

Esterline AVISTA Article: Adapting Legacy Systems for DO-178B Certification

Adapting Legacy Systems for DO-178B Certification

Paul R. Hicks, Esterline AVISTA

Note: This article from Esterline AVISTA/AVISTA Incorporated appeared in CrossTalk: The Journal of Defense Software Engineering.

The avionics world is moving toward greater integration of avionics products used in both commercial and military aircraft. Document Order (DO)-178B certification is now being required in some areas in the military (such as military aircraft flying in European civil airspace), and may be considered in others. It is possible to achieve a cost effective approach to enable legacy systems to meet DO-178B certification requirements by performing a gap analysis to determine what existing activities and artifacts can be reused for DO-178B certification and define the remaining tasks that need to be completed in order to fulfill certification requirements.

RTCA Document Order (DO)-178B [1, 2] is a long-used standard mandated by the Federal Aviation Administration (FAA) for the certification of commercial airborne avionics systems containing embedded software. In recent years, DO-178B is also being applied, at least in principle, to some non-commercial avionics systems. Many of these systems may have been developed with other standards in mind. However, aspects of DO-178B are being applied where certification will be enforced in the future. The level of compliance with DO-178B is typically influenced by budget and schedule constraints. In an increasing number of instances, the military sector is at least considering DO-178B certification.

While DO-178B may be viewed as an eventual requirement for all airborne avionics systems, commercial and military systems alike, it is currently evaluated on a case-by-case basis for military programs. The impact of incorporating DO-178B requirements on a program does not come without significant impact to budget and schedule. This impact varies depending upon the software level (A through E) imposed on the application and is a critical factor in the decision to pursue certification (see Figure 1).

Level A	Failure has catastrophic impact. Most stringent Structural Coverage Analysis (SCA) adds object code analysis requirement.
Level B	Failure has hazardous/severe impact. More stringent SCA and additional independence.
Level C	Failure has major impact. Adds SCA requirements.
Level D	Failure has minor impact. Requires verification against high-level requirements.
Level E	Failure has no safety impact.

Figure 1: DO-178B Certification Levels A Through E

Other critical factors in determining the impact of cost (budget and schedule) include the size and complexity, the system, and the maturity of the procedures and processes utilized by the software development and verification teams. Companies with more mature processes institutionalized across their organization will be able to adapt much more effectively and efficiently.

Impact to Budget and Schedule

While not yet a requirement for every military avionics system, there are some programs that do impose DO-178B certification. In this scenario, the cost and schedule impact certainly needs to be accounted for and minimized. When DO-178B certification is not imposed as a requirement, the impact to the cost and schedule must be measured against the benefits gained. The argument that DO-178B adds significant quality to a legacy system may be disputed when examining the service history of an avionics system that has countless hours of flight time. However, DO-178B processes may help identify potential deficiencies in requirements definition and/or testing by performing structural coverage analysis. In this scenario, it may be difficult to justify the budget and schedule impact when DO-178B is not an imposed requirement.

While the requirement to satisfy the criteria outlined in DO-178B may appear to be a daunting task for the engineering teams who maintain legacy military avionics systems, the effort of adapting the legacy system may be easier (and cheaper) than originally perceived. The key is to accurately estimate the impact to budget and schedule. While it is easy for engineering teams to underestimate the budget and schedule impact, it is also possible to overestimate the impact by not taking advantage of existing processes. To accurately estimate the impact, companies can and should take advantage of their existing planning documents and testing processes.

Value in Legacy Systems

There are significant benefits for a legacy avionics system to incorporate the objectives outlined in DO-178B. Best practice concepts have been derived by key members of the aviation community through implementing the certification process. These best practices continue to be refined and enhanced based on increased use, evolved technology, and gained experience as evidenced by the evolution of DO-178B.

The DO-178B specification enforces good software engineering practices by providing guidelines for the production of embedded software for airborne systems. These guidelines ensure that the systems perform their intended function with a level of confidence in the safety of the system. DO-178B serves simply as a guideline outlining the objectives to be met, the activities to be performed, and the evidence to be supplied.

DO-178B does allow for alternate methods for satisfying one or more objectives [3]. These alternate methods can be used in lieu of some of the more typical methods described throughout DO-178B requirements. However, alternate methods are more of an art than a science. There are several dependencies associated with any of these alternate methods, and there may or may not be opportunities to pursue these alternate methods. If you are considering an alternate method, consult with a Designated Engineering Representative (DER) [4, 5] with experience in the particular alternative method. With that said, the focus of this article describes using a more traditional approach.

Gap Analysis

One common misperception is that very few artifacts can be reused to upgrade a non-DO-178B certified legacy system to a certified legacy system. A start-from-scratch approach is too often the first thought to retrofit DO-178B guidelines within a legacy system. Misunderstanding the scope of a project often leads to wildly inaccurate estimates with regards to the costs and schedules associated with elevating an application to the DO-178B standard. Individuals who are best qualified to perform a gap analysis should

know the specific requirements for each software level of DO-178B certification, understand the existing processes of the legacy system, and have the authority to make decisions.

To accurately estimate the associated costs and schedules, we recommend that you follow these steps while performing a gap analysis (see Figure 2).

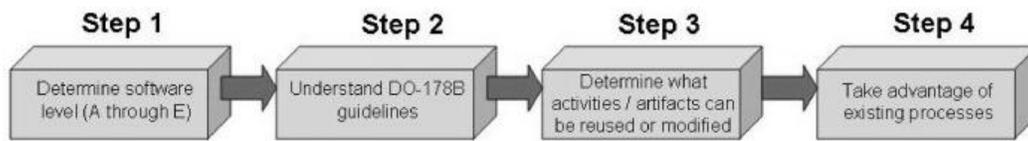


Figure 2: Gap Analysis in Four Steps

- **Step 1: Determine the software level (level A through E) that should be assigned to your application.** The software level is determined by the severity of the failure conditions on the aircraft and its occupants. This is typically identified by performing a system safety assessment as described in DO-178B [1]. The software level may be predictable based on the functionality of the application with respect to similar industry applications.
- **Step 2: Understand the guidelines identified in DO-178B.** Those who have not been involved with these certified systems before can find the learning process overwhelming. However, project teams that are new to DO-178B can learn from the several companies and organizations in the industry that have acquired a breadth of related experience. The tables in Annex A of DO-178B [1] summarize the software life cycle process objectives and outputs by software level. These tables can serve as the foundation for your gap analysis to determine which activities are required to comply with DO-178B.
- **Step 3: Determine what activities have already been accomplished and how they can be applied to the guidelines identified in DO-178B.** Many companies have solid software development processes and procedures already in place. Even though the software engineering activities that were performed may not have focused on DO-178B, these practices provide the most likely opportunities for reuse if the foundation behind the processes followed were built on solid software engineering practices – whether driven by other industry standards, industry certifications (such as the Software Engineering Institute’s Capability Maturity Model® Integration [CMMI®] or International Organization for Standardization [ISO] 9001), or good engineering judgment. Credit for much of the effort previously performed can be used for activities and artifacts identified in DO-178B. Refer to the sidebar for an example of specific activities and artifacts that can be applied to guidelines identified in DO-178B.
- **Step 4: Take advantage of existing processes currently employed that fully or partially achieve compliance to DO-178B.** It is generally not cost-effective to reinvent the wheel. The project team should supplement existing processes wherever possible. However, it is not cost-effective to utilize every existing process, especially if the process is not a useful activity to attain DO-178B certification. Consider eliminating processes not directly related to certification, or replacing these ineffective processes with more efficient ones.

By following these steps, your project team should be able to establish which objectives are completely satisfied, which objectives are partially satisfied, and which objectives are completely unsatisfied. The list of activities and artifacts identified within your gap analysis may vary with each company. If solid practices and processes are consistently implemented, fewer deficiencies will be identified in your gap analysis. If the practices and processes are uniformly institutionalized across the company, the deficiencies identified in the gap analysis should be similar across different product lines with the same software level.

Common Deficiencies

The lack of certification and planning documents are typical examples of deficiencies; specifically, documents necessary for certification submittal. These documents are the Plan for Software Aspects of Certification to describe your certification plan, and the Software Accomplishment Summary to illustrate compliance with your certification plan. If planning documents do exist, they often must be modified to ensure that they address the content described in DO-178B.

If you are using an implementation-based testing approach, the conversion to requirements-based testing could be costly and time consuming. DO-178B endorses a requirements-based functional testing approach, where your test cases and procedures are based upon the software requirements data. If you use this testing approach, you will be able reuse your original verification test suite. You probably will need to enhance your requirements-based test suite to ensure that the requirements are completely tested. In addition, requirements coverage analysis must be performed to ensure all requirements have been sufficiently addressed.

Another example of a deficiency is in the area of structural coverage analysis. The majority of the systems developed outside DO-178B do not perform structural coverage analysis. Performing structural coverage analysis ensures that all software constructs have been exercised by the requirements-based test suite. Software constructs that have not been exercised are used to identify inadequacies in the software requirements, shortcomings in the requirements-based test cases and procedures, deactivated code, and/or dead code. Each shortcoming must be resolved or justified.

Traceability

An area that is occasionally overlooked is traceability. Traceability is used to illustrate evidence of an association from an output to its origination. Typical traceability activities may include the following types:

- Requirements traceability from the lower-level requirements to the higher-level requirements.
- Source code traceability from the source code to the lower-level requirements.
- Test case and procedure traceability from the test cases/procedures to the lower-level requirements.

The goal of traceability is to be able to follow a continuous thread throughout the entire product life cycle to confirm the link between the requirements data and its associated source code and tests cases and procedures.

Independence

Certain objectives of DO-178B also require independence. Independence is the separation of responsibility between the developer and verifier to ensure no implied biases are applied to the objective under review. The objectives that require independence vary with the software level imposed on the system. It may be worth considering applying independence wherever feasible.

Configuration Controls

Some outputs of DO-178B have established configuration management controls imposed on them. Control categories define the configuration management control placed on each data item. The control category placed upon a data item also varies with the software level imposed upon the system. Again, it may be worth considering applying the more stringent configuration controls wherever feasible.

Once you have established the deficiencies found in the gap analysis, the next step is to formulate a plan to resolve the deficiencies.

Efficient Planning

As discussed earlier, the effort to obtain the DO-178B certification does not come without cost, effort, or risk. Even organizations with previous DO-178B experience still experience unexpected pitfalls – not unlike any software engineering effort. A commitment from the stakeholders is required in order to be successful.

With the information collected during the gap analysis, you can then establish a task list. Based on the findings in the gap analysis, some of the tasks may be obvious and estimates can be easily applied. For example, gathering the structural coverage from the existing test suite can be fairly straightforward. However, there may be some tasks that cannot be easily estimated until additional fact finding efforts are completed. For example, to achieve complete coverage, the effort to supplement the requirements data and test suite are strictly dependent upon the results of the structural coverage analysis effort. For this reason, you may want to consider a phased approach.

Adapting a Non-DO-178B Certified System to a DO-178B Certified System

Consider the example of a legacy Global Positioning System (GPS) portion of an inertial navigation unit, in which the system would be required to upgrade to a DO-178B certified system in the future. The engineering team responsible for the upgrade assumed that they would have to start over. But, by performing a gap analysis, they were able to decrease the cost by a factor of six by taking advantage of existing activities previously performed and existing legacy artifacts, such as planning documents, requirements data, code, test cases and test results. They were able to reuse their requirements based testing procedures, and the system already had good processes in place because they had adopted Software Engineering Institute Capability Maturity Model Integration Level 5 processes when developing the original GPS software.

Phased Approach

While a DO-178B requirement may not yet have been imposed, start planning early if there is an expectation that it will be imposed in the future. If you employ a phased approach, there are several benefits that can be realized such as the following:

- The costs may be spread out over multiple fiscal years, easing the financial impact.
- By spreading the work over a large time span, you can utilize a smaller engineering team.
- The higher risk items can be performed earlier so that the risk can be mitigated or addressed in advance of the deadline.
- Activities that lead to better estimates for follow-on activities can be performed earlier so that the follow-on activities can be more accurately estimated in advance of the deadline.
- The team has the opportunity to learn process changes earlier, thus gaining familiarity and more insight to realize process improvement opportunities.
- There is a longer history of subjective evidence to support the project.

Using a phased approach enables you to react more quickly and more effectively when the DO-178B requirement is imposed. It reduces the risk of having to quickly assemble a large team for the project at the last minute.

DERs

Involve a DER or equivalent early in the determination process. A DER is an independent specialist and an experienced engineer designated by the FAA as having authority to sign off on your project as a representative of the FAA [5]. You should establish a solid plan and have the DER approve your plan as early as possible to confirm your approach. In addition, make sure that you execute to the plan. You are not restricted from deviating from the plan when and where it makes sense. However, the deviations must be communicated to the DER as they are identified to ensure approvals. The more familiar the DER is with the plan and your execution of the plan, the more likely it is to receive the final acceptance of the certification package. If you do not have a DER on staff within your company, there are independent DER consultants that your company can hire to work with you.

Conclusion

It is important to understand that cost (both budget and schedule impact) is a significant factor that often prevents organizations that supply avionics systems from providing fully DO-178B compliant software when not required. While there are ways to reduce the cost impact, history has shown that the cost generally prohibits the implementation of DO-178B compliance when it is not a requirement. However, the industry is trending towards some level of DO-178B consideration. When it becomes a requirement, cost can be minimized by taking credit for activities and artifacts already incurred and by establishing cost effective and efficient approaches to achieving DO-178B compliance.

Converting non-DO-178B legacy systems to comply with DO-178B guidelines will become more common as requirements such as the Global Air Traffic Management program begin to enforce DO-178B certification on all avionics systems that share the world's airspace. Do not wait until that day happens; get a head start by integrating DO-178B within your legacy systems now.

By performing a rigorous gap analysis, your project team will be able to accurately assess the cost and schedule involved in developing and implementing a plan for your legacy system to receive certification. Bring in a DER early on in the development process to ensure final acceptance of DO-178B certification.

References

1. Radio Technical Commission for Aeronautics. "Software Considerations in Airborne Systems and Equipment Certification." 1 Dec. 1992. <www.rtca.org>.
2. Radio Technical Commission for Aeronautics. "Final Report for Clarification of DO-178B for Software Considerations in Airborne Systems and Equipment Certification." RTCA/ DO-248B. 12 Oct. 2001 <www.rcta.org>.
3. Certification Authorities Software Team Position Paper, CAST-5. "Guidelines for Proposing Alternate Means of Compliance to DO-178B." June 2000 <www.faa.gov/other_visit/aviation_industry/designers_delegations/designee_types/der/>.
4. "Avionics Software." *Science Daily* <www.sciencedaily.com/encyclopedia/avionics_software/>.
5. Federal Aviation Administration. "FAA Consultant DER Directory." <www.faa.gov/other_visit/aviation_industry/designees_delegations/designee_types/media/DERDirectory.pdf>.

About the Author



Paul Hicks has more than 18 years of experience leading avionics software engineering programs for DO-178B certification. As a senior programs manager for AVISTA Incorporated, Hicks has worked on a variety of avionics systems including primary flight displays, flight management systems, autopilots, and planning and execution of adapting efforts to upgrade legacy products for DO-178B certification. His specialty is in avionics systems engineering. Hicks has a Bachelor's degree in computer science from the University of Wisconsin, Platteville.

About Esterline AVISTA

Esterline AVISTA (AVISTA Incorporated®), a subsidiary of Esterline Corporation, is a full-lifecycle software engineering services company specializing in critical systems software development projects for aerospace, defense and medical electronics applications. Esterline AVISTA fields the strongest, most stable, and most capable DO-178B software development team in the industry. The company has completed more than 1,000 client projects over the last 20 years in systems design, requirements capture and analysis, software design and implementation, and software verification and validation. Esterline AVISTA, headquartered in Platteville, Wisconsin, is a SEI CMMI Maturity Level 5 rated company and an ISO 9001:2000 certified company. www.avistainc.com.

For more information about leveraging legacy software for your next project, please contact us:

Esterline AVISTA
PO Box 636
Platteville, WI 53818-0636
Phone: (608) 348-8815
Fax: (608) 348-8819
E-mail: avista@avistainc.com
Web: <http://www.avistainc.com>