EASA European Union Aviation Safety Agency	**Means of Compliance with Light-UAS.2510**	Doc. No. : MOC Light-UAS.2510-01 Issue : 1 Date : 30 Jun 2023 Proposed ☒ Final ☐ Deadline for comments: 31 Aug 2023

SUBJECT	:	Equipment, Systems and Installation
REQUIREMENTS incl. Amdt.	:	Special condition Light-UAS Medium Risk 01, point Light-UAS.2510
ASSOCIATED IM/MoC	:	Yes☐ / No ☒
ADVISORY MATERIAL	:	N/A

Table of Content

Light-UAS.2510 Equipment, Systems and Installation

(a) The equipment and systems identified in SC-Light UAS.2500, considered separately and in relation to other systems, must be designed and installed such that:

(1) hazards are minimized in the event of a probable failure;
(2) it can be reasonably expected that a catastrophic failure condition will not result from any single failure; and
(3) if the SAIL is IV, a means for detection, alerting and management of any failure or combination thereof, which would lead to a hazard, is available.

(b) Any hazard which may be caused by the operation of equipment and systems not covered by LightUAS.2500 must be minimized.

1. Purpose

This MOC describes an accepted means for showing compliance with the requirements Light-UAS.2510(a) and Light-UAS.2510(b) of SC Light-UAS Medium Risk. These means are intended to supplement the engineering and operational judgement that should form the basis of any compliance demonstration.

2. Applicability

This MOC is applicable to UAS intended to operate in SAIL IV operations and as specified in Light-UAS.2500(a), paragraph Light-UAS.2510 is intended as a general requirement, that should be applied to any equipment or system as installed, in addition to specific systems requirements, considering the following:

(a) General – Light-UAS.2510 addresses OSO #5 and OSO #10/#12 of AMC and GM to Commission Implementing Regulation (EU) 2019/947. This MOC is applicable to UAS intended to operate in SAIL IV, applying SC Light-UAS medium risk. Where a specific SORA or Light-UAS requirement exists which predefines systems safety aspects (e.g., redundancy level or criticality) for a specific type of equipment, system, or installation, then the specific Light-UAS requirement will take precedence. This precedence does not preclude accomplishment of a system safety assessment.
(b) Subpart B, C and D - While Light-UAS.2510 does not apply to the performance and flight characteristics of Subpart B and structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is based. For example, it does not apply to unmanned aircraft (UA) stability characteristics, but it does apply to a stabilisation system used to enable compliance with Light-UAS.2135.
(c) Subpart E – Lift/Thrust/Power systems installations and energy storage and distribution systems are required to comply with Light-UAS.2510, see also Light-UAS.2400(c) and Light-UAS.2430.
(d) Subpart H – C2 Link systems are required to comply with Light-UAS.2510, see also Light-UAS.2715.

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 and qualification (e.g. HIRF/EMI) aspects. 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 may 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 paragraphs Light-UAS.2500 and Light-UAS.2510 (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)

5. Safety Objectives

The objective of Light-UAS.2510 is to ensure an acceptable safety level for equipment and systems as installed in the UAS. Light-UAS.2510 requires that the equipment and systems identified in Light-UAS.2500, considered separately and in relation to other systems, must be designed and installed such that hazards are minimized in the event of a probable failure, it can be reasonably expected that a fatality will not result from any single failure; and if the SAIL is IV, a means for detection, alerting and management of any failure or combination thereof, which would lead to a hazard, is available.

The following Safety Objectives apply for medium risk UAS (SAIL IV):

1. Failure conditions leading to the loss of control of the operation are not probable.
2. Failure conditions leading to the loss of control of the operation will not result from a single failure. (see §7 for applicability)
3. Functions, systems, equipment and items whose development error(s) could directly result in the loss of control of operation should be developed to DAL C.

6. Compliance with Light-UAS.2510(a)(1)

The compliance demonstration for Light-UAS.2510 can be limited to failure conditions which will lead to a loss of control of the operation. Loss of control of operation should be understood as in the SORA semantic model. Situations where the control of the operation is considered to be lost, are e.g.:

- Crash of the UA with the ground/infrastructure/people:
- Unrecoverable loss of controllability
- Controlled flight into terrain
- activation of flight termination system/parachute/other M2 mitigation due to emergency situation
- Erroneous activation of flight termination system/parachute/other M2 mitigation
- UA leaving the operational volume[1]
- Loss of payload (Detachment of part heavy enough to create a risk for people on ground)

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 in showing compliance to Light-UAS.2510.

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.

Guidance on how to perform the safety assessment process to comply with the safety objectives identified in section 5, can be found in ED-280. The applicant may propose other guidance for the safety assessment process. When using ED-280, an FHA should be conducted, which identifies all failure conditions at UAS level. The failure conditions leading to the loss of control of the operation should be selected for further assessment. Failure conditions not resulting in the loss of control of the operation do not need to be further assessed. The severity classification of the failure condition (major, hazardous, catastrophic) is optional, but not required[2]. Hazardous

[1] Additional containment requirements might apply, see Light-UAS.2511.
[2] Definitions for major, hazardous and catastrophic severities should be taken from JARUS AMC RPAS.1309 Issue 2

and catastrophic failure conditions should be understood as those failure conditions leading to the loss of control of operation. See also section 7. A quantitative assessment is not required. If the qualitative assessment is not conclusive then a quantitative assessment should be considered

When assessing the effect of a failure condition, no credit can be taken in the FHA classification from M2 mitigation or containment provisions. These features 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 MOC Light-UAS.2512 and MOC Light-UAS.2511. However, when installing such emergency systems, the malfunction (e.g. erroneous activation) of the system should be addressed within the safety assessment required by MOC Light-UAS.2510. The inadvertent activation of a flight termination system, parachute or other M2 means, will usually lead to the loss of control of operation. It should be noted that this is likely to drive the safety objectives (DAL assignment) for these systems.

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 SORA approval holder, the owner of the data, or, if accepted by the Agency, has an agreement in place with the owner of the data that permits its use by the applicant for this purpose.

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.[3]

[3] 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.

6.1 Development Assurance

Any analysis necessary to show compliance with Light-UAS.2510(a) should consider the possibility of development errors. For simple systems, which are not highly integrated with other UA systems, errors made during development of systems may still be detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterising the behaviour of the system. Such items may be considered as meeting the specified Development Assurance rigor when they are fully assured by a combination of testing and analysis. However, requirements for these items should be validated with the rigor corresponding to the DAL of the function. Systems which contain software and/or complex electronic hardware items, are not considered simple.[4]

For more complex or highly integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests which should be accomplished. For these types of systems, compliance may be shown by the use of development assurance.

The development assurance level should only be allocated to functions, systems and equipment in which an error could directly result in the loss of control of operation. Architectural considerations could be used to alleviate the need for development assurance, provided that sufficient independence is applied. Common mode errors should then be assessed and minimized in the frame of the common cause analysis.

The term directly means, that the functional failure sets leading to the top-level failure conditions, contains only one member. If the UAS or system architecture provides containment for the effect of development error, it is not considered “directly”

It should be noted that accepted means of compliance for development assurance for systems, software and airborne electronic hardware are under development and will be published for consultation by EASA, when available. In the meantime, ARP4754A, AMC 20-115D and AMC 20-152A can be used as acceptable means of compliance.

7. Compliance with Light-UAS.2510(a)(2)

According to Light-UAS.2510(a)(2) and as defined in section 5, the loss of control of the operation shall not result from the failure of any single component, part, or element of a system.

If the UAS operation is conducted in an operational volume which contains populated areas or assemblies of people, Light-UAS.2510(a)(2) applies.

It should then be conservatively assumed that any loss of control of operation could result in one or more fatalities (i.e. is a catastrophic failure condition). **Therefore, a failure condition leading to the loss of control of operation should not result from any single failure**. Certain single failures may be accepted, if it can be shown that they are not expected to lead to a fatality. 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). If technical means are used to mitigate the effect of the loss of control event by reducing the critical area or the likelihood of a fatality to an extent where it can be reasonably expected that a fatality will not occur, these

[4] Definition for complex electronic hardware can be found in AMC 20-152A §5.2

means cannot be utilized as an M2 mitigation to lower the ground risk class in the framework of the SORA. Early concurrence with the agency is advised.

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 Light-UAS.2510(a)(2). 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.).

8. Compliance with Light-UAS.2510(a)(3)

The means referred in Light-UAS.2510(a)(3) are those technical elements installed on a UAS for the detection and crew alerting of safety-relevant failures. They may constitute part of the strategy for the management of these failures.

Any failure or combination thereof that, if not detected and properly accommodated by remote flight crew action, would contribute to loss of control of the operation should be identified and considered under Light-UAS.2510(a)(3).

The means should be addressed as an UAS function. If a failure (including erroneous behaviour) of the detection, alerting and failure management means leads to a loss of control of operation, it may drive the safety objectives for this system. If the remote pilot has alternate cues to detect the erroneous behavior, credit could be given in the safety assessment, considering the feasibility of the detection by the remote pilot is substantiated (e.g. quantity and quality of the information available to the pilot, reaction time, training).

The loss of detection and alerting should be considered as a failure condition and pre-flight checks or built-in test should be utilised to limit the latency of the monitoring system failure.

The expected remote flight crew action and pre-flight checks should be described in the flight manual in compliance with Light-UAS.2620.

9. Compliance with Light-UAS.2510(b)

(b) Any hazard which may be caused by the operation of equipment and systems not covered by LightUAS.2500 must be minimized.

The equipment and systems which are not covered by Light-UAS.2500 are typically those, whose failure or improper functioning should not affect the safety of the UA operation. A Design and Installation Appraisal should be conducted to demonstrate that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by Light-UAS.2500 and does not otherwise adversely influence the safety of the UA operation. In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation.