

Many vendors including LDRA provide a collection of documentation including test cases with expected results and reporting processes. Usually known as Tool Qualification Kits or (as in LDRA’s case) Tool Qualification Support Packs, these artefacts can be used to show whether or not a tool has been configured appropriately to provide the correct results in the tool chain in which it will be deployed. There is nothing in DO-330 to suggest that the use of such supporting TQSPs is obligatory, but their use maximizes the efficiency of the tool qualification process.

Works cited

- [1] RTCA, Inc., RTCA DO-330 Software Tool Qualification Considerations, RTCA, Inc., 2011.
- [2] LDRA, “Products - LDRA tool suite,” LDRA, 2021. [Online]. Available: <https://ldra.com/automotive/products/>. [Accessed 26 August 2021].
- [3] RTCA, DO-178A “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 1985.
- [4] RTCA, DO-178B, “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 1992.
- [5] RTCA, DO-178C “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 2011.



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