

DO-254 Benefits Versus Costs

For Engineers & Managers

By Vance Hilderman



DO-254, the design assurance guideline for airborne electronic hardware, is considered by many to be a simple cut/paste of DO-178, its avionics software sibling. Surely, as with wine and beer, both are fermented liquids which become increasingly expensive with increased complexity. While similarities abound, so do their many differences. And truly, DO-254 is the benefactor, or bane, of avionics projects the world over. But is DO-254 really unduly expensive? Does it add value? Will it improve safety and reliability? Does it have benefits? What are the true costs versus benefits? These important questions are answered herein.

DO-254 is officially titled “Design Assurance Guidance for Airborne Electronic Hardware.” Until DO-254 was codified not so long ago, avionics hardware was deemed “simple” or “verifiable via systems-level testing.” Hence hardware had relatively easy certification standards, particularly compared with software under DO-178. Undoubtedly certain functionality was implemented in hardware instead of software to avoid software’s more rigorous DO-178B certification. However, today most avionics hardware at DAL Level C and higher falls under the DO-254 purvey. DO-254 evolved into the de-facto standard for commercial avionics hardware, then Military avionics and now general aerospace electronics. DO-254 requires planning, consistency, determinism, thorough requirements, design, documentation and testing, thorough process assurance, and proof of the preceding attributes. DO-254 relies upon testing to verify and validate avionics quality. But avionics quality for complex items comes from a quality process, design, and implementation, not just testing. Recently, DO-254 is being required on virtually all aircraft including civilian and new military aircraft (i.e. the A400M, one of many aircraft for which the author contributed his skills).

The DO-254 guideline presumes that hardware and software must operate in harmonic unison, each with proven reliability. Remember, before DO-254, hardware was considered “visible” and tested at the systems level with integrated software; hence hardware was exempt from DO-254 quality attributes. But that exemption resulted in functionality being moved from software to hardware for the purpose of avoiding software certification. Also, hardware complexity has evolved such that hardware is often as complex, or more so, than software due to the embedded logic within the Programmable Logic Devices (PLDs), Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs). Now, everyone recognizes that hardware and software comprise an inextricable chain with the quality equal to that of the weakest link. Hence, the mandate to apply DO-254 to avionics hardware. And the weak links are continually removed through the avionics certification evolution.

DO-254 (and DO-178C) entails five different levels of design assurance, ranging from Level A (most critical) to



Level E (least critical). Each avionics system is assigned a DAL, and each component within that system must meet or exceed its assigned DAL which is generally the same as the System DAL but under some circumstances may be lower. As the DAL increases, so does the degree of rigor associated with documentation, design, reviews, implementation, and verification. Accordingly, cost and schedule increase as well. The following figure and table depict typical actual cost deltas associated with each DO-254 DAL; note that publication CAST-27 is a must read for further clarification (Certification Authorities Software Team – memorandum #27, e.g. CAST-27).

Table: Delta Cost and Schedule of DO-254 per DAL

Level E Cost	Level D Cost	Level C Cost	Level B Cost	Level A Cost
Baseline	Level E+ 0 -15% (See CAST-27)	Level D + 20 - 30%	Level C +40%+	Same as B

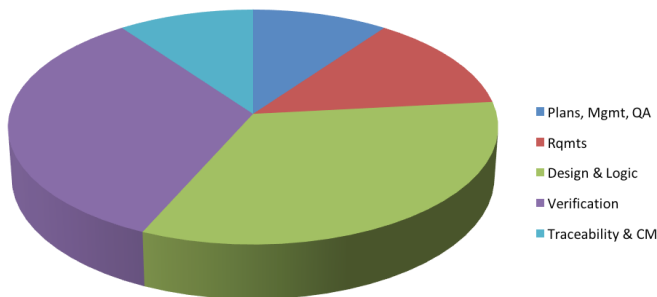
A popular myth is that DO-254 is overly expensive. As can be seen above, DO-254 clearly increases costs. But producing commercial aircraft is more expensive than experimental aircraft for a very simple reason: added costs associated with increased regulation. But those regulations undeniably improve safety and reliability. In automobiles, seatbelts and airbags likewise increase



procurement costs – and they provide no value until they do. However, DO-254 provides many benefits which is why even militaries are requiring adherence. DO-254 truly improves the probability of mission success while containing long-term hardware costs. Interestingly, but not surprisingly, DO-254 cost increases are less pronounced within companies with DO-254 experience producing a wide variety of high-quality customized silicon. Why? Efficiency greatly increases after the second or third project. Companies with a focus on quality across varied hardware product lines already implement most of the process aspects of DO-254 which also help them improve quality and efficiency across varied projects. A typical cost allocation for a Design Assurance Level (DAL) B project is shown below.

Another myth is that the most significant cost escalation occurs when moving from DO-254 Level B DAL to Level A. Untrue. The cost for Level B is the same as for Level A. What about Level C? The cost impact of DO-254 is the most significant between Level B and Level C.

Typical DO-254 Cost Allocation: Level B



Why? Level B (and thus Level A) requires the following which Level C does not and which results in Level B requiring 40% more budget and schedule than Level C:

- Adherence to standards for requirements, design and logic, and V&V
- Ensuring 100% coverage of all paths and interfaces
- Greater rigor placed upon reviews
- More rigorous configuration management and process assurance

As noted, beginning with Level B requires an entirely new additional set of certification tasks. For those more familiar with software, the DO-254 added tasks

migrating from Level C to Level B, is similar to the added tasks for software when migrating from Level D to Level C. For hardware at level B, DO-254 requires in-depth documentation and engineering tasks associated with design, logic, and verification of that logic plus independent reviews. In Level B (and A), there must be detailed hardware design verification of that design/ implementation including reviews and elemental analysis / structural coverage. Remember the DO-254 V&V equation:

$$\text{V\&V} = \text{Reviews} + \text{Tests} + \text{Analysis}$$

During requirements-based testing, the great majority (70-90%) of the DO-254 logic paths should already be executed and hence the coverage is accomplished; you merely affirm such in the traceability matrices. That coverage is satisfied because the hardware requirements, and detailed design, should have had detailed testing performed upon them which inherently would cover most logic paths. Therefore, the seemingly significant cost increase associated with Level B versus C for element analysis (structural coverage) is already mitigated by thorough requirements-based testing. And quality hardware engineering organizations already incorporate a semi-automated and streamlined process which includes independent reviews and tight configuration management; hence the added cost of those aspects for Level B is largely mollified for advanced organizations. The reader is well-advised to undergo upfront DO-254 Training and DO-254 Process Improvement to leverage these cost reduction techniques.

DO-254 also requires reviews (independent for Levels A and B) of hardware engineering processes and artifacts; this is the Validation and Verification aspect of DO-254 (see the V&V equation above). DO-254 reviews must be per approved and configured DO-254 checklists to ensure all required aspects are properly reviewed.



DO-254 Benefits.

DO-254 is not cheap, as noted above. Why then are so many entities adopting DO-254? Of course, many adoptees are forced to adopt because FAA and EASA require it. But there are also actual DO-254 benefits and DO-254 can be cost-effective, when implemented properly. Consider the following benefits of DO-254 adoption:

1. Greater upfront requirements clarity: DO-254 mandates thorough hardware logic requirements. Such detail, and the necessary discipline, force answers to be provided up-front instead of being deferred. Assumptions are drastically minimized. Consistency of requirements and their testability is assured. Iterations and rework due to faulty and missing requirements is greatly reduced.
2. Fewer development iterations: Hardware iterations, or churn, are the bane of hardware engineering. In many cases, 10, 20, and even 30 versions of evolving implementations exist on new products. Nonsense. The implementation should be largely correct the first time it is developed and should not require dozens of updates to get it right. The implementation should be reviewed by analyzing implementation versus documented requirements.
3. Fewer bugs found during testing: Since DO-254 mandates thorough and testable requirements along with design/implementation reviews, far fewer bugs will occur and the test/fix cycle should be expedited. And independent reviews further this aim.
4. Greater consistency within hardware: Hardware is like a chain – only as strong as its weakest link. Hardware which is 99% correct is 1% incorrect, which makes it unsafe. The weakest hardware component, or hardware engineer, is on the critical path of hardware safety. All hardware must be consistent per its DAL, and DO-254 enforces such.
5. Fewer defects found during integration: Integration can be a lengthy iterative process where major defects requiring design changes are uncovered and fixed. Not with DO-254, where integration is typically 50-75% faster than non-DO-254 environments.
6. Improved configuration management: The ability to control and recreate any snapshot of the project is covered by Configuration Management (CM). But CM also ensures security, backups, completed reviews, problem reporting, and version control. DO-254's strong CM requirements, coupled with modern tools which automate many CM tasks, ensure higher hardware quality now and in the future.
7. More thorough testing and traceability: Traceability assists future regression (or "impact") analysis which in turn ensures logic changes are made cleanly without unintended side effects. Traceability also assists with future requirements and/or design changes since it assists with identifying affected requirements, design and logic. Regression testing can be expensive if extensive or manual; DO-254 provides thorough traceability to determine which modules need changes or analysis and corresponding retesting.
8. Improved system and software integration: Often there is finger pointing between hardware and software teams because it takes time to determine if an anomaly was caused by hardware, software or both. With DO-254, hardware is developed more cleanly and the focus is on preventing defects versus simply correcting defects via testing; this means the hardware is of higher quality before it is integrated with software or other system hardware.
9. Fewer in-the-field defects: In-the-field defects and customer returns are hugely expensive in both the short and long term. Products developed under DO-254 have been demonstrated to achieve 80%-90% fewer defects in the field.
10. Improved reusability: Via thorough and consistent documentation required by DO-254, modularization, enforcement of documented modern engineering principles, and reviews to ensure all the above was achieved, reusability can be greatly improved. In hardware, re-usability is the holy-grail. But the reality is that unless a hardware component is at least 80% reusable (e.g. unchanged), then it is quicker and less risky to simply start from scratch. And most hardware is less than 50% reusable. With DO-254 and enforcement of design / coding standards coupled with independent reviews and traceability, most modules should be at least 90% reusable and the requisite DO-254 documentation greatly aids reusability.
11. Improved customer satisfaction: Reliable hardware begets reliably returning customers.
12. Decreased single-point personnel failures: Hardware development is part art, part science. Artists resist documenting their work and subjecting it to common development standards and peer reviews. Without standards, discipline, and modern hardware engineering principles, hardware teams devolve into a group of loosely structured rogue artists; these artists are highly valuable, creative, and talented persons. But, the loss, or deficiency, of any such artist for any reason is catastrophic to the team. Unless, that is, their work is documented, understood, and consistently applied. Therefore, DO-254 greatly reduces the possibility of such single-point personnel failures.
13. Improved management awareness of true schedule status: How many hardware projects report a "99% Complete" status week after week? How is hardware progress measured? How can management truly ascertain completion status of hardware? The answer to all these questions is via modern and accurately detailed management techniques built around DO-254. The provision for insight,



traceability, accurate status on design, development, testing, integration and reviews is found in DO-254.

14. Improved completion schedule due to the above:
“What gets measured gets done.” DO-254 provides for continuous project completion and quality reporting.
15. Wider market acceptance: DO-254 provides for a widely known proof of reliability. Safety-critical applications abound in aerospace, medical, transportation, energy and even entertainment (think amusement parks); all these fields have lives at stake and are in need of reliable safety improvements.
16. Improved differentiation vis-à-vis your competitors:
Capitalism ensures that competitors compete, which means they will continuously adopt your product’s best features thereby eroding your differentiation. The answer? Evolve your own products and differentiate them yourself. Companies, and products, that do not grow are like trees that do not grow – they are dead! Hardware and systems are dramatically growing in complexity while hardware training and engineering barely keeps apace. DO-254 is perceived to provide a defined benchmark for quality. Such a benchmark can be otherwise elusive without DO-254.

Prove your reliability, prove your quality and prove your value-added proposition: Adopting DO-254 is that proof. Far from a rubber stamp, DO-254 requires evidence. “Guilty until proven innocent” is the mantra of hardware reliability and DO-254. Prove your innocence via record keeping of transitions and checklists throughout the hardware development lifecycle.

For more DO-254 Training information (Basic or Intermediate), see:

<http://afuzion.com/avionics-training/workshops/avionics-hardware-do-254-training-class/>

For more DO-254 Gap Analysis information, see:

<http://afuzion.com/gap-analysis/>

What is AFuzion? Fun One-Minute Video:

<https://www.youtube.com/watch?v=RMzLRzcahJE>

For additional details on this white paper topic, or formal training, avionics software design, development, verification and certification, contact Vance Hilderman.

For DO-178 & DO-254 specific details, procure the book “Avionics Certification: A Complete Guide To DO-178 & DO-254”, from major bookstores such as Amazon.com. (The author of this white paper is the primary author of that book.) Also, the new book “Avionics Development Ecosystem” by Vance Hilderman covers the big-picture view of avionics development from safety, to systems, and through all key regulatory and design aspects for modern avionics development. See the Afuzion website, www.afuzion.com, for advanced training modules relevant to DO-178C beginners and experts alike.

About Vance Hilderman

Vance Hilderman is the founder of two of the world’s largest avionics development services companies. He is also the developer of the world’s first training in DO-178 and trainer of over 8,000 engineers in 45 countries in DO-178, DO-254, DO-278, and DO-200A. He is also the primary author of the world’s first and bestselling book on DO-178 and DO-254.

About Jama Software

Jama Software is the definitive system of record and action for product development. The company’s modern requirements and test management solution helps enterprises accelerate development time, mitigate risk, slash complexity and verify regulatory compliance. More than 600 product-centric organizations, including NASA, Thales, and Caterpillar have used Jama to modernize their process for bringing complex products to market. The company is headquartered in Portland, Oregon. For more information, visit www.jamasoftware.com.

