DO-178C compliance: turn an overhead expense into a competitive advantage

Contents

2 Executive summary

2 The cost of designing and building safety-critical systems

2 DO-178C characteristics

6 IBM® solutions to support DO-178C compliance

11 Why IBM?

Executive summary

DO-178C is the international and de facto standard for certifying all aviation safety-critical software. The need to comply with DO-178C can add significant cost to programs under development at a time when cost is becoming an increasingly critical factor in complex product development.

Companies designing and building safety-critical systems need robust methods and collaborative platforms. This white paper introduces best practices for software development and DO-178C compliance and looks at IBM® Rational® solutions and approaches that can help organizations deliver safety-critical products, improve collaboration, and increase efficiency and profitability.

The cost of designing and building safety-critical systems

In the aerospace and defense (A&D) industry, costs associated with product functionality are increasing over time[1]—putting significant pressure on A&D companies to do more with less or to sacrifice functionality to meet cost pressures. Software development and testing alone may be a significant factor in these rising costs, and the DO-178C standard and its related technology supplements have the potential to drive costs up even further.

- Level E - No safety impact, x1
- Level D - Minor impact, x3
- Level C - Major impact, x5
- Level B - Hazardous, x9
- Level A - Catastrophic, x10

Projects that need to comply with DO-178C standards could see cost increases anywhere from 25 percent to 40 percent compared to projects that don't require compliance.[2]
The sources of additional costs may include the following:

- Reduced developer productivity due to increases in process complexity
- Manual reporting and documentation processes that are not suited to the level of detail required to comply with DO-178C
- Qualification activities involved in compliance

In the current economic environment, it is important for companies to minimize the additional costs related to DO-178C development.

DO-178C characteristics

The purpose of DO-178C is to provide guidance for developing airborne software systems to ensure that it performs its intended function with a level of confidence commiserate with its airworthiness requirement. DO-178C is objective driven and companies may use a variety of means to achieve compliance as long as they meet the objective(s) in question. To comply with DO-178C, companies must provide multiple supporting documents and records surrounding their development processes.

Different airworthiness levels within DO-178C—A, B, C, D and E—directly correspond to the consequences of a potential software failure: catastrophic, hazardous/severe-major, major, minor or no effect, respectively. Each software level has a defined number of objectives that need to be satisfied (some with independence). Objectives requiring independence need documentary evidence that the person verifying the item is not be the person who developed the item.

These different software level certifications also determine the rigor required in testing and other aspects of development—the most challenging of which is software verification. DO-178C compliance involves six key processes: planning, development, verification, configuration management, quality assurance (QA) and certification liaison. Because the certification liaison process is not a development activity, this white paper only focuses on the first five areas.

One of the significant changes in DO-178C from DO-178B is that there are four additional supplements that may be used in conjunction with the DO-178C. These supplements cover model based development and verification supplement (DO-331.); Object-oriented technology and related techniques supplement (DO-332); formal methods supplement (DO-333) and software tool qualification considerations (DO-330). These supplements have been used to avoiding the need to update or expand the text inside the main DO-178 document. For example, the qualification criteria for software development and verification tools has been deleted in version C and has been replaced with a section that details the criteria for determining if tool qualification is needed. The objectives, activities, guidance, and life cycle data required for each Tool Qualification Level are described in DO-330, "Software Tool Qualification Considerations".

Planning

As with the other processes involved in proving compliance with DO-178C, planning requires associated output documentation, including the following:

- Plan for software aspects of certification (PSAC)
- Software development plan (SDP)
- Software verification plan (SVP)
- Software configuration management plan (SCMP)
- Software quality assurance plan (SQAP)
- System requirements
- Software requirements standard (SRS)
- Software design standard (SDS)
- Software code standard (SCS)

Level	Failure condition	Objectives	With independence
A	Catastrophic	71	33
B	Hazardous	69	21
C	Major	62	8
D	Minor	26	5
E	No Safety Effect	0	0

Table 1. Objectives for each software level

Development

Output documents associated with meeting DO-178C standards in the development process include software requirements data, software design descriptions, source code and executable object code.

According to DO-178C stipulations, without verifiable, unambiguous, consistent and well-defined requirements, you must create a problem report and submit the issue back to the input source to be clarified and corrected. You must also be able to trace those system requirements that will be realized by high-level software requirements to one or more low-level software requirements, and a low-level requirement to one or more high-level software requirements. Plus, you need to provide all of your derived requirements to the system safety assessment process. In a nutshell, this means that all of the source code you develop needs to be traceable, verifiable and consistent, and it needs to correctly fulfill the low-level software requirements.

DO-178C requires effective capabilities for measuring and reporting project status deliverables. Automated measurement and reporting tools can fulfill DO-178C requirements by enabling you to do the following:

- Gain access to data in multiple tools across the development workflow to avoid slow, costly and error-prone manual data collection
- Automatically generate reports and dashboards to help ensure that you generate consistent evidence of compliance and provide stakeholders with the correct information in a timely manner

Verification

To help ensure that your software fulfills DO-178C requirements, you must submit a verification report that shows the absence of errors—not just that you have tested for and detected errors. You need to prove that all lower-level artifacts satisfy higher-level artifacts, that you have accomplished traceability between requirements and test cases via requirements-based coverage analysis, and that you can show traceability between code structure and test cases through a structural coverage analysis. Each requirement in your software development process must be traceable not only to the code that implements it but also to the review, test or analysis through which it has been verified. You must also ensure that you can trace implemented functionality back to requirements and that testing can prove this—you need to eliminate any dead code or code that is not traceable to requirements.

Output documentation associated with DO-178C includes the following:

- Software verification cases and procedures (SVCP)
- Software verification results (SVR)
- Review of all requirements, design and code
- Testing of executable object code
- Code coverage analysis

As shown in figure 1, DO-178C defines specific verification objectives, including requirements-based testing, robustness testing and coverage testing, depending on the software level for which you are complying. At Level E, DO-178C requirements don’t apply. Level D requires 100 percent requirements coverage. Level C stipulates that companies meet Level D requirements plus 100 percent statement or line coverage. To gain Level B compliance status, companies must meet Level C requirements plus 100 percent decision coverage. Level A requires that companies meet all Level B requirements plus 100 percent modified condition decision coverage. Each type of coverage is defined in the standard—for example, statement coverage means that every statement in the program has been invoked at least once, while decision coverage means that every point of entry and exit in the program has been invoked at least once and every decision in the program has reached all possible outcomes at least once.

Level	Coverage	Coverage requirements
Level A	MCDC	Level B + 100 percent Modified Condition/Decision Coverage
Level B	DC	Level C + 100 percent Decision Coverage
Level C	SC	Level D + 100 percent Statement (or line) Coverage
Level D		100 percent Requirements Coverage
Level E		No coverage

Line, decision and condition coverage requirements are determined by the compliance level (A-E).

Coverage criteria	Statement Coverage	Decision Coverage	Condition Coverage	Condition/Decision Coverage	Modified Condition/ Decision Coverage	Multiple Condition/ Decision Coverage
Every point of entry and exit in the program has been invoked at least once.		●	●	●	●	●
Every statement in the program has been invoked at least once.	●					
Every decision in the program has reached all possible outcomes at least once.		●		●	●	●
Every condition in a decision in the program has reached all possible outcomes at least once.			●	●	●	●
Every condition in a decision has been shown to independently affect that decision's outcome.					●	●
Every combination of condition outcomes within a decision has been invoked at least once.						●

Figure 1. DO-178C stipulates coverage testing requirements by compliance level.

Configuration management

To support compliance with DO-178C elements surrounding configuration management, companies are required to do the following:

- Uniquely identify each configuration item
- Protect baselines of configuration items from change
- Trace a configuration item to the configuration item from which it was derived (lineage and history)
- Trace baselines to the baselines from which they were derived
- Reproduce builds (replicate executable object code)
- Provide evidence of change approvals
- Produce output documentation for a software configuration index (SCI) and a software life-cycle environment configuration index (SECI).

DO-178C also requires that companies implement a problem reporting system to document any change to the formal design baseline.

Quality assurance

The QA process in DO-178C requires reviews and audits to demonstrate compliance. Key output documents in this process include software quality assurance records (SQARs), a software conformity review (SCR) and a software accomplishment summary (SAS).

IBM solutions to support DO-178C compliance

Showing compliance to DO-178C can be a challenge in terms of the rigor, traceability and reporting required. An effective platform and process can reduce both the burden and the costs of compliance. IBM Rational solutions for systems and software development provide the cross-team and cross-life-cycle collaboration, automation and reporting capabilities to address the needs of DO-178C projects.

IBM Rational DOORS® family provides the de facto standard software solution for requirements management. In coordination with IBM Rational Team Concert™, IBM Rational Rhapsody® and IBM Rational Quality Manager software, Rational DOORS technology provides extensive traceability capabilities to help you meet DO-178C requirements. IBM Rational Publishing Engine software provide you with the potential to significantly reduce the time needed to produce requirements documentation, requirements traceability reports, design documentation and test reports.

- *Rational DOORS* is the leading requirements management application that can help you reduce costs, increase efficiency and improve quality by enabling you to optimize requirements communication, collaboration and verification throughout your organization and across your supply chain. Rational DOORS software integrates with Rational Quality Manager software to enable you to demonstrate requirements-based test coverage.
- *Rational DOORS Next Generation* is a web based collaborative Requirements Management application that allows teams to be able to work more effectively across disciplines, time zones and supply chains.
- *Rational Publishing Engine* software is an automated document generation solution with the capability to connect a variety of data sources, including Rational solutions and select third-party tools. Using Rational Publishing Engine software to automate document generation for ad hoc use, formal reviews, contractual obligations and regulatory compliance can help you improve productivity and reduce risk and cost.

IBM Rational Rhapsody family is a collaborative design, development and test environment for systems engineers and software engineers. It provides:

- Rapid prototyping and execution to address errors earlier when they are least costly to fix.
- Automatic consistency checking to enhance agility and improve reuse with collaboration to reduce both recurring and non-recurring costs.
- The ability to share, collaborate, and review your engineering lifecycle artifacts created with Rational Rhapsody or other design tools, such as Mathworks Simulink, with the extended engineering team.

Rational Quality Manager software is a collaborative and customizable solution for test planning, execution management, workflow control, tracking and metrics reporting that provides a central hub through which to manage the verification process. By providing open interfaces, Rational Quality Manager software allows you to connect IBM and third-party testing solutions to manage testing, results and defects.

In addition, *IBM Rational Test RealTime* software is a cross-platform solution for software component testing, run-time profiling and coverage analysis that can help code writers debug and correct errors before they get into production code. Rational Test RealTime software integrates with Rational Quality Manager software to help you effectively manage test coverage related to the DO-178C verification process.

IBM Rational solutions for the planning process

Repeatable processes can significantly reduce the overall time and cost of software development. To address DO-178C requirements and effectively produce planning deliverables, companies need a defined systems and software engineering process that can delineate workflows, inputs, outputs, roles and responsibilities. The IBM Rational Solution for Aerospace and Defense - DO-178C is a set of best practices to help organizations develop products for and is a plug into IBM Rational Method Composer. These best practices scan help accelerate the adoption of common process support, practices and tools so as to reduce the time to value for the client's process improvement initiatives. Each practice is mapped the objects in DO-178C, or its associated supplements, that it helps support compliance to.

These practices can be exported as templates for IBM Rational Team Concert, providing a consistent, executable work flow to help ensure your documented processes are followed and provides a basis for creating automated reports to help with compliance. A variety of templates are included to help reduce the time required to produce the various plans, reports or artifacts required by DO-178C.

IBM Rational solutions for the development process

Effective requirements management—and especially traceability from requirements to related development artifacts—is a key component of DO-178C. The IBM Rational solutions support a traditional development lifecycle as well as model based development according to DO-331. Model based development can translate to reduced development time and the earlier identification of design inconsistencies by using the model-driven development capabilities within Rational Rhapsody family of software.

The IBM Rational Rhapsody Kit for DO-178B/C describes a comprehensive workflow for model based development how each step helps meet the relevant development and tool qualification objectives in DO-178C, and DO-331. This kit contains the following artifacts:

- IBM Rational Rhapsody Kit for DO-178B/C Overview
- IBM Rational Rhapsody Reference Workflow Guide
- IBM Rational Rhapsody TestConductor Add On Reference Workflow Guide
- IBM Rational Rhapsody TestConductor Add On Safety Manual
- IBM Rational Rhapsody TestConductor Add On Qualification Kit for DO-178B/C Over-view
- IBM Rational Rhapsody TestConductor Add On Validation Suite
- IBM Rational PSAC template for SMXF (Plan for Software Aspects of Certification)
- IBM Rational Rhapsody SXF/SMXF Frameworks (C++/C)
- IBM Rational Rhapsody SXF/SMXF Validation Suites

The formality of modeling in the Unified Modeling Language (UML) or the Systems Modeling Language (SysML) in Rational Rhapsody software can help improve quality by providing automatic verification through syntactic and semantic model checking. With Rational Rhapsody software you can execute models to provide early validation of designs and test your software throughout the development life cycle.

With a model-based design process that is linked to requirements management through Rational Rhapsody and Rational DOORS software, you can automatically generate critical deliverables including the following:

- System specifications
- Application and device code
- Requirements traceability reports
- Specification, design and test documentation
- Test suites, test cases and scenarios

Effective modeling can enhance communication among teams to reduce errors and boost product safety and can help companies save money and time associated with maintenance and upgrades.

Leveraging Rational Rhapsody software and UML can help you support safety-critical development and provide stakeholders with key views and deliverables, such as a fault-tree analysis, a hazard analysis and constraint tables. The integration between Rational Rhapsody and Rational DOORS software allows you to link UML models to textual requirements to provide key capabilities such as completeness checks (Are all requirements implemented?), gold plating checks (Does the design contain unnecessary or redundant elements?), and perform a fast and comprehensive impact analysis of changes prior to software and hardware implementation. Rational Team Concert software, which is designed to integrate with Rational Rhapsody and Rational DOORS software through the IBM Rational Jazz™ platform, provides effective change tracking capabilities to help ensure that approved changes are correctly implemented.

Model-based design also facilitates reuse of key components by allowing you to develop rich libraries of formally specified design elements to help you dramatically reduce your design, validation and verification burden as well as DO-178C overhead for future projects. Through effective asset management, you can successfully perform cataloging, asset reviews, an impact assessment of asset changes, and auditing and reporting activities to measure asset value.

- The IBM Rational solution is also integrated with Mathworks Simulink models and can provide file or model level configuration management, model level traceability to other lifecycle artifacts, and co-model execution of SysML, UML and Simulink models.

IBM Rational solutions for the verification process

Testing and validation often are the most expensive areas of the development process. In these phases, it is critical for companies to use effective tooling and best practices to automate as much of the process as possible. Rational testing and quality management solutions can help you meet DO-178C verification requirements by extensively automating the testing and validation process. Requirements in Rational DOORS can be traced to test plans, test cases and test steps in Rational Quality Manager.

Test plans drive activity for distributed teams through all phases of the project lifecycle. The test plan defines the objectives and scope for the test effort and contains criteria to help teams determine the answer to this question: "Are we ready to release?"

- Rational Quality Manager provides robust manual test planning and connected or stand-alone (such as on field tests) test execution and documentation. Rational Quality Manager's integrated test execution environment supports running tests developed within the product as well as running tests created in other manual, functional, performance, and security testing tools. Options for test execution include running a test case directly, grouping test cases into test suites for parallel or sequential execution, or creating test case and test-suite execution records to map test environment information directly to the test cases and test suites.
- Predefined reports to help you get status on your project. You can trace the relationship between test artifacts, requirements, and development artifacts by browsing a list of certain test artifacts and opening the traceability view.

With the lab management capabilities that Rational Quality Manager provides, you can create requests for the test environments that you specify in your test plan. You can then work with the lab manager to ensure that lab resources and test environments are available when needed. Lab managers can track all lab resources from a centralized resource repository and service requests from the test team.

Rational Quality Manager helps ensure that your business processes comply with industry, corporate, and departmental standards and regulations. Throughout the testing lifecycle, Rational Quality Manager provides the tools to obtain an up-to-the-minute measurement of software quality and project metrics. With its comprehensive test plan and integration with requirements management and defect tracking tools, Rational Quality Manager helps streamline your test strategy and produce reliable records of test results and project history that can be used for auditing purposes.

IBM Rational Test RealTime software for software component testing, run-time profiling and code structural coverage analysis, up to MC/DC required for Level A, integrates with Rational Quality Manager software to help you effectively manage test coverage related to the DO-178B verification process. For model based development, IBM Rhapsody TestConductor provides model level coverage results to help satisfy model coverage objectives. Tool qualification kits are available for both Test RealTime and Rhapsody TestConductor.

IBM Rational solutions for the configuration management process

DO-178C processes for configuration management require both configuration management and change control of development artifacts. If not done effectively, configuration management and change control activities can considerably increase your development costs.

IBM Rational technology has long been a leader in these areas with software offerings including Rational Team Concert, IBM Rational ClearCase®, IBM Rational ClearQuest®, IBM Rational Synergy and IBM Rational Change software.

Leveraging these tools can help you effectively formalize and automate workflows and the associated capture of key information, which can help reduce development costs.

Rational Team Concert brings together distributed teams on a unified change, configuration and release management platform. By coordinating software development around a single or multiple configuration management repositories, you can take advantage of the benefits of application life-cycle management on a global scale.

Rational change and configuration management capabilities can also boost your organization's efforts to develop, publish, reuse and distribute software components to support complex systems development projects. Rational Team Concert software connects dispersed teams to increase individual and team productivity, compress development cycles and rapidly deliver high-quality software that supports DO-178C compliance.

IBM Rational solutions for the QA process

The QA process associated with DO-178C compliance is designed to show that you have implemented and carried out the processes documented in the planning stage. As noted above, the following deliverables are required as part of the quality assurance process—SQAR, SCR and SAS.

Reporting capabilities of the IBM Rational solution utilize the data accumulated across the development processes and can be used to demonstrate compliance through automated reporting.

Why IBM?

By adopting best-practice processes designed around a development life-cycle tool platform, you can offset compliance overhead costs by improving efficiency and lower rework costs by reducing late-discovered errors and defects. Specifically, you can make improvements through the following:

- Automation to offset increased process complexity
- Reporting automation to efficiently support the level of detail required to comply with DO-178C
- Automation of the qualification activities involved in compliance

The IBM Rational software platform for systems and software engineering is designed to help engineering teams find new, collaborative ways to develop and deliver the right demands on time, on budget, with the right quality and in compliance with DO-178C requirements—across the systems delivery life cycle. IBM Rational solutions for safety-critical software development are extensible, through both IBM and third-party offerings, to help you in other areas such as architecture management and specialized testing and analysis capabilities. Offerings from IBM provide a measured, incremental implementation approach to help you build confidence, minimize risk and demonstrate return on investment.

By deploying IBM Rational solutions, you can reuse software assets and skills to improve development productivity and accelerate time to market and innovation. Comprehensive traceability functionality allows you to enhance collaboration and communication and enables teams from multiple disciplines to coordinate system and software architecture activities. Standards-based development capabilities provide an open and extensible technology platform as well as support for industry standards throughout the development life cycle—from requirements to implementation. Leveraging IBM Rational solutions, you can enable global development and delivery by supporting communication among original equipment manufacturers, suppliers, agencies and contractors.

IBM is a top-performing technology company with more than 100 years of experience. Our solutions offer a proven track record, providing you with the confidence that you can tap into our expertise throughout the life cycle of your solutions. Offering extensive service and research capabilities, IBM can help you reduce costs and align your capabilities with our innovations and expertise. A leader in the software development marketplace, IBM Rational software offers systems development solutions that can help you automate your development and documentation processes to realize efficiencies and reduce costs.

For more information

To learn more about how IBM Rational solutions for safety-critical software projects and DO-178C compliance can improve your development practices, please contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com**/software/rational/solutions/aerospace/

Additional Information:

- Charlotte Adams (2010-10-21). "Safety-critical software for mission-critical applications to get boost with release of DO-178C". *Military & Aerospace Electronics*. Retrieved 2014-02-04.
- Charlotte Adams (2010-09-01). "DO-178C Core changes". *Avionics Intelligence*. Retrieved 2010-10-23.
- Bill StClair and Nat Hillary (2010). "DO-178C: Improved certification for cost-effective avionics systems". *VME and Critical Systems*. Retrieved 2010-10-23.
- Frederic Pothon (2012). "DO-178C/ED-12C vs DO-178B/ED-12B: Changes and Improvements". *Open DO*. Retrieved 2010-10-23.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2014

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

[1] RAND Corporation, *Why Has the Cost of Fixed-Wing Aircraft Risen?: A Macroscopic Examination of the Trends in U.S. Military Aircraft Costs over the Past Several Decades*, Mark V. Arena and others, 2008. © The RAND Corporation. Reprinted with permission.

[2] Citation: " www.do178site.com/do178b_questions.php"

Please Recycle