

Efficient Certification of Highly Integrated and Complex Aircraft Systems, Such as Integrated Modular Avionics

Marty Gasiorowski
Worldwide Certification Services

ABSTRACT

There are several relatively new certification standards related to Integrated Modular Avionics (IMA) certification that have recently been invoked by the certification authorities. These standards include SAE ARP-4754A, *Guidelines for Development of Civil Aircraft and Systems*, RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, and RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*. RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, and TSO C153, *Integrated Modular Avionics Hardware Elements*, are also applicable to IMA certification. As many of these standards have only recently been invoked in Advisory Circulars by the Certification Authorities, the industry has little experience in complying with them individually, and even less experience complying with them collectively. With the current trend of increased integration, and the application of IMA architectures to systems that are not avionics, such as electric power, fly-by-wire, and air management, companies that were not previously obligated to consider "avionics" standards will be required to define new processes for their engineering organizations. Further, FAA and EASA have different positions on how these standards should be applied, adding complexity to aircraft and system development programs seeking both FAA and EASA certification. Responsibility for compliance with these standards also crosses the boundary between aircraft OEMs and system suppliers, which can add complexity to the Statement of Work and Contract negotiations between OEMs and Suppliers. Additionally, there is overlap between the standards that need to be considered when defining development plans and processes.

This paper provides a brief overview of the standards, the differences in how certification authorities invoke the standards, details of the relationship and interface between these standards, and a structure for aircraft and system developers to consider in generating plans and processes to efficiently complying with all of these related standards to achieve FAA and EASA Certification.

CITATION: Gasiorowski, M., "Efficient Certification of Highly Integrated and Complex Aircraft Systems, Such as Integrated Modular Avionics," *SAE Int. J. Aerosp.* 5(1):2012, doi:10.4271/2012-01-2143.

INTRODUCTION

There are numerous aircraft in service today with Integrated Modular Avionics Systems. Most of these aircraft were certified prior to the invocation of the following standards:

- SAE ARP-4754A, *Guidelines for Development of Civil Aircraft and Systems*, which was invoked by FAA Advisory Circular 20-174 in 2011.
- RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, which was invoked by FAA AC 20-170 in 2010.
- RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, which will be invoked by FAA and EASA in 2013.

It will be challenging for the next aircraft and IMA certification programs to determine an efficient, yet compliant approach related to these newly invoked standards, as well as existing standards such as ARP-4761, *Safety Assessment Process Guidelines and Methods*, DO-254, *Design Assurance Guidance for Airborne Electronic Hardware* and TSO C153, *IMA Hardware Elements*.

OVERVIEW OF STANDARDS

To determine an efficient strategy for compliance to the new standards, one must first understand the focus of the standards, and the interfaces between the standards. This section provides a brief overview of each standard, but note that a more detailed understanding of the standards than what

is provided here is necessary to determine a certification strategy.

SAE ARP-4754A, Guidelines for Development of Civil Aircraft and Systems

ARP-4754A defines processes at the aircraft and systems level, with variation by Development Assurance Level, for development and integral processes. ARP-4754A defines objectives for these processes and these objectives need to be met for certification. The development processes are:

- Planning - defining the Aircraft or System Certification Plan, Development Plan, Validation Plan, Verification Plan, Configuration Management Plan and Process Assurance Plan
- Aircraft Function Development - identification of the functions that will be performed by, or included in, the aircraft
- Allocation of Aircraft Functions to Systems - including determining which system will provide which portion of each function
- Development of System Architecture - definition of redundancy, interfaces, communication, and separation to support the aircraft functions
- Allocation of System Requirements to Items - allocation of requirements to software and hardware (items)
- System Implementation - implementation of functions into items in compliance to DO-178C and DO-254

The integral processes that are applied to the above development processes are:

- Safety Assessment, according to ARP-4761
- Development Assurance Level Assignment - architectural means can be used to reduce DAL in some cases at the aircraft, system or item level
- Requirements Capture - typically captured incrementally at the aircraft, system and item levels
- Requirements Validation - confirming the requirements are correct and complete
- Configuration Management
- Process Assurance - assuring that processes defined in the plans are followed
- Certification and Regulatory Authority Coordination
- Implementation Verification - confirming compliance with the requirements

The output of the above processes is a set of data and documentation that provides evidence that the objectives were met.

DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

DO-297 basically customizes ARP-4754A for IMA, adds IMA-specific design features such as partitioning and health management, and defines an incremental approach to certification with tasks for:

1. Module acceptance (where a module is defined by the applicant, and may be any or all of a hardware module, boot software, operating system software and/or platform software)
2. Application acceptance (where an application is a software and/or hardware component that performs an aircraft level function)
3. An IMA System, consisting of modules and applications
4. An Aircraft, including an IMA System
5. Changes to any of the above
6. Approval to reuse any of items 1 or 2

DO-178C, Software Considerations in Airborne Systems and Equipment Certification

DO-178C is a relatively minor change from DO-178B, primarily focused on improving clarity, usability and standardization. However, four related supplements were published to address Tool Qualification and three development methodologies:

- DO-330, Software Tool Qualification Considerations
- DO-331, Model Based Development and Verification
- DO-332, Object Oriented Technology and Related Techniques
- DO-333, Formal Methods

A key item, in the context of the interface of these standards, is that if Model Based Development is used at the systems level, then DO-331 is applicable at the System Level as well as the Software Level. Further, this standard requires that there be requirements at a level higher than the model, regardless of the level of the model in the requirements hierarchy.

DO-254, Design Assurance Guidance for Airborne Electronic Hardware

DO-254 has been invoked for several years, but recently the FAA has published Order 8110.105, and EASA has published Certification Memo SWCEH-001, Issue 1. These two documents add requirements above and beyond DO-254. The FAA Order adds requirements for a Hardware