A Primer on Software Safety Certification

by
Chip Downing

Introduction. As embedded software pervades all aspects of our lives, it is also being deployed into more safety-critical environments. Due to the potential loss of life due to software failure in these systems, safety agencies, responsible for controlling products in these environments, are developing robust methodologies for qualifying software. This document is a brief introduction on this subject.

SAFETY AGENCIES

Many agencies have developed software standards for safety-critical products. The following is a partial list of these agencies

RTCA. RTCA, in the avionics sense (to which all references in this document refer) is the acronym for Radio Technical Commission for Aeronautics. Though not a government agency, many RTCA guidelines are accepted essentially as standards by the FAA, JAA, and other safety certification organizations (which are also defined in this document).

RTCA, Inc. is located at 1828 L Street, NW, Suite 805, Washington, D.C. 20036 USA. Contacts are: phone 202-833-9339, fax 202-833-9434, email info@rtca.org, and web www.rtca.org/.

(Note: RTCA is also the acronym for Radon Testing Corporation of America. Its web site is http://www.rtca.com. This is also a safety agency, but one not involved in developing software certification standards.)

EUROCAE. EUROCAE is the acronym for the European Organisation for Civil Aviation Equipment. It is the European equivalent of RTCA.

EUROCAE is located at 17 rue Hamelin, 75116 Paris FRANCE. Contacts are: phone +33 (0) 1 4505 7188, fax +33 (0) 1 4505 7230, and web www.eurocae.org.

FAA. FAA is the acronym of the U.S. Federal Aviation Administration, the organization responsible for controlling air traffic safety in the United States. The FAA is located at Federal Aviation Administration, 800 Independence Avenue, S.W., Room 810, Washington, DC 20591 USA.

JAA. JAA is the acronym for the Joint Aviation Authorities in Europe. The JAA is an associated body of the European Civil Aviation Conference (ECAC), representing the civil aviation regulatory authorities of a number of European states that have agreed to cooperate in developing and implementing common safety regulatory standards and procedures. The JAA and the FAA work together to create complementary air traffic safety standards.

The JAA is located at Saturnusstraat 8-10, PO Box 3000, 2130 KA Hoofddorp, The Netherlands. Contact JAA via fax, +31 (0) 23-5621714, or the web, www.jaa.nl/.

IEC. IEC is the acronym for the International Electrotechnical Commission, the international standards and conformity assessment body for electrotechnology; specifically, functional safety of electrical/electronic/programmable electronic (E/E/PE) systems.

The IEC is located in Geneva, Switzerland. Its web site is www.iec.ch.

CENELEC. CENELEC is the European Committee for Electrotechnical Standardization. Most CENELEC standards are identical or very closely based on IEC international standards. Typically, IEC standards in the 60000 to 69999 range map directly to CENELEC standards, for example, IEC 61508 to EN 61508.

CENELEC's web site is: www.cenelec.org

FDA. FDA is the acronym for the U.S. Food and Drug Administration. FDA's mission is to promote and protect the public health by helping safe and effective products reach the market in a timely way, and monitoring products for continued safety after they are in use. Its goal is to protect consumers.

The FDA is located at U.S. Food and Drug Administration, 5600 Fishers Lane, Rockville MD 20857-0001 USA. Contact the agency by phone, at 888-INFO-FDA (1-888-463-6332) and on the web, at www.fda.gov

CDRH. CDRH is the acronym for the Center for Devices and Radiological Health. It is a sub-organization of the U.S. FDA, with the responsibility for controlling the safety all medical devices sold in the United States.

The CDRH web site is: www.fda.gov/cdrh/

SAFETY CERTIFICATION STANDARDS

In a perfect world, the agencies responsible for protecting human life would have organized a meeting and developed a scalable software safety standard that would fit all industries. But in our still-imperfect world, multiple agencies create multiple standards for different software environments. The most stringent of these standards is RTCA DO-178B and IEC 16508. This paper focuses on RTCA/DO-178B, but also briefly covers other standards.

DO-178B. RTCA Document RTCA/DO-178B, titled "Software Considerations in Airborne Systems and Equipment Certification," was developed by the avionics industry to establish software considerations for developers, installers, and users, when aircraft equipment design is implemented using microcomputer techniques. This document outlines verification, validation, documentation, and software configuration management and quality assurance disciplines to be used in microcomputer systems.

In particular, this document gives guidance for the qualification of software tools, reuse of previously developed software, user-modifiable software, onboard data loading, formal methods, multiple-version dissimilar software, and product service history. DO178B is an update of DO-178A, published in 1985, to take into account the significant advancements in the application of digital processing achieved in the intervening period.

The FAA Advisory Circular AC20-115B recognizes DO-178B as the accepted means of certifying all new aviation software. DO-178B is recognized similarly by EUROCAE in Europe as well, where it is known as ED-12B. (Refer to av-info.faa.gov for the text of AC20-115B and many other related items.) (Yes, occasionally agencies do work with each other.) ED-12B is an update of ED-12A, published in 1985. Any company or individual desiring to develop avionics software will need to purchase a copy of DO-178B. Copies of this document can be purchased from the RTCA or EUROCAE.

Note that DO-178B/ED-12B projects must be certified as a system, not a standalone component, as for IEC 61508 software components. The FAA is making great progress in this area with the publication of notice 8110.97, which defines guidelines to Designated Engineering Representatives (DERs) for approving software that is reused from previous DO-178B projects. This can enable well-managed projects to reuse software binaries under controlled circumstances, similar to IEC 61508.

DO-178B and ED-12B were developed by a broad committee of industry representatives from around the world. The official working groups were RTCA SC-167 and EUROCAE WG-12, and comprised representatives of the FAA, CAA, Boeing, Aerospatiale, Bendix/King, Veridatas, NASA, British Aerospace, Smiths Industries, Litton Aero, Rockwell Collins, Honeywell, Deutsche Airbus, ARINC, SNECMA, GE Aircraft Engines, Pratt & Whitney, Rolls-Royce, and many others.

DO-178B/ED-12B provides guidance on designing, specifying, developing, testing, and deploying software in safety-critical avionics systems. It covers software life cycles, software planning processes, software development processes, software verification processes, software configuration management processes, software quality assurance processes, and other aspects of creating quality software for a safety-critical environment.

In sum, DO-178B is a guideline for determining, in a consistent manner and with an acceptable level of confidence, that the software aspects of airborne systems and equipment comply with FAA airworthiness requirements.

DO-178B Details. Basically, DO-178B specifies that every line of code be directly traceable to a requirement and a test routine, and that no extraneous code outside of this process be included in the build. During an FAA (or other agency) review, the examiner will perform traces from design to code to test on the documentation package, along with other due diligence, such as reviewing software development artifacts and qualifying tools.

To accommodate different criticality environments, DO-178B created five software levels (A, B, C, D, E) which are based on the potential of the software to cause safety-related failures identified in the system safety assessment. The software level is therefore directly related to the level of effort required to satisfy DO-178B certification requirements; thus, for Level A, the most critical level, certification requires the most rigorous effort to prove software reliability.

DO-178B has five levels of certification:

Level	Safety Impact
Level A	Software whose failure would cause or contribute to a catastrophic failure of the aircraft.
Level B	Software whose failure would cause or contribute to a hazardous/severe failure condition.
Level C	Software whose failure would cause or contribute to a major failure condition.
Level D	Software whose failure would cause or contribute to a minor failure condition.
Level E	Software whose failure would have no effect on the aircraft or on pilot workload.

The level to which a particular system must be certified is selected by a process of failure analysis and input from the device manufacturers and the certifying authority (FAA or JAA), with the final decision made by the certifying authority.

Note that different software components do not need to be certified specifically at each designated level. Certification at any level automatically covers the lower-level requirement; but, obviously, the converse is not true. Software certified at Level A can be used in any avionics application.

The following table lists the documents and records you may need to provide for a DO-178B certification:

Software Life Cycle Data DO-178B Deliverables List			
Acronym	Document Title	Type	Section
PSAC	Plan for Software Aspects of Certification	Document	11.1
SDP	Software Development Plan	Document	11.2
SVP	Software Verification Plan	Document	11.3
SCMP	Software Configuration Management Plan	Document	11.4
SQAP	Software Quality Assurance Plan	Document	11.5
SRS	Software Requirements Standards	Document	11.6
SDS	Software Design Standards	Document	11.7
SCS	Software Code Standards	Document	11.8
SRD	Software Requirements Data	Document	11.9
SDD	Software Design Description	Document	11.10
	Source Code	Software	11.11
	Executable Object Code	Software	11.12
SVCP	Software Verification Cases and Procedures	Document	11.13
SVR	Software Verification Results	Records	11.14
SECI	Software Life Cycle Environment Configuration Index	Document	11.15
SCI	Software Configuration Index	Document	11.16
PRs	Problem Reports	Records	11.17
	Software Configuration Management Records	Records	11.18
	Software Quality Assurance Records	Records	11.19
SAS	Software Accomplishment Summary	Document	11.20

To control the application and management of DO-178, the FAA created DERs, Designated Engineering Representatives, experienced engineers from the avionics industry designated by the FAA to approve engineering data used for certification. Most customers (and the FAA) will want some assurance in the quality and completeness of your DO-178B documents, and an FAA DER provides this. All FAA projects must have an FAA representative assigned, as well as a DER to review all submissions. A DER has full authority to sign off on your project as a representative of the FAA. DERs are not, however, qualified to certify all aspects of avionics/aircraft; a *software* DER will be required to approve your software activities.

The services of a DER are usually obtained to perform an examination of your documentation before submittal to the certifying agency. For FAA submissions, the signoff document is FAA form 8110. Once the DER has signed off, the product is, essentially, "FAA certified" for the holder of that 8110 form. But note, if the software is updated, another certification examination is required.

Because a DER will eventually examine your documentation, it is a good idea to get a DER involved at an early stage in your development for two primary reasons. First, a DER may insist on witnessing such items as portions of your software testing; second, a DER may not like your documentation (or processes), hence may insist on changes to them before signoff. These changes are a lot easier to do during design and development than at project completion. If you are "retro-certing" existing software that was not developed under any formal guidelines, a DER should be consulted before any resources are expended on the certification effort.

Independent contractor software DERs are available. A partial list of these contractors is located at: www.ValidatedSoftware.com/faa_ders.htm.

Under the GATM (Global Aviation Traffic Management) agreement, all commercial airborne systems have to comply with Federal Aviation Administration (FAA) regulations for avionics and require DO-178B certification. In addition, all airborne military and space systems must also comply with DO-178B. All retrofits, as well as new airborne system designs, also require DO-178B certification. Note that GATM has international validity and applicability.

DO-178B Software Verification. Three primary levels of structural testing concern most DO-178B projects:

SC: Statement Coverage. Means that every statement in the program has been invoked or used at least once. This is the most common use of the term "code coverage."

DC: Decision Coverage. Means that every point of entry and exit in the program has been invoked at least once and that each decision in the program has been taken on all possible (Boolean) outcomes at least once. Essentially, this means that every Boolean statement has been evaluated both TRUE and FALSE.

MCDC: Modified Condition Decision Coverage. Means that every point of entry and exit in the program has been invoked at least once, that every decision in the program has taken all possible outcomes at least once, and that each condition in a decision has been shown to independently affect that decision's outcome. Complex Booleans need to have truth tables developed to set each variable (inside a Boolean expression) to both TRUE and FALSE.

This table details the code coverage requirements for each DO-178B level:

Level	Coverage	Coverage Requirements
Level A	MCDC	Level B + 100% Modified Condition Decision Coverage
Level B	DC	Level C + 100% Decision Coverage
Level C	SC	Level D + 100% Statement (or Line) Coverage
Level D		100% Requirements Coverage Requirements
Level E		No Coverage Requirements

Performing this code coverage exercise is possible using manual methods, but this process is now readily facilitated by implementing commercial code coverage tools. Numerous code coverage tool vendors now supply testing tools that create the appropriate test outputs to demonstrate and satisfy compliance with DO-178B.

DO-178B/ED-12B defines specific verification objectives that must be satisfied; these include:

1. Verification of software development processes
2. Review of software development life cycle artifacts
3. Functional Verification of software
    a. Requirements-based testing and analysis
    b. Robustness testing
4. Structural Coverage Analysis

Structural Coverage Analysis is generally perceived to be the most difficult task to undertake by people unfamiliar with rigorous code development and testing. Furthermore, certifying an operating system that is tightly integrated with the hardware, cache, interrupts, memory management, and process/task management, can make structural testing even more difficult. These low-level aspects create a significant challenge to the verification process.

For example, Level A certified applications must address:

1. Statement Coverage
2. Decision Coverage
3. Modified Condition/Decision Coverage (MCDC)
4. Identification of dead or deactivated code
5. Traceability from source to object code

Fortunately, a variety of commercial tools are available to assist in this challenging task. See www.ValidatedSoftware.com/CodeCoverageTools.htm for a list of known vendors in this space.

DO-248B. RTCA DO-248B is a clarification document to DO-178B. Major topics include Previously Developed Software (PDS), Commercial Off-the-Shelf (COTS) software, verification, service history, tools and control categories. RTCA DO-248B is available from RTCA.

8110.97. 8110.97 is a notice published by the FAA that defines guidelines to DERs for approving software reused from previous DO-178B projects. All software life-cycle data used in DO-178B-certified systems require design approval under Title14, Code of Federal Regulations (14 CFR). 8110.97 RSC (Reusable Software Components) provides formal guidelines for reusing data, if properly planned and packaged, with minimal rework from project to project.

***IEC 61508*.** IEC 61508 was developed to create a standard for the functional safety of electrical/electronic/programmable electronic safety-related systems. It was compiled by SC65A/WG14, an international committee responsible for producing guidelines on IEC 61508. International Standards IEC 61508, like DO-178B/ED-12B, has safety levels, or specifically, Safety Integrity Levels (SILs), from 1 to 4 (4 is the highest). IEC 61508 is often closely associated with other standards, such as IEC 60601-1-4 and German safety standards DIN 19250 and DIN 0801. Most IEC safety certifications are administered by TÜV Product Service.

IEC 61508 allows for the standalone certification of a software component, unlike DO-178B/ED-12B. The documentation requirements of IEC 61508 are similar to DO-178B/ED-12B, but tend to lean more heavily on design, usage, and manufacturing, due to the standalone component aspects of this certification. One of the most critical documents is the Safety Manual, which contains the rules and guidelines on how to use the software component in a system that is certified.

The IEC has a great FAQ at: http://www.iec.ch/61508/Index.htm

IEC 61508 Details. The IEC standard is published in seven parts, as shown in the table below.

IEC 61508 Part References

Reference	Full Part Title
IEC 61508-1	IEC 61508-1:1998, Functional safety of E/E/PE safety-related systems – Part 1: General requirements
IEC 61508-2	IEC 61508-2:2000, Functional safety of E/E/PE safety-related systems – Part 2: Requirements for E/E/PE safety-related systems
IEC 61508-3	IEC 61508-3:1998, Functional safety of E/E/PE safety-related systems – Part 3: Software requirements
IEC 61508-4	IEC 61508-4:1998, Functional safety of E/E/PE safety-related systems – Part 4: Definitions and abbreviations
IEC 61508-5	IEC 61508-5:1998, Functional safety of E/E/PE safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels
IEC 61508-6	IEC 61508-6:2000, Functional safety of E/E/PE safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC 61508-7	IEC 61508-7:2000, Functional safety of E/E/PE safety-related systems – Part 7: Overview of techniques and measures

The first four parts of IEC 61508 define the way to comply with the specification. The last three parts are "informative," essentially providing additional guidance, examples, and recommendations for complying with IEC 16508.

IEC 61508 can be used in a broad variety of safety-critical systems, including emergency shutdown systems in power plants, turbine controls, railway signalling systems, and other electromechanical systems in safety-critical environments.

FDA 501(k). FDA Section 510(k), or Premarket Notification (or PMN), of the Food, Drug and Cosmetic Act requires device manufacturers to register and/or notify the FDA at least 90 days in advance of their intent to market a medical device.

Specifically, medical device manufacturers are required to submit 501(k) premarket notifications if they intend to introduce a device into commercial distribution for the first time or reintroduce a device that will be significantly changed or modified to the extent that its safety or effectiveness could be affected.

The safety implications are similar to FAA requirements, where life-critical devices and/or safety-critical devices are required to have a prudent design, code, and test/QA strategy in order to produce a product that is safe to use.

Validated Software Corporation's Validation Suite

One of the thorniest problems in the embedded software industry is the certification of COTS RTOSs. Most commercial software companies do not have the rigorous internal policies to routinely create certifiable software (at higher levels). Although good progress has been made in the RTOS industry, typically, certifiable packages from RTOS vendors are highly priced and certification is not performed by the mainstream engineering team nor is supported by the company as a whole.
Validated Software created its Validation Suite product for MicroC/OS-II to address this recurring issue of RTOS users requiring DO-178B and/or other safety certification documentation. The key differentiators are that the Validated product is fully supported by Jean Labrosse/Micrium and is offered at a very affordable price. It is a complete set of design, test, and test result documents that create a certifiable collection of documents that satisfy DO-178B requirements for any given safety certification level, including Level A.

In addition, Validated created the Validation Suite for MicroScheduler product to address the requirements of many users who just need a minimal scheduler for their safety-critical systems. The Validation Suite for MicroScheduler is similar to the MicroC/OS-II Validation Suite, except that only tasking, interrupts, semaphores, and the timer are supported. This product is also ideal for projects with severe memory footprint constraints. The pricing is very aggressive, and now enables even the smallest of avionics vendors to use the commercial RTOS in their products and receive all of the required source, documentation, and test material required from a qualified and dedicated vendor.

The Validation Suite consists of the following documentation for Level A through Level C certifications:

Validation Suite Document	***DO-178B Requirement***
Software Design Description	Section 11.10
Software Requirements Document	Section 11.9
Software Correlation Matrix	Section 11.16
Software Integration Test Procedure	Section 11.13
Software Integration Test Plan	Section 11.13
Software Integration Test Report	Section 11.14
Software Verification Test Procedure	Section 11.3
Software Test Plan	Section 11.5
Software Unit Test Procedure	Section 11.13
Software Unit Test Plan	Section 11.5
Software Unit Test Report	Section 11.14
MicroC/OS-II Source Code	Section 11.11
Test Coverage Report	Section 11.14
Test Results Report	Section 11.14
Test Code and Test Scripts	Section 11.13
Version Description Document	Section 11.16

In addition to the above documentation, the Validation Suite includes one project production license from Micrium. Also, the Validation Suite contains all source code to MicroC/OS-II and all source code to test files, test scripts, and build/make files. The Integration Tests of the Validation Suite are tailored to each specific implementation of MicroC/OS-II to ensure that the exact implementation has been tested. This allows the user to rerun the tests if desired.

Note that all improvements Validated found for MicroC/OS-II during our certification efforts were submitted back to Jean Labrosse and folded into the standard release product. We try to synchronize with the standard releases after completing new certifications, if required. This makes the $74.95 price for MicroC/OS-II the best embedded solution on the planet.

To make the Validation Suite even more affordable, it can be reused on new projects under 8110.97 with minimal licensing costs. This is, of course, dependent upon the system changes between projects. FAA projects should refer to DO-248B, FAA Notice 8110.97, and their DERs for full compliance when reusing Validation Suite life-cycle data and artifacts on multiple projects.

MicroC/OS-II. Many people have asked, “Why MicroC/OS-II?” MicroC/OS-II was chosen for many reasons:

1. MicroC/OS-II is a very stable operating system that has been used in tens of thousands of systems and hundreds of commercial applications. It has been in use for over 10 years, with minor modifications made periodically.

2. MicroC/OS-II has been “open source” since its creation. Therefore, it has been reviewed by thousands of individuals. But, unlike some open source projects, revisions are tightly controlled and reviewed by Micrium and then openly reviewed by the MicroC/OS-II community. Problem Reports (PRs) are openly available.

3. MicroC/OS-II was written against a very strict coding standard, which improves readability, understandability, and maintainability – all key aspects of creating software used in critical systems.

4. Every line of MicroC/OS-II is well documented. This is extremely rare in the software industry and is ideal for safety certification where the mapping of requirements to source code to test for every line of code is required.

For more information about MicroC/OS-II, refer to www.Micrium.com. For more information about the Validation Suite, see www.ValidatedSoftware.com. Complete product information, including sample of each DO-178B document in the Validation Suite can be requested from the Validated Software Sales office. Call 650-712-0655 or email Sales@ValidatedSoftware.com.