

THE AVIATION DEVELOPMENT ECOSYSTEM



**APPLYING DO-178C,
ARP4754A,
DO-254, & RELATED
GUIDELINES**

VANCE HILDERMAN
With 25+ Industry Experts



Documents
Document Sharing Hub

THE AVIATION DEVELOPMENT ECOSYSTEM

**Applying DO-178C, ARP4754A,
DO-254, & Related Guidelines**

By

Vance Hilderman

With 25+ Industry Experts

Aviation Press International

Copyright © 2021 by Vance Hilderman

All rights reserved.

No part of this book may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in reviews and certain other non-commercial uses permitted by copyright law.

ISBN: 978-1-950336-16-6 (eBook)

ISBN: 978-1-950336-17-3 (Hardcover)

This book contains information obtained from hundreds of different sources all of which were deemed by the authors to be authentic and highly regarded. Reasonable efforts have been made to publish accurate and reliable data, however the publisher and authors cannot assume responsibility for the validity of any data, materials, or the consequences of their usage. The reader is reminded that the aviation development and certification field is continually updated and no published data can be 100% accurate the following day. The author and publisher have attempted to trace copyright holders of all materials and apologize to copyright holders if permission was not obtained; if any copyright material has not been acknowledged, please write and let us know so we can correct such in any future reprint.

Aviation Press International
PO Box 811547
Los Angeles, California USA 90081

Table of Contents

[Foreword](#)

[Author's Overview & Acknowledgements](#)

[1. Introduction](#)

[2. Aviation & Avionics: Development and Certification Framework](#)

[3. Type Certificates, Technical Standard Orders, and Parts Manufacturing Approval](#)

[4. ARP4761A Aviation Safety](#)

[5. ARP4754A Aircraft & System Development](#)

[6. DO-178C Avionics Software Prelude](#)

[7. DO-178C Avionics Software](#)

[8. DO-254 Avionics Hardware](#)

[9. Aviation Requirements for Systems, Software & Hardware](#)

[10. DO-200B Aeronautical Data](#)

[11. DO-278A CNS/ATM Ground & Satellite Systems/Software](#)

[12. DO-331 Model-Based Development](#)

[13. DO-332 Object-Oriented Technology \(OOT\)](#)

[14. DO-330 Tool Qualification](#)

[15. DO-326A Aviation Cyber-Security](#)

[16. Engineering Transitions](#)

[17. Aviation Development Traceability](#)

[18. Aviation System Validation & Verification](#)

[19. DO-160 Environmental Testing](#)

[20. Quality & Process Assurance in Aviation](#)

[21. Military Aviation Compliance](#)

[22. Multi-Core Processors for Avionics Via CAST-32A](#)

[23. Aviation Development/ Certification Costs vs. Benefits](#)

[24. UAV & UAS Certification Aspects](#)

[25. Conclusion](#)

[Appendix A: Avionics Acronyms](#)

[Appendix B: Aviation System Requirements Checklist](#)

Foreword

By Woodrow Bellamy, III
(Editor In Chief, Access Intelligence: Aerospace)

*“Vance Hilderman’s ability to explain the lifecycle of planning, developing, validating, verifying, and ultimately achieving certification on safety-critical airborne software and hardware systems is evident in his latest work: **Aviation Development & Certification Ecosystem**”.*

One quote Mr. Hilderman told me in an interview a few years ago still informs my coverage today and explains how this segment of aviation will continue to evolve as an interconnected ecosystem of airplane makers, avionics suppliers, aircraft service providers and operators among others:

“Everyone wants to move up the food chain. The component producers want to make subsystems, the subsystems producers want to make full systems, the systems people want to make integrated systems. It’s incredibly dynamic.”

Vance Hilderman’s ability to explain the lifecycle of planning, developing, validating, verifying, and ultimately achieving certification on safety-critical airborne software and hardware systems is evident in his latest work. **Aviation Development & Ecosystem** is truly the capstone of his 40-year career teaching engineers who would go on to advance the concept of airborne hardware and software.

Attention new engineers reading this: There are a myriad number of new type certifications, technical standard orders and parts manufacturer approvals to develop. Tomorrow’s electric air taxis and hydrogen driven turboprops are going to require entirely new methods of measuring power and displaying it to pilots inside and remotely controlling those vehicles, as well as new human-machine graphical user interfaces. The position updates of those vehicles will need to be tracked by traditionally manned aircraft and ATM systems. And that’s just within the burgeoning electric vertical takeoff and landing (eVTOL) segment of aviation.

Artificial intelligence and machine learning are more than just buzzwords for aviation engineering circles these days, EASA specifically told me in February of last year that they expect to certify the first air transport flight control system feature AI by 2025. Here's one thing that I like to keep in mind though when I hear about or see press releases with awesome new out of this world aircraft concepts:

Today's most popular in-service aircraft flown by the most popular commercial airlines feature flight control systems must adhere to the following central principle:

A catastrophic failure event due to aircraft system failure must have a probability of occurrence lower than one in 10^{-9} — or one in a billion — for person-carrying aircraft.

That means, as it always has for aviation electronics engineers, that someone's life is attached to that every line of code, real-time operating system, data bus transmission and quality assurance process in the development of new aircraft technologies. As the industry continues to embrace never-before seen feats of engineering developments in the 2020s, use this book ***Aviation Development Ecosystem*** as a guide to the creating the future.

Over the last nine years, I have been translating technical jargon that defines advancements in aviation electronics into digestible chunks of actionable information through articles and other content for Avionics International as part of Access Intelligence LLC.

Woodrow Bellamy III

About the Author



Mr. Vance Hilderman is a 35-year avionics safety-critical engineering expert. Holding a BSEE and MBA from Gonzaga University, and a Masters in Computer Engineering from USC (Hughes Fellow), Mr. Hilderman has focused on safety-critical aviation and avionics software, safety, systems, hardware development and related technical certification solutions for his entire career. In 1990, Mr. Hilderman co-founded TekSci with Mr. Bill Hubbard which successfully became the largest independent avionics/certification software services company in the world with over 150 fulltime engineers; he served as sole CEO, President, and Chief Technical Officer for its fourteen year duration. Mr. Hilderman developed the world's first DO-178, DO-200, DO-278, and DO-254 training which engineers at 90% of the world's aviation companies have procured and has performed 170+ Gap Analysis on DO-XXX and ARP4754A/4761 to eighty-plus companies onsite in thirty countries. Mr. Hilderman has consulted for 70% of the world's largest 200 aviation development companies worldwide and his contributions are flying in most of the world's aircraft and systems relied upon daily throughout the world. He has also developed advanced technologies and solutions for ARP4761, Real-Time Operating Systems, and Multi-Core computing per FAA/EASA CAST-32A. Governments throughout the world personally request Mr. Hilderman to provide onsite aviation certification services including auditing, gap analysis, mentoring, design, and training to their personnel in the USA, Canada, Germany, Brazil, Australia, New

Zealand, Italy, UK, South Korea, Spain, Israel, and Turkey.

Mr. Hilderman was the principal founder of HighRely Inc, in 2005 and served as sole CEO, President, and Chief Technical Officer for its duration; HighRely was an aviation software/system certification company which was acquired by Atego/Artisan in 2011 with Mr. Hilderman remaining as Chief Technical Officer of Aviation/Certification Services through 2013 and retaining all copyrights to his prior works under California authorship law. Mr. Hilderman also invented and developed the first certification gap analysis for DO-178, DO-278A, DO-200, ARP4754A, and DO-254, and mentored over 75 safety-critical product companies in establishing cost-effective development for avionics projects.

Technically, Mr. Hilderman is a Systems and Software/Computer engineer, and focuses upon developing system and software requirements, design, code, and tests. He also is an expert on certification strategies for both airborne and ground-based aviation (CNS/ATM) systems. Mr. Hilderman was a scientist for Hughes Aircraft where he focused upon ground-based surveillance and radar systems with airborne interfaces. Hilderman is the principal author of the world's best selling book on avionics certification, specifically on DO-178C and DO-254 and has authored 30+ technical papers covering aviation systems and software development and certification. Professional organizations have selected him to be their sole trainer in DO-178C, DO-254, and ARP4754A including Aviation Electronics Europe, Aerospace Tech Conferences, DASC, and Society of Aerospace Engineers (SAE – the Publisher of the standards). Hilderman has personally trained over 25,000 aviation engineers worldwide, and still trains over 2,000 engineers annually in DO-XXX and ARP4754A each year while also consulting for 40+ aviation companies annually.

Mr. Hilderman believes his strengths are integrity, relationship building, communicating complex solutions, and pro-active professional leadership in motivating his company AFuzion's engineers to peak performance, all combined with continual technical innovation. Safe Skies.

Author's Overview & Acknowledgements

Writing this book seemed like such a great idea ... at the time. Like many seemingly “great ideas”, the implementation was more challenging than perceived, and there were reasons more capable persons had not followed through on a similar “great idea”: writing a single, concise book containing the most relevant information developers of tomorrow’s aviation, aircraft, and avionics need today. The real challenge was in condensing forty years of experience and thousands of pages of notes into a succinctly readable book devoid of drivel and proselytizing. Fortunately, thirty of the best senior aviation engineers I’ve had the pleasure to work with have helped to hopefully achieve that goal: this book you’re now reading.

While the “Who Flew First” debate continues (hint: Americans and our French colleagues’ opinions may differ in the efficacy of track-based launches at Kitty Hawk), everyone agrees that aviation technology is vital and its advancements amaze. Tomorrow’s eVTOL, UAM, and AI based aviation systems are a testament to today’s progress. However, aviation’s exponentially increasing systems complexity belies an equally increasing development and certification complexity. While aviation safety has been generally improving, recent multiple crash tragedies show that such increasing complexity is not easily understood or managed. Aviation projects require dozens, hundreds, and for a complex airborne or ground-based system, thousands of engineers to work simultaneously. Truly, it takes 5,000+ engineers to create a safe aircraft, but only a few to let fatal errors slip through. The only solution involves an “Aviation Development Ecosystem” which provides a playbook for each participant to understand and deploy. However, there is no official single Aviation Development Ecosystem reference guide and many agencies and groups are variously involved in defining portions thereof. Thus was born my seemingly great idea of this book: codifying an Aviation Development Ecosystem intended to be applied worldwide.

As an avionics developer, and principal founder of three of the world’s more

significant avionics and aviation development services/certification companies of the past four decades, barely a week went by without an aviation development client asking me for the location of a single repository of the information herein. When I explained that what they were looking for was as impossible to find as the fountain of youth, the common reply was, “I don’t believe it. In this day of simple access to everything digital, there simply must be a source of information, surely! I’m willing to pay – where can I buy such a book containing all this information?” Silence ...

Indeed, after several years of searching for the true fountain of youth, I’m sure the intrepid, though overly optimistic, explorer Ponce de Leon likewise would have been willing to pay for knowledge of the Fountain’s exact location. But even today we’re at the infancy of the digital age. Truly, I’ve no doubt that within a decade or two, AI and Cloud technology will have evolved to enable a quick search of the entire known digital world yielding a customized “book” clarifying all the topics contained in this book. But will that information be distilled and accurate? And in a format allowing the reader to truly understand the What, Why, and How of aviation systems development and certification?

No book can be all things to all people; humans are simply too diverse in their knowledge, needs, and capabilities. So as an author developing, gathering, soliciting, distilling, compiling, and writing the information herein, I have invoked the “80% Rule” which I cite at the beginning of my aviation development training classes provided to over 25,000 aviation students worldwide: “If 80% of this information is 80% useful to 80% of the students, then I’ve achieved 100% success as a teacher.” Best case? Hopefully. Real life? Absolutely.

This book is truly the result of thousands of hours of hard work by many people. Sometimes exciting, many times less so. But always interesting. Those contributor’s and reviewer’s knowledge spans over five hundred person-years of learning which is considerable, particularly with the realization that the commercial aviation industry itself is little over one hundred years old. A sincere “Thank You” is due each of the many persons involved in this book. And to the readers: if you can simply contribute your best efforts to making aviation just a little better, a little more predictable, and

a little safer, then that is more gratifying than a formal thank you. If you have any comments or recommendations for future issues, you can always contact me; finding my contact information will take you less than one minute but we'll make the spammers work a little harder for that.

Again, this book would not have been possible without the direct and indirect contributions of so many people. A heartfelt thank you to my family who experienced more than a few evenings and weekends sharing ideas about content and context. A large thank you to Emilie Mandic and Anna Hilderman who helped to edit early versions of these chapters. A big thank you to all the technical contributors and reviewers whose expertise is reflected within these pages. A huge thank you to 300+ clients and technical colleagues of mine who informally reviewed early chapters and provided feedback. And a very special Thank You again to the formal Chapter Reviewers, and in some cases Authors, cited below; your hundreds of comments and additions were mostly all incorporated, and this book is far better because of you.

Again, I would like to personally acknowledge and thank the many formal expert technical engineering reviewers and contributors involved in this effort: they are all pillars of modern-day aviation and this world is a better, and safer, place because of them. And a huge Thank You to my beautiful wife Colleen Hilderman, whose outer beauty is surpassed only by the inner – you are an inspiration to us all. And four of our six children (Anna, Emilie, Evan, and Dan) who helped edit or review portions of this book – you are appreciated and loved, as are the other two (Carson and Kaitlin) who somehow miraculously were otherwise engaged when early reviewing was needed.

To all the above: thank you for having spent the extra time so the readers benefit from your many inputs. It is no easy matter to succinctly clarify complex subjects and it would have been far easier to simply make yet another one thousand page technical diatribe which no actual working persons have the time or desire to read.

Safe skies,

Vance Hilderman

CEO & CTO, AFuzion Inc. www.afuzion.com

- Bachelor's Degree Electrical Engineering, *Gonzaga University*
- Master's Degree, Electrical/Computer Engineering, *University of Southern California (USC)*
- Master's Business Administration (MBA), *Gonzaga University*

Special “THANK YOU” to the formal Chapter Reviewers & Contributors cited below:

Technical Contributors, Alphabetical Order:

1. Mr. Mark Brown, Senior Architect, Lynx Software
2. Mr. Aharon David, Cyber-Security and Aviation Expert, AFuzion-Infosec
3. Mr. Jon Lynch, FAA DER, AFuzion
4. Mr. Greg Wilson, FAA DER

Technical Reviewers, Alphabetical Order:

1. Mr. Brian Allen, Staff Software Engineer, Sikorsky - a Lockheed Martin Company
2. Mr. Don Coleman, FAA DER
3. Mr. Bunyamin Coskun, Project Manager, Milsoft Inc.
4. Mr. Kevin Crozier, Senior Avionics Software Engineer, FAA Consultant DER, FAA Certified Flight Instructor and Commercial Pilot.
5. Mr. Bill De Leeuw, FAA Designee, Systems and Equipment, Software
6. Dave Deloria, Director of Engineering, Crane Aero.
7. Mr. Eric Dillaber, Development Manager, Simulink Certification & Standards
8. Dr. Bruce Douglass, Chief Evangelist, IBM Internet of Things
9. Ms. Gamze Eroglu, Former Senior Certification Specialist, STM

10. Mr. Marc GATTI, Thales AVS France SAS Scientific Director
11. Ms. Nazan Gozay Gurbuz, Taos Safety Expert, & ARP4754A/4761A Committee Member
12. Mr. Francois Guay, FAA DER
13. Mr. Alan Houpp, Independent DO-160 Expert
14. Mr. Kevin Kendryna, Quality Engineering Leader, General Atomics
15. Dr. J. Lee, Avionics Manager and Colonel Korean Air Force, Retired
16. Mr. Russell McMullan (Former Technical Director – BECA)
17. Mr. George Meier, FAA DER
18. Mr. Vincenzo Mirra, Aerospace Quality & Certification Manager, Leonardo Company
19. Mr. Roger Plieske, Rohde & Schwarz
20. Mr. Bill Potter, Technical Marketing Manager, The MathWorks
21. Mr. Tom Roth, FAA DER
22. Mr. Antonio Silva (MSEE, PE), Head of Software Engineering at AgustaWestland, Compliance Verification Engineer for SW and AEH
23. Mr. Carmelo Tommasi, Software Modeling Expert, AFuzion
24. Ms. Lisa Wynn (Duncan), Software Quality Engineer, M.A., CSQE.

1

Introduction

“It was a dark and stormy night ...”

Wait. This book is about making sense of the aviation development landscape and the myriad associated “standards”. What is the pre-aviation cliché “dark and stormy night” from 1830 doing as the opening sentence here? Simple: If you have had pilot training like myself, then you know that dark and stormy nights are rarely your friend. The same is true for developers of critical aviation and avionics systems: working in a dark cockpit, and unexpected rainy-day scenarios, are never your friend. But in aviation, as in life, we can choose our good friends but never escape exposure to potentially bad influences. The difference between a good outcome and a bad outcome is based on our choices. But making good choices requires great knowledge. And experience. In aviation, there is no substitute for experience: you need it and until you have it, you are at best a “co-pilot”.

Fortunately, pilots and aviation developers alike have access to “friends” which lessen the impact of dark storms. What friends? Aircraft have increasingly advanced airborne avionics and ground-based systems, and that equipment is developed utilizing the guidance explained in this book. Combined, the darkness is illuminated and the storms tamed. Easy, right? Not at all: friends need to be close at hand to be helpful and you need to know how to work with them.

However, one challenge remains even when you have good development friends. It’s a “challenge”, not a “problem”, because challenges are problems with solutions. Quick, what’s the solution? Ahhh, we’re getting ahead of ourselves. In these days of advancing digital access and dexterity, the tendency to try for quick solutions without fully understanding the problem ecosystem permeates daily lives. First, what is the challenge? Well, that is not a simple question either because there are multiple challenges within the dark and stormy night of aviation systems development, including:

- *Every aviation system is different from every other system*

- *The Guidelines are just that: generic guidance lacking easy-to-understand objectives, clarity, or methodology*
- *There is no “one size fits all” optimal approach*
- *There is no external recipe for success, so failures of quality, cost, and schedule, are common.*

Given this non-trivial aviation landscape with multiple challenges, we need to find our friends, and quickly. We need to make sense of myriad aviation guidelines, standards, memorandums, and policies. Every aviation engineer must readily understand how the aviation development ecosystem applies to their unique situation: the aviation systems, aircraft, hardware, and software they are developing.

It's a good bet that most readers of this book have had advanced mathematics courses where similar confusion existed during early coursework. Remember those days? Students didn't want to raise their hand and ask a question, because it seemed all the other students understood; each thought they were the only one having difficulty. Now one realizes those other students were just like them: they had the same textbooks and they too were still in the dark. As an avionics and aviation professional with thirty-five years' experience consulting on 500+ aviation projects in 30 countries, I personally assure you everyone has challenges; most of them think they have problems, and very few problems have perfect solutions.

It may be the reader is smarter than their peers (after all, they acquired this book) but they still had challenges. They are also smart enough to know there is no single Rosetta Stone with which one can decipher the code to developing projects with minimum cost/schedule and still obtain maximum quality and safety. There are no free lunches, not even in government or corporate free lunch programs: someone paid. But almost everyone has competitors, and those competitors have the same challenges, perhaps even “problems”. With this book, I hope to harness the knowledge of almost four decades' experience and in the process convey a useful portion of the knowledge passed along, as I personally trained over 25,000 aviation engineers and 500+ employees how to achieve engineering and certification success. This book is about providing knowledge so you can become a better

co-pilot and ultimately a good pilot of your aviation success... possibly even Great.

What makes a technical book “good”? That is an impossibly difficult question because the answer is within the eyes of the beholder. It is a certainty that every reader of this book has different needs, different questions, and differences within the ways they learn. Indeed, it’s impossible to be all things to all people. But if 80% of the readers find that 80% of the knowledge garnered herein is 80% helpful to them, then I’d say the result was simply as good as it gets. Clearly, it would be easy to simply rehash the published guidelines, e.g. DO-178C, DO-278A, ARP-4754A, etc. Or, rehash DO-248C which is supposed to explain DO-178C. But you’ve probably already perused those documents and found them lacking. Why? They’re general-purpose guidelines whose purpose is codifying guidelines for aviation and avionics system development. What’s missing is layman explanations and integration of an overall aviation **ecosystem** relevant throughout the engineering lifecycle, provided within the context and best-practices of our real-world. That ecosystem includes the relationship and transition from aircraft and system safety to software/hardware safety. Not theoretical classroom musings, but real-world understanding because that is your world: the real world. Let’s take off on a successful learning journey by starting our engines ...

2

Aviation & Avionics: Development and Certification Framework

By Vance Hilderman

Reviewed by:

- Mr. Francois Guay, FAA DER
- Mr. George Meier, FAA DER

Aviation development is important to people for whom aviation development is important. Who are those persons? Developers, manufacturers, integrators, flight crew, airline operators and simple enthusiasts wholeheartedly agree on the importance of aviation. Who should pay attention to this book? Simple: everyone with involvement in the aviation development ecosystem. Passengers will also agree once they realize their safety is in the offing.

Hundreds of years ago, before the concept of Da Vinci's flying machine sowed the seeds of subsequent balloons, gliders, and airplanes, humans were by necessity jacks-of-all-trades. The average earthling required working knowledge of weather, farming, animal husbandry, building, and childbirth. Over time, mankind developed specialization as a pragmatic expediency: productivity improved when individuals could concentrate on their individual skills. Guilds, trade unions, governments, and regulations evolved which, for better and for worse, improved the average person's quality of life.



One outcome of the evolution toward specialization was the decoupling of usage from design knowledge. No longer did the farm implement user need to know how to design a particular farming tool; he placed some trust in the maker based upon their relationship and the price paid. Thus were sown the seeds of the modern ethos ... and then came modern airplanes.

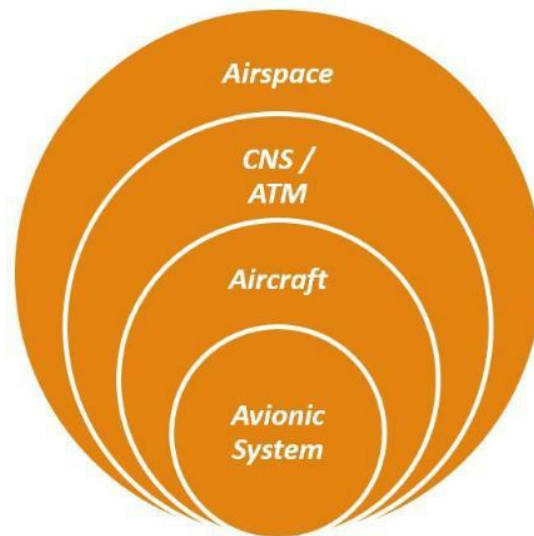
Aircraft, and flying objects in general (balloons, missiles, and unmanned aerial systems) represent hazards above (no pun intended) and beyond that of farming implements: a broken farming tool simply slows down the farming until the tool is fixed. A broken aircraft can have greater repercussions: the slowing of life can be permanent. As a result, governments and developers came together to codify safe foundations for the development and certification of aviation components and systems. The players were almost always well-intentioned but faced challenging trade-offs: over-regulate and both competitiveness and innovation would be sacrificed with the end result of decreased safety. Under-regulate and safety would be compromised with potentially disastrous results. A quandary; what to do?

Everyone wants safety if for no other reason than selfishness: everyone flies or has the potential to be struck by falling aircraft. But the aviation industry is one of most pragmatic and least selfish entities around (at least, in this author's opinion, as compared to banks, governments, lawyers, and politicians). For the aviation industry, safety is good for health AND for business. There is nothing like a bad aircraft accident to dampen flying enthusiasm and business prospects (think Concorde: one of the safest (and most beautiful) aircraft until the first ever crash in 2000 grounded the fleet permanently).

Fortunately many smart and savvy people spent decades defining a protocol for aviation safety. Whereas worldwide protocols exist for other manmade endeavors including peace-keeping (United Nations) and banking (World Bank and IMF), most would agree that aviation safety organizations are the most effective irrespective of cost. The aviation safety framework is generally well funded, science-based with a modest amount of politics, and within the western countries at least has reasonable cooperation and support of the aviation industry. This is not to say all is perfect; not at all. There are notable instances of politicking, nationalism, and some powerful concerns leveraging that power for their principal benefit. Areas of contention in aviation include CO₂ emissions, pilot work rules, noise abatement, over-flight fees, increasing congestion, airline ownership rules, and transatlantic regulation harmonization. The rise of Asia, both as an economic force and an aviation participant, is mandating additional coordination to resolve related challenges. But overall the aviation safety framework is workably intact. So

what is that framework? The following figure depicts aviation's safety layers:

- **Airspace** deals with flight planning, sector and national boundaries, and control of numerous aircraft/operations simultaneously.
- **CNS / ATM** (Communication, Navigation, Surveillance / Air Traffic Management) deals with ground and satellite-based activities relevant to aircraft and flying safety.
- **Aircraft** deals with the safety aspects pertaining to a single aircraft.
- **Avionic System** pertains to safety aspects of an avionics system where an aircraft is comprised of many such avionic systems.



As the above diagram depicts, “safety” is about the entire aviation ecosystem not merely certain aspects. Avionics developers often like to think of themselves as being on the top of the food chain. But as the above diagram clearly depicts, avionics systems are at the bottom. Why? It’s about the aviation ecosystem which is simply bigger than any one system or even any one aircraft.

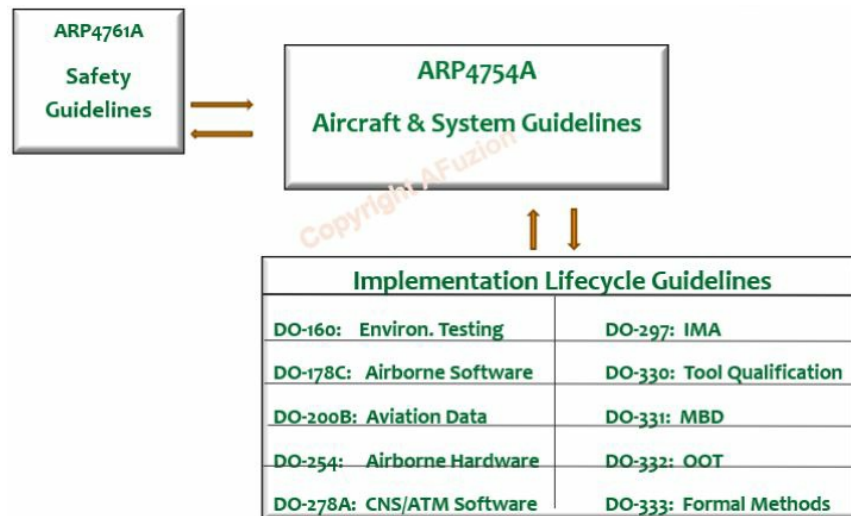
Clearly, some aspects of the aviation safety ecosystem have a greater contribution to safety than others. But if you were to ask an aviation safety expert “which aspect of aviation safety is the most important?” the answer should be “All of them”. In other words, while certain aspects can have a greater influence on safety or require more rigor, all aspects within the aviation safety ecosystem are important. But wait, that’s not the way modern

human brains operate in today's world, everything must be ranked. Think about that; have you ever caught yourself thinking about your weight, height, fitness level, hours of sleep, golf score, bank balance, calories, social media connections, or salary? Congratulations, you're normal. But aviation safety is about an ecosystem which defies simple ranking because each aspect contributes to safety and is thus individually important.

Another way to look at aviation safety is to consider a simple chain. Aviation safety resembles this chain because each link contributes to the function, and the reliability, of the chain. Want to find the chain's weakest link? Easy: simply increase tension by pulling on each end until the chain breaks. Where does it break? At its weakest link. So if a chain had one hundred links, like a modern aircraft can contain over one hundred avionics systems, the chain is only as strong as its weakest link. There is no safety benefit to having ninety-nine links of the chain extra strong with one link being weaker than necessary.



Aviation safety is about defining the “strength” or reliability of each aspect of the aviation ecosystem, with the realization that overall safety is about many different aspects and their interrelationships. Aviation safety cannot be assessed by simply stressing the system until it crashes: aviation safety is about avoiding, not causing, crashes. Therefore, aviation safety must be based upon a scientific approach which uses many techniques including analysis, engineering, process, and standards. Airspace, communications, aircraft, systems, and components are all important, but each represents a different view which must be considered within the safety evaluation process. With each of those views are numerous criteria that contribute to safety; each criterion is important though the individual contribution to safety can differ. (This leads to a discussion of Development Assurance Levels (DALs), commonly referred to as criticality levels, which will be dealt with most thoroughly in the ARP4761/A Safety section herein.) The overall aviation certification framework is depicted in the following figure:



Aviation Certification Ecosystem

As shown in the above figure, aviation certification starts in the upper left with an ARP4761/A-based safety assessment regime. The aircraft and avionics systems architectures are defined along with safety requirements which are fed into the ARP4754A-based aircraft and system development and certification process. Then, underlying avionics system aspects are dealt with via the various “DO-XXX” guidelines, where “DO” simply means North American Document. Europe has a similar ecosystem but the above documents are instead designated “ED-XXX” where “ED” means “European Document”. The remainder of this book is devoted to technical introductions and dissection of each of the above documents to explain their role within the aviation development and certification ecosystem.

Designing and certifying aviation systems has some resemblance to designing and building the links of a chain: the builder must know the purpose of the chain and how strong it is expected to be. Without that knowledge, the builder will make the link either too strong which wastes resources or too weak which causes that link to break prematurely. Either outcome is considered a failure. In avionics, the layman might think it normal to simply build it to be as close as possible to perfection with the highest possible reliability. There is no such thing as “perfection” within the realm of complex systems. Without a defined minimum level of operational reliability and integrity, there would be no way to determine if the system is “good enough”. Reliability without safeguards does not fully address product assurance and

how failures occur and what the system-level effect of such a failure is. If a chain fails, what is the impact upon the operational system? Reliability itself simply gives a failure rate: how it fails, with grace or not becomes an issue. A link in the chain may fail, but how it fails, and the impact of that failure is what causes a bad day from a safety perspective. Thus, there needs to be a dimension of integrity as we cannot simply “rely” upon reliability. Every widget designed and built is imperfect to a degree. When that combination of imperfections aligns in a “Murphy way” is what safety is supposed to identify. Therefore, avionics development becomes a study in the Avionics Development Ecosystem, e.g. this book.

In a truly free marketplace without safety-based regulations, cost and quality would continually be decreased until the link in the aviation safety chain broke, with disastrous results. Instead, avionics systems are analyzed to provide insight into the result of failures upon aircraft and human safety. Then, the relationship of that system’s correct operation to overall safety is determined and assigned a minimum threshold level for reliability: engineering techniques are then employed to ensure the necessary rigor is applied based upon that minimum reliability and integrity level.

A note on aviation development/certification cost versus safety.

Avionics development is not cheap; it’s almost always more expensive to develop products with provable quality attributes versus those without. A common worldwide misconception implies that avionics development is expensive because of the over-burdensome development process and certification considerations. There is no doubt the rigorous development and certification requirements increase initial costs; it’s impossible to be otherwise. However, that common refrain overlooks the two key questions associated with avionics development costs:

1. Given the importance of safety within aviation, are the cost increases associated with avionics development and certification excessive?
2. Are economies of scale really possible in an industry where successful projects yield hundreds of units sold versus consumer electronics where success is measured in the millions of units?

Clearly then, these two questions heavily influence the cost-versus-benefit arena if not changing the game altogether. As with politics and pizza, there will never be total agreement on these two questions. But what everyone does agree with is the following: avionics development can never be cheap, but it is possible to be cost-effective. Also, aviation is a market which perhaps more than any other places an emphasis on quality over cost: a cheap product with failures, high maintenance, or frequent replacement is neither cheap nor cost-effective. Have you ever bought a cheap tool only to be dissatisfied with its performance and replacing it with a more expensive competitor later? That situation is highly relevant in avionics, where product development costs can be in the millions of dollars and unit production costs can be in the tens of thousands.

Aircraft themselves epitomize the very definition of trade-off: cost, fuel-consumption, and payload are inextricably woven together. This explains why today there are hundreds of different new aircraft models currently for sale: each type is well suited for a particular need but incurs trade-offs versus other types. Increase payload and you increase purchase cost and operating cost. Decrease payload and you save fuel but can carry less payload with an adverse effect on revenue. And each category typically has several competitors which explains why hundreds of different aircraft models are currently for sale.

As with cost, avionics safety has a similar relationship. Additional reliability, or safety, can be added but always at additional cost. For example, developing back-up airborne satellite communication systems as if they were thrust reversers would significantly increase cost with little, if any, increase in overall safety. Again, it is a matter of trade-offs. So aviation safety blends both art and science, and the science includes a cost/benefit analysis of each proposed safety related aspect. With unlimited time and budget, safety can always be continuously improved. Consider old military aircraft with eight engines. Why eight? Because “surely” eight must be more reliable than six, which is more reliable than four, which is ... And how many engines does the world’s most modern fighter aircraft in production today have? The F-35 Joint Strike Fighter has one engine. Exactly. Meanwhile, consider the Fly-By Wire (FBW) example: conventional cable and pulley systems were replaced by FBW at what cost? Simplex (single channel) electronics and actuators

typically won't meet safety requirement, so architectures need to double, then possibly triple and sometimes quad to meet safety requirements. This geometrically increases cost, weight, complexity, and of course the cost. So within the entire avionics development ecosystem, pragmatic attention is paid to cost.

A Final Word Before Diving In ...

At the end of the day, there are no projects with unlimited time and budget. Avionics are called avionics because they must support flight and they must meet the safety framework that is explained herein. The following material provides the insights necessary to successfully navigate the cost/benefit trade-off route while still achieving sufficient safety.

3

Type Certificates, Technical Standard Orders, and Parts Manufacturing Approval

By Vance Hilderman

Reviewed by:

- Dr. J. Lee, Avionics Manager and Colonel Korean Air Force, Retired
- Mr. Antonio Silva (MSEE, PE), Head of Software Engineering at AgustaWestland, Compliance Verification Engineer for SW and AEH

So you understand that airborne electronics are part of a safe system, and guidelines exist which must be followed during the engineering lifecycle. Now you're ready to start designing the avionics system ... Not so fast! First, you need to know complete answers to the following questions (hint: the answers are embedded within an understanding of TSO's, TC's, STC's, and PMA's).

- a. Can you normally start developing an avionics system without knowing what type of aircraft it is to be installed on?
- b. Are there any specific standards which are based upon the functionality of the avionics system?
- c. If an avionics system was previously certified for one aircraft, must you always recertify it for a different type of aircraft?
- d. Can any high-quality manufacturing facility be used to produce the avionic units?

If you said “No”, “Yes”, “No”, and “No” to the above four questions, then you have at least some basic knowledge of TSO's, TC's, STC's, and PMA's. Regardless, the context for answering these fundamental questions is an important facet of understanding the avionics development ecosystem.

For commercial avionics, safety of flight is paramount. Perhaps nowhere in the avionics ecosystem is the interdependence of those safety aspects seen via an Airworthiness Pyramid with four building blocks, as depicted below:



And just like a pyramid, the airworthiness pyramid has a foundation with subsequent blocks placed upon each other. First, what is “airworthiness”?

Parts Manufacturer Approval: Combined design and production approval for modification and replacement items. It allows a manufacturer to produce and sell these articles for installation on type certificated products.

PMA

“Airworthiness” is the provable ability for an aircraft to operate safely while performing predefined functionality. When airworthiness is proven for a commercial aircraft, an airworthiness certificate may be granted. The FAA defines an airworthiness certificate to be an “FAA document which grants authorization to operate an aircraft in flight” (www.faa.gov). To receive an airworthiness certificate, FAA Order 8130 states that both of the following two conditions must be met:

- a. *The aircraft must conform to its type design. Conformity to the type design is considered attained when the aircraft configuration and the engine, propeller, and articles installed are consistent with the drawings, specifications, and other data that are part of the TC. This includes any supplemental type certificate (STC) and repairs and alterations incorporated into the aircraft.*
- b. *The aircraft must be in a condition for safe operation. This refers to the*

condition of the aircraft relative to wear and deterioration, for example, skin corrosion, window delamination/crazing, fluid leaks, and tire wear , and any outstanding airworthiness directives (AD's).

The Airworthiness Pyramid thus has the following four building blocks, summarized below with more detailed explanations to follow:

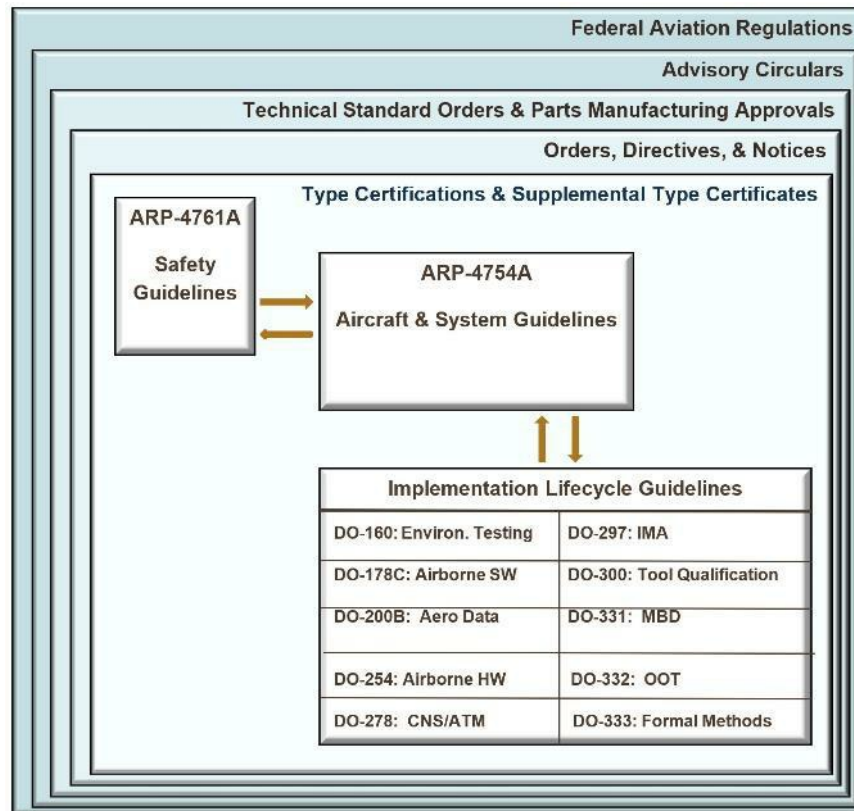
Airworthiness Pyramid So the Airworthiness Pyramid has four essential, integrated building blocks which are discussed in more detail below.



Airworthiness Pyramid

Remember: The Aviation Development & Certification Ecosystem

Remember, in avionics development it is all about the “ecosystem”. Here again is a pictorial view of the key aspects of that ecosystem. Which aspect is most important? Yes, they all are. Like a chain, the system is only as strong as the weakest link. The following figure depicts the aviation development and certification ecosystem:



The Details: TC's, STC's, TSO's, and PMA's ...

First, what is the formal regulatory basis for aircraft and avionics certification? The fundamentals are contained in Title 14 of the US Code of Federal Regulations (CFR) Aeronautics and Space, Parts:

- 21 (Certification Procedures for Products and Parts)
- 23 (Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes)
- 25 (Airworthiness Standards: Transport Category Airplanes)
- 27 (Airworthiness Standards: Normal Category Rotorcraft)
- 29 (Airworthiness Standards: Transport Category Rotor Craft) and the applicable amendment levels which typically define the primary basis for certification)

Type Certificate (TC).

The Type Certificate, or TC, forms the foundation of airworthiness, since it

affirms the soundness of a particular, specified manufacturing design. Harking back to the pre-digital age, a TC is just that: an actual “certificate” which is issued by a governing entity (FAA, EASA, CAA, etc.). However, a TC is more than a simple certificate as it specifies the applicable associated certification criteria which vary based upon the type of item being approved and the current regulatory requirements (including the applicable amendments to regulatory requirements). The TC includes or references sufficient information to demonstrate that the design being approved complies with the “applicable” airworthiness requirements. What are “applicable” requirements? Each type of aircraft or equipment has specific sets of requirements which apply to them. The set of requirements varies according to type, but commonly includes TSO’s, and compliance to DO-178C (software), DO-254 (airborne electronic hardware), DO-160 (environmental/EMI), etc. The TC includes a TCDS identifying the type design, operating limitations, Type Certificate Holder, Make and Model, and also specifies the applicable regulations or restrictions imposed by the certifying agency (including regulations amendment levels). For components, only engines and propellers are eligible components for TC’s. The TC is the foundation for subsequent approvals such as production and airworthiness.

There are really two key reasons Type Certificates form the foundation of airworthiness:

1. TC’s specify the applicable rules which apply and were affirmed for each item; and
2. TC’s are required prior to actually manufacturing that item.

TC Certification Plan.

As with building a house, it’s very difficult to prove compliance with building standards if the inspectors are not involved before and during the building process; that is why most buildings require a plan review prior to building, then incremental reviews as the foundation, walls, electrical, and roof are installed. Same for aircraft and avionics included as part of the TC. TC applicants must submit a detailed certification plan to the certifying agency and involve that agency or its designee throughout the project. What information is contained in a certification plan? Sufficient information to show

the applicant has a thorough understanding of the applicable regulations to enable verifiable implementation of a safe design. Specifically, the Type Certificate certification plan should detail the following information and be approved by the certification authority prior to entering the engineering implementation (actual development) phase:

- Specific information describing “who” is applying, date, and configuration identification;
- Description of design (or design change, particularly for STC (see below)) including sufficient detail in schematics or diagrams to show engineering safety;
- Operational environment, assumptions, constraints, and limitations;
- Certification basis, including applicable regulations (ARP-47XX, DO-XXX, etc.) Parts 23, 25, 27 or 29 for instance (other parts maybe applicable depending on the aircraft);
- Description of, and suitability for, showing compliance and how the configured artifacts will be used to affirm;
- Document list to be submitted which includes all required artifacts based upon the applicable regulations;
- List of test articles used to generate compliance data including any special instructions or characteristics;
- Description of how the continued operational safety requirements will be met after the TC is issued;
- Proposed project schedule showing key milestones, including all activities which require certification agency oversight or witness; and
- If FAA involved, identification of all DERs, DARs, DMIRs, and ODARs intended for use in the certification project along with areas of responsibility and capacity.

The TC applicant submits the documents to their local aviation regulatory agency and that agency provides feedback via an iterative process until the plans are approved. Then the applicant follows the plans with regular auditing of progress by the certifying agency or representatives. Just as with building a

house, inspections are incremental to allow early visibility into progress versus plan and analysis of any deviations. It should be noted that in actual practice, the submittal of plans is usually linked to the formal application for TC by the Original Equipment Manufacturer (OEM). This happens when the A/C is considered at a maturity point (verified also in experimental flights, authorized by “permit to fly” processes) giving confidence about the achievement of certification at a certain date. This is the typical process for a TC. The process for TSO/ETSO is different, since the submittal is to an ACO or EASA in front of the regulation, and it is independent from the certification of a given aircraft. A certified aircraft can be used as the “testbed” for the specific avionics being submitted.

In Europe, the submittal is done directly to the EASA proper central directorate (depending on the type of Aircraft), then EASA defines a Program Certification Management organization and the specialist Panels, one per specialty, which may include specialists from their central offices and/or applicant’s National Aviation Authority specialists. If the applicant has been granted a Design Organization Approval (DOA) and has appointed Compliance Verification Engineers (CVE) for the different specialties, EASA also defines its Level of Involvement (LOI) in the auditing process of each auditable subcomponent. The CVEs perform the auditing process in any case, with EASA specialists participation as per the LOI. An Aircraft TC is usually “validated” by national Airworthiness Authorities when sold to a Customer willing to fly in nations other than the USA or European Union. Validation between the USA and EU are facilitated by the bilateral agreements underwritten between the FAA and the EASA.

Since aviation regulations are undergoing continual revision, what happens to certification projects when the regulations change? To avoid a seemingly endless cycle of project updates to meet evolving regulations, the regulatory basis is considered “frozen” for a reasonable period of project implementation. Thus the regulatory requirements cited in the approved plans become the basis for the TC even if those regulations change before the final certification is completed (note there are exceptions to this). This usually precludes the situation where an applicant would have to change the design just because an unforeseen regulation change happened.

Design Changes.

“There are only two types of avionics designs: those that have already changed, and those that will.” (Vance Hilderman – 2014)

Commercial Aviation is barely a century old and evolution is continuous. Evolution means change. Change means some form of re-certification. What happens when a change is desired for an already-approved Type Certification (TC) design? Typically there are three possibilities:

1. Simple re-cert, where the change is considered Simple and doesn't require extensive analysis of safety implications due to the change (modification to the TC). The classification of the change is solely dependent on the potential safety effect. Example: addition of an HF radio, when keeping the standard two VHF radios active and installed. In such a case only the installation and EMC/EMI rules need to be verified: an extra HF radio is considered a “no hazard” equipment as far as its operation does not affect other equipment within the TC configuration. Note that re-cert can be done for Minor and lower changes by the TSO owner or by a TC holder with a Design Organization Approval (DOA). All other cases require re-cert with involvement of the Certification Authority.
2. Re-certification via a Supplemental Type Certificate (STC) where the change may not be simple, but it doesn't introduce new designs with associated safety considerations. Current understanding for an STC is “additive” to an existing TC, i.e., building “on top of” an approved design, typically adding functionality to avionics or “kits” to an Aircraft configuration. An STC is applicable to specific identified Aircraft serial numbers.
3. Create an entirely new design and repeat the certification process but use (leverage) many of the pre-existing artifacts (previously developed type design data). This is applicable to avionics, but not at the Aircraft level (there is only ONE TC for a given Aircraft, if you do another TC, it is by definition another aircraft type (this is why the TC is a Type Certificate).

Clearly, aviation safety would be maximized by always starting over and

creating a new design, correct? Absolutely not: starting anew simply allows new mistakes to creep into an all-new design while also becoming so expensive as to dissuade new safety-related capabilities from being incorporated. If the change is particularly simple, option #1 above is the simplest choice. If the change may introduce new safety risks not considered in the previously approved design, the certification entity may require the onerous option #3 above. But if the change can be managed within the previously approved safety context, then an STC may be used as described below.

Type Certificate Validity.

The holder of a TC must keep the TC valid by continuously following airworthiness directives (AD's), managing service bulletins, and providing technical support as required (and almost always charging for such). This is commonly referred to as “supporting the type” and often continues after the item has ceased production (and the same rules apply to Supplemental Type Certificates described below). If the TC/STC holder stops supporting the item, the certificate is relinquished back to the certifying agency and usage of that item is then disallowed for commercial aircraft operations.

Supplemental Type Certificate (STC).

An STC is a Type Certificate, but for an item which has a previously approved TC following a modification to that item. When the manufacturer shows the modification does not introduce risks not considered in the original design, that manufacturer typically requests an STC instead of an all new TC because an STC is less work than an all-new TC. The STC details the nature of the aircraft design change and how the modification affects the previously approved design including application of existing regulations. The scope of an STC can vary widely, depending upon the nature of the modification. An STC is the typical vehicle by which new avionics systems (appliances) are installed on an aircraft that has current and active TC. The aircraft installation will require the design and alteration of the aircraft so that the subject appliance can be installed on the aircraft. Like the TC process, a certification plan (Project Specific Certification Plan – PSCP) is developed and this plan defines the STC plans and certification basis. Typically STC projects follow a prescribed process: Planning (PSCP),

installation design, installation, pre-certification testing, type inspection authorization (TIA) including flight test risk assessment, installation conformity, formal (for certification credit) ground testing, and formal (for certification credit) flight testing. As part of the STC process an Experimental Airworthiness Certificate (EAC; or Permit To Fly (PTF) as it's called in Europe) may be issued prior to conducting the formal TIA, including conformity, ground and flight testing. Compliance to the regulatory requirements is substantiated by developing a series of documents to that demonstrate compliance, the following is a typical list of documents developed for an STC project:

1. STC Application
2. Project Specific Certification Plan (PSCP)
3. Conformity Plan
4. Master Data List (MDL) (DER 8110-3 approving this document)
5. Human Factors aspects of Certification Plan (HFCP) (as required)
6. Instructions For Continued Airworthiness (ICA)
7. Airplane Flight Manual Supplement (AFMS) (DER 8110-3 recommending approval of this document)
8. Certification Compliance Matrix Check List (DER review)
9. EMI/RFI Ground Test Procedure and Plan (DER 8110-3 approving this document)
10. Ground Test Function Test Procedure and Plan (DER 8110-3 approving this document)
11. Flight Test Plan Test Procedures and Plan (DER 8110-3 recommending approval of this document)
12. Request for Type Inspection Authorization (TIA)
13. Wiring Diagram
14. Installation Instructions
15. Wire Routing
16. Wire Harness Drawing
17. Equipment Installation Diagram
18. Electrical Load Analysis
19. Special Conditions / Issue Paper (only require for unique, novel, or STC which require compliance in areas not currently controlled by FAA regulations)
20. Installation Kit List

21. Placard Drawings
22. Structural Substantiation Report
23. Weight and Balance
24. Supplemental Flight Test Report (post TIA) (DER 8110-3 approving this document)
25. Supplemental aircraft conformity inspection
26. System Safety Analysis (SSA) (aircraft level) (DER 8110-3 approving this document)
27. Mechanical / Structural Drawings (as applicable)
28. Pitot / Static Drawings (as applicable)
29. Aircraft Experimental Airworthiness Certificate aircraft owner authorization letter
30. Aircraft Experimental Airworthiness Certificate program letter
31. Application for Experimental Airworthiness Certificate (8130-6)
32. Installation Conformity and Statement of conformity (8130-9)

Typically most, if not all, of the data items listed above will need to be developed by the STC applicant in order to substantiate compliance to the STC regulatory requirements. The applicant for an STC can be the owner of one or more Aircraft, or even a separate organization, typically a major Avionics Supplier, not necessarily the same as the original TC holder. In some instances the rigor and effort required to comply with the STC certification requirements for a Part 23 aircraft (Normal, Utility, Acrobatic, and Commuter Category Airplanes) as compared to that of Part 25 aircraft (Transport Category Airplanes) is less thus requiring a reduced level of effort. Once the entire STC certification compliance package is completed and submitted to the regulatory authority the final processing of the STC can be completed and the applicant would be issued the STC.

Technical Standard Order (TSO).

A TSO (or ETSO – European TSO) comprises a unique set of performance and interface standards (MPS) for a specified item used on commercial aircraft. A “TSO Authorization” means a certification agency has reviewed and affirmed that the specified item meets the TSO MPS (design and production requirements), and the manufacturer is able to proceed with production; therefore a TSO comprises both “design” and “production”

approvals. However, depending upon the item type, a TSO is a design/production approval; a TSO is not an installation approval. The installation approval must be obtained separately; it may not necessarily imply an ability to proceed with installation on an aircraft.

An aircraft typically has dozens of different computer-based systems onboard, with large commercial aircraft containing over one hundred unique systems. Since each system performs different functionality, many of those systems must be shown to provide basic capabilities common to that type of system; these basic capabilities are thus termed “minimum performance standards”. Therefore, TSO’s embody those minimum performance and interface standards for an associated system type.

TSO’s cover many items common to civil aircraft, including avionics systems. For avionics, TSO coverage includes primary flight instruments and other systems such as: autopilots, radios, stall-warning, air data computers, AHRS/ADAHRS, windshear, flight management systems, GPS, etc. Some devices only comply with a portion of the TSO requirements; these TSO’s are referred to as partial TSOs. As the name implies, partial TSOs are for devices that provide a portion of the total TSO function. Applicants developing a partial TSO device will need to coordinate their plans with the certification authority well in advance of beginning any development work to ensure the certification authority agrees with the certification basis and partial TSO basis.

TSO’s are written by the regulatory authority and are generally supported by document orders (DO’s) developed by federal advisory committees such as RTCA. The development of DO’s includes input from a loosely integrated group of international organizations, users and the regulatory authorities. These DO’s (such as RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification) form an integral part of the TSO requirements and are generally referenced in the TSO.

One important note: as TSO’s are important and official FAA recognition of approval, TSO’s are only extended to foreign manufacturers meeting all TSO requirements AND manufacturing in a country with a recognized bilateral agreement applicable to the avionics item in question. For example, as of this writing, the USA does not have common bilateral agreements with Turkey

whereas EASA does; therefore Turkish manufacturers can often apply for and receive ETSO's whereas obtaining a TSO (FAA) is more problematic.

Importance of TSO's.

Aside from comprising a mandatory standard for common avionic items, TSO's are important for a number of additional reasons:



Important Aspects of TSO's and Special European Considerations

TSO's then are an important layer within the Airworthiness Pyramid for avionics; they provide a common repository for additional operational characteristics for common avionics systems. For more complex, or less mature, avionics systems it is common for TSO's to be more frequently updated to thus "evolve" the minimum operational requirements for that system type. A TSO update may or may not obviate prior versions of that TSO, but updated TSO will clearly state whether or not such is the case. It should be noted that EASA is now regarding FAA TSO approvals as of limited value, not only if the TSO is outdated, but in general, since the ACO TSO process, especially for changes, is regarded sometimes as a "quick fix" way to obtain an approval; more so when the equipment provides 10% of functionality as per TSO MOPS, and 90% as extra functionality. EASA is requiring for every TSO'd equipment (and even ETSO'd) to fill in questionnaires regarding the regulations followed (AC's, DO's, etc.) explicitly, and in particular how the design assurance for functions NOT specified by the TSO has been achieved. Proceed with knowledge, and caution.

Example TSO.

To help understand TSO fundamentals, consider TSO-C63d, titled, “Airborne Weather Radar Equipment.” The title contains the acronym “TSO” so it is clearly a Technical Standard Order. The classifier “C63” is a unique designation allocated to airborne weather radar equipment. The revision letter “d” means it is the fifth revision of TSO-C63, since the second revision would have been the “a” in “C63a”. This TSO–C63d is 15 pages in length with a specified “Effective Date” of 2/28/12 meaning new weather radar certifications after February 28th, 2012 need to meet the standards specified in TSO-C63d. What does TSO-63d specify? Key contents include:

- a. **“Purpose.”** Describes what functionality is covered by this TSO, which in this case is forward looking windshear capability. It specifically excludes flight guidance system functionality which is covered elsewhere.
- b. **“Applicability.”** States that this TSO is for new airborne weather systems planned for development after the effective date (February 28, 2012) and that the prior versions of this TSO are cancelled.
- c. **“Requirements”.** Detailed enumeration of requirements covering minimum airborne weather equipment functionality, failure condition classifications, functional and environmental qualification must meet RTCA DO-173 and DO-220, Software and Hardware qualification must meet RTCA DO-178 and DO-254, data and documentation requirements,
- d. **“Minimum Performance Standards.”** Actual criteria for measuring and reporting applicable weather data for windshear detection, plus details on simulating and testing this weather data functionality.

TSO-C63d is a typical TSO in terms of its size, format, and organization. But like all TSO’s, its content is specifically tailored to meet the needs of the subject system “Weather Radar”, in this case windshear functionality contained within airborne weather radar systems.

Parts Manufacturer Approval (PMA)

PMA is a combined design and production approval for modification and replacement articles and allows a manufacturer to produce and sell these

eligible items for installation on type certificated products. PMA approval is an approval of the manufacturers Fabrication and Inspection System (FIS). A TSO-ed device does not also require the applicant to obtain PMA since the TSO is a design and production approval. PMA approval can be obtained for a replacement part utilized by a TSO device but in these cases the installer must place their modifiers nameplate on the TSO device. Parts produced under a One Time STC or Field Approval are not eligible for PMA. Standard parts, such as nuts, bolts, etc. do not require PMA.

For certificated aircraft, PMA is the basis by which normally required for devices which can affect safety to be installed on certified aircraft (this is not the case for experimental aircraft). PMA is not a general approval of inspection procedures, or materials, or processes, PMA approval is only applicable to a specific device and specific processes and procedures for that device. Manufacturers who hold a PMA can make and sell replacement parts even though they were not the original manufacturer of the aircraft or the originally installed item. PMA can be used for the production of modification parts from supplemental type certificates (STC). In these cases once an STC is issued the approval of the STC then becomes the basis for approval of a new or modified part and the PMA for that new or modified part will be issued shortly after the STC is issued.

PMA's increased in importance as air travel proliferated and evolved. Aircraft owners/operators do not want to be held hostage to a single supplier for the life of their aircraft, so they want alternate sources for parts. Conversely, certification authorities recognize that aircraft safety resembles a large, complex chain with safety only as good as the weakest link within that chain; unapproved parts could readily become that weakest link thereby affecting safety.

Obtaining a PMA normally requires two distinct and sequential activities, depicted below:



Two Steps For Obtaining PMA

Three Methods for obtaining approval of the PMA part design

Method 1. PMA by Identity by Showing Evidence of a Licensing Agreement (this is not a separate approval method, but is actually a means to substantiate identity):

Often this method is used to obtain PMA via STC licensing agreement. In this case the PMA applicant establishes a licensing agreement with the TC/STC/TSO holder and the type design data from the TC/STC/TSO is used to substantiate identity.

Method 2: PMA by Identity without a Licensing Agreement:

In this case the applicant submits a statement certifying the design is identical in all respects to an approved design. Generally, if the applicant does not have access to the original design data (in the case of complex or sophisticated parts) it is nearly impossible to obtain PMA via identity without a licensing agreement.

Method 3: PMA by Test and Computation:

This method is as it sounds, a comprehensive set of Test and Computation data demonstrating compliance with the applicable airworthiness standards.

The two sequential activities for obtaining a PMA are further described here:

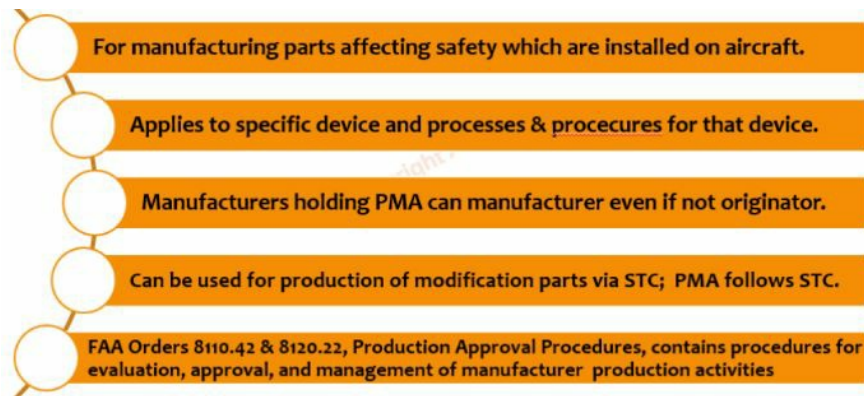
Step 1: Proving Safe Design. The part to be manufactured must first be shown to have a safe design (airworthy). How is a “safe design” shown? Remember, avionics certification is about “proving your innocence” because unlike typical laws, aviation safety is predicated upon the “guilty until proven innocent” paradigm. For PMA’s, the applicant must “prove” the design is safe by:

- a. Proving all applicable certification regulations and standards have been followed for that part. Depending upon the part, for example, some combination of DO-178 (software), DO-254 (hardware), DO-160 (environmental testing), etc. may apply, along with Advisory Circulars (ACs) and possibly other DO’s and requirements.
- b. Lacking a licensing agreement per “Method 1” above, additional

Analysis can be used which shows the part is acceptable. For simple designs, this analysis could be inspection of the part and then comparison with similar approved parts to show that the new part has the same safety attributes as the already approved part. For more complex designs, analysis could be tests and calculations which directly prove the part meets all FAA safety standards. Note that for parts containing hardware or software logic, this Analysis could not be used to replace the need for DO-254 or DO-178 and this option is invalid.

Step 2: Obtaining Production Approval via Conforming QA. After Step 1 above has been accepted, the next step is to obtain actual production approval for the part. Why is this step necessary if the design has already been shown to be safe and meet all standards/regulations? Simple: consider healthy lifestyles and a person who has the “recipe book” for such which includes healthy food, exercise, stress reduction, and sleep. “Owning” such a recipe book hardly guarantees implementation – to live a healthy lifestyle requires diligence, time, money, and no junk-food binges. The same is true for safe aviation parts: the manufacturer must prove they follow the safe design and are able to manufacture it consistently while having provisions for defect detection and prevention. The process of “proof” combined with defect detection and prevention is a Quality Assurance (QA) function whereby QA proves “conformance.” This ensures that parts will be shipped to end-users only when they meet all requirements of the approved design, regulations, and standards.

PMA’s cannot be transferred and they are valid until surrendered, withdrawn, or terminated (usually by the certifying agency). PMA data can be sold (usually under license as mentioned above) but the buyer does not automatically receive permission to produce. Why? Simple: the latter two characters of “PMA” stands for “Manufacturing Approval” and it’s the very manufacturing processes, facility, and quality assurance ecosystem which must first be approved. So a buyer of PMA data, even via a license, is obligated to obtain their own PMA, though such should be easier when procuring a licensed design that previously had its own PMA. Additional notes regarding PMA’s are summarized below:



Key Notes Regarding PMA's

PMA's thus form an important part of the Airworthiness Pyramid. Since 2011, greater emphasis has been placed on a manufacturer's quality system; certification agencies such as the FAA recognize such and regularly audit for conformity as part of their ongoing certification management process.

Conclusion

The Airworthiness Pyramid provides an easy means to understand the seemingly disparate aspects of avionics type certifications. The details lie across thousands of pages of applicable rules, standards, guidelines, regulations, and orders. By following the pyramid approach described herein layer by layer, certification is no more difficult than climbing a tall, curved, ladder: time, strength, courage, and perseverance are all that is required. Enjoy the climb; the view from the top is truly outstanding.

4

ARP4761A Aviation Safety

By Vance Hilderman

With Contributions by:

- Mr. Jon Lynch

Reviewed by:

- Nazan Gozay Gurbuz, Safety Expert, & ARP4754A/4761A Committee Member

4761, 4754 ... Magic Numbers or Real Answers?

Aviation safety does not rely upon magic numbers but begins by determining real answers. Likewise, aviation safety is never an accident, but true mathematically-based Safety should prevent accidents. The numbers “4754” and “4761” are not magic but are associated with aviation safety. Safety and the Numbers have evolved – the new answers for aviation development and safety are found in 4754A and 4761A; specifically the Society of Aerospace & Automotive Engineers (SAE) ARP4754A (Aircraft & Systems Development) and ARP4761A (Safety Assessments).

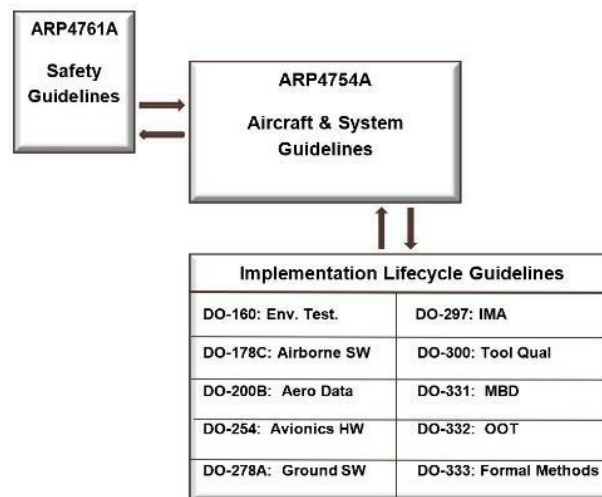
The Old Days.

In technology, the Old Days refer to any time prior to last year. In the Very Old Days (moon landings, space shuttles, new commercial jets with four engines) safety was addressed by brains and refinement: smart engineers did their best to prevent accidents then refinement was applied when those best efforts were less than perfect. In the Very Old days, computing horsepower was thinner, schedules were fatter, and acceptable safety generally ensued: space shuttles had a 98.5% chance of not exploding and commercial aircraft had fatal crashes “only” a few times annually. Then the very old days gave way to mere old days, and the very old ways didn’t work as well. Some said

the engineers were not as smart while others said those engineers were trying to make the computers too smart. But all agreed that more formalized safety was needed and the Society of Automotive Engineers (SAE) had been handling Aerospace Recommended Practices (ARP's) for decades. SAE ARP4754, *Guidelines for Development of Civil Aircraft and Systems*, was published in November 1996. Its tightly-coupled sibling ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, was published the next month, December 1996.

ARP4761A is rather more than a guideline for aircraft safety. ARP4761A (formally issued in 2018) is officially titled “*Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*”. In fact, ARP4761 is almost a tutorial on generalized safety and how to apply various theoretical analysis to assess ongoing development activities toward aircraft safety.

Clearly, ARP4761A is tightly coupled with ARP4754A and lays the foundation for the most fundamental aspect of aircraft regulations: Safety. Clearly, viewing the aviation development and certification ecosystem, ARP4761A's prominent place in the upper left conveys its importance:



The Safety Assessment process is a vital aspect of aviation safety, and for aircraft and avionics, ARP4761 (and its newest version ARP4761A) provides the foundation.

Literally every aspect of aviation undergoes safety assessment to better

understand potential risks, quantify them, and then prevent, detect, or mitigate them. Experienced aviation persons are truthful when stating the safety assessment process is perhaps the most important element of avionics development. For avionics, the role of the safety assessment is to ensure the safety of the aircraft, its crew, and the occupants. Essentially, aircraft safety is optimized by performing careful analysis, architectural optimization, criticality level determination, component selection, architectural improvement, monitoring, and maintenance. Therefore, only by having a thorough safety assessment process can we ensure we have an architecture with additional safety-related requirements which address safety aspects. The title of ARP4761 accurately justifies its importance within this fundamental process:

“Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems & Equipment”

In an ideal world, avionics safety assessments would follow a one-size-fits-all approach consisting of uniform safety analysis steps. And in that same ideal world, humans would never be sick, gain weight, or age. Unfortunately, the ideal world cannot be assured which begets the fundamental premise of safety assessments: analyze potential problems for the real, not ideal, operating conditions. Thus, safety assessments are vital especially because aviation has no ideal world: developers of critical avionics systems spend an inordinate amount of time involved in the myriad “what if” worst-case scenarios associated with potential and realized faults.

Clearly then, if all avionics developers were perfect geniuses and could postulate and solve all possible safety scenarios in their head, they would not need a written formal safety assessment process because they performed such perfectly already. But who reviewed it? How was consistency across assessments assured? What about future systems changes? Is an undefined process really a process? And who is really an infallibly perfect genius? As the answers to these questions are all obvious, so is the need for a formal safety assessment process; ARP4761 provides the basis for that process, and at 300+ pages within that Guideline, the words here can only be a mere summary. But to understand and apply ARP4761, the practitioner needs to understand the overall Safety context and relationship to other documents.

Aviation safety is codified by a large ecosystem of information dissemination and regulations. Every individual with even an indirect role in aviation safety is governed by rules which, at a minimum, require procedures to be defined and followed. In most cases, additional regulations provide rules or guidelines covering “how” the tasks are to be performed and the minimum threshold that must be attained to achieve certification. The aviation aspects governed by safety-related regulations include:

- Aircraft pilots and crew
- Ground operators
- Maintenance personnel
- Air traffic control, communications, navigation, etc.
- Systems, hardware and software development including airborne and ground-based
- Tools including mechanical, hardware, software
- Virtually all aspects of aircraft manufacturing
- Flight testing
- Suppliers, manufacturing, updates

For avionics, the set of regulations is helpfully focused; the avionics safety assessment process primarily utilizes the following relevant industry and government documents:

- **SAE ARP4761/A** – *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*
- **SAE ARP4754A** – *Guidelines for Development of Civil Aircraft and Systems*
- **FAA Advisory Circular AC23.1309-1E** – *Equipment, Systems, and Installations in Part 23 Airplanes*
- **FAA Advisory Circular AC25.1309-1A** – *System Design and Analysis*
- **FAA Advisory Circular AC27-1B** – *Certification of Normal Category Rotorcraft*

- **FAA Advisory Circular AC29-2C** – *Certification of Transport Category Rotorcraft*
- **RTCA DO-160** – *Environmental Conditions and Test Procedures for Airborne Equipment*
- **RTCA DO-178C** – *Software Considerations in Airborne Systems and Equipment Certification*
- **RTCA DO-254** – *Design Assurance Guidance for Airborne Electronic Hardware*

If the information herein were on overall aviation safety, or even aircraft safety, the scope would expand greatly. But the purpose here is purely upon individual avionics systems. The safety assessment process utilizes experienced engineers (versed in the above documents and regulations) to proceed through a series of analyses pertaining to the system and aircraft. As the safety assessment proceeds, the following documentation typically accompanies the various analyses:

- *Aircraft Functional Hazard Assessment (FHA)*
- *Aircraft Fault Tree Analyses (FTAs)*
- *System FHAs*
- *System FTAs*
- *System Failure Modes and Effects Analyses (FMEAs)*
- *Item FTAs*
- *Item FMEAs*

A key to the above is “Traceability”: it’s imperative that relationships between aircraft operations, maintenance, systems, etc. be codified and linked: that process is termed “traceability”. In the Old Days, traceability could be handled manually or by large, institutionalized database-intensive tools. However, those manual and large-tool processes did not readily provide visibility into the relationships, safety assessments, evolution, review evidence, and derived requirements (requirements which are “derived” from a safety assessment, added to clarify a design/implementation decision, or to fill a gap).

Aviation safety involves four key safety activities as depicted in the figure

below:



The world of “safety” has its own language and lexicon. Experienced safety engineers are well versed in this language, but you are probably not reading these words if you are an experienced avionics safety engineer. To begin, please ponder the following words and test yourself by verbalizing a 1-2 sentence definition for each word (answers follow, but please spend just a few minutes pondering these words yourself before looking at the answer. Remember, you didn’t learn to drive a car by simply reading the user manual: the real learning came when you practiced driving):

- *Adverse Effect?*
- *Assessment?*
- *Average probability per flight hour?*
- *Complex System?*
- *Design Assurance Level?*
- *Extremely remote failure condition?*
- *Extremely improbable failure condition?*
- *Failure condition?*
- *Minor?*
- *Major?*
- *Hazardous?*
- *Catastrophic?*
- *Functional hazard assessment?*
- *Hazard?*
- *Primary Function?*

- *Primary System?*
- *Reliability?*
- *Secondary System?*
- *Simple System?*
- *System?*

OK, you've pondered the above words. What is their meaning when applied to avionics safety? First, there is no mandatory definition which everyone in the world adheres to or must follow. If you were to examine the dozen most common sources of aviation terminology, you would discover numerous minor differences within definitions of these terms—and some of the differences are not so minor. The various authorities and authors try to maintain consistency; in aviation this is called “harmonization”, such as when the USA's FAA and Europe's EASA coordinate to resolve differences. But your world is the real world, and that world is constantly evolving with an ever-expanding lexicon. In keeping with the coincidental but unrelated Heisenberg Principle, we should never expect perfect consensus on all definitions. So before using the following definitions, research any binding regulations which apply to your avionics activities and reach agreement with any approval agencies by citing the reference source, and definition itself, within your avionics documentation. With those WWW (wary wise words), here are what this author believes to be the most commonly accepted definitions:

Assessment: An evaluation based upon engineering judgment.

Average probability per flight hour: A representation of the number of times the subject failure condition is predicted to occur during the entire operating life of all airplanes of a type, divided by the anticipated total operating hours of all airplanes of that type.

Complex System: A system whose operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods.

Development Assurance Level (DAL): All of those planned and systematic actions used to substantiate,

at an adequate level of confidence, that errors in requirements, design and