Certification Authorities Software Team (CAST)

Position Paper CAST-11A

Criteria for Assuring Continuous and Complete Software Verification Processes

COMPLETED August 2007

(Rev 0)

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Criteria for Assuring Continuous and Complete Software Verification Processes

1.0 Purpose

The purpose of this paper is to identify the need for continuous and complete software verification, and associated Software Configuration Management (SCM) and Software Quality Assurance (SQA) processes for the development of aircraft embedded system software that can involve multiple entities (e.g., applicant, one or more software developers, one or more hardware developers, integrator). Although the applicant is responsible for ensuring that all the system and software requirements as well as the DO-178B/ED-12B objectives are satisfied for each system installed on the aircraft, there is an increasing tendency to compartmentalize the software verification process at the software developer level, and to not include testing in the system environment (i.e., on the target computer in the target environment), as needed, to complete the software verification process. There are two potential and endemic process issues that can prevent continuous and complete software verification. The first issue is the lack of recognition by the applicant and their development team that selected software tests should be performed in the integrated target computer (system) environment, since some requirements can only be verified in that environment. The second issue is associated with the lack of continuity in the SQA and SCM integral processes, as the different entities involved will have different means of satisfying these objectives. The guidelines in this paper will address the processes that should be applied to assure that the software verification process is continuous and complete, and that adequate SCM and SQA processes are established to support those objectives.

2.0 Related Documents

- RTCA/DO-178B and EUROCAE/ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992 - references particularly relevant to this topic are sections: 6.4.1a., 6.4.3a., 11.3d., 7.2.2, 7.2.4, 11.4b. and e., 8.2, 8.3, 11.5c. and 11.5g.
- FAA Order 8110.4C, CHG 1, Type Certification, dated March 28, 2007.
- FAA AC 20-115B, Radio Technical Commission for Aeronautic, Inc., Document RTCA/DO-178B, dated January 11, 1993.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

3.0 Background

DO-178B/ED-12B addresses the various software verification activities from the perspective that all of these activities are under control of the software developer and that these activities will be performed in their entirety by this single entity. Because of this perspective, there continue to be cases of software development where the software verification activities end at the software developer level. In these cases, it is often not recognized by the software developer, the aircraft system developer and/or the aircraft integrator/applicant (typically an aircraft manufacturer or modifier) that some aspects of completing the software verification may require testing in the system environment and the aircraft environment (system integrated with other systems on the aircraft). The software developer may be a different organization than the system developer, and, in some cases, may not have access to the system environment. Similarly, for aircraft environment testing, accessibility to the aircraft is likely only available from the applicant or aircraft owner and not under the system developer's or software developer's control. Guidance is needed to provide insight into situations where software is developed by one developer or group of developers of software, other than the airborne system developer and the applicant/integrator. Non-continuing, incomplete software verification is often the result of a development relationship that consists of two or more entities. These entities may consist of multiple software development groups, multiple system development groups and, possibly, a separate systems integration organization, in addition to being separate from the applicant or aircraft integrator. Two issues account for most problems associated with non-continuous, incomplete verification processes.

The first issue is the failure to recognize that selected software tests should be performed in the integrated target computer (system) and, possibly aircraft environment, to demonstrate intended function and freedom from anomalous behavior, since some errors can only be detected in those environments. In some cases, it is not possible for the software developer to simulate the system environment to a high level of fidelity, and, for those cases, it may be necessary to conduct some software testing on the integrated airborne system environment, which is under control of the system developer. Also, in some cases, the integrated system environment may be unavailable or not similar enough to the aircraft environment. Therefore, some software testing may need to be conducted in the integrator's System Integration Laboratory, on an Iron Bird and/or on the aircraft which is under the control of the applicant/owner. Some testing can only be completed on the aircraft under operational conditions, e.g., adjusting gains and filters. This aircraft testing may consist of ground testing, flight testing, or both ground and flight testing. If it is possible to simulate the system environment to a high level of fidelity at the software developer's level, then re-verification at the system environment level may not be necessary. Likewise, if

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

the integrated system environment can simulate the aircraft environment to a high level of fidelity, then aircraft ground and flight testing may not be necessary to complete verification of the software. If the environment or performance is simulated, the simulated environment should be validated to ensure the simulation is an accurate representation of the actual aircraft/system performance and/or environment. The validation compares the performance of simulator with the real world aircraft/system using quantitative and qualitative measures. The validation may require ground and/or flight testing to characterize the actual system/aircraft environment or performance.

The second issue is the lack of continuity in the developer(s) and applicant's SQA and SCM processes. When the software developer(s) and the applicant (i.e., aircraft manufacturer) are two or more different entities, there is a tendency to have separate and independent SCM and SQA processes and groups. These processes are related to their individual plans. It is these separate approaches, without proper coordination, that can result in the potential for a lack of continuity in these processes and, in turn, result in an incomplete, non-continuing verification process. It is the quality assurance organization of the applicant that is responsible for monitoring the verification activities and ensuring the completeness of supplier provided systems and its software (see section 11.5g of DO-178B/ED-12B). It is the SCM organization of the applicant that should track changes and ensures that the configuration being tested is the configuration that is intended for the certification accredited tests. Problem reporting should also be closely coordinated between all entities involved in the development to include the software developer, any other sub-developer, system developer, the integrator and the applicant. The software verification activities are likely to be incomplete if there is not close coordination, at the SQA level, between the software developer, any other sub-developer and the applicant (often the aircraft manufacturer, or modifier).

4.0 System Software Verification Testing

It should be determined prior to the start of software development, if the airborne system environment and aircraft environment will be available and at a high level of fidelity for the software developer(s) to accomplish the software verification objectives for testing the software component(s). Some applications of software driven systems are associated with closed loop performance, in relation to external factors, and will need a high fidelity integrated system environment or aircraft environment to complete the verification. These types of systems are not easily simulated at the software development environment or laboratory test bench level. If a high fidelity system environment is not available to accomplish verification of software requirements with system environment or aircraft environment dependencies, and the software developer(s), system developer and

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

the aircraft applicant/integrator are different entities, then software testing may need to be accomplished using the airborne system environment and/or the aircraft environment. Aircraft environment testing typically consists of the appropriate ground and flight testing to complete the software verification. Appropriate testing can be determined by tracing the software to be tested back to the systems requirements and identifying the necessary testing for that system functionality.

5.0 Process Control

The software verification process should be continuous and complete with associated SQA and SCM plans that define monitoring processes to ensure a continuous and complete verification process. The SQA and SCM plans should provide structure to coordinate these monitoring activities between development entities (the applicant and all participating developers) to ensure the required continuity and completeness for the software verification process. An alternate approach would be to have a single set of SQA and SCM plans that would provide for a single monitoring system or provide for coordination between multiple sets of plans, consisting of plans for each participant developer, which would enable a coordinated implementation of SQA and SCM activities. The applicant would then be responsible to harmonize, through the inputs, transition criteria, and outputs, the different sub-processes to meet the objectives of DO-178B/ED-12B sections 4.3 (b), 4.6(c), and 4.6(d). In the case where there is reliance on individual sets of plans from all involved parities, the plans are, in fact, an additional set of plans. In the alternate case, there is one master set of SQA and SCM plans.

6.0 Verification Process

The verification process includes several different types of activities that are partially software level dependent. Some of these activities are not subject to the areas that affect continuity and completeness, because of a separation in the development activities. These activities, such as modified condition/decision coverage, may be affected only from the standpoint that software errors may be undetected due to the incomplete verification process and then these activities would have to be repeated after software correction. The activities of the verification process that may be of concern with respect to continuity and completeness, are system testing that relates to software for verification and systems integration; and the adequacy of controlled verification activities that are supported by the integral processes of SQA and SCM. For example, a Primary Flight Display unit developer may need to perform the software verification activities, including testing and structural coverage analysis, in a multiple display

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

unit environment (e.g., System Integration Laboratory) to verify specific functionality, e.g., reversion characteristics. This environment may only be available as part of a system testing program, may not be co-located, and may even require tests to be performed on the aircraft. Functionality testing utilizing simulation of installation or in the actual functional installation environment should be performed. Also, without control of the multiple activities, it would be difficult to trace to the system requirements from the software module level to assure completeness of the required testing and assure that the tracing is accomplished in a structured manner.

It should be determined during the system and software planning process, if a high fidelity system environment will be available to the software developer to accomplish the software verification objectives for testing at the software developer's test bench. This determination should be a part of the system certification plan or Plan for Software Aspects of Certification. If a high fidelity system environment will be available and software verification objectives can be accomplished on the software developer's test,, then the issue of continuity for verification testing is less, but the concern for SCM is still present from the standpoint that it is still necessary to know the test configuration, and how valid that it is for the end system environment and aircraft environment. However, if a high fidelity system environment is not available to the software developer, then the SQA and SCM processes described in the "Process Control" section above are needed.

Traceability is a necessary activity to determine completeness. In many cases, selected software testing in the system environment is needed. If requirements for software at the source code level are traced back to the system level requirements, the required system functionality and related test cases can be identified and used to demonstrate complete software testing. This will assure that the final steps in the verification activities are complete.

7.0 Summary

The need for continuous and complete software verification activities exists particularly in cases where the software is developed by some entity other than the system developer, and/or aircraft or engine certification applicant or system integrator. SQA and SCM processes should exist that are continuous between the developers and the applicant or integrator. The processes should be capable of monitoring these software verification activities, with special attention given to completion of the software verification objectives (at whatever level they should be achieved). These SQA and SCM integral processes should provide the required coordination for verification identified by tracing from the software to the system requirements and subsequently to the system test requirements.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Coordination should be provided through the respective SQA and SCM plans, as well as their respective implementations, for these activities. Selected software tests may need to be performed in the integrated target computer (system) environment and sometimes the aircraft environment in order to complete the software verification activities. In those cases where a high fidelity system environment is not available to the software developer and system developer, aircraft ground and/or flight testing may be necessary.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**