

ED-280

GUIDELINES FOR UAS SAFETY ANALYSIS FOR THE SPECIFIC CATEGORY (LOW AND MEDIUM LEVELS OF ROBUSTNESS)

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.

DECEMBER 2020

FOREWORD

1. This document was prepared by EUROCAE Working Group 105 “Unmanned Aircraft Systems (UAS)” Sub-Group 6 “Specific Operational Risk Assessment” and was approved by the Council of EUROCAE on 7 December 2020.
2. 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.
3. 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”.
4. 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.
5. 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.
6. 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
CHAPTER 1 INTRODUCTION	1
1.1 SCOPE OF THE REPORT	1
1.2 REPORT CONTENT	1
CHAPTER 2 GUIDELINES FOR LOW LEVEL OF ROBUSTNESS	2
2.1 INTRODUCTION	2
2.2 OVERVIEW OF STEPS TO PERFORM THE SAFETY ANALYSIS	2
2.3 SAFETY OBJECTIVES FOR OSO#5 IN LOW LEVEL OF ROBUSTNESS.....	2
2.4 HAZARDS CLASSIFICATION	3
2.5 DEFINITION OF FLIGHT PHASES	3
2.6 IDENTIFICATION OF FAILURE CONDITIONS AND PROBABLE FAILURES	3
2.7 VERIFICATION THAT SAFETY OBJECTIVES ARE FULFILLED.....	4
CHAPTER 3 GUIDELINES FOR MEDIUM LEVEL OF ROBUSTNESS.....	6
3.1 INTRODUCTION	6
3.2 OVERVIEW OF STEPS TO PERFORM THE SAFETY ANALYSIS	6
3.3 SAFETY OBJECTIVES FOR OSO#5 IN MEDIUM LEVEL OF ROBUSTNESS	7
3.4 HAZARDS CLASSIFICATION	8
3.5 DEFINITION OF FLIGHT PHASES	8
3.6 FAILURE MODES.....	8
CHAPTER 4 CONCLUSIONS.....	9
APPENDIX A ACRONYMS AND GLOSSARY OF TERMS.....	10
APPENDIX B REFERENCES	11
APPENDIX C HAZARD CLASSIFICATION	12
APPENDIX D EXAMPLE OF FUNCTIONAL HAZARD ASSESSMENT FOR LOW LEVEL OF ROBUSTNESS	13
APPENDIX E WG-105 SG-61 MEMBERSHIP	31
IMPROVEMENT SUGGESTION FORM	32

CHAPTER 1

INTRODUCTION

1.1 SCOPE OF THE REPORT

This document contains guidelines for a UAS operator or manufacturer in order to obtain the evidence that the UAS is designed considering system safety and reliability and perform the required safety analyses to fulfil part of OSO#5 requirements, for low and medium level of robustness, as part of the SORA risk assessment (AMC1 to Article 11 Rules for conducting an operational risk assessment in [1]) under the Specific category of EASA drone regulation [2].

With respect to the high level of robustness, this document does not enter into details but the following general guidelines are suggested for high level of robustness in OSO#5:

- A quantitative safety analysis is required (see OSO#5 description in AMC1 to Article 11 in [1]).
- This safety analysis can be performed following a version adapted for UAS of ARP 4761 and ED-79A/ARP 4754A, and after due tailoring of probability / FDAL requirements.

Finally, this guideline is currently focused on safety assessment aspects and does not cover development assurance objectives or the applicability of relevant industry standards for AEH and/or SW where and if required by the Certifying authority in the Specific Category to meet OSO#5. Development assurance aspects for AEH and SW for UAS, depending on robustness levels, will be covered in future EUROCAE standards.

1.2 REPORT CONTENT

The report is divided in the following Chapters:

- Chapter 2: presents the guidelines to perform the safety analysis required to fulfil part of OSO#5 requirements for the low level of robustness.
- Chapter 3: presents the guidelines to perform the safety analysis required to fulfil part of OSO#5 requirements for the medium level of robustness.
- Chapter 4: presents the conclusions of the report.

CHAPTER 2

GUIDELINES FOR LOW LEVEL OF ROBUSTNESS

2.1 INTRODUCTION

This Chapter summarizes the proposed procedure that a UAS operator or manufacturer has to perform in order to develop the safety analysis required to fulfil part of OSO#5 requirements for low level of robustness. In particular, these guidelines cover:

Level of integrity:

Criteria	Covered by these guidelines
The equipment, systems, and installations are designed to minimise hazards in the event of a probable malfunction or failure of the UAS.	Yes, the complete criteria

Level of assurance:

Criteria	Covered by these guidelines
A functional hazard assessment and a design and installation appraisal that shows hazards are minimised, are available.	Only the part of a functional hazard assessment.

Then, apart from fulfilling these guidelines, in order to fulfil OSO#5, it is necessary to provide a design and installation appraisal. However, it is planned to include this part in a future version of these guidelines. Anyway, the correctness and suitability of this should also be within the scope of the required safety analysis.

2.2 OVERVIEW OF STEPS TO PERFORM THE SAFETY ANALYSIS

The following steps are recommended to perform the safety analysis at low level of robustness for OSO#5:

1. Define CONOPS.
2. Describe UAS architecture, including: functions, systems, and implementation.
3. Identify and classify failure conditions.
4. Complete probable failure analysis (using FMEA-like technique).
5. Verify that safety objectives are fulfilled.

If the defined CONOPS and described UAS architecture do not fulfil the required safety objectives, then, the UAS operator or manufacturer should revise the CONOPS and/or UAS architecture and perform again the complete analysis until the required safety objectives are fulfilled.

A complete example of these steps can be found in Appendix D.

2.3 SAFETY OBJECTIVES FOR OSO#5 IN LOW LEVEL OF ROBUSTNESS

As it is indicated above, the final step of the safety analysis is to check if the current UAS system fulfils the safety objectives. For OSO#5 and the low level of robustness, it is proposed to show compliance with the minimization of hazard criterion by fulfilling the following objectives:

- No probable¹ failure results in catastrophic or hazardous failure condition(s), and
- The probability of having a Major failure condition is reduced. This reduction should be performed as far as practicable (e.g. if there is technology available on the market at a reasonable price). Anyway, early concurrence with authorities is highly recommended on these aspects.

However, and due to its low impact on the overall safety of the UA system at the low level of robustness, no objective for minor failure conditions is considered. It is

¹ Probable is considered as “anticipated to occur one or more times during the entire system/operational life of the UAS”.

important to mention that these safety objectives have been deducted from the OSO#5 text (from AMC1 to Article 11 in [1]), that says:

“The equipment, systems, and installations are designed to minimize hazards² in the event of probable malfunction or failure of the UAS”

On the other hand, the UAS operator or manufacturer should revise and modify the CONOPS and UAS architecture until it fulfils these safety objectives (using the FMEA-type table as a tool to create the evidence of this fulfilment). It is important to take into account that changes of CONOPS and UAS architecture will affect the SORA analysis and the fulfilment of other OSOs. Therefore, these changes will require a revision of the complete SORA analysis and the rest of OSOs and cannot be made isolated as changes that only affect OSO#5.

Finally, for OSO#5, the unmanned aircraft, control station and other aircraft systems of the overall system should be considered. External systems like the ones related to GNSS, U-space or Communication Service Providers are not considered for the development of the required functional hazard assessment for OSO#5. However for OSO#10 and OSO#12 external systems supporting the operation should be considered, but as stated in SORA, the objective of OSO#10 and OSO#12 is to complement the technical containment safety requirements by addressing the risk of a fatality while operating over populated areas or gatherings of people, and therefore, their objectives are different than OSO#5 objective. However, and due to the complementarities between OSO#5, OSO#10, OSO#12 and step 9 (containment), in future versions of the standard it may be considered to produce a common guidelines that covers all of them.

2.4 HAZARDS CLASSIFICATION

It is proposed to use the hazards classification that appears in [5]. To facilitate the comprehension of these guidelines, this classification can be found in Appendix C.

2.5 DEFINITION OF FLIGHT PHASES

For this low level of robustness, and in order to simplify the functional hazard assessment, the following flight phases are proposed, which may vary as a function of operating area or altitude (as minimum):

Taxi	The aircraft is moving on the ground prior to takeoff and after landing
Takeoff	From the application of takeoff power, to minimum safe manoeuvring altitude
En route	The aircraft is flying (after taking-off and before approach procedure is started)
Approach	Final manoeuvre to obtain approach fix to landing area
Landing	The UA touches down and exits the Landing Area, or comes to a stop on the Landing Area, or when power is applied for takeoff, dependent on intended action after landing

The taxi flight phase will only be considered if it is applicable. For example, in conventional helicopter or multirotor aerial platforms, it is not applicable. Additionally, other flight phases could be added for multirotor platforms such as hover (the aircraft is flying but loitering in a small area).

2.6 IDENTIFICATION OF FAILURE CONDITIONS AND PROBABLE FAILURES

In order to facilitate the identification of failure conditions, it is proposed that the UAS operator and manufacturer perform the following steps:

- Identify the main systems of the unmanned aircraft and control station from the described architecture.
- For each of these systems, identify all the subsystems.

² For the purpose of this assessment, the term ‘hazard’ should be interpreted as a failure condition that relates to major, hazardous, or catastrophic consequences.

- For each subsystem, identify the main functionalities that these subsystems perform.
- Perform FHA at UAS level³ taking into account the following recommendations:
 - At this low robustness level, at least two failure modes should be considered as a minimum: total loss and malfunction.
 - The “Effect” and “Hazards severity classification” should be assessed at UAS level and not at subsystem level and may account for CONOPS specificities.
 - The failure of the system providing the mitigation should be also be considered in the development of the functional hazard assessment.
- Finally, for each functionality answer to the question:
 - *Is any malfunction or failure of this function anticipated to occur one or more times during the entire system/operational life of an UAS?*

In order to establish a methodology to help the operator and manufacturer to define if failure or malfunction of a function is probable or not, it is suggested that the operator and manufacturer establishes the operational life of the UAS systems. Then, it can be easily related to a quantitative probability of failure. For example, if the operational life of the UAS system is set to 1.000 hours and a subsystems has a MTBF (Mean Time Between Failures) of 10.000 hours, then it can be reasonable to assume that this subsystem will not fail during the operational life of the UAS. However, it is important to point out that setting up the operational life of the UAS will have an impact on the procedures and operations of the UAS. If the operator or manufacturer does not want to establish an operational life of the UAS (or they do not have enough information to do that), it can always be considered that all the functions can fail during the operational life of the UAS, and all of them should be considered in the functional hazard assessment (next step of the procedure).

In order to perform this analysis, a table similar to the one below can be used:

UAS system	Subsystem	Function	Is this function probable to malfunction or fail during the lifetime of the UAS?

2.7

VERIFICATION THAT SAFETY OBJECTIVES ARE FULFILLED

To verify that the safety objectives are fulfilled, it is proposed to use a FMEA-type table, as shown below. This table should only be completed for the functions that are probable to malfunction or fail during the lifetime of the UAS.

The FMEA-type table has been chosen in order to demonstrate, with a basic analysis, that the operation is safe. A combination of FHA and FTA analyses was considered not proportional and too complex for a low level of robustness. The FMEA-like technique is adequate in this case since the requirement is limited to probable failure.

Also, mitigations must be independent from the subsystem failure mode.

It is important to highlight that:

- There must be no common probable failure affecting the subsystem and the system providing the mitigation, and
- the combined failure affecting the subsystem and the system providing the mitigation should not be probable⁴.

³ Guidance material for developing FHA can be found in Appendix A of ARP 4761. Also, specific and useful material for developing FHA at UAS level can be found in [3] and in [4].

⁴ Probable is considered as “anticipated to occur one or more times during the entire system/operational life of the UAS”.

UAS system	Subsystem	Function	Failure mode	Failure description	Potential cause(s)	Flight phase	Effect	Detection method	Detection Dormancy Period	Mitigations	Hazards severity classification	Remarks

CHAPTER 3

GUIDELINES FOR MEDIUM LEVEL OF ROBUSTNESS

3.1

INTRODUCTION

This Chapter summarizes the proposed procedure that a UAS operator or manufacturer has to perform in order to develop the safety analysis required to fulfil part of OSO#5 requirements for medium level of robustness. In particular, these guidelines cover:

Level of integrity:

Criteria	Covered by these guidelines
The equipment, systems, and installations are designed to minimise hazards in the event of a probable malfunction or failure of the UAS. In addition, the strategy for detection, alerting and management of any malfunction, failure or combination thereof, which would lead to a hazard, is available.	Only the first part (The equipment, systems, and installations are designed to minimise hazards in the event of a probable malfunction or failure of the UAS.)

Level of assurance:

Criteria	Covered by these guidelines
A functional hazard assessment and a design and installation appraisal that shows hazards are minimised, are available. In addition: (a) Safety analyses are conducted in line with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. (b) A strategy for the detection of single failures of concern includes pre-flight checks.	Only the part of a functional hazard assessment, and also the part of Safety analyses are conducted in line with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.

Then, there are other requirements to fulfil completely OSO#5 for medium level of robustness, for example a strategy for detection, alerting and management of any malfunction, failure or combination thereof is also required, that are not covered in these guidelines. However, it is planned to include this part in a future version of these guidelines. Anyway, the correctness and suitability of these functions should also be within the scope of the required safety analysis.

3.2

OVERVIEW OF STEPS TO PERFORM THE SAFETY ANALYSIS

The following steps are recommended to perform the safety analysis at medium level of robustness for OSO#5:

1. Define CONOPS.
2. Describe UAS architecture, including: functions, systems, and implementation; and the rationale for this choice.
3. Perform FHA at UAS level⁵. It is important to take into account that failure hazard classification may account for CONOPS specificities.

⁵ Guidance material for developing FHA can be found in Appendix A of ARP 4761. Also, specific and useful material for developing FHA at UAS level can be found in [3] and in [4].

4. Complete qualitative Fault Tree Analysis (FTA)⁶ related to Major, Hazardous and Catastrophic events at UAS level in order to describe the interrelation between failures of the UAS and subsystems functions.
5. Verify that safety objectives are fulfilled.

A complete example of these steps has not been included due to its complexity. However, examples of FHA and FTA at aircraft level can be found in Appendices A and D of ARP 4761.

3.3

SAFETY OBJECTIVES FOR OSO#5 IN MEDIUM LEVEL OF ROBUSTNESS

As it is indicated above, the final step of the safety analysis is to check if the current UAS system fulfils the safety objectives. For OSO#5 and the medium level of robustness, it is proposed to show compliance with the minimization of hazard criterion by fulfilling the following objectives:

- No probable⁷ failure results in catastrophic or hazardous failure condition(s), and
probability of having a Major failure condition is reduced. This reduction should be performed as far as practicable (e.g. if there is technology available on the market at a reasonable price). Anyway, early concurrence with authorities is highly recommended on these aspects.

However, and due to its low impact on the overall safety of the UAS system at the medium level of robustness, no objective for minor failure conditions is considered. It is important to mention that these safety objectives have been deducted from the OSO#5 text (from AMC1 to Article 11 in [1]), that says:

“The equipment, systems, and installations are designed to minimize hazards in the event of probable malfunction or failure of the UAS”

On the other hand, the UAS operator or manufacturer should revise and modify the CONOPS and UAS architecture until it fulfils these safety objectives. It is important to take into account that changes of CONOPS and UAS architecture will affect the SORA analysis and the fulfilment of other OSOs. Therefore, these changes will require a revision of the complete SORA analysis and the rest of OSOs and cannot be made isolated as changes that only affect OSO#5.

Finally, and as commented in previous Chapter, for OSO#5, the unmanned aircraft, control station and other aircraft systems of the overall system should be considered. External systems like the ones related to GNSS, U-space or Communication Service Providers are not considered for the development of the required functional hazard assessment for OSO#5. However for OSO#10 and OSO#12 external systems supporting the operation should be considered, but as stated in SORA, the objective of OSO#10 and OSO#12 is to complement the technical containment safety requirements by addressing the risk of a fatality while operating over populated areas or gatherings of people, and therefore, their objectives are different than OSO#5 objective. However, and due to the complementarities between OSO#5, OSO#10, OSO#12 and step 9 (containment), in future versions of the standard it may be considered to produce a common guideline that covers all of them.

⁶ If preferred, quantitative FTA could also be used to fulfill OSO#5 requirements.

⁷ Probable is considered as “anticipated to occur one or more times during the entire system/operational life of the UAS”.

3.4 HAZARDS CLASSIFICATION

It is proposed to use the hazards classification that appears in [5]. To facilitate the comprehension of these guidelines, this classification can be found in Appendix C.

3.5 DEFINITION OF FLIGHT PHASES

For this medium level of robustness, and in order to simplify the FHA, the same flight phases (as minimum), already proposed for the low level of robustness, will be also proposed (see Section 2.5 for more details).

3.6 FAILURE MODES

It is considered that, at this medium robustness level, common failure modes should be taken into account, i.e., total loss, partial loss and malfunction.