

ARP4754A/ ED-79A - Guidelines for Development of Civil Aircraft and Systems - Enhancements, Novelties and Key Topics

2011-01-2564

Published
10/18/2011Alessandro Landi
AirbusMark Nicholson
York Univ.

Copyright © 2011 SAE International

doi:[10.4271/2011-01-2564](https://doi.org/10.4271/2011-01-2564)

ABSTRACT

ARP4754A/ED-79A guidelines address the development cycle for aircraft and systems that implement aircraft functions. The current trend in system design is an increasing level of integration between aircraft functions and the systems that implement them. While there can be considerable value gained when integrating systems with other systems, the increased complexity yields increased possibilities for errors, particularly with functions that are performed jointly across multiple systems. Following the Aviation Rulemaking Advisory Committee (ARAC) recommendations to respond to this increased integration which referenced ARP4754/ED-79 in advisory materials for compliance to 14CFR/CS 25.1309 (see AMC 25.1309, published in 2002 and AC25.1309-Arsenal draft) the use of ARP4754A/ED79A in aircraft certification has become increasingly widespread.

This presentation constitutes a comparison between the documents SAE [1] / EUROCAE [2] and SAE [3] / EUROCAE [4]; it highlights ARP4754A/ED79A enhancements, novelties and key topics (e.g. Development Assurance Level Assignment FDAL & IDAL).

INTRODUCTION

ARP 4754A/ED-79A is intended as guideline material for the development of civil aircraft and systems. It includes current best practices as identified by the SAE / EUROCAE working committees involved in its writing. The standard is intended to enhance practices throughout industry and assist

companies in developing and meeting their own internal standards. ARP 4754A/ED-79A takes into account experiences on recent aircraft programs (e.g. A380, B787, Falcon 7X, etc.).

ARP 4754 AND ARP 4754A

The title of the ARP4754A/ED79A standards changes to “Guidelines for Development of Civil Aircraft and Systems” replacing the original title ARP4754/ED79 “Certification Considerations for Highly-integrated or Complex Aircraft Systems”. The new title reinforces the development aspect of the recommended practice and extends the scope of the guidance provided. “Certification” has been deleted because the document is a recommended best practice for the development of civil aircraft and systems linked not only with the certification process. The notion of highly integrated or complex systems has been deleted because the wording is ambiguous; how can “Highly integrated” be differentiated from “Complex” systems? How can Highly/not-Highly integrated or Complex/not-Complex systems be differentiated?

The new document extends existing material but also introduces a number of new sections that reflect changes in development best practices since 1996. The following introduces the main differences between ARP4754/ED79 and ARP4754A/ED79A in development life-cycle order.

A new section, Development Planning, is dedicated to the overall development planning process, expanding the scope of the previous issue document that highlighted only

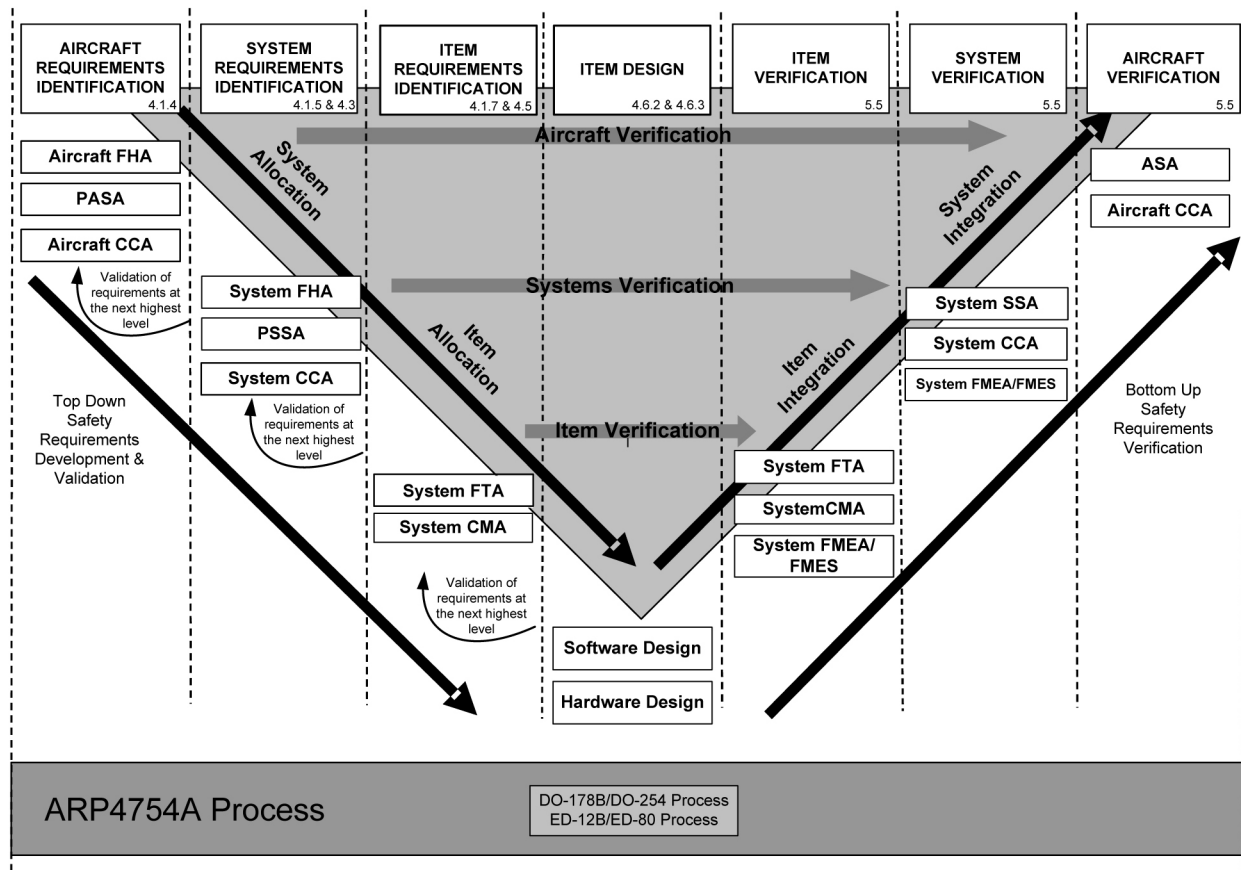


Figure 1. Aircraft and Safety Development Life-cycles

Certification and Verification Planning. The purpose of the development planning process is to define the means of producing an aircraft or system which will satisfy the aircraft/system requirements and provide the level of confidence (assurance) which is consistent with airworthiness requirements. A key component of planning is the establishment of life cycle process checkpoints and reviews, which are aligned with program phases and gates. Maturity expectations and management of deviations from plans are also introduced in this new section.

The Section "Aircraft and system development process" supersedes the ARP4754 section "System Development", expanding the scope and introducing the notion of Integral processes, Aircraft function development, Function Requirements, Function and Item Development Assurance Level (FDAL, IDAL). Integral processes are those, such as safety assessment, that need to be undertaken throughout the development process. An item is now defined to be a hardware or software element having bounded and well-defined interfaces.

The main aircraft and system development activities are: Conceptual Aircraft/System Development, Aircraft Function Development, Allocation of Aircraft Functions to Systems,

Development of System Architecture, Allocation of System Requirements to Items, System Implementation.

The main integral processes are: Safety Assessment, DAL assignment, Requirements Capture, Requirements Validation, Implementation Verification, Configuration Management, Process Assurance, Certification and Regulatory Authority Coordination. Two new statements have been included in the "integral processes", Development Assurance Level assignment and requirements capture, to emphasize these aspects and include them in the group of main processes. Integral processes should be supported by an integral process plan (e.g. safety plan, certification plan, V&V plan), methods (methods to perform the tasks identified in the plan) and technical deliverables (result of the application of the method in a given aircraft program).

Interaction between safety and development processes and the definition of types of Safety Requirements, including their hierarchical levels, have been also highlighted and extended in ARP4754A/ED79A, see [Figure 1](#).

ARP4754A/ED79A regards the activities of ED-12B / DO-178B and ED-80 / DO-254 as a means to implement the development assurance rigor for software and electronic

hardware items (i.e. the objectives for accomplishment of each IDAL). The ED-12B / DO- 178B and ED-80 / DO-254 are no longer considered to be adequate to mitigate aircraft/system errors without a development assurance process from aircraft level down to item level being undertaken. ARP4754A/ED79A provides new guidelines for assigning the FDAL and IDAL and the objectives for accomplishment of each FDAL.

The guidelines state that there is no direct correlation between development assurance levels and numerical probabilities. Thus, two sets of objectives, numerical and DAL, must be met during the development process.

The safety assessment integral process has been expanded with new activities: Safety Program Plan, Preliminary Aircraft Safety Assessment / Aircraft Safety Assessment (PASA/ASA), Safety Case / Safety Synthesis.

- The Safety Program Plan defines the scope and content of the safety activities to be undertaken during development and includes principles for an appropriate safety organization and responsibilities of the safety team. Other topics may also covered through the Safety Program Plan (e.g. key project milestones for which reports are required, references to standards/ methods to be used, etc.).

- A safety case or safety synthesis communicates a clear, comprehensive and defensible argument that the aircraft and systems are acceptably safe to operate in a particular context. The argument supporting the conclusion may include the following: all the safety activities have been performed according to the Safety Plan, safety requirements for the aircraft are satisfied, Safety Validation/Verification process is completed and results accepted. Evidence needs to be provided that these arguments hold true for the project.

- The PASA/ASA activities assess the Failure Conditions (FCs) identified in the aircraft level FHA that combine failures of several systems that are not studied at system level. The PASA process supports the assignment of FDAL for aircraft functions. The ASA process supports the verification of the assigned FDAL and the activities associated with it.

- The Preliminary System Safety Assessment (PSSA) process supports the assignment of FDAL for system functions and IDAL for hardware and software items. The System Safety Assessment (SSA) process supports the verification of the assigned FDAL and IDAL and the activities associated with it. Data from these activities should be included in the PSSA/ SSA report. The PSSA/SSA report should also include data of the non-analytic verification processes (i.e. test, demonstration and inspection) that are being used to verify safety requirements.

- A clearer difference between PSSA and SSA is now provided; PSSA is a method to evaluate proposed

architectures and derive system/item safety requirements; whereas the SSA is a verification that the implemented design meets the safety requirements as defined in the FHA and PSSA. Safety requirements should be derived from FHA and PSSA.

For a given function, safety requirements are derived using the results of the safety assessments.

Requirement Validation and implementation Verification concepts have also been improved, in particular:

- The application of independence in the validation process is dependent upon the assigned Development Assurance Level. This independence needs to be applied between requirements capture and the validation activities. The validation plan should include a description of the validation activities to which independence is applied.

- The Verification plan should include the roles and responsibilities associated with conducting verification activities and a description of how independence between design and verification activities is to be ensured and assured.

The activities of the system configuration management process have been enriched with:

- The development life cycle data of a Configuration Item can be assigned one of two categories: System Control category 1 (SC1) or System Control category 2 (SC2). These categories differ by virtue of the configuration management controls placed on the data. The Data Control Categories assigned depends on the Development Assurance Level of the associated function or item.

- Configuration Management Plan (CMP): identifies all the objectives and tasks to be performed in the configuration management activity.

- Configuration Baseline Establishment (CBE): to create and maintain control and traceability of configuration items.

ARP 4754A / ED-79A acknowledges that an early certification plan may be missing significant detail, necessitating subsequent updates. Despite this, early coordination and approval of the plan is strongly encouraged. Early certification planning can minimize the effects of misinterpretations of internal requirements, industry standards, regulations and advisory materials.

Systems and items which have been used on other aircraft are often reused in new or derivative aircraft. The maturity of these systems and items has benefit, but it should not be assumed that they meet the requirements of the new installation. Even if no design changes are to be made to the system or item, the requirements to which the system or item were certificated should be validated according to the new application, and modified as necessary.