The common cause analysis is subdivided into three areas of study:

(1) *Zonal Safety Analysis.* This analysis has the objective of ensuring that the equipment installations within each zone of the aeroplane are at an adequate safety standard with respect to design and installation standards, interference between systems, and maintenance errors. In those areas of the aeroplane where multiple systems and components are installed in close proximity, it should be ensured that the zonal analysis would identify any failure or malfunction which by itself is considered sustainable but which could have more serious effects when adversely affecting other adjacent systems or components.

(2) *Particular Risk Analysis.* Particular risks are defined as those events or influences, which are outside the systems concerned. Examples are fire, leaking fluids, bird strike, tire burst, high intensity radiated fields 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.

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

g. *Safety Assessment Process.* Appendix 2 provides an overview of the safety assessment process.

[Amdt 25/14]
[Amdt 25/24]

# Appendix 2 – Safety Assessment Process Overview

ED Decision 2020/001/R

In showing compliance with CS 25.1309(b), the considerations covered in this AMC should be addressed in a methodical and systematic manner, which ensures that the process and its findings are visible and readily assimilated. This appendix is provided primarily for those who are not familiar with the various methods and procedures generally used in the industry to conduct safety assessments. This guide and Figures A2-1 and A2-2 are not certification checklists, and they do not include all the information provided in this AMC. There is no necessity for them to be used or for the Agency to accept them, in whole or in part, to show compliance with any regulation. Their sole purposes are to assist, by illustrating a systematic approach to safety assessments, to enhance understanding and communication by summarising some of the information provided in this AMC, and to provide some suggestions on documentation. More detailed guidance can be found in Document referenced in paragraph 3b(3). Document referenced in paragraph 3b(2) includes additional guidance on how the safety assessment process relates to the system development process.

a. Define the system and its interfaces, and identify the functions that the system is to perform. Some functions are intended to be protective, i.e. functions preventing the failures in system X from adversely affecting system Y. As the implementation of the functional requirements becomes more developed, care should be taken to identify all protective functions upon which airworthiness will depend. Determine whether or not the system is complex, similar to systems used on other aeroplanes, or conventional. When multiple systems and functions are to be evaluated, consider the relationships between multiple safety assessments.

b. Identify and classify failure conditions. All relevant engineering organisations, such as systems, structures, propulsion, and flight test, should be involved in this process. This identification and classification may be done by conducting an FHA, which is usually based on one of the following methods, as appropriate:

   (1) If the system is not complex and its relevant attributes are similar to those of systems used on other aeroplanes, the identification and classification may be derived from design and installation appraisals and the service experience of the comparable, previously approved systems.

   (2) If the system is complex, it is necessary to systematically postulate the effects on the safety of the aeroplane and its occupants resulting from any possible failures, considered both individually and in combination with other failures or events.

c. Choose the means to be used to determine compliance with CS 25.1309. The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system failure conditions, and whether or not the system is complex (see Figure A2-2). For major failure conditions, experienced engineering and operational judgement, design and installation appraisals and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For hazardous or catastrophic failure conditions, a very thorough safety assessment is necessary. The early concurrence of EASA on the choice of an acceptable means of compliance should be obtained.

d. Conduct the analysis and produce the data, which are agreed with the certification authority as being acceptable to show compliance. A typical analysis should include the following information to the extent necessary to show compliance:

   (1) A statement of the functions, boundaries, and interfaces of the system.

(2) A list of the parts and equipment of which the system is comprised, including their performance specifications or design standards and development assurance levels if applicable. This list may reference other documents, e.g., European Technical Standard Orders (ETSOs), manufacturers or military specifications, etc.

(3) The conclusions, including a statement of the failure conditions and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that show compliance with the requirements of CS 25.1309.

(4) A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each failure condition (e.g. analysis or ground, flight, or simulator tests). It should also include a description of precautions taken against common-cause failures, provide any data such as component failure rates and their sources and applicability, support any assumptions made, and identify any required flight crew or ground crew actions, including any CCMRs.

e. Assess the analyses and conclusions of multiple safety assessments to ensure compliance with the requirements for all aeroplane-level failure conditions.

f. Prepare compliance statements, maintenance requirements, and flight manual requirements.

*Figure A2-1: Safety Assessment Process Overview*

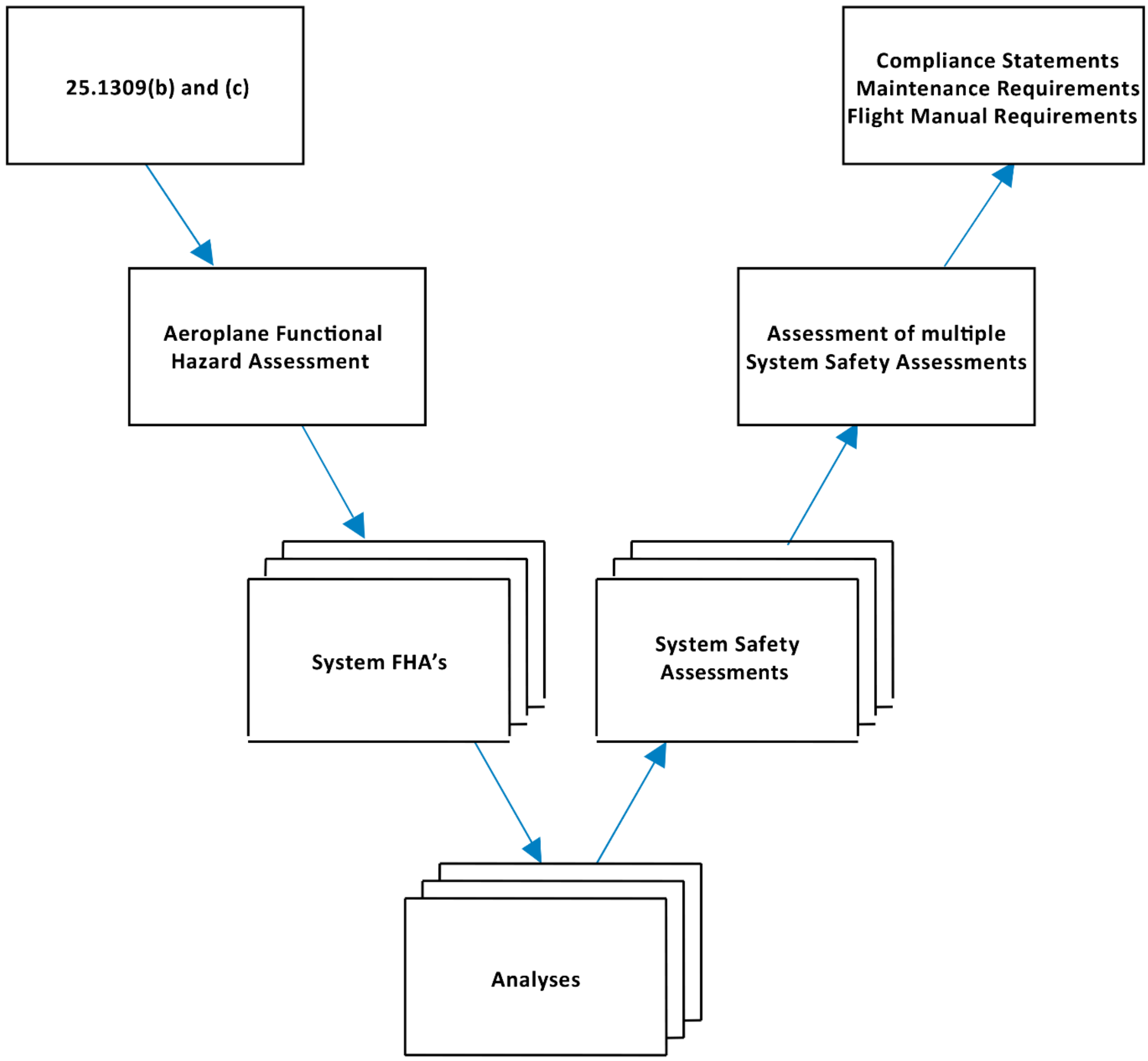
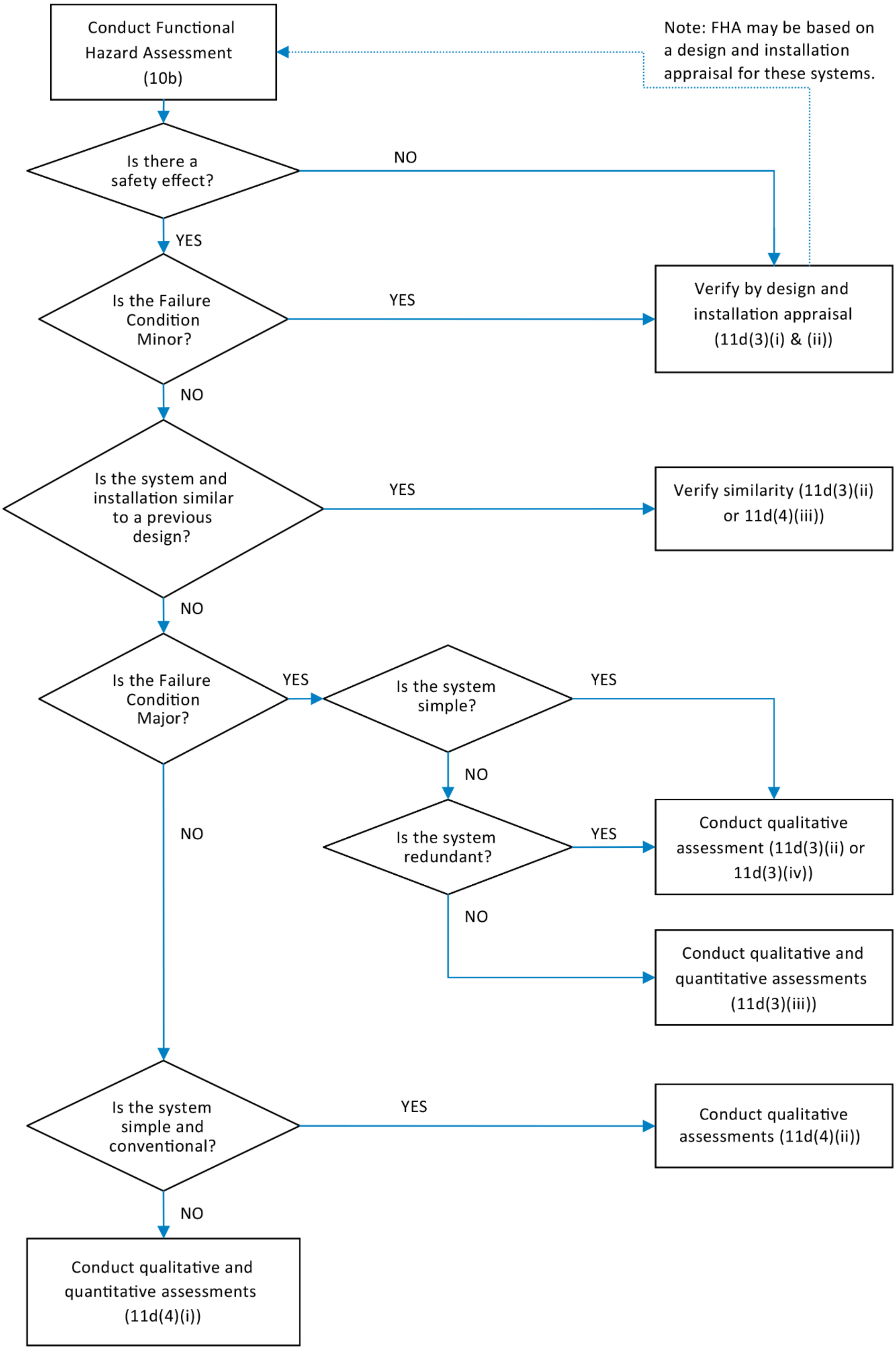


*Figure A2-2: Depth of Analysis Flowchart*



[Amdt 25/2]
[Amdt 25/12]
[Amdt 25/14]
[Amdt 25/24]

# Appendix 3 – Calculation of the average probability per flight hour

ED Decision 2021/015/R

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 criteria of the AMC.

The process of calculating the 'Average Probability per Flight Hour' for a failure condition will be described as a four-step process and is based on the assumption that the life of an aeroplane is a sequence of 'Average Flights'.

Step 1: Determination of the 'Average Flight'

Step 2: Calculation of the probability of a failure condition for a certain 'Average Flight'

Step 3: Calculation of the 'Average Probability per Flight' of a failure condition

Step 4: 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 average flight duration and average flight profile for the fleet of aeroplane to be certified should be estimated. The average flight duration should be estimated based on expectations and historical experience for similar types. The "Average Flight" duration should reflect the best estimate of the cumulative flight hours divided by the cumulative aeroplane flights for the service life of the aeroplane. The "Average Flight" profile should be based on the operating weight and performance expectations for the average aeroplane 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. The "Average Flight" duration and profile should be used as the basis for determining the "Average Probability per Flight Hour" for a quantitative safety assessment.

b. *Calculation of the Probability of a Failure Condition for a certain 'Average Flight'.* The probability of a failure condition occurring on an 'Average Flight' $P_{Flight}$(failure condition) should be determined by structured methods (see Document referenced in paragraph 3.b(3) for example methods) and should consider all significant elements (e.g. combinations of failures and events) that contribute to the failure condition. The following should be considered:

(1) The component failure rates utilised 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. For components whose probability of failure may be associated with non-constant failure rates within the operational life of the aeroplane, a reliability analysis may be used to determine component replacement times (e.g. Weibull analysis). In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). If available, service history of same or similar components in the same or similar environment should be used.

Ageing and wear of similarly constructed and similarly loaded redundant components, whose failure could lead directly, or in combination with one other failure, to a catastrophic or hazardous failure condition, should be assessed when determining scheduled maintenance tasks for such components.

The replacement times, necessary to mitigate the risk due to ageing and wear of such components within the operational life of the aeroplane, should be assessed through the same methodology like other scheduled maintenance tasks that are required to comply with CS 25.1309 (refer to AMC 25-19 for guidance) and documented in the Airworthiness Limitations Section of the Instructions for Continued Airworthiness, as appropriate.

(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 should consider the relevant exposure times (e.g. time intervals between maintenance and operational 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 (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, ... ,n . I.e.

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

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

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

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

Two cases are possible:

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

$$P_{Flight}(Failure) = \sum_{j=1}^{n} P_{Phase\ j}\,(Failure) = \sum_{j=1}^{n} P\big(Failure \mid t \in [t_{j-1}, t_j]\big)$$

$$= 1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)$$

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

$$P_{Flight}(Failure) = P_{prior}(Failure)$$

$$+ \big(1 - P_{prior}(Failure)\big) \cdot \left(1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)\right)$$

where $P_{prior}$ (Failure) is the probability that the failure of the element has occurred prior to the certain flight.

(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 the 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 the failure condition, i.e. the probability of the failure condition for each flight (which might be different although all flights are 'Average Flights') during the relevant time (e.g. the least common multiple of the exposure times or the aeroplane life) should be calculated, summed up and divided by the number of flights during that period. The principles of calculating are described below and also in more detail in the Document referenced in paragraph 3.b(3).

$$P_{Average\ per\ Flight}(Failure\ Condition) = \frac{\sum_{k=1}^{N} P_{FLight\ k}(Failure\ Condition)}{N}$$

Where N is the quantity of all flights during the relevant time, and $P_{Flightk}$ is the probability that the Failure Condition occurs in flight k.

d. *Calculation of the Average Probability per Flight Hour of a Failure Condition.* Once the "Average Probability per Flight" has been calculated it should be normalised by dividing it by the "Average Flight" duration TF 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.

$$P_{Average\ per\ FH}(Failure\ Condition) = \frac{P_{Average\ per\ Flight}(Failure\ Condition)}{T_F}$$

[Amdt 25/14]
[Amdt 25/24]
Amdt 25/27]

# Appendix 4 – Allowable Probabilities

*ED Decision 2020/001/R*

The following probabilities may be used for environmental conditions and operational factors (not caused by aeroplane failures) in quantitative safety analyses:

*Environmental Factors*

| Condition | Model or other Justification | Probability |
|---|---|---|
| CS-25 Appendix C icing conditions | | 1 |
| CS-25 Appendix O icing conditions | | $10^{-2}$ per flight hour |
| Icing conditions beyond certified conditions (considered as 'Severe icing') | | No accepted standard data |
| Head wind >25 kt during takeoff and landing | AC 120-28<br>CS-AWO | $10^{-2}$ per flight |
| Tail wind >10 kt during takeoff and landing | AC 120-28<br>CS-AWO | $10^{-2}$ per flight |
| Cross wind >20 kt during takeoff and landing | AC 120-28<br>CS-AWO | $10^{-2}$ per flight |
| Limit design gust and turbulence | CS 25.341 (Under review by Structures Harmonisation Working Group) | $10^{-5}$ per flight hour |
| Air temperature < -70°C | | No accepted standard data |

*Aeroplane Configurations*

| Configuration | Model or other Justification | Probability |
|---|---|---|
| Centre of gravity | Standard industry practice | Uniform over approved range |
| Landing and Takeoff Weights/Masses | Standard industry practice | Uniform over approved range |

*Flight Conditions*

| Condition | Model or other Justification | Probability |
|---|---|---|
| Flight condition requiring Stall Warning | Assumption | $10^{-2}$ per flight |
| Flight condition resulting in a Stall | Assumption | $10^{-5}$ per flight |
| Excessiveness of $V_{MO}/M_{MO}$ | Assumption | $10^{-2}$ per flight |
| Flight condition greater than or equal to 1.5 g | | No accepted standard data |
| Flight condition less than or equal to 0 g | | No accepted standard data |

*Mission Dependencies*

| Event | Model or other Justification | Probability |
|---|---|---|
| Any rejected take-off | | No accepted standard data |
| High energy rejected take-off | | No accepted standard data |
| Need to jettison fuel | | No accepted standard data |
| Go-around | | No accepted standard data |

*Other Events*

| Event | Model or other Justification | Probability |
|---|---|---|
| Fire in a lavatory not caused by aeroplane failures | | No accepted standard data |
| Fire in a cargo compartment not caused by aeroplane failures | | No accepted standard data |

Notes:

1. If "No accepted standard data" appears in the above tables, the applicant must provide a justified value if a probability less than 1 is to be used in the analysis.
2. The probabilities quoted in this Appendix have been found to be appropriate for use in the context of a quantitative safety analysis performed to demonstrate compliance with CS 25.1309. They may not always be appropriate for use in the context of other requirements.

[Amdt 25/24]