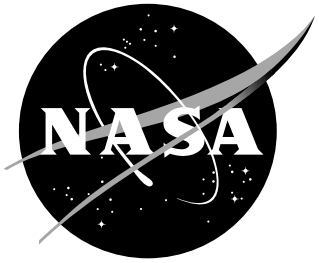
NASA / TM-1998-207648



Streamlining Software Aspects of Certification: Technical Team Report on the First Industry Workshop

Kelly J. Hayhurst and C. Michael Holloway
Langley Research Center, Hampton, Virginia

Cheryl A. Dorsey
Digital Flight, Clifton, Virginia

John C. Knight
University of Virginia, Charlottesville, Virginia

Nancy G. Leveson
University of Washington, Seattle, Washington

G. Frank McCormick
Certification Services, Inc., Carnation, Washington

Jeffrey C. Yang
The MITRE Corporation, McLean, Virginia

April 1998

The NASA STI Program Office ... in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that help round out the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results ... even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

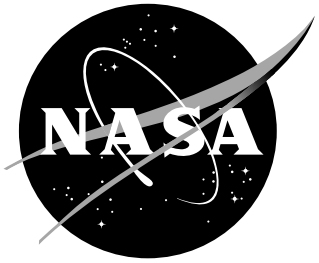
- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at (301) 621-0134

- Phone the NASA Access Help Desk at (301) 621-0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076-1320

NASA / TM-1998-207648



Streamlining Software Aspects of Certification: Technical Team Report on the First Industry Workshop

Kelly J. Hayhurst and C. Michael Holloway
Langley Research Center, Hampton, Virginia

Cheryl A. Dorsey
Digital Flight, Clifton, Virginia

John C. Knight
University of Virginia, Charlottesville, Virginia

Nancy G. Leveson
University of Washington, Seattle, Washington

G. Frank McCormick
Certification Services, Inc., Carnation, Washington

Jeffrey C. Yang
The MITRE Corporation, McLean, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

April 1998

Available from the following:

NASA Center for AeroSpace Information (CASI)
7121 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 487-4650

Outline

Abstract

To address concerns about time and expense associated with software aspects of certification, the Federal Aviation Administration (FAA) began the Streamlining Software Aspects of Certification (SSAC) program. As part of this program, a Technical Team was established to determine whether the cost and time associated with certifying aircraft can be reduced while maintaining or improving safety, with the intent of impacting the FAA's Flight 2000 program. The Technical Team conducted a workshop to gain a better understanding of the major concerns in industry about software cost and schedule. Over 120 people attended the workshop, including representatives from the FAA, commercial transport and general aviation aircraft manufacturers and suppliers, and procurers and developers of non-airborne systems; and, more than 200 issues about software aspects of certification were recorded. This paper provides an overview of the SSAC program, motivation for the workshop, details of the workshop activities and outcomes, and recommendations for follow-on work.

1. Introduction & Background

The FAA has received complaints that the software aspects of certification for high integrity applications require an inordinate amount of time and expense. Although public safety is the proper concern of the government, excessive cost and time burdens can affect safety by contributing to delays in adopting new, safety-enhancing technologies. To address concerns about time and expense, the Federal Aviation Administration (FAA) began the Streamlining Software Aspects of Certification (SSAC) program. The goal of the SSAC program is to determine whether the cost and time associated with certifying aircraft can be reduced while maintaining or improving safety, with the intent of impacting the Flight 2000 program (ref. F2000).

The first public activity of the SSAC program was a workshop in Fairfax, Virginia on 7-8 January 1998. This paper provides an overview of the SSAC program, motivation for the workshop, details of the workshop activities and outcomes, and recommendations for follow-on work.

1.1 Motivation for SSAC Program

According to Huettner, "Aviation in the United States and throughout the world is in the midst of a technological revolution as a result of recent advances in navigation, communications, and computing technologies." (ref. Huettner) Software is at the heart of this revolution. Due to its flexibility, software has become the medium of choice for enabling advanced automation in both airborne and ground-based systems. In the October 1996 issue of Avionics Magazine, David W. Robb wrote (ref. Robb):

> "Avionics have never been more clearly at center stage. The benefits of flat-panel and heads-up displays, the precision of GPS positioning, the efficiency of satellite communications, the revolution in automated test equipment, and the flexibility of integrated avionics, to name just a few areas, are transforming aviation almost faster than we can print these words. … It is no secret that aircraft are becoming ever more dependent on their on-board electronics. The emerging world of CNS and Free Flight promises to accelerate this trend dramatically. As this equipment grows more capable and sophisticated, so does the challenge of testing and maintaining it--for the largest airline to the smallest General Aviation shop."

It is difficult and costly to demonstrate that complex, embedded, real-time software meets its requirements and is safe. An intricate system of rules and regulations govern the use of software in our aviation system. The 14 Code of Federal Regulations (14 CFR) sets forth the rules governing the aircraft certification process. The airworthiness standards for general aviation and civil transport aircraft are covered in 14 CFR part 23 and part 25, respectively. In particular, 14_CFR XX.1301 and XX.1309 require that aircraft systems meet their intended function, do not negatively impact other systems or functions on the aircraft, and are safe for operation. To meet these requirements with software, Advisory Circular # 20-115B specifies the use of RTCA/DO-178B *Software Considerations in Airborne System and Equipment Certification* as a means for obtaining approval of digital computer software (ref. AC 20-115B). Consequently, the DO-178B guidelines influence much of the software development for the commercial civil transport and general aviation industries. With capabilities such as the Future Air Navigation System (FANS) now providing a direct data link between airborne and non-airborne systems, DO-178B may influence non-airborne systems in the near future.

The stated purpose of the DO-178B document is "to provide guidelines for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements" (ref. DO-178B). These guidelines represent the consensus of the avionics software community on the best software engineering practices at the time the document was written. Software engineering is not a mature discipline, and many questions still remain about the relative effectiveness and expense of various software engineering methods and processes embodied in DO-178B.

Although no commercial airline crashes are directly attributed to software, there are several instances where software errors have contributed to incidents. For brevity, only two examples are given.

On December 12, 1991, an Evergreen International Airways Boeing 747 was in cruise flight at 31,000 feet. Suddenly, the aircraft entered a steep right bank and rapidly descended more than 10,000 feet. During the recovery, the right wing was damaged, including extensive damage to the honeycomb structure on both sides of the wing. The crew successfully landed the aircraft, and no one was injured. According to the Transportation Safety Board of Canada, the flight upset was caused by an uncommanded, insidious roll input by the channel A autopilot. (ref. Billings)

The second incident occurred on May 12, 1997. An American Airlines Airbus A300B4-605R was heading to Miami from Boston. While turning into a holding pattern, the A300 slowed from 210 knots to 177 knots. Its stall warning system activated. Suddenly, the aircraft dropped from 16,000 feet to 13,000 feet while pitching and rolling to extreme bank angles both left and right. While the plane was losing altitude and flying erratically, both the captain's and the first officer's Electronic Flight Instrument System (EFIS) primary flight displays and navigation displays went blank for 2-3 seconds. On each screen, only white diagonal lines were displayed. One passenger was hurt during the incident, and the plane had minor damage. The National Transportation Safety Board (NTSB) attributed the EFIS behavior to software saying that a feature of the software "results in the loss of all primary flight displays at a time when pilots need their critical information the most." (ref. McKenna)

These types of errors, which are only examples of many that have occurred, lead to concerns about the effectiveness of the certification procedures for this software, as embodied in DO-178B. In addition, there are economic concerns. As already mentioned, some people assert that software aspects of certification for high integrity applications require an inordinate amount of time and expense. The software aspects of certification are identified as the biggest barrier to meeting the FAA’s Flight 2000 goals and schedules. The Flight 2000 program will require acquisition, development, and implementation of new software-intensive systems in both ground-based and avionics domains. The schedule is tight, and participants in these technology demonstrations expect to recoup their capital investments within a reasonable amount of time.

The FAA initiated the SSAC program in response to these concerns. The kick-off meeting for the program was held in Washington, D. C. on 13-14 November 1997.

1.2 Overview of SSAC Program

The primary objectives of the SSAC program are to: 1) analyze the current software approval process for certification and identify target areas for improvement, 2) determine if the desired safety benefit justifies the expense burden, and 3) if necessary, establish streamlined processes for software aspects of certification that are faster and less expensive than the current processes. Although reducing cost and time is the goal of the SSAC program, these reductions must not compromise safety. Short term cost savings that sacrifice safety could prove fiscally imprudent overall if public confidence in aviation safety is lost. There are many examples today that support this premise.

1.2.1 Division Into Two Tracks

Prior to the January workshop, the FAA identified the need to sponsor two independent but related efforts to address issues with software aspects of certification.

The objective of the first effort, referred to as Fast Track, is to determine immediate steps to reduce cost and schedule of DO-178B certification activities for the Flight 2000 program, without negatively affecting safety. Fast track concerns are characterized more as management and programmatic in nature. Often, anecdotal evidence is sufficient to confirm these industry concerns. Issues such as training, policy, and standardization fall into this category.

The second effort, more technical in nature, is intended to address concerns about the DO-178B standard itself. Technical concerns typically require substantiated rather than anecdotal evidence to establish validity. An example of such a concern is the assertion that modified condition/decision coverage (mc/dc), which is required for Level A software, is not effective at finding errors. These claims from a few, or even many, software developers are not enough to justify a change to the requirement; however, they are enough to warrant further investigation. An example of further investigation would be to determine if errors in Boolean logic are common in software development, and in particular whether mc/dc is a cost effective means to test Boolean logic. This effort to identify and address technical issues is referred to as the Technical Track[*].

1.2.2 The Technical Track

The FAA assembled a team of technical experts to objectively identify the cost and schedule drivers of software developed for systems requiring FAA approval and certification. In addition, the team is to propose solutions for problems discovered, and, where feasible, prototype those solutions. For lack of a better name, this team is called the Technical Team.

The Technical Team is led by Kelly Hayhurst, a research scientist at NASA Langley Research Center. The other members of the team are Cheryl Dorsey from Digital Flight and Frank McCormick from Certification Services, Inc., both Designated Engineering Representatives (DERs); Professor John Knight from the University of Virginia; Professor Nancy Leveson from the University of Washington, both experts in the field of software safety; Michael Holloway, a research engineer at NASA Langley Research Center; and Jeffrey Yang, a software systems engineer from Mitre. The lack of direct industry participation is intentional, to reduce the potential for bias towards or against particular companies.

The lack of direct FAA participation is also intentional. The Technical Team is intended to serve as an independent team to research issues and provide recommendations to the FAA. This does not mean that the FAA is not participating fully. The SSAC Program Manager, Leanna Rierson (AIR-130), provides guidance to the Technical Team and coordination with the Fast Track effort. In addition, the FAA has established an advisory team for the SSAC program; its members are Arthur Pyster (AIT-5), Michael DeWalt (ANM-106N), Roger Cooley (AIT-5), Peter Saraceni (AAR-421), James Williams (AIR-130), Ronald Stroup (ASW-190), and Joe Caravello (AIT-200).

[*] This work was supported by the FAA William J. Hughes Technical Center, Atlantic City International Airport, New Jersey.

The mission of the Technical Team is to gather, analyze, and synthesize objective evidence concerning cost and schedule drivers for software aspects of certification. The team's mission is not to discredit DO-178B, replace RTCA Special Committee 190 (SC-190), or prescribe FAA policy, but rather to validate or invalidate assertions about software aspects of certification. The work done by this team would then be used to consider modification to policy or guidance by the FAA and RTCA SC-190/WG-52.

Historically, meaningful measurements of software engineering processes and products have been frequently difficult and sometimes impossible to obtain. This is largely due to insufficient and inconsistent measures for evaluating cost and quality. Standards, produced by forums such as the RTCA, are based on the consensus of best engineering judgment and current best practice. In some respects, this program is an attempt to see if the consensus process can be augmented by objective, substantive data. The success of this program requires FAA and industry participation to ensure that our investigation is relevant to their concerns. The Technical Team, government, and industry must form a partnership to identify concerns, determine what data is available, find practical ways to get that data, and understand what the data represents.

1.2.3 Technical Track Programmatics

The Technical Track has three phases:

- Data Collection and Analysis,
- Implementation, and
- On-going Activities

The goal of Phase I is to identify major concerns about cost and schedule drivers and to collect data from both airborne and non-airborne systems development activities to either validate or invalidate those concerns. The data collected should be specific enough to support new or alternate guidance preparation by the FAA, as appropriate.

Specifically during this phase, the Technical Team must:

- solicit FAA and industry concerns with respect to the software aspects of certification
- classify the concerns as programmatic or technical
- define practical means for collecting data
- collect and analyze the data
- recommend changes in the certification process or in software development methods

The primary objective of Phase II is to evaluate the proposed recommendations. Ideally, real development projects would be used to test the proposed recommendations. However, using real projects to test recommendations requires close coordination with industry and the FAA. As the proposed recommendations are prototyped, data will be collected to assess the effectiveness of those recommendations, to propose refinements, and to identify other suitable solutions. Finally, Phase III will focus on continuous improvement activities with further data collection and prototyping as necessary.

To impact the FAA's Flight 2000 program, the current schedule requires that both Fast Track and the Technical Track Phase I and Phase II be completed by November, 1999. Given the magnitude of the project and the potential difficulties in collecting consistent metrics for cost, schedule, and problem reports, the schedule is ambitious.

1.2.4 Early Decisions of the Technical Team

The original SSAC program plan called for the Technical Team to define the types of data to be collected, identify the methods for collecting the data, and determine the metrics for analyzing it. The Team would then present their work to industry for comment and criticism. Rather than run the risk

of defining metrics and data collection methods to address non-existent problems, the Technical Team decided to conduct a workshop to elicit concerns about the certification process from industry. This paper further discusses the workshop, the summary and classification of data collected, recommendations, and proposed follow-on activities.

2. SSAC Industry Workshop

The workshop was held at the TRW facilities in Fairfax, Virginia on 7-8 January 1998. The workshop objective was to solicit opinions from industry representatives on the following questions:

- Are the techniques prescribed in DO-178B effective?
- Can software aspects of certification be streamlined without affecting safety?
- Are costs incurred that do not contribute to safety?

2.1 Logistics and a Note on the Questionnaire

Logistics support was provided by TRW/Systems Engineering Technical Assistance (TRW/SETA). In addition to choosing the location for the workshop, TRW/SETA compiled the invitation lists, created information packets in consultation with the SSAC Program Manager, mailed invitations and packets, and maintained the list of attendees.

The information packet sent to invitees included an informal questionnaire about software aspects of certification. The questionnaire was written in a provocative manner, to hopefully stimulate industry response and participation for the workshop. Questionnaire responses are found in Appendix A.

Over 120 people attended the workshop, including representatives from the FAA, commercial transport and general aviation aircraft manufacturers and suppliers, and procurers and developers of non-airborne systems. A list of the attendees is given in Appendix B.

2.2 What We Planned to Happen

Prior to the workshop, each participant was placed in one of four groups, which for ease of identification were labeled by the colors black, red, orange, and green. The intent was to ensure that each group had participants from a cross-section of companies, organizations, and areas of specialization. Each group was led by a member of the Technical Team. Professor Knight led the black group; Professor Leveson led the red group. The orange and green groups were led by Cheryl Dorsey and Frank McCormick, respectively. Each group also had a designated scribe to record the comments.

To facilitate soliciting and recording comments, the Technical Team developed a Comments Acquisition Table (CAT). The format of this table is shown in table 1.

Table 1. Comments Acquisition Table

	Planning	Requirements	Design, Code, & Integration	Verification	CM, SQA, & Certification Liaison
Compliance					
Comprehension					
Completeness					
Cost & Effectiveness					

The columns of the table are based on the software life cycle processes identified by DO-178B. The rows of the table represent the four attributes the Technical Team considered important for each process:

- Compliance: How well do developers follow DO-178B?
- Comprehension: How easy is it to understand what DO-178B requires?
- Completeness: How much of the software development is covered by DO-178B?
- Cost & Effectiveness: What is the cost of applying DO-178B?

The plan was for each group to address each cell of the CAT. For each cell, the group leaders were instructed to have participants do the following: 1) document issues in detail with respect to that life cycle process and that attribute, 2) define metrics to assess those issues, 3) determine viable approaches to empirical evaluation, and 4) document alternative non-proprietary approaches. A database tool was developed for the scribes to use to record their groups' responses for each cell in the CAT.

2.3 What Really Happened

After introductory presentations providing motivation for and an overview of the SSAC program, the workshop participants were divided into the four groups. Two of the groups were able to use the CAT effectively for soliciting and recording comments; two of the groups were not. Whether the CAT was used or not, the focus in each group was on disclosing and recording issues, not on validating, debating, or trying to resolve them. Every issue that was raised was recorded, unless everyone in the group agreed that it should not be. Thus, no one should infer from the inclusion of an issue in the list that the issue is necessarily valid, nor should anyone infer an importance ranking for the issues. Determining the validity and importance of the issues will be the subject of future work.

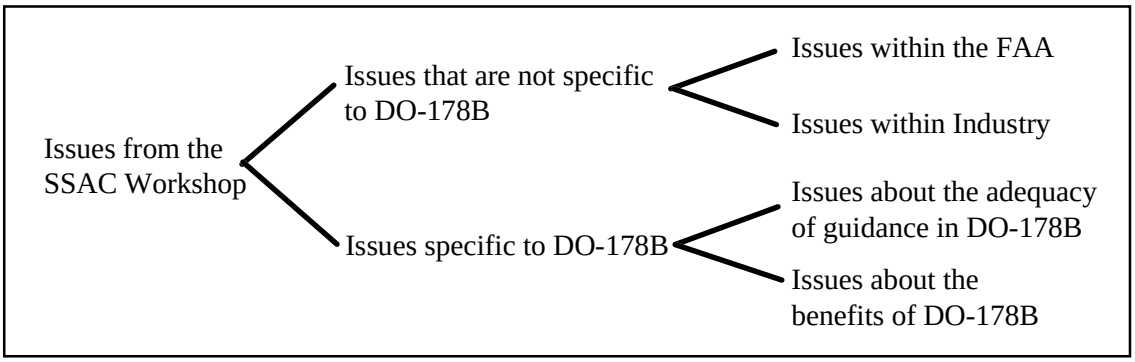
Four steps were taken to allow participants to express their concerns freely. First, no individual or company names were recorded in the issues database. Second, time was set aside in each of the groups during which no FAA personnel were permitted in the room. Third, participants were allowed to submit anonymous written comments on index cards. Fourth, FAA participation was limited to encourage open discussion.

Including four anonymous comments, a total of 215 issues were recorded during the discussion sessions. These issues are listed in Appendix C. Due to the volume of issues raised and the time spent expressing and recording them, very few issues address metrics, evaluation criteria, or alternative approaches. Metrics, evaluation criteria, and alternate approaches recorded in the database may be used for completing recommended future activities.

3. Classification of Issues

Even a casual perusal of the 215 workshop issues reveals that overlap and similarities exist. Classification of these issues is somewhat subjective. Consistent classification of issues is difficult, but necessary to provide focus and direction for further investigation and validation.

After several attempts, a workable scheme for classifying these issues was defined. Each comment recorded at the workshop is mapped onto the classification scheme and presented in Appendix D. As with most classification schemes, many issues are found in more than one category. The hierarchy for the classification scheme is shown below:



Each workshop issue was classified by whether or not the issue is specific to DO-178B. Issues not specific to DO-178B include those things that would be likely to exist even if DO-178B did not. Some of these issues mention DO-178B, but it is clear that the issue would remain even if major changes were made to the standard. Issues that are specific to DO-178B involve the details of the standard.

3.1 Issues That Are Not Specific to DO-178B

Most issues not specific to DO-178B are concerned with organizational and programmatic matters such as communication, resource management, planning, and training. The issues not specific to DO-178B were divided into the sub-categories: Issues within the FAA, and Issues within Industry. Issues that involve people employed or authorized by the FAA, or procedures used or overseen by the FAA are classified as "issues within the FAA." An issue was within industry if it involved people or procedures over which the FAA had no direct control.

3.1.1 Issues within the FAA

The following issues fall under the sub-category "issues within the FAA":

1. Inconsistencies exist among ACOs in interpreting and following policy and guidance.
2. ACOs do not provide quick, meaningful responses to applicants.
3. Insufficient knowledge of software engineering and related disciplines exists within the FAA.
4. Inadequacies, inconsistencies, and inefficiencies exist in the DER system.
5. Insufficient information is available about the certification process.
6. Problems exist within the TSO, TC, STC, ATC, and PMA processes.
7. Working with non-U. S. certification authorities is difficult.

Each of the seven sub-categories is discussed separately and briefly.

- *Inconsistencies exist among ACOs in interpreting and following policy and guidance.*

In all four groups, issues related to inconsistencies among the FAA's various ACOs were discussed frequently. These inconsistencies included varying documentation requirements, and different interpretations of DO-178B requirements such as "with independence", "tool qualification", and "partitioning". Workshop participants also cited instances of inconsistencies within the same ACO when personnel changed.

Two specific comments from the database that fall within this sub-category are 1) "What plans does the FAA have to monitor and regulate consistency between ACOs in compliance findings, and in educating their people to be consistent?" and 2) "In areas of interpretation difficulty, much time is spent in negotiating with regulators." The same issue was raised in a questionnaire response in the

following way: "Not all ACOs are equal when it comes to rigor in analysis and fairness in judgment. What is rejected in one region is acceptable in another."

- *ACOs do not provide quick, meaningful responses to applicants.*

Workshop participants asserted that ACOs respond slowly to submissions. Justifications for information requests or revisions can be ambiguous. For example, a workshop participant asserted that "Regulators buy time by asking irrelevant questions requiring a response from the applicant, while stopping all review activities until after they receive the response."

- *Insufficient knowledge of software engineering and related disciplines exists within the FAA.*

Another frequently asserted problem was the lack of adequately trained personnel, especially for software issues. One workshop participant observed, "There is a definite lack of software experience in the FAA on a national basis. The FAA has a few good people but like the Marines they need more." Lack of knowledge about software and systems engineering can also cause problems. In one group, participants discussed the hidden costs of applicants "caving in" to FAA demands that seem unreasonable, solely to avoid schedule delays. Many participants thought that lack of knowledge caused ACOs to take an overly conservative approach to compliance, relying on checklists instead of informed engineering judgment.

- *Inadequacies, inconsistencies, and inefficiencies exist in the DER system.*

Some workshop participants thought the DER system does not work well for software aspects of certification. Some thought that the FAA should delegate much more authority to the DERs than they currently do. Others thought that the current qualification standards for DERs were inadequate.

- *Insufficient information is available about the certification process.*

Much of the information about the certification process is not well documented, and that which is documented is not readily available to industry. As a specific example, one participant said, "There is a lack of central repository for availability of the checklist used by the FAA, issue papers, policy letters, etc."

- *Problems exist within the TSO, TC, STC, ATC, and PMA processes.*

Several participants thought the TSO, TC, STC, ATC, and PMA processes do not work nearly as well for software aspects of certification as they do for other aspects of certification. An example comment is, "Why is there a wide variance in software approval between TC, STC, TSO? How can the processes be made more similar? How can the playing field be leveled?"

- *Working with non-U. S. certification authorities is difficult.*

Several workshop participants experienced difficulties in working with certification authorities other than the FAA. Some thought that reciprocal agreements with other certification authorities were not being granted or honored as often as in the past. A specific example cited in a questionnaire response was this: "We are currently preparing for the Joint Aviation Authority (JAA) for a [product] that was recently certified for the FAA. Preparation of additional documentation for the JAA software certification will take about 200 hours. There are no additional software tests or analysis in this effort, so the product will be identical."

3.1.2 Issues within Industry

Although industry participants had quite a few criticisms of the FAA, they did not ignore similar concerns within their own companies. For issues within industry, three sub-categories were identified:

1. Insufficient knowledge of software engineering and related disciplines exists within industry.
2. Lack of cooperation among companies increases costs.
3. Requirements definition is difficult independent of certification.

Each of these is discussed separately below.

- *Insufficient knowledge of software engineering and related disciplines exists within industry.*

Some workshop participants asserted that industry lacks sufficient expertise in the disciplines necessary for software development. One participant raised the issue of qualifying professionals in software engineering, stating that: "Qualification for systems and software related work is not formalized in the same sense as other engineering fields."

- *Lack of cooperation among companies increases costs.*

The failure of companies to share information with one another was cited as a contributor to unnecessary costs. The following two comments are typical: "Companies spend a great amount of resources researching which tools to use" and "Can an industry-wide group exist to do data gathering on new topics? Issues include exposing dirty linen, so data needs to be kept without company/person/system association."

- *Requirements definition is difficult independent of certification.*

At least one group spent time discussing their perceptions of the cost drivers in generic software development efforts. According to that group, the "Greatest cost driver is poor requirements." Other comments supporting the difficulties with requirements definition include "Poor requirements is a cost driver" and "Minor requirements changes affect documentation and certification."

3.2 Issues That Are Specific to DO-178B

Classification of DO-178B specific issues was relatively straightforward, although determining categories for these issues was much more difficult. The two categories used are: Issues about the adequacy of guidance in DO-178B, and Issues about the benefits of DO-178B. The first category includes those issues where workshop participants thought that the written guidance in DO-178B is deficient, especially with respect to completeness and clarity of the existing guidance. The second category covers DO-178B activities or objectives that were considered unnecessary or insufficiently justified. It also includes assertions about things that might be missing from the standard.

3.2.1 Issues about the adequacy of guidance in DO-178B

Quite a few comments were made about the guidance offered in DO-178B. Those comments were grouped into the following ten sub-categories addressing inadequate and ambiguous guidance in DO-178B … :

1. . . . for documentation
2. . . . for planning and configuration management
3. . . . for requirements definition and analysis
4. . . . for partitioning
5. . . . for verification activities
6. . . . for tool qualification
7. . . . for Commercial Off The Shelf (COTS) software
8. . . . for reuse of certification data
9. . . . for reuse of legacy systems
10. . . . for non-airborne systems

Each sub-category is discussed below.

- *DO-178B has inadequate and ambiguous guidance for documentation.*

Workshop participants asserted that the standard's documentation guidance is inadequate in at least three ways. First, there are inadequate provisions for electronic document submission. "DO-178B/ED-12B does not address modern documentation tool systems. The Certification Authority will require hard copy documents and not accept access to the automatic document system," is a representative comment.

Another perceived inadequacy is the failure to properly define when specific documents are due to the certification authority. As one participant put it, there is an "issue of when the life cycle data and qualification data are due, and when the FAA certification authority approvals are due. For example, the PSAC is useless if not submitted or approved early enough to be effective."

Some participants also thought that the standard gave too much leeway to ACOs to determine exactly what documents are required. One area in which this was asserted to be true is that of derivative products: "Currently, complete plans are required for the derivatives, even if they are only barely different from previous products. There is little value in producing the plan for the derivative."

- *DO-178B has inadequate and ambiguous guidance for planning and configuration management.*

Some workshop participants thought that additional guidance is needed for planning. This was expressed in one group by the following comment: "DO-178B is a what and not a how standard, and experienced developers are able to understand the level of effort required. However, DO-178B does not provide sufficient information for the new applicant to scope their level of effort."

Some participants also thought that configuration management was not discussed adequately. In particular, there is "confusion about CC1s and CC2s" and the "description in CM section is difficult to understand."

- *DO-178B has inadequate and ambiguous guidance for requirements definition and analysis.*

Some workshop participants thought that better guidance is needed for requirements definition and analysis. For example, at least one person asserted that there is "much confusion caused by the distinction between high and low level requirements." Another said that "lack of good requirements definition impacts the cost of verification," and asked the question, "Is the guidance in DO-178B sufficient and consistent to help the developer?" The potential impact of "implied requirements" was also a concern, and the assertion was made that "DO-178B guidance should address how implied requirements that affect safety should be addressed."

- *DO-178B has inadequate and ambiguous guidance for partitioning.*

The growing importance of partitioning was recognized by workshop participants. For example, the question was asked, "what types of techniques are acceptable and what are the criteria to accept a partitioning strategy?"

- *DO-178B has inadequate and ambiguous guidance for verification activities.*

Verification activities were discussed frequently in most of the groups. Areas of discussion included, but were not limited to, structural coverage, independence, the conformity process, and regression analysis. Example comments include "DO-178B/ED-12B fails to provide clear direction on regression analysis", "For lower levels of software, there are different interpretations about the extent to which testing has to be done on the target," and there are "Different interpretations of the applicability of coverage analysis techniques to different stages of verification."

- *DO-178B has inadequate and ambiguous guidance for tool qualification.*

Tool qualification was another area that was the subject of much discussion. Some people asserted explicitly that DO-178B has deficient guidance in this area: "DO-178B/ED-12B does not clearly define the difference between development and verification tools and the requisite requirements." Others suggested that the intent of the standard is often misunderstood: "There is

major misunderstanding of the intent behind the tool qualification requirements in DO-178B/ED-12B. In many cases more stringent requirements are imposed than intended or the requirements are misapplied to inappropriate items."

- *DO-178B has inadequate and ambiguous guidance for COTS software.*

Unlike many of the other areas in which multiple, similar comments were recorded, each group recorded only one comment about COTS. This does not mean that workshop participants did not consider this an important area; they did. One group recorded the concern this way: it is "imperative to develop a set of guidelines to establish how COTS can and will be certified."

- *DO-178B has inadequate and ambiguous guidance for reuse of certification data.*

Some workshop participants thought that DO-178B does not provide adequate support for the use of data from previous certifications in new certifications. Comments in this area included "The reuse of certification data is extremely difficult", and "Same product, different customers causes a repetition of activities."

- *DO-178B has inadequate and ambiguous guidance for reuse of legacy systems.*

This category differs from the previous one in that it refers to reuse of data from systems certified under standards other than DO-178B. Systems previously certified under DO-178A were the subject of particular concern: "DO-178B does not provide adequate guidance for migrating legacy programs being used. A legacy may not have done its certification to meet DO-178B objectives, but still may be a safe system", and "Forcing the use of DO-178B/ED-12B on systems originally developed to DO-178A is intrusive and expensive especially when there is extensive service experience."

- *DO-178B has inadequate and ambiguous guidance for non-airborne systems.*

The final area in which workshop participants expressed dissatisfaction with the current guidance in DO-178B was non-airborne systems. One group asserted that there is an "issue of how to certify human-computer interface software to be compliant with DO-178B. As a result, cost, schedule, and safety may be impacted. This may be difficult to get air and ground community to agree." Someone in another group claimed to be "having a difficult time determining who in the FAA approves ground systems, and getting different answers. Most common answer is to do the most expensive thing possible."

3.2.2 Issues about the benefits of DO-178B

Under the final category “Issues about the benefits of DO-178B”, four sub-categories were identified.

1. The extent to which DO-178B provides benefits beyond those that are provided by other industry accepted practices is unclear.
2. The effectiveness of some specific activities required by DO-178B is unclear.
3. DO-178B inadequately provides for innovation.
4. DO-178B inadequately addresses the effect of software on the safety of the overall system.

Each is discussed below.

- *The extent to which DO-178B provides benefits beyond those that are provided by other industry accepted practices is unclear.*

Some of the workshop participants thought that their internal company practices were sufficient to ensure the quality and safety of their products. For example, one person asserted that their company had "parallel, or shadow, processes --- one to develop the product, the second to satisfy certification objectives." Another asked, "... shouldn't a sound development methodology suffice?"

Suggestions were also made that the FAA should give certification credit to a company based on its rating by process auditing organizations such as the Software Engineering Institute (SEI) or the

International Standards Organization (ISO). This idea was expressed like this: "Why couldn't SEI maturity level be used as an alternate means?"

While some participants wanted increased concentration on process, others criticized DO-178B for concentrating too heavily on process. For example, contrast the following two comments: "DO-178B does not allow for qualification of process once versus product each time," and "Transition criteria forces developers to focus on process rather than products and does this focus on process, versus product, affect safety?"

- *The effectiveness of some specific activities required by DO-178B is unclear.*

While the previous category included concerns about the overall effectiveness of DO-178B, this category includes concerns about the effectiveness of specific requirements of DO-178B. Activities whose effectiveness was questioned included, but were not limited to, preparing documentation, tracing requirements to code, establishing independence, and demonstrating structural coverage. For example, in one group the assertion was made that "One of the major software development costs has been requirement changes resulting in rework changes. DO-178B/ED-12B exacerbates this issue due to the stringent requirements for documentation that may not be done otherwise."

- *DO-178B inadequately provides for innovation.*

In various ways, workshop participants asserted that DO-178B did not provide adequately for the use of innovative techniques. Many people thought that the approach taken by DO-178B to permit alternate means of compliance is not working well: "DO-178B specifies that alternative methods can be used as long as the objectives are met, but in practice it is not feasible." Also, "Alternative methods are not up to date with current software development methods. A means [is needed] to easily/generically accommodate advances in technology without specifically including the technology in the document. DO-178B/ED-12B forces the applicant to address the objectives directly which may not be applicable for a given technology or the base intent of the objective."

- *DO-178B inadequately addresses the effect of software on the safety of the overall system.*

The last category in our classification includes concerns about the relationship between DO-178B requirements and the effect of software on system safety. Discussions about safety were frequent. Here is an example comment: "The objective of certifying software is safety. DO-178B does not specifically address safety. Unless we assume all the safety areas are covered by systems and all software has to do is replicate the system correctly. The end software product design needs to be checked for safety."

This completes the discussion of our classification scheme. Although others might classify the issues differently, the scheme presented here provides a basis for discussing future work. Our recommendations for future work are given in the next section.

4. Recommendations

As shown in the previous section, the classification has four main sub-categories:

- Issues within the FAA
- Issues within Industry
- Issues about the adequacy of guidance in DO-178B
- Issues about the benefits of DO-178B

The classification scheme presented in section three signifies the need for a multifaceted approach to the streamlining software aspects of certification task. The issues identified in each of the four main sub-categories should be addressed differently and by different groups. In particular, the last

sub-category contains those issues appropriate for the Technical Team. Specific recommendations for each sub-category follow.

4.1 For Issues Within the FAA

For several reasons, issues within the FAA should be handled by Fast Track rather than the Technical Team. These issues involve internal FAA personnel and procedures, and only the FAA has the authority necessary to make those changes. Determining the validity, or lack thereof, of most of these issues does not require the type of comprehensive data collection for which the Technical Team was formed. For some of the issues, little or no new data should be required. For others, the required data is either already available within the FAA, or simple to obtain from industry.

Perhaps a more important reason why Fast Track should handle these issues is that workshop participants claimed that these issues cause the most frustration and account for a large percentage of the unnecessary costs and schedule delays. Resolution of the technical issues without some kind of resolution of the internal FAA issues is insufficient. Addressing these issues quickly, as Fast Track is intended to do, should go a long way towards both developing trust and cooperation with industry and reducing unnecessary costs and delays.

Not all issues recommended for Fast Track can be handled quickly. For example, consider the issue *Insufficient knowledge of software engineering and related disciplines exists within the FAA*. Determining whether this is true should be simple; the FAA probably already knows the answer. If it is true, devising and implementing an appropriate strategy to address it will not be easy.

For some of these issues, the FAA already has some programs in place. For example, training courses for FAA management and personnel (airborne and non-airborne) on the use and misuse of DO-178B are currently in progress. In conjunction with the training program, topics requiring additional policy will be identified and addressed. Standardization issues are also being studied.

4.2 For Issues Within Industry

Obviously, organizational and programmatic issues within industry should be handled by industry. Training and communication issues especially are common within most industries. However, addressing issues about insufficient knowledge or lack of cooperation is beyond the legitimate scope of either the SSAC program or the government. It is not our job to dictate to industry how they should train their people or how they should get along.

Addressing the difficulty of requirements definition is different, in that a legitimate role may exist for government-sponsored research. Such research, however, is beyond the scope of the SSAC program.

4.3 For Issues about the adequacy of guidance in DO-178B

Many of the issues within this category should be handled by SC-190/WG-52. Others can perhaps be handled by Fast Track. Determining which are appropriate for SC-190/WG-52 and which are appropriate for Fast Track should be done by representatives from both groups. For several of the sub-categories, SC-190/WG-52 already has established teams. Although participation in SC-190/WG-52 by individual members of the Technical Team is appropriate, it would not be appropriate for the Technical Team as a whole to address these issues.

4.4 For Issues about the benefits of DO-178B

Although the issues identified in this category are probably the most difficult to validate and remedy, the Technical Team is best suited to address these. The technical aspects of the software approval process should be based on sound, objective foundations. This requires objective data collection and analysis to establish the benefits of those activities required by DO-178B.

Data collection for these issues requires that the Technical Team have unprecedented access to cost, time, reliability, and safety data from both industry and the FAA. Unlike the first three sub-categories, these issues can not be validated with anecdotal information collected from questionnaires or interviews. It is with reference to these types of issues that Professor Leveson said at the workshop, "The plural of anecdote is not data."

Schedule and cost constraints prohibit the Technical Team from analyzing each individual issue to determine the specific data requirements. A more suitable approach, and one that reduces duplication of effort, is to investigate the root cause underlying all, or many, of the issues.

What is the root cause? There is a lack of evidence to establish the overall cost-benefit of the current process for software aspects of certification, especially in relation to alternative approaches. In part, the lack of evidence is due to insufficient measures or inadequate attempts to measure many aspects of software engineering. The recommendations of the Technical Team involve defining and collecting data that will permit accurate determination of both the costs of the current process and the associated benefits. There are three specific recommendations: 1) to collect cost data on software projects, 2) to collect safety and reliability data for systems developed under DO-178A and B, and 3) to collect benefit data on alternate means of compliance.

4.4.1 Collecting Cost Data

The first recommendation is to collect basic cost information on software projects. This data would be collected from both the FAA and the manufacturers for each project. The following types of information would be required:

- project start and stop date
- project size
- software level
- type of system (function and whether it was based on an existing company product line or a new company product line)
- type of aircraft
- type of approval sought
- development costs, including number of work-hours
- development process used
- verification methods employed
- quality assurance records
- software development background and experience in using DO-178B
- basic software metrics such as number of source lines of code, programming language used, complexity index, and similar things
- number and types of changes prior to and after approval.

This information should lead to an understanding of the costs of the current software approval process. Although companies may be reluctant to provide some of this information, most of it should exist in some form or another.

4.4.2 Collecting Safety and Reliability Data

The information required to understand the primary benefits (those intended to assure safety and reliability) of the current certification process may be more difficult to collect. For software, no good metrics exist for safety or reliability. Thus, information on key indicators of safety and reliability must suffice.

Towards that end, the Technical Team should collect information on the software safety and reliability of systems developed under DO-178A and B. Should companies be unwilling to provide internal data about safety and reliability of fielded systems, records such as Airworthiness Directives and incident and accident reports will be used. This data should then be compared with safety and reliability data from software critical systems in other communities, such as the military, the nuclear industry, and the medical industry. To secure a more complete picture of software safety and reliability, anomaly data of digital systems captured in-flight might be worth pursuing.

4.4.3 Collecting Benefit Data

Finally, cost and benefit data for innovative or alternative methods should be addressed. The Technical Team should collect experience data on new or alternative methods of compliance. To do this well requires a common database and a consistent data definition for comparisons among methods.

As these recommendations are further fleshed out, a minimum set of data required for analyses will be defined. This data will then be used to objectively determine the cost-benefit of DO-178B. Access to accurate information about company practices, costs and schedules, and software quality is essential. Without that access, there will be insufficient data to build sound, objective foundations for making decisions and suggestions for improvement.

5. Concluding Remarks

No program to streamline costs can succeed without addressing the fundamental issues associated with certification and safety. A new FAA initiative called Streamlining Software Aspects of Certification is investigating ways to reduce the cost and time associated with certifying aircraft while maintaining or improving safety. As part of the SSAC program, a Technical Team has been established to identify the cost and schedule drivers of aviation software, to propose solutions for any problems discovered, and to prototype those solutions.

As part of this effort, the Technical Team conducted the SSAC Industry Workshop to gain a better understanding of the major concerns in industry about cost and schedule. Over 120 people attended the workshop, including representatives from the FAA, commercial transport and general aviation aircraft manufacturers and suppliers, and procurers and developers of non-airborne systems. Workshop participants freely expressed their issues about software aspects of certification.

The workshop issues were partitioned into four major categories: issues within the FAA, issues within industry, issues about the adequacy of guidance in DO-178B, and issues about the benefits of DO-178B. The Technical Team proposed three specific recommendations to address these concerns: 1) collect cost data on software projects, 2) collect safety and reliability data for systems developed under DO-178A and B, and 3) collect benefit data on alternate means of compliance. The ultimate goal of the Technical Team is to collect data that can help provide an empirical basis from which decisions about software aspects of certification can be made. If appropriate, new guidance might be created to reduce the cost and time associated with software aspects of certification while maintaining or improving safety.

In response to concerns about previous unsuccessful attempts at process improvement, the Technical Team will prepare an action plan in coordination with the FAA to provide additional detail on how the workshop issues will be addressed. A second SSAC Industry Workshop is planned for May 1998 to present this plan to industry. In addition, the progress and results of this project will be made publicly available through a NASA-sponsored web page (http://shemesh.larc.nasa.gov/ssac/).

References

Billings, Charles E.: *Aviation Automation The Search for a Human-Centered Approach*. Lawrence Erlbaum Associates, Publishers, 1997.

Huettner, Charles H.: Toward a Safer 21st Century, Aviation Safety Research Baseline and Future Challenges. NASA NP1997-12-231-HQ, December 1996.

McKenna, James T.: NTSB Warns of A300 Display Reset Problem. *Aviation Week & Space Technology*, February 9, 1998, p. 76.

Robb, David W.: Editor's Note "Endless Horizons", *Avionics Magazine*, October 1996, p. 8.

Advisory Circular # 20-115B. U. S. Department of Transportation, Federal Aviation Administration, issued January 11, 1993.

RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification. Requirements and Technical Concepts for Aviation, Washington, D. C., December 1992.

Flight 2000 Program Plan, http://www.nasi.hq.faa.gov/nasiHTML/f2000/

Appendix A

Responses to the Questionnaire

The following questions were asked in an informal questionnaire distributed with the invitation to participate in the SSAC Industry Workshop:

1. Do you believe there are opportunities to reduce cost/schedule impacts of the certification process without jeopardizing safety? What are they?
2. What is the impact of DO-178B on your organization and process?
3. What has been imposed on you due to DO-178B that you think has no value added?
4. Do you think that DO-178B implementation enhances the safety/quality/reliability of the product? How?
5. Have you had any experiences with certification authorities that have resulted in added cost and scheduling with no value-added? If so, what are they?
6. What other issues do you have with the certification process that adds to cost and delays in the schedule?
7. List alternatives to DO-178B that you think can be used without sacrificing safety/reliability/quality.

The purpose of these questions was to stimulate thinking about software aspects of certification and to stimulate industry response and participation for the workshop. A total of 16 responses to the survey questions were received. However, not all respondents answered all seven questions. Each of the following tables, Tables A1-A7, contains the responses to one of the survey questions. Information about the respondents has been deleted.

Table A1. Do you believe there are opportunities to reduce cost/schedule impacts of the certification process without jeopardizing safety? What are they?

Yes. I believe that cost can be reduced by making more use of previously developed software usually called commercial-off-the-shelf (COTS). This would reduce development schedule but some increase in testing would be expected. The USA military and western European military aircraft fly without FAA certified software. The cost of doing the military software is usually about the same as level "D" DO-178B software.
Qualifying, certifying routines or Sub-routines. So they can be used in different applications providing the level is satisfactory.
Eliminate the redundancies inherent in the software verification documents.
When a submittal, argument, or request in regards to software is made, the FAA should commit to a completion date. It has been our experience that software related delays are not directly in the project managers control. Changing software is a major task that impacts our projects by man-months. A simplified version of the change process with respect to documentation (not less testing) could reduce this impact.
Yes. By addressing safety from the beginning and designing it into the system. The certification process should be based on safety and not in checking boxes and paper work.
Yes. Refer to the body of this letter. We feel strongly that the safety aspects of software certification should NOT be reduced in order to streamline. This process should not be used to provide for blanket approval of software developed for non-aviation environments unless that software can be found to meet the appropriate safely criteria including configuration management and production control. We do not find the requirements of DO-178B to be excessive or cumbersome; however, we do often find the FAA certification process to be unacceptably slow and unresponsive.

Table A1. Concluded.

Yes. Most, if not all, of the steps outlined in DO-178B are necessary for safety reasons. The problem we faced was the learning curve. On numerous occasions we were 'off the mark' as to what was being asked for. There is some ambiguity when reading the text and associated tables, and there is little guidance material. Many times we found ourselves wondering “What are they getting at?” To properly prepare a document, it is beneficial to understand the topic in the spirit in which it was written. We found too much emphasis on the conformance of the design and requirements documents to the associated standards. We performed far too many iterations addressing whether the documents were formatted correctly. The pertinent questions regarding conformance to standards should be related solely to safety, not style. Perhaps this is self-inflicted, as a result of poorly conceived standards, but these standards were themselves reviewed and iterated several times by both the FAA and an independent verification group.
Yes, provide appropriate system safety engineering at inception of design and make this part of certification process.
Emphasize stringent functional/performance testing, software reliability testing. Do it right the first time to minimize the need for repeated re-certifications. Integrate safety and software processes.
The structural coverage analysis is required on target code for software level A (of par. 6.4.4.2 of DO 178B). An analysis should be done to confirm the opportunity of performing this activity on source code.
Yes. We use the same version of a software module for multiple similar products. When we have a problem report on that code, we must retest it in all the products that use that software. This is required by section 11.3.h. We feel that we should be able to reference the problem report and testing performed on the same software in previously certified products without repeating this effort for each product that uses this software module. We feel the requirements of section 11.10 concerning the documentation of the Design Description are excessive, especially for very small projects, or software projects where the development is based on a previously developed and documented software platform. We also feel that Level C should not require statement coverage. We feel requirements based test coverage is sufficient for Level C software to provide an acceptable level of safety/quality/reliability.
Yes there are several ways that costs can be reduced and schedules maintained. Some ways to reduce the cost and schedule of the software life cycle are: a) Use of automated tools to reduce each phase (specification, design, code, test) of the life cycle process. b) Design software to be reusable. By use of object oriented design and making code database driven when possible. c) Successful use of metrics to estimate present and future systems. d) Develop better software safety and risk assessment methods.
The document itself could be modernized and written in a more “user-friendly” manner. It should not take a DO-178 “expert” to implement; this reduces the safety improvement impact due to diminished understanding and thus diminished implementation of 178 processes and practices. It also adds to the amount of cost in dollars and schedule to reach a clear understanding and implementation plan. During system concept development phases, software is often prototyped to demonstrate concepts. Methods to address previously developed prototyped should be added to incorporate the flexibility inherent in software development while maintaining safe processes.
Better guidance to the interpretation and implementation of DO-178B is strongly needed. A set of reference designs or industry best practice documents would be a great tool towards this goal. The FAA should accept more electronic data rather than its reliance on paper. The FAA needs more staff at the ACO to keep the backlog down and have a proper turn time on submittals. This is especially the case when the ACO is out of the office for extended periods of time with no one else to continue their work in their absence. In an effort to reduce certification time without sacrificing safety, the ACO should rely more on an independent review of software submittals by an approved Software DER. Currently, the ACO re-reviews and audits the software submittals already accepted by an approved DER.
Based on the criticality level of developed software, there seems to be no identifiable magnitude of software specified. A small effort (measured in LOC or executable byte size) is expected to be document the same as a large effort.
There are 2 prime areas that are candidates for cost/schedule impact reduction. The first is use of CASE tools to automatically generate certified software. The second is to determine how much safety is gained by using DO-178B Level A, instead of Level B.

Table A2. What is the impact of DO-178B on your organization and process?

We spend a great deal of time making sure our subcontractors adhere to DO-178B. We review much of their documentation even though it will go to the FAA for review prior to TSO or TC. We are duplicating what the FAA should do and has little personpower or capability to do.
Our products are all DO-178B certified since software is extensively used in digital audio system as well as SSCVER and SELLAL Systems.
Generally, the impact is good. It is a reliable way to verify that our software is well tested and documented. However, too much of a good thing can also be bad. The certification process needs flexibility based on the product being produced. [company statement deleted]. A small group of individuals write, test, and implement the software. In our case, we could effectively govern our software activity with half the documents. Extensive manpower in engineering, marketing, and secretarial is required to update documents and process change for even minor changes.
If implemented without planning and coordination or finding it may be a major impact to current developments that are not compliant with.
DO-178B does not add significantly to our software development costs. We would need to assure ourselves that software meets a level of safety appropriate to its intended function even if there were no DO-178B, In fact, having an accepted tool to apply for this purpose probably reduces our development costs. DO-178B is not a 'test" document, but one that applies to the entire software development and configuration processes. Without accepted guidance, we would have to develop our own methods of assuring ourselves as well as certification authorities, that the software provides an appropriate safety level. We have had significant cost and schedule impact associated with compliance finding in spite of having our own Software DERs. Significant improvement can be made in this area. Please refer to the body of this letter
We have two main product lines, each with approximately the same sales potential. Every project in one line must conform to DO-178B. Some projects in the other line may require DO-178B. Every DO-178B project is burdened with at least a nine month lead time to delivery. We turned a non-DO-178B project from inception to delivery in 5 1/2 months, counting hardware, software and manufacturing times. We believe it will be cost-effective to hire additional employees to perform the Independent Verifications in-house. In the first project, we spent about 20% of the total project cost in contracting this service out.
If the input safety analysis is inappropriate, it will cost excessive money.
It is better than DO-178B for software acquisition management.
DO-178A described software development in terms of objectives, offering industry the possibility to present its own solution in order to meet these objectives. DO 178B is much more directive, making it difficult to present its own means of compliance, in accordance with its company methodology and progress plan.
We feel that other that the issues mentioned above, the requirements of DO-178B provide an acceptable guideline for software development.
[Our] systems that require deliverable software are presently using DO-178B as a guideline for the development of this software. The software life cycle process in place is tailored to address all areas that DO-178B covers. The impact is a large amount of certification paper work required to show compliance with DO-178B.
DO-178B has had a positive impact. It forces rigorous processes and constant improvements to the processes.
DO-178B has forced a documentation requirement on our engineering (SW) design group. It is an attempt at structured design - yet can be worked around. The design engineers are often not the ones require to produce the documents.
There are many benefits to a standard such as DO-178B. It forces discipline in all areas of software development that result in a safer product. It has been a good tool for us to enforce safety and quality in the engine control software that we procure. On the other hand, this type of software development in very expensive and it makes it difficult for smaller, innovative companies to get in to the business of developing safety-critical avionics software.

Table A3. What has been imposed on you due to DO-178B that you think has no value added?

We don't allow our suppliers to use COTS unless it is previously certified because it is our experience that the certification process as presently invoked by DO-178B is too costly unless software is designed from the start with the meeting of DO-178B goals as an objective. It is not obvious to me that level "B" and level "A" requirements add the cost equivalent of safety/quality to the product. This is particularly true of the independence requirements.
Re-certification to DO-178B when equipment was DO-178A (Level D)
The compliance matrices are valuable tools for integrating the software document into a cohesive interrelated package. However, reducing the size and number of these matrices would benefit both the FAA and the software developing companies. The fact that all changes are considered major changes (with very few exceptions) and need fall certification approval. All software changes are not major and a simpler certification change process would reduce unnecessary work for both parties. Approve from the beginning of program the appropriate software level per DO-178B definitions without pushing for higher than required levels for months or years.
Nothing this far.
Nothing. There is an inverse relationship and disproportionate amount of value added by higher levels of structural analysis. Structural analysis adds significant cost and yields marginal benefits. Most of the unnecessary expenses we associate with software certification are not because of the requirements of DO-178B. They are due to the FAA certification processes.
There was far too much focus and discussion on how a document should be presented so that it would pass an audit. I am unsure of the value of some of the code requirements such as having no dead code or unused variables. I would maintain that unused variables are not detrimental if it does not cause your processor to run out of memory to declare them. (The memory map is checked for this condition). Likewise, if you can prove that code is truly unreachable, it should also be deemed safe. These two restrictions affect our ability to have common routines between different Configuration Items when only small differences in functionality are apparent. In this case you must completely test two very-similar modules, which is arguably redundant.
True - when DO-178B is applied to an open system, it is inappropriately applied.
The biggest impact is certifying to Level A. We believe there is little benefit to Level A versus Level B. The key differences between Level A and Level B are: a) Verifying object code that is not directly traceable to source code (section 6.4.4.2.a) b) Independence for verifying software architecture and partitioning (Table A-4) c) Independence for verifying source code complies with architecture and is "accurate and consistent" (Table A-5) d) Independence for verifying object code is robust with low-level requirements (Table A-6) e) Independence for verifying test results (Table A-7). Many of the independence requirements are not necessary since the software testing is assurance that the previous software processes were performed correctly. Level B also requires a disciplined and independent QA organization which will handle any concerns that the software developers might be coerced into releasing software that is not safe (i.e. due to budget and schedule constraints). The only other issue is low level software testing. DO-178B Section 6.4.4.2.b requires software structural coverage. The two differences in the requirements for Level A and Level B are that Level A requires "each condition in a decision takes on every possible outcome at least once" and "each condition is shown to independently affect the decision outcome". These two additional criteria are essentially testing the compiler. In my experience, there has not been one defect found by this testing. The reliability of compilers (especially Ada) has become much better in the last 5 years. Because of the amount of time to perform this work, and the very limited benefit, this is one area that could be reduced or eliminated. This type of testing should be done by the compiler vendor. One suggestion is to have the FAA maintain a list of compilers that can not be used for safety critical applications. This list could be made accessible to all applicants via electronic media.
Quality of software suffers when the software level in C or below. Long-term acquisition cost is increased.

Table A3. Concluded

Verification of outputs of software coding process should be covered by testing of outputs of software integration process. For example, source code complies with low-level requirements is covered by executable object code complies with low-level requirements, while low level test activity, and specific source code aspects like source code conforms to standards should be covered with a source code sample covering all coders and all languages.
None.
The position by some that it more than a guideline and must be followed to the letter. This causes a lot of excess generation of information to be redundantly placed in many documents.
Nothing.
If 178B were not in affect, I'm afraid no structured approach would even be considered. The importance of the structured approach is not clearly enforced or appreciated.

Table A4. Do you think that DO-178B implementation enhances the safety/quality/reliability of the product? How?

I believe that adhering to an effective (i.e. it produces the desired result) process is necessary to produce a safe and quality product. Software is always reliable and exhibits only unreliable behavior when executed on unreliable hardware. We should perhaps make sure that the hardware is always reliable, i.e. enough memory and processing power to start with and environmentally sound (DO-160 now). DO- 178B provides guidance to an effective process, it is not the only process. DO- 178A must have been good enough for a while since aircraft certified under that spec are still flying. The MIL-STDs produced effective software processes as there are many aircraft produced under MlL-STD-1679 and DOD-STD-2167A that are still flying.
Yes, it's providing ourselves visibility and the assurance that software is properly tested and supported during development.
Based on the success of our software in the field today, I would have to agree that the implementation of DO-178B enhances the safety, quality, and reliability of our products. Once we have completed the certification process there are very few changes. The changes that are made are implemented for performance purposes and not safety issues. The testing methodology and implementation is valid.
Not necessarily. You can follow the whole process and not get enhancements or proof of better safety, quality or reliability.
In general, yes. It causes us to be more thorough than we might have been otherwise.
It is appropriate for reliability and quality. It is not directly appropriate to system safety.
Levels A, B software enhances software quality. Adequately performed system hazard analysis and subsequent PSSA enhances safety. DO-178B lacks emphasis on reliability testing; software reliability suffers under DO-178B.
Yes. By requiring consistent design, coding, documentation and record keeping.
Yes, the DO-178B guidelines helps to define and steer the development of a software product through a software life cycle process. It provides a good emphasis on requiring the traceability of requirements through each phase of the software process.
The discipline and thoroughness required by DO-178B definitely can increase reliability and quality. DO-178B used in conjunction with methods and architectural considerations of ARP-4754 and ARP-4761 can definitely increase system safety.
The 178B approach (philosophy) provides for definable, explainable, code. Review cycles (when seriously conducted) allow errors to be found, ideas to be communicated, abstractions to be discussed. Requirement definition narrows the target, but forcing requirements to be written when its not clear how to is fruitless.

Table A4. Concluded

Yes - absolutely. A structured process of requirement-driven development with an emphasis on verification and validation as well as quality assurance and configuration management is essential. DO-178B provides an accepted guideline for accomplishing its objectives. There are probably other guidelines which may also be acceptable in order to be able to provide the appropriate assurances; however, if they are equivalent, and they are applied, it should not be difficult to show that the objectives of DO-178B have been met. DO-178B is somewhat unique in that it is objective oriented not process oriented. You can use other guidelines or standards and still meet the objectives of D0-178b. I have evaluated software developed to ML-STD-2167 for DO-178B compliance. While the MIL-STD does not allow for different levels of software, and I would not go so far as to say that all software developed in accordance with the MIL-STD also meets all DO-178B objectives, it was not difficult in this case to determine that the software did in fact meet DO-178B objectives for level C software. DO-178B is a very good guideline and, we believe it would be difficult to replace it and still provide the same level of safety with anything that is more "streamlined." It is undoubtedly possible to replace it with other guidance material which provides for an equivalent level of safety, but it is difficult to see where any reduction in burden could be obtained from such an activity.
Yes. The activities and objectives of DO-178B are ones that require proper systems and software design processes that leads to better safety, reliability, and quality of the software product.
Yes, DO-178B implementation does improve safety. It forces small and start-up companies to take a methodical approach to software development and testing. It requires a financial and engineering commitment to the testing and safety of the software products.

Table A5. Have you had any experiences with certification authorities that have resulted in added cost and scheduling with no value-added? If so, what are they?

There have been instances cited to me though I have not been party to them where things were redone just to take credit for getting them done under the FAA reviewing eye that added no value and caused delays/schedule problems. This usually only happens once. Once is enough.
When equipment has been installed for aircraft for years (before DO-178A being in force). For new release of DO-178C...D...E, closely verify that previously qualifying any certifying equipment should not re-qualify.
Long delays in the program because of insufficient man power at the FAA. Specifically, because only one person is responsible for software related issues. The implementation of PSAC by the FAA is ambiguous and from our experience leads to years in delays. The clear cut manner in which hardware requirements and hardware verification documents are approved should be used as an example of how to implement the aspects of software certification. Not approving the proper software level per the DO-178B definitions.
Not applicable.
Yes, see the body of this letter. Compliance finding and re-use of previously evaluated software add the highest cost and unnecessary schedule delays.
Yes. I believe I've detailed these in 1) and 3).
Yes - WAAS
No. On the other hand, the certification authorities are not strong enough in enforcing DO-178B guidance. Sometimes, they are not consistent in application of DO-178B guidance (differences among certification authorities-some branch and across branches.)
No.
It would be helpful for the same certification authority, when possible, be involved with a given project from beginning to end. This would allow for a more concurrent software product process to take place between the certification authority and vendor.
Yes. There are significant differences in the understanding of software and systems design from ACO region to region. Not all ACOs are equal when it comes to rigor in analysis and fairness in judgment. What is rejected in one region is acceptable in another. There are significant differences in backlog from ACO to ACO resulting in much greater than 30 day responses to submittals.
Often updates are required to documentation. This paper work causes delay in receiving TSO approval and hefty document publishing time and materials. Some “updates” are typographical in nature, others add clarification. If a document could be approved with updates to follow - or by magnetic media publication it would help.
Yes. We are currently preparing a package for the Joint Aviation Authority (JAA) for an engine that was recently certified for the FAA. Preparation of additional documentation for the JAA software certification will take about 200 hours. There are no additional software tests or analysis in this effort, so the product will be identical. These hours are strictly for creating reports. Better coordination of the certification authority regulations would eliminate this unnecessary expense.

Table A6. What other issues do you have with the certification process that adds to cost and delays in the schedule?

There is inconsistency in FAA offices in the interpretation of DO-178B. There is a definite lack of software experience in the FAA on a national basis. The FAA has a few good people but like the marines they need more. Not being able to get answers on a local level adds to schedule and cost.
Re-qualification when new standards are in force.
We deal with several certification offices. However only one office knows the detailed aspects of our products. Long delays and struggles between ACOs could be eliminated by allowing the company more control over which ACO has approval authority. Presently all our software product approvals are delegated to one office but only after delays,
It seems that is a box checking and auditing activity that for ground systems would have to be modified to ensure proactive-participation to minimize delays.
See the body of this letter. Use of DERs for full compliance findings both for STC and TSO projects and/or facility/developer certification to self certify software to safety-driven levels would provide significant benefit with no reduction in safety.
I am confused with the role, or lack thereof, of Designated Engineering Representatives (DERs) in the certification efforts of Ground-based units. I understand they have jurisdiction in air-borne units. We have to follow the same rules and guidelines as air-borne equipment manufacturers. We have a DER under contract in an advisory role. We have experienced conflicts between the views expressed by our auditors with those expressed by the DER. I would have suspected their views to have been more aligned.
It is only appropriate for a white box on a commercial aircraft.
When certification authorities are not able to provide guidance with respect to COTS. (Why is DOS or Windows not acceptable for critical systems? what are the alternatives?, etc.) and tools qualification (Why do we need the tools qualified to the same level as the SW?) It's never done in practice any way.
The use of tools enhances the safety/quality/reliability of the embedded software, but the cost and delay of tool qualification are too high. The requirements on tools (of par. 12.2 of DO 17813) are at the same level as the requirements for generated code. It should not be. Some low-level verifications and/or tests should be suppressed, and a structural coverage analysis should be performed on the source code.
Getting feedback and responses of TSO deviations can take a long time, especially if they must be sent to Washington.
The level of testing of the software product in some instances should be reduced to a higher level such as functional testing. The added time to accomplish formal low level testing in some instances provides no greater degree of safety/quality/reliability.
None.
[Our] development of [our product] and coordination with certification authorities dates back to 1991, however, it was not until 1996 that a definitive requirement to demonstrate system safety to Level B was understood. At this point the [our product's] architecture was re-vamped to use 2 dissimilar processors running 2 dissimilar operating systems. One of the two sides of the system would also have to have software developed to Level B per DO-178B. All of these steps are necessary and are resulting in a system that is easily verified to be safe. Ground based software systems had been certified previously using other means. Knowledge and understanding of these requirements and processes sooner would have been enormous help to [us]. For the future, a clear path through the certification process for ground-based systems needs to be established. Allowance for evolving methods and practices also needs to be addressed so that newer, better methodologies can be incorporated to increase safety.
Review of the documentation by certification authorities often takes 60-90 days. (well in excess of the published 30 day cycle. The Planning documents that we have submitted are not reviewed and approved which seems like a waste of time.

Table A6. Concluded

As a safety professional with two FAA programs running, I can see a basic problem with the safety rationale used in starting the process. If this rationale could be fixed, a lot of the perceived problems with this document could be eliminated. Taken at face value, the DO-178B process requires software to be developed at a much higher level than intended. Developers wind up coming up with fixes or simplifying assumptions to resolve the disconnect. This practice appears to be "cheating" and will normally raise objections by safety professionals. The key issue is actually in the definitions used in sections 2.1.1 and 2.2.1. When compared with MIL-STD-882, considered best practice in the conventional system safety community, "failure condition" is actually a "hazard". "Failure condition" is a poor choice of wording because it implies a failure, when in fact no failure need occur. Reliability is the discipline where failures are the only cause considered. There is no doubt that this terminology has in itself limited some safety analyses to only consider failures. To complicate things, failure condition category is actually a hazard severity. Hazard severity is actually of little significance until combined with probability. I can imagine an event that could cause massive damage to my system and personnel (thermonuclear war), but rarely is it relevant because the probability of my system causing it is so small as to be non credible. Yet in D)-178B, the probability of software is never considered. Therefore software contributing to an aircraft collision should be level A. The method chosen to overcome this usually involves dropping the severity (failure condition category) down to a reasonable level. So aircraft collision due to this cause is actually only a minor event. This is not only technically wrong, and misleading, it also leads to bad decisions after the fact when software is maintained and not re analyzed. "It is only a minor hazard so we can afford to lose the control." This thinking is incompatible with MIL-STD-882 and will be very hard to explain in court, where we all wind up after the crash. The only valid solution is to rewrite the front end to make it compatible with best practice, and assign "credit" in terms of hazard likelihood reduction or probability for each level of software process. The unwillingness to do that tells me that it is the consensus of the authors that this does not really mitigate hazards.
Our counterparts in the Aircraft Certification Office are involved in many projects with several other applicants. Sometimes it takes months to get them to review and approve submitted material. I don't believe this is the fault of the individuals, but the workload in the office. The quantity of avionics systems has grown tremendously in the last few years and this is probably straining the FAA resources in this area. Some suggested solutions might be to give more authority to the DERs, shift resources with in the FAA (from other specialties), or increase the size of the FAA staff performing these functions.

Table A7. List alternatives to DO-178B that you think can be used without sacrificing safety/reliability/quality.

Mil-Std-498 would be acceptable. CMM level 2 would probably be all right. Certain RAD approaches would be acceptable. Results with performance and requirements traceability are what we need, there are many paths that will produce what we want. We need to be open minded enough to accept there is more than one way.
None. I think DO-l78B can be used efficiently with the comments listed above.
Risk Analysis - FAA order, Safety Assessments - FAA order
None that would also reduce software development or certification cost.
I believe the largest factor that would save us time without sacrificing safety/reliability/quality would be to develop tools that would maintain a database of requirements to code to testing techniques. Of course, the initial cash outlay to create or purchase such tools may be prohibitive. It would be an asset to be able to modify, say, a Low Level Requirement in one place, and have the traceability to the High Level Requirements, the System Requirements as well as to the code and test procedures be updated automatically.
Classic System Safety Engineering!
We don't know of any alternatives.
DO-178B provides sufficient guidelines to address many aspects of a given software life cycle process. However, there needs to be ways to reduce the amount of paperwork for a given certification. The concept of reusable code should lend itself to reusable documentation. As automated tools for requirements, design, code and testing become more prevalent they will need to be addressed more fully in DO178B in such a way as to encourage the use of such tools. As for alternatives to the DO-178B, any means that can be devised to show that the software product is safe, reliable and a quality product should be considered.
Other software development standards exist, but as an industry consensus, the members of RTCA SC-190 have stated that DO-178B is not broken and should stand. The issues with DO-178B are those of interpretation and implementation of the processes and objectives that it calls out. Guidance, training, and communication are the keys to improving the software certification process, particularly between the ACO and the manufacturer.
On line templates pre-structured for document writing and generation.
Use of CASE tools to generate and test software has great potential to reduce the cost of certifying software. There is a class of CASE tools which allow engineers to develop controls based on graphical modeling techniques. These tools offer the following advantages: a) Reduce translation errors. The typical software process has a system engineer specifying the system software requirements in a requirements document. The software system engineer must then manually translate the system requirements into software requirements. DO-178B does not detail the verification of this process. With CASE tools and automatic code generation, the manual translation source of errors is eliminated. b) Allow verification of system requirements and high level software requirements- The software life cycle in DO-178B starts with the high level software requirements definition. There is no process currently required to verify the system satisfies the operational needs and that the high level software requirements meet the system requirements. These CASE tools allow a system to be modeled and executed so the system requirements can be tested. The control portion of the model is the implementation of the high software. This can also be executed with test cases to verify the high level software requirements It also gives an environment to verify. c) Automatic code generation to reduce manual coding errors- These tools allow source code to be generated directly from the tested control model. Since the automatic code generation is a repeatable process, the verified control model can be automatically translated to source code. This step eliminates the software design and software coding process and integration processes (DO-178B sections 5.2, 5.3, and 5.4). While DO-178B does have a mechanism to qualify a software development tool, there are many other areas of DO-178B that would have to be addressed. a) Section 5.3. software coding process and the related verification activities would be reduced or eliminated. b) After tool qualification, would model diagram structural coverage be sufficient or would source (object) structural coverage still be required?

Appendix B

SSAC Workshop Attendees

Table B1 contains the list of attendees at the SSAC Industry Workshop.

Table B1. Workshop Attendees

Michael Allocco	TRW
Patty Andrews	Rockwell Collins, Inc.
Lorna Atienza	Innovative Solutions International (ISI)
Chris Baum	Air Line Pilots Association
Dave Bedrosian	Avidyne Corporation
John Besnard	Raytheon
Tevis Boulware	Computers and Concept
Alan Caine	Allison Engine Company (Rolls-Royce)
Ross Cairns	Interstate Electronics Corporation
Cesar Cantos	Dukes, Inc
Lewis Center	Innovative Solutions International, Inc.
George Chang	Air Economics Group, Inc.
Gary Church	Aviation Management Associates, Inc.
John Coleman	Hamilton Standard
Roger Cooley	FAA AIT-5
Bonnie Danner	TRW/SETA
Joseph Dauksys	Aerospace Industries Association
Dale Davidson	Honeywell, Inc.
Carl DeBruine	BFGoodrich Avionics Systems, Inc.
Ulrich Dembinski	D&F Gesellschaft fur Daten-Systeme mbH
Nancy Depoy	TRW/SETA
Mike DeWalt	FAA ANM-106N
George Donohue	FAA ARA-1
Cheryl Dorsey	Digital Flight
Brian Eckmann	Universal Avionics Systems
R Evans	Pratt & Whitney Canada
Thomas Fancy	Gulfstream Aerospace Corp.
Thomas Ferrell	Boeing Commercial Airplane Group
Paul Fiduccia	Small Aircraft Manufacturers Association
Wayne Findley	FAA
Dan Fisher	Advance Navigation and Positioning Corporation
Jack Foidl	TRW
Ken Foote	AvroTec, Inc.
Dan Fredrick	Lockheed Martin Federal Systems
Steven Friedman	PMEI
John Fritts	AlliedSignal
Russell Furstnau	Allison Engine Company
Terry Gallien	Trimble NA
Charlotte Gauss	Science Applications International Corporation
Jerome Gelover	Systems Resources Corporation
Tanae Gilmore	TRW/SETA
Mars Gralia	Johns Hopkins University, Applied Physics Laboratory
Brett Gundlach	BF Goodrich Avionics Systems
Jim Hand	Interstate Electronics Corporation
Kelly Hayhurst	NASA Langley Research Center
Marla Herns	TRW/SETA

Table B1. Continued

Michael Holloway	NASA Langley Research Center
Alfred Hughes	FAA AFS-350
Bob Jackson	Raytheon Systems Company
Jack Janelle	Honeywell Air Transport Systems
Leland Johnson	Raytheon Aircraft
Bradley Jones	TRW Avionics Systems Division
Koos Keizer	Universal Avionics
John Kerr	Smith's Industries
Randy Key	FAA AOS-240
John Knight	University of Virginia, Department of Computer Science
Jay Lad	de Havilland Inc (Bombardier Aerospace)
Robert Laws	FAA ASU-250
Nancy Leveson	MIT, Aeronautics/Astronautics Dept. University of Washington, Computer Science & Eng. Dept.
Pat Loh	Innovative Solutions International, Inc.
Howard Lowe	Smiths Industries Aerospace, CS-UK
Dave Lubkowski	MITRE/CAASD
Archie Maclellan	Honeywell, Inc.
Frank McCormick	Certification Services, Inc
Janell McKay	Lockheed Martin Air Traffic Management
James Meer	Digital Equipment Corporation
Scott Millar	ARINC
Arun Murthi	Strategic Technology Institute, Inc.
Armen Nahapetian	Teledyne Controls
Prasad Nair	Project Management Enterprises, Inc.
David Oelschlaeger	Honeywell, Inc., Honeywell CAS-SPO
Terry Pearsall	Aircraft Electronics Association
Joel Petersen	FAA AND-730
Gerald Pilj	Lear Jet
Carmine Primeggia	FAA ASD-100
Arthur Pyster	FAA AIT-5
Long Quach	TRW/SETA
Brian Quillen	Unison Industries
Rene Ramos	Gables Engineering
Leanna Rierson	FAA AIR-130
Ronald Roseman	Lucas Aerospace
Tom Roth	AlliedSignal
Rudolph Ruana	Jeppesen Sanderson, Inc.
Arthur Salomon	FAA ASD-130
Peter Saraceni	FAA William J. Hughes Technical Center, AAR-421
Uma Satyen	MITRE / CAASD
Leslie Schad	Boeing Commercial Airplane Group
Bill Schultz	General Aviation Manufacturers Association
Michael Severson	Bell Helicopter Textron, Inc.
Roger Shultz	Rockwell Collins, Inc.
Louis Silva	Smiths Industries - CSM
Steve Silver	Litton Aero Products
Arnold Smith	TRW/SETA
Henry Smith	ARINC
Steve Smith	FAA ASY-300
Marge Sonnek	Honeywell, Inc.
Robin Sova	FAA ACE-111
Brenda Spielman	Avionics Specialties, Inc.

Table B1. Concluded

Craig Stallwitz	Raytheon Aircraft Company
Thomas Starnes	Cessna Aircraft Company
Corey Stephens	Air Line Pilots Association
Joseph Stoddart	Lockheed Martin
Ron Stroup	FAA ASW-170
Perry Stufflebeam	Raytheon Aircraft Company
Abdul Tahir	Aviso Inc.
Charles Tamburo	Teledyne Controls
Laurie Thompson	Honeywell Air Transport Systems
Earl Thorndyke	Interstate Electronics
Tom Tougas	Airsys ATM, Inc
Greg Turgeon	Williams International
Shannon Uplinger	Uplinger Translation Services
Dennis Wallace	Rockwell Collins, Inc.
Stephen Ward	Rockwell Collins, Inc.
Elroy Wiens	Cessna Aircraft Company
Theresa Wolfrom	ARINC
Mary Gayle Wright	L-3 Communications Aviationics
Henry Wykoff	Airline Pilots Association
Jeff Yang	Mitre
Andrew Yip	Penny & Giles Aerospace, Inc.
Philip Zeilinger	Allied Signal Engines
Kenneth Zemrowski	TRW

Appendix C
Issues with Mapping to Classification Scheme

Table C1 lists all of the issues recorded during the SSAC Industry Workshop. The ID number represents the identification number of each comments in the workshop database. The last column in the table maps each comment to the classification scheme given in Appendix D.

Table C1. Workshop Issues

ID	Comment/Issue	Mapped
1	On particular project, FAA elevated criticality level at the last minute, despite the applicant having an approved cert plan. This was not a one time event. Also, personnel changes within FAA have resulted in changed requirements. Essentially, agreements made between applicants and FAA are not always honored by the FAA. There is significant variation between regions, also.	1.1.1
2	Lack of common understanding between applicants and FAA	1.1.1 & 1.2.1
3	FAA resources and abilities are not always adequate. This is particularly true for response time from FAA. Even stated minimum response times are too long, and they are rarely met. (This overlaps with another)	1.1.2 & 1.1.3
4	ACOs responsible for software often can't use judgment, because they don't have enough knowledge, so they rely on super-conservative approach to compliance. They hide behind a checklist.	1.1.3
5	Currently, complete plans are required for the derivatives, even if they are only barely different from previous products. There is little value in producing the plan for the derivative.	2.1.1
6	Differences between offices about what they want to see.	1.1.1
7	To what extent should accident statistics guide the allocation of resources in certification? Perhaps too much concentration has been given to software.	2.2.4
8	Approvals take too long to obtain. There is wasted effort in current approval process.	1.1.2
9	Having difficult time determining who in the FAA approves ground systems, and getting different answers. Most common answer is to do the most expensive thing possible.	2.1.10
10	Supplier is held to higher level criticality requirements by the customer than by the FAA.	1.2.2
11	System engineering process is immature compared to the software engineering process.	1.2.1
12	Agreement between applicant and regulator as to what constitutes adequate level of partitioning.	2.1.4
13	FAA ACO engineers who speak English as a second language	1.1.2
14	Definition of independence varies, and sometimes independence is required when DO-178B does not require it.	1.1.1 & 2.1.5
15	Independence required by ACO without sufficient justification	2.2.2
16	How much traceability is required, and how is it documented? (for example, is a matrix required, or are other methods acceptable?)	2.1.3
17	structural coverage (group expects that SC-190 will handle this issue, but thinks its important)	2.1.5
18	In areas of interpretation difficulty, much time is spent in negotiating with regulators	1.1.1
19	Fear of failure to comply causes companies to take super-conservative approach to compliance.	1.2.1
20	Regulators buy time by asking irrelevant questions and requiring response from applicant, while stopping all review activities until after they receive the response.	1.1.2
21	Serial approval process is required by some ACOs: approval of TSO required before company can begin STC process	1.1.6
22	Reciprocal agreements with other cert authorities are not working as well as they did in the past.	1.1.7
23	Even after approval of PSAC, there are different interpretations about what additional documents must be inspected by the FAA	1.1.1 & 2.1.1
24	Is compliance to DO-178B an issue?	1.2.1
25	Tests on target require a conformed unit when the production unit is identical	2.1.5

Table C1. Continued

26	For lower levels of software, there are different interpretations about the extent to which testing has to be done on the target	2.1.5
27	Different interpretations of the applicability of coverage analysis techniques to different stages of verification	2.1.5
28	Much confusion caused by the distinction between high and low level requirements	2.1.3
29	Inadequate emphasis on the software contribution to system hazards	2.2.4
30	COTS (SC-190 has subgroup looking at this issue)	2.1.7
31	Lack of prescription in DO17B of the packaging for the verification data permits ACOs to impose additional requirements on the format	2.1.8
32	No requirements on test requirements for flight test software or for software for other types of tests	2.1.5
33	Confusion about CC1s and CC2s. Description in CM section is difficult to understand	2.1.2
34	Due to the costs involved with the publication of written (paper) documentation, can consideration be given to "on-line" magnetic media, creation, update, and submittal of documents. Options are available for standardized word processing, E-mail, web site documentation. If the FAA would accept a media form of this material it would save time and development cost, as well as submittal and review approval.	2.1.1
35	Lack of consistency between different offices about tool qualification. Interpretation of what it means to be qualified differs widely. Interpretation of what tools must be qualified differs widely	2.1.6
36	Lots of documents required to be generated by ACOs	2.1.1
37	Traceability is an important technology for software development. What techniques are acceptable to the FAA?	2.1.3
38	Individual ACO specialists impose requirements beyond that required by DO178B	1.1.3
39	paragraph 9.4 is confusing	2.1.1
40	Lack of understanding at the beginning of a program result in large increased downstream costs. This also occurs if a rapid prototyping model is invoked. (lack of predictability)	2.1.2
41	The definitions for (software/system and any other terms) safety, safety assessments, reliability, quality, certification, costs, etc are not defined well enough to provide consistent review and completion criteria. Nor is the relationship between them defined. If we don't have good definitions we cannot know when we achieved them.	2.2.4
42	The definition of best practices should be codified into an extension of existing regulatory guidance.	2.2.1
43	The regulatory requirements result in expensive reverse engineering costs as a result of inadequate understanding of DO-178B/ED-12B	2.2.1
44	There is major misunderstanding of the intent behind the tool qualification requirements in DO-178B/ED-12B. In many cases more stringent requirements are imposed than intended or the requirements are misapplied to inappropriate items.	2.1.6
45	Upgrading between any software level is very expensive as currently required in DO-178B/ED-12B without being able to take credit for work already done.	2.1.9
46	The qualification of software tools is difficult to move between different certification projects. There is no way to publish and take credit for certification of tools (e.g. MS visual c++, forth, etc.) This implies that there should be a list of pre-qualified tools and other types of software.	2.1.6
47	The reuse of certification data is extremely difficult.	2.1.8
48	Incremental development or any modern and innovative process is not supported in DO-178B/ED-12B.	2.2.3
49	Is there a way to reduce the extensive documentation requirements (e.g. more reliance on the integrity of the developers) and subsequent extensive regulatory review.	2.2.2
50	Is there a way to take more credit for service history and or non-developed software (e.g. COTS) as a means of relief from some of the requirements in DO-178B/ED-12B.	2.1.9
51	DO-178B/ED-12B fails to provide clear direction on regression analysis resulting in inconsistent application of the standard possibly causing unnecessary costs.	2.1.5
52	DO-178B/ED-12B requirements to show that a tool works but no requirement on the human performance results in a bias against the use of tools.	2.1.6

Table C1. Continued

53	DO-178B/ED-12B was developed for level A but does not offer sufficient relief for lower levels.	2.1.8
54	Imposition of regulatory requirements that do not provide Customer value/benefits commensurate with the costs .	2.2.1
55	The requirements for structural coverage are onerous and result in unnecessary effort.	2.1.5
56	Explore the benefit of using risk based analysis similar to military and NASA programs.	2.2.4
57	Extract only the important elements to concentrate on.	2.2.1
58	One of the major software development costs has been requirement changes resulting in rework changes. DO-178B/ED-12B exacerbates this issue due to the stringent requirements for documentation that may not be done otherwise.	1.2.3 & 2.2.2
59	A single source of calibration/education for the certification process needs to be identified so all ACOs and developers know where to go/send people for the correct interpretation.	1.1.1
60	Certification authorities are generally (except for a few key individuals) incompetent in dealing with safety of flight issues. This includes software.	1.1.3
61	Certification authorities seem to be largely ignorant of software issues (i.e. system engineers who deal with software). ACOs tend to make excessive requirements/overly conservative to cover inadequacy.	1.1.3
62	DO-178B/ED-12B and the system safety assessment process need to pay specific attention to non-airborne systems.	2.1.10
63	FAA allows JAA to dominate in joint airworthiness findings (intellectual domination)	1.1.7
64	FAA software specialists tend to know nothing about systems and safety issues. (There are some exceptions). Knowledge of systems engineering and system management are apparently foreign to this industry but applied in others.	1.1.3
65	FAA unwillingness to agree in writing to a comprehensive listing of remaining work to be done to completion and a schedule. Incremental requirements that continue to change as the certification progresses.	1.1.2
66	FAA unwillingness to allow DER final approval as defined and allowed by their own orders.	1.1.4
67	Government officials tend not to understand their professional responsibilities and liabilities.	1.1.3
68	Government people tend to be influence by politics. Special requirements are generated that result in overkill	1.1.3
69	Level of rigor applied in granting DER authority varies widely and in fact this variability undermines the system.	1.1.4
70	Prefer that FAA software specialist have had software development experience	1.1.3
71	Prefer that software DERs have had software development experience	1.1.4
72	Qualification for systems and software related work is not formalized in the same sense as other engineering fields. (this not a certification authority (e.g. regulatory) specific issue)	1.1.3 & 1.2.1
73	Software safety assessment is not required/supported by DO-178B/ED-12B	2.2.4
74	The audit process is not well documented. There are different audit philosophies and they are auditing for the wrong things. Q: How many safety defects are found by the audit process?	1.1.5
75	There is no grievance or appeal process	1.1.5
76	There is no primary education source for the certification process.	1.1.3 & 1.2.1
77	Excessive delays in Certification Authorities response to submission of applicants documents.	1.1.2
78	Tie in to DO-178B/ED-12B and the PMA (parts manufacturing authority) process has been a problem.	1.1.6
79	Tie in to DO-178B/ED-12B and the TSOA (Technical Standard Order Authorization) process has been a problem.	1.1.6
80	The same product and same processes taken to 2 different ACOs result in significantly different costs (e.g. excessive) to get approval. Lack of mutually/universally understood definitions also results in not knowing what to do based on definition differences between different documents. This also relates to different interpretations between ACOs (e.g. different assignment of safety levels).	1.1.1
81	Forcing the use of DO-178B/ED-12B on systems originally developed to DO-178A is intrusive and expensive especially when there is extensive service experience. (There was some concern that this implies that DO-178A and DO-178B/ED-12B provide equivalent levels of assurance.)	2.1.9

Table C1. Continued

82	Legacy systems for example back to DO-178A, 2167A etc. might provide real opportunities for streamlining by trying to take credit for service experience and the fact that changes are relatively small/incremental. This is more applicable for level B and C systems as opposed to Level A systems.	2.1.9
83	Alternative methods are not up to date with current software development methods. A means to easily/generically accommodate advances in technology without specifically including the technology in the document. DO-178B/ED-12B forces the applicant to address the objectives directly which may not be applicable for a given technology or the base intent of the objective.	2.2.3
84	Customizing documents specifically for presentation to the FAA is very costly when the original (e.g. redlined documents) is the basis for internal company approval and acceptance.	2.1.1
85	ACSEP (Aircraft Certification Suppliers Evaluation program) audit need better criteria for production acceptance software.	1.1.5
86	Documentation DO-178B/ED-12B does not address modern documentation tool systems. The Certification Authority will require hard copy documents and not accept access to the automatic document system. This is exacerbated by the 8110.3 requirements for approval of documents.	2.1.1
87	The Certification Authorities are requiring the wrong documents (e.g. propose use of software safety analysis, or other appropriate documentation).	2.2.4
88	Some ACOs requires documents beyond the requirements of DO-178B/ED-12B.	2.1.8
89	The final documentation should be ultimately related to the safety requirements/assessment.	2.2.4
90	Design systems properly so that safety critical software is isolated from non-safety critical software which limits the application of more stringent requirements to a much smaller component.	2.1.4
91	Review the documentation requirements to ensure that they provide value added attributes for both the regulatory authorities and the developers.	2.2.2
92	Delegation to the organization instead of on a product basis could contribute to reducing costs considerably.	2.2.1
93	What is the percentage of overall cost due strictly to certification over and above what good practices would dictate (e.g. cost of structural coverage documentation). Caller 1 see no decrease Caller 2 would see improvement in legacy systems in excess of 50% Caller 3 Qualification of tools and non developed software (e.g. COTS) add about 90% increase of tool qualification which translates into about 5%?? of overall certification. Caller 4 FAA only contributes 10% of documentation costs probably less for overall costs. Caller 5 Due to ability to use non developed software (e.g. COTS) a savings of 30% might be realized. One example was OSI stacks $20k off the shelf vs %500K for uniquely developed. Caller 6 Might see additional innovation using other types of development processes which might provide productivity gains. (e.g. domain analysis, safety directed development, different reuse techniques) The actual cost benefit is difficult to quantify. Caller 7 If left to own devices might save 25-30% Caller 8 Distributed application would be done in 1/4 to 1/5 the cost if DO-178B/ED-12B were not applied. Caller 9 The majority of the cost saved may not be due to DO-178B/ED-12B requirements but may be due to the interaction with the certification authorities. Caller 10 The release of the existing completion criteria (e.g. structural coverage) could result in 25% reduction in overall certification of software based systems. Caller 11 On a given system dramatic amounts of money (50% or greater) by using alternate means of compliance is being realized	2.2.1
94	Would a uniform understanding of DO-178B/ED-12B within a given developers organization produce a lower cost of development. Caller 1 NO for a given company but true for all companies. Caller 2 Yes within a large company Caller 3 For the TSO system the driver is the certification authority driving the non-uniformity.	1.2.1
95	The testing/verification costs can run between 50-60% of the total cost of development. It is unclear how much of this would go away without the requirements of DO-178B/ED-12B but is obviously a great driver.	2.1.5

Table C1. Continued

96	No way to evaluate that a company is capable of doing DO-178B/ED-12B prior to release of contract resulting in retraining of suppliers delaying schedule and increasing costs. Even though the contractor may be found capable by other measures (e.g. SEI CMM, ISO 9000, etc.)	2.2.1
97	DO-178B/ED-12B does not clearly define the difference between development and verification tools and the requisite requirements.	2.1.6
98	DO-178B/ED-12B requirements applied to compiler issues results in extensive no value added. During audit government position is you are guilty until proven innocent. Excessive demand for proof of compliance. Much easier if documentation demands are clarified up front. A proof is required (independent authority) that documents provided by manufacturers matches requirements of standard.	2.1.6
99	Does Level A SW buy you more safety than level B, C, D? (Difference for level A: structural coverage, independence,). Does 178B add safety? (Lack of clearness on safety process and interplay with SW process)	2.2.4
100	Is there a way to move from an absolute safety std to a relative std to evaluate safety? What is level of safety now? (ex: GenAv aircraft with older equipment safer than newer equipment at a lower safety level?)	2.2.4
101	Is there a need to submit data on very minor software changes? (Difference between TSO and TC/STC/ATC)	2.1.8
102	Is there any other alternative besides SDD that is allowed outside of DO-178B? Are there alternatives to 178B that have been accepted? How would an alternate method be evaluated?	2.2.3
103	Why do some ACOs not permit alternate means to DO-178B? (What if we could provide data regarding alternate methods to show that they are more effective?) Redundant	2.2.3
104	What plans does FAA have to monitor and regulate consistency between ACOs in compliance findings? And educating their people to be consistent?	1.1.1
105	Is there consistency among ACOs? (already a definite answer: NO) Redundant.	1.1.1
106	Is 178B a good standard? (The best but is costly to manufacture/use)	2.2.1
107	Is there a consistent understanding to the DO-178B objectives? (No -- within and outside of the FAA)	1.1.3 & 1.2.1
108	Is there info available from military applications regarding SW incidents?	2.2.4
109	Why is there a wide variance in sw approval between TC, STC, TSO? How can the processes be made more similar? How can the playing field be leveled? (Inconsistencies between ACOs--different ways of doing TSO among ACOs) (DERs used in some ACOs and not others)(TC/STC/ATC Installations causing TSO pkg to be re-opened due to ACOs examination)	1.1.6
110	How is previously developed SW approved when transitioning from 178A to 178B? What kind of credit can be taken from the 178A work. (Reference issue paper, CAST paper, SC-190 work)	2.1.9
111	When will FAA make formal attempt to harmonize with foreign agencies? (1 cert vs. 28 certs?)	1.1.7
112	How is SW certified when used in conjunction with non-certified SW. (example: use of previously developed SW--COTS operating system).	2.1.7
113	Have we thought of an appeals process outside of the FAA that could be used to resolve SW issues with the cert process? What is the appropriate way to deal with an ACO engineer who will not provide certification approval, because he/she feels there is a SW problem that is unacceptable? (What is the procedure to deal with an issue when the applicant and ACO do not agree?)	1.1.5
114	When doing end-to-end, how do you look at avionics with respect to ground systems (ex: WAAS and datalink)? Answer: Being handled by SC-190	2.1.10
115	Are there any possibilities of expanding DER authorities? (to allow quicker turn around). New DER mgt process in work -- ODAR	1.1.4
116	How to avoid re-analysis when integrating TSO products as part of the TC, STC, ATC product? (Appears that ACO approving TCs do not trust other ACOs approving TSO). Redundant	1.1.6
117	How much confidence should be placed on assessment of previously used tools for support of developing software? (ex: qualified verification tools). Specify re-use of a previously qualified tool--different for verification vs. development tool.	2.1.6
118	Why couldn't SEI maturity level be used an alternate means?	2.2.1

Table C1. Continued

119	How does the FAA deal with changing technology? How do we keep the cert process up to date with changing technology?	2.2.3
120	What is "good enough" testing? (Related to previous comment--testing req changes as technology advances)	2.2.2
121	What is good enough requirements analysis? (Sys engr issue). Missing element in 178B.	2.2.2
122	Lack of requirements validation?	2.2.2
123	Poor requirements is a cost driver.	1.2.3
124	Lack of emphasis in certification on an integrated systems view, seeing software as an integral component	2.2.4
125	Teaching SW cert requirements to affected people (at any level).	1.1.5
126	Level of people's understanding of good SW developing practice/DO-178B	1.2.1
127	Inappropriate methods levied by DERs/FAA/other cert authorities to meet 178B	1.1.3
128	Rote reliance by the reg agencies on a metric w/o regard to value.	1.1.3
129	Waiting for FAA approval/lack of reliance on DERs	1.1.2 & 1.1.4
130	Continual change in interpretation of guidance	1.1.1
131	Excessively wide interpretation of what constitutes a safety requirement. Too many things are treated as safety issues that are not safety issues.	1.1.1 & 2.2.4
132	Lack of industry experience or/and naivete within the regulators	1.1.3
133	A practice requiring 3 ACO reviews for SW, regardless of derivative cert effort or not.	1.1.1
134	Inappropriate level of experience in reg agencies due to lack pay. (high turnover). Retraining ACO personnel every few years.	1.1.3
135	Continuous push on part of FAA to upgrade the SW criticality assessment, especially on previously certified products.	2.1.9
136	Excessively wide interpretation of the term "with independence"	1.1.1 & 2.1.5
137	Minor requirements changes affect documentation and certification.	1.2.3
138	Pre-maturity (of documents, sys req, sw req, etc) is a cost driver. Also, pre-maturity of people. (14 yr exp; 2.5 mill lines of code)	1.2.1
139	Excessively wide interpretation of the need for tool qualification. (i.e., tool qualification) Interpretation of tool qualification need.	1.1.1 & 2.1.6
140	Conformity process. (First article conformity is costly; re-testing due to sw changes (HW qual, etc); regression testing issues as sw changes;	2.1.5
141	Waiting for FAA approval. Slow response.	1.1.2
142	Maintaining traceability to code level	2.2.2
143	As tech changes, a standard can never be 100% correct.	2.2.3
144	Greatest cost driver is poor requirements.	1.2.3
145	Formal methods are a cost driver for foreign agency certification (CAA).	1.1.7 & 2.2.3
146	Static analysis and structural coverage are cost drivers, due to training, few tools available.	2.2.2
147	Lack of tool use data and industry experience available - no forum for it; no network for information	2.1.6
148	There is some feeling that some methods may be helpful but there is no data available or may be proprietary, i.e., formal methods. It may not have standardized metrics. They may require a special study. Will there be uniform standards for both military and civil applications?	1.2.2 & 2.2.3
149	Can an industry-wide group exist to do data gathering on new topics? Issues include exposing dirty linen, so data needs to be kept without company/person/system association. Using an industry association between the FAA and the companies involved, such as AIA and GAMA, will be necessary. This should include military data. Non-disclosure agreements may be necessary. Independent studies may be necessary. The data to be collected needs to be defined, including parameters, constraints, process definitions which generated the data.	1.2.2
150	Issues relating to compliance: reverse engineering required to comply to 178B, particularly for existing systems.	2.1.9
151	variance between DERs/regulatory agencies on a given subject	1.1.1

Table C1. Continued

152	there is no technically current and correct definition for completeness for independence, data flow and control flow coupling and MCDC	2.1.5
153	low level of understanding of safety assessment/analysis/techniques within the FAA; lack of expertise in the FAA of software and electrical knowledge - this has required an excessive amount of data to be developed and reviewed;	1.1.3
154	lack of open communication between the FAA and the DER(s).	1.1.4
155	Qualified tools on previous projects, used in the same way are required to be re-qualified.	2.1.6
156	Guidance on transition (exit) criteria needs to be better defined in DO-178B so it is not black-and-white and allows for more flexibility. As a result, developers do not necessarily comply with transition criteria they define.	2.1.2
157	Transition criteria forces developers to focus on process rather than products and does this focus on process, versus product, effect safety.	2.2.1
158	Lack of good requirements definition impacts the cost of verification. Is the guidance in DO-178B sufficient and consistent to help the developer?	1.2.3 & 2.1.3
159	Parallel, or shadow, processes. One to develop the product, the second to satisfy certification objectives.	2.2.1
160	Same product, different customers causes a repetition of activities	2.1.8
161	Interpretation of compliance activities is different between applicant and certification authority and how long it takes issues to be resolved.	1.1.1
162	No credit given for prototyping of requirements. (i.e., modeling before development)	2.2.3
163	Additional informal validation/verification activities used to decrease required DO-178B verification activities renders formal review less effective. Are the additional activities accomplished to achieve quality or to "patch" inadequate DO-178B guidance?	2.2.2
164	Relative effectiveness of SQA and SCM representatives during all the activities and it is possible to meet all SQA and SCM DO-178B objectives without producing a quality product.	2.2.2
165	Alternative methods scrutinized extensively or are rejected by ACO. As a result, more efficient designs, activities, tools cannot be used for product development or significant re-engineering needs to be done. DO-178B specifies that alternative methods can be used as long as the objectives are met, but in practice it is not feasible.	2.2.3
166	Experience of developer in getting process credit is not taken into account. Competence of developer is given no consideration when certifying the product.	2.2.1
167	Turnover of certification authority personnel causes constant reiteration of negotiating process.	1.1.2
168	DO-178B does not allow for qualification of process once versus product each time.	2.2.1
169	Imperative to develop a set of guidelines to establish how COTS can and will be certified.	2.1.7
170	Cost of data generation is too high and ACOs should be more receptive to using electronic media.	2.1.1
171	No direct feedback mechanism for cost effectiveness path coverage analysis.	2.1.5
172	Need periodic, timely feedback from FAA on what is acceptable, and/or recommended practice.	1.1.2
173	DO-178B is a "what" and not a "how" standard, and experienced developers are able to understand the level of effort required. However, DO-178B does not provide sufficient information for the new applicant to scope their level of effort.	2.1.2
174	Consider that some of the tracking (e.g., Traceability Matrix and coverage analysis) should be a function of size the job, develop environment, and the number of programmers as well as criticality level.	2.2.2
175	It seems that the "data coupling" objective must be satisfied via test cases whereas analysis should suffice to achieve the data coupling objective.	2.1.5
176	The difficulty of qualifying a production tool so that credit can be taken for its use. The tool must now be created at the same level as the code it produces. This intuitively seems to be overkill, but no alternative has been found that all (FAA & Industry) can agree to. Difficulty in qualifying a production tool (e.g., code generator).	2.1.6
177	Approve and audit the manufacturer's software process rather than individual product submittals.	2.2.1
178	ACO availability does not coincide with submittals and can cause significant delays.	1.1.2
179	Inconsistent interpretation by FAA certification authority may be a problem.	1.1.1

Table C1. Continued

180	FAA software audits are inconsistent between reviewers. Reviews can be insightful, or not, depending on the experience of the evaluators.	1.1.1
181	Lack of consistency between ACOs, DERs, and different regions.	1.1.1
182	FAA should accept DER's input and accepted without further review for areas that have been delegated to the DER.	1.1.4
183	Interpretation of DO-178B may be a challenge for fast-track implementation and shouldn't a sound development methodology should suffice?	2.2.1
184	Concern that different organizations in FAA may not be in agreement.	1.1.1
185	What level of verification for COTS components is required (software and hardware)?	2.2.3
186	"Implied requirements" on either side can cause delay and DO-178B guidance should address how implied requirements that affect safety should be addressed.	2.1.3
187	DERs ask for more that what is necessary which causes increased workload and implementation of new processes.	1.1.4
188	Requirements for documentation, data, and verification testing are daunting. DO-178B and DO-160D impose more stringent requirements for tests, processes and internal visibility	2.2.2
189	Certification process can be ad hoc, subjective and repetitive. There needs to be consistent application, and expectations established up front.	1.1.1
190	Level of knowledge among ACOs is not uniform. Systems being proposed for implementation, potential interactions with existing systems, effects of system changes on ATC environment, and latest H/W & S/W design and testing methodologies.	1.1.3
191	Maximum constraints imposed when in doubt. Developers over-produce to ensure passage.	1.1.3
192	There is a lack of central repository for availability of the checklist used by the FAA, issue papers, policy letters. Etc.	1.1.5
193	Companies spend a great amount of resources researching which tools to use.	1.2.2
194	What credit can a developer receive for using alternative means, architecture, and safety monitoring versus what is commonly accepted (current TSO says apply for deviations). How criticality is assign and flows to software is an issue.	2.2.3
195	Partitioning integrity, what types of techniques are acceptable and what are the criteria to accept a partitioning strategy?	2.1.4
196	How can the applicant obtain credit for reuse of "shrink-wrapped" code for legacy systems previously certified, for so called "derivative systems"	2.1.9
197	Reciprocal agreements with JAA are not a common as they used to be.	1.1.7
198	Issue of "when" the life cycle data and qualification data are due, and when the FAA certification authority approvals are due. For example, the PSAC is useless if not submitted or approved earlier enough to be effective.	2.1.1
199	Issue of how to certify human-computer interface software to be compliant with DO-178B. As a result, cost, schedule, and safety may be impacted. This may be difficult to get air and ground community to agree.	2.1.10
200	Better use of DERs and get them involved earlier in the architecture design as opposed to current practice or later in the process in a review role.	1.1.4
201	Current certification process may not adequately address today's hardware and software architecture. In addition, obsolete parts cannot be replaced and companies cannot take advantage of new technology	2.2.3
202	DO-178B does not provide adequate guidance for migrating legacy programs being used. A legacy may not have done its certification to meet DO-178B objectives, but still may be a safe system.	2.1.9
203	Right now the only difference between levels A and B is structural coverage. This is not safety assurance. Hence what is the relative benefit of each of the objectives in terms of safety.	2.1.5
204	There is a lack of consistency in level of regression testing required, particularly in changes made late in the program.	2.1.5
205	The objective of certifying software is safety. DO-178B does not specifically address safety. Unless we assume all the safety areas are covered by systems and all software has to do is replicate the system correctly. The end software product design needs to be checked for safety.	2.2.4
206	Some ACOs do not really accept a alternative means of compliance that deviate from DO-178B.	2.2.3

Table C1. Concluded

207	DO-178B notes that high level test provides best indication of system performance, but then DO-178B asks for increased structural coverage as the measure of level A. [Focusing on structures tends to "pervert" the focus away from system performance oriented tests toward code structure rather than requirements.	2.1.5
208	Objectives in Annex tables are not all objectives--some are specific means of compliance MCDC), so an alternative means of compliance are not feasible as specified in Chapter 12.	2.1.5 & 2.2.3
209	The basis of DO-178B is quality-by-process. The goal of certification is safety of the public is flight. Does process rigor effectively address safety.	2.2.1
210	DO-178B is back loaded with most certification credit from testing. I'd have to say the building safety into design is better than trying to test it in, but software designs do not have to be built or reviewed for safety.	2.2.4
211	Records required for FAA audits can be excessive. ACOs interpretation of DO-178B varies so a company rarely uses a single process, thus process become project or ACO specific.	2.1.8
212	Certification of multiple applications in modular software and hardware architectures. Including mixtures of criticality and function, isolation of applications, system performance, considerations, data fusion issues, etc. Fault protection and failure recovery mechanisms and incremental certification of new applications. There is no guidance on how to certify systems that incremental systems and systems that will run on multiple platforms will be handled.	2.2.3
213	Use of COTS software and operating systems.	2.1.7
214	Applicability of airborne system certification standards to ground-based systems. Issues relating to relative scale of systems, testing, etc.	2.1.10
215	End-to-end certification of ground and airborne software. Need to protect and recover from syntactical and logical errors. As a result, the scope of standards and guidance need to expand to cover the end-to-end system, including the communication pathways.	2.1.10

Appendix D

Classification Scheme with List of Issues

All of the issues and comments recorded by the four groups during the workshop are assigned to one or more categories in the classification scheme below. The number in front of each individual comment is its identification number in the database of workshop issues. Issues identified in the questionnaire responses that were not already in the database of workshop issues were included in the classification scheme. The issues identified from the survey are designated as "from survey".

1. Issues that are not specific to DO-178B

1.1 Issues within the FAA

1.1.1 Inconsistencies exist among ACOs in interpreting and following policy and guidance.

- 1 On particular project, FAA elevated criticality level at the last minute, despite the applicant having an approved cert plan. This was not a one time event. Also, personnel changes within FAA have resulted in changed requirements. Essentially, agreements made between applicants and FAA are not always honored by the FAA. There is significant variation between regions, also.
- 2 (see also 1.2.1) Lack of common understanding between applicants and FAA
- 6 Differences between offices about what they want to see.
- 14 (see also 2.1.5) Definition of independence varies, and sometimes independence is required when DO-178B does not require it.
- 18 In areas of interpretation difficulty, much time is spent in negotiating with regulators
- 23 (see also 2.1.1) Even after approval of PSAC, there are different interpretations about what additional documents must be inspected by the FAA
- 59 A single source of calibration/education for the certification process needs to be identified so all ACOs and developers know where to go/send people for the correct interpretation.
- 80 The same product and same processes taken to 2 different ACOs result in significantly different costs (e.g. excessive) to get approval. Lack of mutually/universally understood definitions also results in not knowing what to do based on definition differences between different documents. This also relates to different interpretations between ACOs (e.g. different assignment of safety levels).
- 104 What plans does FAA have to monitor and regulate consistency between ACOs in compliance findings? And educating their people to be consistent?
- 105 Is there consistency among ACOs? (already a definite answer: NO) Redundant.
- 130 Continual change in interpretation of guidance
- 131 (see also 2.2.4) Excessively wide interpretation of what constitutes a safety requirement. Too many things are treated as safety issues that are not safety issues.
- 133 A practice requiring 3 ACOs reviews for SW, regardless of derivative cert effort or not.
- 136 (see also 2.1.5) Excessively wide interpretation of the term "with independence"
- 139 (see also 2.1.6) Excessively wide interpretation of the need for tool qualification. (i.e., tool qualification) Interpretation of tool qualification needed.
- 151 variance between DERs/regulatory agencies on a given subject
- 161 Interpretation of compliance activities is different between applicant and certification authority and how long it takes issues to be resolved.
- 179 Inconsistent interpretation by FAA certification authority may be a problem.
- 180 FAA software audits are inconsistent between reviewers. Reviews can be insightful, or not, depending on the experience of the evaluators.
- 181 Lack of consistency between ACOs, DERs, and different regions.
- 184 Concern that different organizations in FAA may not be in agreement.

- 189 Certification process can be ad hoc, subjective and repetitive. There needs to be consistent application, and expectations established up front.
- (from survey) There are significant differences in the understanding of software and systems design from ACO region to region. Not all ACOs are equal when it comes to rigor in analysis and fairness in judgment. What is rejected in one region is acceptable in another.

1.1.2 ACOs do not provide quick, meaningful responses to applicants.

- 3 (see also 1.1.3) FAA resources and abilities are not always adequate. This is particularly true for response time from FAA. Even stated minimum response times are too long, and they are rarely met. (This overlaps with another)
- 8 Approvals take too long to obtain. There is wasted effort in current approval process.
- 13 FAA ACO engineers who speak English as a second language
- 20 Regulators buy time by asking irrelevant questions and requiring response from applicant, while stopping all review activities until after they receive the response.
- 65 FAA unwillingness to agree in writing to a comprehensive listing of remaining work to be done to completion and a schedule. Incremental requirements that continue to change as the certification progresses
- 77 Excessive delays in Certification Authorities response to submission of applicants documents.
- 129 (see also 1.1.4) Waiting for FAA approval/lack of reliance on DERs
- 141 Waiting for FAA approval. Slow response.
- 167 Turnover of certification authority personnel causes constant reiteration of negotiating process.
- 172 Need periodic, timely feedback from FAA on what is acceptable, and/or recommended practice
- 178 ACOs availability does not coincide with submittals and can cause significant delays.
- (from survey) There have been instances cited to me though I have not been party to them where things were redone just to take credit for getting them done under the FAA reviewing eye that added no value and caused delays/schedule problems.
- (from survey) The implementation of PSAC by the FAA is ambiguous and from our experience leads to years in delays.

1.1.3 Insufficient knowledge of software engineering and related disciplines exists within the FAA.

- 4 ACOs responsible for software often can't use judgment, because they don't have enough knowledge, so they rely on super-conservative approach to compliance. They hide behind a checklist.
- 3 (see also 1.1.2) FAA resources and abilities are not always adequate. This is particularly true for response time from FAA. Even stated minimum response times are too long, and they are rarely met. (This overlaps with another)
- 38 Individual ACOs specialists impose requirements beyond that required by DO178B
- 60 Certification authorities are generally (except for a few key individuals) incompetent in dealing with safety of flight issues. This is includes software.
- 61 Certification authorities seem to be largely ignorant of software issues (i.e. system engineers who deal with software). ACOs tend to make excessive requirements/overly conservative to cover inadequacy.
- 64 FAA software specialists tend to know nothing about systems and safety issues. (There are some exceptions). Knowledge of systems engineering and system management are apparently foreign to this industry but applied in others.
- 67 Government officials tend not to understand their professional responsibilities and liabilities.
- 68 Government people tend to be influence by politics. Special requirements are generated that result in overkill
- 70 Prefer that FAA software specialist have had software development experience

- 72 (see also 1.2.1) Qualification for systems and software related work is not formalized in the same sense as other engineering fields. (this not a certification authority (e.g. regulatory) specific issue)
- 76 (see also 1.2.1) There is no primary education source for the certification process.
- 107 (see also 1.2.1) Is there a consistent understanding to the DO-178B objectives? (No -- within and outside of the FAA)
- 127 Inappropriate methods levied by DERs/FAA/other cert authorities to meet 178B
- 128 Rote reliance by the reg agencies on a metric w/o regard to value.
- 132 Lack of industry experience or/and naivete within the regulators
- 134 Inappropriate level of experience in reg agencies due to lack pay. (high turnover). Retraining ACOs personnel every few years.
- 153 low level of understanding of safety assessment/analysis/techniques within the FAA; lack of expertise in the FAA of software and electrical knowledge - this has required an excessive amount of data to be developed and reviewed;
- 190 Level of knowledge among ACOs is not uniform. Systems being proposed for implementation, potential interactions with existing systems, effects of system changes on ATC environment, and latest H/W & S/W design and testing methodologies.
- 191 Maximum constraints imposed when in doubt. Developers over-produce to ensure passage.

1.1.4 Inadequacies, inconsistencies, and inefficiencies exist in the DER system.

- 66 FAA unwillingness to allow DER final approval as defined and allowed by their own orders.
- 69 Level of rigor applied in granting DER authority varies widely and in fact this variability undermines the system.
- 71 Prefer that software DERs have had software development experience
- 115 Are there any possibilities of expanding DER authorities? (to allow quicker turn around). New DER mgt process in work - ODAR
- 129 (see also 1.1.2) Waiting for FAA approval/lack of reliance on DERs
- 154 lack of open communication between the FAA and the DER(s).
- 182 FAA should accept DER’s input and accepted without further review for areas that have been delegated to the DER.
- 187 DERs ask for more that what is necessary which causes increased workload and implementation of new processes.
- 200 Better use of DERs and get them involved earlier in the architecture design as opposed to current practice or later in the process in a review role.
- (from survey) We have had significant cost and schedule impact associated with compliance finding in spite of having our own Software DERs. Significant improvement can be made in this area.
- (from survey) I am confused with the role, or lack thereof, of Designated Engineering Representatives (DERs) in the certification efforts of Ground-based units. I understand they have jurisdiction in air-borne units. We have to follow the same rules and guidelines as air-borne equipment manufacturers.

1.1.5 Insufficient information is available about the certification process.

- 74 The audit process is not well documented. There are different audit philosophies and they are auditing for the wrong things. Q: How many safety defects are found by the audit process?
- 75 There is no grievance or appeal process
- 85 ACSEP (Aircraft Certification Suppliers Evaluation program) audit need better criteria for production acceptance software.

- 113 Have we thought of an appeals process outside of the FAA that could be used to resolve SW issues with the cert process? What is the appropriate way to deal with an ACOs engineer who will not provide certification approval, because he/she feels there is a SW problem that is unacceptable? (What is the procedure to deal with an issue when the applicant and ACOs do not agree?)
- 125 Teaching SW cert requirements to affected people (at any level).
- 192 There is a lack of central repository for availability of the checklist used by the FAA, issue papers, policy letters. Etc.

1.1.6 Problems exist within the TSO, TC, STC, ATC, and PMA processes.

- 21 Serial approval process is required by some ACOs: approval of TSO required before company can begin STC process
- 78 Tie in to DO-178B/ED-12B and the PMA (parts manufacturing authority) process has been a problem.
- 79 Tie in to DO-178B/ED-12B and the TSOA (Technical Standard Order Authorization) process has been a problem.
- 109 Why is there a wide variance in sw approval between TC, STC, TSO? How can the processes be made more similar? How can the playing field be leveled? (Inconsistencies between ACOs--different ways of doing TSO among ACOs) (DERs used in some ACOs and not others)(TC/STC/ATC Installations causing TSO pkg to be re-opened due to ACOs examination)
- 116 How to avoid re-analysis when integrating TSO products as part of the TC, STC, ATC product? (Appears that ACOs approving TCs do not trust other ACOs approving TSO). Redundant
- (from survey) Getting feedback and responses of TSO deviations can take a long time, especially if they must be sent to Washington.

1.1.7 Working with non-U. S. certification authorities is difficult.

- 22 Reciprocal agreements with other cert authorities are not working as well as they did in the past.
- 63 FAA allows JAA to dominate in joint airworthiness findings (intellectual domination)
- 111 When will FAA make formal attempt to harmonize with foreign agencies? (1 cert vs. 28 certs?)
- 145 (see also 2.2.3) Formal methods are a cost driver for foreign agency certification (CAA).
- 197 Reciprocal agreements with JAA are not as common as they used to be.
- (from survey) We are currently preparing a package for the Joint Aviation Authority (JAA) for an engine that was recently certified for the FAA. Preparation of additional documentation for the JAA software certification will take about 200 hours. There are no additional software tests or analysis in this effort, so the product will be identical. These hours are strictly for creating reports. Better coordination of the certification authority regulations would eliminate this unnecessary expense.

1.2 Issues within Industry

1.2.1 Insufficient knowledge of software engineering and related disciplines exists within industry.

- 2 (see also 1.1.1) Lack of common understanding between applicants and FAA
- 11 System engineering process is immature compared to the software engineering process.
- 19 Fear of failure to comply causes companies to take super-conservative approach to compliance.
- 24 Is compliance with DO-178B an issue?
- 72 (see also 1.1.3) Qualification for systems and software related work is not formalized in the same sense as other engineering fields. (this not a certification authority (e.g. regulatory) specific issue)
- 76 (see also 1.1.3) There is no primary education source for the certification process.

- 94 Would a uniform understanding of DO-178B/ED-12B within a given developers organization produce a lower cost of development. Caller 1 NO for a given company but true for all companies. Caller 2 Yes within a large company Caller 3 For the TSO system the driver is the certification authority driving the non-uniformity.
- 107 (see also 1.1.3) Is there a consistent understanding to the DO-178B objectives? (No -- within and outside of the FAA)
- 126 Level of people's understanding of good SW developing practice/DO-178B
- 138 Pre-maturity (of documents, sys req, sw req, etc) is a cost driver. Also, pre-maturity of people. (14 yr exp; 2.5 mill lines of code)

1.2.2 Lack of cooperation among companies increases costs.

- 10 Supplier is held to higher level criticality requirements by the customer than by the FAA.
- 148 (see also 2.2.3) There is some feeling that some methods may be helpful but there is no data available or may be proprietary, i.e., formal methods. It may not have standardized metrics. They may require a special study. Will there be uniform standards for both military and civil applications?
- 149 Can an industry-wide group exist to do data gathering on new topics? Issues include exposing dirty linen, so data needs to be kept without company/person/system association. Using an industry association between the FAA and the companies involved, such as AIA and GAMA, will be necessary. This should include military data. Non-disclosure agreements may be necessary. Independent studies may be necessary. The data to be collected needs to be defined, including parameters, constraints, process definitions which generated the data.
- 193 Companies spend a great amount of resources researching which tools to use.

1.2.3 Requirements definition is difficult independent of certification.

- 58 (see also 2.2.2) One of the major software development costs has been requirement changes resulting in rework changes. DO-178B/ED-12B exacerbates this issue due to the stringent requirements for documentation that may not be done otherwise.
- 123 Poor requirements is a cost driver.
- 137 Minor requirements changes affect documentation and certification.
- 144 Greatest cost driver is poor requirements.
- 158 (see also 2.1.3) Lack of good requirements definition impacts the cost of verification. Is the guidance in DO-178B sufficient and consistent to help the developer?

2. Issues specific to DO-178B

2.1 Issues about the adequacy of guidance in DO-178B

2.1.1 DO-178B has inadequate and ambiguous guidance for documentation.

- 5 Currently, complete plans are required for the derivatives, even if they are only barely different from previous products. There is little value in producing the plan for the derivative.
- 23 (see also 1.1.1) Even after approval of PSAC, there are different interpretations about what additional documents must be inspected by the FAA
- 34 Due to the costs involved with the publication of written (paper) documentation, can consideration be given to "on-line" magnetic media, creation, update, and submittal of documents. Options are available for standardized word processing, E-mail, web site documentation. If the FAA would accept a media form of this material it would save time and development cost, as well as submittal and review approval.
- 36 Lots of documents required to be generated by ACOs
- 39 paragraph 9.4 is confusing
- 84 Customizing documents specifically for presentation to the FAA is very costly when the original (e.g. redlined documents) is the basis for internal company approval and acceptance.

- 86 Documentation DO-178B/ED-12B does not address modern documentation tool systems. The Certification Authority will require hard copy documents and not accept access to the automatic document system. This is exacerbated by the 8110.3 requirements for approval of documents.
- 170 Cost of data generation is too high and ACOs should be more receptive to using electronic media.
- 198 Issue of "when" the life cycle data and qualification data are due, and when the FAA certification authority approvals are due. For example, the PSAC is useless if not submitted or approved earlier enough to be effective.
- (from survey) Eliminate the redundancies inherent in the software verification documents.
- (from survey) We found too much emphasis on the conformance of the design and requirements documents to the associated standards. We performed far too many iterations addressing whether the documents were formatted correctly. The pertinent questions regarding conformance to standards should be related solely to safety, not style.
- (from survey) We feel the requirements of section 11.10 concerning the documentation of the Design Description are excessive, especially for very small projects, or software projects where the development is based on a previously developed and documented software platform.

2.1.2 DO-178B has inadequate and ambiguous guidance for planning and configuration management.

- 33 Confusion about CC1s and CC2s Description in CM section is difficult to understand
- 40 Lack of understanding at the beginning of a program result in large increased downstream costs. This also occurs if a rapid prototyping model is invoked. (lack of predictability)
- 156 Guidance on transition (exit) criteria needs to be better defined in DO-178B so it is not black-and-white and allows for more flexibility. As a result, developers do not necessarily comply with transition criteria they define.
- 173 DO-178B is a "what" and not a "how" standard, and experienced developer are able to understand the level of effort required. However, DO-178B does not provide sufficient information for the new applicant to scope their level of effort.
- (from survey) There is some ambiguity when reading the text and associated tables, and there is little guidance material. Many times we found ourselves wondering “What are they getting at?”
- (from survey) The document itself could be modernized and written in a more “user-friendly” manner. It should not take a DO-178 “expert” to implement; this reduces the safety improvement impact due to diminished understanding and thus diminished implementation of 178 processes and practices. It also adds to the amount of cost in dollars and schedule to reach a clear understanding and implementation plan.
- (from survey) Better guidance to the interpretation and implementation of DO-178B is strongly needed. A set of reference designs or industry best practice documents would be a great tool towards this goal.

2.1.3 DO-178B has inadequate and ambiguous guidance for requirements definition and analysis.

- 16 How much traceability is required, and how is it documented? (for example, is a matrix required, or are other methods acceptable?)
- 28 Much confusion caused by the distinction between high and low level requirements
- 158 (see also 1.2.3) Lack of good requirements definition impacts the cost of verification. Is the guidance in DO-178B sufficient and consistent to help the developer?
- 186 "Implied requirements" on either side can cause delay and DO-178B guidance should address how implied requirements that affect safety should be addressed.

2.1.4 DO-178B has inadequate and ambiguous guidance for partitioning.

- 12 Agreement between applicant and regulator as to what constitutes adequate level of partitioning.
- 90 Design systems properly so that safety critical software is isolated from non-safety critical software which limits the application of more stringent requirements to a much smaller component.
- 195 Partitioning integrity, what types of techniques are acceptable and what are the criteria to accept a partitioning strategy?

2.1.5 DO-178B has inadequate and ambiguous guidance for verification activities.

- 17 structural coverage (group expects that SC-190 will handle this issue, but thinks its important)
- 14 (see also 1.1.1) Definition of independence varies, and sometimes independence is required when DO-178B does not require it.
- 25 Tests on target require a conformed unit when the production unit is identical
- 26 For lower levels of software, there are different interpretations about the extent to which testing has to be done on the target
- 27 Different interpretations of the applicability of coverage analysis techniques to different stages of verification
- 32 No requirements on test requirements for flight test software or for software for other types of tests
- 51 DO-178B/ED-12B fails to provide clear direction on regression analysis resulting in inconsistent application of the standard possibly causing unnecessary costs.
- 55 The requirements for structural coverage are onerous and result in unnecessary effort.
- 136 (see also 1.1.1) Excessively wide interpretation of the term "with independence"
- 140 Conformity process. (First article conformity is costly; re-testing due to sw changes (HW qual, etc); regression testing issues as sw changes
- 95 The testing/verification costs can run between 50-60% of the total cost of development. It is unclear how much of this would go away without the requirements of DO-178B/ED-12B but is obviously a great driver.
- 152 there is no technically current and correct definition for completeness for independence, data flow and control flow coupling and MCDC
- 171 No direct feedback mechanism for cost effectiveness path coverage analysis.
- 175 It seems that the "data coupling" objective must be satisfied via test cases whereas analysis should suffice to achieve this the data coupling objective
- 203 Right now the only difference between levels A and B is structural coverage. This is not safety assurance. Hence what is the relative benefit of each of the objectives in terms of safety.
- 204 There is a lack of consistency in level of regression testing required, particularly in changes made late in the program.
- 207 DO-178B notes that high level test provides best indication of system performance, but then DO-178B asks for increased structural coverage as the measure of level A. [Focusing on structures tends to "pervert" the focus away from system performance oriented tests toward code structure rather than requirements.
- 208 (see also 2.2.3) Objectives in Annex tables are not all objectives--some are specific means of compliance MCDC), so an alternative means of compliance are not feasible as specified in Chapter 12.
- (from survey) DO-178B lacks emphasis on reliability testing; software reliability suffers under DO-178B.

2.1.6 DO-178B has inadequate and ambiguous guidance for tool qualification.

- 35 Lack of consistency between different offices about tool qualification Interpretation of what it means to be qualified differs widely Interpretation of what tools must be qualified differs widely

- 44 There is major misunderstanding of the intent behind the tool qualification requirements in DO-178B/ED-12B. In many cases more stringent requirements are imposed than intended or the requirements are misapplied to inappropriate items.
- 46 The qualification of software tools is difficult to move between different certification projects. There is no way to publish and take credit for certification of tools (e.g. MS visual c++, forth, etc.) This implies that there should be a list of pre-qualified tools and other types of software.
- 52 DO-178B/ED-12B requirements to show that a tool works but no requirement on the human performance results in a bias against the use of tools.
- 97 DO-178B/ED-12B does not clearly define the difference between development and verification tools and the requisite requirements.
- 98 DO-178B/ED-12B requirements applied to compiler issues results in extensive no value added. During audit government position Is you are guilty until proven innocent. Excessive demand for proof of compliance. Much easier if documentation demands are clarified up front. A proof is required (independent authority) that documents provided by manufacturers matches requirements of standard.
- 117 How much confidence should be placed on assessment of previously used tools for support of developing software? (ex: qualified verification tools). Specify re-use of a previously qualified tool--different for verification vs. development tool.
- 139 (see also 1.1.1) Excessively wide interpretation of the need for tool qualification. (i.e., tool qualification) Interpretation of tool qualification needed.
- 147 Lack of tool use data and industry experience available - no forum for it; no network for information
- 155 Qualified tools on previous projects, used in the same way are required to be re-qualified.
- 176 The difficulty of qualifying a production tool so that credit can be taken for its use. The tool must now be created at the same level as the code it produces. This intuitively seems to be overkill, but no alternative has been found that all (FAA & Industry) can agree to. Difficulty in qualifying a production tool (e.g., code generator).

2.1.7 DO-178B has inadequate and ambiguous guidance for COTS software.

- 30 COTS (SC-190 has subgroup looking at this issue)
- 112 How is SW certified when used in conjunction with non-certified SW. (example: use of previously developed SW--COTS operating system).
- 169 Imperative to develop a set of guidelines to establish how COTS can and will be certified.
- 213 Use of COTS software and operating systems.

2.1.8 DO-178B has inadequate and ambiguous guidance for reuse of certification data.

- 31 Lack of prescription in DO17B of the packaging for the verification data permits ACOs to impose additional requirements on the format
- 47 The reuse of certification data is extremely difficult.
- 53 DO-178B/ED-12B was developed for level A but does not offer sufficient relief for lower levels.
- 88 Some ACOs requires documents beyond the requirements of DO-178B/ED-12B.
- 101 Is there a need to submit data on very minor software changes? (Difference between TSO and TC/STC/ATC)
- 160 Same product, different customers causes a repetition of activities
- 211 Records required for FAA audits can be excessive. ACOs interpretation of DO-178B varies so a company rarely uses a single process, thus process become project or ACOs specific.

- (from survey) When we have a problem report on that code, we must retest it in all the products that use that software. This is required by section 11.3.h. We feel that we should be able to reference the problem report and testing performed on the same software in previously certified products without repeating this effort for each product that uses this software module.
- (from survey) Qualifying, certifying routines or Sub-routines. So they can be used in different applications providing the level is satisfactory

2.1.9 DO-178B has inadequate and ambiguous guidance for reuse of legacy systems.

- 45 Upgrading between any software level is very expensive as currently required in DO-178B/ED-12B without being able to take credit for work already done.
- 50 Is there a way to take more credit for service history and or non-developed software (e.g. COTS) as a means of relief from some of the requirements in DO-178B/ED-12B.
- 81 Forcing the use of DO-178B/ED-12B on systems originally developed to DO-178A is intrusive and expensive especially when there is extensive service experience. (There was some concern that this implies that DO-178A and DO-178B/ED-12B provide equivalent levels of assurance.)
- 82 Legacy systems for example back to Do-178A, 2167A etc. might provide real opportunities for streamlining by trying to take credit for service experience and the fact that changes are relatively small/incremental. This is more applicable for level B and C systems as opposed to Level A systems.
- 110 How is previously developed SW approved when transitioning from 178A to 178B? What kind of credit can be taken from the 178A work. (Reference issue paper, CAST paper, SC-190 work)
- 135 Continuous push on part of FAA to upgrade the SW criticality assessment, especially on previously certified products.
- 150 Issues relating to compliance: reverse engineering required to comply to 178B, particularly for existing systems.
- 196 How can the applicant obtain credit for reuse of "shrink-wrapped" code for legacy systems previously certified, for so called "derivative systems"
- 202 DO-178B does not provide adequate guidance for migrating legacy programs being used. A legacy may not have done its certification to meet DO-178B objectives, but still may be a safe system.

2.1.10 DO-178B has inadequate and ambiguous guidance for non-airborne systems.

- 9 Having difficult time determining who in the FAA approves ground systems, and getting different answers. Most common answer is to do the most expensive thing possible.
- 62 DO-178B/ED-12B and the system safety assessment process need to pay specific attention to non-airborne systems.
- 114 When doing end-to-end, how do you look at avionics with respect to ground systems (ex: WAAS and datalink)? Answer: Being handled by SC-190
- 199 Issue of how to certify human-computer interface software to be compliant with DO-178B. As a result, cost, schedule, and safety may be impacted. This may be difficult to get air and ground community to agree.
- 214 Applicability of airborne system certification standards to ground-based systems. Issues relating to relative scale of systems, testing, etc
- 215 End-to-end certification of ground and airborne software. Need to protect and recover from syntactical and logical errors. As a result, the scope of standards and guidance need to expand to cover the end-to-end system, including the communication pathways.

2.2 Issues about the benefits of DO-178B.

2.2.1 The extent to which DO-178B provides benefits beyond those that are provided by other industry accepted practices is unclear.

- 42 The definition of best practices should be codified into an extension of existing regulatory guidance.

- 43 The regulatory requirements result in expensive reverse engineering costs as a result of inadequate understanding of DO-178B/ED-12B
- 54 Imposition of regulatory requirements that do not provide Customer value/benefits commensurate with the costs .
- 57 Extract only the important elements to concentrate on.
- 92 Delegation to the organization instead of on a product basis could contribute to reducing costs considerably.
- 93 What is the percentage of overall cost due strictly to certification over and above what good practices would dictate (e.g. cost of structural coverage documentation). Caller 1 see no decrease Caller 2 would see improvement in legacy systems in excess of 50% Caller 3 Qualification of tools and non developed software (e.g. COTS) add about 90% increase of tool qualification which translates into about 5%?? of overall certification. Caller 4 FAA only contributes 10% of documentation costs probably less for overall costs. Caller 5 Due to ability to use non developed software (e.g. COTS) a savings of 30% might be realized. One example was OSI stacks $20k off the shelf vs %500K for uniquely developed. Caller 6 Might see additional innovation using other types of development processes which might provide productivity gains. (e.g. domain analysis, safety directed development, different reuse techniques) The actual cost benefit is difficult to quantify. Caller 7 If left to own devices might save 25-30% Caller 8 Distributed application would be done in 1/4 to 1/5 the cost if DO-178B/ED-12B were not applied. Caller 9 The majority of the cost saved may not be due to DO-178B/ED-12B requirements but may be due to the interaction with the certification authorities. Caller 10 The release of the existing completion criteria (e.g. structural coverage) could result in 25% reduction in overall certification of software based systems. Caller 11 On a given system dramatic amounts of money (50% or greater) by using alternate means of compliance is being realized
- 96 No way to evaluate that a company is capable of doing DO-178B/ED-12B prior to release of contract resulting in retraining of suppliers delaying schedule and increasing costs. Even though the contractor may be found capable by other measures (e.g. SEI CMM, ISO 9000, etc.)
- 106 Is 178B a good standard? (The best but is costly to manufacture/use)
- 118 Why couldn't SEI maturity level be used as an alternate means?
- 157 Transition criteria forces developers to focus on process rather than products and does this focus on process, versus product, effect safety.
- 159 Parallel, or shadow, processes. One to develop the product, the second to satisfy certification objectives.
- 166 Experience of developer in getting process credit is not taken into account. Competence of developer is given no consideration when certifying the product.
- 168 DO-178B does not allow for qualification of process once versus product each time.
- 177 Approve and audit the manufacturer's software process rather than individual product submittals.
- 183 Interpretation of DO-178B may be a challenge for fast-track implementation and shouldn't a sound development methodology should suffice?
- 209 The basis of DO-178B is quality-by-process. The goal of certification is safety of the public is flight. Does process rigor effectively address safety.

2.2.2 The effectiveness of some specific activities required by DO-178B is unclear.

- 15 Independence required by ACOs without sufficient justification
- 49 Is there a way to reduce the extensive documentation requirements (e.g. more reliance on the integrity of the developers) and subsequent extensive regulatory review.
- 58 (see also 1.2.3) One of the major software development costs has been requirement changes resulting in rework changes. DO-178B/ED-12B exacerbates this issue due to the stringent requirements for documentation that may not be done otherwise.
- 91 Review the documentation requirements to ensure that they provide value added attributes for both the regulatory authorities and the developers.

- 120 What is "good enough" testing? (Related to previous comment--testing req changes as technology advances)
- 121 What is good enough requirements analysis? (Sys engr issue). Missing element in 178B.
- 122 Lack of requirements validation?
- 142 Maintaining traceability to code level
- 146 Static analysis and structural coverage are cost drivers, due to training, few tools available.
- 163 Additional informal validation/verification activities used to decrease required DO-178B verification activities renders formal review less effective. Are the additional activities accomplished to achieve quality or to "patch" inadequate DO-178B guidance?
- 164 Relative effectiveness of SQA and SCM representatives during all the activities and it is possible to meet all SQA and SCM DO-178B objectives without producing a quality product.
- 174 Consider that some of the tracking (e.g., Traceability Matrix and coverage analysis) should be a function of size the job, develop environment, and the number of programmers as well as criticality level.
- 188 Requirements for documentation, data, and verification testing are daunting. DO-178B and DO-160D impose more stringent requirements for tests, processes and internal visibility
- (from survey) It is not obvious to me that level "B" and level "A" requirements add the cost equivalent of safety/quality to the product. This is particularly true of the independence requirements.
- (from survey) I am unsure of the value of some of the code requirements such as having no dead code or unused variables. I would maintain that unused variables are not detrimental if it does not cause your processor to run out of memory to declare them. (The memory map is checked for this condition). Likewise, if you can prove that code is truly unreachable, it should also be deemed safe. These two restrictions affect our ability to have common routines between different Configuration Items when only small differences in functionality are apparent. In this case you must completely test two very-similar modules, which is arguably redundant.
- (from survey) There is an inverse relationship and disproportionate amount of value added by higher levels of structural analysis. Structural analysis adds significant cost and yields marginal benefits.
- (from survey) We also feel that Level C should not require statement coverage. We feel requirements based test coverage is sufficient for Level C software to provide an acceptable level of safety/quality/reliability.
- (from survey) The use of tools enhances the safety/quality/reliability of the embedded software, but the cost and delay of tool qualification are too high. The requirements on tools (of par. 12.2 of DO 17813) are at the same level as the requirements for generated code. It should not be. Some low-level verifications and/or tests should be suppressed, and a structural coverage analysis should be performed on the source code.

2.2.3 DO-178B inadequately provides for innovation.

- 48 Incremental development or any modern and innovative process is not supported in DO-178B/ED-12B.
- 83 Alternative methods are not up to date with current software development methods. A means to easily/generically accommodate advances in technology without specifically including the technology in the document. DO-178B/ED-12B forces the applicant to address the objectives directly which may not be applicable for a given technology or the base intent of the objective.
- 102 Is there any other alternative besides SDD that is allowed outside of DO-178B? Are there alternatives to 178B that have been accepted? How would an alternate method be evaluated?

- 103 Why do some ACOs not permit alternate means to DO-178B? (What if we could provide data regarding alternate methods to show that they are more effective?) Redundant
- 119 How does the FAA deal with changing technology? How do we keep the cert process up to date with changing technology?
- 143 As tech changes, a standard can never be 100% correct.
- 145 (see also 1.1.7) Formal methods are a cost driver for foreign agency certification (CAA).
- 148 (see also 1.2.2) There is some feeling that some methods may be helpful but there is no data available or may be proprietary, i.e., formal methods. It may not have standardized metrics. They may require a special study. Will there be uniform standards for both military and civil applications?
- 162 No credit given for prototyping of requirements. (i.e., modeling before development)
- 165 Alternative methods scrutinized extensively or are rejected by ACOs. As a result, more efficient designs, activities, tools cannot be used for product development or significant re-engineering needs to be done. DO-178B specifies that alternative methods can be used as long as the objectives are met, but in practice it is not feasible.
- 185 What level of verification for COTS components is required (software and hardware)?
- 194 What credit can a developer receive for using alternative means, architecture, and safety monitoring versus what is commonly accepted (current TSO says apply for deviations). How criticality is assign and flows to software is an issue.
- 201 Current certification process may not adequately address today's hardware and software architecture. In addition, obsolete parts cannot be replaced and companies cannot take advantage of new technology
- 206 Some ACOs do not really accept a alternative means of compliance that deviate from DO-178B.
- 208 (see also 2.1.5) Objectives in Annex tables are not all objectives--some are specific means of compliance MCDC), so an alternative means of compliance are not feasible as specified in Chapter 12.
- 212 Certification of multiple applications in modular software and hardware architectures. Including mixtures of criticality and function, isolation of applications, system performance, considerations, data fusion issues, etc. Fault protection and failure recovery mechanisms and incremental certification of new applications. There is no guidance on how to certify systems that incremental systems and systems that will run on multiple platforms will be handled
- (from survey) There are 2 prime areas that are candidates for cost/schedule impact reduction. The first is use of CASE tools to automatically generate certified software.
- (from survey) We don't allow our suppliers to use COTS unless it is previously certified because it is our experience that the certification process as presently invoked by DO-178B is too costly unless software is designed from the start with the meeting of DO-178B goals as an objective.

2.2.4 DO-178B inadequately addresses the effect of software on the safety of the overall system.

- 7 To what extent should accident statistics guide the allocation of resources in certification? Perhaps too much concentration has been given to software.
- 29 Inadequate emphasis on the software contribution to system hazards
- 41 The definitions for (software/system and any other terms) safety, safety assessments, reliability, quality, certification, costs, etc are not defined well enough to provide consistent review and completion criteria. Nor is the relationship between them defined. If we don't have good definitions we cannot know when we achieved them.
- 56 Explore the benefit of using risk based analysis similar to military and NASA programs.
- 73 Software safety assessment is not required/supported by DO-178B/ED-12B
- 87 The Certification Authorities are requiring the wrong documents (e.g. propose use of software safety analysis, or other appropriate documentation).

- 89 The final documentation should be ultimately related to the safety requirements/assessment.
- 99 Does Level A SW buy you more safety than level B, C, D? (Difference for level A: structural coverage, independence,). Does 178B add safety? (Lack of clearness on safety process and interplay with SW process)
- 100 Is there a way to move from an absolute safety std to a relative std to evaluate safety? What is level of safety now? (ex: GenAv aircraft with older equipment safer than newer equipment at a lower safety level?)
- 108 Is there info available from military applications regarding SW incidents?
- 124 Lack of emphasis in certification on an integrated systems view, seeing software as an integral component
- 131 (see also 1.1.1) Excessively wide interpretation of what constitutes a safety requirement. (Too many things are treated as safety issues that are not safety issues.
- 205 The objective of certifying software is safety. DO-178B does not specifically address safety. Unless we assume all the safety areas are covered by systems and all software has to do is replicate the system correctly. The end software product design needs to be check for safety.
- 210 DO-178B is back loaded with most certification credit from testing. I'd have to say the building safety into design is better than trying to test it in, but software designs do not have to be built or reviewed for safety.
- (from survey) The key issue is actually in the definitions used in sections 2.1.1 and 2.2.1. When compared with MIL-STD-882, considered best practice in the conventional system safety community, "failure condition" is actually a "hazard". "Failure condition" is a poor choice of wording because it implies a failure, when in fact no failure need occur. Reliability is the discipline where failures are the only cause considered. There is no doubt that this terminology has in itself limited some safety analyses to only consider failures.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 1998	Technical Memorandum

4. TITLE AND SUBTITLE
Streamlining Software Aspects of Certification:
Technical Team Report on the First Industry Workshop

5. FUNDING NUMBERS
RTR 505-64-10-58

6. AUTHOR(S)
Kelly J. Hayhurst, C. Michael Holloway, Cheryl A. Dorsey,
John C. Knight, Nancy G. Leveson, G. Frank McCormick, and
Jeffrey C. Yang

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L-17716

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
NASA/TM-1998-207648

11. SUPPLEMENTARY NOTES
Hayhurst and Holloway: Langley Research Center, Hampton, VA; Dorsey: Digital Flight, Clifton, VA; Knight: University of Virginia, Charlottesville, VA; Leveson: University of Washington, Seattle, WA; McCormick: Certification Services, Inc., Carnation, WA; Yang: The MITRE Corporation, McLean, VA.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category 61 Distribution: Nonstandard
Availability: NASA CASI (301) 621-0390

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

To address concerns about time and expense associated with software aspects of certification, the Federal Aviation Administration (FAA) began the Streamlining Software Aspects of Certification (SSAC) program. As part of this program, a Technical Team was established to determine whether the cost and time associated with certifying aircraft can be reduced while maintaining or improving safety, with the intent of impacting the FAA's Flight 2000 program. The Technical Team conducted a workshop to gain a better understanding of the major concerns in industry about software cost and schedule. Over 120 people attended the workshop, including representatives from the FAA, commercial transport and general aviation aircraft manufacturers and suppliers, and procurers and developers of non-airborne systems; and, more than 200 issues about software aspects of certification were recorded. This paper provides an overview of the SSAC program, motivation for the workshop, details of the workshop activities and outcomes, and recommendations for follow-on work.

14. SUBJECT TERMS
software, certification, streamlining, DO-178B, SSAC

15. NUMBER OF PAGES
59

16. PRICE CODE
A04

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	