Demystify the who, what, when and why of successful DO-178C compliance.

DO-178C/ED-12C (henceforth DO-178C) is the primary document referenced by certification authorities including the FAA, EASA and Transport Canada to approve all commercial software-based civil aviation avionics systems. The document is jointly published by RTCA (formerly the Radio Technical Committee for Aeronautics) and EUROCAE.
DO-178C recognizes that to ensure correctness, control and confidence in software, functional safety must be addressed systematically throughout the software development life cycle.

DO-178C recognizes that to ensure correctness, control and confidence in software, functional safety must be addressed systematically throughout the software development life cycle.

- What is DO-178C?
- What is the difference between DO-178C and DO-178B?
- What other standards are related to DO-178C?
    - DO-178C and SAE ARP4754
    - DO-178C and SAE ARP4761
    - DO-178C and DO-278A/ED-109
    - DO-178C a

    - DO-178C and DO-332/ED-217
    - DO-178C and DO-333/ED-218
    - DO-178C and DO-200/ED-76
    - DO-178C and DO-333/ED-218
    - DO-178C, CAST-32A, and A(M)C 20-193
- What does DAL mean in the context of DO-178C?
- What is involved with DO-178C compliance?
- How does LDRA help with DO-178C compliance?
    - Static analysis
    - Dynamic analysis
    - Multicore processors, execution timing and interference research
    - Bidirectional requirements traceability
    - Data Coupling and Control Coupling
    - Modified Condition / Decision Coverage (MC/DC)
    - Source code to object code traceability
    - Evidential artefacts
    - Tool Qualification
    - Certification services
- Additional information
        - DO-178C pdf free downloads
        - DO-178C further information

What is DO-178C?

DO-178C is a formal process standard that covers the complete software lifecycle – the planning process, development process, and

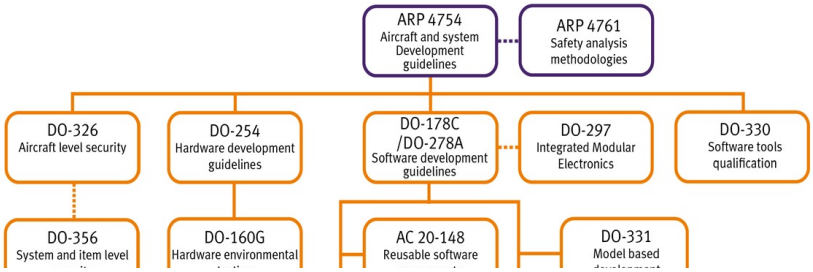
integral processes – to ensure correctness and robustness in software developed for civil avionics systems. The integral processes include software verification activities, software quality assurance, configuration management assurance and certification liaison with the regulatory authorities. Increasingly, standards developed for civil avionics systems including DO-178C have also become recognized as best practice in the defence sector.

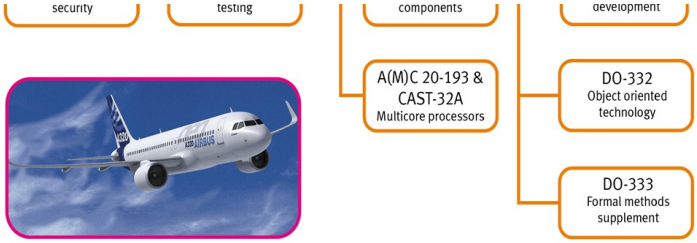
What is the difference between DO-178C and DO-178B?

In January 2012 DO-178C replaced the long-standing DO-178B standard as the de facto reference for the development of embedded software in the civil aviation sector. Its introduction improved safety requirements and the accommodation of new technologies for development and verification activities in civil avionics systems.

LDRA has participated extensively on both the DO-178B and DO-178C committees over nearly two decades. Mike Hennell, LDRA's CEO, was instrumental in the inclusion of several test measurement objectives in the standard, including those relating to structural coverage analysis. The LDRA tool suite® was itself a forerunner in automated verification for certification to DO-178B.

What other standards are related to DO-178C?





There are several standards and other documents that are intended to be used as a collective in the development of software systems that are applicable to civil avionics systems.

DO-178C and SAE ARP4754

SAE ARP4754 Guidelines for Development of Civil Aircraft and Systems.
ARP 4754 provides the overarching framework for system development, while DO-178C provides specific guidance for the development and certification of software within that system. Together, the two documents help ensure that the entire airborne system, including its software components, meets the necessary safety and reliability standards for certification in the aerospace industry.

DO-178C and SAE ARP4761

SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.
ARP 4761 provides guidance on conducting safety assessments for the systems that are developed in accordance with ARP4754. In turn, ARP 4754 provides the overarching framework for system development, while DO-178C provides specific guidance for the development and certification of software within that system.

DO-178C and DO-278A/ED-109

RTCA DO-278A Guidelines for communication, navigation, surveillance and air traffic management (CNS/ATM) system software integrity assurance.

DO-278A serves a similar purpose for ground-based systems to that served by DO-178C for airborne systems, and was developed in parallel to it. As a result, around 75% of it is similar.

DO-178C and DO-330/ED-215

RTCA DO-330 Software tool qualifications considerations.
"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. DO-330 provides guidance in the achievement of DO-178C tool qualification and DO-278C tool qualification for tools to be used in the pursuit of compliance with those documents. It is also designed for use in other domains unlike the other supplementary documents DO-332 and DO-333.

DO-178C and DO-332/ED-217

RTCA DO-332 "Object Oriented Technology and related technologies supplement to DO-178C and DO-278A".

DO-332 is supplementary to DO-178C and DO-278A and includes additional objectives that apply when using object-oriented programming and complementary practices. It also provides advice on how the objectives in DO-178C should be approached in the Object Oriented (OO) environment.

DO-178C and DO-333/ED-218

RTCA DO-333 “Formal Methods Supplement to DO-178C and DO-278A”.

DO-333 is supplementary to DO-178C and DO-278A and identifies additional objectives that apply when using formal methods as part of a software life cycle. It also provides advice on how the objectives in DO-178C should be approached when formal methods are being applied.

DO-178C and CO-200/ED-76

RTCA DO-200 “Standards for Processing Aeronautical Data”.

DO-200 establishes the essential criteria and recommendations for handling aeronautical data applied in navigation, flight planning, terrain/obstacle awareness, flight deck displays, flight simulators, and various applications. It outlines the requirements for developing, evaluating changes, and supporting the implementation of data quality management. The standard covers aeronautical databases and the related data processing, which may interface directly with DO-178C compliant applications utilized in airborne aviation products.

DO-178C, CAST-32A, and A(M)C 20-193

CAST-32A was a Position Paper relating to multicore processors (MCPs), written by the Certification Authorities Software Team (CAST). Multicore processors are a relatively new challenge in the world of civil aviation, and this paper describes a set of objectives to be fulfilled when such devices are selected for use in a DO-178C compliant project. Although CAST papers do not represent official guidance, they are authoritative, and their advice is often adopted even before it is formally integrated into subsequent published

standards.

CAST-32A has been deprecated for projects under the jurisdiction of EASA and the FAA. Its recommendations relating to multicore processors are incorporated in the harmonized standards EASA AMC 20-193 and FAA AC 20-193 known collectively as A(M)C 20-193. The advice and guidance in these documents is designed to be supplemental to DO-178C and other related standards such as DO-278A.

The LDRA tool suite supports the use of MCPs, which brings a host of challenges associated with interference paths and their potential impact on worst-case execution timing (WCET).

What does DAL mean in the context of DO-178C?

DAL is an abbreviation for Design Assurance Level, sometimes referred to a simply a Level. The ARP 4754A standard dictates that functional hazard analyses and system safety assessments are completed prior to a system's development. A Design Assurance Level (DAL) is assigned accordingly for that system, and for the subsystems that implement its hardware and software requirements. The DO-178C standard then provides detailed guidance for the development and verification of safety critical airborne software systems in accordance with the assigned DAL, such that the effort and expense of producing such as a flight control system is necessarily higher than that required to produce (say) a bathroom smoke detector.

What is involved with DO-178C compliance?

DO-178C covers the complete software lifecycle: the planning process, development process and integral processes to ensure

correctness and robustness in the software. The integral processes include software verification activities, software quality assurance, configuration management assurance and certification liaison with the regulatory authorities and although they do not oblige developers to use analysis, test, and traceability tools in their work, such tools improve efficiency in all but the most trivial projects to the extent that they have a significant part to play. The extent of the work is proportionate to the risk involved should the software fail, and hence is proportionate to that DAL applied to it.

How does LDRA help with DO-178C compliance?

The DO-178C standard calls for phased development with the application of verification and validation techniques along the way to confirm compliance with the standard. LDRA validation and verification tools (exemplified by the LDRA tool suite) lend themselves to integration with third party development tools, providing a seamless platform for compliant application development.

Static analysis

LDRA tools perform static analysis on the code in accordance with DO-178C's recommended practices. Static analysis can be likened to an automated "inspection" of the source code, comparing the code under review with the chosen software coding standard and deriving code quality metrics.- Non-conformances are highlighted as required by DO-178C, along with other undesirable characteristics such as high complexity.

Dynamic analysis

The use of LDRA tools' dynamic analysis capabilities involves the execution of some or all of the code as part of low-level (unit) test, integration test, and system test. The objective here is to show that it has been exercised sufficiently and that it behaves in accordance with requirements. The on-target, dynamic test capabilities are particularly important in demonstrating that the code is appropriate for its target environment.

Structural coverage is used to identify which code structures and component interfaces have been exercised during the execution of requirements-based test procedures, facilitating the empirical measurement of requirements-based test effectiveness. As the name implies, structural coverage analysis involves the scrutiny of the structural coverage to determine if there are any parts of the code which have not been sufficiently exercised, and if not, why. The level of coverage required is proportionate to the Design Assurance Level (DAL) of the software under development.

The optional TBjustify module can be specified to manage the documentation of justifications concerning coverage for certification and compliance purposes.

Multicore processors, execution timing and interference research

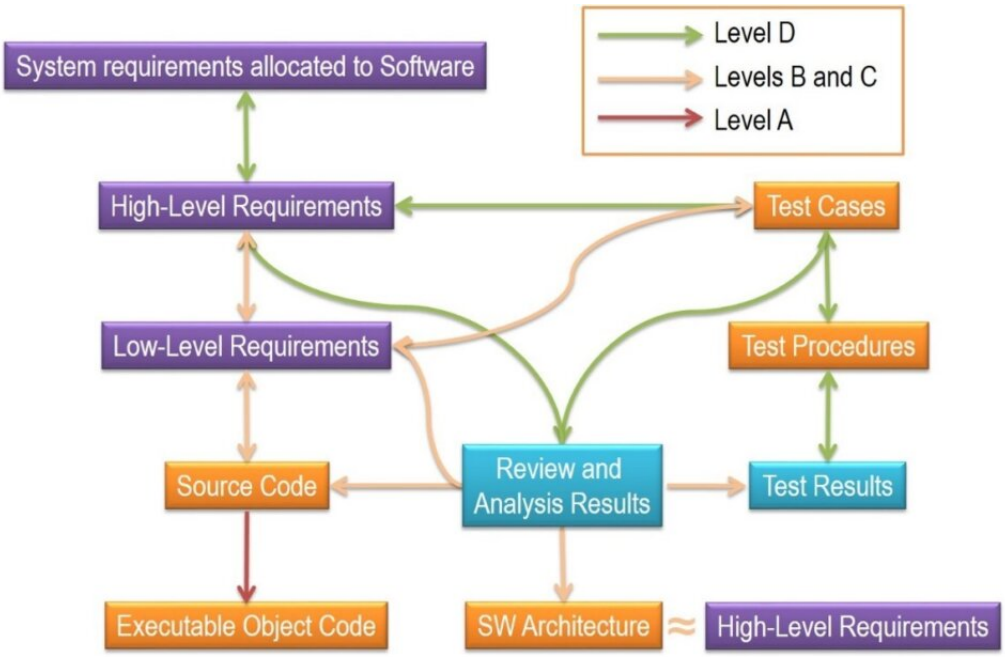
Real-time critical systems demand quick decision-making processes. They deploy closed-loop control, allowing only a tight time window to gather data, process that data, and update the system. As referenced by the CAST-32A & A(M)C 20-193 documents, Hardware Shared Resources (HARs) and associated interference channels make that a particularly thorny challenge when developing systems to run on multicore processors (MCPs).
LDRA offers a uniquely malleable tool set to meet the challenge of analysing execution times and hence demonstrating that Worst Case Execution Times (WCET) will not exceed their allotted windows.

Bidirectional requirements traceability

DO-178C insists that systems requirements should be traceable through to every stage of development, and vice versa to ensure that the whole code base is traceable to requirements. LDRA provides a comprehensive, role-based approach to bidirectional traceability.

Systems requirements and verification tasks can be assigned to team members, and all resulting artefacts can be aggregated and linked. The result is a complete bidirectional process across the life cycle, ensuring that any changes to requirements, design, or source code are easily understood, verified, and traced.

LDRA tools help to detect changes in requirements or the developed software and easily organize and re-run appropriate tests against any affected components. They provide an optimal environment for determining impact analysis either upstream to requirements or design or downstream to implementation and test.



Data Coupling and Control Coupling

LDRA verification tools provide the facility to fulfil DO-178C's

requirements for data control coupling metrics. The intent is to show that the software modules affect one another only in the ways intended by the software design, ensuring that there are no unplanned, anomalous, or erroneous behaviours. Documenting data and control coupling during design provides a set of requirements to test during the software integration process. Similarly, ensuring that the data and control coupling between modules are exercised and exhibit no faults during software test demonstrates that the integration and architecture of the software is fully verified.

Modified Condition / Decision Coverage (MC/DC)

In addition to statement and branch coverage, for level A software MC/DC coverage is obligatory. MC/DC requires that 'Each condition in a decision has been shown to independently affect that decision's outcome'. LDRA verification tools provide a mechanism to automate that process.

Source code to object code traceability

For Level A systems, structural coverage at the source level isn't enough. Compilers often add additional code or alter control flow, and often their behaviour is not deterministic. To ensure that functionality is not compromised, DO-178C 6.4.4.2.b demands source to object code traceability. It states:

"*if the software level is A and a compiler, linker, or other means generates additional code that is not directly traceable to Source Code statements, then additional verification should be performed to establish the correctness of such generated code sequences*"

An automated mechanism to provide evidence of that verification can make that process much more efficient. Because there is a direct one-to-one relationship between object code and assembly code, one way for a tool to represent this is to display a graphical

representation of the source code alongside the equivalent representation of the assembly code. Object Code Verification (OCV) measures code coverage at both the source and the assembly level by instrumenting each in turn

Evidential Artefacts

DO-178C compliance requires that compliance demonstration data – a collection of documents, records, and evidence – are presented to regulatory authorities to demonstrate that the software development and verification processes adhere to DO-178C.

This data typically includes various reports and artefacts that showcase how the software was developed, tested, and verified, and the reports generated by the LDRA tool suite are designed to be appropriate for that purpose.

For example, key components of DO-178C compliance demonstration data
include:

- Software Accomplishment Summary (SAS): Offers an overall summary of the software development and verification activities, providing a compliance position, timing, and memory margins, and summarizing any deviations or outstanding issues.
- Software Verification Results (SVR): Lists the results of verification activities, such as reviews, analyses, and tests. It includes information on passed and failed verification tasks, along with traceability and coverage data.
- Traceability Matrix: Demonstrates the traceability between software requirements, design artifacts, and verification activities, ensuring that each requirement is covered by corresponding verification tasks.
- Code Coverage Analysis Report: Provides information on the extent to which the source code has been exercised by test

cases. This is important for ensuring that the software has been thoroughly tested.

- Structural Coverage Analysis Report: Examines the coverage of various structural elements in the code, such as branches, statements, and conditions, to assess the thoroughness of testing.
- Object Code Verification Report: Required for critical software levels, this report demonstrates that the binary or executable code matches the source code, and that the compilation process has been correctly executed.

This data is submitted to aviation authorities for review and approval before
the software can be certified for use in aircraft.

Tool Qualification

DO-178C requires that development tools are qualified for use on a compliant system. The LDRA Tool Qualification Support Packs (TQSPs) contain the test cases to demonstrate both the structural coverage analysis and programming rules checking capabilities of the tool suite itself in accordance with DO-330 Software Tool Qualification. In addition, associated documentation for the development and verification of the product is provided, including plans, procedures, and expected results.

Certification services

LDRA Certification Services (LCS) is a division of LDRA that offers the first comprehensive and fully compliant FAA and EASA certification solution. Proficient in both commercial and military airworthiness regimens, LCS can address all critical project requirements as they relate to certification, including systems and safety analyses, management and planning, staff training, development, and

verification.

Additional information

DO-178C pdf free downloads

Technical briefing: DO-178C: Get on a High with your software development

Technical white paper: Verification of Airborne Software in Compliance with DO-178C

Technical white paper: Developing compliant critical software systems with multicore processors

Technical briefing: Getting to grips with CAST-32A & A(M)C 20-193

Technical white paper: Following the recommendations of CAST-32A & A(M)C 20-193

Technical white paper: Developing compliant critical software systems with multicore processors

DO-178C further information

On Demand DO-178C “First Flight” Self-paced online training course

LDRA Civil Aviation Resource Centre

LDRA Defence Resource Centre

Ensuring the compliance of avionics software with DO-178C

Richland technologies case study

DO-330 Test tool qualification for aerospace applications

Company

About Us

ISO and TÜV certification

Partners

Careers

Newsroom

Resource Centre

Blog

Contact Us

Email Us

Email: info@ldra.com

Call Us

EMEA: +44 (0)151 649 9300

USA: +1 (855) 855 5372

INDIA: +91 80 4080 8707

Connect with LDRA

Privacy Policy | Cookie Policy