| | | |
|---|---|---|
| **SUBJECT** | : | **Equipment, systems, and installations** |
| **CERTIFICATION SPECIFICATION** | : | CS-VLA / CS-VLR |
| **PRIMARY PANEL** | : | Panel 12 (Development Assurance and Safety Assessment), |
| **SECONDARY PANELS**[1] | : | Panel 01 (Flight and Human Factors),<br>Panel 03 (Structure),<br>Panel 04 (Hydromechanical Systems),<br>Panel 05 (Electrical Systems),<br>Panel 06 (Avionics Systems),<br>Panel 07 (Powerplant Installation and Fuel Systems),<br>Panel 08 (Environmental Control Systems),<br>Panel 10 (Software and Airborne Electronic Hardware). |
| **NATURE** | : | Special Condition |

---

## SPECIAL CONDITION

## Equipment, systems, and installations

This special condition and the related AMC are applicable to any RPAS:

- for which a type certification is requested,
- for which the kinetic energy assessment in accordance with section 6 of the EASA policy E.Y013-01 results in an initial certification basis according to CS-VLA or CS-VLR, and
- with no occupant on board.

### SC-RPAS.1309 Equipment, systems, and installations

The requirements of this paragraph are applicable, in addition to specific design requirements of the applicable type certification basis, to any equipment or system as part of the Remotely Piloted Aircraft System (RPAS).

(a) The RPAS equipment and systems must be designed and installed so that:

(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the RPAS operating and environmental conditions; and

(2) Any other equipment and system does not adversely affect the proper functioning of those covered by paragraph (a)(1) of this section.

(b) The RPAS systems and associated components considered separately and in relation to other systems, must be designed and installed so that:

---

[1] The Secondary Panels can be adapted depending on the project.

(1) Each catastrophic failure condition is extremely improbable and does not result from a single failure;
(2) Each hazardous failure condition is extremely remote; and
(3) Each major failure condition is remote.

(c) Information concerning an unsafe system operating condition must be provided in a timely manner to the remote crew to enable them to take appropriate corrective action. An appropriate alert must be provided in accordance with the requirements for remote crew alerting. RPAS systems and controls, including indications and annunciations, must be designed in accordance with the requirements for installed systems and equipment for use by the remote crew, when applicable, to minimise remote crew errors which could create additional hazards.

**ANNEX, Appendix 1** Acceptable Means of Compliance to SC-RPAS.1309

**Appendix 1**

**ACCEPTABLE MEANS OF COMPLIANCE**

**AMC to SC-RPAS.1309**

## 1. PURPOSE

This AMC describes acceptable means for showing compliance with the requirements of SC-RPAS.1309. These means are intended to provide guidance to supplement the engineering and operational judgement that must form the basis of any compliance demonstration.

Whilst this AMC details "what" needs to be addressed, the development assurance process and the safety assessment process and material providing guidance on "how to" comply with this Special Condition are not provided in this AMC. Sources of "how-to" guidance are published in ED-79A/ARP4754A (ref. [8]) and ARP4761 (ref. [10]).

The extent to which the more structured methods and guidelines referenced /described in this AMC should be applied is a function of a system's complexity and failure consequences. In general, the extent and structure of the analyses required to show compliance with SC-RPAS.1309 will be greater when the system is more complex and the effects of the Failure Conditions are more severe. The means referenced/described in this AMC are not mandatory. Other means may be used if they show compliance with SC-RPAS.1309.

This AMC does not address the "Detect and Avoid" function and related requirements. Therefore, as mentioned in the EASA policy E.Y013-01 (ref. [1]), appropriate limitations, as accepted by the Agency, should be reflected by a statement in the Aircraft Flight Manual (AFM) limitations section (e.g. operations limited to segregated airspace only).

This AMC does not cover "Security" aspects. Interactions and interfaces between the system safety assessment process and the security assessment process exist however. Particularly, should a function be implemented or a system/equipment installed on the RPAS as a result of the security assessment process, this function or system/equipment needs to undergo the system safety assessment process.

## 2. RELATED DOCUMENTS

### 2.1. Policies

[1] E.Y013-01, EASA Policy statement on airworthiness certification of Unmanned Aircraft Systems (UAS), http://easa.europa.eu/document-library/policy-statements/ey013-01

[2] EASA Concept of Operations for Drones, A risk based approach to regulation of unmanned aircraft, http://easa.europa.eu/newsroom-and-events/general-publications/concept-operations-drones

### 2.2. Guidance and advisory materials

[3] AC 23.1309-1E, System safety analysis and assessment for Part 23 airplanes, http://www.faa.gov/regulations_policies/advisory_circulars/
[4] AC 27.1309-1B, Equipment, systems, and installations, http://www.faa.gov/regulations_policies/advisory_circulars/
[5] AMC 20-115(), Software considerations for certification of airborne systems and equipment, http://easa.europa.eu/document-library/certification-specifications/group/amc-20-general-acceptable-means-of-compliance-for-airworthiness-of-products-parts-and-appliances
[6] AMC RPAS.1309, JARUS Working Group 6, Safety assessment of Remotely Piloted Aircraft Systems (RPAS), issue 02 dated April 2015

### 2.3. Industry documents

[7] EUROCAE ED-12C/RTCA DO-178C, Software considerations in airborne systems and equipment certification
[8] EUROCAE ED-79A/SAE ARP4754A, Guidelines for development of civil aircraft and systems
[9] EUROCAE ED-80/RTCA DO-254, Design assurance guidance for airborne electronic hardware
[10] SAE ARP4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment.

## 3. APPLICABILITY OF SC-RPAS.1309

This special condition and the related AMC are applicable to any RPAS:
- for which a type certification is requested,
- for which the kinetic energy assessment in accordance with section 6 of the EASA policy E.Y013-01 (ref. [1]) results in an initial certification basis according to CS-VLA or CS-VLR, and
- with no occupant on board.

This AMC does not apply to the performance, flight characteristics requirements of equivalent manned certification specifications Subpart B, and structural loads and strength requirements of equivalent manned certification specifications Subparts C and D. The flight structure such as wing, empennage, control surfaces; the fuselage, engine mounting, and landing gear and their related primary attachments are also excluded, as are rotorcraft rotors and transmissions.

## 4. DEFINITIONS

**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. (ED-79A/ARP4754A, ref. [8])

**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. (ED-79A/ARP4754A, ref. [8])

**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).
Note: Errors may cause failures but are not considered failures. (AC 23.1309-1E, ref. [3])

**Failure Condition:** A condition having an effect on the RPAS (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.

**Error:** An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation. (AC 23.1309-1E, ref. [3])

**Event:** An occurrence which has its origin distinct from the RPAS, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, payload fire. The term is not intended to cover sabotage.

**Remote Pilot Station (RPS):** The component of the remotely piloted aircraft system containing the equipment used to pilot the remotely piloted aircraft.

**Remotely Piloted Aircraft (RPA):** An unmanned aircraft which is piloted from a remote pilot station. (Note – this is a subcategory of Unmanned Aircraft).

**Remotely Piloted Aircraft System (RPAS):** A remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components as specified in the type design.

**Separation Assurance:** The capability to maintain safe separation from other aircraft in compliance with the applicable rules of flight.

**Unmanned Aircraft (UA):** An aircraft which is intended to operate with no pilot on-board.

**Unmanned Aircraft System (UAS):** An aircraft and its associated elements which is operated with no pilot on-board.

## 5. BACKGROUND

At the time of writing, the Agency is following a new regulatory approach for safely operating remotely piloted aircraft. This flexible approach, called “Concept of Operations” (ref. [2]), has been based on input from users and manufacturers of RPAS and provides a set of rules which are proportionate and risk based.

Considering the broad range of aircraft operations and types, it has been proposed by the Agency to establish three categories of operations and their associated regulatory regime: Open category, Specific Operation category, and Certified category. The special condition SC-RPAS.1309 falls within the Certified category.

The AMC to SC-RPAS.1309 has been mainly built upon:
- the principles laid down in the section 7.7 of the EASA policy E.Y013-01 (ref. [1]), and
- the issue 02 of the AMC RPAS.1309 from the JARUS Working Group 6 (ref. [6]).

This special condition and the related AMC are then applicable to any RPAS:
- for which a type certification is requested,
- for which the kinetic energy assessment in accordance with section 6 of the EASA policy E.Y013-01 (ref.[1]) results in an initial certification basis according to CS-VLA or CS-VLR, and
- with no occupant on board.

## 6. COMPLIANCE WITH SC-RPAS.1309(a)

SC-RPAS.1309(a) requires that the RPAS equipment and systems must be designed and installed so that:
(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the RPAS operating and environmental conditions; and
(2) Any other equipment and system does not adversely affect the proper functioning of those covered by paragraph (a)(1) of this section.

SC-RPAS.1309(a)(1) covers the equipment and systems installed to meet a regulatory requirement, or whose improper functioning would adversely influence the safety of the RPAS, the remote crew or third parties. Such systems and equipment are required to "perform as intended under the RPAS operating and environmental conditions." The RPAS operating and environmental conditions include:
- the full normal operating envelope of the RPAS, as defined by the AFM, with any modification to that envelope associated with abnormal or emergency procedures,
- any anticipated external RPAS environmental conditions,
  External environmental conditions such as atmospheric turbulence, HIRF, lightning, and precipitation, which the RPAS is reasonably expected to encounter, must then be considered. The severities of the external environmental conditions to be considered are limited to those established by certification standards and precedence.
- any anticipated internal RPAS environmental conditions, and
  The environmental effect within the RPA must be considered. These effects should include vibration and acceleration loads, variations in fluid pressure and electrical power, and fluid or vapour contamination due to either the normal environment or accidental leaks or spillage and handling by personnel.
- any additional conditions where equipment and systems are assumed to "perform as intended."

Per SC-RPAS.1309(a)(2), any other installed equipment or system, is required to be analysed in order to ensure it does not adversely affect the proper functioning of those covered by paragraph (a)(1) of this section.

Operational and environmental qualification requirements for those equipment, systems, and installations are thus reduced to the necessary tests that show their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations under SC-RPAS.1309(a)(1) and does not otherwise adversely influence the safety of the RPAS, the remote crew or third parties. Examples of adverse influences include fire, explosion, exposure to high voltages, etc.

## 7. COMPLIANCE WITH SC-RPAS.1309(b)

### 7.1. Failure condition classification

The classification of a failure condition does not depend on whether a system or function is required by specific regulation. Some systems required by regulation, such as position lights and transponders, may have the potential for only minor failure conditions. Conversely, other systems not required by any specific regulation, such as automatic take-off and landing systems may have the potential for catastrophic failure conditions.

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 RPAS or increase the remote crew workload.
2) **Minor:** Failure conditions that would not significantly reduce RPAS 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 RPAS 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 RPAS 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 RPA 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 Aircraft and Systems Functional Hazard Assessment, the applicant will have to substantiate the effects of failure conditions with consideration to operational conditions and events.

An emergency recovery capability may be used as a means of mitigating Catastrophic failure conditions. Where an emergency recovery function 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 analysis to ensure a level of performance acceptable to the Agency. The use of emergency crash sites is

one option available to applicants to mitigate against high severity failure conditions. The applicant will need to provide evidence to the Agency that their use will not result in unacceptable risks.

"Health and Safety at work" legislations are applicable to ground equipment and personnel. This is outside the scope of this AMC. The effects of a Remote Pilot Station failure or event on the ability of the flight crew to perform their duties (e.g. workload and Human Factors) and the effect on the RPA, will need to be assessed as part of the System Safety Assessment covered by this AMC.

### 7.2. Safety objectives

SC-RPAS.1309(b) requires that the RPAS systems and associated components considered separately and in relation to other systems, must be designed and installed so that any catastrophic failure condition is extremely improbable and does not result from a single failure. It also requires that any hazardous failure condition is extremely remote, and that any major failure condition is remote.

#### 7.2.1. Single failure and common cause failure considerations

According to SC-RPAS.1309(b)(1), a catastrophic failure condition must not result from a single failure.
While single failures must normally be assumed to occur, experienced engineering judgment and 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.

A single failure includes any set of failures which cannot be shown to be independent from each other. The analysis should then also pay particular attention to common cause failures (including common mode failures) and cascading failures.

Protection from multiple malfunctions or failures should be provided when the first malfunction or failure would not be detected during normal operations of the RPAS, which includes preflight checks, or if the first malfunction or failure would inevitably cause other malfunctions or failures.

Sources of common cause and cascading failures include development, manufacturing, installation, maintenance, shared resource, event outside the system(s) concerned, etc. The ARP4761 (ref. [10]) 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).

#### 7.2.2. Allowable probabilities

The Table 1 below provides the relationship among Severity of Failure Conditions and Probabilities.

| **Classification of Failure Conditions (Note 4)** | | | | |
|---|---|---|---|---|
| No Safety Effect | Minor | Major | Hazardous | Catastrophic |
| **Allowable Qualitative Probability (Note 4)** | | | | |
| No Probability Requirement | Probable | Remote | Extremely Remote | Extremely Improbable |
| **Allowable Quantitative Probabilities (Note 2) (Note 4)** | | | | |
| No Probability Requirement | **$<10^{-3}$** (Note 1) | **$<10^{-4}$** (Note 1) | **$<10^{-5}$** | **$<10^{-6}$** (Note 3) |

*Table 1*
*Relationship among Severity of Failure Conditions and Probabilities*

Notes pertaining to Table 1:

- Note 1: Numerical values indicate an order of probability range and are provided here as a reference. The applicant is usually not required to perform a quantitative analysis for minor and major failure conditions.
- Note 2: The allowable quantitative probabilities are expressed in terms of acceptable ranges for the average probability per flight hour.
- Note 3: The allowable quantitative probability relies on the assumption that the total number of potentially catastrophic failure conditions for the product is in the order of magnitude of 10. Early concurrence with the Agency is required if this assumption is not valid on a specific project.
- Note 4: An average flight profile (including flight phases duration) and an average flight duration should be defined.

### 7.3. Development assurance

This AMC recognises the ED-79A/ARP4754A (ref. [8]), ED-12C/DO-178C (ref. [7]) and ED-80/DO-254 (ref. [9]) as acceptable guidelines for establishing a development assurance process for aircraft, systems, software and airborne electronic hardware.

The extent of application of ED-79A/ARP4754A (ref. [8]) to substantiate functional development assurance activities would be related to the complexity of the systems used and their level of interaction with other systems. Early concurrence with the Agency is essential.

The Table 2 below provides the relationship among Severity of Failure Conditions and Development Assurance Levels (DAL).

| **Classification of Failure Conditions** | | | | |
|---|---|---|---|---|
| No Safety Effect | Minor | Major | Hazardous | Catastrophic |
| **Allowable Development Assurance Level (DAL)** | | | | |
| No DAL Requirement | DAL=D | DAL=C | DAL=C | DAL=B |

*Table 2*
*Relationship among Severity of Failure Conditions and Development Assurance Levels (DAL)*

For those cases where the Agency has agreed that functional development assurance activities need not to be performed, Table 2 should be used to assign DALs at software and airborne electronic hardware levels.

The DAL assignment method proposed in ED-79A/ARP4754A (ref. [8]) section 5.2 may be used to assign DALs lower than those proposed in Table 2. Early concurrence with the Agency is required on the DAL assignment method.

The DAL assignments in other AC/AMCs, when applicable, should take precedence over the application of Table 2.

## 8. COMPLIANCE WITH SC-RPAS.1309(c)

SC-RPAS.1309(c) requires that information concerning an unsafe system operating condition must be provided in a timely manner to the remote crew to enable them to take appropriate corrective action. An appropriate alert must be provided if immediate awareness and immediate or subsequent corrective action is required. The particular method of indication depends on the urgency and need for remote crew awareness or action necessary for the particular failure. The alerting must be provided in accordance with the requirements for remote crew alerting. The use of periodic maintenance or remote crew checks to detect significant latent failures when they occur should not be used in lieu of practical and reliable failure monitoring and indications.

SC-RPAS.1309(c) specifies that RPAS systems and controls, including indications and annunciations, must be designed in accordance with the requirements for installed systems and equipment for use by the remote crew, when applicable, to minimise remote crew errors which could create additional hazards. The additional hazards to be minimized include those caused by inappropriate actions by a remote crewmember in response to the failure, or those that could occur after a failure.

## 9. OPERATIONAL AND MAINTENANCE CONSIDERATIONS

Quantitative assessments of the probabilities of remote crew and maintenance errors are not considered feasible. Reasonable tasks are those for which full credit can be taken because the remote crew or maintenance personnel can realistically be anticipated to perform them correctly when they are required or scheduled. For the purposes of quantitative analysis, a probability of one can be assumed for remote crew and maintenance tasks that have been evaluated and found to be reasonable. In addition, based on experienced engineering and operational judgment, the discovery of obvious failures during normal operation and maintenance of the RPAS may be considered, even though such failures are not the primary purpose or focus of the operational or maintenance actions.

### 9.1. Remote crew actions

When assessing the ability of the remote crew to cope with a failure condition, the information provided to the crew and the complexity of the required action should be considered.

Annunciation that requires remote crew actions should be evaluated to determine if the required actions can be accomplished in a timely manner without exceptional pilot skills. 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 pilot skill or strength, credit may be taken for correct and appropriate corrective action for both qualitative and quantitative assessments. 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 pilot skill or strength.

Unless remote crew actions are accepted as normal airmanship, the appropriate procedures should be included in the Agency approved AFM or in the AFM revision or supplement. The AFM should include procedures for operation of complex systems such as integrated flight guidance and control systems. These procedures should include proper pilot response to cockpit indications, diagnosis of system failures, discussion of possible pilot-induced flight control system problems, and use of the system in a safe manner.

### 9.2. Maintenance actions

Credit may be taken for 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 Agency approved ICA. Annunciated failures will be corrected before the next flight or a maximum duration will 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 hazardous or catastrophic, then a maintenance task should be established. Some latent failures can be assumed to be identified based upon a return to service test on the equipment following its removal and repair (component MTBF should be the basis for the check interval time).