

# Certification Authorities Software Team (CAST)

## Position Paper CAST-5

Guidelines for Proposing Alternate Means of Compliance to DO-178B

Completed June, 2000

***NOTE:*** This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.

# Guidelines for Proposing Alternate Means of Compliance to DO-178B

## Purpose

The purpose of this paper is to provide guidelines for industry in proposing alternate means and for the certification authorities and designees to evaluate the feasibility of those proposed alternate means for meeting the safety objectives of the regulations.

## Definitions

For purposes of this position paper, an “alternate means” is an alternate way of meeting the safety objectives of the regulations by using some means other than DO-178B/ED-12B. An “alternate method” is an alternate way of meeting the DO-178B/ED-12B objectives. Alternate methods are addressed in Section 12.3 of DO-178B/ED-12B and in Section 4.5 of ED-248A (reference Appendix A of this paper). While alternate means and alternate methods are closely related, this paper focuses on alternate means.

## Background

Advisory Circular AC 20-115B, “RTCA, Inc., Document RTCA/DO-178B” states that the applicant may use the considerations outlined in RTCA/DO-178B as “a means, but not the only means, to secure FAA approval of the digital computer software.” The Joint Aviation Authority (JAA) recognizes ED-12B via Temporary Guidance Leaflet Number 4 (TGL No. 4). Other airworthiness authorities have similar means of recognizing either DO-178B or ED-12B as a means of showing compliance to the regulations. The Streamlining Software Aspects of Certification (SSAC) survey results indicate that it is unclear to both the FAA and industry how to approach alternates to DO-178B/ED-12B.

DO-178B/ED-12B provides objectives that should be considered for the appropriate safety level of the system being deployed. Since both the certification authorities and industry have adopted DO-178B/ED-12B as a “standard” for development and assurance of airborne and safety critical software, it is difficult to determine what alternate means still meet the level of safety required by XX.1309 and XX.1301.

Currently, certification authorities typically require that applicants meet the appropriate objectives of DO-178B/ED-12B. If an applicant proposes a non-traditional approach to one or more of the DO-178B/ED-12B objectives, they must show how that approach meets the “intent” of the objective(s). This requires a thorough understanding of the “intent” of each objectives. For example, the intent of software testing is stated in DO-178B/ED-12B, paragraph 6.4. Any alternate means for objectives related to paragraph 6.4 should demonstrate the same intentions as paragraph 6.4

## Discussion

Alternate means may be approached on three different levels: the objective level, the process level (e.g., SCM or SQA), or the system/safety level. This paper focuses on the objective and process levels. The system/safety level is covered in a different paper.

There are a number of steps that the certification authority and applicant should consider when assessing an alternate mean:

Applicant	Certification Authority
<ol style="list-style-type: none"> <li>1) The applicant should involve the certification authority and designees in the discussion of alternate means as soon as possible. Involve them from conception to implementation.</li> <li>2) The applicant should identify the objectives that will require alternate means by mapping their proposed processes, etc. to the objectives or set of objectives of DO-178B/ED-12B. Use the DO-178B/ED-12B matrix for the mapping. (Note: Order of (1) and (2) may vary.)</li> <li>3) The applicant should document the intention of each objective or process that they are seeking alternate means approval for. They may need to discuss this with the cert authority.</li> <li>4) The applicant should document their rationale (including any supporting data, logic, analysis, etc.) and the means that is being considered as an alternate to DO-178B/ED-12B objective or process in their PSAC. This should demonstrate why the alternate means is adequate from an engineering and safety perspective. When proposing an alternate means, the means the applicant should review and document the alternate means against: <ul style="list-style-type: none"> <li>• the FARs/JARs</li> <li>• the safety objectives of the certification authorities,</li> <li>• known industry best practices for safety,</li> <li>• research evidence, and</li> <li>• scientific evidence.</li> </ul> </li> <li>5) The applicant should document plan for data to be produced in the PSAC. The PSAC should also document what data will be submitted or made available to the certification authority as evidence.</li> </ol>	<ol style="list-style-type: none"> <li>1) The certification authority should review the applicant’s proposed alternate means against the objectives of DO-178B/ED-12B to determine which objectives are not met in the “traditional” manner.</li> <li>2) The certification authority should work with appropriate technical experts (e.g., NRS, international cert authorities, etc.) to understand the “intent” of the DO-178B/ED-12B objectives that are not met. Many of the objectives of DO-178B/ED-12B, Annex A, are clearly stated in the related DO-178B references; however, some are still unclear and controversial.</li> <li>3) The certification authority should evaluate the applicant’s analysis of how their method meets the intent of the DO-178B/ED-12B objectives.</li> <li>4) The certification authority and applicant should come to an agreement on the adequacy of the alternate as soon as possible in the program. The agreement should be documented in the PSAC. (Note: need to reword for applicant and cert authorities’ roles).</li> <li>5) The certification authority should review and approve (or provide feedback to) data submitted for alternate means.</li> </ol> <p>Note: For some highly technical methods, software experts may need to work with academics and experts outside of certification authority to verify and support the assessment.</p>

**NOTE:** This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.

6) The applicant should submit appropriate results from the alternate mean as agreed to in the PSAC.	
7) The applicant should address the impact of the alternate mean on post-certification modifications.	

Note: Since alternate means is a unique technical consideration, the certification authority responsible for software approval should involve the proper specialists in the evaluation and approval of alternate methods. Particularly, the first time the alternate has been used.

### **A Potential Example**

An example of an alternate means might be an applicant that desires to have a system developed using DOD-STD-2167A approved on a product seeking certification. The applicant could map their 2167A process to the DO-178B/ED-12B objectives and activities; identify the objectives that are not met in a “traditional manner”; develop an argument for why their process satisfied the intent of those objectives; discuss the approach with the certification authority to obtain buy-in and/or feedback. Additionally, the applicant would need to correlate the DO-178B/ED-12B data items with the 2167A documents and demonstrate adequacy; any missing data items would need to be provided (e.g., PSAC, SAS, ...).

### **References**

- 1) DO-248A/ED-94A, “SECOND ANNUAL REPORT FOR CLARIFICATION OF DO-178B/ED-12B ‘SOFTWARE CONSIDERATIONS IN AIRBORNE SYSTEMS AND EQUIPMENT CERTIFICATION’” (Fall 2000)
- 2) DO-178B/ED-12B, “SOFTWARE CONSIDERATIONS IN AIRBORNE SYSTEMS AND EQUIPMENT CERTIFICATION” (December, 1992).
- 3) “Using the Software Capability Maturity Model for Certification Projects” by L. Rierson provides some ideas of approaching the FAA with a project that implements CMM.

**NOTE:** This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.

## Appendix A – Excerpts on Alternate Methods

**Section 12.3 of DO-178B/ED-12B is entitled “Alternative Methods” and states the following:**

*Some methods were not discussed in the previous sections of this document because of inadequate maturity at the time this document was written or limited applicability for airborne software. It is not the intention of this document to restrict the implementation of any current or future methods. Any single alternative method discussed in this subsection is not considered an alternative to the set of methods recommended by this document, but may be used in satisfying one or more of the objectives of in this document.*

*Alternative methods may be used to support one another. For example, formal methods may assist tool qualification or a qualified tool may assist the use of formal methods.*

*An alternative method cannot be considered in isolation from the suite of software development processes. The effort for obtaining certification credit of an alternative method is dependent on the software level and the impact of the alternative method on the software life cycle processes. Guidance for using an alternative method includes:*

- a. An alternative method should be shown to satisfy the objectives of this document.*
- b. The applicant should specify in the Plan for Software Aspects of Certification, and obtain agreement from the certification authority for:
  - (1) The impact of the proposed method on the software development processes.*
  - (2) The impact of the proposed method on the software life cycle data.*
  - (3) The rationale for use of the alternative method which shows that the system safety objectives are satisfied.**
- c. The rationale should be substantiated by software plans, processes, expected results, and evidence of the use of the method.*

**Section 4.5 of DO-248A/ED-94A is entitled “Application of Potential Alternative Methods of Compliance for Previously Developed Software (PDS)”. Section 4.5.1 states the following:**

*The purpose of this discussion paper is: (1) to present some potential alternatives that contribute to satisfying DO-178B/ED-12B objectives in cases where the conventional artifacts are not available or are only*

**NOTE:** This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.

*partially available, and (2) to suggest methods for presenting this information to a certification authority. This condition will most likely occur for software-based systems that incorporate previously developed software (PDS). For this discussion paper, PDS is defined as software already developed for use. This encompasses a wide range of software, including commercial off-the-shelf (COTS) software through software developed to previous or current software guidance.*

*This information is developed on the basis that the conventional DO-178B/ED-12B development processes are performed on the software-based system as a whole, but credit is sought for as much of the PDS development as possible. Integration of the PDS into the software-based system and subsequent verification would be included as part of the software-based system development.*

Section 4.5 goes on to describe seven potential alternative methods and their achievements, inputs, and limitations. The seven alternatives discussed are:

- Process Recognition
- Prior Product Certification
- Reverse Engineering
- Restriction of Functionality
- Product Service History
- Formal Methods
- Audits and Inspections