AEROSPACE INFORMATION REPORT

AIR6218™

Issued 2012-09
Reaffirmed 2018-10

Constructing Development Assurance Plan for Integrated Systems

RATIONALE

This SAE Aerospace Information Report presents a collection of lessons learned for constructing development assurance plans for integrated systems based on past certification programs.

FOREWORD

Integrated aircraft system architectures have flourished in civil aircraft development since the 1990s, and the use of such architectures will likely accelerate in future design practices. To date, the industry standards (and regulatory guidance) on integrated systems have not progressed much further than a firm acknowledgment of the rapid integrated systems growth trend, and a recognition of potential safety risks if development errors are not identified and corrected during the development process. Chapter 4 of the SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, recognizes this issue and states, "*Complex systems and integrated aircraft level functions present greater risk of development error (requirements determination and design errors) and undesirable, unintended effects.*" In today's practices, development assurance plans for integrated systems are predominantly based on the tried-and-true concept of separation of responsibilities between various disciplines. This is incongruent with the demands of integrated system architectures. While system separation, fault isolation, or error containment, will continue to be effective risk management practices that must not be compromised or overlooked, a new approach for constructing a development assurance plan for integrated systems is needed to cope with the reality of system design trends.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2018 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit http://standards.sae.org/AIR6218

Documents Document Sharing Hub

Full document details: SAE AIR6218

1. SCOPE

This SAE Aerospace Information Report (AIR) supplements ARP4754A by identifying the crucial elements to be considered when constructing the development assurance plans described in Chapter 3 (Development Planning) of ARP4754A for integrated systems. This AIR presents a collection of lessons learned from past certification programs involving integrated systems. This AIR is not guidance for system integration technologies.

2. APPLICABLE DOCUMENTS

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

ARP4754A Guidelines for Development of Civil Aircraft and Systems

Beland, S. and Miller, A., "Assuring a Complex Safety-Critical Systems of Systems," SAE Technical Paper 2007-01-3872, 2007, doi:10.4271/2007-01-3872

3. DEVELOPMENT ASSURANCE PLANNING

Development Assurance involves all of those planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis. Chapter 3 of ARP4754A provides a general planning process to address development assurance. This general process involves a number of “development planning elements,” repeated in Table 1:

TABLE 1 - DEVELOPMENT PLANNING ELEMENTS

Planning Elements	Element Description
Development	Establish the process and methods to be used to provide the framework for the aircraft/system architecture development, integration and implementation.
Safety Program	Establish scope and content of the safety activities related to the development of the aircraft or system.
Requirements Management	Identify and describe how the requirements are captured and managed. Sometimes these elements are included in conjunction with the validation elements.
Validation	Describe how the requirements and assumptions will be shown to be complete and correct.
Implementation Verification	Define the processes and criteria to be applied when showing how the implementation satisfies its requirements.
Configuration Management	Describe the key development related configuration items and how they will be managed.
Process Assurance	Describe the means to assure the practices and procedures to be applied during system development are followed.
Certification	Describe the process and methods that will be used to achieve certification.

Documents
Document Sharing Hub
Full document details: SAE AIR6218

The various planning data described in ARP4754A is reproduced graphically in Figure 1 using the traditional development "V" diagram. This graphic conveys a potential for gaps in conventional system development planning to occur (i.e., the white space in between the aircraft plans and the system plans). An integrated system may, therefore, have these same plan disconnects as well as additional system implementation strategy induced short falls.

Although the ARP4754A comprehensively describes a general development process and life cycle, it does not focus on the development assurance activities that are unique to integrated systems. To begin this discussion we need to have a common set of terms. Within this AIR we consider the following:

1. What is an "integrated system"?

   In the context of this AIR, an "integrated system" is the set or arrangement of interdependent systems that have complex relationship or connection to provide a given capability. It can be visualized as a system of systems. Integrated systems enable more efficiency and robustness in providing system functions. Shared system resources, especially computers and communication networks, enable the implementation of functions more complex than can be provided by an individual system. However, integrated system architectures can introduce complex mechanisms for cascading failures or other unintended consequences.

2. How is the Development Assurance Plan for Integrated Systems (DAPIS) different from the plan elements shown in Table 1 and graphed in Figure 1?

   The planning elements shown in Table 1 and Figure 1 reflect practices commonly associated with the development of stand-alone systems. While the concept they represent is generally applicable to any system arrangement, be it integrated or standalone, DAPIS focuses on the interrelationships between those elements, to help answer lingering concerns that something may be missing or overlooked when integrated systems are developed and certified. Compared to standalone system development, the integrated system plan must contemplate the larger number of multi-dimensional interactions between functions, systems, and the organizations who work on them to minimize the risk of "missing something important." This AIR provides a "hands-on" set of elements based on lessons learned from past certification programs.

Because a plan is tailored to the needs of the individual project, the elements discussed in Section 4 are not intended to be a general "template". Rather, they provide insights on issues that experience has shown may not always be obvious (i.e., missing) when the development assurance activities of ARP4754A are planned or executed.

4. DEVELOPMENT ASSURANCE PLANNING FOR INTEGRATED SYSTEMS (DAPIS)

The classic planning considerations prescribed in ARP4754A provide for nominal integration of systems with considerations for the physical interfaces between electrical systems, interfaces between electrical systems and mechanical systems, or logical interfaces between hardware and software. These considerations may not be enough to assure the development of integrated systems.

The planning elements for integrated systems should also be considered when executing the planning process described in ARP4754A. DAPIS effects on the overall planning process should cover some or all of the following: design, test, manufacturing, maintenance, make allowances for follow-on product improvement. The following integrated systems effects on the ARP4754A plans should be contemplated. [Note: As the following information is a collection of "lessons learned," readers should assess them for applicability to their projects and the equivalency of their existing methods and tools.]

Figure 2 presents the additional planning and implementation relationships for integrated systems. The magenta highlighted integration plans gain importance when the development objective is an integrated system. The mechanisms for interface control also increase the interactions between activities and enhance communication for the integrated system.

Documents
Document Sharing Hub
Full document details: SAE AIR6218