 European Union Aviation Safety Agency	<b>SC Consultation paper</b>  <b>Special Condition</b>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	--	--

**SUBJECT** : **AWO – CAT II in CS-23**  
**REQUIREMENTS incl. Amdt.** : **CS-23.773, 23.1301, 23.1309, 23.1322, 23.1329, 23.1585 amdt 3.**  
**ASSOCIATED IM/MoC<sup>1</sup>** : Yes ☒ / No ☐  
**ADVISORY MATERIAL** : **Flight Test Guide FAA AC 25-7D, AC 120-29A CAT I & II**

#### INTRODUCTORY NOTE:

The following Special Condition (SC) has been classified as important and as such shall be subject to public consultation in accordance with EASA Management Board decision 12/2007 dated 11 September 2007, Article 3 (2.) which states:

*"2. Deviations from the applicable airworthiness codes, environmental protection certification specifications and/or acceptable means of compliance with Part 21, as well as important special conditions and equivalent safety findings, shall be submitted to the panel of experts and be subject to a public consultation of at least 3 weeks, except if they have been previously agreed and published in the Official Publication of the Agency. The final decision shall be published in the Official Publication of the Agency."*

#### IDENTIFICATION OF ISSUE:

CAT II approach minima are commonly used by commercial and business aviation aircraft around the world that would typically hold a CS-25 aircraft Type Certificate (TC). The CS-AWO refers directly to CS-25. Therefore, the CS-AWO does not repeat certain requirements already covered by CS-25 and provides only the additional requirements deemed necessary to perform approaches down to 100ft Height above touchdown elevation (HAT).

At Low Visibility Operation (LVO) on an airport the capacity is drastically reduced to accommodate larger separations between aircraft. This in turn creates a high demand on ATC to provide a strictly organized traffic flow. In LVO, any flow perturbation has a strong impact on the airport capacity. As of today, only aircraft compliant to more stringent airworthiness requirements of CS-25 are participating to LVO. This means the flight deck compartment view under low visibility weather conditions must be adequate.


The purpose of this Special Condition is to provide the additional and adapted requirements deemed necessary for a safe CAT II operation with CS-23 aircraft when complying with CS-AWO Subpart 2 (CAT II).

The following topics are verified for certification basis adequacy and completeness:

1. Autopilot/Flight Director Architecture, Reliability and Performance  
(Fail safe, Failure modes, Flight path error, MUH).

---

<sup>1</sup> In case of SC, the associated Interpretative Material and/or Means of Compliance may be published for awareness only and they are not subject to public consultation.

 European Union Aviation Safety Agency	<p align="center"><b>SC Consultation paper</b></p> <p align="center"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

2. Auto Thrust Architecture, Reliability and Performance
3. Radar Altimeter Architecture, Reliability and Presentation
4. Indications and Alerting (Loc 1/3 dot deviation, Cautions, Warnings, Flags)
5. External View (Rain, Snow, and freezing fog Removal)
6. Human Factors (Min Flight Crew, Standard Operating Procedure, Flight deck adequacy)

#### **Certification Basis Comparison CS-23 vs. CS-25 and CS-AWO**

CS AWO Subpart 2 contains relevant requirements and the corresponding acceptable means of compliance to demonstrate that an aircraft can safely fly an ILS/MLS precision approach with published minima below 200ft down to 100ft above Touch Down Zone Elevation (TDZE) (or HAT). These requirements are additional to the CS-25 certification basis.

It is the EASA position that for a CS-23 aircraft the applicant may choose to use the equivalent CS-23 requirement providing it exists and is equivalent in nature to the CS-25 requirement within the scope of the related project.

Where CS-23 (at pre- amendment 5 issue) is missing or not adequate to support CAT II when compared to a CS-25 requirement, a special condition (SC) is added based on CS-25.

For the gap analysis of this identification of issue EASA CS-23 is considered at amdt. 3 and CS-25 is considered at amdt. 24;

CS-AWO for CAT II requirements has been written for CS-25 aircraft. These aircraft already intrinsically fulfil these CS-25 requirements, what CS-23 aircraft do not. The objective of the table below is to identify CS-25 paragraphs that serve as a basis on which the CS-AWO requirements are build. In making a gap analysis with these specific CS-25 paragraphs, as identified in the right column of the table, EASA identified requirements that serve as a discussion basis to determine a new set of Part-23 Special Conditions for CAT II operations in addition to the compliance to the CS-AWO and its AMC.

<b>CS-AWO for CAT II</b>	<b>related CS-25 or CS-AWO</b>
<b>None</b>	<b>CS-25.773(a)(b)(d)</b> Pilot compartment view
<b>None</b>	<b>CS-25.1585</b> AFM Operational Procedure
<b>CS AWO.201</b> Safety Level	<b>CS-25.1309</b> Equipment, systems, Install.
<b>CS AWO.202</b> Go around Rate	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.204</b> Control Flight Path	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.206</b> Control of Speed	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.207</b> Manual Control	<b>CS-25.1302</b> Sys used by Flight Crew
<b>CS AWO.208</b> Oscillations and Deviations	<b>CS-25.1302</b> Sys used by Flight Crew
<b>CS AWO.215</b> Decision height Recognition	<b>CS-25.1301</b> Function and Installation
<b>CS AWO.216</b> Go Around	<b>CS-25.1302</b> Sys used by Flight Crew


<b>CS AWO.221</b> Installed Equipment	<b>CS-25.1301</b> Function and Installation <b>CS-25.1329</b> Flight Guidance Systems <b>CS-25.1322</b> Flight Crew Alerting
<b>CS AWO.222</b> Min Equipment	<b>CS-25.1583</b> Operating Limitations
<b>CS AWO.231</b> Flight path & speed control	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.233</b> Decision Height	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.236</b> Excessive deviation alert	<b>CS-25.1322</b> Flight Crew Alerting
<b>CS AWO.243</b> Go Around Performance	<b>CS-25.1587</b> AFM Performance Information
<b>CS AWO.251</b> Mode selection	<b>CS-25.1322</b> Flight Crew Alerting <b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.252</b> Presentation of information	<b>CS-25.1302</b> Sys used by Flight Crew <b>CS-25.1322</b> Flight Crew Alerting
<b>CS AWO.253</b> Audible warning of autopilot disengagement	<b>CS AWO.153</b> Audible AP disengagement <b>CS-25.1309</b> Equipment, System, Install
<b>CS AWO.262</b> Automatic Pilot	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.263</b> Flight Director Systems	<b>CS-25.1329</b> Flight Guidance Systems
<b>CS AWO.268</b> Radio Altimeter	<b>CS-25.1309</b> Equipment, System, Install
<b>CS AWO.269</b> Excess-deviation alerts	<b>CS-25.1309</b> Equipment, System, Install
<b>CS AWO.281</b> AFM	<b>CS-25.1581</b> AFM GEN
<b>CS AWO.303</b> Minimum Flight Crew	<b>CS-25.1523 &amp; Appendix D</b> Min Flight Crew
<b>CS AWO.352</b> Indications & Warnings	<b>CS AWO.361</b> Failure general CAT III <b>CS AWO.161</b> Failure general CAT I <b>CS AWO.172</b> ILS/MLS Gnd facility failure <b>CS AWO.268</b> Radio Altimeter reliability <b>CS AWO.269</b> Excess-dev alerts reliability <b>CS-25.1309</b> Equipment, System, Install <b>CS-25.1322</b> Flight Crew Alerting

### **Significant differences requiring supplementing requirements to CS-23:**

EASA wants to highlight that the following discussions and determinations of supplemental requirements to CS-23 for CAT II operation with CS-23 aircraft are obviously additional to the direct compliance demonstration to CS-AWO and its AMC.

#### **1. CS-25.773 Pilot compartment with non openable windows discussion**

In CAT II at DH of 100 ft, the aircraft is about 580 m from the aiming point markings center. Instrumented runways for CAT II operation have normally the threshold at 400 m from the center of the aiming point center. This means that the aircraft is at about 180 m from the runway threshold at this moment with a RVR that can be as low as 300m. With the downward view masked by the aircrafts nose, being nearly on the runway, the approach lights are mostly not anymore visible. This makes CAT II decision making and visual segment hand flying more difficult compared to CAT I due to lesser visual cues and time to pilots

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

reaction. The lateral elements patterns recognition, THD lights or Touch Down (TD) zone lights, are essential for a safe attitude control in the visual segment.

EU 965/2012 CAT.P.MPA 305(e) states that the visual references for a CAT II continuation to land:

(c) CAT II or OTS CAT II operations

At DH, the visual references specified below should be distinctly visible and identifiable to the pilot:

- (1) a segment of at least three consecutive lights being the centreline of the approach lights, or touchdown zone lights, or runway centreline lights, or runway edge lights, or a combination of them;
- (2) this visual reference should include a lateral element of the ground pattern, such as an approach light crossbar or the landing threshold or a barrette of the touchdown zone light unless the operation is conducted utilising an approved HUDLS to touchdown.

CS-25 is significantly different and is not fully covered by the CS-23 equivalent. The organization of the rain removal, de/anti-icing and de/anti-fogging requirements and guidance are also slightly different between xx.773 and xx.775.

Anti/De-Fogging System and Reliability discussion:

CS-25.773(c) de-fogging function is mainly covered by CS-23.773(b). In CS-23, the reliability of the windshield internal de-fogging can make use of the “[..] unless fogging can be easily cleared by the pilot without interruption of normal pilot duties”. This credit is not anymore acceptable for CAT II operation.

Rain removal System discussion (Heavy rain and Rain removal system necessity):


CS-23-773(a)(3)(i) states “design so that each pilot is protected [..] so that **moderate rain** conditions do not unduly impair the pilot’s view of the flight path [..] while landing”.

CS-25-773(b)(1) states “The aeroplane must have a means to maintain a clear portion of the windshield during precipitation conditions. Sufficient for both pilots to have a sufficiently extensive view along the flight path in normal flight attitudes of the aeroplane. This means must be designed to function, without continuous attention on the part of the crew, in [..] **heavy rain** at speeds up to 1.5 VSR1, with lift and drag devices retracted [..]”.

AMC-25.773 states “Total loss of external visibility is considered **catastrophic**. A sufficient field of view must exist to allow the pilot to safely operate the aeroplane during all operations, including taxi. This field of view must remain clear in all operating conditions. Precipitation conditions such as outside ice, **heavy rain** must be considered.

AC 120-29A requires an equipment for rain removal where CS AWO does not. CS-25.773(b)(1)(i) requires a means to maintain a clear portion of the windshield during **heavy rain** precipitation condition. CS-23 does not provide a requirement for rain removal and addresses only **moderate rain** instead.

For CAT I operations the horizontal RVR is 550m, whereas in CAT II weather conditions the horizontal RVR can be as low as 300m. This lower visibility is driven by more moisture in the air leading to more demanding performance to provide a clear portion of the windshield. Therefore CS-23.773 is amended accordingly.

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	<p>Doc. No. : SC-O23-div-08</p> <p>Issue : 1</p> <p>Date : 04 May 2021</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p> <p>Deadline for comments: 25 May 2021</p>
--	---	---

Concerning the rain requirements, CAT II operations predominantly take place in persistent meteorological conditions such as fog, mist or any combination of MIFG and or precipitation (DZ, RA-). Usually, rain clears the atmosphere and increases the visibility to above CAT II criteria. Should a microburst or thunderstorm produce rain that reduces the visibility to a CAT II standard, a landing would be very difficult if not impossible due to side effects such as wind-shears, flooded runway. Therefore, this special condition does not increase the requirement to heavy rain conditions and maintains the moderate rain level required in CS-23, however the AFM needs to indicate if flight testing has been done up to moderate rain conditions only.

#### Anti/De-Icing System discussion:

CS-25.773(b)(1)(ii) states the requirements for windshield de-icing system. The de-icing function is deemed sufficiently covered by the CS-23.775(f). It is noted that the appendix O for the icing envelope (supercooled large drop conditions) is excluded from this discussion.

#### De-Icing and Rain removal Reliability discussion:

CS-25.773(b)(2) states “No single failure of the systems used to provide the view required by subparagraph (b)(1) of this paragraph must cause the loss of that view by both pilots in the specified precipitation conditions”.

CS-25.773(b)(4) states “that an openable windows does not need to be provided if it is shown that an area of transparent surface will remain clear sufficient for one pilot to land the aeroplane safely in the event of – (i) Any system failure or combination of failures, which is not, extremely improbable in accordance with CS-25.1309 [..]”.

AMC-25.773 states “Unless system failures leading to loss of a sufficient field of view for safe operation are shown to be **extremely improbable**, the following provides acceptable means to show compliance with CS-25.773(b)(4):

- Each main windshield should be equipped with an independent protection system. The systems should be designed so that no malfunction or failure of one system will adversely affect the other.”

#### Design Eye Reference point discussion:


CS-23 does not require a Design Eye Reference Point (DERP). AC 23.1311-1C states “Part 23 rules do not require the applicant to establish a cockpit design eye reference point from which to measure viewing distances and angular displacement to various cockpit equipment”.

CS-25.773(d) requires such DERP. In CAT II operation, it is essential that the pilot seats so that the visual acquisition of external references and the instruments scanning are optimal or not masked by glareshield or other cockpit frames.

## **2. CS-25.1302 Systems and equipment used by Flight Crew discussion**

There is no such requirement in CS-23 addressing Human Factors performances.

CS AWO.252 (a) Presentation and Information to the crew requires that all indications must be designed to prevent crew errors.

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

CS AWO.252 (b) Presentation and Information to the crew requires that essential information and warnings permit a rapid recognition of malfunctions.

AMC AWO.252 states for installations involving more than one type of precision approach system the following should be taken into account “(iii) The ILS [...] system selected for the approach [...] should be indicated positively in the primary field of view at each pilot station.”. Experience has shown that CS-23 equipment is not optimized to support such information for CAT II operations. They tend to provide only subtle indications with no clear approach mode labelling and with no automatic systems availability control.

A Human Factors special condition is added by SC-O23-div-08.01, if not already existing in the Certification Basis of the aircraft, for a good level of safety into Part 23 cockpit that wishes to operate in CAT II.

### **3. CS-25.1309 Systems, equipment and installations discussion**

CS-25.1309 is significantly different and is not fully covered by the CS-23 equivalent. Consequently, the AMC of CRI F-51 ‘Equipment, systems and installations’ has to be applied.

### **4. CS-25.1322 Flight Crew Alerting discussion**


CS-25.1322 is significantly different and is not fully covered by the CS-23 equivalent. Since amendment 11 the CS-25.1322(c)(2) states for cautions and warnings to provide timely attention-getting cues through at least two different senses by a combination of aural, visual, or tactile indications.

In many existing aircraft designs the warning and/or caution alerts are presented only via one sensory means. While these designs are currently in-service on numerous aircraft, they do not meet the intent of CS-25.1322(c)(2); there is no assurance that visual methods alone can sufficiently attract the pilot’s attention should he or she be focused elsewhere. This is a particular concern during certain phases of flight and situations that place higher demands on the flight crew’s attentional resources, increasing the likelihood of cognitive tunnelling or perceptual blindness (25.1322(a)(2)). The addition of a second sensory channel is intended to mitigate these phenomena and enhance safety

Loss of CAT II capability below 200 feet requires immediate recognition and immediate action. Per 25.1322(b)(1), the loss of CAT II capability under those conditions is appropriately classified as a warning and must comply with 25.1322(c) through (f). In addition, CS AWO.253(a) states “Where the approach flight path is controlled automatically, an audible warning must be given following disengagement of the automatic pilot or loss of the automatic approach mode.” In essence the pilot must immediately determine to continue (if runway reference lights are visible) or initiate the missed approach procedure. An amber indication would imply that the decision could be delayed. Proximity to terrain and limited time to react necessitate a red warning with dual cues.

### **5. CS-25.1329 Flight Guidance System discussion**


CS AWO.262 requires that the autopilot complies with CS-25.1329 and its AMC. Therefore, at the airworthiness certification level, the applicant must show compliance to CS-25.1329 and its associated AMC at least for the entire CAT II operation phase of flight.

 European Union Aviation Safety Agency	<p align="center"><b>SC Consultation paper</b></p> <p align="center"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

However, the CAT II requires to delete an alternative design in CS-23.1329(a) that allows the override of the autopilot instead of a quick disconnect switch.

Considering all the above, the following Special Condition is proposed:



 European Union Aviation Safety Agency	<p align="center"><b>SC Consultation paper</b></p> <p align="center"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

## Appendix A

### Special Condition SC-O23-div-08

#### AWO – CAT II in CS-23

#### **SC-O23-div-08.01 - Applicability**

This special condition is applicable to CS-23 commuter aircraft intended to be certified for CAT II operations in accordance with CS-AWO Subpart 2 complying with CS-23 amendment 3 or later.

The certification basis of the aircraft has to include the Special Condition SC-B23.div-01 'Human Factors'.

Note: If this SC has not been addressed during initial certification, it must be addressed to allow the application of this special conditions within the scope of CAT II operations.

#### **SC-O23-div-08.02 - Front windshield protection:**

CS-23.773 is replaced by the following:

(a) Each pilot compartment must be –

(1) Arranged with sufficiently extensive clear and undistorted view to enable the pilot to safely taxi, take-off, approach, land and perform any manoeuvres within the operating limitations of the aeroplane.

(2) Free from glare and reflections that could interfere with the pilot's vision. Compliance must be shown in all operations for which certification is requested.


(b) The aeroplane must have a means to maintain a clear portion of the windshield during precipitation conditions, enough for both pilots to have a sufficiently extensive view along the flight path in normal flight attitudes of the aeroplane. This means must be designed to function, without continuous attention on the part of the crew, in moderate rain considering approach, landing and go-around speeds in all weight and CG configurations.

(c) Each pilot compartment must have a means to either remove or prevent the formation of fog or frost on an area of the internal portion of the windshield and side windows sufficiently large to provide the view specified in sub-paragraph (a) (1). Compliance must be shown under all expected external and internal ambient operating conditions. It must be shown that the windshield and side windows can be easily cleared without interruption of normal pilot duties and without any pilot manual removal actions.

(d) No single failure of the systems used to provide the view required by subparagraph (b) of this paragraph must cause the loss of that view by both pilots in the specified precipitation conditions.

(e) An openable windows does not need to be provided if it is shown that an area of transparence surface will remain clear sufficient for one pilot to land the aeroplane safely in the event of any system failure or combination of failures, which is not, extremely improbable in accordance with CS-23.1309.



 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

(f) Fixed markers or other guides must be installed at each pilot station to enable the pilots to position themselves in their seats for an optimum combination of outside visibility and instrument scan. If lighted markers or guides are used, they must comply with the requirements specified in CS-25.1381.

(g) The means to maintain the clear portion of the windshield during precipitations should be an active rain removal means (e.g. windshield wipers, windshield bleed air). If a passive rain removal means is used (e.g. coating and/or windshield physical/geometrical properties) to achieve the acceptable forward visibility in precipitation conditions, then SC-O23-div-08.03 has to comply with.

#### **SC-O23-div-08.03 – Passive Rain Removal:**

SC-O23-div-08.02 (b) is replaced by the following:

(b) The aeroplane must have a means to maintain a clear portion of the windshield during precipitation conditions, enough for both pilots to have a sufficiently extensive view along the *ground or flight path* in normal *taxi and flight* attitudes of the aeroplane. This means must be designed to function, without continuous attention on the part of the crew, *in conditions from light misting precipitation to moderate rain from fully stopped in still air* up to the approach, landing and go-around speeds in all weight and CG configurations.

#### **SC-O23-div-08.04 Flight Crew Alerting**

In addition to CS-23.1322 during CAT II operations the following must be complied with:

(a) Flight crew alerts must:

(1) provide the flight crew with the information needed to:

- (i) identify non-normal operation or aeroplane system conditions, and
- (ii) determine the appropriate actions, if any;

(2) be readily and easily detectable and intelligible by the flight crew under all foreseeable operating conditions, including conditions where multiple alerts are provided;


(3) be removed when the alerting condition no longer exists.

(b) Warning and Caution alerts must:

(1) be prioritised within each category, when necessary;

(2) provide timely attention-getting cues through at least two different senses by a combination of aural, visual, or tactile indications;

(3) permit each occurrence of the attention-getting cues required by subparagraph (b)(2) to be acknowledged and suppressed, unless they are required to be continuous.

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

#### **SC-O23-div-08.05 - Flight Guidance System:**

Sub-paragraph CS-23.1329 (a)(2) is deleted and replaced by:

The autopilot must not create an unsafe condition when the flight crew applies an override force to the flight controls.

Sub-paragraph CS-23.1329(h) is deleted and replaced by:

The flight guidance system functions, controls, indications, and alerts must be designed to minimise flight crew errors and confusion concerning the behaviour and operation of the flight guidance system. Means must be provided to indicate the current mode of operation, including any armed modes, transitions, and reversions. Selector switch position is not an acceptable means of indication. The controls and indications must be grouped and presented in a logical and consistent manner. The indications must be visible to each pilot under all expected lighting conditions.

The following additional requirements must be fulfilled:


Following disengagement of the autopilot, a warning (visual and aural) must be provided to each pilot and be timely and distinct from all other cockpit warnings.

Following disengagement of the autothrust function, a caution must be provided to each pilot.

#### **SC-O23-div-08.06 – Operating procedures**

CS-23.1585 is amended by the following additional point:

- (6) The maximum demonstrated precipitation rate (in terms of moderate or heavy rain) pertinent to CAT II operations.

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

## Appendix B

### Associated Interpretative Material and Means of Compliance to Special Condition AWO – CAT II in CS-23

#### Means of Compliance

##### MOC to SC-O23-div-08.03 – Passive Rain Removal

##### **Performance of the passive rain removal means:**

The method should address combinations of precipitation conditions, speeds, time exposure and airplane configurations that may result in areas on the windshield where airflow is stagnated or may otherwise interfere with maintaining the required clear vision area and should establish the effectiveness of the hydrophobic coating to maintain the required area of clear vision.

The definition of the precipitation rate is provided in table 1.

Note: The definition of the median droplet volume diameter should be considered in the method to show compliance when it involves artificial or simulated raining conditions.


-	Misting conditions :	0.05 mm/hour (MVD 0.1 mm)
-	Light :	from 0.25 (MVD 0.2 mm) to 4.5 mm/hour (MVD 1.0 mm)
-	Moderate :	from 4.5 (MVD 1.0 mm) to 12.5 mm/hour (MVD 1.5 mm)
-	Heavy :	from 12.5 (MVD 1.5 mm) to 50 mm/hour (MVD 2.1 mm)

Table 1: Precipitation rate(mm/hour) & median droplet volume diameter (mm)

The performance of the passive rain removal should be demonstrated for rain conditions, but it should also be confirmed that the implementation of the passive rain removal capability do not create any distortion, glare or reflection that may interfere with pilot's vision during day and night, with or without precipitation conditions such as rain, icing conditions and snow.

**The following paragraph only applies for passive rain removal based on windshield hydrophobic coating implementation:**

Coating durability and reliability:

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

Yet, the windshield hydrophobic coating may have a limited and variable effective life, and the failure of the coating may be latent. These aspects should be considered in order to comply with CS 23.603, and SC-O23-div-08.03 (b), since CS 23.1309 cannot apply to the hydrophobic coating.

It should be described how the continued airworthiness of the hydrophobic coating is assured as required by CS 23.1529, even considering its latent failure. This information should include consideration of any factors that can cause long term degradation of the effectiveness of the coating such as aging, aerodynamic erosion, thermal effects, and exposure to water, salt spray, sand, dust, UV, ozone and expected airborne chemicals.

Furthermore any factors that could cause unacceptable degradation of the coating from a single exposure, such as hail, volcanic ash, or wind-blown sand, should be identified and it should be described how continued airworthiness will be assured following such exposure event. If the continuing airworthiness of the coating relies on an inspection/maintenance interval, it should be substantiated that such interval is appropriate in relation with the variable effective life of the coating.

The analysis and the tests supporting the instruction for continuing airworthiness of the hydrophobic coating should consider the encountering of the above environmental conditions with a probability of one.

The pilot compartment view should be shown to comply with SC-O23-div-08.03 with no more than 5% remaining of the substantiated service life or the proposed inspection interval of the windshield coating, as applicable.

In addition to the above considerations, it has been recently recognised that hydrophobic coatings may be particularly susceptible to degradation when the windscreen is handled in a way that would not normally pose a threat in case it relies on conventional means of precipitation removal. The means proposed to avoid or mitigate this failure mechanism of the coating should be described. Specific areas that must be addressed in the Instructions for Continued Airworthiness are:

- approved windscreen cleaning materials and procedure: type of rags, type of cleaners, waxes, etc.,
- appropriate warnings/placards near the windshields, if any,
- any information on the acceptability on the use of de-icing fluids.

Including appropriate information/limitation in both the Airplane Flight Manual and Aircraft Maintenance Manual can be found an acceptable way to mitigate this risk.


#### **MOC to SC-O23-div-08.04 Flight Crew Alerting:**

For the area specific to CAT II operations:

Prevention of crew errors and the rapid recognition of malfunctions request to provide a separate approach mode annunciator in the primary field of view in a position consistent with the other approach modes used. This annunciator can only be in active state when all equipment supporting this selected approach status are met (LOCs, GSs, DMEs, Radar Altimeters, FDs 1/2, APs 1/2, Channel comparators, etc..). The colour philosophy must be consistent with the existing avionics colour philosophy.

Loss of approach capability during an approach requires immediate recognition and immediate action from the pilot. Therefore the loss of CAT II capability below 200 feet is classified as a warning.

In addition, CS-AWO 253(a) states, in part, "Where the approach flight path is controlled automatically, an audible warning must be given following disengagement of the automatic pilot or loss of the automatic approach mode."

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

In the case of CAT II without automatic downgrade to CAT I, it means that the pilot must immediately determine to continue (if he or she can see the runway) or initiate the missed approach procedure. An amber indication implies that the decision can be delayed. Proximity to terrain and limited time to react indicate that a warning alert is appropriate.

**MOC to SC-O23-div-08.05 Flight Guidance System:**

For the area specific to CAT II operations:

**Quick Disengagement Control.**

The purpose of the “Quick Disengagement Control” is to ensure the capability for each pilot to manually disengage the autopilot quickly with a minimum of pilot hand/limb movement. The “Quick Disengagement Control” must be located on each control wheel or equivalent and should be within easy reach of one or more fingers/thumb of the pilot’s hand when the hand is in a position for normal use on the control wheel or equivalent.

The “Quick Disengagement Control” should meet the following criteria :

- (a) Be accessible and operable from a normal hands-on position without requiring a shift in hand position or grip on the control wheel or equivalent;
- (b) Be operable with one hand on the control wheel or equivalent and the other hand on the thrust levers;
- (c) Be easily located by the pilot without having to first locate the control visually;
- (d) Be designed so that any action to operate the “Quick Disengagement Control” should not cause an unintended input to the control wheel or equivalent; and
- (e) Be designed to minimize inadvertent operation and interference with other nearby control wheel (or equivalent) switches/devices (e.g. radio control, trim).


**System Safety Assessment.**

Dependent upon the functionality provided in a specific FGS, the failure conditions could potentially impact the following:

- the control of the aeroplane in the pitch, roll and directional axes,
- the control of thrust,
- the integrity and availability of guidance provided to the flight crew,
- the structural integrity of the aeroplane,
- the ability of the flight crew to cope with adverse operating conditions,
- the flight crew’s performance and workload,
- the safety of the occupants of the aeroplane.

**The type of the FGS Failure Conditions** will depend, to a large extent, upon the architecture, design philosophy and implementation of the system. Types of Failure Conditions can include:

- Loss of function – where a control or display element no longer provides control or guidance
- Malfunction – where a control or display element performs in an inappropriate manner which can include the following sub-types:

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

- a) Hardover – the control or display goes to full displacement in a brief period of time – the resultant effect on the flight path and occupants of the aeroplane are the primary concern.
- b) Slowover - the control or display moves away from the correct control or display value over a relatively long period of time – the potential delay in recognizing the situation and the effect on the flight path are the primary concern.
- c) Oscillatory - the control or display is replaced or augmented by an oscillatory element – there may be implications on structural integrity and occupant well being.

#### **Failure Condition Mitigation**

The propagation of potential Failure Conditions to their full effect may be nullified or mitigated by a number of methods. These methods could include, but are not limited to, the following:

- failure detection and monitoring,
- fault isolation and reconfiguration,
- redundancy,
- authority limiting, and
- flight crew action to intervene.

#### **Flight Test requested.**

##### **A. Autopilot Override and Pitch Trim behavior**

The autopilot should disengage when the flight crew applies a significant override force to the controls. The applicant should interpret “significant” as a force that is consistent with an intention to overpower the autopilot by either or both pilots. The autopilot should not disengage for minor application of force to the controls (e.g. a pilot gently bumping the control column while entering or exiting a pilot seat during cruise).

If the autopilot is designed such that it does not automatically disengage due to a pilot override, verify that no unsafe conditions are generated due to the override. The evaluation should be repeated with progressively increasing rate of force application to assess FGS behavior.


The pilot should then apply an input to the pitch cockpit controller (i.e., control column or sidestick) below that which would cause the autopilot to disengage and verify that the automatic pitch trim system does not generate unsafe conditions.

If the system design is such that the autopilot does not have an automatic disengagement on override feature, the pilot should initiate an intentional override for an extended period of time. The autopilot should then be disengaged, with the Quick Disconnect Button, and any transient response assessed. The effectiveness and timeliness of any Alerts used to mitigate the effects of the override condition should be assessed during this evaluation.

##### **B. Fault Recognition and Pilot Action during approaches with vertical path reference**

The Safety Assessment process may identify a vulnerability to the following types of Failure Condition:

- hardover
- slowover
- oscillatory

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--

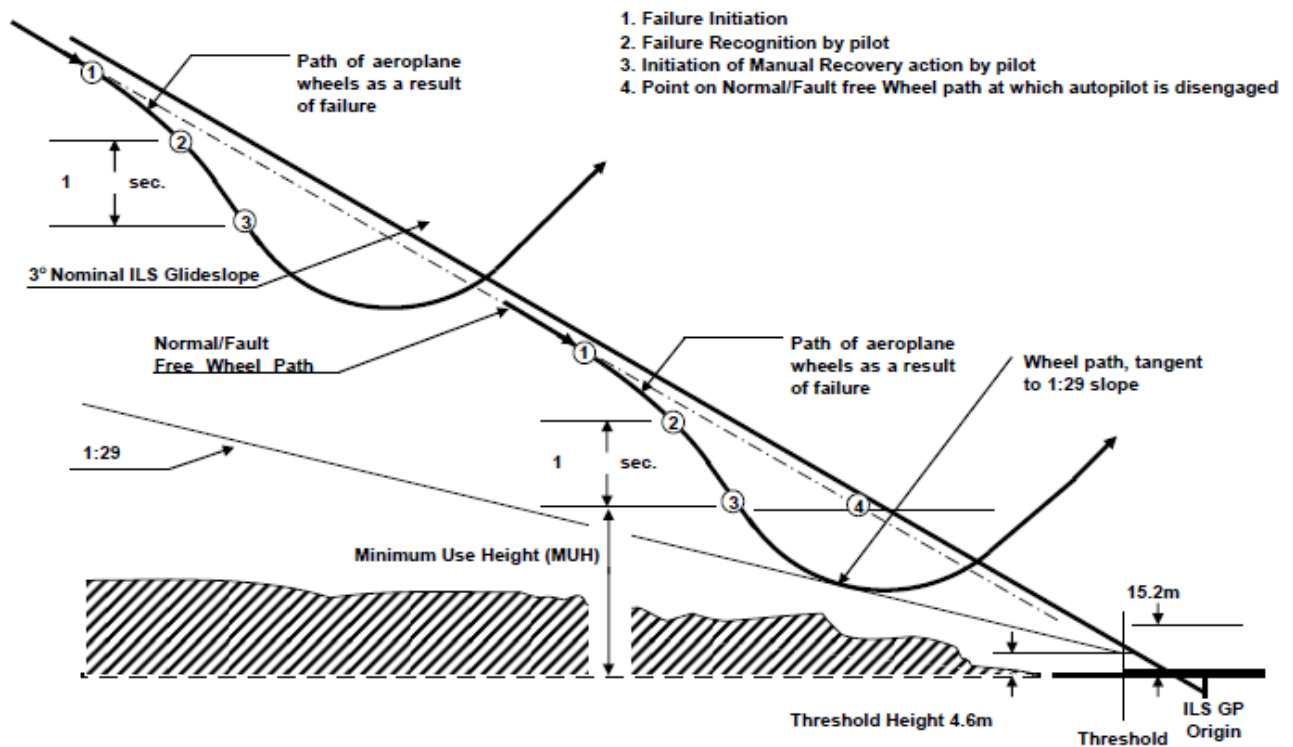
The various types of effect will cause differing response in the aeroplane and resultant motion and other cues to the flight crew to alert them to the condition. The flight crew attention may be gained by additional alerting provided by systems on the aeroplane. The recognition is then followed by appropriate action including recovery. The assessment of the acceptability of the Failure Condition and the validation of the Safety Assessment assumptions are complete when a stable state is reached as determined by the test pilot.

Figure 1 provides a depiction of the deviation profile method. The first step is to identify the deviation profile from the worst-case malfunction. The next step is to 'slide' the deviation profile down the glidepath, until it is tangential to the 1:29 line or the runway. The Failure Condition contribution to the Minimum Use Height may be determined from the geometry of the aircraft wheel height determined by the deviation profile, relative to the 1:29 line intersecting a point 4.5 m (15 ft) above the threshold. The method of determination may be graphical or by calculation.

**NOTE:** The Minimum Use Height is based on the recovery point because:

- i) It is assumed that in service the pilot will be "Hands off" until the autopilot is disengaged at the Minimum Use Height in normal operation.
- ii) The test technique assumes a worst case based on the pilot being "Hands off" from the point of malfunction initiation to the point of recovery.
- iii) A failure occurring later in the approach than the point of initiation of the worst case malfunction described above is therefore assumed to be recovered earlier and in consequence to be less severe.






**Figure FT-1: Deviation Profile Method**

## Interpretative Material

### **IM to SC- SC-O23-div-08.02 (d) Front windshield protection**

Often Single pilot aircraft have a prioritization of the essential system to the left seat. Therefore, a CAT II visual segment and the landing phase might not be flyable from the right seat in case of windshield protection failure. Depending on the ice and rain protection architecture, it must be determined if a limitation is necessary when the landing cannot be conducted from one pilot station following a system failure.

 European Union Aviation Safety Agency	<p align="center"><b>SC Consultation paper</b></p> <p align="center"><b>Special Condition</b></p>	Doc. No. : SC-O23-div-08 Issue : 1 Date : 04 May 2021 Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/> Deadline for comments: 25 May 2021
--	---	--


## Appendix C

### Means of Compliance to CS-23.1309

#### AMC 23.1309                      Equipment, systems, and installations

### Contents

1. Applicability .....	18
2. EASA and Industry documents .....	18
3. Showing compliance with the requirements of CS 23.1309(a), (a)(1) and (a)(3) .....	19
4. Application of CS 23.1309(a)(4) .....	22
5. Application of CS 23.1309(b) .....	22
6. Safety assessments .....	23
7. Failure conditions.....	26
8. Assessment methods .....	28
9. Assessment of failure condition probabilities and analysis considerations .....	29
10. Operational and maintenance considerations .....	31
11. Acronyms.....	32
12. Definitions .....	33
13. Guidance on the calculation of the average probability per flight hour .....	40

 European Union Aviation Safety Agency	<p style="text-align: center;"><b>SC Consultation paper</b></p> <p style="text-align: center;"><b>Special Condition</b></p>	<p>Doc. No. : SC-O23-div-08</p> <p>Issue : 1</p> <p>Date : 04 May 2021</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p> <p>Deadline for comments: 25 May 2021</p>
--	---	---

## 1. Applicability

This document should not be utilised to replace any specific guidance intended for individual types of equipment, systems, and installations. Because CS 23.1309 is a regulation of general requirements, it should not be used to supersede any specific requirements of CS 23. For example, CS 23.1311, Electronic display instrument systems, has specific requirements on the number of electronic displays required for attitude, airspeed, and altitude; therefore, CS 23.1309 should not be used to increase or decrease the requirements (except for determining the Software Development Assurance Level). For either mechanical, hydro-mechanical or analogue electromechanical systems, or both, where the installation is not complex, the single fault concept and experience that are based on service-proven designs and engineering judgement may be appropriate. In this case, a Functional Hazard Assessment (FHA), a design appraisal, and an installation appraisal, may satisfy CS 23.1309(b).

The CS 23.1309 does not apply to the performance, flight characteristics, and structural loads and strength requirements of Subparts C and D, but it does apply to any system on which compliance with the requirements of Subparts B, C, and D is based. For example, it does not apply to an aircraft's inherent stall characteristics or their evaluation of CS 23.201, Wings level stall, but it does apply to a stick pusher (stall barrier) system installed to attain compliance with CS 23.201. CS 23.1309 is applicable to the installation of all aeroplane systems and equipment, which includes pneumatic systems, fluid systems, electrical/electronic systems, mechanical systems, and powerplant systems included in the airplane design, except for the following: (1) Systems and installations approved only as part of a type-certificated engine or propeller, and (2) The flight structure (such as wings, fuselage, empennage, control surfaces, mechanical flight control cables, pushrods, control horns, engine mounts, and structural elements of the landing gear) requirements are specified in Subparts C and D of CS 23.

Terms such as “must” are used in this CRI only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance described herein is used. The word “must” is also used when referring to a specific regulation or guidance that is essential when the applicant uses this AC for the means of compliance. In this case there is no deviation. The word “should” is used to express a recommendation. Deviation from the specified recommendation may require justification.

This section does not change the intent of the certification basis and the related guidance material with regard to the review process, but it clarifies the approach to compliance substantiation and determination.

## 2. EASA and Industry documents

- Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) **4754A** / EUROCAE ED-79A, Guidelines for development of civil aircraft and systems.
- Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) **4761**, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

Note: ARPs 4754A / ED79A and 4761 provide guidelines and methods of performing the safety assessment for certification of civil aircraft.

### 3. Showing compliance with the requirements of CS 23.1309(a), (a)(1) and (a)(3)

In order to show compliance with the requirements of CS 23.1309(a), (a)(1) and (a)(3), it will be necessary to verify that the installed systems and each item of equipment will cause no unacceptable adverse effects and to verify that the airplane is adequately protected against any hazards that could result from probable malfunctions or failures. Analyse, inspect, and test equipment, systems, and installations to ensure compliance with the requirements of CS 23.1309(a), (a)(1), and (a)(3). A step-by-step diagram to comply with CS 23.1309(a), (a)(1) and (a)(3) is shown in figure 1. These steps are described below.

- (1)** Evaluate all airplane systems and each item of equipment in order to determine whether they are the following:
  - (a)** Essential to safe operation; or
  - (b)** Not essential to safe operation.
- (2)** Determine that operation of installed equipment has no unacceptable adverse effects. Verify this by applicable flight or ground checks, as follows:
  - (a)** If it can be determined that the operation of the installed equipment will not adversely affect equipment essential to safe operation, the requirements of CS 23.1309(a)(1)(i) have been satisfied; and
  - (b)** If it is determined that the operation of the installed equipment has an adverse effect on equipment not essential to safe operation and a means exists to inform the pilot of the effect, the requirements of CS 23.1309(a)(1)(ii) have been met. An acceptable means to inform the pilot that the affected system is not performing properly would include any visual or aural method (flags, lights, horns, loss of display, etc.).
- (3)** Determine that failure or malfunction of the installed equipment could not result in unacceptable hazards.
  - (a)** Each item of equipment must be evaluated for general installation hazards. These types of hazards would normally include those hazards that would directly compromise the safety of the airplane or its occupants, such as fire, smoke, explosion, toxic gases, depressurization, etc. A hazard could also result from loss of equipment or systems essential to safe operations when the minimum required functions are lost. Individual failure of redundant equipment would not necessarily be considered a hazard. For example, the single failure of either a communication transceiver or a navigation receiver (but not both) during IFR operation is not considered a hazard; however, a single failure of a common power supply to those systems would be considered a hazard.
  - (b)** Systems and equipment essential to safe operation must also be assessed for probability of malfunction or failure. Where the installation is conventional, and where there is a high degree of similarity in installations and a significant amount of service history is available for review, this determination can be an engineering judgment. Service history should show that past malfunctions or failures have not resulted in hazards and there are no unresolved problems.
  - (c)** Hazards identified and found to result from probable failures are not acceptable in multiengine aeroplanes. In these situations, a design change may be required to remove the hazard or to reduce the probability of failure, such as increasing redundancy, substitution of more reliable equipment, annunciation, etc.
  - (d)** If it has been determined that a probable failure or malfunction could result in a hazard to a single-engine aeroplanes, that hazard must be minimized or prevented in a multiengine airplane. To

**SC Consultation paper**  
**Special Condition**

Doc. No. : SC-O23-div-08

Issue : 1

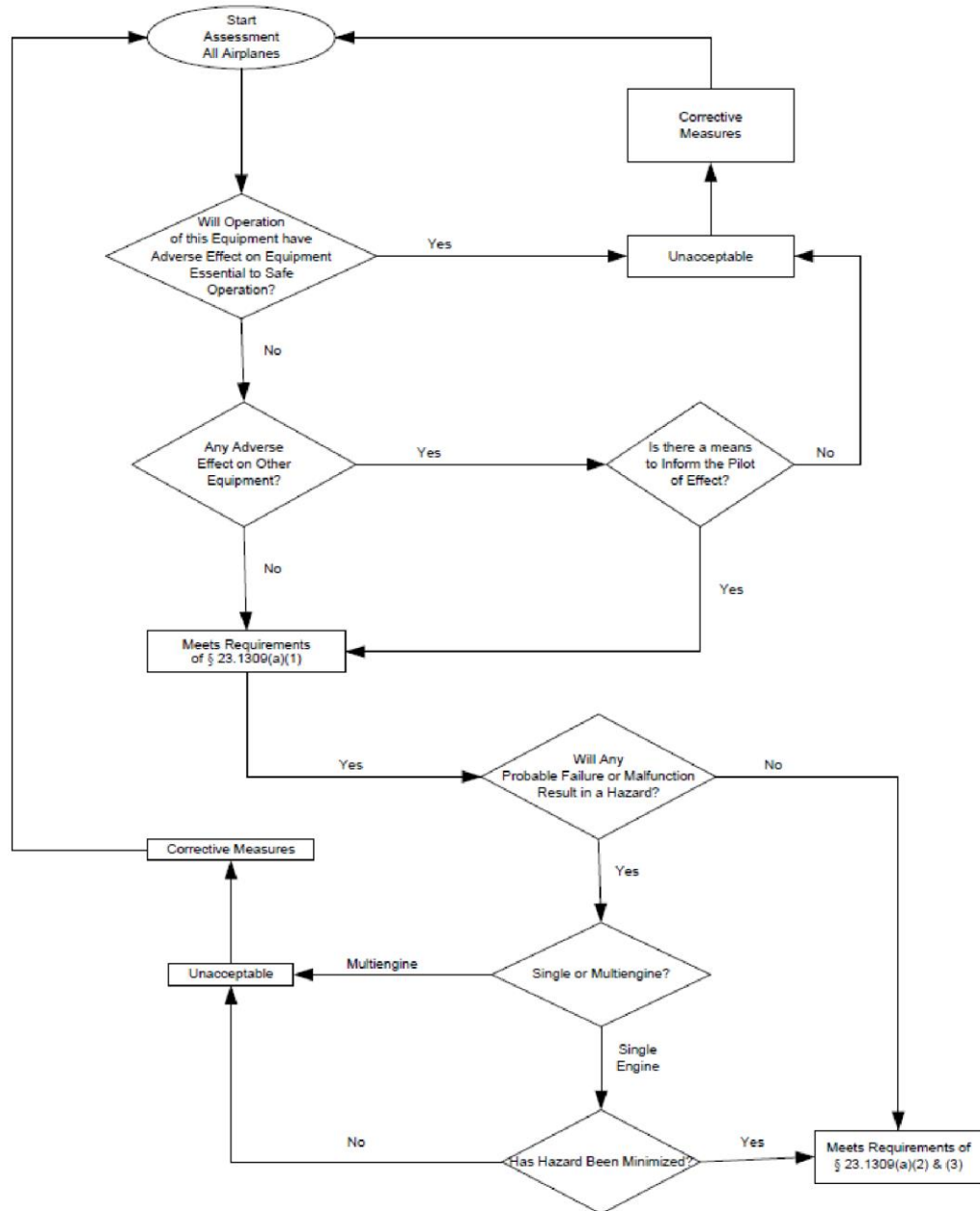
Date : 04 May 2021

Proposed ☒ Final ☐

Deadline for comments: 25 May 2021

minimize is to reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. Design features should be taken into account to prevent hazards either by ensuring that the failure condition will not occur or by having redundancy or annunciation with the associated flight crew's corrective action. In either case, the hazards should be addressed to the least practical amount to the point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction that is practical for this type of airplane. Additional efforts would not result in any significant improvements of safety and would inappropriately add to the cost of the product without a commensurate benefit. This determination should come from an experienced engineering judgment based on the criticality of the hazard and the intended kinds of operation.

**FIGURE 1. METHOD OF COMPLIANCE DIAGRAM OF CS 23.1309(a)**



## 4. Application of CS 23.1309(a)(4)

**a.** Design features should be taken into account to safeguard against hazards either by ensuring that the failure condition will not occur or by having redundancy or annunciation with the associated flight crew's corrective action. The reliability should be such that independent failures of the redundant systems are not probable during the same flight. If a redundant system is required, a probable failure in one system should not adversely affect the other system's operation. No probable failure should result in a "safe" indication of an "unsafe" condition so that the flight crew would incorrectly assume the system is available or functional. When the unsafe condition is annunciated or detected, the AFM should have clear and precise corrective procedures for handling the failure without an excessive increase in workload.

**b.** Service history for similar installations may be utilized to meet part or all of this requirement if a system or installation has a significant and favorable service history in environments similar to the airplane. The claim of similarity should be based on equipment type, function, design and installation similarities, and other relevant attributes. It is the applicant's responsibility to provide accepted/approved data that supports any similarity claims to a previous installation.

## 5. Application of CS 23.1309(b)

The installed systems should be evaluated by performing a safety assessment as shown in this CRI. The depth and scope of the safety assessment depends on the types of functions performed by the systems, the severity of the failure conditions, and whether the system is complex. The types of analyses selected by an applicant and approved by EASA should be based on factors such as the system architecture, complexity, particular design, etc.


The safety assessment objective is to ensure an acceptable safety level for equipment and systems installed on the airplane. A logical and acceptable inverse relationship should exist between the average probability per flight hour and the severity of failure conditions effects (as shown in figure 2). The relationship between probability and severity of failure condition effects are as follows:

- (1)** Failure conditions with no safety effect have no probability requirement.
- (2)** Minor failure conditions may be probable.
- (3)** Major failure conditions must be no more frequent than remote.
- (4)** Hazardous failure conditions must be no more frequent than extremely remote.
- (5)** Catastrophic failure conditions must be extremely improbable.

Compliance with CS 23.1309(b) may be shown by analysis and, where necessary, by appropriate ground, flight, or simulator test. The analysis should consider—

- (1)** Possible modes of failure, including malfunctions and damage from external sources;
- (2)** The probability of multiple failures and the probability of undetected faults;
- (3)** The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions; and
- (4)** The crew warning cues, corrective action required, and the crew's capability of determining faults.



 <b>EASA</b> European Union Aviation Safety Agency	<b>SC Consultation paper</b> <b>Special Condition</b>	Doc. No. : SC-023-div-08
		Issue : 1
		Date : dd mmm yyyy
		Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/>
		Deadline for comments: ddMMMyyyy

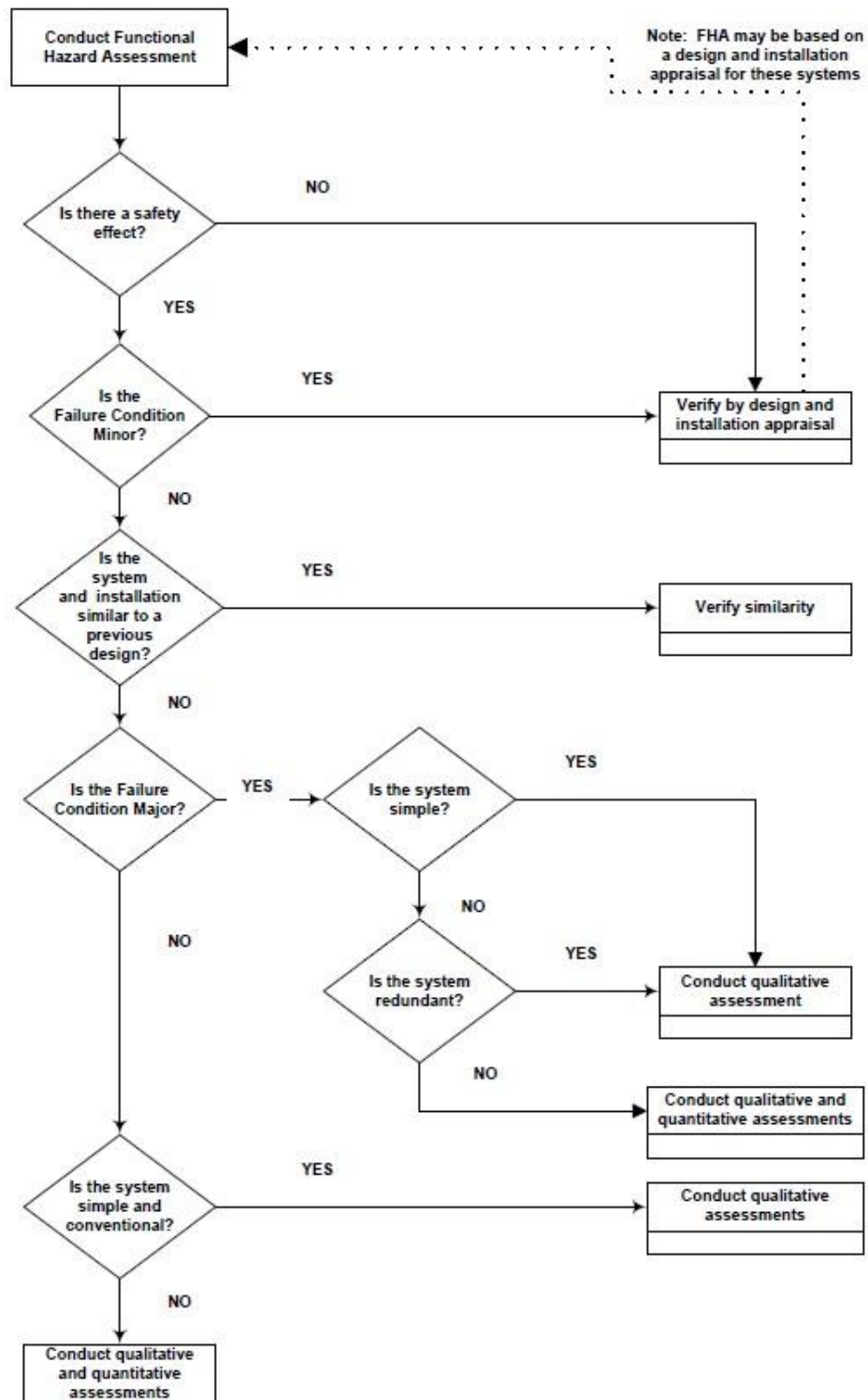
**FIGURE 2. RELATIONSHIP AMONG PROBABILITIES, SEVERITY OF FAILURE CONDITIONS, AND SOFTWARE AND COMPLEX HARDWARE DAL (for Class IV)**

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
<b>Allowable Quantitative Probabilities and DAL assignment</b>					
Allowable Quantitative probabilities	No Probability	<10 <sup>-3</sup> Note 1	<10 <sup>-5</sup>	<10 <sup>-7</sup>	<10 <sup>-9</sup> Note 3
Functional DAL and Item DAL assignment (Note 2)	E	D	C	B	A
Note 1: Numerical values indicate an order of probability range and are provided here as a reference.  Note 2: Further consideration on DAL assignment may be found in ED-79A section 5.2.  Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.					

## 6. Safety assessments

**a.** The applicant is responsible for identifying and classifying each Failure Condition and choosing the methods for safety assessment. The applicant should then obtain early concurrence from EASA on the identification of Failure Conditions, their classifications, and the choice of an acceptable means of compliance. Figure 3 provides an overview of the information flow to conduct a safety assessment. This figure is a guide and it does not include all information provided in this CRI or the documents referenced in section 2.





**(5)** After each failure condition is classified, refer to figure 2 to identify the failure condition probability and software and complex hardware IDALs or FDAL.

**(6)** The classification of failure conditions does not depend on whether a system or function is required by any specific regulation. Some systems required by specific regulations, such as transponders, position lights, and public address systems, may have the potential for only minor failure conditions. Conversely, other systems not required by any specific regulation, such as flight management systems and automatic landing systems, may have the potential for major, hazardous, or catastrophic failure conditions.

**(7)** The classification of failure conditions should consider all relevant factors. Examples of factors include the nature of the failure modes, which includes common mode faults, system degradation resulting from failures, flight crew actions, flight crew workload, performance degradation, reduced operational capability, effects on airframe, etc. It is particularly important to consider factors that would alleviate or intensify the severity of a failure condition. An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by a failure condition. Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a failure condition, such as weather or other adverse operational or environmental conditions. The ability of a system to inform the pilot of potential or real failure conditions so that timely corrective action can be taken to reduce the effects of the combination of events is desirable. This approach may reduce the severity of the failure condition.

**(8)** Because of the large number of combinations of failures, various mitigating factors, airplane characteristic effects, and similar factors, a specific FHA and the related safety assessments may be significantly different for each evaluated airplane type and configuration. These factors preclude providing a concrete example of a FHA that applies across the board to every installation. It is critical to understand that significant engineering judgment and common sense are necessary to provide a practical and acceptable evaluation of the airplane and its systems.

## 7. Failure conditions

**a.** Failure conditions. A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events.

Failure conditions may be classified according to the severity of their effects as follows:

**(1) No safety effect.** Failure conditions that would have no effect on safety (that is, failure conditions that would not affect the operational capability of the airplane or increase crew workload).

**(2) Minor.** Failure conditions that would not significantly reduce airplane safety and involve crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in crew workload (such as routine flight plan changes), or some physical discomfort to passengers or cabin crew.

**(3) Major.** Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins or functional capabilities. In addition, the failure condition has a significant increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.

**(4) Hazardous.** Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following:

(a) A large reduction in safety margins or functional capabilities;

- (b) Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or (c) Serious or fatal injury to an occupant other than the flight crew.

**(5) Catastrophic.** Failure conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane. Notes: (1) The phrase “are expected to result” is not intended to require 100 percent certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic. (2) The term “catastrophic” was defined in previous versions of advisory materials as a failure condition that would prevent continued safe flight and landing.

**b. Failure conditions with no safety effect.** An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation. If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

**c. Analysis of minor failure conditions.** An analysis should consider the effects of system failures on other systems or their functions. An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. In general, common design practice provides physical and functional isolation from components that are essential to safe operation. If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

**d. Analysis of major failure conditions.** An assessment based on engineering judgment is a qualitative assessment, as are several of the methods described below:

**(1)** Similarity allows validation of a requirement by comparison to the requirements of similar certified systems. The similarity argument gains strength as the period of experience with the system increases. If the system is similar in its relevant attributes to those used in other aeroplanes and if the functions and effects of failure would be the same, then a design and installation appraisal and satisfactory service history of either the equipment being analysed or of a similar design is usually acceptable for showing compliance. It is the applicant’s responsibility to provide data that is accepted, approved, or both, and that supports any claims of similarity to a previous installation.

**(2)** For systems that are not complex and where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment that shows that the major failure conditions of the system, as installed, are consistent with the FHA (for example, redundant systems).

**(3)** To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is necessary to conduct a qualitative functional FTA or FMEA supported by failure rate data and fault detection coverage analysis.

**(4)** An analysis of a redundant system in the airplane is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems, where functional redundancy is required, a qualitative FMEA or FTA may be necessary to determine that redundancy actually exists (for example, no single failure affects all functional channels).

**e. Analysis of hazardous and catastrophic failure conditions.** For these failure conditions, a thorough safety assessment is necessary. The assessment usually consists of an appropriate combination of qualitative and quantitative analyses. Except as specified in the next paragraphs below, a detailed safety analysis must be completed for each hazardous and catastrophic failure condition identified by an FHA. The analysis will usually be a combination of qualitative and quantitative assessments of the design.

**(1)** For simple and conventional installations (that is, low complexity and similarity in relevant attributes), it may be possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for the assessment will be the degree of redundancy, the established independence and isolation of the channels, and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many aeroplanes may be sufficient when a close similarity is established regarding both the system design and operating conditions.

**(2)** For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may also be possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. A high degree of similarity in both design and application is required.

**(3) No catastrophic failure condition** (Note 3 in figure 2) **should result from the failure of a single component, part, or element of a system.** Experienced engineering judgment and service history should show that a catastrophic failure condition by a single failure mode is not a practical possibility. The logic and rationale used in the assessment should be so straightforward and obvious that the failure mode simply would not occur unless it is associated with an unrelated failure condition that would, in itself, be catastrophic.

## 8. Assessment methods

**a. Assessment methods.** Methods for qualitatively and quantitatively assessing the causes, severity, and likelihood of potential failure conditions are available to support experienced engineering and operational judgment. Some of these methods are structured. The various types of analyses are based on either inductive or deductive approaches. The applicant should select analyses to validate the safety of a particular design based on factors such as the system architecture, complexity, criticality of the function, etc. ARP 4761 has more details of the various methods. Descriptions of typical types of analyses that might be used are provided below.

**(1) Design appraisal.** A qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment.

**(2) Installation appraisal.** This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices should be evaluated. An effective appraisal requires experienced judgment.

**(3) Failure Modes and Effects Analysis (FMEA).** A structured, inductive, and bottom-up analysis that is used to evaluate the effects on the system and the airplane of each possible element or component failure. When properly formatted, it should aid in identifying latent failures and the possible causes of each failure mode. ARP 4761 provides methodology and detailed guidelines that may be used to perform this type of analysis. An FMEA could be a piece-part FMEA or a functional FMEA. For modern microcircuit-based line replaceable units and systems, an exhaustive piece-part FMEA is not practically feasible with the present state of the art. In that context, an FMEA may be more functional than piece-part oriented. A functional-oriented FMEA can lead to



uncertainties in the qualitative and quantitative aspects, which can be compensated for by more conservative assessments, such as the following: Assuming all failure modes result in failure conditions of interest, carefully choosing system architecture, and using lessons learned from similar technology.

**(4) Fault Tree Analysis (FTA).** A structured, deductive, and top-down analysis that is used to identify the conditions, failures, and events that would cause each defined failure condition. FTAs are graphical methods of identifying the logical relationship between each particular failure condition and the primary element or component failures, other events, or combinations thereof that can cause it. The fault tree should be developed to the lowest level for which failure rates can be substantiated. Rates derived from applicable service experience, acceptable industry wide sources, manufacturer's accelerating testing data, or from an FMEA may be used as inputs to the lowest level events.

**(5) Common cause analysis.** The acceptance of adequate probability of failure conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense, and specific studies are necessary to ensure that independence can either be assured or deemed acceptable. The "common cause analysis" is divided into three areas of study:

**(a) Zonal safety analysis (ZSA):** This analysis has the objective of ensuring that the equipment installations within each zone of the airplane are at an adequate safety standard regarding design and installation standards, interference between systems, and maintenance errors.

**(b) Particular Risk Analysis (PRA):** Particular risks are defined as those events or influences outside the systems concerned (e.g., fire, leaking fluids, bird strike, tire burst, HIRF exposure, lightning, uncontained failure of high energy rotating machines, etc.). Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects, or influences, which may violate independence.

**(c) Common Mode Analysis (CMA):** This analysis is performed to confirm the assumed independence of the events that were considered in combination for a given failure condition. The effects of specification, design, implementation, installation, maintenance errors, manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered.

## 9. Assessment of failure condition probabilities and analysis considerations

**a.** An assessment of the probability of a failure condition may be either qualitative or quantitative. An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the type of functions performed by the system, the severity of failure conditions, and whether the system is complex. A quantitative analysis is intended to supplement, but not replace, qualitative methods based on engineering and operational judgment. A quantitative analysis is often used for catastrophic or hazardous failure conditions of systems that are complex and major failure conditions that are complex without redundancy. For the cases where there is insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems.





## 10. Operational and maintenance considerations

### a. Alerts

**(1)** CS 23.1309(b)(3) requires information concerning unsafe system operating condition(s) must be provided in a timely manner to the crew to enable them to take appropriate corrective action. An appropriate alert must be provided if immediate pilot awareness and immediate or subsequent corrective action is required. The particular method of indication depends on the urgency and need for flight crew awareness or action necessary for the particular failure. Inherent airplane characteristics may be used in lieu of dedicated indications and annunciations if they can be shown to be timely and effective. However, the use of periodic maintenance or flight crew checks to detect significant latent failures when they occur should not be used in lieu of practical and reliable failure monitoring and indications.

**(2)** CS 23.1309(b)(3) specifies that the design of systems and controls, including indications and annunciations, must be design to minimize crew errors, which could create additional hazards. The additional hazards to be minimized include those caused by inappropriate actions by a crewmember in response to the failure, or those that could occur after a failure.

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

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

**(1)** If the evaluation indicates that a potential failure condition can be alleviated or overcome in a timely manner without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, correct crew action may be assumed in both qualitative and quantitative assessments.

**(2)** Annunciation that requires flight crew actions should be evaluated to determine if the required actions can be accomplished in a timely manner without exceptional pilot skills. If the evaluation indicates that a potential failure condition can be alleviated or overcome during the time available without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, credit may be taken for correct and appropriate corrective action for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance if overall flight crew workload during the time available is not excessive and if the tasks do not require exceptional pilot skill or strength.

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

**d. Maintenance actions.** Credit may be taken for correct accomplishment of maintenance tasks in both qualitative and quantitative assessments if the tasks are evaluated and found to be reasonable. Required maintenance tasks, which mitigate hazards, should be provided for use in the approved maintenance programs such as the ICA. Annunciated failures will be corrected before the next flight or a maximum duration will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. A scheduled maintenance task may detect latent failures. If this approach is taken, and the failure condition is hazardous or catastrophic, then a maintenance task should be established. Some latent failures can be assumed to be identified based upon a return to service test on the equipment following its removal and repair (component MTBF should be the basis for the check interval time).

## 11. Acronyms

AC	Advisory Circular
AFM	Airplane Flight Manual
AFMS	Airplane Flight Manual Supplement
ARP	Aerospace Recommended Practice
ATC	Amended Type Certificate
CFR	Code of Federal Regulations
CMA	Common Mode Analysis
CRI	Certification Review Item
CS	Certification Specification
DAL	Development Assurance Level
EASA	European Aviation Safety Agency
ED	EUROCAE Document
EUROCAE	Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HW	Hardware
ICA	Instructions for Continued Airworthiness
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
MFD	Multifunction Flight Display
MTBF	Mean Time Between Failures
NAA	National Aviation Authority

P	Primary System
PCM	Project Certification Manager
PFD	Primary Flight Display
PMA	Parts Manufacturer Approval
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
R	Reserved
S	Secondary System
SAE	Society of Automotive Engineers
SSA	System Safety Assessment
STC	Supplemental Type Certificate
STE	Single Turbine Engine
SW	Software
TC	Type Certificate
ZSA	Zonal safety analysis

## 12. Definitions

The following definitions apply to the system design and analysis requirements of CS 23.1309 and the guidance material provided in this CRI. They should not be assumed to apply to the same or similar terms used in other regulations or CRI/AMCs. Terms for which standard dictionary definitions apply are not defined herein.

Definition	Source
<b>Acceptance.</b> Acknowledgment by the certification authority that a submission of data, ED79A argument, or claim of equivalence satisfies applicable requirements.	
<b>Adverse effect.</b> A response of a system that results in an undesirable operation of an AC 23.1309-1E airplane system, or subsystem.	
<b>Adverse operating condition.</b> A set of environmental or operational circumstances AC 23.1309-1E applicable to the airplane, combined with a failure or other emergency situation that results in a significant increase in normal flight crew workload.	
<b>Agreement.</b> Acknowledgment by the certification authority that a plan or proposal ED79A relating to, or supporting, an application for approval of a system or component, is an acceptable statement of intent with respect to applicable requirements.	
<b>Analysis.</b> An evaluation based on decomposition into simple elements. Note : Analysis. AC 23.1309-1E The terms "analysis" and "assessment" are used throughout. Each has a broad definition and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, Preliminary System Safety Assessment, etc.	
<b>APPROVAL:</b> The act of formal sanction of an implementation by a certification authority. ED79A	

**APPROVED:** Accepted by the certification authority as suitable for a particular purpose. ED79A (ICAO).

**Assessment.** An evaluation based upon engineering judgment. AC 23.1309-1E and ED79A

**ASSUMPTIONS:** Statements, principles, and/or premises offered without proof. ED79A

**ASSURANCE:** The planned and systematic actions necessary to provide adequate ED79A confidence and evidence that a product or process satisfies given requirements. (ED-12B / DO-178B)

Definition	Source
------------	--------

**Attribute.** A feature, characteristic, or aspect of a system or a device, or a condition AC 23.1309-1E affecting its operation. Some examples would include design, construction, technology, installation, functions, applications, operational uses, and environmental and operational stresses. It would also include relationships with other systems, functions, and flight or structural characteristics.

**Average probability per flight hour.** A representation of the number of times the AC 23.1309-1E subject failure condition is predicted to occur during the entire operating life of all airplanes of a type, divided by the anticipated total operating hours of all airplanes of that type. Note: The average probability per flight hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration. See Appendix.

**Candidate Certification Maintenance Requirements (CCMR):** A periodic maintenance AC 23.1309-1E or flight crew check may be used in a safety analysis to help demonstrate compliance with CS 23.1309 for Hazardous and Catastrophic Failure Conditions. Where such checks cannot be accepted as basic servicing or airmanship they become Candidate Certification Maintenance Requirements (CCMRs). AMC 25.19 defines a method by which Certification Maintenance Requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the aeroplane.

**Caution.** A clear and unambiguous indication to the flight crew or pilot of a failure that AC 23.1309-1E requires subsequent crew action. An inherent characteristic of the airplane or a device that will give clearly distinguishable indications of malfunction or misleading information may provide this caution.

**COMMON CAUSE ANALYSIS:** Generic term encompassing zonal safety analysis, ED79A particular risk analysis, and common mode analysis.

**Common Mode Analysis:** An analysis performed to verify that failure events identified in ED79A the ASA/SSA are independent in the actual implementation.

**COMMON MODE ERROR:** An error which affects a number of elements otherwise ED79A considered to be independent.

**Complex system.** A system is "complex" when its operation, failure modes, or failure AC 23.1309-1E effects are difficult to comprehend without the aid of analytical methods or structured assessment methods. FMEA and FTA are examples of such structured assessment methods. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships. For example, for these types of systems, a portion of the compliance may be shown by the use of DALs such as by processes in RTCA/DO-178B or RTCA/DO-254 or equivalent. See the definitions for "conventional" and "simple" for more information.

**COMPLIANCE:** Successful performance of all mandatory activities; agreement between ED79A the expected or specified result and the actual result.

**COMPONENT:** Any self-contained part, combination of parts, subassemblies or units, that ED79A perform a distinctive function necessary to the operation of the system.

Definition	Source
<b>CONFIGURATION BASELINE:</b> A known aircraft/ system /item configuration against ED79A which a change process can be undertaken.	
<b>CONFIGURATION ITEM:</b> Aircraft, system, item and related data that is under ED79A configuration control.	
<b>Continued safe flight and landing.</b> This phrase means that the airplane is capable of AC 23.1309-1E continued controlled flight and landing, possibly using emergency procedures, without requiring exceptional pilot skill or strength. Upon landing, some airplane damage may occur as a result of a failure condition.	
<b>Conventional system.</b> A system is considered "conventional" if its function, the AC 23.1309-1E technological means to implement its function, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used. The systems that have established an adequate service history and the means of compliance for approval are generally accepted as "conventional." Normally conventional and simple systems may be analyzed by qualitative assessments as shown in Figure 3. See the definitions for complex and simple systems for more information.	
<b>Critical function.</b> A function whose loss would prevent the continued safe flight and AC 23.1309-1E landing of the airplane. Note: The term "critical function" is associated with a catastrophic failure condition. Newer documents may not refer specifically to the term "critical function."	
<b>Design appraisal.</b> A qualitative appraisal of the integrity and safety of the system design. AC 23.1309-1E An effective appraisal requires experienced judgment.	
<b>Design assurance level.</b> All of those planned and systematic actions used to AC 23.1309-1E substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the items (hardware, software) satisfy the applicable certification basis. This term may be used in some SAE and RTCA documents, but in this AC it is intended that design assurance levels will correlate to the same levels as the DALs for the safety assessment process. See section 21 for more information.	
<b>Development Assurance Level (DAL).</b> All those planned and systematic actions used to AC 23.1309-1E substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis. <b>Note:</b> For this AC, DALs in figure 2 and throughout this AC are also intended to correlate to software levels in RTCA/DO-178B and complex hardware design assurance levels in RTCA/DO-254 for the system or item.	
<b>DEVELOPMENT ASSURANCE:</b> All of those planned and systematic actions used to ED79A substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis. (AMC 25).	
<b>DEVELOPMENT ERROR:</b> A mistake in requirements determination, design or ED79A implementation.	
<b>Equipment essential to safe operation.</b> Equipment installed in order to comply with the AC 23.1309-1E applicable certification requirements of CS 23 or operational requirements.	

Definition	Source
<b>ERROR:</b> An omitted or incorrect action by a crewmember or maintenance person, or a mistake in requirements, design, or implementation (derived from AMC 25.1309). similar to AC 23.1309-1E	ED79A and







**HARDWARE:** An item that has physical being.

ED79A

**Hazard.** A potentially unsafe condition resulting from failures, malfunctions, external AC 23.1309-1E events, errors, or combinations thereof. This term is intended for single malfunctions or failures that are considered probable based on either past service experience or analysis with similar components in comparable airplane applications, or both. There is no quantitative analysis intended in this application. **Note:** There is a difference between “hazardous” as used in general policy or regulations and “hazardous failure condition” as used in an FHA. When the term “hazard” or “hazardous” is used in general policy or regulations, it is generally used as shown in this definition. A hazard could be a failure condition that relates to major, hazardous, or catastrophic.

**IMPLEMENTATION:** The act of creating a physical reality from a specification.

ED79A

**Improbable failure conditions.** Those failure conditions unlikely to occur in each AC 23.1309-1E airplane during its total life, but that may occur several times when considering the total operational life of a number of airplanes of this type. Also, those failure conditions not anticipated to occur to each airplane during its total life but that may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for major and hazardous failure conditions in figure 2. For more specific guidance, see definitions of “remote failure conditions” and “extremely remote failure conditions”

**INDEPENDENCE:** 1. A concept that minimizes the likelihood of common mode errors and ED79A cascade failures between aircraft/system functions or items, 2. Separation of responsibilities that assures the accomplishment of objective evaluation e.g. validation activities not performed solely by the developer of the requirement of a system or item.

**Installation appraisal.** A qualitative appraisal of the integrity and safety of the AC 23.1309-1E installation. Any deviations from normal industry-accepted installation practices should be evaluated.

**INTEGRATION:** 1. The act of causing elements of a system / item to function together. ED79A 2. The act of gathering a number of separate functions within a single implementation.

**ITEM DEVELOPMENT Assurance Level (IDAL):** The level of rigor of development ED79A assurance tasks performed on Item(s). [e.g. IDAL is the appropriate Software Level in ED-12B / DO-178B/, and design assurance level in ED-80 / DO-254 objectives that need to be satisfied for an item].

Definition	Source
------------	--------

**ITEM DEVELOPMENT ASSURANCE:** All of those planned and systematic tasks used to ED79A substantiate, to an adequate level of confidence, that development errors have been identified and corrected such that the items satisfy a defined set of requirements.

**ITEM DEVELOPMENT INDEPENDENCE** – An attribute that minimizes the likelihood of a ED79A common mode error in the item development process.

**ITEM:** A hardware or software element having bounded and well-defined interfaces.

ED79A

**Latent failure.** A failure is latent until it is made known to the flight crew or maintenance AC 23.1309-1E personnel.

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

**MEAN TIME BETWEEN FAILURES (MTBF):** Mathematical expectation of the time ED79A interval between two consecutive failures of a hardware item. NOTE: The definition of this statistic has meaning only for repairable items. For non-repairable items, the term Mean Time To Failure (MTTF) is used.

**Minimize.** To reduce, lessen, or diminish a hazard to the least practical amount with AC 23.1309-1E current technology and materials. The least practical amount is that point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction. Additional efforts would not result in any significant improvements to safety and would inappropriately add to the cost of the product without a commensurate benefit.

**PARTICULAR RISKS:** Particular risks are defined as those events or influences which are ED79A external to the aircraft or within the aircraft but external to the system(s) and item(s) being analyzed, but which may violate failure independence claims.

**Power source.** A system that provides power to installed equipment. This system would AC 23.1309-1E normally include prime mover(s), required power converter(s), energy storage device(s), and required control and interconnection means.

**PRELIMINARY SYSTEM SAFETY ASSESSMENT:** A systematic evaluation of a proposed ED79A system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items.

Definition	Source
<p><b>Primary function.</b> A function installed to comply with applicable regulations for the AC 23.1309-1E required function and provides the most pertinent controls or information instantly and directly to the pilot. For example, the PFD is a single physical unit that always provides the primary display and complies with the requirements of all the following: altitude, airspeed, aircraft heading (direction) and attitude. The PFD is located directly in front of the pilot and used instantly and first by the pilot. A standby or another display intended to be used in the event of failure of the PFD or as a cross reference is an example of a secondary system. For example, a brake control system normally uses the electronic brake system most of the time because of its better performance, but it does not comply with all the requirements. In this case, the mechanical brakes are used as the backup systems; yet, it is consider the primary with regard to meeting the requirements and the electronic brake system is the secondary.</p>	

**Primary system.** A system that provides the primary function. AC 23.1309-1E

**Probable failure conditions.** Those failure conditions anticipated to occur one or more AC 23.1309-1E times during the entire operational life of each airplane. These failure conditions may be determined on the basis of past service experience with similar components in comparable airplane applications. For quantitative assessments, refer to the probability values shown for minor failure conditions in figure 2.

**Probable.** Probable as defined for CS 23.1309(a) as a probable malfunction or failure, is AC 23.1309-1E any single malfunction or failure that is considered likely on the basis of either past service modified experience or analysis with similar components in comparable airplane applications, or both. **Note:** Normally, there is no quantitative analysis intended in this application. This should not be confused with a probable failure condition when used for a safety assessment process.

**PROCESS:** A set of interrelated activities performed to produce a prescribed output or ED79A product. (ED-80 / DO-254)

**Qualitative.** Those analytical processes that assess system and airplane safety in an AC 23.1309-1E objective non-numerical manner.

**Quantitative.** Those analytical processes that apply mathematical methods to assess the AC 23.1309-1E system and airplane safety.

**REDUNDANCY:** Multiple independent means incorporated to accomplish a given function. ED79A

**Reliability.** The determination that a system, subsystem, unit, or part will perform its AC 23.1309-1E intended function for a specified interval under certain operational and environmental conditions.

**Remote failure conditions.** Those failure conditions that are unlikely to occur to each AC 23.1309-1E airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type. For quantitative assessments, refer to the probability values shown for major failure conditions in figure 2.

**REQUIREMENT:** An identifiable element of a function specification that can be validated ED79A and against which an implementation can be verified.

Definition	Source
------------	--------

**RISK:** The combination of the frequency (probability) of an occurrence and its associated ED79A level of severity.

**Secondary system.** A redundancy system that provides the same function as the primary AC 23.1309-1E system.

**Similarity.** The process of showing that the equipment type, form, function, design, and AC 23.1309-1E installation have only minor differences to previously approved equipment. The safety and operational characteristics and other qualities of the new proposed installation should have no appreciable effects on the airworthiness of the airplane.

**SIMILARITY:** Applicable to systems similar in characteristics and usage to systems used on ED79A previously certificated aircraft. In principle, there are no parts of the subject system more at risk (due to environment or installation) and that operational stresses are no more severe than on the previously certificated aircraft.

**Single failure concept.** The objective of this design concept is to permit the airplane to AC 23.1309-1E continue safe flight and landing after any single failure. Protection from multiple malfunctions or failures should be provided when the first malfunction or failure would not be detected during normal operations of the airplane, which includes preflight checks, or if the first malfunction or failure would inevitably cause other malfunctions or failures.

**SOFTWARE:** Computer programs, procedures, rules, and any associated documentation ED79A pertaining to the operation of a computer system.

**SPECIFICATION:** A collection of requirements which, when taken together, constitute ED79A the criteria that define the functions and attributes of a system, component or item.

**SYSTEM SAFETY ASSESSMENT:** A systematic, comprehensive evaluation of the ED79A implemented system to show that the relevant safety requirements are met.

**SYSTEM:** A combination of inter-related items arranged to perform a specific function(s). ED79A

**TRACEABILITY:** The recorded relationship established between two or more elements of ED79A the development process. For example, between a requirement and its source or between a verification method and its requirement.

**VALIDATION:** The determination that the requirements for a product are correct and ED79A complete. [Are we building the right aircraft/ system/ function/ item?]

**VERIFICATION:** The evaluation of an implementation of requirements to determine that ED79A they have been met. [Did we build the aircraft/ system/ function/ item right?]

**Warning.** A clear and unambiguous indication to the flight crew or pilot of a failure that AC 23.1309-1E requires immediate corrective action. An inherent characteristic of the airplane or a device that will give clearly distinguishable indications of malfunction or misleading information may provide this warning.

**ZONAL SAFETY Analysis:** The safety analysis standard with respect to installation, ED79A interference between systems, and potential maintenance errors that can affect system safety.

## 13. Guidance on the calculation of the average probability per flight hour

The purpose of this material is to provide guidance for calculating the "average probability per flight hour" for a failure condition so that it can be compared with the quantitative requirements set in this CRI as AMC to CS 23.1309. The process of calculating the "average probability per flight hour" for a failure condition is a four-step process and based on the assumption that the life of an aircraft is a sequence of "average flights."

- a) Determination of the "average flight;"
- b) Calculation of the probability of a failure condition for a certain "average flight;"
- c) Calculation of the "average probability per flight" of a failure condition; and
- d) Calculation of the "average probability per flight hour" of a failure condition.

**a. Determination of the "average flight:"** The "average probability per flight hour" is to be based on an "average flight." The applicant should estimate the average flight duration and average flight profile for the fleet of aircraft to be certified. The average flight duration should be estimated based on the applicant's expectations and historical experience for similar types. The average flight duration should reflect the applicant's best estimate of the cumulative flight hours divided by the cumulative aircraft flights for the service life of the aircraft. The average flight profile should be based on the operating weight and performance expectations for the average aircraft when flying a flight of average duration in an ICAO standard atmosphere. The duration of each flight phase (e.g., takeoff, climb, cruise, descent, approach and landing) in the "average flight" should be based on the average flight profile. Average taxi times for departure and arrival at an average airport should be considered where appropriate and added to the average flight time to obtain "average flight-block time." The average flight duration and profile should be used as the basis for determining the "average probability per flight hour" for quantitative safety assessment as means of compliance with this AC.

The probability of a failure condition occurring on an "average flight" should be determined by structured methods (see ARP 4761 for various methods) and should consider all elements (e.g., combinations of failures and events) that contribute to a failure condition. If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce a failure condition. The probabilities of the basic events (component or part level failures) that contribute to the probability of a failure condition should consider the following:

**(1)** The individual part, component, and assembly failure rates utilized in calculating the "average probability per flight hour" should be estimates of the mature constant failure rates after infant mortality and prior to wear-out. Alternatively, a non-constant failure rate can be used (i.e. Weibull or other accepted means). Inspection intervals or component life limits employed to protect against wear out are to be placed in chapter 4 or 5 of the maintenance manual. In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). Where available, service history of same or similar components in the same or similar environment should be used.

**(2)** If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant "at risk" time for the "average flight." **(3)** If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation has to consider the relevant exposure times (e.g., time intervals between maintenance checks/ inspections). In such cases, the probability of the failure condition increases with the number of flights during the latency period.

**(4)** If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the failure condition occurring on an "average flight." It is assumed that the "average flight" can be divided into  $n$  phases (e.g., phase 1, ..., phase  $n$ ). Let  $T_F$  the "average flight" duration,  $T_j$  the duration of phase  $j$  and  $t_j$  the transition point between  $T_j$  and  $T_{j+1}$ ,  $j = 1, \dots, n$ . I.e.

$$T_F = \sum_{j=1}^n T_j \quad \text{and} \quad t_j - t_{j-1} = T_j ; j = 1, \dots, n$$

Let  $\lambda_j(t)$  the failure rate function during phase  $j$ , i.e. for  $t \in [t_{j-1}, t_j]$ .

Remark:  $\lambda_j(t)$  may be equal 0 for all  $t \in [t_{j-1}, t_j]$  for a specific phase  $j$ .

Let  $P_{\text{Flight}}$  (failure) the probability that the element fails during one certain flight (including nonflying time) and  $P_{\text{Phase } j}$  (failure) the probability that the element fails in phase  $j$ .

Two cases are possible:

- (i) The element is checked operative at the beginning of a certain flight. Then

$$\begin{aligned} P_{\text{Flight}} (\text{failure}) &= \sum_{j=1}^n P_{\text{Phase } j} (\text{failure}) = \sum_{j=1}^n P(\text{failure} | t \in [t_{j-1}, t_j]) \\ &= 1 - \prod_{i=1}^n \exp \left( - \int_{t_{i-1}}^{t_i} \lambda_i(x) dx \right) \end{aligned}$$

- (ii) The state of the item is unknown at the beginning of a certain flight. Then

$$\begin{aligned} P_{\text{Flight}} (\text{failure}) &= P_{\text{prior}} (\text{failure}) \\ &+ (1 - P_{\text{prior}} (\text{failure})) \cdot \left( 1 - \prod_{i=1}^n \exp \left( - \int_{t_{i-1}}^{t_i} \lambda_i(x) dx \right) \right) \end{aligned}$$

where prior (failure) is the probability that the failure of the element has occurred prior to a certain flight.

Note: For the two mathematical operators,  $\prod$  is a product sign and  $\in$  is element of.

**(5)** If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce a failure condition.

**c. Calculation of the “average probability per flight” of a failure condition:** The next step is to calculate the "average probability per flight" for a failure condition, that is, the probability of a failure condition for each flight (which might be different, although all flights are "average flights") during the relevant time (for example, the least common multiple of the exposure times or the aircraft life) have to be calculated, summed up, and divided by the number of flights during that period. The principles of calculating are described below and are in more detail in ARP 4761.

$$P_{\text{Average per Flight}}(\text{failure condition}) = \frac{\sum_{k=1}^N P_{\text{Flight } k}(\text{failure condition})}{N}$$

**Note:** N is the number of all flights during the relevant time, and  $P_{\text{Flight } k}$  is the probability that a failure condition occurs in flight k. In the special case of a duplex system (i.e., one component failure latent, the other detected), this method results in an "average probability per flight," which equals the product of both failure rates multiplied by the "average flight" duration  $T_F$  multiplied by one-half (50 percent) of the relevant exposure time.

**d. Calculation of the “average probability per flight hour” of a failure condition:** Once the "average probability per flight" is calculated, it should be normalized by dividing it by the "average flight" duration  $T_F$  in “flight hours” to obtain the "average probability per flight hour." This quantitative value should be used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant for the failure condition being analysed.

$$P_{\text{Average per FH}}(\text{failure condition}) = \frac{P_{\text{Average per Flight}}(\text{failure condition})}{T_F}$$