Reuse Strategy for the Previously Qualified Software Tool of Airborne Software

Jianfang Liu*, Xinai Zhang, Yi Zhao and Hui Fan

COMAC Shanghai Aircraft Design&Research Institute, Shanghai, 201210, China
*liujianfang@comac.cc

Abstract. Although the software tool qualification should be based on the specific airborne software, it is impractical to develop the software tool for one software program. Most software tools, especially for the COTS tools, would be reused in multiple software programs. This paper capture and analyzes the requirements for the previously qualified software tool in the related standards and certification guidance, and proposes a strategy and framework for the reusing the previously qualified software tool to meet the requirements of different standards and certification authority.

1. Introduction

The software tool becomes more important in the airborne software development process along with the increase of the software complexity and the application of the model-based development (MBD), automatic code generation (ACG), and formal method (FM). When the output of the software tool is trusted without further verification, the software tool should be qualified according to the requirements of RTCA/DO-178B/C “Software Consideration in Airborne Systems and Equipment Certification”[1][2]. In the tool qualification framework of the RTCA/DO-178B/C, the software tool should be qualified based on the specific airborne system.

However, it is too expensive to develop the software tool specially for only one airborne system. Therefore most software tools are reused in multiple programs. In practice, some tools are developed by the teams other than the airborne system developers, which is called as “COTS (Commercial off-the-shelf) tool”. For example, the software tools are categorized in requirements, design, implementation, analysis, testing, and target, etc. in FAA AR-06/35 “Software Development Tools for Safety-Critical, Real-Time System Handbook” [3], and more than 30 COTS tools are summarized for the structure coverage analysis purpose in FAA AR-06/54 “Software verification Tools Assessment Study”. Generally, the vendor of the COTS tool will provide the tool qualification kits which intend to be reused across programs. Thus, it is an important problem to reuse and qualify the previously qualified tool in a new airborne software program.

2. Previously qualified tool requirements in RTCA standards

2.1. Previously qualified tool requirements in RTCA/DO-178B

There is not any guidance for previously qualified tools in RTCA/DO-178B. And a general idea for the changes to previously qualified tools is provided in FAA order 8110.49 “Software Approval Guidelines” [5]. It states that the change impact analysis should be conducted on all changes to tools previously qualified. The analysis should be thorough enough to assess the impact of the tool change
on the product, as well as other tools under the influence of the change. Regression analysis may form a part of the change impact analysis. However, this guidance does not provide detailed operation suggestions and does not cover the concerns of the development tool and verification tool. In practise, the guidance for the previously developed software in RTCA/DO-178B is usually referred for the tool reuse which is not applicable enough for the software tool.

2.2. Previously qualified tool requirements in RTCA/DO-330

After the RTCA/DO-330 “Software Tool Qualification Considerations” is released in 2011, the guidance for the previously qualified tool is clearly defined [6]. There are three scenarios covered in RTCA/DO-330: unchanged, change to the tool operational environment and changes to the tool itself. When reusing the previously qualified tool but without any change, the following criteria should be evaluated:

- The tool was qualified and approved by the certification authority in previous software program.
- The TQL for the reuse tool is same as or lower than the previous qualification.
- The tool life cycle data has not changed since the tool’s previous qualification.
- The tool operational environment is equivalent to the previous qualification.
- The tool operational requirements are same to the previous qualification.
- The applicant has evaluated the approved tool qualification data.
- The applicant ensures the same version of the tool is used as that supported by the tool qualification data.

When the operational environments, e.g., upgrade the operating system of the tool hosted target, is changed but the software tool does not change, the reuse of the qualified tool should be evaluated for:

- The tool verification environments are representative of the tool operational environment which will be used.
- The tool operational environment compatibility requirements described in the Tool Operational Requirements are complete and applicable to the new tool operational environment.
- The tool installed in the new tool operational environment complies with the needs of the software life cycle processes.

If there are changes to the tool itself, change impact analysis is required to cover the following areas:

- Tool Operational Requirements.
- Tool Requirements.
- Tool Design Description.
- Tool Source Code.
- Tool development environment and development process.

The impact analysis should also identify any needed re-verification activities, e.g., traceability analysis, data coupling and control coupling analysis, regression testing, requirements review, etc.

3. Previously qualified tool requirements in certification guidance

3.1. Previously qualified tool requirements in AC 20-115D/AMC 20-115D

Because among the detailed guidance for the previously qualified tool in RTCA/DO-330, the scenario did not cover how to reuse the qualified tool with RTCA/DO-178B and reuse the qualified tool in a software program which does not follow RTCA/DO-178C. The AC 20-115C “Airborne Software Assurance” [7] and the AMC 20-115C “Software Considerations for Certification of Airborne Systems and Equipment” [8] are released by FAA and EASA individually in 2013. Because there are minor differences, the workgroup from FAA and EASA made an agreement to address these problems. The AC 20-115D “Airborne Software Development Assurance Using EUROCAE ED-12 ( ) and RTCA DO-178 ( )” [9] and AMC 20-115D “Airborne Software Development Assurance Using EUROCAE
ED-12 and RTCA DO-178” [10] are released in 2017 with identical technical content. The requirements for previously qualified tools in the A(M)C 20-115D are summarized as follows:

The requirements for reusing previously qualified tool are different base on the compliance methods of the airborne software. If the previously qualified tool is used to support the modification of the airborne software which approved using RTCA/DO-178 or RTCA/DO-178A, then the criteria of section 12.2 of RTCA/DO-178C should be used to determine the TQL and the tool reuse or modification should comply with the applicable requirements in RTCA/DO-330.

If the previously qualified tool is used to support the modification of the airborne software which is approved using RTCA/DO-178B, the requirements are different depending on whether the RTCA/DO-178C compliance for airborne software are declared or not. When the airborne software does not intend to declare compliance with RTCA/DO-178C, the previously qualified tool can be reused or modified according to the requirement in RTCA/DO-178B. The RTCA/DO-178C and RTCA/DO-330 are also encouraged to be used for the reuse or modification of the previously qualified tool. But when the airborne software intends to comply with RTCA/DO-178C, the previously qualified tool should be evaluated according to table 1. If the RTCA/DO-178B software level assigned to the tool correlates with or exceeds the required TQL established by RTCA/DO-178C, the previously qualified tool can be reused or modified by the RTCA/DO-178B. Otherwise, the RTCA/DO-330 qualification requirements should be followed.

| RTCA/DO-178C Tool Criteria and TQL |
|------------------------------------|
| RTCA/DO-178B Tool Qualification Type | Software Level | RTCA/DO-178C Tool Criteria | RTCA/DO-178C/DO-330 TQL |
| Development | A | 1 | TQL-1 |
| Development | B | 1 | TQL-2 |
| Development | C | 1 | TQL-3 |
| Development | D | 1 | TQL-4 |
| Verification | A, B | 2 | TQL-4 |
| Verification | C, D | 2 | TQL-5 |
| Verification | All | 3 | TQL-5 |

3.2. Previously qualified tool requirements in CAAC guidance

After the RTCA/DO-178C collection released, CAAC also prepared the updated advisory circular for the software certification policy revise and provided the draft document on the website [11]. Based on guidance from FAA and EASA, CAAC proposes additional requirements for the previously qualified tool, which is summarized as following.

No matter the compliance method used for airborne software is RTCA/DO-178B or RTCA/DO-178C, RTCA/DO-178B tool qualification process can only be used for the previously qualified tool when the following preconditions are satisfied:

- The TQL-4 which defined in RTCA/DO-178C section 12.2 is not applicable.
- The previously qualified tool is not used to verify the output of unqualified development tool, only if the FAQ D.7 of RTCA/DO-330 is satisfied.
- The model based development, object oriented technology and formal method, etc. are not used for the development tool unless the related issue paper is satisfied.
- The external components are used only is the T-4#11 and T-7#5 in RTCA/DO-330 are satisfied when applicable.

In addition, CAAC advisory circular also addresses the problem which reuses the previously qualified tool in newly developed airborne software.
4. Reuse framework for the previously qualified tool in airborne software development

Based on the requirements in RTCA/DO-330 and the certification requirements from CAAC, FAA and EASA, a reuse framework for previously qualified tool is proposed and summarized in figure 1. The following four steps should be conducted when reusing the previously qualified tool.

![Reuse framework of previously qualified tool](image-url)

**Figure 1. Reuse framework of previously qualified tool**

4.1. Airborne software compliance method

There are no significant requirements when reusing the previously qualified tool in previously developed software or newly developed software. But it is usually the precondition for the previously qualified tool that the qualification conclusion is approved or validated by the certification authority.

The compliance method of the airborne software should be identified at first. For the software using RTCA/DO-178 or RTCA/DO-178A, the previously qualified tool should comply with RTCA/DO-330. And for the software using RTCA/DO-178B or RTCA/DO-178C, the previously qualified tool can comply with RTCA/DO-178B or RTCA/DO-330 depending on the RTCA/DO-330 is declared or not.

It is noteworthy that the preconditions identified in section 3.2 should be met when reusing the previously qualified tool by RTCA/DO-178B according to CAAC requirements.

4.2. Tool Qualification Standard

When the standard is clearly defined as RTCA/DO-178B or RTCA/DO-330, the different reuse scenarios should be considered. As identified in RTCA/DO-330, the previously qualified tool may be unchanged, environment changed or too changed. But there is clear guidance for the different reuse scenarios in RTCA/DO-178B, so the guidance in RTCA/DO-330 could be followed.

4.3. Tool Reuse Scenarios

When the previously qualified tool intends to be reused without any change, the previously qualification standards, tool type and TQL should be evaluated. If it cannot meet the requirements of the airborne software program, the qualification baseline should be upgraded. This may include changing the qualification standard from RTCA/DO-178B to RTCA/DO-330 and upgrading the verification tool to TQL-4 tool.

When the tool operational environment is updated or changed, the evaluation should be performed to confirm that the new environment is covered and verified in the previous qualification effort.
Otherwise, the re-verification will be required to show the compatibility between the previously qualified tool and the new operating environment.

When the tool itself is changed, an impact analysis should be conducted to identify the necessary development and verification activities.

4.4. Tool Reuse Activities
After the activities for the reuse of previously qualified tool are clearly defined, the chose qualification standard, which is RTCA/DO-178B or RTCA/DO-330, should be followed. The compliance evidence for the affected activities should be recorded and presented to the certification authority.

5. Conclusion
After summarizing and analysing the previously qualified tool background and criteria, this paper proposes a framework for the reuse of previously qualified tool which meets the requirements in different standards and certification policy. This framework can be used for tool reuse in the airborne software development process. However, with the widespread usage of the complex and large scale tools in airborne software and other safety critical software, how to furthest reuse the tool qualification efforts in different process and domains will become an important topic to reduce the repeat qualification and certification activities.

References
[1] RTCA. (1992), DO-178B, Software Consideration in Airborne Systems and Equipment Certification.
[2] RTCA. (2011), DO-178C, Software Consideration in Airborne Systems and Equipment Certification.
[3] FAA. (2007), DOT/FAA/AR-06/35, Software Development Tools for Safety-Critical, Real-Time System Handbook.
[4] FAA. (2007), DOT/FAA/AR-06/54, Software Verification Tools Assessment Study.
[5] FAA. (2003), Order 8110.49, Software Approval Guidelines.
[6] RTCA. (2011), DO-330, Software Tool Qualification Considerations.
[7] FAA. (2013), AC 20-115C, Airborne Software Assurance.
[8] EASA. (2013), AMC 20-115C, Software Considerations for Certification of Airborne Systems and Equipment.
[9] FAA. (2017), AC 20-115D, Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178 ( ).
[10] EASA. (2017), AMC 20-115D, Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178.
[11] CAAC. (2020) Software Review Methods in Airborne System and Equipment Certification. http://www.caac.gov.cn/HDJL/YJZJ/202008/t20200831_204290.html.