

LDRA tool suite® and DO 278A

RTCA DO-278A (also known as EUROCAE ED-109A) “Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance” is used in developing software associated with ground-based systems that are involved with aircraft operations. Its scope includes the “Next Generation Air Transportation System” (NextGen), a modernization of the CNS/ATM system. DO-278A was deliberately designed to be analogous to its sister document, DO-178C. For the most part, developers who are familiar with DO-178C terminology, practices, and processes will be similarly comfortable with the objectives of DO-278A.

The capabilities offered by the tool suite are equally applicable to both standards. The LDRA tool suite is designed to support the key software verification activities specified in them. Features including static analysis, dynamic analysis, unit test, on-target testing and requirements traceability collectively provide a means to achieve compliance in an efficient, timely and cost-effective manner. All these capabilities are described in LDRA’s DO-178C related collateral and documentation.

This document can therefore be regarded as an addendum to that content. There are two key differences between DO-178C and DO-278A to be aware of. They concern assurance levels and Commercial Off-The-Shelf (COTS) software.

Assurance Levels

	DO-178C Design Assurance Level		DO-278A Assurance Level
Catastrophic	DAL A	is equivalent to	AL1
Hazardous	DAL B	is equivalent to	AL2
Major	DAL C	is equivalent to	AL3
(No assignment)	There is no equivalent to		AL4
Minor	DAL D	is equivalent to	AL5
No effect	DAL E	is equivalent to	AL6

Figure 1: Equivalence of DO-178C and DO-278A assurance levels

As shown by Figure 1 DO-178C DALs map directly to DO-278A ALs with one exception. There is no equivalent to DO-278A’s AL4.

DO-278A AL4 and COTS

DAL C and AL3 are each concerned with how software is designed and implemented. On the other hand, DAL D and AL5 are concerned only that software fulfils its intended function within a system-level engineering process. AL4 represents a “halfway house” in that it retains some design-level verification (unlike AL5) but it does not require any code-level analysis (unlike AL3).

This is pertinent to DO-278A but not DO-178C because ground-based systems often make far more extensive use of both COTS and legacy technologies.

CNS/ATM system developers and certification authorities are generally more accepting of reused proven technology, even if not developed in accordance with DO-278A. As a result, DO-278A provides explicit provisions for potentially utilizing “alternate methods” which become Alternate Means of Compliance (AMC). Software that has been verified as compliant using an alternative method is assured to AL4.

The LDRA tool suite and DO-278A



Figure 2: Key functionalities of the LDRA tool suite

The LDRA tool suite is designed primarily to be an automated set of verification and validation tools for developers developing critical embedded or host-based software in accordance with related standard (Figure 2). It is therefore precisely relevant to software development that is required to meet DO-278A AL1-AL3 and AL5-AL6 inclusive.

Any such development is likely to be part of a larger system that includes software to be approved in accordance with AMCs. The TBmanager component of the LDRA tool suite can monitor and demonstrate both the bidirectional traceability to requirements of code developed from first principles, and that of AL4 compliant software through links to externally generated documentation.

Summary

For the most part, DO-278A compliant software development is equivalent to similarly critical DO-178C software. The LDRA tool suite is designed to support that development, including NextGen. DO-278A has many provisions for Alternative Means of Compliance of COTS and legacy software. The TBmanager of the LDRA tool suite supports these provisions, facilitating bidirectional traceability of both types of software to project requirements and standards' objectives.



LDRA
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, Suite 228
Lewisville, Texas 75056
United States
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