ADVISORY MATERIAL JOINT – AMJ

AMJ 25.1309
System Design and Analysis
See JAR 25.1309

1 PURPOSE

This AMJ is similar to FAA Advisory Circular AC 25.1309-1A, dated 21 June 1988. Differences between the two texts are indicated, in accordance with normal JAA practice, by underlining.

This AMJ describes various acceptable means for showing compliance with the requirements of JAR 25.1309 (b), (c) and (d). These means are intended to provide guidance for the experienced engineering and operational judgement that must form the basis for compliance findings. They are not mandatory. Other means may be used if they show compliance with this section of the requirements.

2 RESERVED

3 APPLICABILITY

Paragraph 25.1309 is intended by the Joint Aviation Authorities (JAA) as a general requirement that should be applied to all systems and Powerplant installations (as required by JAR 25.901(c)) to determine the effect on the aeroplane of a functional failure or malfunction. It is based on the principle that there should be an inverse relationship between the severity of the effect of a failure and the probability of its occurrence.

This principle may in some instances be at variance with specific paragraphs elsewhere in JAR–25. That is to say that a specific requirement may call for a higher safety objective than is warranted in relation to the effect it has on the particular aeroplane type. In other instances the reverse may apply.

The JAA will consider such instances on a case-by-case basis, and such instances would be the subject of negotiation with the applicant in a specific case. However, notwithstanding that a forcible argument to replace or alter the requirements of a specific paragraph may exist, it may not necessarily justify the waiving of a long-established tradition of engineering practice.

4 BACKGROUND

a. 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 loss of function(s) or malfunction(s) (leading to a serious Failure Condition) and the degree of hazard to the aeroplane and its occupants arising therefrom. In assessing the acceptability of a design it was recognised that rational probability values would have to be established. This was worked out on the following basis:

AMJ 25.1309 (continued)

Historical evidence indicates that the risk of a serious accident due to operational and airframe-related causes is approximately 1 per million hours of flight. Furthermore, about 10 percent of the total can be attributed to Failure Conditions caused by the aeroplane's systems problems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is thereby possible to require for new designs that the probability of a serious accident from all such Failure Conditions be not greater than 1 per ten million flight hours or 1×10^{-7} per flight hour.

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 is assumed, arbitrarily, that there are about 100 potential Failure Conditions in an aeroplane which would prevent Continued Safe Flight and Landing. The target allowable risk of 1×10^{-7} was thus apportioned equally among these Conditions, resulting in a risk allocation of not greater than 1×10^{-9} to each. The upper-risk limit for Failure Conditions which would prevent Continued Safe Flight and Landing would be 1×10^{-9} for each hour of flight which establishes an approximate probability value for the term "Extremely Improbable". Failure Conditions having less severe effects could be relatively more likely to occur.

In parallel with the above, various analytical techniques were developed to assist the applicant and Airworthiness Authority in conducting a safety analysis. These help to carry out a thorough qualitative analysis. The techniques also allow the analyst to carry out a quantitative assessment as and when appropriate.

b. This AMJ identifies various analytical approaches, both qualitative and quantitative, which may be used to assist applicant and JAA personnel in determining compliance with the requirement. It also provides guidance for determining when, or if, a particular analysis should be conducted. Numerical values are assigned to the probabilistic terms included in the requirement, for use in those cases where the impact of system failures is examined by quantitative methods of analysis. These analytical tools are intended to supplement, but not replace, engineering and operational judgement.

5 THE FAIL-SAFE DESIGN CONCEPT

The fail-safe design concept considers the effects of failures and combinations of failures in defining a safe design.

a. The following basic objectives pertaining to failures apply:

(1) In any system or subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent Continued Safe Flight and Landing.

(2) 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.

b 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 and Hazardous Failure Conditions are Improbable and that Catastrophic Failure Conditions are Extremely Improbable:

(1) **Designed Integrity and Quality**, including life limits, to ensure intended function and minimise the occurrence and/or the effects of failures.

AMJ 25.1309 (continued)

(2) **Redundancy or Back-Up 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.

(3) **Isolation** (especially physical or spatial separation) and independence of Systems, Components, and elements so that the failure of one does not cause the failure of another.

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

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

(6) **Flightcrew Procedures** for use after failure detection, to enable Continued Safe Flight and Landing by specifying crew corrective action.

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

(8) **Failure Containment** to limit the safety impact of a failure.

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

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

(11) **Margins or Factors of Safety** to account for foreseeable but uncertain or undefined adverse conditions.

6 DEFINITIONS

The following definitions apply to the system design and analysis requirements of JAR 25.1309(b), (c), and (d) and the guidance material provided in this AMJ. They should not be assumed to apply to the same or similar terms used in other requirements, ACJs or AMJs. Terms for which standard dictionary definitions apply are not defined herein.

a. ATTRIBUTE: A feature, characteristic, or aspect of a system or a device, or a condition affecting its operation. Some examples would include design, construction, technology, installation, functions, applications, operational uses, environmental and operational stresses, and relationships with other systems, functions, and flight or structural characteristics.

b. CERTIFICATION CHECK REQUIREMENT (CCR): A recurring flight crew or ground crew Check that is required by design to help show compliance with JAR 25.1309(b) and (d)(2) by detecting the presence of, and thereby limiting the exposure time to, a significant latent failure that would, in combination with one or more other specific failure or events identified in a safety analysis, result in a Hazardous or Catastrophic Failure Condition.

c. CHECK: An examination (e.g. an inspection or test) to determine the physical integrity or functional capability of an item.

d. COMPLEX: Applicable to systems whose architecture and logic are difficult to comprehend without the aid of analytical tools, e.g. Failure Modes and Effects Analysis, Fault Trees, Reliability Block Diagrams.

e. CONTINUED SAFE FLIGHT AND LANDING: The capability for continued controlled flight and landing, possibly using emergency procedures, but without requiring exceptional pilot skill or strength. Some aeroplane damage may be associated with a Failure Condition, during flight or upon landing.

AMJ 25.1309 (continued)

f. CONVENTIONAL: An attribute of a system is considered to be conventional if it is the same as, or closely similar to, that of previously-approved systems that are commonly used.

g. ERROR: An occurrence arising as a result of incorrect action by the flight crew or maintenance personnel.

h. EVENT: An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, cabin and baggage fires. The term is not intended to cover sabotage.

i. FAILURE: A loss of function, or a malfunction, of a system or part thereof.

j. FAILURE CONDITION: The effect on the aeroplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operational or environmental conditions. Failure Conditions may be classified according to their severities as follows:

(1) 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 inconvenience to occupants.

(2) 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 occupants, possibly including injuries.

(3) 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 higher 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.

(4) CATASTROPHIC: Failure Conditions which would prevent Continued Safe Flight and Landing.

k. REDUNDANCY: The presence of more than one independent means for accomplishing a given function or flight operation. Each means need not necessarily be identical.

l. QUALITATIVE: Those analytical processes that assess system and aeroplane safety in a subjective, non-numerical manner.

m. QUANTITATIVE: Those analytical processes that apply mathematical methods to assess system and aeroplane safety.

7 DISCUSSION

JAR 25.1309(b) and (d) require substantiation by analysis and, where necessary, by appropriate ground, flight, or simulator tests, that a logical and acceptable inverse relationship exists between the probability and the severity of each Failure Condition. However, tests are not required to verify Failure Conditions that are postulated to be Catastrophic. As discussed in paragraph 3, some

AMJ 25.1309 (continued)

systems and some functions already receive such an evaluation to show compliance with other specific requirements or special conditions and thereby normally meet the intent of JAR 25.1309 without a need for additional analyses. In either case, however, the goal is to ensure an acceptable overall aeroplane safety level, considering all Failure Conditions of all systems.

a. The requirements of JAR 25.1309(b) and (d) are intended to ensure an orderly and thorough evaluation of the effects on safety of foreseeable failures or other events, such as errors or external circumstances, separately or in combination, involving one or more system functions. The interactions of these factors within a system and among relevant systems should be considered.

b. The severities of Failure Conditions may be evaluated according to the following considerations:

(1) Effects on the aeroplane, such as reductions in safety margins, degradations in performance, loss of capability to conduct certain flight operations, or potential or consequential effects on structural integrity

(2) Effects on crew members, such as increases above their normal workload that would affect their ability to cope with adverse operational or environmental conditions.

(3) Effects on the occupants; i.e. passengers and crew members.

c. For convenience in conducting design assessments, Failure Conditions may be classified according to their severities as Minor, Major, Hazardous, or Catastrophic. Paragraph (6)(j) provides accepted definitions of these terms.

(1) The classification of Failure Conditions does not depend on whether or not a system or function is the subject of a specific requirement. Some “required” systems, such as transponders, position lights, and public address systems, may have the potential for only Minor Failure Conditions. Conversely, other systems which are not “required”, such as flight management systems, may have the potential for Major, Hazardous, or Catastrophic Failure Conditions.

(2) Regardless of the types of assessment used, the classification of Failure Conditions should always be accomplished with consideration of all relevant factors; e.g. system, crew, performance, operational, external, etc. Examples of factors would include the nature of the failure modes, any effects or limitations on performance, and any required or likely crew action. 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 the 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.

d. The probability that a Failure Condition would occur may be assessed as Probable, Improbable (Remote or Extremely Remote), or Extremely Improbable. These terms are explained in paragraph 9.e. and 10.b. Each Failure Condition should have a probability that is inversely related to its severity, as illustrated in figure 1, Relationship between Probability and Severity of Effects:

(1) Minor Failure Conditions may be Probable.

(2) Major Failure Conditions must be no more frequent than Improbable (Remote).

(3) Hazardous Failure Conditions must be no more frequent than Improbable (Extremely Remote).

(4) Catastrophic Failure Conditions must be Extremely Improbable.

AMJ 25.1309 (continued)

e. An assessment to identify and classify Failure Conditions is necessarily qualitative. On the other hand, 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 types of functions performed by the system, the severities of Failure Conditions, and whether or not the system is complex. Regardless of its type, an analysis should show that the system and its installation can tolerate failures to the extent that Major and Hazardous Failure Conditions are Improbable and Catastrophic Failure Conditions are Extremely Improbable (see figure 1):

(1) Experienced engineering and operational judgement should be applied when determining whether nor not a system is complex. Comparison with similar, previously-approved systems, is sometimes helpful. All relevant systems Attributes should be considered; however, the complexity of the software used to program a digital-computer-based system should not be considered because the software is assessed and controlled by other means, as described in paragraph 7.i.

(2) An analysis should consider the application of the fail-safe design concept described in paragraph 5, 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. When considering such common-cause failures or other events, consequential or cascading effects should be taken into account if they would be inevitable or reasonably likely.

(3) Some examples of such potential common-cause failures or other events would include rapid release of energy from concentrated sources such as uncontained failures of rotating parts or pressure vessels, pressure differentials, non-catastrophic stuctural failures, loss of environmental conditioning, disconnection of more than one subsystem or component by overtemperature protection devices, contamination by fluids, damage from localised fires, loss of power, excessive voltage, physical or environmental interactions among parts, human or machine errors, or events external to the system or to the aeroplane.

f. As discussed in paragraphs 8.c.(1) and 8.d.(2), compliance for a system or part thereof that is not complex may sometimes be shown by design and installation appraisals and evidence of satisfactory service experience on other aeroplanes using the same or other systems that are similar in their relevant Attributes.

g. In general, a Failure Condition resulting from a single failure mode of a device cannot be accepted as being Extremely Improbable. In very unusual cases, however, experienced engineering judgement may enable an assessment that such a failure mode is not a practical possibility. When making such an assessment, all possible and relevant considerations should be taken into account, including all relevant Attributes of the device. Service experience showing that the failure mode has not yet occurrred may be extensive, but it can never be enough. Furthermore, flight crew or ground crew checks have no value if a Catastrophic failure mode would occur suddenly and without any prior indication or warning. The assessment's logic and rationale should be so straightforward and readily obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that the failure mode simply would not occur.

h. JAR 25.1309(c) provides requirements for system monitoring, failure warning, and capability for appropriate corrective crew action. Guidance on acceptance means of compliance is provided in paragraph 8.g.

i. In general, the means of compliance described in this AMJ are not directly applicable to software assessments because it is not feasible to assess the number or kinds of software errors, if any, that may remain after the completion of system design, development, and test. RTCA DO-178A and EUROCAE ED-12A, or later revisions thereto, provide acceptable means for assessing and controlling the software used to program digital-computer-based systems. The documents define and use certain terms to classify the criticalities of functions. For information, these terms have the

AMJ 25.1309 (continued)

following relationships to the terms used in this AMJ to classify Failure Conditions: Failure Conditions adversely affecting non-essential functions would be Minor, Failure Conditions adversely affecting essential functions would be Major or Hazardous, and Failure Conditions adversely affecting critical functions would be Catastrophic.

8 ACCEPTABLE TECHNIQUES

The methods outlined in this section provide acceptable techniques, but not the only techniques, for determining compliance with the requirements of JAR 25.1309(b), (c) and (d). Other comparable techniques exist and may be proposed by an applicant for use in any certification programme. Early agreement between the applicant and the Certificating Authority should be reached on the methods of assessment to be used.

After the applicant has established an acceptable classification level for a particular Failure Condition by means of a hazard assessment, it is the applicant's responsibility to determine how to show compliance with the requirement and obtain the concurrence of the Certificating Authority. Design and installation reviews, analyses, flight tests, ground tests, simulator tests or other approved means may be used. Flight tests are not required for verifying the postulated effects of either Hazardous or Catastrophic Failure Conditions.

a. *Functional Hazard Assessment*

Before an applicant proceeds with a detailed safety assessment, it is useful to prepare a preliminary hazard assessment of the system functions in order to determine the need for and scope of subsequent analysis. This assessment may be conducted using service experience, engineering and operational judgement, or a top-down deductive qualitative examination of each function performed by the system. A functional hazard assessment is a systematic, comprehensive examination of a system's functions to identify potential Major, Hazardous and Catastrophic Failure Conditions which the system can cause or contribute to, not only if it malfunctions or fails to function, but also in its normal response to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of the system rather than with the detailed hardware analysis.

Each system function should also be examined with respect to functions performed by other aeroplane systems, because the loss of different but related functions provided by separate systems may affect the severity of Failure Conditions postulated for a particular system. In assessing the effects of a Failure Condition factors which might alleviate or intensify the direct effects of the initial Failure Condition should be considered, including consequent or related conditions existing within the aeroplane which may affect the ability of the crew to deal with direct effects, such as the presence of smoke, acceleration vectors, interruption of communication, interference with cabin pressurisation, etc.

When assessing the consequences of a given Failure Condition, account should be taken of the warnings given, the complexity of the crew action, and the relevant crew training. The number of overall Failure Conditions involving other than instinctive crew actions may influence the flight crew performance that can be expected. Training requirements may need to be specified in some cases.

A functional hazard assessment may contain a high level of detail in some cases, such as for a flight guidance and control system with many functional modes, but many installations may need only a simple review of the system design by the applicant. The functional hazard assessment is a preliminary engineering tool. It should be used to identify design precautions necessary to ensure independence, to determine the required software level and to avoid common mode and cascade failures.

If further safety analysis is not provided, then the functional hazard assessment could itself be used as certification documentation.

AMJ 25.1309 (continued)

b. *Analysis of Minor Failure Conditions*

(1) Although a functional hazard assessment has determined that malfunction of a particular system can result in only Minor Failure Conditions by itself, it is also necessary that the assessment verifies that failures of the system will not contribute to more severe Failure Conditions if combined with failures of other systems or functions. In general, the installation of systems which do not perform any airworthiness-related functions should be accomplished in a manner which ensures their independence of function and physical separation from airworthiness-related components.

(2) If the hazard assessment, based on experienced engineering judgement, determines that system malfunctions cannot result in worse than Minor Failure Conditions, or affect other airworthiness-related functions, no further safety analysis is necessary to show compliance with JAR 25.1309.

c. *Analysis of Major Failure Conditions*

(1) Major Failure Conditions identified by the functional hazard assessment should be Improbable (Remote). If the complexity of the system is low, and the system is similar in its relevant Attributes to those used in other aeroplanes (see figure 1) and the effects of failure would be the same, then design and installation appraisals, and satisfactory service history of the equipment being analysed, or of similar design, will usually be acceptable for showing compliance.

(2) If similarity cannot be justified, but the system is conventional in its relevant Attributes, then compliance may be shown by means of a qualitative assessment. This also applies to systems of high complexity, provided that there is reasonable confidence that the Failure Condition is not worse than Major.

(3) For complex systems which include functional redundancy, a qualitative failure modes and effects analysis or fault tree may be necessary to determine that redundancy actually exists (e.g. no single failure affects all functional channels), and to show that the failure modes of the equipment do not have any airworthiness-related effects on other functions.

d. *Analysis of Hazardous and Catastrophic Failure Conditions*

(1) Except as specified in paragraph 8.d.(2), a detailed safety analysis will be necessary for each Hazardous and Catastrophic Failure Condition identified by the functional hazard assessment (see figure 1). Hazardous Failure Conditions should be Improbable (Extremely Remote), and Catastrophic Failure Conditions should be Extremely Improbable. The analysis will usually be a combination of qualitative and quantitative assessment of the design. Probability levels which are related to Catastrophic Failure Conditions should not be assessed only on a numerical basis, unless this basis can be substantiated beyond reasonable doubt.

(2) For very simple and conventional installations, i.e. low complexity and similarity in relevant Attributes (see figure 1), it may be possible to assess a Catastrophic Failure Condition as being Extremely Improbable, on the basis of experienced engineering judgement, without using all the formal procedures listed above. 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 in respect of both the system design and operating conditions. However, as discussed in paragraph 7.g., a Failure Condition resulting from a single failure mode of a device cannot generally be accepted as being Extremely Improbable, except in very unusual cases.

e. *Operational or Environmental Conditions*

A probability of one should usually be used for encountering a discrete condition for which the aeroplane is designed, such as instrument meteorological conditions or Category III weather

AMJ 25.1309 (continued)

operations. On the other hand, reasonable and rational consideration of the statistically-derived probability of a random condition may usually be included in an analysis, provided it is based on an applicable supporting data base and its statistical distribution. When combining the probability of such a random condition with that of a system failure, care should be taken to ensure that the condition and the system failure are independent of one another, or that any dependencies are properly accounted for. Two examples of the reasonable and rational use of such random conditions are the encountering of hazardous turbulence or gust levels after the failure of a structural load alleviation system, and the availability of a suitable alternate airport having a crosswind lower than that at the intended destination airport after a system failure that results in a loss of high rudder authority. The applicant should obtain early concurrence of the Certificating Authority when such conditions are to be included in an analysis.

f. *Latent Failures*

A latent failure is one which is inherently undetected when it occurs. A significant latent failure is one which would, in combination with one or more other specific failures or events, result in a Hazardous or Catastrophic Failure Condition. Because the frequency at which a device is checked directly affects the probability that any latent failure of that device exists, CCRs (see paragraph 6.b.) may be used to help show compliance with JAR 25.1309(b) and (d)(2) for significant latent failures.

g. *Acceptable Means of Compliance with JAR 25.1309(c) and (d)(4)*

JAR 25.1309(c) requires that warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. It also requires that systems, controls, and associated monitoring and warning means must be designed to minimise crew errors which could create additional hazards. Compliance with this section is shown qualitatively:

(1) Failure warning or indication may be either natural (inherent) or designed into the system. In either case, it should be timely, rousing, obvious, clear and unambiguous. It should occur at a point in a potentially-catastrophic sequence of failures where the aeroplane's capability and the crew's ability still remain sufficient for appropriate corrective crew action.

(2) 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.

(3) Even if operation or performance is unaffected or insignificantly affected at the time of failure, warning is required if it is considered necessary for the crew to take any action or observe any precautions. Some examples would 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 serious failure condition that would result from subsequent failures or operational or environmental conditions. Warning is also required if a failure must be corrected before a subsequent flight. If operation or performance is unaffected or insignificantly affected, warning may be inhibited during specific phases of flight where corrective action by the crew is considered more hazardous than no action.

(4) The use of CCRs or other checks in lieu of practical and reliable failure monitoring and warning systems to detect significant latent failures when they occur does not comply with JAR 25.1309(c) and (d)(4). A practical failure monitoring and warning system is one which is considered to be within the state of the art. A reliable failure monitoring and warning system is one which would not result in either excessive failures of a genuine warning, or excessive or untimely false warnings which can sometimes be more hazardous than lack of provision for, or failures of, genuine but infrequent warnings. Experienced judgement should be applied when determining whether or not a failure monitoring and warning system would be practical and reliable. Comparison with similar, previously-approved systems is sometimes helpful. Paragraph 11. provides further guidance on the use of CCRs.

AMJ 25.1309 (continued)

(5) The assumptions of paragraph 11.a. that the flight crew will take appropriate corrective action and perform required checks correctly are based on compliance with the requirement for a design that minimises the potential for serious crew errors; however, quantitative assessments of the probabilities of crew errors are not considered feasible. 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.

9 QUALITATIVE ASSESSMENT

Various methods for assessing the causes, severities, and likelihood of potential Failure Conditions are available to support experienced engineering and operational judgement. Some of these methods are structured. The various types of analysis are based on either inductive or deductive approaches. Descriptions of typical types of analysis and explanations of qualitative probability terms are provided below.

a. *Design Appraisal.* A qualitative appraisal of the integrity and safety of the design. An effective appraisal requires experienced judgement and, in accordance with paragraph 7.e., should place special emphasis on any Failure Conditions that are likely to prevent Continued Safe Flight and Landing.

b. *Installation Appraisal.* A qualitative appraisal of the integrity and safety of the installation. An effective appraisal requires experienced judgement and, in accordance with paragraph 7.e., should place special emphasis on any Failure Conditions that are likely to prevent Continued Safe Flight and Landing. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

c. *Failure Modes and Effects Analysis.* A structured, inductive, bottom-up analysis which is used to evaluate the effects on the system and the aeroplane of each possible element or component failure. When properly formatted, it will aid in identifying latent failures and the possible causes of each failure mode.

d. *Fault tree or Dependence Diagram (Reliability Block Diagram) Analysis.* Structured, deductive, top-down analyses which are used to identify the conditions, failures, and events that would cause each defined Failure Condition. They 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. A failure modes and effects analysis is usually used as the source document for those primary failures or other events. A fault tree analysis is failure oriented, and is conducted from the perspective of which failures must occur to cause a defined Failure Condition. A dependence diagram analysis is success-oriented, and is conducted from the perspective of which failures must not occur to preclude a defined Failure Condition.

e. *Qualitative Probability Terms.* When using qualitative analyses to determine compliance with JAR 25.1309(b), the following descriptions of the probability terms used in the requirement and this AMJ 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) Improbable Failure Conditions are divided into two categories as follows:

(i) Remote. 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.

AMJ 25.1309 (continued)

(ii) Extremely Remote. Unlikely to occur when considering the total operational life of all aeroplanes of the type, but nevertheless has to be considered as being possible.

(3) 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.

10 QUANTITATIVE ASSESSMENT

A quantitative analysis may be used to support experienced engineering and operational judgement and to supplement qualitative analyses. A description of such an analysis, discussion and guidance information, and explanations of quantitative probability terms, are provided below. A quantitative analysis is often used for Hazardous or Catastrophic Failure Conditions of systems that are complex, that have insufficient service experience to help substantiate their safety, or that have Attributes that differ significantly from those of conventional systems.

a. *Probability Analysis.* A failure modes and effects, fault tree, or dependence diagram analysis which also includes numerical probability information. The probabilities of primary failures can be determined from failure rate data and exposure times, using failure rates derived from service experience on identical or similar items, or acceptable industry standards. The conventional mathematics of probability can then be used to calculate the estimated probability of each Failure Condition as a function of the estimated probabilities of its identified contributory failures or other events.

(1) It is recognised that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of Failure Conditions. This results in some degree of uncertainty, as indicated by the expression 'of the order of' in the descriptions of the quantitative probability terms that are provided in paragraph 10.b. When calculating the estimated probability of each Failure Condition, this uncertainty should be accounted for in a way that does not compromise safety.

(2) Unless acceptable probability criteria are provided elsewhere, such as in other AMJs, acceptable probabilities for Failure Conditions should be derived from complete event scenarios leading to an inability for Continued Safe Flight and Landing. The considerations described in paragraphs 7.c. and 7.e. should always be taken into account so that the required probabilities are rational and realistically-based. Using experienced engineering and operational judgement, acceptable probabilities should have reasonable tolerances because the uncertainty is accounted for as discussed in paragraph 10.a.(1).

b. *Quantitative Probability Terms.* When using quantitative analyses to help determine compliance with JAR 25.1309(b), the following descriptions of the probability terms used in this requirement and this AMJ have become commonly accepted as aids to engineering judgement. They are usually expressed in terms of acceptable numerical probability ranges for each flight hour, based on a flight of mean duration for the aeroplane type. However, for a function which is used only during a specific flight operation; e.g., take-off, landing, etc., the acceptable probability should be based on, and expressed in terms of, the flight operation's actual duration.

(1) Probable Failure Conditions are those having a probability greater than of the order of 1×10^{-5}.

(2) (i) Improbable (Remote) Failure Conditions are those having a probability order of 1×10^{-5} or less but greater than of the order of 1×10^{-7}.

(ii) Improbable (Extremely Remote) Failure Conditions are those having a probability of the order of 1×10^{-7} or less, but greater than of the order of 1×10^{-9}.

(3) Extremely Improbable Failure Conditions are those having a probability of the order of 1×10^{-9} or less.

11 OPERATIONAL AND MAINTENANCE CONSIDERATIONS

AMJ 25.1309 (continued)

This AMJ addresses only those operational and maintenance considerations that are directly related to compliance with JAR 25.1309(b), (c), and (d); other operational and maintenance considerations are not discussed herein. Flight crew and ground tasks related to compliance with this requirement should be appropriate and reasonable. However, as discussed in paragraph 8.g.(5), quantitative assessments of the probabilities of crew errors are not considered feasible. Therefore, 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 and when they are required or scheduled. In addition, based on experienced engineering and operational judgement, the discovery of obvious failures during normal operation and maintenance of the aeroplane may be considered, even though such failures are not the primary purpose or focus of the operational or maintenance actions.

a. *Flight Crew Action*. When assessing the ability of the flight crew to cope with a Failure Condition, the warning information and the complexity of the required action should be considered (see paragraph 8.g.). If the evaluation indicates that a potential Failure Condition can be alleviated or overcome without jeopardising 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 of CCRs, if overall flight crew workload during the time available to perform them is not excessive and if they do not require exceptional pilot skill or strength. Unless flight crew actions are accepted as normal airmanship, they should be described in the approved AFM or AFM revision or supplement.

b. *Ground Crew Action*. Credit may be taken for correct ground crew accomplishment of reasonable CCRs, for both qualitative and quantitative assessments. Such requirements should be provided for use in approved maintenance programmes.

c. *Certification Check Requirements.* As defined in paragraph 6.b. and as discussed in 8.f., CCRs (also referred to as Certification Maintenance Requirements, or CMRs) may be needed to help show compliance with JAR 25.1309(b) and (d)(2) for significant latent failures. Rational methods, which usually involve quantitative analyses or relevant service experience data, should be used to determine CCR intervals. These intervals should have reasonable tolerances so that CCRs can be performed concurrently with other maintenance, inspection, or check procedures not required by design for compliance with JAR 25.1309(b) and (d)(2). Such tolerances are acceptable because the uncertainty described in paragraph 10.a.(1) is accounted for as discussed therein. If CCRs are used, they and their intervals and tolerances, and any post-certification changes, or procedures provided in the type design for an aeroplane owner or operator to make such changes, should be approved by, or with the concurrence of, the Certificating Authority having cognizance over the type design that relates to the system and its installation.

(1) Any applicant originating CCRs that are to be performed by flight crews should provide all relevant information to owners and operators of the aeroplane in the approved AFM or AFM revision or supplement.

(2) Any applicant originating CCRs that are to be performed by ground crews should provide all relevant information to owners and operators of the aeroplane early enough for well-planned, timely incorporation into approved maintenance programmes. If appropriate, approved procedures for reasonable adjustments to CCR intervals as a result of knowledge acquired from service experience may be provided for use in approved maintenance programmes.

(3) Any owner or operator of an aeroplane may request that alternative CCRs or their intervals be allowed and specified in an operator's specification approved under the applicable operating requirement or in accordance with an approved maintenance programme. As discussed in paragraph 11.c., concurrence of the Certificating Authority having cognizance over the type design that relates to the system and its installation is necessary.

AMJ 25.1309 (continued)

d. *Flight with Equipment or Functions Inoperative*. Any applicant may elect to develop a list of equipment and functions which need not be operative for safe flight and landing, based on stated compensating precautions that should be taken; e.g. operational or time limitations, or flight crew or ground crew checks. The documents used to show compliance with JAR 25.1309(b), (c) and (d), together with any other relevant information, should be considered in the development of this list, which then becomes the basis for a Master Minimum Equipment List (MMEL). Experienced engineering and operational judgement should be applied during the development of the MMEL.

12 STEP-BY-STEP GUIDE

This guide and figure 2, Depth of Analysis Flowchart, are provided primarily for the use of applicants who are not familiar with the various methods and procedures generally used by industry to conduct design safety assessments. This guide and figure 2 are not certification checklists, and they do not include all the information provided in this AMJ. There is no necessity for an applicant to use them or for the Certificating Authority to accept them, in whole or in part, to show compliance with any requirement. Their sole purposes are to assist applicants by illustrating a systematic approach to design safety assessments, to enhance understanding and communication by summarising some of the information provided in this AMJ, and to provide some suggestions on documentation.

a. Define the system and its interfaces, and identify the functions that the system is to perform. Determine whether or not the system is complex, similar to systems used on other aeroplanes, and conventional .

b. Identify and classify the significant (i.e. non-trivial) Failure Conditions. All relevant applicant 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 a Functional Hazard Assessment, which is usually based on one of the following methods, as appropriate:

(1) If the system is not complex, and if its relevant Attributes are similar to those of systems used on other aeroplanes, this 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 failure, considered both individually and in combination with other failures or events.

c. Choose the means to be used to determine compliance with JAR 25.1309(b), (c) and (d). The depth and scope of the analysis depends on the types of functions performed by the system, the severities of system Failure Conditions, and whether or not the system is complex. 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 applicant should obtain the early concurrence of the Certificating Authority on the choice of an acceptable means of compliance.

d. Implement the design and produce the data which are agreed with the Certificating Authority as being acceptable to show compliance. To the extent feasible, an analysis should be self-contained; however, if it is not, all other documents needed should be referenced. 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.

AMJ 25.1309 (continued)

(2) A list of the component parts and equipment of which the system is comprised, and their design standards. This list may reference other documents; e.g. Technical Standard Orders, manufacturer's or military specifications, etc.

(3) The conclusions, including a statement of the Failure Conditions and their classifications and probabilities (expressed qualitatively and quantitatively, as appropriate), that show compliance with the requirements of JAR 25.1309(b), (c) and (d).

(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-mode or 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 CCRs.

EFFECT ON AIRCRAFT AND OCCUPANTS	Normal	Nuisance	Operating limitations; emergency procedures	Significant reduction in safety margins; difficult for crew to cope with adverse conditions; passenger injuries	Large reduction in safety margins; crew extended because of workload or environmental conditions serious or fatal injury to a small number of occupants	Multiple deaths usually with loss of aircraft
F.A.R. PROBABILITY (REF ONLY)	< – – – – – – – – – – –	PROBABLE	– – – – – – – – >	<- – – – – –IMPROBABLE- – – – –>		EXTREMELY < – – – – – – – – – > IMPROBABLE
JAR–25 PROBABILITY	< – – – – – – – – – – – < – – – FREQUENT 10^{0} 10^{-1}	PROBABLE – – – – – – > 10^{-2}	– – – – – – – – > < REASONABLY > PROBABLE 10^{-3} 10^{-4}	<- – – – – –IMPROBABLE- – – – –> < – REMOTE – > 10^{-5} 10^{-6}	< EXTREMELY-> REMOTE 10^{-7} 10^{-8}	EXTREMELY < – – – – – – – – – > IMPROBABLE 10^{-9}
CLASSIFICATION OF FAILURE CONDITIONS	< – – – – – – – – – – –	– MINOR –	– – – – – – – – >	<-– MAJOR –- >	< HAZARDOUS >	<-CATASTROPHE->

FIGURE 1 – RELATIONSHIP BETWEEN PROBABILITY AND SEVERITY OF FAILURE CONDITION

INTENTIONALLY LEFT BLANK

AMJ 25.1309 (continued)

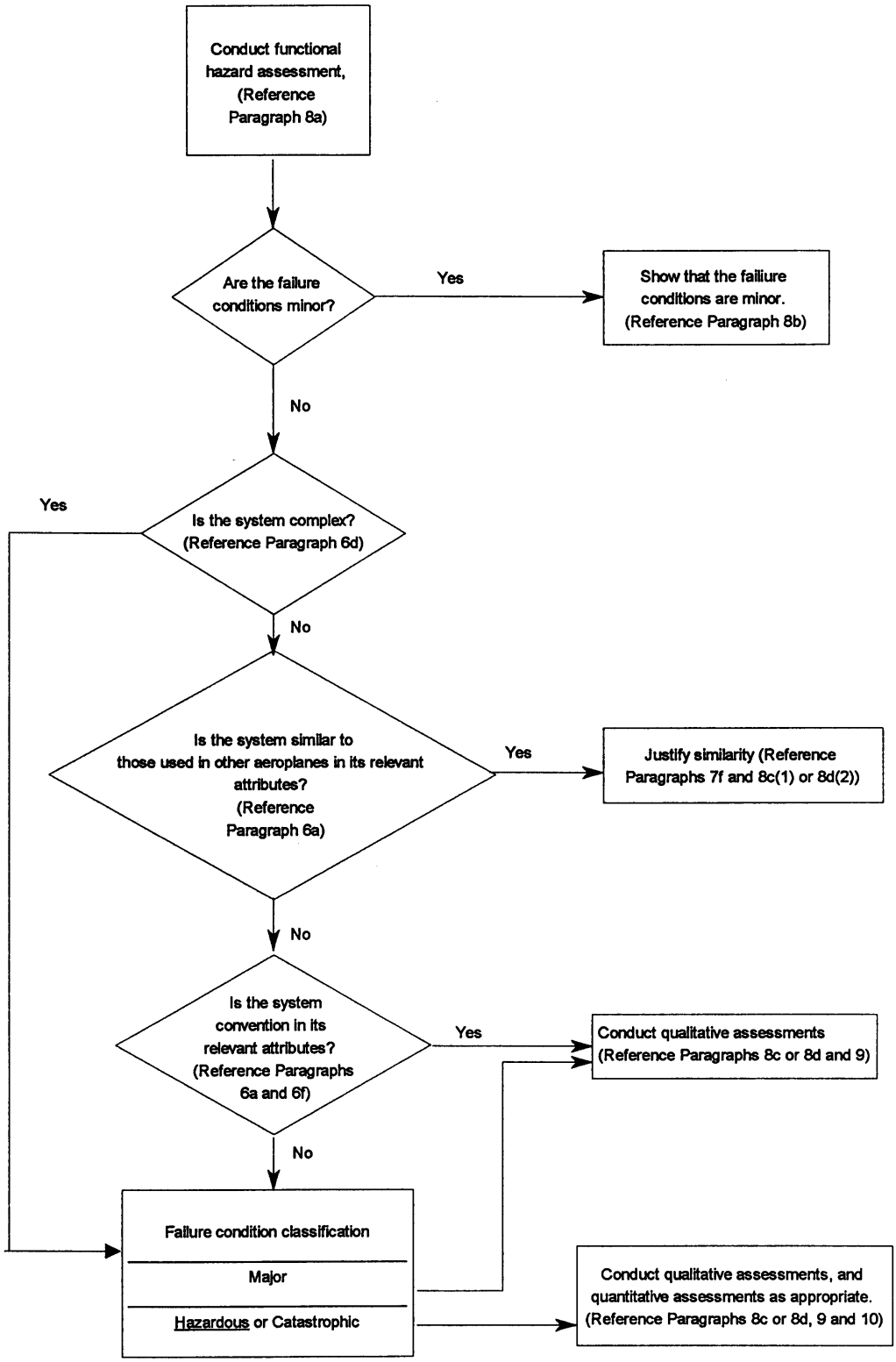

FIGURE 2 DEPTH OF ANALYSIS FLOW CHART