

SUBJECT : UAS is designed considering system safety and reliability

REQUIREMENTS incl. Amdt. : Operational Safety Objectives #05/10/12 as per Annex E to AMC1 to Article 11 of Regulation (EU) 2019/947

ASSOCIATED IM/MoC : Yes / No

ADVISORY MATERIAL : N/A

Table of Content

1. Purpose	2
2. Applicability	2
3. Reference Documents	2
4. Definitions	3
5. Operational Safety Objective #05 – System Safety and Reliability – Low level of robustness	4
6. Compliance evidence for OSO #05	4
7. Guidance on safety assessment as per ED-280	5
7.1 Guidance for the description of functional and operational principles of the UAS and its architecture	5
7.2 Guidance for the UAS level FHA	5
7.3 Guidance on FHA/FMEA	7
8. Guidance on Design and Installation appraisal	8
9. Operational Safety Objective #10/12 – System Safety and Reliability – Low level of robustness ..	9
10. Compliance evidence for OSO#10/12	9
10.1 Guidance on OSO#10/12 applicability	9
10.2 Guidance on common cause analysis as per ED-280	9

1. Purpose

This MOC describes an accepted means for declaring compliance with the requirements of OSO #05 within the frame of an operational authorization process as per Article 11 of regulation (EU) 2019/947.

2. Applicability

This MOC is applicable to UAS intended to operate in SAIL III operations for which an EASA Design Verification is not deemed necessary.

While OSO#05 does not apply to the performance and structural requirements of the UAS, it does apply to any system on which compliance with any of those other requirements are based. For example, it does not apply to unmanned aircraft (UA) stability characteristics, but it does apply to a stabilisation system.

This MOC covers the complete Unmanned Aircraft System, which is comprised of the unmanned aircraft and the equipment to control it remotely (command unit).

This MOC does not cover cybersecurity (addressed under in SAIL III under OSO#6) and qualification (e.g. HIRF/EMI) aspects which should be addressed under OSO #24. However, interactions and interfaces between the system safety assessment process and the security and qualification assessment process exist, as the classification of failure condition is usually used as an input for cybersecurity and qualification processes. Therefore, should a function be implemented, or a system/equipment installed on the aircraft as a result of the airworthiness security assessment process, this function or system/equipment needs to undergo the system safety assessment process.

Artificial Intelligence technologies are not covered by this MOC and will require particular compliance demonstration.


3. Reference Documents

The following references are quoted in different sections of this MOC as a source of additional guidance:

- (a) EUROCAE ED-280 initial revision, Guidelines for UAS Safety Analysis for the specific category (low and medium levels of robustness)
- (b) ASTM F3309-21, Standard Practice for Simplified Safety Assessment of Systems and Equipment in Small Aircraft
- (c) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for development of civil aircraft and systems.
- (d) EASA AMC 20-115D – Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178
- (e) EASA AMC 20-152A – Development Assurance for Airborne Electronic Hardware (AEH)

4. Definitions

- (a) Development Assurance: 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. (Source: ED-79A/ARP4754A).
- (b) Development Assurance Level (DAL): the level of rigor of development assurance tasks necessary to demonstrate compliance with OSO #05 and OSO #10/12 (Source: adapted from ED79A/ARP4754A). The DALs are determined by the system safety assessment process.
- (c) Failure: an occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). Errors may cause failures, but are not considered to be failures. Some structural or mechanical failures may be excluded from the criterion if it can be shown that these mechanical parts were designed according to aviation industry best practices; (Source: Regulation 2019/947)
- (d) Failure Condition: A condition having an effect on the UA (incl. separation assurance), the remote crew and/or third parties, either direct or consequential, which 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. (Source: adapted from SC-RPAS.1309)
- (e) Hazard: A failure condition that relates to major, hazardous, or catastrophic consequences. (Source: AMC to Regulation 2019/947)
- (f) Probable Failure Condition: Probable Failure Conditions are those that are anticipated to occur one or more times during the entire operational life of each UAS. (Source: AMC to Regulation 2019/947)

 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#05/10/12</p> <p>“System safety and reliability”</p>	<p>Doc. No. : MOC OSO #05/10/12 -01</p> <p>Issue : 1</p> <p>Date : 18 Dec 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p> <p>Deadline for comments:</p>
--	--	---

5. Operational Safety Objective #05 – System Safety and Reliability – Low level of robustness

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

A functional hazard assessment and a design and installation appraisal that shows hazards are minimised, are available.”

The following Safety Objective should be demonstrated for medium risk UAS (SAIL III):

- Failure conditions leading to the loss of control of the operation should not be probable.
- SW/AEH whose development error(s) could directly result in the loss of control of operation should be developed to DAL D

In order to demonstrate compliance with OSO#05, ED-280 can be followed to perform the safety assessment. The applicant should conduct a Functional Hazard Analysis as per Eurocae ED-280, which identifies all failure conditions at UAS level.

Explanatory Note:

The medium risk UAS operation safety objectives and their compliance substantiation methods are of a qualitative nature. This is intended to be proportionate with the operational risk and ease the burden on applicants that might not be familiar with traditional Safety Assessment methods and processes. However, if an applicant intends to conduct a quantitative assessment, it should verify that the sum of the probabilities of all failure conditions leading to a loss of control is inferior to $5 \times 10^{-4}/FH$, under the assumption that half of the loss of control events will be caused by a technical issue. This should be substantiated with a FHA, a FTA and a FMEA as needed.

6. Compliance evidence for OSO #05


Task description:

The applicant should perform the following compliance demonstration activities with adequate confirmation of the compliance:

- Perform and document a safety assessment as per ED-280 containing
 - o Description of functional and operational principles of the UAS and its architecture
 - o UAS level FHA
 - o FMEA-like analysis
- Perform a design and installation appraisal as per ASTM F3309-21.
- Provide additional evidences as needed for substantiating compliance with the Tactical Mitigation Performance Requirements (TMPRs).

Upon establishment of the above listed compliance evidence, the applicant could declare that hazards in the event of any probable failure or malfunction are minimised.



 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#05/10/12</p> <p>“System safety and reliability”</p>	<p>Doc. No. : MOC OSO #05/10/12 -01</p> <p>Issue : 1</p> <p>Date : 18 Dec 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p> <p>Deadline for comments:</p>
--	--	---

7. Guidance on safety assessment as per ED-280

7.1 Guidance for the description of functional and operational principles of the UAS and its architecture

The description should provide an understanding of the physical and mechanical operation of the UAS, the architecture including functions, systems and implementation.

The level of detail in the content should be limited to the information that will contribute to the substantiation of the hazard assessment in the steps below.

7.2 Guidance for the UAS level FHA

Severity Classification

In order to simplify the safety analysis, only failure conditions, which lead to a loss of control of operation should be further assessed. Failure conditions not resulting in the loss of control of the operation do not need to be further assessed. When the applicant decides to use the definitions of failure conditions severities as stated in JARUS AMC RPAS.1309 Issue 2 (i.e. NSE, MIN, MAJ, HAZ, CAT), the following mapping should be applied.

Failure Condition severity classification as per JARUS AMC RPAS.1309 Issue 2	Failure condition effect	Qualitative Safety Objective
Minor	No loss of control of operation	None
Major	No loss of control of operation	None
Hazardous	Loss of control of operation	Less than probable
Catastrophic	Loss of control of operation, but fatalities are not expected in SAIL III operations	Less than probable



Explanatory Note:

The definitions of failure conditions severities used in JARUS AMC RPAS.1309 Issue 2 (i.e. NSE, MIN, MAJ, HAZ, CAT) were developed for the certified UAS category. However in the specific category, the SORA concept develops specific operational and technical requirements which should result in the target level of safety for the whole operation. This TLOS is the combination of the probability of loss of control and the probability to cause a fatality as a consequence of the loss of control. In SAIL III operation a probability of fatality after a loss of control of operation is assumed to be 1/1000, which is acceptable to meet the target level of safety. Consequently, a failure condition leading to a loss of control of operation is not expected to lead to a fatality (it would be equivalent to “Hazardous” according to JARUS RPAS.AMC.1309). However, if loss of control events occurs too frequently the Target Level of Safety (TLOS) would not be met. Therefore, the applicant should verify that failure conditions leading to a loss of control are not probable.

Loss of control of operation definition

In this MoC, the loss of control of operation should be understood as in the SORA semantic model, limited to technical failures and malfunctions. Situations where the control of the operation is considered to be lost shall be identified by the applicant. Typical examples are e.g.:

- Crash of the UA with the ground/infrastructure/people
- Unrecoverable loss of controllability
- Controlled flight into terrain (e.g. remote pilot receives misleading flight or position data)
- Emergency situation leading to activation of flight termination system/parachute/other M2 mitigation
- Erroneous activation of flight termination system/parachute/other M2 mitigation
- UA leaving the operational volume
- System failure leading to loss of payload (Detachment of a part or a load heavy enough to create a risk for people on ground)

Explanatory Note:

The above list of events classified as “loss of control of operation” is exemplary and non-exhaustive. It is acknowledged that most of the stated events will ultimately lead to a “crash of the UA”. The intent is to clarify that not only the direct consequence of a technical failure should be assessed. Although SORA Step 9 addresses the case “UA leaving the operational volume”, this MoC can be used to support the compliance demonstration for the containment requirements. Although it is acknowledged that an M2 mitigation is reducing the probability to cause a fatality, it does not improve the reliability of the UAS. If a technical failure leads to the automatic or manual activation of the M2 means, it should be considered as a loss of control of operation. It should not discourage the applicant from implementing M2 mitigation, since credit can be taken for it, by reducing the SAIL.

7.3 Guidance on FHA/FMEA

The scope of the safety assessment is limited to technical failures. Other causes which could lead to loss of control of operation, like pilot error or errors in operational procedures are not considered.

The assessment should include failures of the command unit, unmanned aircraft and any system installed on the aircraft, such as flight termination system, that affect the ability to control the attitude, speed and flight path of the UA. Environmental and operational aggravating factors need to be considered when relevant (e.g. temperature, icing, night time, turbulence, etc.).

Without prejudice to the performance requirements laid out in the SORA, which should also be substantiated in the compliance evidence for OSO#05, the systems and equipment supporting the Technical Mitigations for air risk should be assessed following the same approach as other safety critical systems.

M2 mitigation or containment provisions (e.g. flight termination systems) are considered emergency systems, as they are intended to reduce the risk, after the control of the UAS has already been lost. Specific requirements can be found in Annex B to AMC1 to Article 11 (M2) and Step #9 - Adjacent area/airspace considerations. However, when installing such emergency systems, the malfunction (e.g. erroneous activation) of the system should be addressed within the safety assessment required by this MOC. The erroneous activation of a flight termination system, parachute or other M2 means, will lead to the loss of control of operation.

In the frame of ED-280, relevant service experience of similar systems may be used to substantiate that the probability of failure of this system is less than probable. Service history data are limited to the fleet of UAS for which the applicant is the holder of the operational authorization, the owner of the data, or has an agreement in place with the owner of the data that permits its use by the applicant for this purpose. The applicant should be able to substantiate that a close similarity in respect of both the system design and operating conditions exists. In case of lack of service experience, all failures are deemed to be more likely than probable (i.e. anticipated to occur one or more times during the entire operational life of each UAS). A change in design to remove the hazard or increasing redundancy to reduce the probability of failure may be needed.

The applicant should conduct a design and installation appraisal as per ASTM F3309-21 §4.4 to summarize the results of the safety assessment process.

Guidance on Development errors

The applicant should identify within the FMEA-like analysis those elements (Software (SW)/ Airborne Electronic Hardware (AEH)) whose development errors may directly lead to a loss of control. The term “directly” means, that there is no other mitigation in place which could prevent the loss of control, if a particular error leads to a failure of one or more items/equipment/system. If these elements exist, they should be developed in accordance with EASA AMC 20-115D or ASTM F3201-16, ED-80 or alternative industry standard deemed by the applicant to be appropriate to provide equivalence with DAL D objectives. If a items/equipment/system is able to prevent a loss of control due to an error in SW/AEH development in another items/equipment/system, no Development Assurance requirements would apply. Consequently, the DAL alleviation process, allowed by ARP4754A should not apply.

To propose different standards, applicants should contact their Competent Authority¹.

The applicant may use the FMEA-like analysis and of ED-280 and a Design Appraisal to demonstrate the absence of SW/HW errors that may directly lead to a loss of control of operation.

8. Guidance on Design and Installation appraisal

Design and Installation Appraisal should be used to summarize the results of the safety assessment process. They consist of a qualitative appraisal of the integrity and safety of the system design/installation. Accepted guidance for performing a Design and Installation Appraisal can be found in ASTM F3309-21 §4.4:

A design appraisal is a qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment. The design features that provide integrity and safety must be explained in a form that are easy to follow. The use of system architecture/block diagrams are effective ways to aid the understanding of the system. Other tools that can aid the design appraisal include an extended Functional Hazard Assessment table where the failure effects can be shown along with the failure mitigations. Integrity and safety considerations like the use of component qualification, independence, separation, and redundancy should be assessed as appropriate.

An installation appraisal is a qualitative appraisal of the integrity and safety of the installation. An effective appraisal requires experienced judgment. The installation features must be presented in forms that are easy to follow such as installation drawings, equipment installation requirements, and any required analyses. The appraisal must consider any potential interference with other UA systems and issues introduced by maintenance.[...] the potential for events or influences outside of the systems concerned that might invalidate independence must also be considered.²

¹ As per message provided on the EASA website and accompanying the publication of this document.

² Reprinted, with permission, from ASTM F3309/F3309M-21 Standard Practice for Simplified Safety Assessment of Systems and equipment in Small Aircraft, copyright ASTM International. A copy of the complete standard may be obtained from www.astm.org.

9. Operational Safety Objective #10/12 – System Safety and Reliability – Low level of robustness

“When operating over populated areas or assemblies of people, it can be reasonably expected that a fatality will not occur from any single failure of the UAS or any external system supporting the operation. SW and AEH whose development error(s) could directly lead to a failure affecting the operation in such a way that it can be reasonably expected that a fatality will occur, are developed to a standard considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority.

A design and installation appraisal is available. In particular, this appraisal shows that: (a) the design and installation features (independence, separation and redundancy) satisfy the low integrity criterion; and (b) particular risks relevant to the ConOps (e.g. hail, ice, snow, electromagnetic interference, etc.) do not violate the independence claims, if any. , the level of integrity claimed is substantiated by analysis and/or test data with supporting evidence”

10. Compliance evidence for OSO#10/12

Task description:

- Perform a design and installation appraisal as per ASTM F3309-21
- Perform a common cause analysis as per ED-280

10.1 Guidance on OSO#10/12 applicability

Catastrophic Failure Conditions are in principle not expected in SAIL III operations, therefore no failure conditions are reasonably expected to lead to a fatality (see also explanatory note on page 6.) This means that the OSO #10 & OSO #12 are assumed to be complied with for most UAS operating in SAIL III.

Some UAS designs may employ inherently dangerous design features or perform operations with a high risk to fatally injure persons on ground, when certain single failures are assumed to occur. Examples would be failure conditions leading to release of explosive or toxic materials or highly flammable fluids as part of the payload (not as part of propulsion system), malfunction of launch or recovery system using high energy parts/compressed gas. If these features are identified in the safety assessment process, the design and installation appraisal required for OSO#05 can be amended to verify no single failure will lead to these failure conditions.

10.2 Guidance on common cause analysis as per ED-280

Means to mitigate the effect of an otherwise critical single failure, could be of technical or operational nature (e.g. definition of controlled ground areas during critical flight phase).

Failure containment should be provided by system design to limit the propagation of the effects of any single failure to preclude loss of control of the operation.

In addition, there must be no common-cause failure, which could affect both the single components, parts, or elements, and their failure containment provisions. A single failure includes any set of failures, which cannot be shown to be independent from each other. Common-cause failures (including common mode

failures) and cascading failures should be evaluated as dependent failures from the point of the root cause or the initiator. Considerations should be given to errors in development, manufacturing, installation, and maintenance, which can result in common-cause failures (including common mode failures) and cascading failures.

When applying ED-280, possible common cause failures should be considered in the analysis and a Design and Installation Appraisal should be performed to show compliance with OSO10/12. As a minimum the following should be considered when common modes between the single component, part or element and its failure containment provision are analysed:

- Common hardware
- Common software
- Common power source
- Common resource system (input data, external services (e.g.GNSS))

This analysis should also consider particular risks relevant to the ConOps (e.g. hail, ice, snow, electromagnetic interference etc.).