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

2 Executive summary
2 The cost of designing and building safety-critical systems
3 DO-178B characteristics
6 IBM solutions to support DO-178B compliance
10 Why IBM?

Executive summary
DO-178B is the international and de facto standard for certifying all aviation safety-critical software. The need to comply with DO-178B 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-178B 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—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 DO-178B standards have the potential to drive costs up even further.

<table>
<thead>
<tr>
<th>Dollars and sense</th>
<th>Initial cost increase as a result of DO-178B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical DO-178B project</td>
<td>• Added 60–100 percent cost</td>
</tr>
<tr>
<td>Successful DO-178B project</td>
<td>• Added 25–40 percent cost for initial development</td>
</tr>
<tr>
<td>Avionics project without DO-178B</td>
<td>• Solid process  • Experienced team</td>
</tr>
</tbody>
</table>

Figure 1: To facilitate compliance with DO-178B requirements, companies will have to budget for project cost increases.
According to a recent study by HighRely, projects that need to comply with DO-178B standards could see cost increases anywhere from 25 percent to 100 percent. 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-178B
- Qualification activities involved in compliance

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

**DO-178B characteristics**

The purpose of DO-178B is to provide guidance to companies developing software-intensive systems to ensure that projects conform to specified requirements. While DO-178B imposes strict requirements, it is also objectives driven—companies may use alternate means of compliance as long as they meet the objective in question. To comply with DO-178B, companies must provide multiple supporting documents and records surrounding their development processes.

Different software levels within DO-178B—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. 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-178B 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.

The use of tools within a DO-178B development process may also be subject to qualification standards, including the following:

- Tools that can introduce errors in the code must be qualified as development tools—a stringent process with the same constraints as those associated with embedded code.
- Tools that can miss errors in the code must be qualified as verification tools—a less onerous process.
- Other tools that may significantly improve automation and efficiency—but which do not directly affect delivered code—are not subject to qualification proof.

Companies face hurdles in obtaining software tool qualification and approval, which is done on a case-by-case basis and which requires supporting data from the tool vendor.
**Planning**
As with the other processes involved in proving compliance with DO-178B, 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)

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

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

- Gain access to 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-178B 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-178B 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 2, DO-178B 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-178B 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. During this verification activity, you need to qualify the verification tooling that can miss errors (for example, test coverage or static analysis).

<table>
<thead>
<tr>
<th>Level</th>
<th>Coverage</th>
<th>Coverage requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level A</td>
<td>MCDC</td>
<td>Level B + 100 percent Modified Condition/Decision Coverage</td>
</tr>
<tr>
<td>Level B</td>
<td>DC</td>
<td>Level C + 100 percent Decision Coverage</td>
</tr>
<tr>
<td>Level C</td>
<td>SC</td>
<td>Level D + 100 percent Statement (or line) Coverage</td>
</tr>
<tr>
<td>Level D</td>
<td>100 percent Requirements Coverage</td>
<td></td>
</tr>
<tr>
<td>Level E</td>
<td>No coverage</td>
<td></td>
</tr>
</tbody>
</table>

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

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

Figure 2: DO-178B stipulates coverage testing requirements by compliance level.
Configuration management
To support compliance with DO-178B 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-178B 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-178B 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-178B compliance
Addressing DO-178B standards can be a challenge in terms of the rigor, traceability and reporting required. An effective platform and process can potentially 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-178B projects.

IBM Rational solutions for the planning process
Repeatable processes can significantly reduce the overall time and cost of software development. To address DO-178B 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 Unified Process methodology—an iterative software development process framework—and IBM Rational Harmony and IBM Rational Method Composer software can help companies quickly and effectively implement or refine repeatable processes and best practices.

Especially in the planning stage, templates are extremely helpful in reducing the time required to produce the various plans stipulated by DO-178B. The Rational Unified Process framework,
the Rational Harmony process framework and Rational Method Composer software provide templates that companies can use to create the following:

- Software development plan
- Software verification plan
- Software configuration management plan
- Software quality assurance plan

Using Rational Method Composer software, companies can create and store templates for the software design standard (SDS) and software code standard (SCS).

A recent study shows that requirements can be a major cause of program problems in aerospace and defense. Effective requirements management—and especially traceability from requirements to related development artifacts—is a key component of DO-178B. Rational solutions offer extensive help with system requirements and the software requirements standard (SRS).

IBM Rational DOORS® software provides the de facto standard 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-178B requirements. IBM Rational Insight and 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.

**IBM Rational solutions for the development process**

Reducing the cost of development, especially in the context of DO-178B, can translate to reduced development time, which companies can achieve by using the model-driven development capabilities within Rational Rhapsody software.

With a well-defined modeling process, you can find and fix errors earlier in the development life cycle to significantly reduce costs. 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. Using 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 requirements to provide key capabilities, including completeness checks (Are all requirements implemented?) and 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. IBM Rational Asset Manager software can then leverage these elements across multiple projects and configurations to help you dramatically reduce your design, validation and verification burden as well as DO-178B 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.

**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-178B verification requirements by extensively automating the testing and validation process.

- **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.

- **Rational DOORS software** is a 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.
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-178B verification process.

IBM Rational Logiscope® software is a software quality assurance tool. It automates code reviews, provides identification and detection of error-prone modules for software testing, and performs codebase refactoring to help eliminate duplicate code.

IBM Rational solutions for the configuration management process
DO-178B 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. With Rational Team Concert software, you can bring together distributed teams on a unified change, configuration and release management platform. By coordinating software development around a single configuration management repository, 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. Based on Jazz technology, Rational Team Concert software can help you connect dispersed teams to increase individual and team productivity, compress development cycles and rapidly deliver high-quality software that supports DO-178B compliance.

IBM Rational Build Forge® software is an adaptive process execution framework that automates, orchestrates, manages and tracks the processes between handoffs within the assembly line of software development to create an automated software factory that helps reduce costs.

IBM Rational solutions for the QA process
The QA process associated with DO-178B 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.
In conjunction with Rational Insight and Rational Publishing Engine software, Rational Quality Manager software helps you more easily prepare reports from the data accumulated across the development processes and demonstrate compliance through automated reporting. Rational Quality Manager software provides a role-based, customizable solution for test planning, execution management, test status and defect management, workflow control, and reporting for reviews and audits.

A performance measurement and management solution, Rational Insight software provides objective dashboards and measures for transparency and control of risks, status and trends. It delivers measurement best practices, helps improve efficiency and quality, and helps you take greater control of software and systems development and delivery.

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.

Why IBM?
DO-178B is a requirement in safety-critical airborne systems development, yet organizations typically see compliance with its standards as a significant overhead cost. 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-178B
- Automation of the qualification activities involved in compliance

The IBM Rational software platform for systems 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-178B 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-178B compliance can improve your development practices, please contact your IBM sales representative or IBM Business Partner, or visit: ibm.com/software/rational/solutions/aerospace/

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: ibm.com/financing

2 Data compiled from June 2010 survey by HighRely via the DO-178 Industry Group members at [www.do178site.com](http://www.do178site.com)