EASA European Union Aviation Safety Agency	**Means of Compliance with Light-UAS.2510 Equipment, Systems and Installation**	Doc. No. : MOC Light-UAS.2510-01 Issue : 1 Date : 01 Feb 2024 Proposed ☐ Final ☒

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

1. Purpose

This MOC provides an accepted means for showing compliance with the requirements of Special Condition Light-UAS.2510(a) and (b). 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. As specified in Light-UAS.2500(a), it is intended as a general requirement, that should be applied to any equipment or system, in addition to system-specific requirements, considering the following:

(a) General – Light-UAS.2510 specifies the technical safety objectives derived from 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 SORA or Light-UAS requirement will take precedence. This precedence does not preclude accomplishment of a system safety assessment.

(a) 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 any system used to enable compliance with Light-UAS.2135.

(b) 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.

(c) Subpart H – C2 Link systems are required to comply with Light-UAS.2510, see also Light-UAS.2715.

(d) Subpart G - Remote Crew Interface are required to comply with Light-UAS.2510, see also Light-UAS.2600.

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

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

This MOC considers the operation of one aircraft for each control and monitoring unit (CMU). Additional provisions may apply for systems that allow the operation of multiple UA with a single CMU.

3. Referenced 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) EUROCAE ED-79B, Guidelines for development of civil aircraft and systems.
(d) EUROCAE ED-135 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
(e) EASA AMC 20-115D – Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178
(f) EASA AMC 20-152A – Development Assurance for Airborne Electronic Hardware (AEH) AMC & GM to Part-UAS Regulations (EU) 2019/947

4. List of acronyms

AMC	Acceptable Means of Compliance
ASTM	ASTM International
C2	Command and Control
CMU	Control and Monitoring Unit
DAL	Development Assurance Level
EASA	European Union Aviation Safety Agency
EMI	Electro-Magnetic Interference
EU	European Union
FAA	Federal Aviation Administration
FH	Flight Hour(s)
FHA	Functional Hazard Assessment
FTS	Flight Termination System
GNSS	Global Navigation Satellite System
HIRF	High Intensity Radiated Field
LOC	Loss of Control of operation
MOC	Means of Compliance
RPAS	Remotely Piloted Aircraft System
RTCA	RTCA, Inc
SAIL	Specific Assurance and Integrity Level
SORA	Specific Operations Risk Assessment
TLOS	Target Level of Safety
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System

5. Definitions

(a) Catastrophic failure condition: Failure conditions that are expected to result in one or more fatalities. (Source: SC-RPAS.1309-03)

(b) 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. (Source: ED-79B).

(c) 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). The DALs are determined by the system safety assessment process.

(d) Development Error: a mistake in requirements, design, or implementation (Source: ED-79B)

(e) 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. (Source: Regulation 2019/947)

(f) Failure Condition: A condition having an effect on the UAS (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.1309-03)

(g) Hazard: A failure condition that relates to major, hazardous, or catastrophic consequences. (Source: Annex E to AMC1 to Article 11 of Regulation 2019/947)

(h) Hazardous failure condition: Failure conditions that would reduce the capability of the UAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following:

i) Loss of the UA where it can be reasonably expected that one or more fatalities will not occur, or

ii) A large reduction in safety margins or functional capabilities or separation assurance, or

iii) High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely. (Source: adapted from SC-RPAS.1309-03)

(i) Major failure condition: Failure conditions that would reduce the capability of the UAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency. (Source: adapted from SC-RPAS.1309-03)

(j) Minor failure conditions: Failure conditions that would not significantly reduce UAS safety and that involve remote crew actions that are well within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes. (Source: adapted from SC-RPAS.1309-03)

(k) 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)

(l) Resource System: A system that provides common energy or information to multiple systems. Providing power or data may be the primary function of the resource or a secondary function (Source: ED-135)

6. 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. In addition it can be reasonably expected that a fatality will not result from any single failure; and 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 (LOC) are not probable[1].
2) Catastrophic failure conditions do not result from any single failure.
3) Functions, systems, equipment and items whose development error(s) could directly result in the loss of control of operation should be developed with an appropriate level of rigor.

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

- Crash of the UA with the ground/infrastructure/people
- Unrecoverable loss of controllability
- Controlled flight into terrain (e.g. an event in which an airworthy UA that is fully controllable, either directly by the remote pilot or by an automatic system, is unintentionally flown into the ground or into an obstacle)
- 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)

The above list of LOC events is exemplary and non-exhaustive. Most of the stated events will ultimately lead to a crash of the UA. However, not only the direct consequence of a technical failure should be assessed. Although SC Light- UAS.2511 addresses the case “UA leaving the operational volume”, this MoC supports also the compliance demonstration for the containment requirements. While an M2 mitigation is reducing the probability to cause a fatality, it does not improve the inherent reliability of the UAS. A

[1] Probable is to be understood in its qualitative meaning, see definitions.

technical failure leading to the unintended activation of the M2 means should be considered as LOC. It should not discourage the applicant from implementing M2 mitigation, since credit can be taken for it, by reducing the SAIL.

The scope of the safety assessment is limited to technical failures. Other causes which could lead to a LOC, e.g. pilot error or errors in operational procedures, should not be considered in the compliance demonstration to Light-UAS.2510.

The assessment should include failures of the CMU, unmanned aircraft and any system installed on the aircraft, such as a 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.).

The assessment should demonstrate that the loss of control of the UA due to technical failures is reduced to an acceptable level. In quantitative terms, the SORA model establishes the allowable loss of control probability for a SAIL IV operation in the order of 10^{-4}/FH, including LOC events due to operational causes (e.g. erroneous operational planning, crew errors, etc.). Consequently, the allowable LOC probability due to technical reasons is assumed to be in the order of 10^{-5}/FH (depending on the level of automation of the operation). A quantitative assessment is not required. However, if the qualitative assessment is not conclusive then a quantitative assessment should be considered, demonstrating that the cumulative probability of all failure conditions leading to LOC is below 10^{-5}/FH.

Acceptable guidance on the safety assessment process to comply with the safety objectives identified in section 6, are provided in ED-280. The applicant may propose other guidance for the safety assessment process (e.g. ED-135). An FHA should be conducted, which identifies all failure conditions at UAS level. The failure conditions leading to a LOC should be selected for further assessment. Other failure conditions do not need to be further assessed in the scope of this MOC. Hazardous and Catastrophic failure conditions should be understood as those leading to a LOC.
As explained, the probability of LOC in SAIL IV is expected to be less than 10^{-4} /FH. This implies that such operations should not lead to fatalities more frequently than every 100 loss of control events, in order to meet the overall target level of safety (TLOS). Consequently, failure conditions leading to a loss of control of operation, like an impact with the ground or an obstacle, are generally not expected to be Catastrophic, and should be classified as Hazardous. However, there are exceptions:

- If technical means are used to lower the ground risk class (e.g. M2), a failure condition in which a failure is affecting both the UA and the mitigation means should be classified as Catastrophic. For example, a failure that would lead to the UA impacting the ground and making the mitigation means ineffective should be classified Catastrophic. Rationale: the mitigation means is not effective, the ground risk class is not reduced, and the assumption behind the former Hazardous classification would be invalid.
- Intrinsically unsafe design features that would lead to a fatality. For example a system failure that would lead to the electrocution, beheading or other fatal injuries of the UAS crew (including ground support crew, if any).

M2 mitigations may be used in the FHA to mitigate Catastrophic failure conditions. M2 mitigations and containment means like a Flight Termination System (FTS) are considered emergency systems, as they are intended to reduce the risk, after the control of the UAS has already been lost. Specific information is provided 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 established by MOC Light-UAS.2510. The erroneous activation of a flight termination system, parachute or other M2 means, may lead to the loss of control of the aircraft. This fact may 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 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. The applicant should be able to substantiate that a close similarity in respect of both the system design and operating conditions exists.

Compliance for qualification of systems or equipment may be demonstrated through evidence of certification or qualification of systems or components to acceptable specifications, e.g. certified engines, ETSO equipment, etc.

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]

[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.

7.1 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.[3]

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.

Development assurance should be applied at system and equipment level. For SW/AEH items whose development error could directly result in the loss of control of operation, development assurance is applicable as well. 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".

ED-79B, AMC 20-115D and AMC 20-152A objectives for DAL C, can be used as an acceptable means of compliance to demonstrate that development errors have been addressed and minimized with a level of rigor appropriate to the safety objective, even if less stringent objectives may be acceptable. More proportionate means of compliance for UAS development assurance are under development by some standardisation organisation and might become available in the future. Alternatively, the applicant may propose different development assurance methodologies at project level.

Architectural considerations could be used to alleviate the need for development assurance at item-level, provided that sufficient independence is applied. Common mode errors should then be assessed and minimized in the frame of the common cause analysis. If an item/equipment/system is able to prevent a loss of control due to an error in SW/AEH development in another item/equipment/system, no item-level Development Assurance activities would be required.

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

According to Light-UAS.2510(a)(2), a Catastrophic failure condition shall not result from the failure of any single component, part, or element of a system. A single failure includes any set of failures, which cannot be shown to be independent from each other.

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

Failure containment should be provided by system design to limit the propagation of the effects of any single failure that is expected to lead to a fatality. Means to mitigate the effect of an otherwise critical single failure, could be of technical or operational nature.

Single failures leading to Hazardous failure conditions can be accepted. Such single failures are expected to have a probability in the order of magnitude of 10^{-6}/FH.

Common cause failures should be considered. There should be no common-cause failure, which could affect both single components, parts, or elements, and their failure containment provision(s). 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. Further guidance can be found in ED-135.

When applying ED-280, possible common cause failures (including common mode 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.).

9. 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 a UAS function. If a failure (including erroneous behaviour) of the failure detection, alerting or management means leads to a LOC, 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 detectability by the remote pilot is substantiated (e.g. quantity and quality of

the information available to the pilot, reaction time, training). ED-280 or ED-135 can be used as a means of compliance to assess the detection/alerting systems.

The loss of detection and alerting should be considered as a failure condition and pre-flight checks, built-in tests or other regular testing 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.

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

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.