European Union Aviation Safety Agency

Comment-Response Document (CRD) to Proposed MoC Light-UAS 2510-01 SAIL V and VI

Comment-Response Document (CRD) to Proposed MoC Light-UAS 2510-01 SAIL V and VI, MOC Light-UAS High Risk.2510-01, Issue 01, dated 08 July 2024

European Union Aviation Safety Agency

Comment-Response Document (CRD) to Proposed MoC Light-UAS 2510-01 SAIL V and VI

Table of contents

1. Summary of the outcome of the consultation 3
2. Individual comments and responses 4
   2.1. IV. CRD table of comments, responses and resulting text 4
3. Appendix A Attachments 46
4. Explanatory Note 47

1. Summary of the outcome of the consultation

During the public consultation of the above referenced proposed MOC Light-UAS High

Risk.2510-01 to Special condition Light-UAS High Risk 01 from 08 July 2024 to 22 August 2024, EASA has received

- 106 comments
- From 12 differenct commenters

Several commenters questioned the rationale behind the stringent safety objectives, particularly the probability thresholds for catastrophic failure conditions (e.g., 10^-8 for SAIL VI). Concerns were raised that these thresholds were arbitrary and overly conservative compared to manned aviation. An Explanatory note can be found in this document to clarify the rationale, which aligns with SORA's Target Levels of Safety (TLS). SAIL V and VI operations assume higher risks, necessitating stricter safety objectives. Adjustments for proportionality, such as assigning FDAL D for major failure conditions, were incorporated.

The transition from SAIL IV to SAIL V was described as steep, with disproportionately higher safety requirements, especially regarding development assurance and safety analyses. The agency emphasized that these requirements reflect the increased complexity and risk of SAIL V/VI operations. Proposals to soften transitions were noted, but no fundamental changes were made, as the requirements are tailored to the risk levels and operational environments.

Comments sought clarification on how "loss of control of operation" is defined and whether all such failures should always be catastrophic. Clarification is provided in the explanatory note. An additional of scenario was provided for consideration as non-catastrophic.

The rationale for separating FDAL and IDAL and their specific use cases was unclear. Some questioned why higher development assurance levels were required compared to manned VTOL aircraft. FDAL/IDAL usage was clarified as being aligned with ED-135 guidelines. A note was added to clarify the assignment of lower FDAL/IDAL to functions/item contributing to catastrophic and hazardous failure conditions.

Comments noted redundancy and complexity in the text, potentially leading to difficulties in interpretation. Editorial changes were made to simplify language and remove ambiguities.

2. Individual comments and responses

In responding to comments, EASA states its position as follows:

(a) **Accepted** — EASA agrees with the comment and any proposed change is incorporated into the text.

(b) **Partially accepted** — EASA either partially agrees with the comment or agrees with it but the proposed change is partially incorporated into the text.

(c) **Noted** — EASA acknowledges the comment, but no change to the text is considered necessary.

(d) **Not accepted** — EASA does not agree with the comment or proposed change.

2.1. IV. CRD table of comments, responses and resulting text

(General Comments)	-

comment	*4*	comment by: *S.PIZZIOL*
	Most of the comments proposed hereafter have the general purpose of preserving a coherent (within this very document and wrt many JARUS documents) definition of a 'Loss of control, and of a Hazardous/Catastrophic Failure Condition'. For all SAIL levels fatalities are uniformly expected at a TLOS of 1*E-6 FH. Nevertheless, the probability of a fatality after a LOC changes depending on the SAIL level (for instance 1000 LOC are expected to lead to a fatality in SAIL III versus only 10 LOC in SAIL V). That fact alone justifies (we think) to put a requirement on the absence of points of single failure on the FCs leading to a LOC, starting from SAIL V. For our prospective the proposed MOC obtains the desired effect (no single failure leading to a LOC SAIL V/VI), but sometimes ambiguously mixes two concepts: a FC leading to a LOC and a CAT-FC. That leads to provide quantitative requirements that seem wrongly defined to us. The comments proposed hereafter have, if combined, the effect of keeping that qualitative requirement on LOC without altering the meaning of the initial definitions. Moreover, since in principle not all CAT-FC stems from a LOC event, and that not all LOC events lead to a CAT-FC (for instance on a controlled area, as remembered in 9.1), one should avoid mixing the two concepts.	
response	Noted The relationship between LOC and CAT FC are explained in the MOC: "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." See also the explanatory note for clarification.	

comment	*19*	comment by: *AESA*

	It is not clear the reason to separate between FDAL and IDAL since at the end of the assessment the IDAL is neglected and considered equal to DAL/FDAL. Some clarification is needed. MoC Light-UAS 2510 does only take into account DAL. Not FDAL nor IDAL.
response	Noted The use of FDAL and IDAL is to be understood as described in ED-135. The Certification Memorandum on the use of System Development Assurance also clearly requires the use of full system level Development Assurance. Hence the IDAL is not considered equal to FDAL.

comment	*63* comment by: *FOCA (Switzerland)* Thank you for the opportunity to comment and for considering our inputs on Means of Compliance UAS 2510-01 SAIL IV. We have no further remarks on this document.
response	Noted

comment	*96* comment by: *AOPA Sweden* **AOPA Sweden** **General comment on Means of Compliance with Light-UAS.2510-01.** **Stockholm 24-08-18** We do not have any objections to the proposal as such. As always we object to the amount of text which is very much redundant and does not contribute to clarification. Persons that do not have experience of reading text, will have difficulties to follow the rules. A good idea is to minimize the text and that will not jeopardize the safety of UAS operations. Best regards Fredrik Brandel Board member AOPA Sweden
response	Noted.

2. Applicability p. 2

comment	*37* comment by: *AESA* **Referenced text:** 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). **Comment:** Add a comma after "Likewise"
response	Accepted Text will be changed

comment	*41* comment by: *Michel Allouche* (e) The inclusion of pre-flight preparations is ambiguous and should be clarified since it may also be considered as a maintenance activity. Usually, the phases of the safety

	assessment start from the taxi phase and then include all the phases of the flight (e.g. take-off, (possibly: climb), flight and (possibly descent), landing).
response	Not accepted the MOC already provided guidance that maintenance is not considered as pre-flight preparations. As for any application the applicant is expected to defined the flight phases in their safety plan and propose the scope of "pre-flight preparation". These may be specific to each UAV operations. The wording used in this paragraph is common wording already in use in other xx.1309/xx.2510.

comment	*42* comment by: *Michel Allouche* It is suggested to add: "Artificial Intelligence / Machine Learning (AI/ML) techniques are not covered by this MOC and may require particular compliance demonstration, **unless it may be shown that they have no safety effects**"
response	Not accepted The sentence does not mean, that no AI/ML can be used in the UAS design. It should be understood that the MOC 2510 does not provide sufficient guidance to demonstrate that the safety objectives of AI/ML constituents have been met. The MOC 2510 can be used to demonstrate that the AI/ML constitutent has no safety effect.

comment	*44* comment by: *Michel Allouche* (a) Note that OSO #05 has been amended in the SORA 2.5 and that this amendment should normally be soon endorsed by EASA. (b) Also, the comments (3) and (4) included in OSO # 05 (referring to JARUS AMC RPAS.1309 Issue 2 Table 3, in both SORA 2.0 and 2.5) will become irrelevant once new specific safety objectives will be finalized after formal issuance of this MoC
response	Noted a) SORA 2.5 does not impact the MOC for High Risk Light UAS (SAIL V and VI). b) noted

comment	*55* comment by: *DGAC FR* When referred to as “As specified in SC Light-UAS High Risk.2500 (a)”, should not it be SC Light-UAS High Risk . 2510 (a) or SC Light-UAS Medium Risk . 2500 (a) ?
response	Partially Accepted Text will be changed to SC Light-UAS.2500 (a)

comment	*56* comment by: *DGAC FR*

	Instead of writing “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”, we recommend the following formulation: “If the use of AI/ML is envisaged by the applicant, early coordination with EASA is required".
response	Noted This paragraoh intends to clarify that the methods prescribed in this MOC are not necessarily sufficient to demonstrate that hazards from systems employing AI/ML techniques are minimized to an acceptable level. Wording is therefore deemed necessary

comment	*65* comment by: *UAV DACH AC* EDITORIAL - Para 1, 1st sentence: replace "to operate" by "for"
response	Accepted Wording will be changed

comment	*66* comment by: *UAV DACH AC* Item (a): add SC in "General SC Light-UAS"
response	Not accepted common terminology also used in other CSs/SCs

comment	*67* comment by: *UAV DACH AC* EDITORIAL - Item (a), 2nd sentence, last word "risk": "Risk" (capital letter) in order to be consistent
response	Accepted Wording will be changed

comment	*68* comment by: *UAV DACH AC* EDITORIAL - Page3, penultimate sentence: Change to "This MOC considers the operation of one aircraft per control and monitoring unit (CMU)" instead of "This MOC considers the operation of one aircraft for each control and monitoring unit (CMU)" Otherwise it could be interpreted that for each UAS a dedicated, specific CMU must exist and must be used.
response	Accepted Wording will be changed

1. Purpose p. 2

comment	*64* comment by: *UAV DACH AC* EDITORIAL - "Special Condition Light-UAS High Risk.2510 (a) and (b).": For CLEARNESS: General: It would be more logical to append the risk class to the general SC, e.g.: "SC Light-UAS.2510(a) and (b) (high risk)"
response	Noted The requirements in SC Light-UAS High Risk do not have the risk classes appended. (e.g. Light-UAS.2510). This approach is followed, with the exception of §1, where it is supposed to be emphasized that the scope of this MOC is related to High risk

3. Referenced documents p. 3

comment	*5* comment by: *S.PIZZIOL* Missing reference to a JARUS SORA 2.5 document: JARUS guidelines on Specific Operations Risk Assessment (SORA) DOCUMENT IDENTIFIER : JAR-DEL-SRM-SORA-MB-2.5 Edition Number 2.5 Edition Date 13.05.2024
response	Not accepted the legal reference is Regulation 2019/947, which at time of writing, contains the SORA 2.0 methodology.
comment	*43* comment by: *Michel Allouche* (a) Some of the quoted documents have been purely established for a manned CS-25 Type Certification process. Whereas parts of those documents could be used as guidance in UAS application, some other parts would not be adequate. The following notes are thus proposed to be added: Note 1: References (c), (d), (e), (f), (g), (h), (i) have been specifically established for manned aircraft and some of the sections may have to be tailored to UAS applications Note 2: Refer to Shepherd Project Report regarding the assessment of ASTM F3309-21 and relevant sections that may or may not be used as guidance. (b) It is proposed to add in the list the EUROCAE document ED-279 "Generic FHA for UAS/RPAS" that also provide useful guidance to conduct an UAS FHA. It also includes a preliminary review of the applicability of ED-135 considering the specific character of UAS applications, see its Appendix D.
response	Partially accepted a)Quoting those documents in the "references" chapter does not mean, that the entire document is applicable or required for compliance to MOC 2510. This is made clear by the statement that these documents provide "additional guidance".

	Throughout the MOC there are references to specific chapters of these documents. A change to the wording will be made to make clear that documents like ED-135 need tailoring for the UAS context. b) ED-279 will be added

comment	*69* comment by: *UAV DACH AC* EDITORIAL - items (h),(i): add "EASA" before "AMC"
response	Accepted wording will be changed

comment	*70* comment by: *UAV DACH AC* QUESTION - Why is there no (cross) reference made to the already published MOC Light-UAS.2510 Medium Risk. As well as the (still proposed MOC OSO#5)? A scoping with regards to these would be helpful.
response	Noted This MOC is standalone and does not require cross reference to SAIL III and SAIL IV MOCs

4. List of acronyms p. 4

comment	*57* comment by: *DGAC FR* ASTM International: (previously American Society for Testing and Material).
response	Accepted wording will be changed

5. Definitions p. 5

comment	*6* comment by: *S.PIZZIOL* Maybe the definition + the examples (i.e. flyaway, crash etc..) taken from SORA 2.5 could be cited here (for the sake of clarity only): -Loss of control of the operation is a state that corresponds to situations: i. Where the outcome of the situation highly relies on providence, or ii. Which could not be handled by a contingency procedure. -In the context of the semantic model, 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.

response	Accepted wording will be changed

comment	*20* comment by: *AESA* **Referenced text:** (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) **Comment:** Add AMC 25.1309 to reference list
response	Not accepted AMC 25.1309 is only referred to in the definitions chapter, there is no need to quote is as additional guidance.

comment	*21* comment by: *AESA* **Referenced text:** (h) 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) **Comment:** Since errors are not considered to be failures, please add "error" to definitions list in order to separate it from (f) (development error)
response	Accepted Definition will be added

comment	*22* comment by: *AESA* **Referenced text:** (j) Function Development Assurance Level (FDAL): The level of rigor od 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) **Comment 1:** It is not clear the reason to separate between FDAL and IDAL since at the end of the assessment the IDAL is neglected and considered equal to DAL/FDAL. Some clarification is needed. MoC Light-UAS 2510 does only take into account DAL. Not FDAL nor IDAL. **Comment 2:** Typo: "od" instead of "of"
response	Partially Accepted 1) The use of FDAL and IDAL is to be understood as described in ED-135. The Certification Memorandum on the use of System Development Assurance also clearly requires the use of full system level Development Assurance. Hence the IDAL is not considered equal to FDAL.

	2) wording will be changed

comment	*59* comment by: *Michel Allouche* Add: "or events result in a Hazardous or Catastrophic Failure Condition, **as defined in section 7**" (to avoid any ambiguity: Cat / Haz severity definitions are different from C-25 Amdt 27!)
response	Not accepted CAT/HAZ severities are defined in section 7, which is deemed sufficiently clear

comment	*71* comment by: *UAV DACH AC* MAJOR CONECPTUAL - item (d) "are developed according to the semiconductor manufacturer's proprietary development processes. (Source:...)": COTS products sold (regardless if produced or imported) in the EU must comply with the EU Market Regulations (see Blue Guide 202/C 247/01). It goes without saying that such products must be developed to the manufacturer's intenal standards and processes. This implies that COTS products are manufactured (designed and produced) to meet the essential product and tracing requirements set forth in the applicable regulations manifest in product standards that typically include life cycle processes and development and test standards, in particular in regards of products safety. With this in mind the statement is at the very least missleading and cannot be upheld. Suggesting to add "are developed to comply with applicable regulations and product standards other than aviation standards, as well as according to the semiconductor manufacturer's proprietary development processes."
response	Not accepted refer to AMC20-152A definition, which is reused in this MOC. The definition does not contradict the fact that COTS equipment needs to comply with the EU market regulation.

comment	*72* comment by: *UAV DACH AC* EDITORIAL - item (j) Typo "level of rigor"
response	Accepted wording will be changed

comment	*73* comment by: *UAV DACH AC* EDITORIAL/CONCEPTUAL - item (j) "ED-79B/ARP4754B": To be consistent: Reference either EuroCAE documents only (not preffered) or together with the SAE/RTCA

	pendant as well ("ED-79N/SAE ARP4754B") (preferred). Add SAE ARP 4754B to the list of referenced documents in section 3. Suggestion: For shortness, this should be done in the reference list only.
response	Accepted wording will be changed

comment	*74* comment by: *UAV DACH AC* EDITORIAL - item (n) b.: Add JARUS SORA 2.5 to list of referenced documents in section 3
response	Not accepted the legal reference is Regulation 2019/947, which contains the SORA 2.0 methodology, at the time of writing, but will be updated and reflect the SORA 2.5

comment	*75* comment by: *UAV DACH AC* EDITORIAL MAJOR - item (p) "Gartner": This reference is not meeting minimum citation standards and cannot be reproduced. Add with minimum details to list of referenced documents in section 3.
response	Noted The definition source is: https://www.gartner.com/en/information-technology/glossary/open-source

comment	*76* comment by: *UAV DACH AC* EDITORIAL - item (t), Source: add (EASA) CS-25 Amt. 27 to list of referenced documents in section 3.
response	Not accepted the documents referenced are sources of additional guidance, CS-25 Amdt 27 is not considered additional guidance in this context

comment	*77* comment by: *UAV DACH AC* EDITORIAL - item (u), Source: add ASTM F3230-20a to list of referenced documents in section 3. Active issue isF3230-**21a** and should be applied
response	Not accepted see comment 76

comment	*99* comment by: *S. Sellem-Delmar / Safran* Comment :

	Definition of "Failure Condition" refer to "separation assurance" which is not defined in section 5, nor used in the MOC. Suggested resolution : Suggest to either remove "(inc. Separation assurance)" from the definition of "Failure Condition", or alternatively add definition of "Separation Assurance" in section 5.
response	Partially accepted There are specific TMPR availability requirements defining an allowable loss of function and performance, therefore the loss of an equipment used for separation assurance, needs to be addressed.

6. Principles of Fail-Safe design concept p. 6

comment	*7* comment by: *S.PIZZIOL* Possibly add a reference to the adapted source (AMC 25.1309).
response	Not accepted the documents referenced are sources of additional guidance, CS-25 Amdt 27 is not considered additional guidance in this context

comment	*23* comment by: *AESA* **Referenced text:** (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. **Comment:** Remove the "one" in "any one flight"
response	Not accepted "Any one flight" implies that this consideration applies to every individual flight, not just specific flights or types of flights.

comment	*60* comment by: *Michel Allouche* (1) : "Such single failures should not be catastrophic" Please see our comments under 8.2 and proposed addition regarding the cases of "single failure not a practical possibility" and add: "Such single failures should not be catastrophic **(see also section 8.2)**"
response	Noted see answer to comment 45

comment	*78* comment by: *UAV DACH AC*

	EDITORIAL - para 3, item (1) "life limits": correct would be "lifetime limits" or "operating time limits".
response	Noted the term life limit is an appropriate term used in other CSs/AMCs

7. Failure Condition classification p. 7

comment	*58* comment by: *DGAC FR* At the point “hazardous” it is mentioned “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”. How should be classified a failure condition that would have effects such as physical distress or non serious injuries (Major to be aligned with AC23.1309 or Hazardous) ? How should it be evaluated that this consequence can be "reasonably expected" or not (Operational limitations ?)
response	Noted As stated in §9.1 a loss of control in SAIL V and VI should be expected to lead to a fatality. This is considered to be appropriate, due to the relationship between the acceptable loss of control rate and the TLOS (as defined in JARUS SORA Annex F). Operational limitations may be one way to demonstrate that a LOC may not lead to a fatality, in which case the failure condition could be classified HAZ. These cases should be discussed with EASA early in the project.

comment	*79* comment by: *UAV DACH AC* CONCEPTUAL MINOR - Why is there no cross reference to the JARUS AMC RPAS.1309, where this failure classification is clearly coming from.
response	Noted The EASA SC-RPAS.1309 uses the same definitions, it is not considered adding value to add a reference

comment	*80* comment by: *UAV DACH AC* CONCEPTUAL MAJOR - item 3) "reduction in (...), functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency." As - separation assurance is a functional capability - "in addition" implies that the following condition has to be met as well (logical "AND"), consider rephrasing, e.g.: "reduction in (...) or functional capabilities (including separation assurance), a significant increase in remote crew workload or in conditions impairing remote crew efficiency."
response	Noted There could be a reduction of functional capability of the UA, without an increase of crew workload (e.g. latent failures), nevertheless this should be classified at least major.

comment	*81* comment by: *UAV DACH AC* EDITORIAL - item 4) i) "one or more" - is including "one" or "at least one" - Rephrase: "no fatality will occur".
response	Not accepted this is an established wording, also found in other .1309/.2510

comment	*82* comment by: *UAV DACH AC* CONCEPTUAL MAJOR - item 4) ii) (same as comment on item 3) "reduction in (...), functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency." As - separation assurance is a functional capability - "in addition" implies that the following condition has to be met as well (logical "AND"), consider rephrasing, e.g.: "reduction in (...) or functional capabilities (including separation assurance), a significant increase in remote crew workload or in conditions impairing remote crew efficiency."
response	Noted see answer to comment 80

8.1 Safety Objectives per SAIL and failure condition classification p. 8

comment

1 comment by: *THALES*

" with the exception that no FDAL D should contribute to catastrophic failure conditions"

As per ED-135, "Development Assurance Level assignment to members of a functional failure set" Table P-2, for a Top level Failure Condition requiring a FDAL B, FDAL (IDAL) D is authorized for functional Failure sets with multiple members.

This draft MoC identifies FDAL B for CAT Failure Conditions (Top Level) (in place of FDAL A (Top Level) for CAT Failure Condition in ED-135), this exception should consequently not be identified for a Top Level Failure FDAL B.

If this exception is kept, an alternative should be proposed to have specific mitigiation for such FDAL D members, such as failure detection or specific procedure to reduce time risk exposure.

response

Noted

A note will be added, to clarify that the content of Table P-2 will need to be tailored in line with the content of this MoC.
The reason for Note 4 is, that it is not considered adequate to develop a member to DAL D in a functional failure set contributing to a Catastrophic failure condition.
This is also considering the higher level of integration and automation of most UAS.

comment

2 comment by: *THALES*

"SAIL VI Safety Objective FC ≤ 10-8/FH"

Such Safety Objective corresponds to CS23 having a MTOM greater than 6000 pounds (<=> 2721 kg) as per AC23.1309 Issue 1E. For UAV with MTOM not exeeding 600 kg, the quantitative safety objective should be proportional.

Thales proposal is the following one:
If FC CAT quantitative items 10-8/FH is not achieved and alternative solution could be:
- to demonstrate that all FC leading to CAT events not greater than 10-6/FH and
- some of these CAT FC are not greater than 10-7/FH

response

Noted

Aircraft level safety objective such as 10^-6 /FH for the sum of all CAT FCs is not considered a practical solution for several reasons: 1) Whether compliance has been demonstrated, will only be possible, once all systems have been collectively analysed at the end of a project, 2) Continued Airworthiness processes for certified products (determination of unsafe condition and definition of rectification intervals) is based on a "per failure condition" basis 3) Predicting at an early stage the number of CAT FCs is not an easy task and changes in the course of the program may have a cascading effect on many systems.

comment	*3* comment by: *THALES* SAIL VI FC MAJ: Qualitative objective FDAL C Such qualitative objective is the same than the one applicable to large aircraft (as per CS25). The impact of such FC is not same between an UAV & a large aircraft. For UAV (completely automatic), the remote pilote's workload can be significantly increased by such events. However, as the UAV is fully automatic, even if the remote pilot takes a wrong decision due to his workload increase, there cannot be any loss of control. Consequently, Thales proposes the following safety objectives for FC Maj: Qualitative FDAL D / Quantitative 10-3/FH
response	Not accepted The increase in crew workload is not the only consideration for a major classification. A significant reduction of safety margins or functional capabilities or separation assurance also needs to be taken into account. The numerical safety objectives proposed are therefore considered adequate. In order to introduce proportionality, it will become: DAL D for Major FC.

comment	*8* comment by: *S.PIZZIOL* Table 1: Allowable quantitate probabilities for CATastrophic-FailureCondition, SAIL V vs SAIL VI. We suspect a slip in the computation or an error in the heading of the table. SAIL VI: If for each FC leading to a CAT event we take 1*E-8/FH (as for table1), if the number of potential FC is 10 we get 1*E-7/FH for the sum of all technical FC leading to a CAT event. If we assume that less than half (for instance 10%) of all FC-CAT is technical, we get 1*E-6/FH overall for a CAT event. The acceptable TLOS (i.e. rate of fatalities) is respected. If we take the same assumptions for SAIL V: SAIL V: If for each FC leading to a CAT event we take 1*E-7/FH (as for table1), if the number of potential FC is 10 we get 1*E-6/FH for the sum of all technical FC leading to a CAT event. If we assume that less than half (for instance 10%) of all FC-CAT is technical, we get 1*E-5/FH overall for a CAT event. The acceptable TLOS (i.e. rate of fatalities) is ***not respected***. Indeed, both SAIL V and SAIL VI should have (if the assumptions are the same) the same quantitative requirement for CAT-FC. Note that the same is not true for FC leading to a LOC, for which (under the same assumptions) in SAIL VI 1*E-8/FH should hold, in SAIL V 1*E-7/FH should hold instead.

Correction proposed:

1.Add the detail on the assumption taken, similarly to what is done in AMC25.1309.
2.If our computation is considered correct, uniform the quantitative and qualitative requirements for FC-CAT SAIL V and SAIL VI (1*E-8/FH - No Single Failure).
3.If our computation is considered correct, add as an explanatory note that only for those CAT-FC expected to result from a LOC event, that the following qualitative and quantitative requirements are deemed as acceptable (in replacement of the objectives on the same CAT-FC):

FC-LOC - SAIL VI - No single failure <= 1*E-8/FH
FC-LOC - SAIL V - No single failure <= 1*E-7/FH

response

Noted

In order to align between the TLOS approach established in SORA 2.5 Annex F (LOC probability) and the safety objectives at UA technical level (probability per FC), the assumption has been made, that for a SAIL V conservatively a LOC should be considered to lead to a fatality (i.e. CAT), although it is aknowledged, that the conditional probability to cause a fatality is 0.1, it is considered sufficiently likely to meet the CAT definition (is expected to lead to one or more fatalities). A loss of control in the operational volume needs to be assumed to have the potential for fatalities. In justified cases, as described in the MoC an FC leading to loss of control, could be classified HAZ.
An explanatory note will provide a rationale for the safety objectives.

comment

11 comment by: *THALES*

FC HAZ Quantitative objective: 10-6/FH

This objective is the same for:
- CS23 Class II
or
- CS27 Class II

Thales proposal:
This SAIL VI FC HAZ quantitative objective should be reduced to 10-5/FH

response

Not accepted

quantitative objective considered adequate considering different operational environment of SAIL VI and CS 23/27 class II

comment

13 comment by: *JEDA*

In order to encourage the installation of new systems enhancing the safety, it would be good to include in this MoC the alleviation already granted to General Aviation as Net Safety Benefit (Certification Memoranda CM-SA-001)

response

Not accepted

	The intent of the Net Safety Benefit CM is not in line with the UAS regulatory development. Net safety benefit intends to allow safety enhancing technology to be implemented in the general aviation fleet, improving situational awareness of the crew.
comment	*14* comment by: *JEDA* The FDAL level assigned are agreed, as long as the FDAL to IDAL reduction is allowed. The quantitative probability are, as reference value, to high for the Hazardous and Catastrophic levels. Due to the fact that these are reference values and that the SAIL V and VI will require a certification with EASA, we would include the following sentence: "A reduction of one order of magnitude may be possible upon agreement with the Agency and presentation of appropriate justifications and limitations".
response	Not accepted see explanatory note on the rationale for the safety objectives. The MoC is presenting one acceptable means of compliance, not the only means. The certification process is always including discussions on the means of compliance applied project by project.
comment	*17* comment by: *JEDA* This comment is related to the Allowable Qualitative Probabilities in Table 1. The proposed quantitative objectives will be difficult to demonstrate and will be dependent on reliability figures of equipment. These will be difficult to find due to the relative newness of the components and/or not actually being known by the suppliers and therefore very difficult to prove. In addition, to fulfill 10-8, it may be difficult in the drone industry context to address integrity requirements like “critical parts” for example through certified propellers or engines. With reference to EASA document “ftb_moc_to_sc_light-uas” and FOCA document “FOCA AltMoC SORA 2.0 Containment” the “probability of loss of control of an operation rate equals 10-SAIL”. Flying over a populated area, the risk of loss of control of an aircraft could be expected to result in 1 or more fatalities and is therefore rated as catastrophic, up from hazardous at SAIL III and IV. Based on the “probability of loss of control of an operation rate equals 10-SAIL”, SAIL V catastrophic safety objective should be ≤ 10-5 with SAIL VI at ≤ 10-6. Furthermore, the Allowable Quantitative Probability does not seem to match JARUS AMC RPAS.1309 which is refered to in the OSO #05 of the AMC1 to Article 11 of EU Reg. 2019/947. In JARUS AMC RPAS.1309, the allowable quantitative probability of failure condition is 10-5 for hazardous and 10-6 for catastrophic failure conditions for CS-LUAS/CS-LURS. This is consistent with SC-VTOL quantitative objectives. It would be reasonable to consider that an unmanned aircraft would require lower safety objectives than an aircraft containing a pilot and passengers (where catastrophic is 10-7). We suggest to align the safety objective to 10^-SAIL for catastrophic failure conditions and proportionally 10-SAIL+1 for hazardous and 10-SAIL+2 for major.
response	Noted 1)If the reliability figures of an equipment are not known, its failure needs to be assumed to be probable and it may not be suitable for a SAIL V /VI application.

2)critical parts are not in the scope of .2510 or Subpart F and will require specific compliance demonstration
3)see explanatory note on the rationale for the safety objectives
4)In the absence of MoC the SORA 2.0 contained in Regulation 2019/947 referred to JARUS AMC RPAS.1309 for the definition of safety objectives, the SORA 2.5 of Reg 2019/947 will remove this reference. JARUS AMC RPAS.1309 as well as SC VTOL is based on different operational assumptions (certified category, population density) which makes a direct comparison difficult.

comment *24* comment by: *AESA*

Referenced text: Table 1: Safety Objectives

Comment: We believe the probabilties assigned to FDAL should be closer to the probability of LoC defined in SORA 2.5, which is 10^-SAIL. Since the system failure happens before the LoC and is still evitable, this probability should be higher, in order to be able to reduce it with mitigations to achieve the target probability of LoC event. Is recoverabilty not possible at this point of the operation? Are we assuming a fatality as a consequence of the failure of these systems? Which reference has been used to assign these probabilities of failure? Please, consider the use of JARUS RPAS.1309 and the separation between UAS classes rather than SAIL.

response Noted

See explanatory note, on how the safety objectives have been derived. JARUS RPAS.1309 has been developed for certified category UAS, not in the SORA context.

comment *25* comment by: *AESA*

Referenced text: 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.

Comment: Would you consider adding a column for minor effect and DAL D? What are considered best practices? Are minor failure conditions excluded from the assessment? In that case, we understand that they are not included in the table

response Noted

The omission of a column for minor has been intentional, as there is no requirement in SC Light UAS addressing minor failure conditions, which is found to be proportionate in this context. Aspects of industry best practices are configuration management, quality assurance, comprehensive testing considering environmental conditions, etc.

comment *39* comment by: *Michel Allouche*

Allowable Quantitative probability
(1) Absence of Rationale

The rationale behind the Catastrophic Failure probability requirements set forth for SAIL V and SAIL VI (resp. 10-7/FH and 10-8/FH) is not presented and in the absence of such a rationale these requirements appear to be quite arbitrary.

(2) Need to have a rationale consistent with SORA TLS
Such a rationale should however remain consistent with the overall SORA Target Level of Safety Approach (set at 10-6/FH) i.e.:
TLS= Loss of Control Probability x "Probability of kill"
whereas the Probability of kill (in fact related to the Probability of Hit and the Probability to kill in case of hit) is directly linked to critical area and population density (see SORA Annex F 1.2.2)
As per SORA methodology provided that all relevant OSOs are complied with, the probability of Loss of control (from all causes, system design and operational related) is 10-SAIL/FH, meaning that the "Probability of kill" would be 10-1/crash for SAIL V and 1 for SAIL VI.

(3) Potential justifying assumptions
The following table provides example of potential assumptions that may or may not lead to currently proposed MoC criteria: 10-7/FH for SAIL V 10-8/FH for SAIL VI for the probability of CAT individual system failure conditions by applying rationale similar to the one presented in e.g. manned AMC 25.1309 (6a).

SORA Target Level of Safety	1.E-06	1.E-06
SORA LOC proba from all causes (10-SAIL)	1.E-05	1.E-06
Current Draft MOC 2510 CAT FC reqt	1.E-07	1.E-08
Formula to be used to determine the required individual CAT FC probability	= (10-SAIL * Percentage of System Causes)/ (Nb of CAT System FC)	
Set 1 of Potential assumptions		
% LOC due to system causes	10%	10%
SORA LOC proba due to system causes	1.E-06	1.E-07
Nb of CAT System FC	10	10
Derived CAT proba reqt	1.E-07	1.E-08
Set 2 of Potential assumptions		
% LOC due to system causes	10%	10%
SORA LOC proba due to system causes	1.E-06	1.E-07
Nb of CAT System FC	100	100
Derived CAT proba reqt	1.E-08	1.E-09
Set 3 of Potential assumptions		
% LOC due to system causes	100%	100%
SORA LOC proba due to system causes	1.E-05	1.E-06
Nb of CAT System FC	10	10
Derived CAT proba reqt	1.E-06	1.E-07

In the above example, only Set 1 assumptions could theoretically correspond to some kind of rationale to justify the proposed EASA MoC probability requirements. However, it is clear that none of the above "attempted" assumptions can be really be validated, on one hand due to the lack of actual historical evidence (% of LOC due to system causes) or on the other hand due to the unknown number of CAT System FC which is highly dependent on the UAS level of complexity and automation. Both latter unknown parameters have a significant impact on the CAT FC probability requirements.

(4) Proposed solution
One way could nevertheless be to establish / assume a priori a given % of LOC due to system causes, e.g. as a function of the Level of Automation (as per JARUS Methodology for Evaluation of Automation
for UAS Operations or as proposed in section 5 of EASA concept paper - Guidance for Level 1 & Level 2 ML applications) and then provide only a requirement of the probability of the sum of all CAT System FC (it wpuld be then up up to the applicant to take into account the number of potential CAT FC in his system to derive the corresponding probability requirement).

response

Noted

see explanatory note on the rationale for the safety objectives.

comment

50 comment by: *Michel Allouche*

FDAL/DAL assignment
(1) The principle of required consistency between DAL assignment and required quantitative probability should be applied as e.g. consensually agreed in previous JARUS-EUROCAE 1309 Conciliation Team report and re-stated in EUROCAE ER-19 report:

- DAL A development gives confidence that the manifestation of a possible remaining error is consistent with a quantitative safety objective ≤ 10-9/fh.
- DAL B development gives confidence that the manifestation of a possible remaining error is consistent with a quantitative safety objective less than 10-7/fh and greater than 10-9/fh.
- DAL C development gives confidence that the manifestation of a possible remaining error is consistent with a quantitative safety objective of less than 10-5/fh and greater than 10-7/fh
- DAL D development gives confidence that the manifestation of a possible remaining error is consistent with a quantitative safety objective greater than 10-5/fh

Refer to previous comment on allowable quantitative probability, the eventual FDAL assignment should be consistent with the finally agreed quantitative probability.

	(2) Note that even when applying the above principle to the currently proposed MoC table, the following changes should be brought: SAIL V: Major / FDAL D, Hazardous-Catastrophic FDAL C SAIL VI: Major / FDAL D, Hazardous FDAL C (OK for FDAL B - Catastrophic if the probability of 10-8/FH would be retained
response	Accepted It will become: DAL D for Major FC to introduce proportionality

comment	*51* comment by: *Michel Allouche* Note 4: It is agreed to use the principles of FDAL/IDAL assignment in taking account of architectural considerations as stated in ED-135 Appendix P. However, the table P-2 of ED-135 has to be adapted since a lower FDAL is assigned to Catastrophic effect. One way could be to add: Using architectural considerations for assigning a FDAL as described in ED-135 Appendix P **(as duly tailored to take into considerations that a lower FDAL is assigned to Catastrophic Effect in the context of this MoC)**
response	Partially accepted Wording will be changed to clarify that the table P-2 of ED-135 needs adaptation

comment	*83* comment by: *UAV DACH AC* MAJOR - Table 1 Where do these numbers come from? Rationale and reference are missing. The numbers by themselves cannot be comprehended or reproduced and appear disproportionate: (a) Why are 10^-8/10^-7 safety targets necessary, if the overall safety target of the specific group is only 10-^6/FH (as per Jarus SORA 2.5 Annex F)? (b) The number of major failure conditions is much higher than hazardous or catastrophic failure conditions. However, they do not cause injuries (as in manned aeroplanes). Therefore, it should be considered to waive a SSA that determines the allowable quantitative probability. It would be helpful to publish a "Safety Continuum" document for UAS and VCA, similar like the FAA "Safety Continuum for Powered-Lift" PS-AIR-21.17-01. This would make it much easier crossreferencing from OSO#5, MOC Light-UAS.2510 medium risk and MOC Light-UAS.2510 high risk.
response	Noted see explanatory note on the rationale for the safety objectives.

comment	*84* comment by: *UAV DACH AC* MAJOR - It should be explained how different mission durations should be treated, that means short missions < 1 fh and durations far above 10 or 100 fh.

response | Noted

Probabilities should be expressed as an average probability per flight hour

comment | *97* comment by: *S. Sellem-Delmar / Safran*

Attachment #1

Comment :
Transition from SAIL IV to SAIL V safety objectives currently seem very steep and not in line with the progressivity of requirements with SAIL increase (excessive step effect compared to GRC scale). Transition from SAIL IV design effort, development assurance requirements and safety assessment, to full fledged activities and much higher standards would mean SAIL V systems are disproportionately more costly than SAIL IV in safety requirements compliance activities, and thus unachievable. In particular, FDAL B for CAT FC, FDAL C for MAJ FC, and a 2 orders of magnitude increase in quantitative objectives seem unachievable to us.
We suggest that the transition from SAIL IV to SAIL V focuses mainly on broadening the scope of safety analyses, including operational hazards and less dangerous FC from MAJ and HAZ categories, and common cause analysis, as required by ED135.
We also propose a more progressive increase of safety objectives as follows, upgrading Safety level from SAIL IV but more in consistency with GRC scale than current proposal.

Suggested resolution :
Soften requirements increases from SAIL IV to SAIL V, in consistency with risk progressivity (no step effect).
Proposal = table in attachment and update of the text accordingly.

CAT	MAJ	HAZ
SAIL V	FDAL D	FDAL C	FDAL C
	(No Single Failure)		
	10^{-3}	10^{-5}	10^{-6}
SAIL VI	FDAL C	FDAL C	FDAL B
	(No Single Failure)		
	10^{-4}	10^{-6}	10^{-8}

response | Noted

	see explanatory note on the rationale for the safety objectives. SORA is imposing the need to have more stringent safety objectives for SAIL V/VI compared to SAIL IV and below). In order to introduce proportionality, it will become: DAL D for Major FC.
comment	*105* comment by: *THALES* SAIL V/VI FC MAJ 10-4/FH Quantitative objective & FDAL C Remark: Delta with Jarus AMC RPAS 1309 Issue 2: No DAL C for 10-4/FH quantitative objective in the Jarus document only DAL D is allocated to such quantitative objective. Why such DAL level is defined for such FC MAJ? FC MAJ for SAIL V & VI is identical. Could you please explain this choice?
response	Noted There is no direct connection between an assigned Development Assurance Level and a numerical probability objective. In order to introduce proportionality, it will become: DAL D for Major FC.
comment	*106* comment by: *ANZEN* It is unclear how the safety objectives have been allocated. EU implementing regulation 2019/947 under AMC 1 to article 11 (SORA) Annex E.2 within the OSO#5 high integrity within the comments the following is stated: "*Safety objectives may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the kinetic energy assessment made in accordance with Section 6 of EASA policy E.Y013-01. Development assurance levels (DALs) for SW/AEH may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the kinetic energy assessment made in accordance with Section 6 of EASA policy E.Y013-01*.". JARUS AMC RPAS.1309 provides justifications on how the target levels of safety and thus the probability requirements are derived. Following such justifications it is unclear how the required levels have been achieved as the required probabilities are lowrr than those required in JARUS AMC RPAS.1309 Issue 2 Table 3 which allocate a probability of 1.0E-06 for CAT failure conditions associated with class I complexity level and 1.0E-07 for CAT failure conditions associated with class I complexity level where the complexity levels are mainly linked with the number of CAT failure conditions and not with the SAIL level. These figures are one order of magnitude higher than those required in table 1. In addition, acknowledging that SORA 2.5 has not yet been adopted by EASA, it has been noticed that the target level of safety seems diffeent as the one considered here. JARUS SORA 2.5 main body published by JARUS provides the following target level of safety: • For ground risk - less than one fatality per million hours (1E-6 fatalities per hour)

- For air risk - less than one mid-air collision per 10 million flight hours (1E-7 mid-air collisions per flight hour) for operations that primarily occur under self-separation and see-and-avoid (primarily uncontrolled airspace). For operations that occur with separation provided by an Air Navigation Service Provider (primarily controlled airspace), the TLOS is one mid-air collision per billion flight hours (1E-9 mid-air collisions per flight hour).

In line with previous comments, could it be possible to have the rational on how the required quantitative objectives in table 1 are obtained from the general Target Level of Safety?

response

Noted

See explanatory note on the rationale for the safety objectives
In the absence of MoC the SORA 2.0 contained in Regulation 2019/947 referred to JARUS AMC RPAS.1309 for the definition of safety objectives, the SORA 2.5 of Reg 2019/947 will remove this reference. JARUS AMC RPAS.1309 is based on different operational assumptions (certified category, population density) which makes a direct comparison difficult.

comment

107 comment by: *ANZEN*

Question, might it be worth to allocate as well an overall safety objective for the UAS (cumulative probability of all CAT FCs) which could somehow alleviate the individually allocated probability for CAT FC? There should be no issue in case a few CAT FCs do not comply with the requested figures in table 1 provided the overall target level of safety for the UAS is achieved.

response

Noted

Aircraft level safety objective such as 10^-6 /FH for the sum of all CAT FCs is not considered a practical solution for several reasons: 1) Whether compliance has been demonstrated, will only be possible, once all systems have been collectively analysed at the end of a project, 2) Continued Airworthiness processes for certified products (determination of unsafe condition and definition of rectification intervals) is based on a "per failure condition" basis 3) Predicting at an early stage the number of CAT FCs is not an easy task and changes in the course of the program may have a cascading effect on many systems.

comment

108 comment by: *ANZEN*

In terms of Development Assurance it is not understood why the required FDAL for a specific category high risk UAS is higher than the one requested for a VTOL basic category able to transport 1 passenger. Is there any difference in the risk or the target level of safety between VTOL and UAS? What it is clear in the case of a VTOL basic category trasnporting 1 person is that a crash will result in a fatality, and a FDAL C is requested, however in the case of table 1 a FDAL B is requested for a hazard with the same outcomes (fatality)

response

Noted

	VTOL safety objectives are derived, in order to address primarily the risk for people in the aircraft. UAS safety objectives are related to the risk for third parties (uninvolved). Third parties, not involved in UAS operation are expecting a higher level of safety, compared to a passenger of a VTOL/GA aircraft. Comparison with other manned aviation categories is therefore difficult, in addition operational environment and operational rules may vary significantly, which may have an influence on the risk for people on the ground. In addition for VTOL category Basic 1, DAL C is allowed with the limitation, that no further DAL reduction is allowed (using ARP5754A or ARP4761A/ED135 principles of system architecture independence). However this is allowed for SAIL V/VI (see note 4 related to Table 1 in MoC 2510 High Risk).

8. Safety Objectives p. 8

comment	*12* comment by: *JEDA* The sentence : "A logical and acceptable inverse relationship must exist between the average probability per flight hour and the severity of failure condition effects." is not entirely clear. Which average probability per flight hour is meant here? The average probability of failure condition per flight hour? Could you clarify this sentence? We suggest: "A logical and acceptable inverse relationship must exist between the average probability per flight hour of failure condition and severity of failure condition effects."
response	Not accepted This is a standard sentence reflecting a standard approach in safety assessment. Please refer to e.g. AMC CS 25.1309 Appendix 3 - Calculation of the average probability per flight hour

9.1 Identification and classification of failure conditions p. 9

comment	*9* comment by: *S.PIZZIOL* Proposition for an explanatory note in this sentence: 'Therefore, failure conditions leading to the loss of the UA inside the operational volume, should be expected [note] to result in one or more fatalities, unless mitigations apply.' Note: Even if in principle for SAIL V fatalities are 'estimated' to happen 'in mean' only every 10 LOC events, for the application of this MOC consider that every single LOC inside the operational volume is 'expected' to result into fatalities for both SAIL V and SAIL VI. In other words, it is deemed not acceptable to label as HAZARDOUS an event that is fatal to one of more people 10% of the time.
response	Partially accepted

	See explanatory note.

comment	*15* comment by: *JEDA*
	"For the definition of the UAS and system level functions, the CONOPS, UAS operational modes, the level of automation, contingency procedures or emergency procedures should be considered, in order to ensure a complete and correct identification of UAS and system level functions." For completeness we suggest to add the external systems supporting the operation description. Therefore modifying the sentence to: "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."
response	Accepted Text will be amended, as proposed.

comment	*18* comment by: *DE-LBA*
	Page 10, 2nd paragraph: "For the definition of the UAS and system level functions, the **CONOPS**, [...] should be considered" The use of the term CONOPS might refer to what is known today as the *Operations Manual* created by an operator. Do you mean the *operating limits* provided by the manufacturer in this context?
response	Noted All functions performed by the UAS shall be identified. These functions may vary significantly from one product to another, depending on the mission objectives and the operational environment of the UAS. These should be taken into account when defining the functions.

comment	*26* comment by: *AESA*
	Referenced text: [End of 1st paragraph]. Environmental and operational aggravating factors need to be considered when relevant (e.g. temperature, icing, night time, turbulence, etc.). **Comment:** Please, mention a possible connection with OSO#24.
response	Not accepted This sentence does not relate to the environmental qualification of an equipment. Instead, when an analysis of the UAS functions and functional failures is conducted, environmental or operational factors which could lead to a more severe effect of the failure condition, should be considered. E.g. cross winds at design limit

comment	*27* comment by: *AESA*

Referenced text: 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.

Comment: We believe the probabilties assigned to FDAL should be closer to the probability of LoC defined in SORA 2.5, which is 10^-SAIL. Since the system failure happens before the LoC and is still evitable, this probability should be higher, in order to be able to reduce it with mitigations to achieve the target probability of LoC event. Is recoverabilty not possible at this point of the operation? Are we assuming a fatility as a consequence of the failure of these systems? Which reference has been used to assign these probabilities of failure?

response

Noted

See explanatory note, on how the safety objectives have been derived.

comment

47 comment by: *Michel Allouche*

(1) The statement "Failure conditions leading to the loss of the UA inside the operational volume, should be expected to result in one or more fatalities" is tantamount to state that the kill probability is equal to 1. According to SORA approach (as more clearly stated in SORA 2.5, whereby the LOC probability is equal to 10-SAIL/FH), this statement is only true in SAIL VI operations. In SAIL V, the probability of kill should be 10-1/FH (see also our comment under 8.1). Therefore, such a statement should only apply to SAIL VI operations.
(2) As per above comment, whilst the inadvertent activation of the FTS within the operation volume is equivalent to the Loss of Control, that *potentially* lead to a Catastrophic effect, its acceptable probability should be different whether we are in SAIL V or SAIL VI operations. Refer our comments raised under 8.1.

response

Noted

(1) The definition for Catastrophic FCs is: Failure conditions that are expected to result in one or more fatalities. When it can be "reasonably expected that one or more fatalities will not occur", an FC can be classified Hazardous. Having a probability of 1/10 to kill a person on ground after the loss of control is not considered low enough to classify it Hazardous. Therefore a simplification is made, which assumes that all LOC are leading to fatalities. If this assumption should not be valid and a lower risk for people can be demonstrated, than this FC could be classified HAZ (This is also described in the next sentence in the MOC)
(2) comment unclear, the safety objectives are different for a SAIL V and SAIL VI CAT FC

comment

87 comment by: *UAV DACH AC*

CONCEPTUAL MAJOR - page 10, para 5, 2nd sentence "demonstrate that no probable single failure": Clearly define "no probable single failure" or provide a suitable

	reference. Is it once in the UAVs design life? The design life can vary significantly. Is there a minimum value?
response	Noted The term 'probable' needs to be understood in its qualitative interpretation, i.e. 'Anticipated to occur one or more times during the entire system/operational life of an item.

comment	*88* comment by: *UAV DACH AC* EDITORIAL - page 10, headers "Relationship with Light-UAS.2511" and ".. 2512" - add references to SC Light-UAS in list of referenced documents in section 3.
response	Not accepted No need for reference. By definition this MOC relates to SC Light UAS, which is also clearly stated in §2 Applicability

comment	*89* comment by: *UAV DACH AC* CONCEPTUAL MAJOR - page 10, para 6, 2nd sentence "volume should be considered catastrophic": whilst a final GRC of 6 (7) is always associated with SAIL V (VI), a residual ARC-d will always result in SAIL VIregardless of the ground risk. As an example an operation over controlled ground when conducted in ARC-d will be SAIL V - invoking the use of this MoC - despite the fact that the inadvertant activation of the FTS would pose no risk to persons on the ground at all. With that in mind it is not correct to conclude as a fact that an inadvertant activation of the FTS that then leads to a crash inside the OV should be considered as catastrophic, when this is not the case for a SAIL IV operation in ARC-c, because the ground victim fatality risk depends on the fGRC and not the ARC. In other words: from a ground risk perspective SAIL IV and VI are the same for fGRC of less than 2 to 5, where the SAIL heavily depends in ARC-c or ARC-d conditions. The statement is incorrect and should be removed or clarified.
response	Partially accepted The paragraph already indicates, that failure conditions might be classified as hazardous, if it can be demonstrated that the failure condition effect is not expected to lead to a fatality. An example will be added, to clarify that SAIL driven by the air risk may have different FC severities for FCs leading to crash on the ground.

comment	*90* comment by: *UAV DACH AC* CONCEPTUAL - Relationship with Light-UAS.2512:in MoC 2510-01 Medium Risk it is stated that mitigations cannot be taken into account in the safety assessment if they have been used to reduce the final GRC. In this context, this could have been done

	to reduce the GRC down to 6 (to achieve SAIL V) or down to 7 (to acheive SAIL VI). Why is this OK here, or is it not?
response	Noted In SAIL IV, the failure conditions are related to the "loss of control of the operation". An M2 does not prevent the UA from a crash, but it improves the survivability of people on ground after a loss of control event. In this MoC for SAIL V and VI, the failure conditions are related to major, hazardous or catastrophic effects. A loss of control event can have two outcomes - expected to eading to a fatality (CAT) or not expected (HAZ) As stated in §9.1 a loss of control in SAIL V and VI should be conservatively classified CAT. However, if an M2 or other technical means to lower the ground risk have been implemented, the severity could be lowered to HAZ under certain conditions/limitations.

8.2 Single failure and common cause considerations p. 9

comment	*45* comment by: *Michel Allouche* (1) Requested clarification: In this context single failures addressed here only relate to Hardware failure. (2) It is proposed to add, as an example of "single failure not a practical possibility": (a) Some structural or mechanical failures may be excluded from the no-single failure criterion if it can be shown that these mechanical parts were designed to a standard considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority (see comment under current OSO#10 in AMC to (EU) 2019/947; for some reasons it has been omitted in SORA 2.5 updated OSO#5) (b) Low Risk time leading to a probability of occurrence less than 10-6/FH
response	Noted 1) single failure is a failure of any part, component or element of a system. It is related to physical hardware 2) a)It is not the point of this paragraph to exclude structural failures. They are not in the scope of .2510, as stated in §2 (a) . If there are system specific safety objectives, they take precedence over .2510. b) it is not the intent to allow single failures, based on a short exposure time.

comment	*85* comment by: *UAV DACH AC* EDITORIAL - Para 2, 2nd sentence: Definition of "common mode" should be included in Section 5. For CLARIFICATION: A design error (error in the requirements) that affects the software of multiple redundant, functional similar systems is a common-cause error that can lead to a single (point) failure. Add an MOC for this case.
response	Noted

ARP4761 defines Common Mode Failure as "An event which affects a number of elements otherwise considered to be independent." It could be also understood as: common cause failures where multiple components fail in the same mode.
As this definition has been removed from ARP4761A and there is no agreed consensus definition, it will not be introduced in the MoC

comment *98* comment by: *S. Sellem-Delmar / Safran*

Comment :
The sentence "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." looks close to similar section from:
-SC VTOL MOC VTOL.2510 Equipment, systems, and installations
(b) Single failure and common cause failure considerations: ... 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 in the frame of the common –cause and cascading failures consideration.
-Newer versions of CS25 (amdt>=24) / AMC 1309 - Single Failure Considerations.
"...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 in the frame of the common-cause and cascading failures consideration. "

For several years, in manned aviation, EASA is bringing emphasis on "architecture aspects to be resilient to design errors." and is pushing applicants to assess their vulnerabilities to design errors in order to contain "avoidance strategies" to design errors. This §8.2 sentence is almost identical from latest version of CS25 and SC VTOL, inducing significant effort from manufacturer. Based on this, it is considered that transition from SAIL IV to SAIL V safety objectives currently seem very steep and not in line with the progressivity of requirements with SAIL increase (excessive step effect compared to GRC scale). We suggest that the transition from SAIL IV to SAIL V focuses mainly on broadening the scope of safety analyses, including operational hazards and less dangerous FC from MAJ and HAZ categories, and common cause analysis, as required by ED135.

Suggested resolution :

Soften requirements increases from SAIL IV to SAIL V, in consistency with risk progressivity (no step effect).
Proposal: **Replace current wording**
"*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 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)."

by wording below:
"**For SAIL V application**
Development assurance should be applied at system and equipment level. For SW/AEH items whose development error could directly result in Catastrophic failure conditions, 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.
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.

Possible common cause failures (including common mode failures) should be considered in the analysis. 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)
- Particular Risk Analysis
- Zonal Safety Analysis

(Wording was derived from §7.1-"Development Assurance" of "Means of Compliance with Light-UAS.2510 Equipment, Systems and Installation" MOC Light-UAS.2510-01, and completed.)

For SAIL VI applications:
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 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)."

response	Not accepted see answer to comment 97. The proposed alleviation for SAIL V is not possible, since the SORA OSO #05 of Regulation 2019/947 states: "SW and AEH whose development error(s) may **cause or contribute to hazardous or catastrophic** failure conditions are developed to an industry standard or a methodology considered adequate by EASA"

9. Safety Assessment Process p. 9

comment	*46* comment by: *Michel Allouche* "Guidance on how to perform the Safety Assessment process can be found in ED-79B and ED-135" : see our comments under Section 3 "References" and use or refer to the proposed added wording ("whereas some of the sections may have to be tailored to UAS applications")
response	Partially accepted see answer to comment 43

comment	*86* comment by: *UAV DACH AC* MAJOR - para 1, 2nd sentence: As it is well-known that the definition of alternative guidance is extremely difficult, the MOC should contain an advice on the minimum required characteristics of such an approach.
response	Not accepted Out of scope of this MoC.

9.2 Depth of analysis p. 11

comment	*16* comment by: *JEDA* We would like to suggest to consider SAIL III or at least SAIL IV verified designs to demonstrate compliance to show that major failure conditions are correctly addressed and to potentially reduce the required DAL for hazardous or catastrophic failure conditions. We suggest adding the following bulletpoint for major failure conditions: "If a system safety assessment according to MOC Light-UAS.2510-01 for Special Condition Light-UAS medium risk 01 has been verified by EASA, major or hazardous failure conditions may be considered addressed."
response	not accepted Acceptance for hazardous failure conditions will not be possible, since it is required to perform a quantitative assessment of the design, which is not required in SAIL III and IV. For Major FCs, the requirements are not the same. SAIL V/IV requires Major to be remote, while there is no qualitative target in SAIL III and IV.

comment	*49* comment by: *Michel Allouche* Add a note at the end of section 9.2: For Minor Failure Conditions, see Note 1 in section 8.1
response	Accepted Information from Note 1 can be repeated here

comment	*91* comment by: *UAV DACH AC* MAJOR- Page 12, last para "ETSO equipment" - it should be noted that ETSO equipment is certified for environmental conditions (incl. temperature, vibration and EME) corresponding to typical installation locations inside a manned aircraft, such as flight deck, (pressurized) cabin or avionics bay, that may not exist or have not the same conditions inside an unmanned aircraft, and it must therefore be ensured that the (E)TSO'd equipment is operated inside its approved and certified envelope. It should be mentioned that DO-160 conditions do not translate well into unmanned aircraft zones or may not be transferable at all. For example an IRS that is ETSO C201 certified in the categories A1H1 may not be able to endure the manufacturer's rated number of operating hours when installed in an unmanned rotorcraft and there is no way of predicting the MTBF without re-testing. It should also allow equipment with military or space certificates when meeting the installation conditions, therefore suggesting to add "or suitably certified"
response	partially accepted The comment is valid and we concur, that the conditions in the standards need to match the conditions of UAS operations. However environmental qualification is out of scope of this MoC. A sentence will be added to clarify that standards from manned aviation may need adaptation.

comment	*100* comment by: *S. Sellem-Delmar / Safran* <u>Comment :</u> "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." This sentence is clear, however it does not seem to belong to section 9 and maybe it is not belonging to the MOC either. <u>Suggested resolution :</u> Suggest to confirm pertinence to keep sentence starting with "Compliance for qualification of systems or equipment" in section 9.2.
response	Noted

Paragpraph is considered adequate.

9.3 Development Assurance p. 12

comment	*28* comment by: *AESA* **Referenced text:** 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. **Comment:** Please, clarify if this is FDAL or DAL, as the DAL of the function is mentioned.
response	Partially accepted Systems that may contain simple items (i.e. items that can be fully assured by combination of testing and analysis) can be considered to meet the DAL (IDAL for the item and FDAL for the system), considering that the requirements have been validated with the corresponding rigor. Sentence will be clarified.

comment	*29* comment by: *AESA* **Referenced text:** 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. **Comment:** Please, clarify if this is FDAL or DAL
response	Noted FDAL is allocated to systems/equipment, IDAL is allocated to items

comment	*30* comment by: *AESA* **Referenced text:** The level of development assurance should be commensurate with the severity of the failure conditions the system is contributing to. **Comment:** Please, clarify if this is FDAL or DAL. Which reference is recommended to commesurate and assign this DAL?
response	Noted This is a generic sentence to explain the concept. The required DAL should be the one identified in Table 1 page 8. This principle applies to FDAL and IDAL equally. In terms of process, the FDAL assignment is the starting point.

comment	*101* comment by: *S. Sellem-Delmar / Safran* Comment : The beginning of the first paragraph is evoking simple systems, the end of the same paragraph is evoking simple items, this is not consistent. Suggested resolution : Suggest to replace: "Such items may be considered" by "Such systems may be considered"; and "However, requirements for those items" by "However, requirements for those systems".
response	Accepted Sentence will be clarified.

comment	*102* comment by: *S. Sellem-Delmar / Safran* Comment : "However, requirements for these items should be validated with the rigor corresponding to the DAL of the function." Considering that use of 'items' is erroneous and that the sentence was intended to read "However, requirements for these systems should be validated with the rigor corresponding to the DAL of the function." Then the issue raised by this sentence is that it does imply that Development Assurance is applied on requirements allocated to the simple system, which in general would not be the case (because only requirements allocated to complex systems would be submitted to Development Assurance). Suggested resolution : Remove sentence "However, requirements for these items should be validated with the rigor corresponding to the DAL of the function".
response	not accepted

First requirements are allocated to functions (FDAL) and then are flown down to system, equipment and items (IDAL), Requirements need to be allocated to any system, simple or complex. Development Assurance processes will need to be applied to the whole UAS.

9.3.1 Development Assurance Level (DAL) assignment p. 12

comment	*31* comment by: *AESA* **Referenced text:** For functional failure sets with multiple members, no FDAL/IDAL lower than FDAL/IDAL D should be allocated to any member. **Comment:** Please, clarify if member is a synonym of systems in this context
response	Noted A member should be understood as a UAS-level or system function or item, that may contain a development error (see also ED-135)

comment	*32* comment by: *AESA* **Referenced text:** In the absence of agreed guidelines on FDAL/IDAL assignment, the FDAL should be assigned as per Table 1 in this MOC and the IDAL of all components contributing to a given function should be equal to the FDAL of that function. **Comment:** It is not clear the reason to separate between FDAL and IDAL since at the end of the assessment the IDAL is neglected and considered equal to DAL/FDAL. Some clarification is needed. MoC Light-UAS 2510 does only take into account DAL. Not FDAL nor IDAL.
response	Noted FDAL is assigned to systems and equipment and IDAL is assigned to Items. They follow different standards. (ED-79B for systems/equipment DA and ED-12, ED-80 for item DA). Please consult with ED-79B and ED-135 for further information. ED-135 provides possibilities to assign DAL taking into account architectural aspects. The sentence you highlight, tries to clarify that table 1 DAL allocation should be used, when there is no further agreement on a different methodology with the agency. Sentence will be changed to clarify.

comment	*52* comment by: *Michel Allouche* Same comment as in section 8.1. Add after Appendix P: **(as duly tailored to take into considerations that a lower FDAL is assigned to Catastrophic Effect in the context of this MoC)**
response	Accepted information will be added

comment	*92* comment by: *UAV DACH AC* CONCEPTUAL MAJOR - para 3, "with the exception, that no FDAL D should be allocated": This comes without justification or rationale, and is in contradiction with the IDAL allocation practices set forth in ED-79B. Recommending to remove this "exception".

response	Noted Since the assurance that can be put into a DAL D, that errors in development have been minimized is relatively low, it is not considered adequate to assign a DAL D to a functional failure set member contributing to a catastrophic FC. The approach is the same as introduced to CS 27.1309 Amd 10

comment	*93* comment by: *UAV DACH AC* CONCEPTUAL MAJOR - page 13, para 2 "In the absence of agreed guidelines on FDAL/IDAL assignment": this could be misinterpreted as why is ED-79B / SAE ARP 4754B not agreeable, when in section 9.3.2 it is referenced and regarded as "acceptable guideline". Suggesting to remove or rephrase to "When not applying an agreed guideline on FDAL/IDAL assignment, such as ED-79B/ SAE ARP 4754B, then"
response	Partially accepted wording will be changed to clarify.

9.3.5 Open Problem Report management p. 13

comment	*33* comment by: *AESA* **Referenced text:** Any problem 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 (OPRs). **Comment:** Typo: "Any problem identified during the development **is** addressed" instead of "are addressed"
response	Accepted wording will be changed

9.3.2 UAS/System development assurance p. 13

comment	*53* comment by: *Michel Allouche* Regarding the use of ED-79B, refer to and consider our comment under Section 3 "References"
response	Noted see answer to comment 43

comment	*103* comment by: *S. Sellem-Delmar / Safran* Comment : "The extent of application of ED-79B to substantiate functional development assurance activities may vary depending […]" The word 'functional' seems to be extraneous. Suggested resolution : Remove 'functional' from sentence "The extent of application of ED-79B to substantiate functional development assurance activities may vary depending […]"
response	partially accepted Will be replaced by" system and equipment development assurance"

9.3.4 Airborne Electronic Hardware development assurance p. 13

comment	*61* comment by: *Michel Allouche* Regarding the use of AMC 20-152, refer to and consider our comment & proposed wording under Section 3 "References"
response	Noted see answer to comment 43

9.3.6 Considerations for highly integrated systems p. 13

comment	*62* comment by: *Michel Allouche* Regarding the use of AMC 20-170, refer to and consider our comment & proposed wording under Section 3 "References"
response	Noted see answer to comment 43

comment	*104* comment by: *S. Sellem-Delmar / Safran* Comment : "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." Reference to AMC 20-170 is misleading as AMC 20-170 is applicable to Integrated Modular Avionics and not to integration of multiple functions in the same system or equipment, the latter case being standard practice (with or without partitioning). Suggested resolution : Suggest to remove mention of AMC 20-170 : "When incorporating multiple functions into the same system or equipment, particular care should be taken in the analysis of interactions between functions for achitectures with no partitioning."
response	Not accepted wording is deemed sufficient to provide flexibility to the applicant to determine whether AMC 20-170 is or is not applicable. This paragraph does not prescribe the systematic application of AMC 20-170.

9.3.3 Software development assurance p. 13

comment	*110* comment by: *Michel Allouche* Regarding the use of AMC 20-115, refer to and consider our comment under Section 3 "References"
response	Noted see answer to comment 43

10.2 Remote Crew and Maintenance considerations p. 14

comment	*10* comment by: *THALES*

	MTBF to detect latent failure : it is authorized by AMC 25.1309 : proposal to remove the sentence for CAT events or that dormant failure shall not be above 10-3 /FH
response	Not accepted The MTBF could be used as the basis for defining a check interval time, where the equipment has to be replaced or repaired, in order to detect latent failures. It is not related with 25.1309 (5) (iii). There is not an equivalent requirement in SC Light UAS.

comment	*34* comment by: *AESA* **Referenced text:** 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. **Comment:** Please, mention a possible connection with OSO#18.
response	Noted OSO 18 "Automatic protection of the flight envelope from human errors", is not considered related to the referenced text.

comment	*35* comment by: *AESA* **Referenced text:** (2) Maintenance Actions **Comment:** Please, mention a possible connection with OSOs #03 and #07.
response	Noted OSO 3 and 7 are not in the scope of SC Light UAS.

10.1 Latent failure considerations p. 14

comment	*54* comment by: *Michel Allouche* Please clarify this is a purely recommended design aim but not a firm requirement. Indeed, this is implied in Section 10.2 (b) that does not exclude such a possibility, provided an adequate maintenance action is defined to detect possible latent failure.
response	Noted It is not a requirement, as this is Means of Compliance; but it is recommended.

comment	*94* comment by: *UAV DACH AC*

	para 1, 1st sentence: EDITORIAL - this does not belong here; move to 10.2 (2) CONCEPTUAL - what kind of periodic (scheduled) maintenance can detect the failure when it occurs? Maintenance can detect that a failure ... 1. is not going to happen (because it cannot be detected at the moment), 2. is going to happen soon (shows indications to manifest itself) and may require preventive actions (replacement, repair, other actions) or 3. has already happened (in this case preventive maintenance has failed).
response	Partially accepted The wording will be changed.

11. Compliance with Light-UAS.2510(b) p. 15

comment	*36* comment by: *AESA* **Referenced text:** The equipment and systems which are not covered by Light-UAS.2500 are typically those, whose failure or **Comment:** Remove the comma
response	Accepted Will be removed

comment	*95* comment by: *UAV DACH AC* EDITORIAL - Ultimate sentence "In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation" - The sentence is difficult to understand. Suggestion: "For example, the Design and Installation Appraisal shows that physical and functional isolation is assured from all components, which are essential to safe operation; assurance can be achieved by applying common design practices."
response	Noted Wording is deemed sufficiently clear.

3. Appendix A
Attachments

	MAJ	HAZ	CAT
SAIL III	-	FDAL D *(Loss of Control of operation)*	
	-	-	
SAIL IV	-	-	FDAL C *(Loss of Control of operation)* *(No Single Failure)*
	-	-	10^{-5}
SAIL V	FDAL D	FDAL C	FDAL C *(No Single Failure)*
	10^{-3}	10^{-5}	10^{-6}
SAIL VI	FDAL C	FDAL C	FDAL B *(No Single Failure)*
	10^{-4}	10^{-6}	10^{-8}

Table Safety objectives proposed.JPG
Attachment #1 to comment #97

4. Explanatory Note

The relationship between the TLOS, LOC and Safety Objectives

The Target Level of Safety (TLOS) for ground risk is defined in SORA 2.5 as less than one fatality per million hours 10^{-6} fatalities/FH. This is independent from the SAIL. In order to meet this TLOS, an allowable rate of loss of control of the operation per flight hour (LOC) is established, which depends on the SAIL. The definition for LOC is contained in MOC 2510. For SAIL V the LOC is defined in SORA 2.5 Annex F as 10^{-5} /FH and for SAIL VI the LOC is 10^{-6} /FH. It should be noted, that the LOC is taking into account the UAS technical and operational failures. Since in SAIL VI the LOC rate equals the TLOS, implying that every LOC event is expected to result in one or more ground fatalities. In SAIL V there is a conditional probability of 10^{-1}, that the loss of control will not lead to a fatality. This has been reflected in the MOC in § 9.1, by allowing to classify certain failure conditions as hazardous, if it can be demonstrated that these failure conditions will not lead to a fatality. In all other cases, a LOC in the operational volume shall be assigned a catastrophic severity, considering that a residual probability of 0.1 is not sufficient to assume that a "fatality is not expected" (from the definition of hazardous failure conditions).

The establishment of safety objectives

For the establishment of safety objectives, it has been assumed that 10% of the LOC events are due to technical failures. It is acknowledged that UAS may have a higher contribution of system failures to the overall LOC rate, due to the higher level of automation and less authority of the remote crew. However there is currently no data available to substantiate a different proportion and as a conservative approach it is proposed to limit system failures to 10%. This view is also shared by JARUS AMC RPAS.1309 and SORA 2.5 OSO #05.

The number of potentially catastrophic failure conditions is set to 10, which is following the traditional assumption used for general aviation aircraft. Considering that complex and highly integrated UAS may have more than 10 catastrophic failure conditions, this approach is more permissive than what is proposed by JARUS AMC RPAS (for a complexity level 2, which is expected to be the majority of UAS applications in SAIL V/VI). As it can be assumed that the number of catastrophic failure conditions and the percentage of system failures contributing to LOC is correlated, the resulting safety objectives are considered adequate. These numbers will be reviewed, when there is more in service experience and accident data available.

The following table summarizes the establishment of quantitative safety objectives.

	SAIL V	SAIL VI
TLOS (fatalities/FH)	10^{-6}	10^{-6}
LOC (/FH)	10^{-5}	10^{-6}
% due to technical failures	10%	10%
LOC due to technical failures (/FH)	10^{-6}	10^{-7}
Number of potentially catastrophic failure conditions	10	10
Probability of each catastrophic failure condition (/FH)	10^{-7}	10^{-8}

Table 1: Derived quantitative safety objectives

The Development Assurance Level (DAL) assignment follows the same approach as for other products which introduce a graduated scale of safety objectives, like CS 23, CS 27 Amdt 10 or SC VTOL. This is deemed consistent and proportional, considering as well the fact that UAS are expected to feature more complex and highly integrated systems and equipment. An additional level of proportionality has been introduced for FDAL contributing to major failure conditions, where an FDAL D has been introduced, acknowledging the JARUS WG6 – Eurocae WG 73 Conciliation Team Report [1]

Comparison with manned aviation

A comparison between safety objectives used in manned aviation and UAS is difficult because the risks that the two categories of aircraft are addressing are different. In manned aviation the safety objectives are established primarily to protect the occupants on board of the aircraft. Whereas UAS safety objectives need to consider the risk for people on the ground (and in other aircraft). The risk for people on the ground posed by a CS 23 aircraft may be much different compared to the risk posed by a SAIL V and VI UAS. The JARUS scoping paper to AMC RPAS.1309 compares the accident rates of different manned aviation aircraft categories and concludes that the risk of ground fatalities is two orders of magnitude lower than the number of fatal accidents. Whereas the assumption for SAIL V and VI is, that a LOC is expected to lead to a fatality on the ground with probability 10^{-1} or 1.

Comparison with JARUS AMC RPAS.1309 objectives

The assumptions used by JARUS AMC RPAS.1309 are different compared to the SORA approach. The basic objective from JARUM AMC RPAS.1309 is to achieve a similar accident rate compared to equivalent manned aviation category aircraft: *"This leads to the conclusion that it is not necessary to define a specific airworthiness risk to people and property on the ground from a RPA as the current manned aircraft accident based statistics remain valid, and ground based risk should not be a function of whether an aircraft is manned or unmanned."*

"Maintaining the same accident rate/category [as manned aviation] *will therefore ensure that one of the defining principles of taking a cautious and defendable approach is met."*

To conclude, the JARUS RPAS 1309 approach defines safety objectives based on the observed accident rate of equivalent manned products and concludes that this is sufficiently protecting people on the ground

On the other hand SORA Annex F starting point is the definition of an acceptable fatality rate, which is set to be at 10^{-6} /FH. This results in a lower allowable LOC rate for UAS, compared to accepted accident rate in manned aviation.

[1] JARUS WG6 – EUROCAE WG73 "1309" CONCILIATION TEAM REPORT – NOVEMBER 2015 §5.7

The JARUS Scoping paper explains the higher acceptable accident rate used in JARUS AMC RPAS.1309:
"To counter this trend and prevent an overall increase in the accident rate (all categories), a minimum target level of safety of 1x10-4/fh (all causes) is established commensurate with the lowest safety target applied to manned aircraft. Those RPAS that have no direct equivalence with manned aircraft due to their lower weights will therefore need to meet this minimum target level of safety."
SORA Annex F clearly defines the allowable LOC rate (i.e. accident rate) to be 10^{-6} /FH (for SAIL VI) and 10^{-5} /FH (for SAIL V), which is clearly different from what is prescribed in JARUS AMC RPAS.1309 objectives for the lowest end UAS (CS LUAS).