



ER-33

RATIONALE FOR A SOFTWARE DEVELOPMENT ASSURANCE STANDARD FOR LOWER-RISK AVIATION APPLICATIONS

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.

MAY 2024

FOREWORD

This document was developed by EUROCAE Working Group 127 “Lower-risk Aviation Applications”, and was approved by the Working Group 127 on 27 May 2024.

1. 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 of our members and stakeholders across the global aviation community.
2. 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”.
3. 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.

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.

4. 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

Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	i
TABLE OF CONTENTS	ii
TABLE OF FIGURES	ii
TABLE OF TABLES	ii
CHAPTER 1 INTRODUCTION	1
CHAPTER 2 CONTEXT	2
CHAPTER 3 DEFINITION OF LOWER RISK	4
CHAPTER 4 KEY ASPECTS.....	9
CHAPTER 5 METHODOLOGY	11
WG-127 MEMBERSHIP	A-1
IMPROVEMENT SUGGESTION FORM.....	B-1

TABLE OF FIGURES

FIGURE 2-1: RELATIONSHIP OF WG-127 TO OTHER WORKING GROUPS OF INTEREST	3
--	---

TABLE OF TABLES

TABLE 3-1 POTENTIAL SCOPE FOR LOWER-RISK SOFTWARE DEVELOPMENT ASSURANCE LEVELS FOR NORMAL CATEGORY AIRPLANES (ADAPTED FROM ASTM F3061).....	4
TABLE 3-2 SOFTWARE DAL REQUIREMENTS FOR SAIL III AND IV OPERATIONS.....	5
TABLE 3-3 SOFTWARE DAL REQUIREMENTS FOR LOWER-RISK ATM APPLICATIONS.....	6
TABLE 3-4 POTENTIAL SCOPE FOR LOWER RISK SOFTWARE DEVELOPMENT ASSURANCE LEVELS FOR UTM/U-SPACE APPLICATIONS	8
TABLE 5-1 EXAMPLES OF LOWER-RISK USE CASES IN GENERAL AVIATION	11
TABLE 5-2 EXAMPLES OF LOWER-RISK USE CASES IN THE UAS DOMAIN	12
TABLE 5-3 EXAMPLES OF LOWER-RISK USE CASES IN THE UTM/ U-SPACE DOMAIN	12

CHAPTER 1

INTRODUCTION

1.1 PURPOSE

EUROCAE Working Group 127 (WG-127) on Lower-risk Aviation Applications committed in September 2023 to develop a Software Development Assurance Standard for Lower-Risk Aviation Applications. The purpose of this report is to provide the industry and potential users such as, Unmanned Aircraft Systems (UAS), Unmanned Traffic Management (UTM), U-space, and General Aviation (GA¹) communities with an understanding and rationale for the scope, background, and methodology behind the new standard in its initial phases of development.

1.2 SCOPE

The report contains contextual information for the reader to understand the motivation behind the WG-127 efforts, the regulatory framework for which the deliverables are created, and key aspects that shape the development of the standard. It also contains the proposed methodology for the ED created by WG-127 and a roadmap for the creation of the ED.

1.3 STAKEHOLDERS

This ER is aimed at manufacturers, service providers, and operators creating software for lower-risk aviation applications in the GA, UAS and UTM/U-space industry as direct consumers and users of this standard. The ER is also aimed at regulatory authorities who may recognize this standard as an acceptable means of compliance to software assurance requirements for lower risk aviation applications.

¹ The usage of GA in this document is intended to cover both normal category airplanes (CS-23 in Europe) and small category rotorcraft (CS-27 in Europe) categories. VTOL aircraft are not covered under the use of GA in this document.

CHAPTER 2

CONTEXT

2.1 WG-127 TERMS OF REFERENCE

The EUROCAE Working Group on Lower-risk Aviation Applications was approved in April 2023 by the EUROCAE Council following the recommendation of the Technical Advisory Committee. The terms of reference were approved under the following description.

Sourced from the Terms of Reference, revision of March 2024:

“The regulatory framework of certain lower-risk applications for VTOL, UAS, UAS Traffic Management (UTM), and General Aviation (GA) is evolving. EASA has established UAS regulation in Europe around three operational categories- open, specific and certified. Whereas the risk of the operation in the open category is reduced through operational mitigations and the certified category is not fully defined but expected to be aligned along traditional development assurance guidelines (e.g. ED-12/DO-178), there is a lack of guidance for the specific category, particularly for the medium risk (i.e. SAIL III and IV) UAS operations, including services facilitated by UTM.

EASA has also released their Net Safety Benefit policy introducing proportionality via reduced Development Assurance Level (DAL) for certain GA CS-23 airplanes and CS-27 rotorcraft when a net safety benefit can be shown.

The continued release of information on UAS development and UAS operations by EASA, advances in UTM services, and continued work towards proportionate approaches to certification for GA airplanes and small rotorcraft provides an opportunity for a new software development assurance standard that will be tailored to lower-risk aviation applications such as the specific UAS category defined by EASA, UTM, and certain GA airplanes and rotorcraft. The VTOL industry may also benefit from a simplified software development assurance methodology.”

The new standard produced by this working group should also facilitate the introduction of:

- New technological aspects non-typical to aviation (e.g. cloud computing vs platform/target computers);
- New verification approaches to address robustness aspects; and
- Approaches enabling regular or faster software product release (e.g. regular cyber security updates or mitigating immediate threats)

2.2 PARTICIPANTS

At the time of publication of this ER, WG-127 is composed of participants from the GA, UAS and UTM industry, researchers from the UAS and GA domains as well as regulators from various countries across the world (e.g. EASA, FAA, ANAC, DGA).

2.3 RELATION TO OTHER WORKING GROUPS IN EUROCAE

FIGURE 2-1 provides an overview of the different EUROCAE working groups with which WG-127 is attempting to coordinate and the potential scope of information that could be exchanged between the working groups and WG-127. Readers may refer to the Terms of Reference of the respective working groups for a more authoritative description of the scope of the individual working groups, including WG-127.

2.3.1 WG-63 Complex Aircraft Systems

WG-63 SG-1 is developing an EUROCAE report evaluating the applicability of existing development assurance and system safety practices to UAS and VTOL.

WG-127 will liaise with WG-63 SG-1 to coordinate system-level aspects of certification and provide input on software aspects of lower-risk aviation applications.

2.3.2 WG-105 Unmanned Aircraft Systems

WG-105 is tasked to develop standards and guidance documents that will allow the safe operation of UAS in all types of airspace, at all times and for all types of operations.

WG-127 will liaise with WG-105 to solicit participation in peer reviews and consultations to receive feedback from key user groups in the UAS and UTM communities.

2.3.3 WG-114 Artificial Intelligence

The primary scope of WG-114 is preparing technical standards, guides, and any other material required to support the development of systems and the certification of aeronautical systems implementing AI technologies.

WG-127 will liaise with WG-114 to solicit participation in peer reviews and consultations to receive feedback from key user groups creating AI-based lower-risk aviation applications.

2.3.4 WG-117 Aviation Software Standards

WG-117 is tasked with developing aviation software standards working jointly with RTCA SC-240. WG-117 SG-2 is developing a supplement to ED-12C/DO-178C or ED-109A/DO-278A for the approved use of Off the Shelf Software² (OTSS) and consideration of service history for credit.

WG-127 will coordinate with WG-117 through a steering committee to avoid any inconsistencies and duplications.

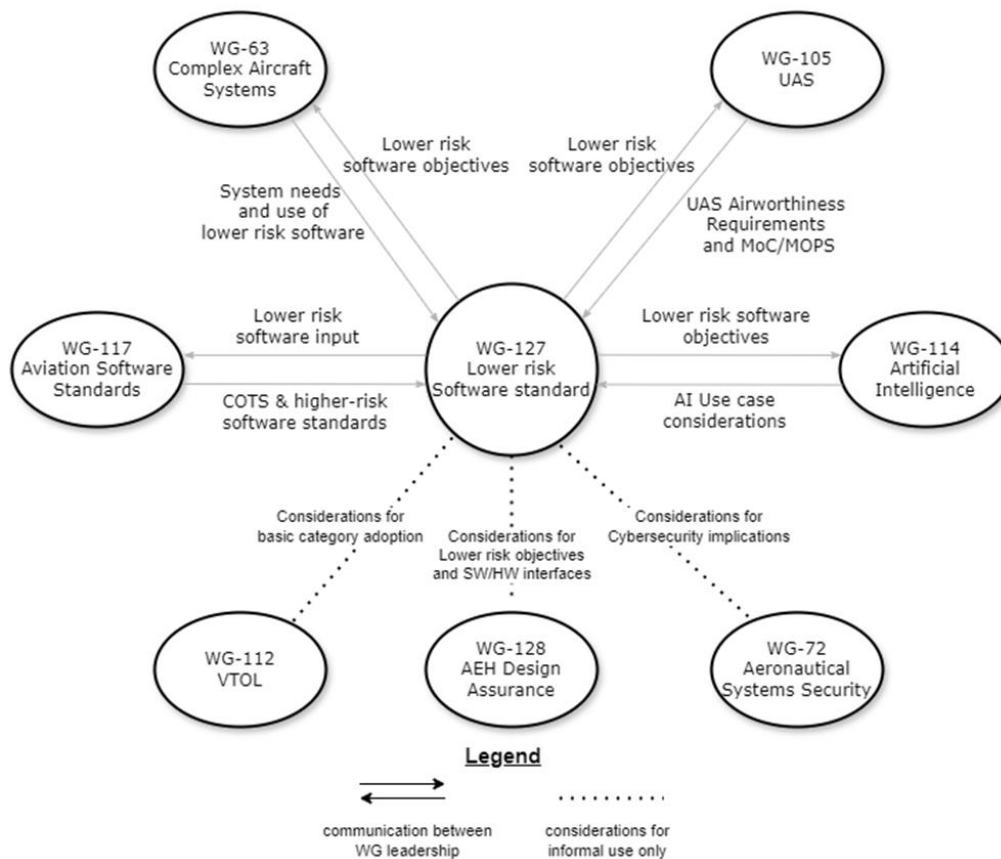


FIGURE 2-1: RELATIONSHIP OF WG-127 TO OTHER WORKING GROUPS³ OF INTEREST

² Off the Shelf Software (OTSS) is the term used by WG-117 SG-2 to refer to Commercial-Off-The-Shelf (COTS) and Open Source Software.

³ The list of working groups described in Section 2.3 is not exhaustive and may include WG-72 (Aeronautical Systems Security), WG-112 (VTOL), and WG-128 (Airborne Electronic Hardware Design Assurance). Additional working groups may find the deliverables of WG-127 relevant to their efforts.

CHAPTER 3

DEFINITION OF LOWER RISK

3.1 INTRODUCTION

One of the main goals of WG-127 is the creation of development assurance objectives for lower-risk software applications. There may be applications currently classified in different (higher or lower) development assurance levels that may serve as potential candidates for this standard. While the attribution of new development assurance levels and their correlation to safety/risk levels is finally determined by the certification authorities, the initial proposal for such changes may be put forward in the scope of this working group. In this chapter, the regulatory framework for the different stakeholder domains of WG-127 is studied and candidates (i.e. safety levels) for the application of lower-risk software assurance objectives are identified. Potential candidates are identified in the respective tables with an asterisk.

3.2 GENERAL AVIATION

General Aviation Assessment Levels I⁴ and II and Small Rotorcraft Class I and II have Development Assurance Level (DAL) C as the highest safety objective.

The table below is adapted from ASTM F3061, and AMC1 27.1309. ASTM F3061 is accepted as a means of compliance with the so-called “system safety requirement” CS 23.2510 while AMC1 27.1309 is accepted for CS 27.1309. TABLE 3-1 highlights through an asterisk where modulation of the objectives may be available to applicants.

TABLE 3-1 POTENTIAL SCOPE FOR LOWER-RISK SOFTWARE DEVELOPMENT ASSURANCE LEVELS FOR NORMAL CATEGORY AIRPLANES (ADAPTED FROM ASTM F3061)

Assessment Level	Classification of Failure Conditions				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
	Software (SW) Development Assurance Levels (DALs)				
I	No SW DAL requirement	D*	C*	C*	C*
II		D*	C*	C*	C*
III		D	C*	C	B
IV		D	C	B	A

Based on this table, it is identified by the working group that General Aviation and Small Rotorcraft could not only benefit in this category from a streamlined Development Assurance Process that equates to DAL D and DAL C but also from a Development Assurance Level between the two.

Further, EASA’s Net Safety Benefit Certification Memorandum [CM-SA-001] has provided applicants with the possibility to reduce DAL for certain Major changes to an existing Type Certificate or Supplemental Type Certificate when the change provides operational safety benefit. This currently may allow a reduction to DAL D for Major and Hazardous failure conditions in these categories (CS-23 Assessment level I and II and CS-27 Class I and II), although CM-SA-001 states additional conditions and limitations may be required for Hazardous failure conditions. It is identified by the working group that the application of EASA’s Net Safety Benefit policy may benefit from a new DAL

⁴ Assessment Level I airplanes with Low-Stall, VFR only characteristics are excluded from consideration for the purposes of this document, as such airplanes may not require any software development assurance activities.