LDRA
Software Technology

Technical White Paper

Test tool qualification for functional safety

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.

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.

All standards have a classification phase to establish the required confidence in the tool and a qualification phase that provides this level of confidence for some or all of its functionality. However, the classification and qualification methods differ in some details.

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 and commercial aviation environments, respectively.

This paper discusses the principles and concepts underpinning tool qualification processes and reviews the similarities and differences between these processes as detailed by ISO 26262 and DO-330.

With the shortfall in advice offered by other standards in mind, the document goes on to consider how the tool qualification processes laid out in ISO 26262 and DO-330 might lend themselves to adoption elsewhere.

It references the LDRA tool suite [4] 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 [5]:

"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 and DO-278A . For that reason, this document includes them within that collective term.

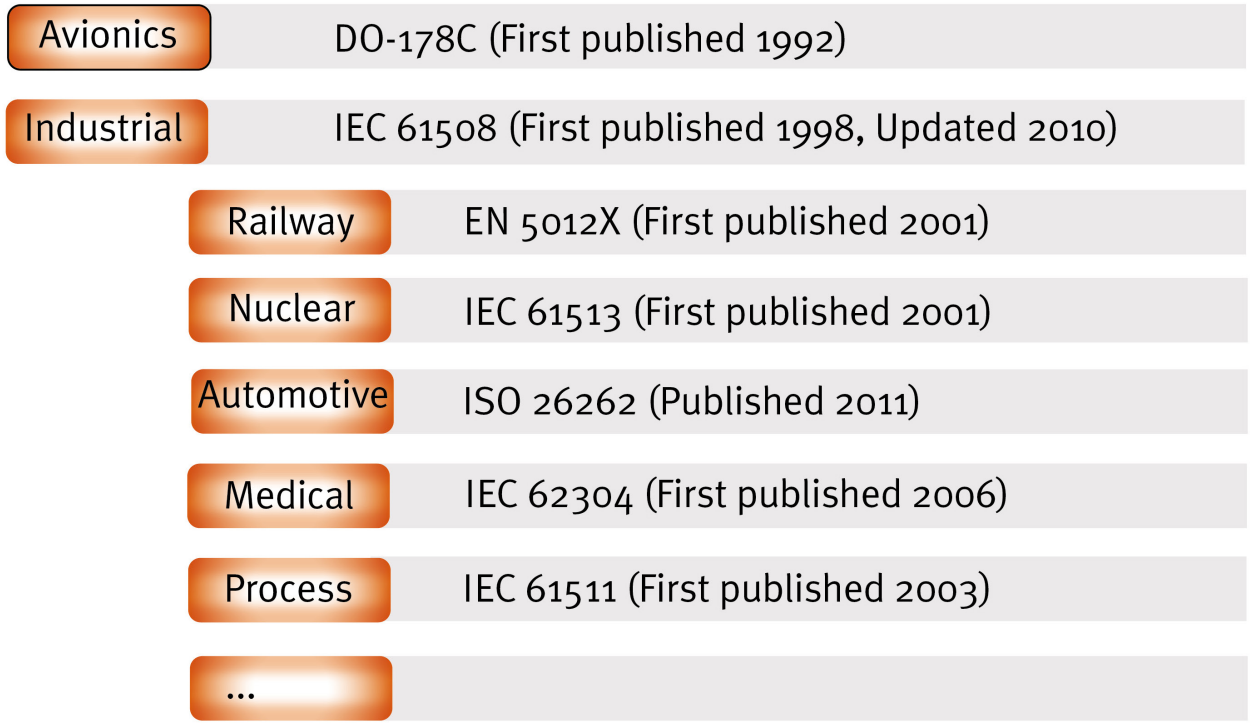


Figure 1: Most functional safety standards are direct derivatives of IEC 61508 – part of the "IEC 61058 family"

Approaches to tool qualification

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

- **Tool verification:** This represents the most thorough but most time consuming approach, but is generally applicable to all applications. Each feature of the tool is analyzed 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.
- **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.
- **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. 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 can be and often is applied in sectors outside commercial aircraft, as discussed later.

Detailed tool qualification processes in the functional safety standards

ISO 26262 Road Vehicles - Functional safety

ISO 26262 is an automotive industry specific derivation of the more generic functional safety standard IEC 61508. Despite that, ISO 26262-8 [6] §11 "*Confidence in the use of software tools*" presents a much more detailed definition of tool qualification than IEC 61508 itself, or most of its other derivatives.

This ISO 26262 supporting process defines a mechanism to provide evidence that the software tool chain can be relied upon. The required level of confidence in a software tool depends upon the circumstances of its deployment, with particular reference in §11.2 to "*the possibility that the malfunctioning software tool and its corresponding erroneous output can introduce or fail to detect errors in a safety-related item or element being developed; and the confidence in preventing or detecting such errors in its corresponding output.*"

The LDRA tool suite is classified as a TI2 (Tool Impact - 2) category tool because although a verification tool can fail to detect existing errors in source code, unlike (say) an auto code generator it cannot introduce errors into an application.

The TI2 classification dictates that the organization using the tool suite in the development of a compliant application is required to estimate the likelihood of them detecting any error in the tool's operation (Tool Error Detection), with categories ranging from TD1 (high confidence) to TD3. Evidence of the reasoning behind that assessment is required.

		Tool Error Detection		
		TD1	TD2	TD3
Tool Impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

Figure 2: Mapping the characteristics of the LDRA tool suite to "Table 3: Determination of the tool confidence level" from ISO 26262-8:2018

In turn, the TCL (Tool Confidence Level) is then derived from a look-up table as shown in Figure 2. Depending on the user's assessment of the application and with reference to its TÜV certification status (below), the resulting TCL will be either TCL1 or TCL2 for the LDRA tool suite. Generally, only TCL2 is realistically achievable.

For all ASILs, tools may be submitted to a validation process in order to confirm their suitability for purpose. However, that is a time consuming and costly approach, and alternatives are offered in the standard for all cases except where the tool suite is assigned TCL2 and the product is designated ASIL D (Figure 2).

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	+	+	+	++
"++" The method is highly recommended for this ASIL. "+" The method is recommended for this ASIL. Applying TCL2 designation					

Figure 3: Assessing the need for the qualification the LDRA tool suite when it is designated TCL2 from "Table 5: Qualification of software tools classified TCL2" from ISO 26262-8:2018

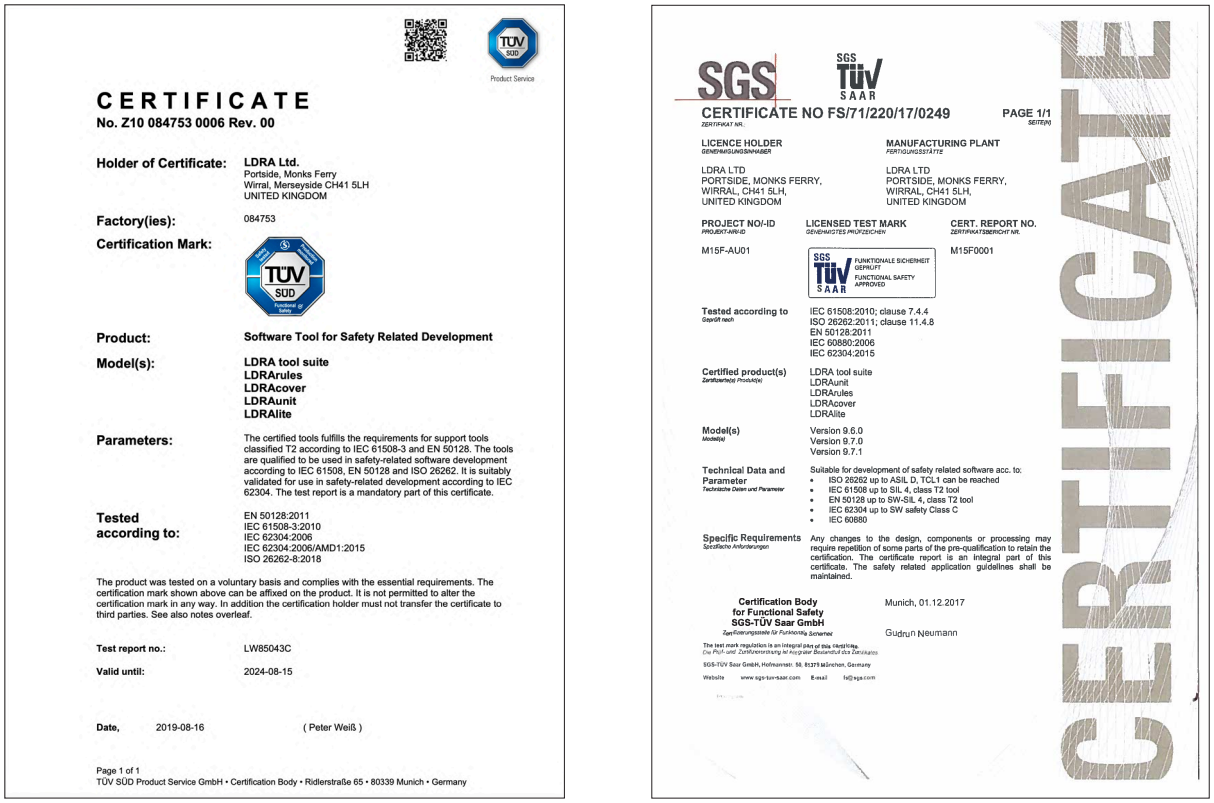
Alternative qualification methods for test tools

ISO 26262 permits the use of alternative qualification methods under some circumstances:

- **Proof in use:** Applicable where a software tool has been used previously for the same purpose with comparable use cases, in similar circumstances (highly recommended for ASIL A-C only).
- **Evaluation of the tool development process** such that evidence can be provided that a suitable software development process has been applied (highly recommended for ASIL A-C only).
- **Development in accordance with a safety standard** where the development of the tool itself complies with a safety standard (highly recommended for ASIL D).

TÜV certification

The second of these alternatives, the evaluation of the tool development process, provides a path followed by many to dramatically reduce the overhead involved with the tool qualification process.



CERTIFICATE
No. Z10 084753 0006 Rev. 00

Holder of Certificate: LDRA Ltd.
Portside, Monks Ferry
Wirral, Merseyside CH41 5LH
UNITED KINGDOM

Factory(ies): 084753

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): LDRA tool suite
LDRArules
LDRAcover
LDRAunit
LDRAlite

Parameters: The certified tools fulfills the requirements for support tools classified T2 according to IEC 61508-3 and EN 50128. The tools are qualified to be used in safety-related software development according to IEC 61508, EN 50128 and ISO 26262. It is suitably validated for use in safety-related development according to IEC 62304. The test report is a mandatory part of this certificate.

Tested according to: EN 50128:2011
IEC 61508-3:2010
IEC 62304:2006
IEC 62304:2006/AMD1:2015
ISO 26262-8:2018

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: LW85043C

Valid until: 2024-08-15

Date, 2019-08-16 (Peter Weiß)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

SGS TÜV SAAR

CERTIFICATE NO FS/71/220/17/0249 PAGE 1/1

LICENCE HOLDER
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

MANUFACTURING PLANT
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

PROJECT NO/-ID: M15F-AU01

LICENSED TEST MARK: SGS TÜV SAAR FUNKTIONALE SICHERHEIT GEPRÜFT FUNCTIONAL SAFETY APPROVED

CERT. REPORT NO.: M15F0001

Tested according to: IEC 61508:2010; clause 7.4.4
ISO 26262:2011; clause 11.4.8
EN 50128:2011
IEC 60880:2006
IEC 62304:2015

Certified product(s): LDRA tool suite
LDRAunit
LDRArules
LDRAcover
LDRAlite

Model(s): Version 9.6.0
Version 9.7.0
Version 9.7.1

Technical Data and Parameter: Suitable for development of safety related software acc. to:
- ISO 26262 up to ASIL D, TCL1 can be reached
- IEC 61508 up to SIL 4, class T2 tool
- EN 50128 up to SW-SIL 4, class T2 tool
- IEC 62304 up to SW safety Class C
- IEC 60880

Specific Requirements: Any changes to the design, components or processing may require repetition of some parts of the pre-qualification to retain the certification. The certificate report is an integral part of this certificate. The safety related application guidelines shall be maintained.

Certification Body for Functional Safety SGS-TÜV Saar GmbH
Munich, 01.12.2017
Gudrun Neumann

SGS-TÜV Saar GmbH, Hofmannstr. 50, 81379 München, Germany
Website www.sgs-tuv-saar.com E-mail fs@sga.com

CERTIFICATE

Figure 4: TÜV certification for LDRA tools

The most efficient way to comply with functional safety standards for complex projects is to use process automation, including automated test tools. However, regulatory authorities require that software tools used to automate, reduce or eliminate processes that contribute to the safety lifecycle must be qualified for their intended use. That implies detailed and thorough testing of those tools which is a time consuming and costly process.

In most cases, the most cost-effective approach is therefore to use a tool that is already approved for the applied standard by a TÜV certifying organization.

There are several TÜV certifying organizations. Although they each perform similar services, nevertheless there are sometimes subtle differences in approach between them. LDRA have chosen to secure approval from two completely independent TÜV certifying organizations for their products, leaving no room for doubt from any perspective that best practices have been applied in their development.

ISO 26262 qualification using Tool Qualification Support

For the most demanding ASIL D applications where a tool is assigned TCL 2, there is no alternative but to follow the ISO 26262 validation process.

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.

Referencing the LDRA tool suite as an example, the 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.

These five documents are as follows:

Tool Criteria Evaluation Report (TCER)

LDRA provide a generic Tool Criteria Evaluation Report 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.

Tool Operational Requirements (TOR)

The LDRA Tool Operational Requirements 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.

Tool Verification Plan (TVP)

The Tool Verification Plan 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.

Tool Verification Cases and Procedures (TVCP)

The Tool Verification Cases and Procedures provided by LDRA include source code, test cases, and expected results, for use in verifying the effectiveness of the tool in 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)

Tool Verification Results 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 customised operating conditions.

Details of the ISO 26262 tool qualification objectives fulfilled by following this process are detailed in Figure 5.

Part	Section	Description	Document/Life Cycle Data Reference
ISO 26262 Part 8	11.4.3	Compliance Check	TCER
	11.4.4	Planning of usage of a software tool	SVP, TCER, TVP
	11.4.4.1 (a), (b) and (d)	Tool Identification, Environment and Configuration	TCER, TVP, TQR
	11.4.4.1 (c)	Use Cases	TCER, TOR
	11.4.4.2 (a)	Features and Function of Tool	TCER, TVP
	11.4.4.2 (b)	User Manual	TVP
	11.4.4.2 (d), (e) and (f)	Anomalous condition, malfunction (including detection and prevention)	TCER, TOR
	11.4.5	Tool Evaluation	TCER
	11.4.6	Tool Qualification	TCER
	11.4.2	Validity Check of Tool confidence level and Qualification	TCER
	11.4.9	Validation of the software tool	TCER, TVP, TVCP, TVR
	11.4.9.2	Test Cases and Procedures	TVCP
	11.4.9.2	Test Verification Result	TVR
	11.4.10	Confirmation Review	TCER, TQR
	11.5.1	Software tool criteria evaluation report	TCER
	11.5.2	Software tool qualification report	TQR
ISO 26262 Part 6	9.4.5 Table 12 and 9.4.6	Structural coverage metrics at the software unit level and Test Environment	TCER, TVP, TVCP, TVR, TQR
ISO 26262 Part 2	6.4.7 Table 1	Confirmation review of the software tool criteria evaluation report and the software tool qualification report	Review Record
	6.4.7 Table 1	Independence regarding the developers of the item and project management Item 1: the confirmation measure shall be performed by a different person	Review Record

Figure 5: Tool qualification objectives fulfilled through the application of the LDRA Tool Qualification Support Package

RTCA DO-330 Software Tool Qualification Considerations

The guidance document DO-178 "Software Considerations in Airborne Systems and Equipment Certification" was first published in 1982. That first edition, which is known retrospectively as DO-178A [7], was re-written in 1992 as DO-178B [8] and updated again in 2011 as DO-178C [9] 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. Note, however, that DO-330 was specifically designed to be equally applicable to other functional safety sectors. From DO-330 §1.2 "Scope":

"Software tools are widely used in multiple domains, to assist in developing, verifying, and controlling other software... Examples are automated code generators, compilers, test tools, and modification management tools. This document explains the process and objectives for qualifying tools.

This document was developed for the following reasons:

a. *Tools are different from the software using the tools and form a unique domain; therefore, tool-specific guidance for both tool developers and tool users is needed.*

b. *Tools are often developed by teams other than those who use the tools to develop software. These tool development teams frequently do not have software guidance background (examples of guidance include DO-178C or DO-278A). This tool specific document benefits tool development teams and helps them avoid confusion and misinterpretation.*

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."***

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 used 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 6).

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 6: 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 Packages (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.

As for ASIL D ISO 26262 projects, 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 Package (TQSP) consists of five sub-packages 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 7).

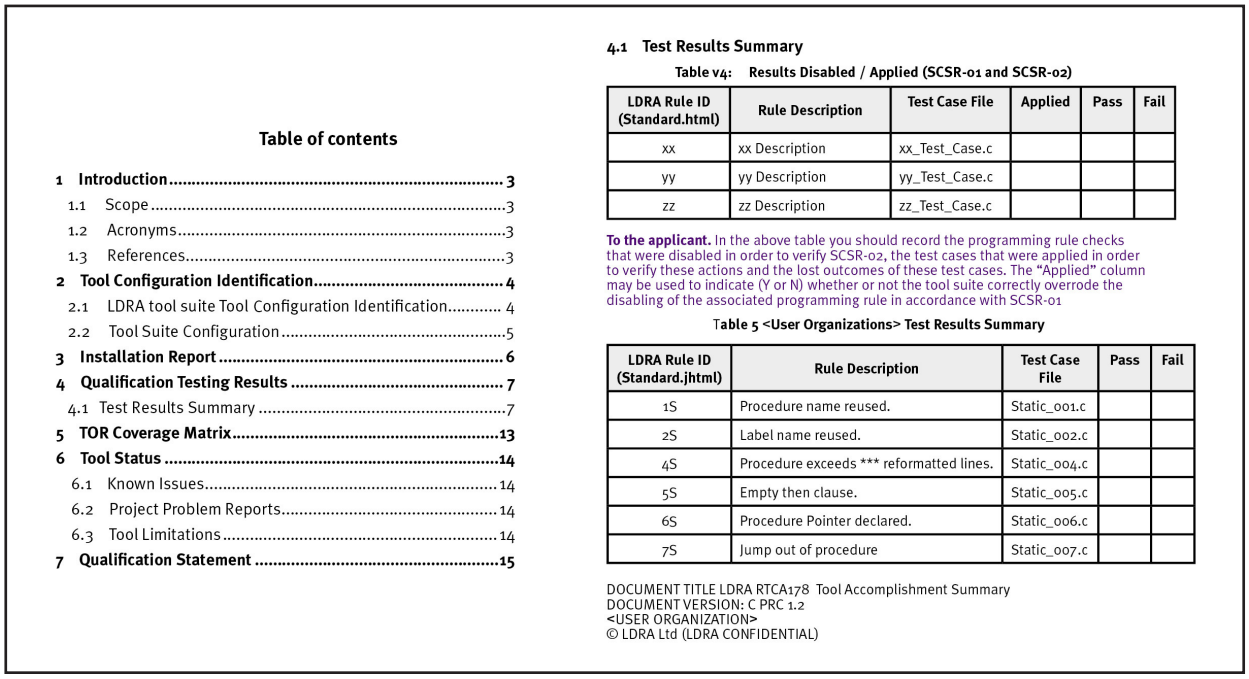


Table of contents

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 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 8.

3 Tool Operational Requirements

3.1 Application of specified Coding Standars 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 8: 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 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).

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

Tool qualification for 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. Consider these three examples.

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

This is perhaps most surprising in the case of IEC 61508, given that it forms the basis for the more sector specific ISO 26262.

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 [10] 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 [11] 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 26262 and DO-330 principles elsewhere

In general, it is the responsibility of the development team to decide what constitutes adequate "assessment", "justification" or "verification" which is not an easy judgement to make, let alone defend. 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. DO-330 is one of a set of supporting standards that were developed when DO-178B gave way to DO-178C, but unlike similar documents such DO-331 and DO-332 there is no specific reference to it being a "*supplement to DO-178C and DO-278A*". As previously discussed, the scope of the document itself reinforces the notion 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 perhaps a more obvious parallel in that regard. 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.

Potential impact of errors

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.

Type of tool

Both DO-330 and ISO 26262 differentiate between tools that can create an error (such as a code generator) and tools that may fail to detect one (test tools, including the LDRA tool suite).

Confidence requirements

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.

Alternative qualification methods

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.

Test verification technique

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.

ISO 26262 states that for most ASILs using tools that evidence of acceptable assessment (usually TÜV certification) will be sufficient reassurance that they are fit for purpose. But the fact that the most critical automotive applications demand tool qualification in the context of the nominated development environment suggests that a similar approach would be best practice elsewhere for the most demanding SILs or Classes covered by other sector specific standards.

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

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

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

[7] RTCA, DO-178A “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 1985.

[8] RTCA, DO-178B, “Software Considerations in Airborne Systems and Equipment Certification”, RTCA, 1992.

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

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

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

[12] International Electrotechnical Commission (IEC), IEC 61508:2010 “Functional safety of electrical/electronic/programmable electronic safety-related systems” (all parts), IEC, 2010.

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

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