q. **Quantitative.** Those analytical processes that apply mathematical methods to assess system and aeroplane safety.

t. **Redundancy.** The presence of more than one independent means for accomplishing a given function or flight operation.

s. **System.** A combination of components, parts, and elements, which are inter-connected to perform one or more functions.

6. **BACKGROUND**

a. **General.**

For a number of years aeroplane systems were evaluated to specific requirements, to the "single fault" criterion, or to the fail-safe design concept. As later-generation aeroplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the aeroplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions. This has led to the general principle that an inverse relationship should exist between the probability of a Failure Condition and its effect on the aeroplane and/or its occupants (see Figure 1). In assessing the acceptability of a design it was recognised that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 percent of the total were attributed to Failure Conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such Failure Conditions be not greater than one per ten million flight hours or $1 \times 10^{-7}$ per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason it was assumed, arbitrarily, that there are about one hundred potential Failure Conditions in an aeroplane, which could be Catastrophic. The target allowable Average Probability per Flight Hour of $1 \times 10^{-7}$ was thus apportioned equally among these Failure Conditions, resulting in an allocation of not greater than $1 \times 10^{-9}$ to each. The upper limit for the Average Probability per Flight Hour for Catastrophic Failure Conditions would be $1 \times 10^{-9}$, which establishes an approximate probability value for the term "Extremely Improbable". Failure Conditions having less severe effects could be relatively more likely to occur.

b. **Fail-Safe Design Concept.**

The Part 25 airworthiness standards are based on, and incorporate, the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

(1) The following basic objectives pertaining to failures apply:

(i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be Catastrophic.

(ii) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

(2) The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e. to ensure that Major Failure Conditions are Remote, Hazardous Failure Conditions are Extremely Remote, and Catastrophic Failure Conditions are Extremely Improbable:

(i) **Designed Integrity and Quality,** including **Life Limits,** to ensure intended function and prevent failures.
(ii) **Redundancy or Backup Systems** to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(iii) **Isolation and/or Segregation of Systems, Components, and Elements** so that the failure of one does not cause the failure of another.

(iv) **Proven Reliability** so that multiple, independent failures are unlikely to occur during the same flight.

(v) **Failure Warning or Indication** to provide detection.

(vi) **Flight crew Procedures** specifying corrective action for use after failure detection.

(vii) **Checkability:** the capability to check a component's condition.

(viii) **Designed Failure Effect Limits**, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(ix) **Designed Failure Path** to control and direct the effects of a failure in a way that limits its safety impact.

(x) **Margins or Factors of Safety** to allow for any undefined or unforeseeable adverse conditions.

(xi) **Error-Tolerance** that considers adverse effects of foreseeable errors during the aeroplane's design, test, manufacture, operation, and maintenance.

c. **Highly Integrated Systems.**

(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of highly integrated systems that perform complex and interrelated functions, particularly through the use of electronic technology and software based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems. Thus, other assurance techniques, such as development assurance utilising a combination of process assurance and verification coverage criteria, or structured analysis or assessment techniques applied at the aeroplane level, if necessary, or at least across integrated or interacting systems, have been applied to these more complex systems. Their systematic use increases confidence that errors in requirements or design, and integration or interaction effects have been adequately identified and corrected.

(2) Considering the above developments, as well as revisions made to the CS 25.1309, this AMC was revised to include new approaches, both qualitative and quantitative, which may be used to assist in determining safety requirements and establishing compliance with these requirements, and to reflect revisions in the rule, considering the whole aeroplane and its systems. It also provides guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analysis. The analytical tools used in determining numerical values are intended to supplement, but not replace, qualitative methods based on engineering and operational judgement.

7. **FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS**

a. **Classifications.** 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; for example, Failure Conditions that would not affect the operational capability of the aeroplane or increase crew workload.

(2) **Minor:** Failure Conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, 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 which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

(4) Hazardous: Failure Conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions, to the extent that there would be:

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

(ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or

(iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

(5) Catastrophic: Failure Conditions, which would result in multiple fatalities, usually with the loss of the aeroplane. (Note: A “Catastrophic” Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)

b. Qualitative Probability Terms.

When using qualitative analyses to determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in CS 25.1309 and this AMC have become commonly accepted as aids to engineering judgement:

(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 an Average Probability Per Flight Hour greater than of the order of $1 \times 10^{-5}$.

(ii) Remote Failure Conditions are those having an Average Probability Per Flight Hour of the order of $1 \times 10^{-5}$ or less, but greater than of the order of $1 \times 10^{-7}$.

(iii) Extremely Remote Failure Conditions are those having an Average Probability Per Flight Hour of the order of $1 \times 10^{-7}$ or less, but greater than of the order of $1 \times 10^{-9}$.
(iv) Extremely Improbable Failure Conditions are those having an Average Probability Per Flight Hour of the order of $1 \times 10^{-9}$ 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 safety objectives associated with Failure Conditions are described in Figure 2.
The safety objectives associated with Catastrophic Failure Conditions, may 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.

d. Exceptionally, for paragraph 8c(2) above of this AMC, if it is not technologically or economically practicable to meet the numerical criteria for a Catastrophic Failure Condition, the safety objective may be met by accomplishing all of the following:

(1) Utilising well proven methods for the design and construction of the system; and

```
<table>
<thead>
<tr>
<th>Effect on Aeroplane</th>
<th>No effect on operational capabilities or safety</th>
<th>Slight reduction in functional capabilities or safety margins</th>
<th>Significant reduction in functional capabilities or safety margins</th>
<th>Large reduction in functional capabilities or safety margins</th>
<th>Normally with hull loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effect on Occupants excluding Flight Crew</td>
<td>Inconvenience</td>
<td>Physical discomfort</td>
<td>Physical distress, possibly including injuries</td>
<td>Serious or fatal injury to a small number of passengers or cabin crew</td>
<td>Multiple fatalities</td>
</tr>
<tr>
<td>Effect on Flight Crew</td>
<td>No effect on flight crew</td>
<td>Slight increase in workload</td>
<td>Physical discomfort or a significant increase in workload</td>
<td>Physical distress or excessive workload impairs ability to perform tasks</td>
<td>Fatalities or incapacitation</td>
</tr>
<tr>
<td>Allowable Qualitative Probability</td>
<td>No Probability Requirement</td>
<td>↓Probability→Remote→</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:</td>
<td>No Probability Requirement</td>
<td>&lt;10^{-3} Note 1</td>
<td>&lt;10^{-5}</td>
<td>&lt;10^{-7}</td>
<td>&lt;10^{-9}</td>
</tr>
<tr>
<td>Classification of Failure Conditions</td>
<td>No Safety Effect</td>
<td>↓Safety→Minor→Major→Hazardous→</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

```

**Figure 2: Relationship Between Probability and Severity of Failure Condition**
(2) Determining the Average Probability per Flight Hour of each Failure Condition using structured methods, such as Fault Tree Analysis, Markov Analysis, or Dependency Diagrams; and

(3) Demonstrating that the sum of the Average Probabilities per Flight Hour of all Catastrophic Failure Conditions caused by systems is of the order of $10^{-7}$ or less (See paragraph 6a for background).

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 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 operating envelope of the aeroplane as defined by the Aeroplane Flight Manual 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.

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 6b, and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events