(1) Probable failure conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane.

(2) Remote failure conditions are those unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type.

(3) Extremely remote failure conditions are those not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type.

(4) Extremely improbable failure conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type.

c. Quantitative Probability Terms.

When using quantitative analyses to help determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in this requirement and this AMC have become commonly accepted as aids to engineering judgement. They are expressed in terms of acceptable ranges for the average probability per flight hour.

(1) Probability Ranges.

(i) Probable failure conditions are those having average probability per flight hour greater than of the order of 1×10^{-5}.

(ii) Remote failure conditions are those having an average probability per flight hour of the order of 1×10^{-5} or less, but greater than of the order of 1×10^{-7}.

(iii) Extremely remote failure conditions are those having an average probability per flight hour of the order of 1×10^{-7} or less, but greater than of the order of 1×10^{-9}.

(iv) Extremely improbable failure conditions are those having an average probability per flight hour of the order of 1×10^{-9} or less.

8. SAFETY OBJECTIVE.

a. The objective of CS 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the aeroplane. A logical and acceptable inverse relationship must exist between the average probability per flight hour and the severity of failure condition effects, as shown in Figure 1, such that:

(1) Failure conditions with no safety effect have no probability requirement.

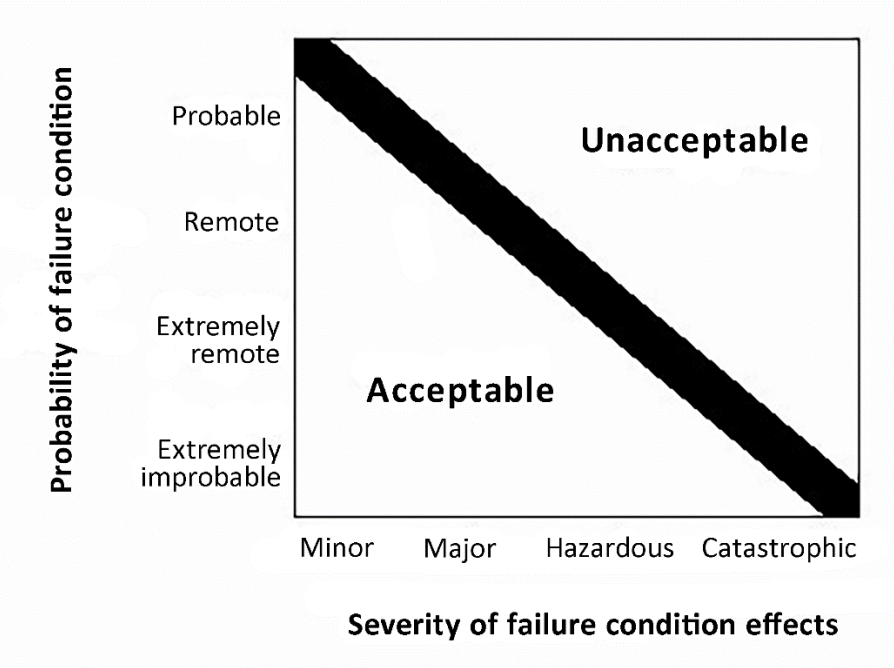
(2) Minor failure conditions may be probable.

(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.

Figure 1: Relationship between Probability and Severity of Failure Condition Effects



b. The classification of the failure conditions associated with the severity of their effects are described in Figure 2a.

The safety objectives associated with failure conditions are described in Figure 2b.

Figure 2a: Relationship Between Severity of the Effects and Classification of Failure Conditions

Severity of the Effects	Effect on Aeroplane	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 excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
	Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of Failure Conditions		No Safety Effect	Minor	Major	Hazardous	Catastrophic

Figure 2b: Relationship Between Classification of Failure Conditions and Probability

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Qualitative Probability	No Probability Requirement	<-Probable->	<--Remote-->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative	No Probability Requirement	<---------->	<---------->	<---------->	

Probability: Average Probability per Flight Hour on the Order of:		$<10^{-3}$ Note 1	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$

Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

c. The safety objectives associated with catastrophic failure conditions must be satisfied by demonstrating that:

(1) No single failure will result in a catastrophic failure condition; and

(2) Each catastrophic failure condition is extremely improbable; and

(3) Given that a single latent failure has occurred on a given flight, each catastrophic failure condition, resulting from two failures, either of which is latent for more than one flight, is remote.

9. COMPLIANCE WITH CS 25.1309.

This paragraph describes specific means of compliance for CS 25.1309. The applicant should obtain early concurrence of the certification authority on the choice of an acceptable means of compliance.

a. Compliance with CS 25.1309(a).

(1) Equipment covered by CS 25.1309(a)(1) must be shown to function properly when installed. The aeroplane operating and environmental conditions over which proper functioning of the equipment, systems, and installation is required to be considered includes the full normal envelope of the aeroplane as defined by the Aeroplane Flight Manual operating limitations together with any modification to that envelope associated with abnormal or emergency procedures. Other external environmental conditions such as atmospheric turbulence, HIRF, lightning, and precipitation, which the aeroplane is reasonably expected to encounter, should also be considered. The severity of the external environmental conditions, which should be considered, are limited to those established by certification standards and precedence.

(2) In addition to the external operating and environmental conditions, the effect of the environment within the aeroplane should be considered. These effects should include vibration and acceleration loads, variations in fluid pressure and electrical power, fluid or vapour contamination, due either to the normal environment or accidental leaks or spillage and handling by personnel. Document referenced in paragraph 3b(1) defines a series of standard environmental test conditions and procedures, which may be used to support compliance. Equipment covered by (CS) Technical Standard Orders containing environmental test procedures or equipment qualified to other environmental test standards can be used to support compliance. The conditions under which the installed equipment will be operated should be equal to or less severe than the environment for which the equipment is qualified.

(3) The required substantiation of the proper functioning of equipment, systems, and installations under the operating and environmental conditions approved for the aeroplane may be shown by test and/or analysis or reference to comparable

service experience on other aeroplanes. It must be shown that the comparable service experience is valid for the proposed installation. For the equipment systems and installations covered by CS 25.1309(a)(1), the compliance demonstration should also confirm that the normal functioning of such equipment, systems, and installations does not interfere with the proper functioning of other equipment, systems, or installations covered by CS 25.1309(a)(1).

(4) The equipment, systems, and installations covered by CS 25.1309(a)(2) are typically those associated with amenities for passengers such as passenger entertainment systems, in-flight telephones, etc., whose failure or improper functioning in itself should not affect the safety of the aeroplane. Operational and environmental qualification requirements for those equipment, systems, and installations are reduced to the tests that are necessary to show that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by CS 25.1309(a)(1) and does not otherwise adversely influence the safety of the aeroplane or its occupants. Examples of adverse influences are: fire, explosion, exposing passengers to high voltages, etc. Normal installation practices should result in sufficiently obvious isolation so that substantiation can be based on a relatively simple qualitative installation evaluation. If the possible impacts, including failure modes or effects, are questionable, or isolation between systems is provided by complex means, more formal structured evaluation methods may be necessary.

b. Compliance with CS 25.1309(b).

Paragraph 25.1309(b) requires that the aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that any catastrophic failure condition is extremely improbable and does not result from a single failure. It also requires that any hazardous failure condition is extremely remote, and that any major failure condition is remote. An analysis should always consider the application of the fail-safe design concept described in paragraph 6.b, and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions.

(1) *General.* Compliance with the requirements of CS 25.1309(b) should be shown by analysis and, where necessary, by appropriate ground, flight, or simulator tests. Failure conditions should be identified and their effects assessed. The maximum allowable probability of the occurrence of each failure condition is determined from the failure condition's effects, and when assessing the probabilities of failure conditions, appropriate analysis considerations should be accounted for. Any analysis must consider:

(i) Possible failure conditions and their causes, modes of failure, and damage from sources external to the system.

(ii) The possibility of multiple failures and undetected failures.

(iii) The possibility of requirement, design and implementation errors.

(iv) The effect of reasonably anticipated crew errors after the occurrence of a failure or failure condition.

(v) The effect of reasonably anticipated errors when performing maintenance actions.

(vi) The crew alerting cues, corrective action required, and the capability of detecting faults.

(vii) The resulting effects on the aeroplane and occupants, considering the stage of flight, the sequence of events/failures occurrence when relevant, and operating and environmental conditions.

(2) *Planning.* This AMC provides guidance on methods of accomplishing the safety objective. The detailed methodology needed to achieve this safety objective will depend on many factors, in particular the degree of systems complexity and integration. For aeroplanes containing many complex or integrated systems, it is likely that a plan will need to be developed to describe the intended process. This plan should include consideration of the following aspects:

(i) Functional and physical interrelationships of systems.

(ii) Determination of detailed means of compliance, which should include development assurance activities.

(iii) Means for establishing the accomplishment of the plan.

(3) *Availability of Industry Standards and Guidance Materials*. There are a variety of acceptable techniques currently being used in industry, which may or may not be reflected in the documents referenced in paragraphs 3.b(2) and 3.b(3). This AMC is not intended to compel the use of these documents during the definition of the particular method of satisfying the objectives of this AMC. However, these documents do contain material and methods of performing the system safety assessment. These methods, when correctly applied, are recognised by EASA as valid for showing compliance with CS 25.1309(b). In addition, the Document referenced in paragraph 3.b(3) contains tutorial information on applying specific engineering methods (e.g. Markov analysis, fault tree analysis) that may be utilised in whole or in part.

(4) *Acceptable Application of Development Assurance Methods*. Paragraph 9.b(1)(iii) above requires that any analysis necessary to demonstrate compliance with CS 25.1309(b) must consider the possibility of development errors. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterising the performance of the system. These direct techniques may still be appropriate for systems containing non-complex items (i.e. items that are fully assured by a combination of testing and analysis) that perform a limited number of functions and that are not highly integrated with other aeroplane systems. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests that must be accomplished. For these types of systems, compliance may be demonstrated by the use of development assurance. The level of development assurance (function development assurance level (FDAL)/item development assurance level (IDAL)) should be commensurate with the severity of the failure conditions the system is contributing to.

Guidelines, which may be used for the assignment of development assurance levels to aeroplanes and system functions (FDAL) and to items (IDAL), are described in the Document referenced in 3.b(2) above. Through this Document, EASA

recognises that credit can be taken from system architecture (e.g. functional or item development independence) for the FDAL/IDAL assignment process.

Guidelines, which may be used for providing development assurance, are described for aeroplane and system development in the Document referenced in 3.b(2), and for software in the Document referenced in 3.a(3) above. (There is currently no agreed development assurance standard for airborne electronic hardware.)

(5) *Crew and Maintenance Actions*.

(i) Where an analysis identifies some indication to, and/or action by, the flight crew, cabin crew, or maintenance personnel, the following activities should be accomplished:

1 Verify that any identified indications are actually provided by the system. This includes the verification that the elements that provide detection (e.g. sensors, logic) properly trigger the indication under the relevant situations considering various causes, flight phases, operating conditions, operational sequences, and environments.

2 Verify that any identified indications will, in fact, be recognised.

3 Verify that any actions required have a reasonable expectation of being accomplished successfully and in a timely manner.

(ii) These verification activities should be accomplished by consulting with engineers, pilots, flight attendants, maintenance personnel, and human factors specialists, as appropriate, taking due consideration of any relevant service experience and the consequences if the assumed action is not performed or performed improperly.

(iii) In complex situations, the results of the review by specialists may need to be confirmed by simulator, ground tests, or flight tests. However, quantitative assessments of the probabilities of crew or maintenance errors are not currently considered feasible. If the failure indications are considered to be recognisable and the required actions do not cause an excessive workload, then for the purposes of the analysis, such corrective actions can be considered to be satisfactorily accomplished. If the necessary actions cannot be satisfactorily accomplished, the tasks and/or the systems need to be modified.

(6) *Significant Latent Failures.*

(i) Compliance with CS 25.1309(b)(4)

For compliance with CS 25.1309(b)(4), the hereafter systematic approach should be followed:

1. The applicant must first eliminate significant latent failures to the maximum practical extent utilising the current state-of-the-art technology, e.g. implement practical and reliable failure monitoring and flight crew indication systems to detect failures that would otherwise be latent for more than one flight. Additional guidance is provided in AMC 25-19 Section 8, Design Considerations Related to Significant Latent Failures.

2. For each significant latent failure which cannot reasonably be eliminated, the applicant must minimise the exposure time by design utilising current state-of-the-art technology rather than relying on scheduled maintenance tasks at lengthy intervals, i.e. implementing pilot-initiated checks, or self-initiated checks (e.g. first flight of the day check, power-up built-in tests, other system automated checks).

3. When relying on scheduled maintenance tasks, quantitative as well as qualitative aspects need to be addressed when limiting the latency. Additional guidance is provided in AMC 25-19 Section 10, Identification of Candidate CMRs (CCMRs).

Note: For turbojet thrust reversing systems, the design configurations in paragraphs 8.b(2) and 8.b(3) of AMC 25.933(a)(1) have traditionally been considered to be acceptable to EASA for compliance with CS 25.1309(b)(4).

(ii) Compliance with CS 25.1309(b)(5)

When a catastrophic failure condition involves two failures, either one of which is latent for more than one flight, and cannot reasonably be eliminated, compliance with CS 25.1309(b)(5) is required. Following the proper application of CS 25.1309(b)(4), the failure conditions involving multiple significant latent failures are expected to be sufficiently unlikely such that the dual-failure situations addressed in CS 25.1309(b)(5) are the only remaining significant latent failures of concern.

These significant latent failures of concern should be highlighted to EASA as early as possible. The system safety assessment should explain why avoidance is not practical, and provide supporting rationale for the acceptability. Rationale should be based on the proposed design being state-of-the-art, past experience, sound engineering judgment, or other arguments, which led to the decision not to implement other potential means of avoidance (e.g. eliminating the significant latent failure or adding redundancy).

Two criteria are implemented in CS 25.1309(b)(5): limit latency and limit residual probability.

Limit latency is intended to limit the time of operating with one evident failure away from a catastrophic failure condition. This is achieved by requiring that the sum of the probabilities of the latent failures, which are combined with each evident failure, does not exceed 1/1 000. Taking one catastrophic failure condition at a time,

— in case an evident failure is combined only once in a dual failure combination of concern, the probability of the individual latent failure needs to comply with the 1/1 000 criterion;

— in case an evident failure is combined in multiple dual failure combinations of concern, the combined probabilities of the latent failures need to comply with the 1/1 000 criterion.

Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be ‘remote’. Residual probability is the combined average probability per flight hour of

all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred.

These requirements are applied in addition to CS 25.1309(b)(1), which requires that catastrophic failure conditions be shown to be extremely improbable and do not result from a single failure.

Appendix 5 provides simplified examples explaining how the limit latency and limit residual probability analysis might be applied.

For compliance with the 1/1 000 criterion, the probability of the latent failures of concern should be derived from the probability of the worst-case flight, i.e. the probability where the evident failure occurs in the last flight before the scheduled maintenance inspection, while the latent failure may have occurred in any flight between two consecutive scheduled maintenance inspections. When dealing with constant failure rates, the probability of the latent failure should be computed as the product of the maximum time during which the failure may be present (i.e. exposure time) and its failure rate, if this probability is less than or equal to 0.1.

c. Compliance with CS 25.1309(c).

CS 25.1309(c) requires that information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action in a timely manner, thereby mitigating the effects to an acceptable level. Any system operating condition that, if not detected and properly accommodated by flight crew action, would contribute to or cause a hazardous or catastrophic failure condition should be considered to be an 'unsafe system operating condition'. Compliance with this requirement is usually demonstrated by the analysis identified in paragraph 9.b(1) above, which also includes consideration of crew alerting cues, corrective action required, and the capability of detecting faults. The required information may be provided by dedicated indication and/or annunciation or made apparent to the flight crew by the inherent aeroplane/systems responses. When flight crew alerting is required, it must be provided in compliance with CS 25.1322. CS 25.1309(c) also requires that installed systems and equipment for use by the flight crew, including flight deck controls and information, be designed to minimise flight crew errors that could create additional hazards (in compliance with CS 25.1302).

(1) The required information will depend on the degree of urgency for recognition and corrective action by the crew. It should be in the form of:

(i) a warning, if immediate recognition and corrective or compensatory action by the crew is required;

(ii) a caution if immediate crew awareness is required and subsequent crew action will be required;

(iii) an advisory, if crew awareness is required and subsequent crew action may be required;

(iv) a message in the other cases.

CS 25.1322 (and AMC 25.1322) give further requirements (and guidance) on the characteristics of the information required (visual, aural) based on those different categories.

(2) When failure monitoring and indication are provided by a system, its reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a system failure and not annunciating that system failure are catastrophic, the combination of the system failure with the failure of its annunciation must be extremely improbable. The loss of annunciation itself should be considered a failure condition, and particular attention should be paid to the impact on the ability of the flight crew to cope with the subject system failure. In addition, unwanted operation (e.g. nuisance warnings) should be assessed. The failure monitoring and indication should be reliable, technologically feasible, and economically practical. Reliable failure monitoring and indication should utilise current state-of-the-art technology to maximise the probability of detecting and indicating genuine failures while minimising the probability of falsely detecting and indicating non-existent failures. Any indication should be timely, obvious, clear, and unambiguous.

(3) In the case of aeroplane conditions requiring immediate crew action, a suitable warning indication must be provided to the crew, if not provided by inherent aeroplane characteristics. In either case, any warning should be rousing and should occur at a point in a potentially catastrophic sequence where the aeroplane's capability and the crew's ability still remain sufficient for effective crew action.

(4) Unless they are accepted as normal airmanship, procedures for the crew to follow after the occurrence of failure warning should be described in the approved Aeroplane Flight Manual (AFM) or AFM revision or supplement.

(5) Even if operation or performance is unaffected or insignificantly affected at the time of failure, information to the crew is required if it is considered necessary for the crew to take any action or observe any precautions. Some examples include reconfiguring a system, being aware of a reduction in safety margins, changing the flight plan or regime, or making an unscheduled landing to reduce exposure to a more severe failure condition that would result from subsequent failures or operational or environmental conditions. Information is also required if a failure must be corrected before a subsequent flight. If operation or performance is unaffected or insignificantly affected, information and alerting indications may be inhibited during specific phases of flight where corrective action by the crew is considered more hazardous than no action.

(6) The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. When this is not accomplished, refer to paragraph 9.b(6) for guidance.

Paragraph 12 provides further guidance on the use of periodic maintenance or flight crew checks. Comparison with similar, previously approved systems is sometimes helpful. However, if a new technical solution allows practical and reliable failure monitoring and indications, this should be preferred in lieu of periodic maintenance or flight crew checks.

(7) Particular attention should be given to the placement of switches or other control devices, relative to one another, so as to minimise the potential for inadvertent incorrect crew action, especially during emergencies or periods of high workload. Extra protection, such as the use of guarded switches, may sometimes be needed.

10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS.

a. *Identification of Failure Conditions*.

Failure conditions should be identified by considering the potential effects of failures on the aeroplane and occupants. These should be considered from two perspectives:

(1) by considering failures of aeroplane-level functions — failure conditions identified at this level are not dependent on the way the functions are implemented and the systems' architecture.

(2) by considering failures of functions at the system level — these failure conditions are identified through examination of the way that functions are implemented and the systems' architectures. It should be noted that a failure condition might result from a combination of lower-level failure conditions. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all significant failure conditions, that arise from multiple failures and combinations of lower-level failure conditions, are properly identified and accounted for. The relevant combinations of failures and failure conditions should be determined by the whole safety assessment process that encompasses the aeroplane and system level functional hazard assessments and common-cause analyses. The overall effect on the aeroplane of a combination of individual system failure conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, failure conditions classified as minor or major by themselves may have hazardous effects at an aeroplane level, when considered in combination.

b. *Identification of Failure Conditions Using a Functional Hazard Assessment*.

(1) Before a detailed safety assessment is proceeded with, a functional hazard assessment (FHA) of the aeroplane and system functions to determine the need for and scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgement, and/or a top-down deductive qualitative examination of each function. An FHA is a systematic, comprehensive examination of aeroplane and system functions to identify potential minor, major, hazardous, and catastrophic failure conditions that may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of systems rather than with a detailed analysis of the actual implementation.

(2) Each system function should be examined with respect to the other functions performed by the system, because the loss or malfunction of all functions performed by the system may result in a more severe failure condition than the loss of a single function. In addition, each system function should be examined with respect to functions performed by other aeroplane systems, because the loss or malfunction of different but related functions, provided by separate systems may affect the severity of Failure Conditions postulated for a particular system.

(3) The FHA is an engineering tool, which should be performed early in the design and updated as necessary. It is used to define the high-level aeroplane or system safety objectives that must be considered in the proposed system architectures. It should also be used to assist in determining the development assurance levels for the