

Certification Authorities Software Team (CAST)

Position Paper CAST-22

Reuse of Software Tool Qualification Data Across Company Boundaries (Applying the Reusable Software Component Concept to Tools)

COMPLETED March 2005

(Rev 1)

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.

Reuse of Software Tool Qualification Data Across Company Boundaries (Applying the Reusable Software Component Concept to Tools)

1.0 Introduction and Background

1.1 Software verification and development tools are often packaged in such a way that their qualification data may be reusable on multiple projects. Chapter 9 of FAA Order 8110.49 and Section 12.2 of DO-178B/ED-12B address the tool qualification process. Chapter 12 of Order 8110.49 addresses reuse of tool qualification data within a company, when used in the same way as a previous project. FAA Advisory Circular (AC) 20-148, “Reusable Software Components,” addresses reuse of software components across company boundaries, when all stakeholders agree on the reuse approach. However, none of the policy or guidance to date addresses the reuse of tool qualification data across company boundaries. A note is included in Section 2 of AC 20-148 to allow some tool qualification reuse consideration. The note states: *“The reuse concept in this AC may apply to verification and development tools. Applicants and tool developers must discuss with the FAA the details of each reusable tool qualification project. Because tools differ from airborne software, there are other concerns to address when trying to reuse tool qualification data. The FAA plans to address tool reuse in future guidance.”* However, at the time of completing the AC, the approach for addressing tool qualification reuse was not yet documented.

1.2 The purpose of this paper is to document the process for reusing tool qualification data across company boundaries (i.e., to approach tools as a kind of reusable component that may be reused with minimal certification authority involvement on the subsequent projects). This paper builds upon the guidance of AC 20-148 with specific focus on tool-unique aspects.

Note: If the tool is not used across company boundaries, this approach may not be desirable (i.e., Chapter 12 of Order 8110.49 should be consulted instead).

1.3 This position paper will likely become the basis for additional guidance or an update to AC 20-148 to specifically address the reuse of tool qualification data across company boundaries. It must be noted that if this position paper progresses to be implemented into an AC, the AC contents will take precedence over this paper.

2.0 Overview of AC 20-148

AC 20-148 is summarized below:

- Sections 1 through 3 explain the purpose of the AC, discuss the motivation for the guidance, and outline factors for getting certification authority to accept a reusable software component (RSC).
- Section 4 provides general guidelines for RSC acceptance.
- Sections 5 through 7 provide guidance for RSC developers, integrators, and applicants on developing or using an RSC.

- Sections 8 through 10 provide typical activities the RSC developers, integrators, and applicants can expect from the certification authorities for the first acceptance of an RSC and its subsequent use.
- Section 11 discusses common issues that should be addressed when developing and using an RSC. These issues may affect multiple DO-178B/ED-12B objectives. Section 11 is not an exhaustive list of issues that may arise, since each project will have its own specific issues.
- Section 12 addresses changes to an RSC.
- Section 13 provides guidance for concurrent uses of an RSC.
- Section 14 lists related documents to assist with RSC compliance.
- Appendices 1 through 3 provide definitions of key terms, list of acronyms, and a sample format for an RSC developer to document DO-178B/ED-12B credit.

Note: As discussed in AC 20-148, the AC has been coordinated with international certification authorities and their comments have been addressed. However, it is not certain if international authorities will adopt the AC. International certification projects should be coordinated with the appropriate authorities to determine the applicability of the AC.

Figure 1 below illustrates the approach outlined in AC 20-148.

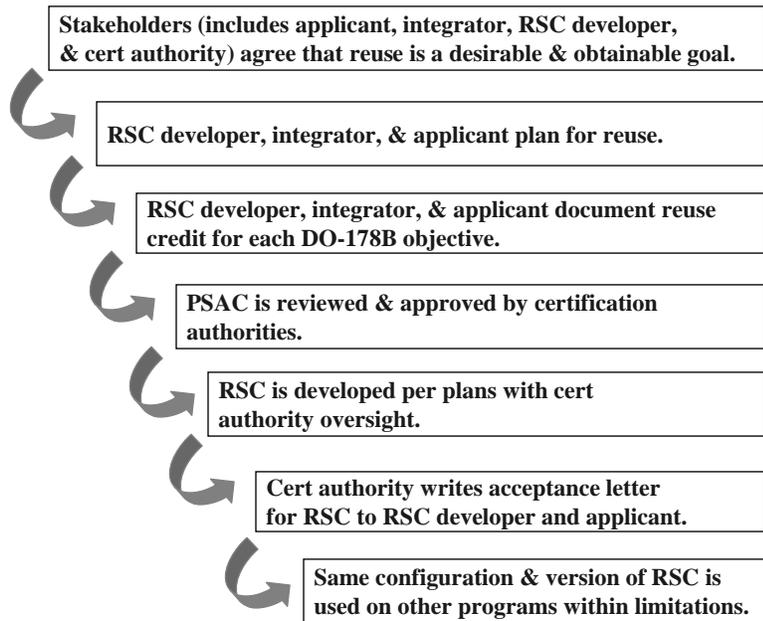


Figure 1 – AC 20-148 Approach

3.0 General Guidelines for Reusable Tool Qualification

- 3.1 Proposed reusable software development and verification tools should be packaged and qualified in such a way that some of the tool qualification data may be reused on other projects. The boundaries and limitations of what is reusable and what will be project-specific should be established during the first acceptance of the reusable tool qualification package.
- 3.2 Projects that desire to obtain “credit” for a reusable tool should follow the guidelines of AC 20-148 and this paper, as applied to tools. The majority of the AC’s guidelines may be applied to tools, as well as embedded airborne software components. Specific reusable tool guidelines are discussed below for both development tools and verification tools.
- 3.3 The acceptance letter for the reusable tool qualification will be similar to that described in Section 9 of AC 20-148. The letter will likely reference the Reusable Tool Qualification Plan (RTQP), Reusable Tool Accomplishment Summary (RTAS), Reusable Tool Configuration Index (RTCI), and Reusable Tool Data Sheet (RTDS). The identification, revision, and dates of these referenced documents must be included in the acceptance letter to ensure that the proper configuration is considered in subsequent projects. Other data associated with the initial tool qualification should be available for review by the certification authority, as requested.

4.0 Development Tool Guidelines

- 4.1 Reusable development tools should follow the guidance in AC 20-148 for reusable software components, and the guidance of this paper as applied to tools. Where an RSC Plan for Software Aspects of Certification (PSAC), Software Configuration Index (SCI), Software Accomplishment Summary (SAS), Data Sheet, etc. are described in AC 20-148, an RTQP, RTCI, RTAS, RTDS, etc. should be used instead (i.e., the appropriate tool qualification data should be substituted for the RSC data).
- 4.2 As with an RSC, the initial reusable tool qualification must be done in the context of an actual certification project and must have the documented agreement of all the stakeholders (i.e., the applicant, the system developer, the reusable tool developer, the tool user, and the certification authority must agree on the plan for tool reuse). (Note: The stakeholders may vary depending on the nature of the project.)
- 4.3 The concept of defining credit and roles for each DO-178B/ED-12B objective will still apply for the development tool, as described in Section 5 of AC 20-148. For each objective, the following should be described in the RTQP and RTAS: amount of credit being sought (full, partial, or no credit), assumptions, means of compliance, and remaining activities to be completed by the applicant, system developer and/or tool user.
- 4.4 The credit being claimed for the tool (i.e., the DO-178B/ED-12B objective(s) that it automates, replaces, or supplements) should also be described in detail in the RTQP and RTAS with appropriate justification of the tool’s development assurance level. For each objective that the tool automates, replaces, or supplements, the following should be described in the RTQP and RTAS: amount of credit being sought (full, partial, or no

credit), assumptions, means of compliance, tool limitations, and remaining activities to be completed by the tool user, system developer, and/or applicant.

- 4.5 Any assumptions and limitations that affect proper tool operation should also be identified in the RTAS and RTDS (as well as in the tool user's guide).
- 4.6 Additionally, the guidance of DO-178B/ED-12B Section 12.2 should be addressed in the RTQP, RTAS, and other reusable tool qualification data.
- 4.7 The reusable tool data to be supplied to the tool user, system developer, and/or applicant is comparable to the data listed in Section 6 of AC 20-148. That is, the tool user, system developer, and/or applicant will need all data to support software compliance substantiation and aircraft type certification and continued airworthiness.
- 4.8 A RTDS and acceptance letter for the development tool will be similar to an airborne RSC data sheet and acceptance letter (see Sections 6.i and 9 of AC 20-148). That is, the RTDS and acceptance letter should include the same types of information as described in AC 20-148.

5.0 Reusable Verification Tool Qualification Guidelines

Defining reuse criteria for verification tool qualification is slightly more challenging than development tool qualification, because objectives for verification tools are not directly listed in Annex A of DO-178B/ED-12B and Chapter 9 of Order 8110.49 addresses only the tool qualification process itself and not reuse of the tool qualification data. The concept of AC 20-148 applies for verification tools; however, the following guidelines should also be considered:

- 5.1 The initial reusable tool qualification must be done in the context of an actual certification effort and must have the documented agreement of all the stakeholders (i.e., the applicant, the system developer, the tool developer, the tool user(s), and the certification authority must all agree on the plan for tool reuse). (Note: The stakeholders may vary depending on the nature of the project.)
- 5.2 The reusable tool developer should package the verification tool data separately from the project documents. This is not typically required for a verification tool, but if reuse credit is sought, it should be separately packaged. (It may be necessary also to protect company proprietary information, since the data needs to cross company boundaries.) That is, the verification tool should have a RTQP, RTCI, RTAS, RTDS, and supporting reusable tool qualification data.
- 5.3 AC 20-148 relies on the concept of full, partial, or no credit for DO-178B/ED-12B objectives. That is, the objectives serve as the mechanism for determining responsibilities of the RSC developer, and the integrator or applicant. Prior to the end of the project, all applicable objectives must be satisfied. Since objectives for verification tool objectives are not listed in Annex A of DO-178B/ED-12B, Table 1 was generated to describe the objectives for reusable verification tool qualification.
- 5.4 The verification tool objectives in Table 1 should be described in detail in the RTQP and RTAS. In generating these objectives, the objectives for airborne software and development tools were considered for their relevance to reusable verification tools. Additionally, Section 12.2 of DO-178B/ED-12B and Chapter 9 of FAA Order 8110.49 were considered. A set of 15 verification tool qualification objectives was generated and is shown in Table 1. Note that, since Table 1 was generated specifically for qualification

of reusable verification tools, its objectives may go beyond existing guidance, e.g., Chapter 9 of Order 8110.49. The first two columns provide the reusable verification tool qualification objective number and description (the objective number is unique to this position paper and has no relevance or tie to DO-178B/ED-12B objective numbering). The third column describes the output of the objective and DO-178B/ED-12B references. The fourth column provides additional description of each objective and the applicability to reusable verification tools. The fourth column also describes the similarity of the reusable verification tool objective to the objectives for airborne software and development tools. The last column describes if the output needs to be CC1 or CC2 (control category 1 or 2), using Table 7-1 in DO-178B/ED-12B to define CC1 and CC2. The goal of Table 1 is to provide a set of reusable verification tool qualification objectives that can then be used to communicate full, partial, or no qualification credit in a verification tool reuse project.

Table 1 – Reusable Verification Tool Qualification Objectives

Obj	Description	Output Description and DO-178B/ED-12B Reference	How the Objective Applies for Reusable Verification Tools (<i>and similarity to DO-178B/ED-12B Annex A objectives</i>)	CC
1	Define the intended use of the tool, its architecture and environment, the qualification approach, and a description of credit claimed.	Reusable Tool Qualification Plan (RTQP) (12.2.3.1 a, b, e, and f only)	While there is no requirement for a RTQP for a verification tool under DO-178B/ED-12B, a RTQP should be provided to obtain reusable credit. The RTQP includes a description of the intended use of the tool, its architecture and environment, the qualification approach, a description of credit claimed, and other information as described in Section 12.2.3.1 of DO-178B/ED-12B. For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(4). <i>This is similar to objective A1-1, Software development and integral processes activities are defined.</i>	1
2	Define and document the use of the verification tool, when qualification is required (i.e., when DO-178B/ED-12B objectives are eliminated, reduced, or automated by the use of a software tool without its output being verified).	RTQP 12.2.3.1 b	This section of the RTQP should identify which DO-178B/ED-12B objectives the tool will automate, replace, or supplement. Justification for the tool’s adequacy for claiming such credit should also be documented. Additionally, it should be clear what the applicant, system developer, and/or tool user will need to do to properly claim credit for this objective in their project. <i>This is related to objective A1-4, Additional considerations are addressed.</i>	1

Obj	Description	Output Description and DO-178B/ED-12B Reference	How the Objective Applies for Reusable Verification Tools (<i>and similarity to DO-178B/ED-12B Annex A objectives</i>)	CC
3	Reusable tool operational requirements are developed.	Reusable Tool Operational Requirements (RTOR) 12.2.3.2 (a, b, and c only),	For additional guidance, see FAA Order 8110.49, Chapter 9-6.a. <i>This is similar to objective A2-2, High-level requirements are developed.</i>	1
4	Tool complies with reusable tool operational requirements.	Reusable Tool Qualification Data (12.2.2),	The tool qualification data should include tool verification cases, procedures, and results demonstrating that each operational requirement is tested over its normal range. For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(3) and DO-178B/ED-12B, Sections 11.13 and 11.14. <i>This is similar to objective A6-1, Executable Object Code complies with high-level requirements.</i>	2
5	Test coverage of reusable tool operational requirements is achieved.	Reusable Tool Qualification Data (12.2.2)	As part of the verification results, a coverage analysis should be performed to demonstrate that all of the tool operational requirements have been tested (or otherwise verified). For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(3) and DO-178B/ED-12B, Sections 11.13 and 11.14. <i>This is similar to objective A7-3, Test coverage of high-level requirements is achieved.</i>	2
6	Tool configuration items are identified.	Reusable Tool SCM Records (12.2.3.b)	A means should be provided to uniquely identify all components of the qualified tool and its reusable tool qualification data and their associated configuration. For additional guidance, see FAA Order 8110.49, Chapter 9-6.f and DO-178B/ED-12B, Section 11.18. <i>This is similar to objective A8-1, Configuration items are identified</i>	2
7	Baselines and traceability are established.	Reusable Tool Configuration Index (RTCI), Reusable Tool SCM Records (12.2.3.b)	While there is no requirement for a separate configuration index for a tool under DO-178B/ED-12B, a RTCI should be provided to obtain reusable credit. DO-178B/ED-12B Section 11.16 can be used to provide guidance for the structure of an RTCI . For additional guidance, see FAA Order 8110.49, Chapter 9-6.f and DO-178B/ED-12B, Section 11.18. <i>This is similar to objective A8-2, Baselines and traceability are established.</i>	1 (TCI) 2 (SCM records)

Obj	Description	Output Description and DO-178B/ED-12B Reference	How the Objective Applies for Reusable Verification Tools (<i>and similarity to DO-178B/ED-12B Annex A objectives</i>)	CC
8	Problem reporting is established.	Reusable Tool Problem Reports, Reusable Tool SCM records (12.2.3.b)	<p>In addition to any open problem reports at time of qualification, the tool developer should track and analyze all problems found after release and notify the tool user, system developer, and applicant. Problem reports should be addressed by users, developers, and applicants in subsequent reuse of the tool, and in continuing airworthiness. For additional guidance, see FAA Order 8110.49, Chapter 9-6.f and DO-178B/ED-12B, Section 11.18.</p> <p><i>This is similar to objective A8-3, Problem reporting, change control, change review, and configuration status accounting are established. However, only the problem report (section 7.2.3) is applicable to tools.</i></p>	2
9	Tool life cycle data should be retrievable (7.2.7a), stored to ensure that no unauthorized changes can be made (7.2.7.b(1)), released prior to use for software manufacture (7.2.7.d), and retained to satisfy airworthiness requirements and enable software modifications (7.2.7.e).	Reusable Tool SCM Records (12.2.3.b)	<p>For additional guidance, see FAA Order 8110.49, Chapter 9-6.f and DO-178B/ED-12B, Section 11.18.</p> <p><i>This is related to objective A8-4, Archive, retrieval, and release are established. However, only the portions of the objective applicable to CC2 are addressed, plus the addition of data release prior to use (7.2.7.d).</i></p>	2
10	Reusable tool operational environment and limitations are defined.	<p>Reusable Tool SCM Records (12.2.3.b),</p> <p>Reusable TOR (12.2.3.2.b, c)</p>	<p>The reusable tool should be properly installed within the its qualified operational environment. The credit given for the reusable tool developer, and the associated tool user and applicant responsibilities will be dependent on the installation constraints.</p> <p><i>This is similar to objective A8-5, Software load control is established.</i></p>	<p>2 (SCM records)</p> <p>1 (RTOR)</p>
11	Assurance is obtained that reusable tool qualification process complies with approved RTQP.	Reusable Tool Software Quality Assurance (SQA) Records (11.19)	<p>SQA should monitor the reusable tool qualification process and products, as with any other software development or qualification effort.</p> <p><i>This is similar to objective A9-1, Assurance is obtained that software development and integral processes comply with approved software plans and standards.</i></p>	2

Obj	Description	Output Description and DO-178B/ED-12B Reference	How the Objective Applies for Reusable Verification Tools (<i>and similarity to DO-178B/ED-12B Annex A objectives</i>)	CC
12	Software conformity review is conducted.	Reusable Tool SQA Records (11.19)	<p>The conformity review applies to RTQP, RTAS, RTCI, and other Reusable Tool Qualification Data. See Section 8.3 of DO-178B/ED-12B for conformity review guidance.</p> <p><i>This is similar to objective A9-3, Software conformity review is conducted.</i></p>	2
13	Communication and understanding between the applicant and the certification authority is established.	RTQP (12.2.3.1 a, b, e, and f only)	<p>While there is no requirement for a RTQP for a verification tool under DO-178B/ED-12B, a RTQP should be provided to obtain reusable tool qualification credit. For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(4). The RTQP provides the basis for negotiating the degree and type of credit that will be accepted.</p> <p>The RTQP should address the specific items documented in AC 20-148 and this position paper.</p> <p><i>This is similar to objective A10-1, Communication and understanding between the applicant and the certification authority is established.</i></p>	1
14	The means of compliance is proposed and agreement with the RTQP is obtained.	RTQP (12.2.3.1 a, b, e, and f only)	<p>While there is no requirement for a RTQP for a verification tool under DO-178B/ED-12B, a RTQP should be provided to obtain reusable tool qualification credit. For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(4). The RTQP provides the basis for negotiating the degree and type of reusable credit that will be accepted.</p> <p><i>This is similar to objective A10-2, The means of compliance is proposed and agreement with the Plan for Software Aspects of Certification is obtained.</i></p>	1
15	Tool compliance substantiation is provided.	RTAS (12.2.3, 12.2.4), RTCI, RTDS	<p>While there is no requirement for a separate RTAS, RTCI, or RTDS for a verification tool under DO-178B/ED-12B, this data should be provided to obtain reusable tool qualification credit. This data provides the basis for acceptance of the reusable credit for a tool. For additional guidance, see FAA Order 8110.49, Chapter 9-5.b(4). Note: In some cases RTAS and RTCI may be a combined document.</p> <p><i>This is similar to objective A10-3, Compliance substantiation is provided.</i></p>	1

5.5 As described in Section 5.c of AC 20-148, each of the following items should be detailed in the RTQP and RTAS for each objective, using Table 1 above for reusable verification tool qualification objectives:

- Credit being sought by the reusable verification tool developer;
- Assumptions and use limitations of the reusable verification tool or its data;
- Description of how the applicant, system developer, or tool user should operate the tool in order to claim credit;
- Means of compliance for each of the above Table 1 objectives and other applicable guidance (e.g., DO-178B/ED-12B, orders, issue papers, etc.);
- Activities remaining for the user, system developer, and/or applicant using the tool.

5.6 The DO-178B/ED-12B objectives that the software verification tool is replacing, supplementing, or automating should be thoroughly described in the RTQP and RTAS, along with any assumptions about the way the tool will be used in the overall system and any limitations of the tool's usage. As with the objectives described in the table above, each objective for which the tool is claiming credit should document:

- Credit (Full, partial, none) being sought by the tool developer;
- Description of how the tool user, system developer, and/or applicant should operate and use the tool to maintain the credit;
- Means of compliance for the applicable objective and justification for its automation;
- Activities remaining for the tool users (i.e., tool user, software developer, system developer, and/or applicant).

5.7 Section 6 of AC 20-148 addresses data to be supplied by the RSC developer to the tool user, system developer, and applicant to support compliance substantiation, type design and continued airworthiness. That list differs for a reusable verification tool project. For a reusable verification tool qualification, the following data should be supplied to the tool users, developers, and applicant:

- RTQP;
- RTCI;
- RTAS;
- Reusable Tool Operational Requirements (Note: In some cases, these requirements may be made available to the user and system developer and stored in a data escrow, rather than supplied to the applicant. However, access to this must still be available for certification authorities and designees for review, as requested).
- Reusable tool qualification data to support objectives that will require tool user's, system developer's, or applicant's action(s);
- Reusable tool user's guide;
- Reusable tool data sheet that concisely describes the tool's functions, limitations, interface requirements, compliance concerns, assumptions, configuration, supporting data, open problem reports, tool characteristics, and other relevant information. The data sheet should support the user, system developer, and/or applicant's use of the tool and should be submitted to the cognizant certification authority.

6.0 Summary

Software development and verification tools may be considered as reusable software components if they have the written agreement of all stakeholders (i.e., the applicant, the reusable tool developer, the system developer, the tool user, and the certification authorities) and follow the guidelines of this position paper. The software tools must first be qualified in the context of an actual certification project before being proposed for reuse on other projects. There may be project-specific issues that are not addressed in this paper that must be addressed on a case-by-case basis.