

# ER-023

## DEVELOPMENT ASSURANCE PRINCIPLES FOR AEROSPACE VEHICLES AND SYSTEMS

### LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

**OCTOBER 2022**

## FOREWORD

1. This document was developed jointly by EUROCAE Working Group 63 “Complex Aircraft Systems” and SAE S-18 “Aircraft and Sys Dev and Safety Assessment Committee”.
2. This document is technically identical to SAE AIR7209.
3. RATIONALE: This document 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 ED-79/ARP4754 (at latest revision) across a variety of applications. If further elaboration of specific technologies is determined to be required, additional ERs/AIRs may be created.
4. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.
5. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
6. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
7. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
8. Copies of this document may be obtained from:

EUROCAE

9 – 23 rue Paul Lafargue

93200 Saint-Denis

France

Telephone: +33 1 49 46 19 65

Email: [eurocae@eurocae.net](mailto:eurocae@eurocae.net)

Website: [www.eurocae.net](http://www.eurocae.net)

## TABLE OF CONTENTS

|                                                   |    |
|---------------------------------------------------|----|
| FOREWORD .....                                    | i  |
| TABLE OF FIGURES .....                            | ii |
| CHAPTER 1 SCOPE .....                             | 1  |
| 1.1 PURPOSE .....                                 | 1  |
| 1.2 BACKGROUND .....                              | 1  |
| CHAPTER 2 REFERENCES AND DEFINITIONS.....         | 2  |
| 2.1 REFERENCES .....                              | 2  |
| 2.2 DEFINITIONS .....                             | 2  |
| CHAPTER 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 .....          | 6  |
| 3.3.3 MANAGE DEVELOPMENT ERRORS .....             | 7  |
| 3.3.4 MANAGE ASSUMPTIONS.....                     | 7  |
| 3.4 DEFINE THE PRODUCT .....                      | 7  |
| 3.4.1 IDENTIFY PRODUCT FUNCTIONS .....            | 7  |
| 3.4.2 DEFINE AND VALIDATE REQUIREMENTS .....      | 8  |
| 3.4.3 IDENTIFY FUNCTIONAL SAFETY EFFECTS.....     | 8  |
| 3.4.4 ANALYZE PROPOSED ARCHITECTURE .....         | 8  |
| 3.5 EVALUATE THE IMPLEMENTATION .....             | 9  |
| 3.5.1 VERIFY IMPLEMENTATION.....                  | 9  |
| 3.5.2 ASSESS UNINTENDED BEHAVIORS .....           | 9  |
| 3.5.3 EVALUATE IMPLEMENTATION.....                | 10 |
| WG-63 MEMBERSHIP .....                            | 11 |
| IMPROVEMENT SUGGESTION FORM.....                  | 17 |

## TABLE OF FIGURES

|                                                  |   |
|--------------------------------------------------|---|
| Figure 1: Development assurance principles ..... | 5 |
|--------------------------------------------------|---|

## CHAPTER 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.

## CHAPTER 2

### REFERENCES AND DEFINITIONS

#### 2.1 REFERENCES

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.

[1] ED-79/ARP4754 Guidelines for Development of Civil Aircraft and Systems, EUROCAE, November 1996

Available from [EUROCAE eShop](#) or [www.sae.org](http://www.sae.org).

[2] AC 25.1309 System Design and Analysis, FAA

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866 835 5322, [www.faa.gov](http://www.faa.gov).

[3] TAEsdaT2-5241996 Task 2 - System Design and Analysis Harmonization and Technology Update, FAA

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866 835 5322, [www.faa.gov](http://www.faa.gov).

#### 2.2 DEFINITIONS

|                       | DEFINITION                                                                                                                                                                                                                                              |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 [2]).   |
| 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 [2]).                                                                                         |
| 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 [2]). |
| 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 [2]).                                                                                                                                                                                                                                                       |
| FAILURE<br>CONDITION<br>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<br>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<br>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<br>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.                                                                                                                                                                                                                                                                                                                                                             |