EASA European Union Aviation Safety Agency	**Means of Compliance with Light-UAS.2510 Equipment, Systems and Installation**	Doc. No. : MOC Light-UAS High Risk.2510-01 Issue : 01 Date : 11 February 2025 Proposed ☐ Final ☒

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

Contents

1. Purpose

This MOC provides an accepted means for showing compliance with the requirements of Special Condition Light-UAS High Risk.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 for SAIL V and VI operations. As specified in SC 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 of AMC and GM to Commission Implementing Regulation (EU) 2019/947. This MOC is applicable to Unmanned Aircraft Systems (UAS) intended for operation in SAIL V and VI, applying SC Light-UAS High 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.

(b) Subpart B, C and D - While Light-UAS High risk.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.

(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.

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

(f) The safety assessment process should consider all phases during flight and on ground when the UA is in service. While this includes the conditions associated with the pre-flight preparation, taxi phase, etc., it, therefore, does not include periods of shop maintenance, storage, or other out-of-service activities.

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 UA 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 / Machine Learning (AI/ML) techniques are not covered by this MOC and may require particular compliance demonstration. If the use of AI/ML is envisaged by the applicant, early coordination with EASA is advised.

This MOC considers the operation of one UA per 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. As some have been established in the context of manned aviation, tailoring may be needed to adapt to the UAS context:

(a) AMC & GM to Part-UAS Regulations (EU) 2019/947
(b) ASTM F3309-21, Standard Practice for Simplified Safety Assessment of Systems and Equipment in Small Aircraft
(c) EASA AMC 20-115( ) – Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178
(d) EASA AMC 20-152( ) – Development Assurance for Airborne Electronic Hardware (AEH)
(e) EASA AMC 20-170( ) – Integrated modular avionics (IMA)
(f) EASA AMC 20-189( ) – The Management of Open Problem Reports (OPRs)
(g) EUROCAE ED-79B/SAE ARP4754B, Guidelines for Development of Civil Aircraft and Systems.
(h) EUROCAE ED-109A/RTCA DO-278A, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems
(i) EUROCAE ED-135/SAE ARP4761A - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
(j) EUROCAE ED-279 – Generic Functional Hazard Assessment (FHA) for UAS/RPAS

4. List of acronyms

AEH	Airborne Electronic Hardware
AL	Assurance Level
AMC	Acceptable Means of Compliance
ASTM	ASTM International (formerly American Society for Testing and Materials)
ATM	Air Traffic Management
C2	Command and Control
CONOPS	Concept of operations
CMU	Control and Monitoring Unit
CNS	Communication, Navigation Surveillance
COTS	Commercial Off The Shelf
DAL	Development Assurance Level
EASA	European Union Aviation Safety Agency
EMI	Electro-Magnetic Interference
ETSO	European Technical Standard Order
EU	European Union
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FDAL	Function Development Assurance Level
FH	Flight Hour(s)
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
FTS	Flight Termination System
GNSS	Global Navigation Satellite System
HIRF	High Intensity Radiated Field
IDAL	Item Development Assurance Level
LOC	Loss of Control of operation
MOC	Means of Compliance
MTBF	Mean Time Between Failure
OSO	Operational Safety Objectives
RTCA	RTCA, Inc. (formerly Radio Technical Commission for Aeronautics)
SAE	SAE International (formerly Society of Automotive Engineers)
SAIL	Specific Assurance and Integrity Level
SORA	Specific Operations Risk Assessment
SSA	System Safety Assessment
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System

5. Definitions

(a) Common Cause: A single failure, error or event that can produce undesirable effects on two or more systems, equipment, items or functions (Source: ED-135/ARP4761A)

(b) Complex System: A system is complex, when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods. (Source: AMC 25.1309)

(c) Complexity: An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods. (Source: AMC 25.1309)

(d) Commercial off-the-shelf (COTS) device: a device, integrated circuit or multi-chip module developed by a supplier for a wide range of customers (not restricted to airborne systems), whose design and configuration is controlled by the supplier or an industry specification. A COTS device can encompass digital, analogue, or mixed-signal technology. COTS electronic components are generally developed by the semiconductor industry for the commercial market, not particular to the airborne domain. These devices have widespread commercial use and are developed according to the semiconductor manufacturer's proprietary development processes. (Source: AMC 20-152A)

(e) 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/ARP4754B).

(f) Development Error: a mistake in requirements, design, or implementation (Source: ED-79B/ARP4754B)

(g) Error: an omitted or incorrect action by a manufacturer, crew member, or maintenance person, or a mistake in requirements, design, or implementation (Source: ED-135/ARP4761A)

(h) External System: A system that is not already part of the UAS but is used to: launch/take off the UA; make pre-flight checks; or keep the UA within its operational volume (e.g. GNSS, satellite systems, air traffic management, U-space, Internet) (Source: derived from AMC to Regulation 2019/947)

(i) 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)

(j) 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)

(k) Function Development Assurance Level (FDAL): The level of rigor of the development assurance tasks performed to functions. Note The FDAL is used to identify the ED-79B/ARP4754B objectives that need to be satisfied for the aircraft/system functions. (Source: ED-79B/ARP4754B)

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

(m) Item Development Assurance Level (IDAL): The level of rigor of development assurance tasks to be performed on item(s); e.g., IDAL is the appropriate software level in ED-12/C/DO-178C, and design

assurance level in ED-80/DO-254 objectives that need to be satisfied for an item (Source: ED-79B/ARP4754B)

(n) Latent Failure: A failure which is not detected and/or annunciated when it occurs (Source: ED-135/ARP4761A)

(o) Loss of control of operation: Loss of control of the operation is a state that corresponds to situations:
   a. Where the outcome of the situation highly relies on providence, or
   b. Which could not be handled by a contingency procedure.

   […] This includes situations where a UA has exited the operational volume and is potentially operating over or in an area of higher ground or air risk for which it is not approved. The "loss of control" state is also entered, if a UA does not follow the predefined route and the remote pilot is unable to control it, it crashes or if an unplanned flight termination sequence is executed, even if this happens inside the operational volume. (Source: JAR-DEL-SRM-SORA-MB-2.5)

(p) Malfunction: Failure of a system, subsystem, unit, or part to operate in the normal or usual manner. The occurrence of a condition whereby the operation is outside specified limits. (Source: AC 23.1309-1E)

(q) Open-source software: describes software that comes with permission to use, copy and distribute, either as is or with modifications, and that may be offered either free or with a charge. The source code should be available. (Source: Gartner.com)

(r) Operational Volume: the volume in which the operation is intended to take place safely. It is made up of the flight geography and the contingency volume. (Source : JAR-DEL-SRM-SORA-MB-2.5)

(s) 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)

(t) Problem report: a means to identify and record the resolution of anomalous behaviour, process non-compliance with development assurance plans and standards, and deficiencies in life-cycle data (Source: AMC 20-189)

(u) 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/ARP4761A)

(v) Significant latent failure: A significant latent failure is one, which would in combination with one or more specific failures, or events result in a Hazardous or Catastrophic Failure Condition. (Source: adapted from AMC 25.1309 in Book 2 of CS-25 Amdt. 27).

(w) Simple system: A simple system is a system that can be evaluated by only qualitative analysis and that is not a complex system; functional performance is determined by combination of tests and analyses. (Source: ASTM F3230-20a)

6. Principles of Fail-Safe design concept

The requirements of SC Light-UAS incorporate the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

The following basic objectives pertaining to failures apply:

(1) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.

(2) Subsequent failures of related systems during the same flight, whether detected or latent, and combinations thereof, should also be considered.

The fail-safe design concept uses the following design principles or techniques to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design, i.e. to ensure that major failure conditions are remote, hazardous failure conditions are extremely remote, and catastrophic failure conditions are extremely improbable:

(1) Designed integrity and quality, including life limits, to ensure intended function and prevent failures.

(2) Redundancy or backup systems to enable continued function after any single (or other defined number of) failure(s); e.g. two or more engines, hydraulic systems, flight control systems, etc.

(3) Isolation and/or segregation of systems, components, and elements so that the failure of one does not cause the failure of another.

(4) Proven reliability so that multiple, independent failures are unlikely to occur during the same flight.

(5) Failure warning or Indication to provide detection.

(6) Remote crew procedures specifying corrective action for use after failure detection or automated corrective action after onboard failure detection.

(7) Checkability: the capability to check a component's condition.

(8) Designed failure effect limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(9) Designed failure path to control and direct the effects of a failure in a way that limits its safety impact.

(10) Margins or factors of safety to allow for any undefined or unforeseeable adverse conditions.

(11) Error-tolerance that considers adverse effects of foreseeable errors during the UAS design, test, manufacture, operation, and maintenance.

7. Failure Condition classification

Failure Conditions are classified according to the severity of their effects as follows:

(1) **No safety effect**: Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the UAS or increase the remote crew workload.

(2) **Minor**: 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.

(3) **Major**: 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.

(4) **Hazardous**: 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 UAS 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) Excessive workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.

(5) **Catastrophic**: Failure conditions that are expected to result in one or more fatalities.

When establishing the UAS and Systems Functional Hazard Assessment, the applicant will have to substantiate the effects of failure conditions with consideration to operational conditions and events. Additional guidance is provided in section 9.1

8. Safety Objectives

The objective of Light-UAS.2510 is to ensure an acceptable safety level for equipment and systems as installed as part of the UAS. A logical and acceptable inverse relationship must exist between the average probability per flight hour and the severity of failure condition effects.

8.1 Safety Objectives per SAIL and failure condition classification

The safety objectives for each failure condition are:

	Failure Condition Classification		
	Major	Hazardous	Catastrophic (Note 2)
	Allowable Qualitative Probability		
	Remote	Extremely Remote	Extremely Improbable
	Allowable Quantitative Probability (Note 3) and Functional Development Assurance Level (FDAL) (Note 4)		
SAIL VI	$\leq 10^{-4}$ FDAL D	$\leq 10^{-6}$ FDAL C	$\leq 10^{-8}$ FDAL B
SAIL V	$\leq 10^{-4}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B

Table 1: Safety Objectives

Note 1: The applicant is not expected to perform a formal analysis for minor failure conditions. Their probability should be reduced using industry best practices.
Note 2: No single failure shall result in a catastrophic failure condition.
Note 3: The quantitative safety objectives are expressed per flight hour. An average flight profile (including the duration of flight phases) and an average flight duration should be defined. It is recognised that, for various reasons, component failure rate data may not be precise enough to enable accurate estimates of the probabilities of failure conditions. This results in some degree of uncertainty. When calculating the estimated probability of each failure condition, this uncertainty should be accounted for in a way that does not compromise safety.
Note 4: Using architectural considerations for assigning an FDAL/IDAL as described in ED-135/ARP4761A Appendix P[1] is possible, in accordance with the following additional principles:

(1) Catastrophic failure conditions: Two members contributing to catastrophic failure conditions should be assigned at least FDAL/IDAL C. Other additional members should not be lower than FDAL/IDAL D.

[1] ED-135 Appendix P, notably table P-2 needs to be adapted to account for the different Top-Level Function FDAL assignment of UAS performing SAIL V and VI operations, as defined in Table 1.

(2) Hazardous and major failure conditions: For functional failure sets with multiple members, no FDAL/IDAL lower than level D should be assigned to any member.

8.2 Single failure and common cause considerations

According to Light-UAS.2510(a)(1), a catastrophic failure condition should not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure conditions. In addition, there must be no common-cause failure, which could affect both the single component, part, or element, and its 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. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (including common mode failures) and cascading failures. They should, therefore, be assessed and mitigated as far as practicable in the frame of the common–cause and cascading failures consideration.

Sources of common cause and cascading failures, which should be assessed within the compliance demonstration of this MOC include development, shared resource and events outside the system(s) concerned. ED-135/ARP4761A describes types of common cause analyses, which may be conducted, to ensure that independence is maintained (e.g. particular risk analyses, zonal safety analysis, common mode analyses).

While single failures should normally be assumed to occur, experienced engineering judgment and relevant service history may show that a catastrophic failure condition by a single failure mode is not a practical possibility. The logic and rationale used in the assessment should be so straightforward and obvious that the failure mode simply would not occur unless it is associated with an unrelated failure condition that would, in itself, be catastrophic.

Analyses should always consider the application of the fail-safe design concept and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions.

9. Safety Assessment Process

Guidance on how to perform the safety assessment process can be found in ED-79B/ARP4754B and ED-135/ARP4761A. As these standards have been established in the context of manned aviation, tailoring will be needed to adapt to the UAS context. The applicant may propose other guidance for the safety assessment process, which should be agreed with EASA in conjunction with the overall proposed

Development Assurance process. The depth and scope of the analyses are dependent on the system criticality and/or complexity.

Any assumptions made during the safety assessment process need to be justified and validated.

9.1 Identification and classification of failure conditions

The UAS level and system level functions need to be examined, identifying potential failure conditions and classifying associated hazards in accordance with section 0. The assessment should encompass all elements of the UAS, i.e. CMU, unmanned aircraft, C2 link and any external system supporting the operation. Environmental and operational aggravating factors need to be considered when relevant (e.g. temperature, icing, nighttime, turbulence, etc.). In addition to ED-135/ARP4761A, ED-279 provides supplementary guidance for UAS specific aspects of conducting an FHA at UAS level.

For the definition of the UAS and system level functions, the CONOPS, UAS operational modes, the level of automation, contingency procedures or emergency procedures as well as the description of the external systems supporting the operation should be considered, in order to ensure a complete and correct identification of UAS and system level functions.

In SAIL V and VI operations there is an increasing contribution of the UAS design (and external system supporting the operation) to the loss of control of operation inside the operational volume. Therefore, failure conditions leading to the loss of the UA inside the operational volume, should be expected to result in one or more fatalities, unless mitigations apply. If operational limitations limit the risk for people on ground during certain phases of flight, a loss of control of operation could be accepted to be classified as hazardous. Possible examples are:

(1) Failure conditions leading to a crash during take-off and landing, when it can be ensured that the take-off and landing area is a controlled ground area, without uninvolved persons.

(2) Failure conditions resulting in a ground crash within the operational volume, when the air risk is the main contributor of the SAIL determination and the ground risk is sufficiently low, i.e. a loss of control of operation is not expected to lead to fatalities on the ground.

9.1.1 Relationship with Light-UAS.2511

If Light-UAS.2511(b) applies, the methods described in this MOC can be used to demonstrate compliance with the containment requirements. Light-UAS.2511 provides specific safety requirements. These requirements should take precedence over the objectives stipulated in this MOC.

The functional hazard assessment should identify those failure conditions that could result in the UA leaving the operational volume and failure conditions resulting in the operation outside of the ground risk buffer. Qualitative assessments of the systems, equipment and items contributing to the containment functions are acceptable to demonstrate that no probable single failure of the UAS or any external system supporting the operation will lead to operation outside of the operation volume.

The safety assessment conducted within this MOC should also address the malfunction of the systems, equipment or items providing the containment function. For example, the inadvertent activation of a flight termination system within the operational volume should be considered catastrophic.

Complying with this MOC for containment functions is also demonstrating compliance with Light-UAS.2511(b).

9.1.2 Relationship with Light-UAS.2512

Technical means may be implemented to reduce the ground risk (e.g. M2 mitigation). These means are considered part of the emergency procedures and Light-UAS.2512 would apply. An emergency procedure may be used as a means of mitigating catastrophic failure conditions. Where an emergency procedure is used as mitigation for what would otherwise be a catastrophic failure condition, the systems and equipment that supports this functionality would be required to undergo safety assessment to ensure a level of performance and independence acceptable to EASA. The use of flight termination systems, parachutes, autorotation or emergency crash sites are examples of options available to applicants to mitigate against high severity failure conditions. The applicant will need to provide evidence to EASA that their use will not result in unacceptable risks.

The safety assessment should assess failures (i.e. loss and malfunction) of the mitigation by itself and in relation with other system failures. Special care should be taken, when a loss or malfunction would lead to a loss of control of operation and the loss of the mitigation effectiveness, as this would invalidate the assumptions taken when defining the SAIL of the operation. This failure condition should be considered catastrophic and the safety objectives of this MOC should apply.

9.2 Depth of analysis

The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system failure conditions.

The following activities are expected:

1) Minor failure conditions
   a) The applicant is not expected to perform a formal analysis for minor failure conditions, see Note 1 in section 8.1.
2) Major failure conditions
   a) If the system is similar in its relevant attributes to those used in other UAS and the effects of failure would be the same, then design and installation appraisals and satisfactory service history of the equipment being analysed, or of similar design, will usually be acceptable for showing compliance. Service history data are limited to the fleet of UAS for which the applicant is the owner of the data, or, if accepted by EASA, 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.

b) For simple systems and where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment that shows that the system-level major failure conditions, of the system as installed, are consistent with the FHA and are remote, e.g. redundant systems.

c) For complex systems, to show that malfunctions are indeed remote in systems without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative failure modes and effects analysis (FMEA) supported by failure rate data and fault detection coverage analysis.

d) An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative FMEA and qualitative fault tree analysis may be necessary to determine that redundancy actually exists (e.g. no single failure affects all functional channels).

3) Hazardous and catastrophic failure conditions

a) The analysis should be a combination of qualitative and quantitative assessment of the design.

Compliance of systems, equipment or items may be demonstrated through evidence of certification or qualification to acceptable specifications, e.g. certified engines, ETSO equipment, etc. If standards or specifications are re-used from manned aviation domain, it needs to be ensured that they remain applicable to the specific UAS operational context.

9.3 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. Systems may be considered as meeting the specified Development Assurance rigor when they contain non-complex items, which can be fully assured by a combination of testing and analysis. However, requirements for these systems/items should be validated with the rigor corresponding to the DAL of the function. Systems which contain software and/or complex electronic hardware items[2], are not considered simple.

For 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.

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

The level of development assurance should be commensurate with the severity of the failure conditions the system is contributing to.

9.3.1 Development Assurance Level (DAL) assignment

The development assurance level of a function or of an item is assigned depending on the classification of the failure conditions it contributes to.

Initial FDAL assignment is performed in accordance with Table 1 in this MOC and the IDAL of all items contributing to a given function should be equal to the FDAL of that function.

Guidelines, which may be alternatively used for the assignment of development assurance levels to UAS and system functions (FDAL) and to items (IDAL), are described in the document ED-135/ARP4761A, Appendix P. In addition the Note 4 in section 8.1 should be considered when assigning FDAL/IDAL.

9.3.2 UAS/System development assurance

For the UAS and for its systems, this MOC recognises the ED-79B/ARP4754B as acceptable guideline for establishing a development assurance process from UAS level down to the level where software/ Airborne Electronic Hardware (AEH) development assurance is applied. The extent of application of ED-79B/ARP4754B to substantiate system and equipment development assurance activities may vary depending on the complexity of the systems and on their level of interaction with other systems. Early concurrence with EASA is essential.

9.3.3 Software development assurance

This MOC recognises AMC 20-115( ) as an accepted means of compliance with requirement Light-UAS.2510(a). For Commercial-Off-The-Shelf (COTS) software items used in the CMU, in addition to the provisions of AMC 20-115( ), this MOC recognises guidance from ED-109A/DO-278A section 12.4 as an alternative that could be generally applied beyond the limits of CNS/ATM systems. In this case, the association between ED-12C/DO-178C software level and ED-109A/DO-278A AL (Assurance Level) can be found in ED-109A/DO-278A table 2-2 of section 2.3.3 ‘Assurance Level Definitions’.

9.3.4 Airborne Electronic Hardware development assurance

This MOC recognises AMC 20-152( ) as accepted means of compliance for requirement Light-UAS.2510(a).

9.3.5 Open Problem Report management

Any problem(s) identified during the development are addressed, and any remaining problem(s) at the time of approval are assessed for their impact on safety and demonstrated to be acceptable. AMC 20-189( ) is an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the management of open problem reports.

9.3.6 Considerations for highly integrated systems

When UAS functions are provided by a combination of systems, the relevant requirements of those systems should be validated together, including the following activities:

(1) Analysis of the potential interactions and interferences between systems,
(2) Planning of dedicated activities at system and UAS levels to ensure validation of those requirements that are affected by interactions or interference.

When incorporating multiple functions into the same system or equipment, applicability of AMC 20-170( ) should be considered. For architectures with no partitioning, particular care should be taken in the analysis of interactions between functions.

10. Latent Failure and Crew considerations

10.1 Latent failure considerations

The use of periodic maintenance or remote crew checks to detect significant latent failures after they occurred is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. Significant latent failures are latent failures that would, in combination with one or more specific failure(s) or event(s), result in a catastrophic failure condition and should be avoided in system design.

Within the frame of the no single failure criterion, dual failure combinations, with either one latent, that can lead to a catastrophic failure condition should be avoided in system design. Any such combinations should be highlighted in the relevant System Safety Assessment (SSA) and discussed with EASA as early as possible after identification.

10.2 Remote Crew and Maintenance considerations

10.2.1 Remote Crew Actions

When assessing the ability of the remote crew to cope with a failure condition, the information that is provided to the remote crew and the complexity of the required action should be considered. If the evaluation indicates that a potential failure condition can be alleviated or overcome during the time available without jeopardizing other safety related remote crew tasks and without requiring exceptional remote pilot skill, credit may be taken for correct and appropriate corrective action for both qualitative and quantitative assessments. The evaluation should substantiate the detectability by the remote pilot by assessing e.g. quantity and quality of the information available to the pilot, reaction time, training. Similarly, credit may be taken for correct remote crew performance if overall remote crew workload during the time available is not excessive and if the tasks do not require exceptional remote pilot skill. The information on the UA systems status necessary to take appropriate action in case of failure need to be identified and will

depend on the level of automation. The appropriate procedures should be included in the flight manual and should be consistent with the assumptions made regarding remote crew actions in the safety assessment process. See also Light-UAS.2602, Light-UAS.2605 and Light-UAS.2620

10.2.2 Maintenance Actions

Credit may be taken for the correct accomplishment of maintenance tasks in both qualitative and quantitative assessments if the tasks are evaluated and found to be reasonable. Required maintenance tasks, which mitigate hazards, should be provided for use in the maintenance instructions. Annunciated failures should be corrected before the next flight or a maximum duration should be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. A scheduled maintenance task may detect latent failures. If this approach is taken, and the failure condition is catastrophic, then a maintenance task should be established. Credit could be given to tests performed due to mean time between failures (MTBF) to detect the presence of latent failures, if it can be ascertained that the equipment is removed and inspected at a rate much more frequent than the safety analysis requires. This credit should be substantiated in the relevant SSA. The means of detection of the latent failures should be clearly identified, either at the opportunity of the acceptance tests performed before the equipment enters service or leaves the manufacturer, or at the opportunity of test of system integrity when it is installed back on the UAS. This substantiation should be recorded in the relevant SSA. In case of double failures, with either one or both latent, that can lead to catastrophic failure condition, no credit should be taken from MTBF for failure detection, and the maintenance task enabling detection of the latent failure should be identified as a required maintenance task.

11. 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.