

ECSS standards: Compliance with ECSS-E-ST-40C and ECSS-Q-ST-80C Rev1

The ECSS set of standards are for use in all European space activities and are designed to be coherent and user friendly. Many of the standards have an impact on the software development process, with two in particular being specific to software development:

- ECSS-E-ST-40C concerns product software that is part of a space system product tree and developed as part of a space project.
- ECSS-Q-ST-80C Rev1 defines a set of software product assurance requirements pertinent to the development and maintenance of software for space systems.

The LDRA tool suite is designed to support the key software development and verification activities specified in the standards. Features including static analysis, source and object code coverage analysis, unit test, on-target testing and requirements traceability collectively provide a means to achieve compliance in an efficient, timely and cost-effective manner.

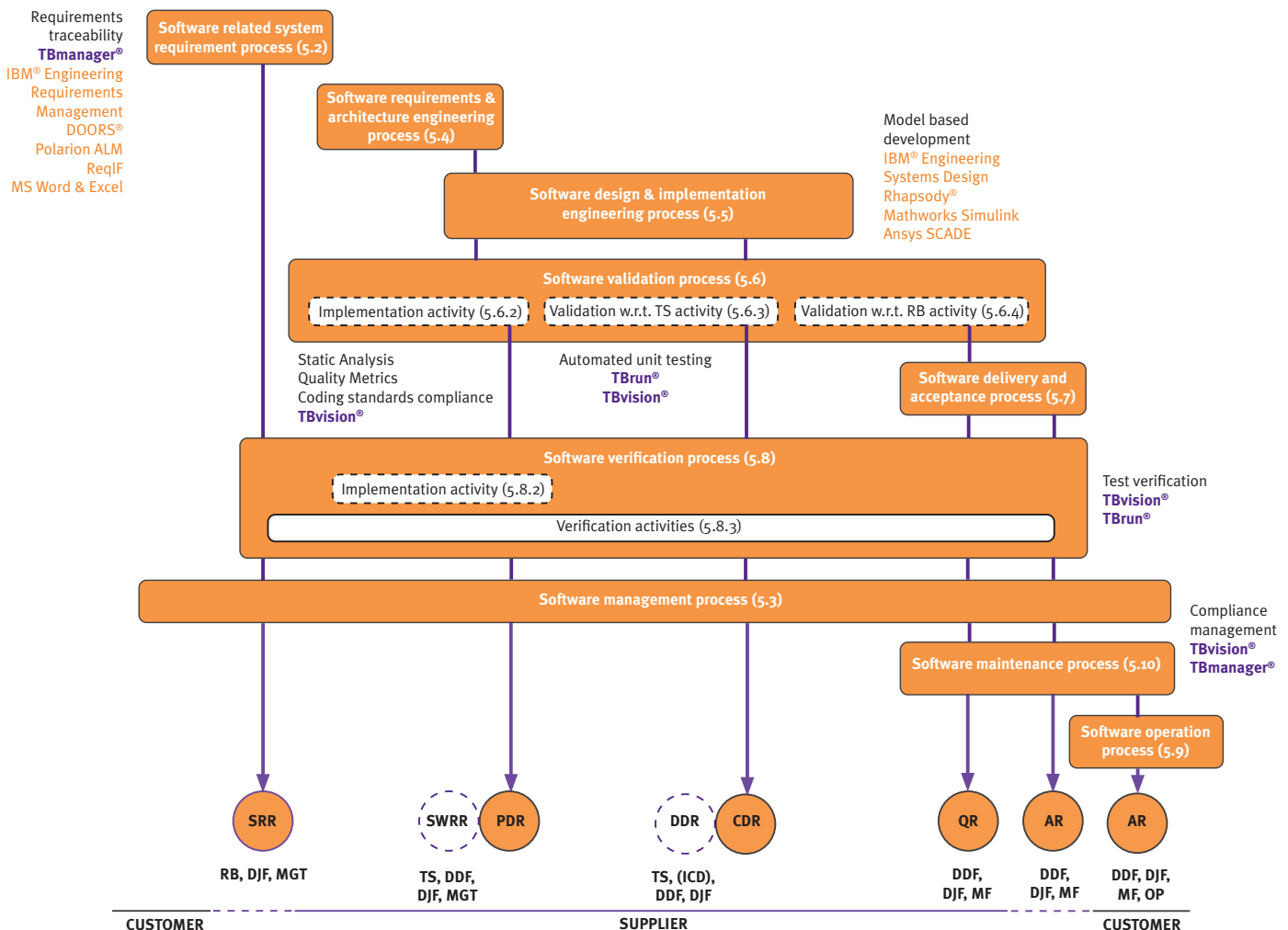


Figure 1: Mapping the capabilities of an automated tool chain including the LDRA tool suite to the ECSS-E-ST-40C process model

Key Benefits

LDRA's ECSS software development compliance solutions:

- rapidly perform automated static analysis, dynamic analysis, unit testing, structural coverage, test case creation, and on-target hardware execution, complete with post execution analysis and reviews
- integrate rules checking in consideration of MISRA, CERT and other coding standards
- automate test case, harness, and stub generation for robustness testing
- automate the bidirectional traceability to project functionality requirements referenced throughout the ECSS-E-ST-4oC and ECSS-Q-ST-8oC Rev1 standards
- support object code verification for software of criticality category A, as specified in ECSS-E-ST-4oC §5.8.3.5 e
- generate configurable software metrics in support of ECSS-Q-ST-8oC Rev.1 §7.1 Product quality assurance and metrication
- expose high-risk areas and defects by way of automated code analysis and report generation
- are underpinned by LDRA's ISO 9001:2015 certified Quality Management System, and the LDRA tool suite's TÜV SÜD and SGS-TÜV Saar certification
- provide an automated approach to testing re-used software on different target hardware in accordance with ECSS-Q-ST-8oC Rev.1 §7.3
- integrate seamlessly into any development process model including V-model, waterfall, and CI/CD

LDRA tool suite

The LDRA tool suite helps developers of space project related software products developed in accordance with ECSS standards ECSS-E-ST-4oC and ECSS-Q-ST-8oC Rev1 (Figure 2).

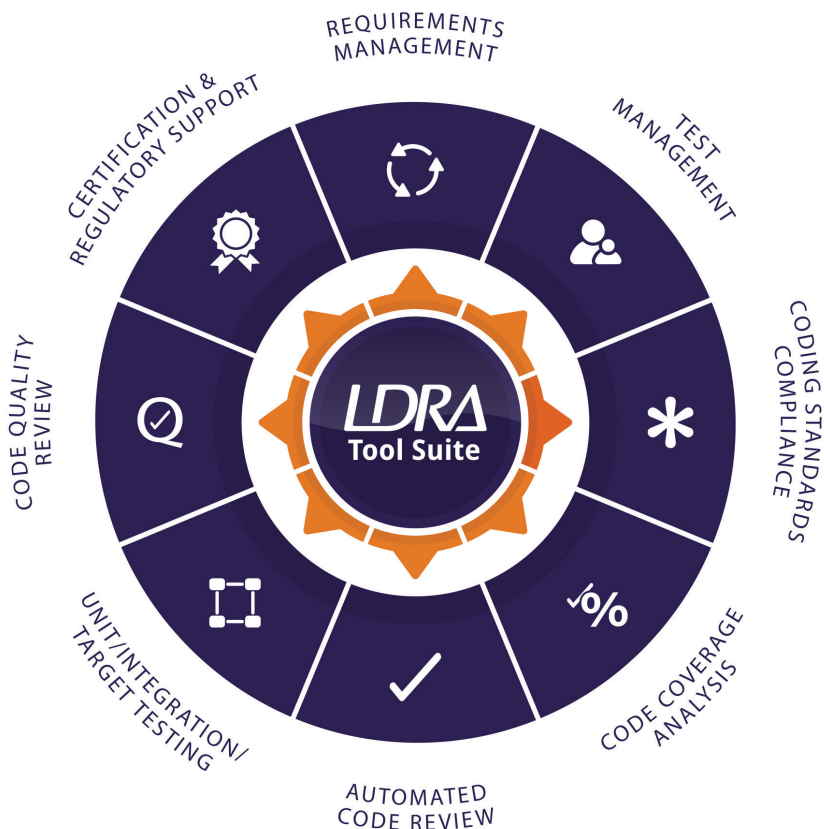


Figure 2: Key functionalities of the LDRA tool suite

Justification of tool use. (ECSS-Q-ST-8oC Rev.1 §5.6) The LDRA tool suite has been certified as “fulfilling the requirements of support tools” for many functional safety standards by two separate TÜV organizations. LDRA Tool Qualification Support Packs (TQSPs) are also available complete with test cases to demonstrate the capabilities of the tool suite.

Requirements and traceability. Bidirectional traceability is a recurring theme of the ECSS standards (ECSS-E-ST-4oC §5.2, §5.4.2, §5.6.4 etc.). The LDRA tool suite supports the automated bidirectional tracing of requirements, development, and verification artefacts and activities throughout the entire software development life cycle.

Static analysis and coding standards compliance. The LDRA tool suite’s static analysis capabilities help to quickly identify and eliminate latent defects in code and to enforce coding standards compliance in compliance with ECSS-Q-ST-8oC Rev.1 §6.3.4.1a. With today’s increasingly complex space applications and ever more demanding functional safety and security requirements, the ability to efficiently assess code quality is imperative. Examples of supported standards include MISRA C, MISRA C++, CERT C, CERT C++, BARR-C, and JSF++ AV (Figure 3).

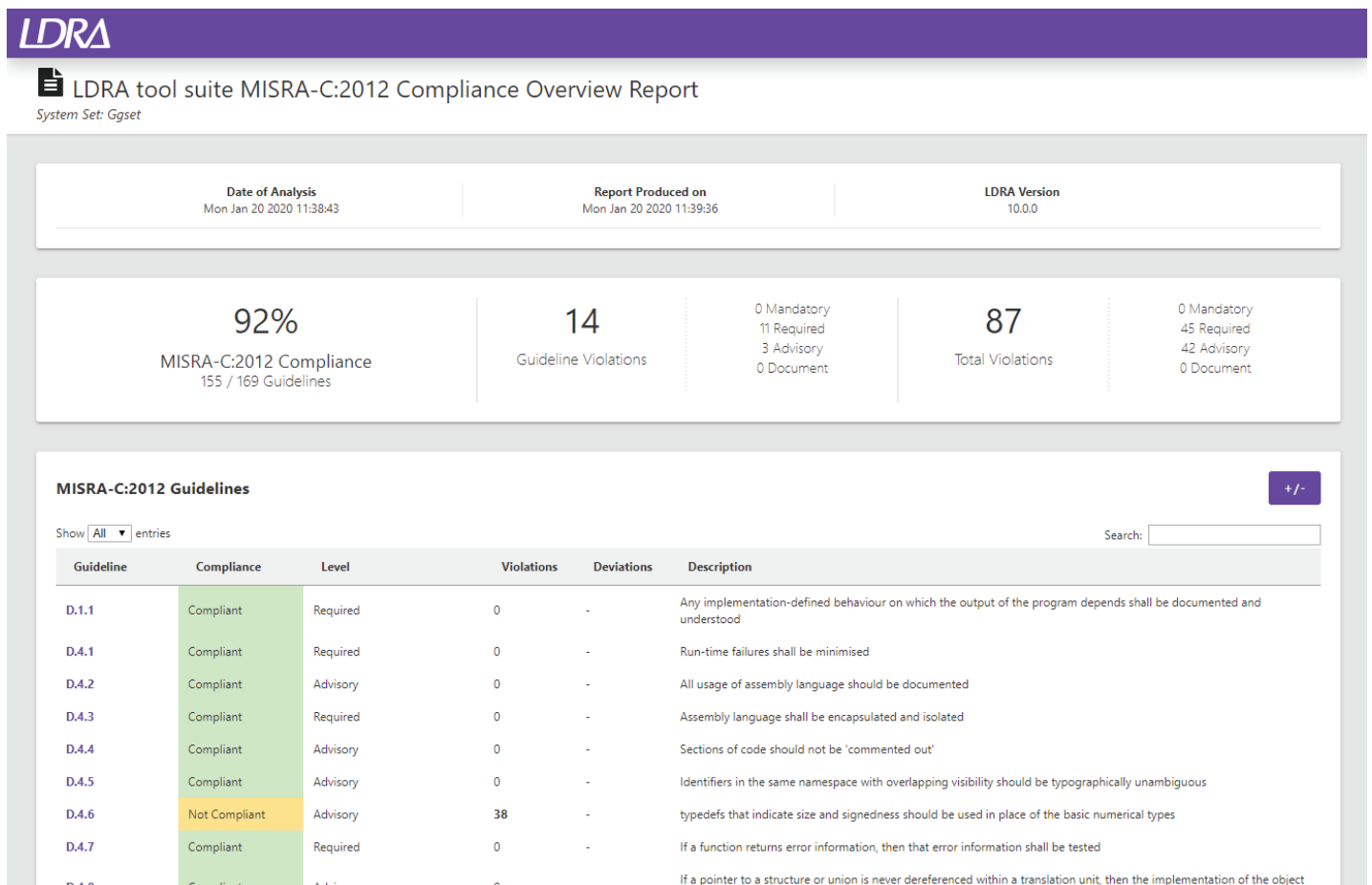


Figure 3: MISRA C compliance report from the LDRA tool suite

Unit testing. The LDRA tool suite provides rigorous unit testing early in the development lifecycle as advocated by ECSS-E-ST-40C §5.8.3.6, §5.3.3.2.a, and elsewhere. TBrun automates the generation and execution of requirements driven tests both on the host platform as well as the embedded target and produces the necessary verification evidence. TBrun also supports regression testing, saving time and money when requirements or code change during the software development life cycle.

Automated test case generation. The LDRA tool suite provides configurable automated test case generation to exercise the code beyond requirements-based testing. ECSS-E-ST-40C §5.8.3.5 advocates static analysis to prove the robustness of code, and adherence to coding standards helps to fulfil that aspiration. Dynamic robustness testing complements that functionality.

Source code coverage analysis. The LDRA tool suite meets the source code structural coverage analysis requirements detailed in ECSS-E-ST-40C §5.8.3.5 and ECSS-Q-ST-80C Rev 1 §6.3.5 including statement, branch/decision, and Modified Condition/Decision Coverage (MC/DC) coverage. Evidential artefacts are also automatically created.

Object code coverage analysis. The LDRA tool suite is uniquely equipped to meet the object code structural coverage analysis requirements detailed in ECSS-E-ST-40C §5.8.3.5 and ECSS-Q-ST-80C Rev 1 §6.3.5.

Summary

The ECSS standards look to apply best practice development practices with a functional safety focus. ECSS-E-ST-40C and ECSS-Q-ST-80C are complementary, viewing these best practices from different perspectives, which can lead to some confusing overlap between the two

The LDRA tool suite is proven to ease compliance with such standards, both in space and elsewhere. In particular, The TBmanager component of the tool suite helps by ensuring that requirements traceability information is never out of date.

LDRA's Object Code Verification has been shown to provide an efficient mechanism to demonstrate compliance for category A applications, especially with regards to similarly demanding DO 178 DAL A systems.



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