Boeing 767

DO-178B Tool Qualification Support Packs

Introduction

DO-178B/ED "Software Considerations in Airborne Systems and Equipment Certification", is the prevailing standard for critical software development in the avionics industry worldwide. As one of the most stringent software development standards, it is also becoming (partially) adopted within sectors such as automotive, medical, defence or transportation where life-critical systems are manufactured.

DO-178B classifies software into 5 levels of criticality related to software anomalous behaviour that would cause or contribute to a failure of system function:

- Level E: with no effect on system operational capability
- Level D: resulting in a minor failure condition for the system
- Level C: resulting in a major failure condition for the system
- Level B: resulting in a hazardous/severe-major failure condition for the system
- Level A: resulting in a catastrophic failure condition for the system

Each level clearly specifies software testing requirements:

- Level E: no specific requirement
- Level D: 100% Requirement Coverage
- Level C: Level D + 100% Statement Coverage
- Level B: Level C + 100% Decision Coverage
- Level A: Level B + 100% Modified Condition Coverage (MC/DC)

Sukhoi Superjet 100

As an important complement to LDRA tool suite, LDRA offers a Tool Qualification Support Pack (TQSP). Qualification of a verification (test) tool is needed when the test processes are eliminated, reduced or automated by the use of a software tool without its output being verified as specified in [DO178B-§6]. The use of software tools to automate activities of the software lifecycle processes can help satisfy system safety objectives insofar as they can enforce conformance with software development standards and use automatic checking.

The objective of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of the processes eliminated, reduced or automated. If partitioning of tool functions can be demonstrated, only those functions that are used and whose outputs are not verified need to be qualified.

As required in DO-178B for qualified verification tools, LDRA products are tools that cannot introduce errors in the embedded code, but are in charge of detecting them. For that purpose, the LDRA tool suite satisfy qualification requirements that are mandatory for verification tools [DO178B-§12.2.2].

Tool Qualification Support Packs (TQSPs)

LDRA provide the following Tool Qualification Support Packs (TQSPs) to support the qualification of the key facilities of the LDRA tool suite:

1. Programming Standards Checking (PSC)

   As part of Section 5.3, the software development process, DO-178B specifies that software must meet certain software coding process requirements. These include adherence to a set of software coding standards. This TQSP is designed to support the qualification of the tool supported Programming Standards Checks which may form part of a user-defined quality model for which the users wish to take credit.

2. Structural Coverage Analysis (SCA)

   Structural Coverage Analysis requirements are laid out in section 6.4.4.2 of DO-178B. This TQSP is designed to support the qualification of the tool supported Structural Coverage Analysis facilities for which the users wish to take credit.

3. Programming Standards Checking & Structural Coverage Analysis

   This TQSP is designed to support the qualification of both the Programming Standards Checking and Structural Coverage Analysis facilities of the LDRA tool suite.

Programming Standards Checking and Structural Coverage Analysis currently represent the two main spheres of tool usage in support of DO-178B compliance. Users wishing to take credit for tool facilities which fall outside these areas must provide their own, additional, qualification artifacts.

Pratt & Whitney F135 Engine for Joint Strike Fighter

Tool Qualification Artifacts

A TQSP is an aid to tool qualification, but requires user input to complete the process. The key qualification artefacts for which the LDRA supplied TQSPs provide support are as follow:

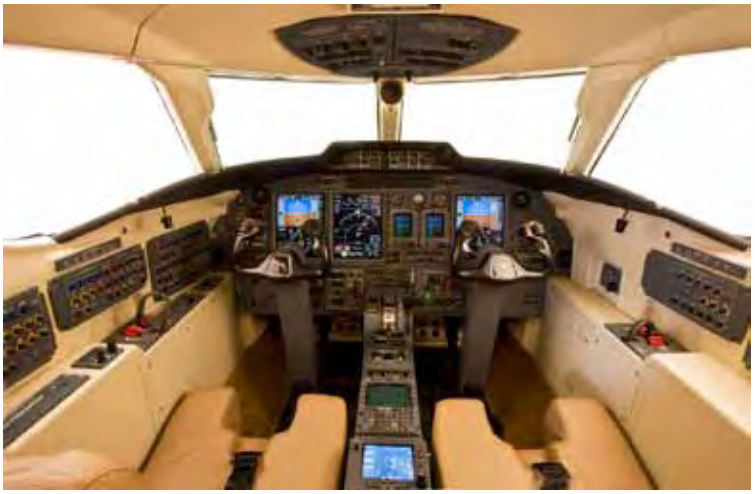
1. **Plan for Software Aspects of Certification (PSAC)**

   In support of PSAC requirements the TQSP document - LDRA Tool Qualification Support Document - provides an overview of the LDRA tool suite itself, an insight into the development, configuration management and quality assurance processes that are applied to the tool and new tool releases and the stringent, company-wide quality processes that are applied at all levels.

2. **Tool Qualification Plan (TQP)**

   In support of TQP requirements the TQSP identifies and documents the Tool Operational Requirements (TOR) in the document LDRA Tool Qualification TOR. In addition to identifying the TOR this document also provides a basic outline of the verification process and the LDRA supplied test cases that are required to satisfy each individual TOR. For any given TOR the outline of the verification process that is provided is only a guideline as it cannot take into account any additional process requirements that are specific to the user's particular target/qualification environment. As such any additional detail, if required, must be provided and documented by the individual user/qualifier. The TQP requirements are then further supported through the document - LDRA Tool Qualification TOR Appendix TOR1. The purpose of this latter document is to provide a greater depth of information relating to the analysis techniques and combinations of analysis techniques that facilitate the set of available Programming Standards Checks and Structural Coverage Analysis metrics provided by the LDRA tool suite and also describe in detail exactly how those metrics/checks are calculated and presented to the user/qualifier. In particular this document outlines how the output of the LDRA tool suite satisfies the MC/DC coverage requirements as specified by the CAST-10 position paper. While not essential for the purposes of verifying the identified TOR the information within this document provides supporting information which is designed to assist users/qualifiers who are perhaps less familiar with the tool and the analysis facilities and techniques that it supports.

Embraer 170/190 Family of Comercial Aircraft



The Sino Swearingen SJ30 cockpit features the Honeywell Primus Epic™(CDS) avionics package.

Eurofighter Typhoon

3. Tool Accomplishment Summary (TAS)

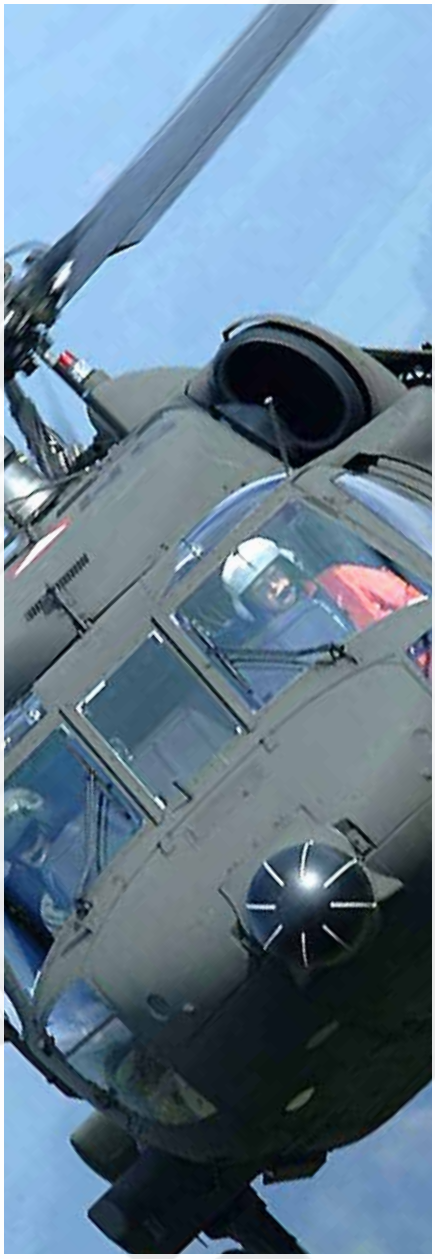
In support of the TAS requirements the LDRA supplied TQSP provides sets of deterministic test cases (depending on licensed tool configuration) which are designed to demonstrate the identified TOR. The user/qualifier must then apply the test processes identified and documented in the Tool Qualification Plan (TQP) against these test cases and record the results.

The Programming Standards Checking test cases that are provided are each intended to demonstrate the identification and reporting of a specific, individual, programming standards check supported by the tool suite. The user/qualifier must then identify the set of programming standards checks and set of associated test cases which are applicable to their user-defined quality model, apply the test processes identified and documented in the Tool Qualification Plan (TQP) against these test cases and record the results.

In respect of TOR related to the Structural Coverage Analysis aspects of tool suite functionality, unless explicitly stated, the test cases and input values specified by LDRA will allow for the accumulation of 100% Structural Coverage Analysis to the desired DO-178B qualification level. Those test cases which do not allow for the accumulation of 100% MC/DC coverage are specifically designed to demonstrate the affects of strongly-coupled condition pairs within the same Boolean expression which, when analysed through the application of a unique-cause approach which is the LDRA tool suite default, cannot be shown to satisfy MC/DC criteria with independence.

The Structural Coverage Analysis test case source files that are provided are designed to be host and target independent. All of the source files take the form of single functions with no main programs. The LDRA suggested data must be passed to these files via input parameters. As the method for passing data to and from any given test case is entirely test/qualification environment specific it is the responsibility of the user/qualifier to generate the required driver (main) program and any additional, target specific facilities that will enable this process. Such mechanisms must also take into account that any such user-defined data transfer method must be bi-directional to allow for data input and the corresponding data retrieval of control flow data (execution history output) that forms the input to the structural coverage analysis facilities provided by the LDRA tool suite.

In respect of the recording and presentation of test case outcomes, the TQSP incorporates templated 'Tool Accomplishment Summary' tables which are provided in the document, LDRA Tool Qualification Support Document Appendix TQSD1.



Sikorsky UH 60 M Black Hawk

Pedigree

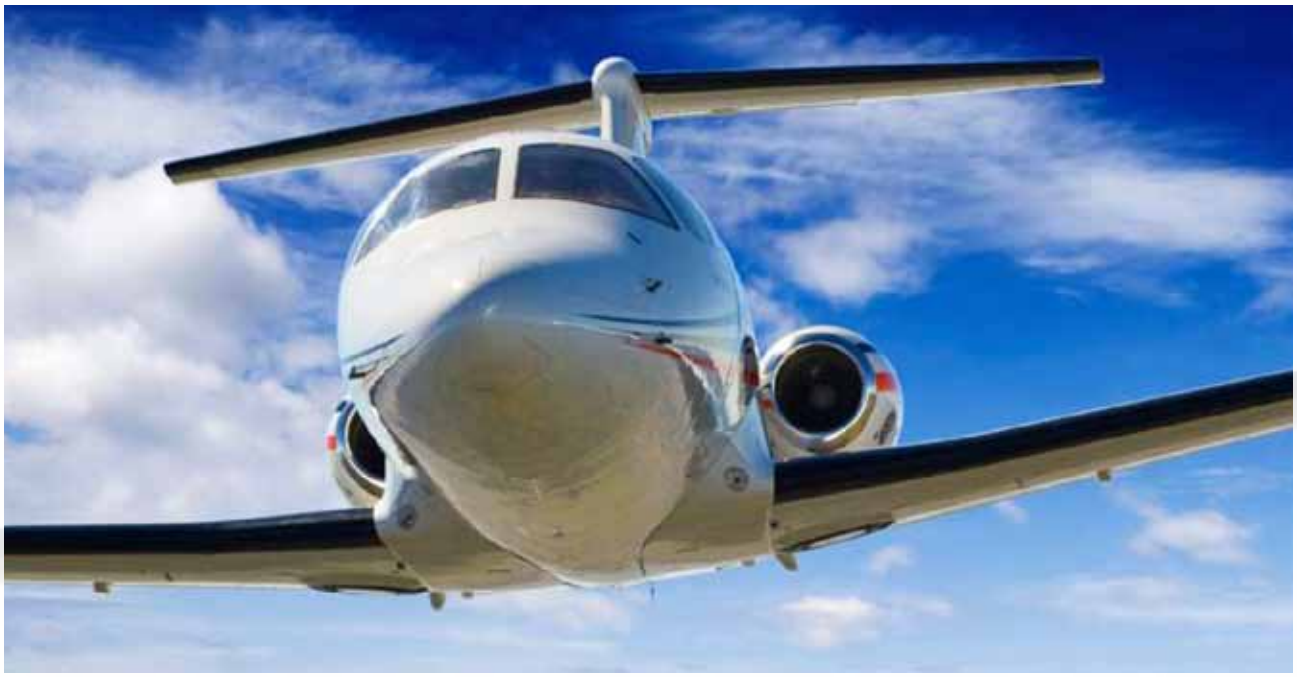
LDRA has 16+ years of experience supporting its customers through the DO-178B Tool Qualification process. This has included company audits performed by LDRA's customers and certifying authorities. In this timescale the LDRA tool suite has been qualified for use on a large number of DO-178B certified civil and military aerospace projects to Levels A, B, & C. The track record since LDRA issued its first TQSP in 2004 speaks for itself:

- 99 certifications for 40+ companies
- 40+ Level A certifications
- Many more certifications prior to the availability of the LDRA TQSP

Availability

TQSPs are produced for:

- Programming Standards Checking and/or
- Structural Coverage Analysis
- A specified high level programming language (Ada, C, C++, Java) and/or Object Code (Assembler incl. PowerPC, Intel, Texas Instruments.....)
- DO-178B Certification Levels A, B & C



Total Eclipse 500

For more information please contact LDRA either through you local representative or email:

w: www.ldra.com e: info@ldra.com