

AEROSPACE INFORMATION REPORT

AIR7209™

Issued

2022-10

Development Assurance Principles for Aerospace Vehicles and Systems

RATIONALE

This SAE Aerospace Information Report (AIR) provides a high-level set of principles for the development assurance of aerospace vehicles and systems, including emerging technologies. The principles are meant to address experience of applying ARP4754/ED-79 (at latest revision) across a variety of applications. This document is technically identical to ER-023. If further elaboration of specific technologies is determined to be required, additional AIRs/ERs may be created.

TABLE OF CONTENTS

1.	SCOPE.....	2
1.1	Purpose.....	2
1.2	Background.....	2
2.	References.....	2
2.1	Applicable Documents.....	2
2.1.1	SAE Publications.....	2
2.1.2	FAA Publications.....	3
2.2	Definitions.....	3
3.	DEVELOPMENT ASSURANCE PRINCIPLES.....	4
3.1	Overview.....	4
3.2	Define the Development Assurance Process.....	6
3.2.1	Identify Planned Activities.....	6
3.3	Perform Supporting Processes.....	6
3.3.1	Perform Process Assurance.....	6
3.3.2	Manage Product Configuration.....	7
3.3.3	Manage Development Errors.....	7
3.3.4	Manage Assumptions.....	7
3.4	Define the Product.....	8
3.4.1	Identify Product Functions.....	8
3.4.2	Define and Validate Requirements.....	8
3.4.3	Identify Functional Safety Effects.....	9
3.4.4	Analyze Proposed Architecture.....	9
3.5	Evaluate the Implementation.....	10
3.5.1	Verify Implementation.....	10
3.5.2	Assess Unintended Behaviors.....	10
3.5.3	Evaluate Implementation.....	10
4.	NOTES.....	11
4.1	Revision Indicator.....	11
Figure 1	Development assurance principles.....	5

SAE Executive Standards Committee 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 © 2022 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
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE AIR7209

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR7209/>

Documents

Document Sharing Hub

1. SCOPE

1.1 Purpose

The purpose of this SAE Aerospace Information Report (AIR) is to provide a high-level set of principles to support aerospace projects required to use a formal development assurance process, such as ARP4754/ED-79 (at latest revision), to show regulatory compliance. Examples of projects where a formal development assurance process is needed are those that have significant functional interactions or whose products cannot be fully analyzed or tested. Development assurance techniques reduce the likelihood of undetected errors that could have safety impacts in the operation of the product. Design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems.

This document does not mandate specific processes to meet each development assurance principle. These principles are written at a high level to allow flexibility so that users can develop and evaluate their own compliant development assurance processes. Users are responsible for presenting their development assurance approach to certification authorities and obtaining agreement. The framework in this document can assist with this coordination.

1.2 Background

The industry has commonly relied on ARP4754/ED-79 (at latest revision) for guidelines for development assurance processes. However, ARP4754/ED-79 (at latest revision) has presented several challenges:

- a. Some potentially effective development assurance methods are not adequately addressed by ARP4754/ED-79 (at latest revision) techniques (e.g., system level application of formal methods, model-based system engineering, systems theoretic process analysis).
- b. Novel technologies are not adequately addressed by ARP4754/ED-79 (at latest revision) techniques (e.g., neural networks, artificial intelligence, machine learning).
- c. Developers have had difficulty obtaining acceptance of existing company processes and practices that meet the intent of ARP4754/ED-79 (at latest revision).
- d. ARP4754/ED-79 (at latest revision) has been misinterpreted or misapplied, requiring activities that were intended as recommendations.

The development assurance principles in this document describe the fundamental principles from ARP4754/ED-79 (at latest revision). These principles provide a framework within which these challenges may be addressed. ARP4754/ED-79 (at latest revision) remains one means, but not the only means, of meeting these principles. Users are responsible for coordinating their development assurance approach with certification authorities.

2. REFERENCES

2.1 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.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

ARP4754/ED-79 Guidelines for Development of Civil Aircraft and Systems

2.1.2 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

AC 25.1309 System Design and Analysis

TAEsdaT2-5241996 Task 2 - System Design and Analysis Harmonization and Technology Update

2.2 Definitions

ANALYSIS: A detailed examination based on decomposition into simple elements.

COMMON CAUSE: A single failure, error, or event that can produce undesirable effects on two or more systems, equipment, items, or functions.

DEVELOPMENT ASSURANCE: All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable safety objectives. (Adapted from AC 25.1309)

DEVELOPMENT ERROR: A mistake in requirements determination, design, or implementation.

ERROR: An omitted or incorrect action by a manufacturer, operator, or maintenance person, or a mistake in requirements, design, or implementation. (Adapted from AC 25.1309.)

FAILURE: An occurrence that affects the operation of a product such that it can no longer function as intended. This includes both loss of function and malfunction. Note: Errors may cause failures, but are not considered to be failures. (Adapted from AC 25.1309.)

FAILURE CONDITION: A condition having an effect on the aerospace vehicle and/or its occupants, either direct or consequential, that is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events. The condition may have effects on third parties and critical infrastructure. (Adapted from AC 25.1309.)

FAILURE CONDITION CLASSIFICATION: A discrete scale allowing categorization of the severity of the effects of a failure condition. Classification levels are defined in the applicable regulation and advisory material. For example, AC 25.1309 draft ARSENAL (ARAC report TAEsdaT2-5241996 includes AC/AMJ 25.1309 Draft ARSENAL revised System Design and Analysis) and AC 25.1309 define the following classifications: catastrophic, hazardous, major, minor, and no safety effect.

FUNCTION: Intended behavior of a product regardless of implementation.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

PROCESS: A set of interrelated activities performed to produce a prescribed output or product.

PROCESS INDEPENDENCE: A practice that minimizes the likelihood of development errors by using separation of responsibilities that assures the accomplishment of objective evaluation by someone other than the performer of the activity, e.g., validation activities are not performed solely by the developer of the requirement(s) of a product.

PRODUCT: An aerospace vehicle or system (this is different from the regulatory Part 21 definition).

REQUIREMENT: A necessary physical and/or functional characteristic of a product that can be validated and against which an implementation can be verified.

SAFETY: The state in which risk is acceptable.

SAFETY OBJECTIVE: A qualitative and/or quantitative attribute necessary to achieve the required level of safety for the identified failure condition, depending on its classification.

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

UNINTENDED BEHAVIOR: Unexpected operation of a product in ways contrary to its intended functionality.

VALIDATION: The determination that the requirements for a product are correct and complete.

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met.

3. DEVELOPMENT ASSURANCE PRINCIPLES

3.1 Overview

The development assurance principles in this document are grouped into the following sections:

- a. **Define the development assurance process:** The principle in this section establishes the development assurance process to be used for the product's development. As described in Section [1](#), users of this document are responsible for presenting their development assurance approach to certification authorities and obtaining agreement.
- b. **Perform supporting processes:** The principles in this section are essential for effective development assurance and impact all principles in the other sections. These principles are met continuously or repetitively throughout the product's development.
- c. **Define the product:** The principles in this section are typically met prior to product implementation. They guide the identification and validation of what the product is expected to do and the analysis of the proposed product architecture.
- d. **Implement the product:** Implementation of the product is performed outside the scope of the processes described in this document.
- e. **Evaluate the implementation:** The principles in this section are typically met after product implementation. They guide verification that the implementation meets its corresponding requirements, does not exhibit undesirable or unsafe effects, and is safe for its intended use.

[Figure 1](#) provides an illustration of the development assurance principles during product development.