systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An FHA requires experienced engineering judgement and early co-ordination between the applicant and the certification authority.

(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to FHA may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interrelationships are relatively simple, it may be feasible to conduct separate FHAs for each system, providing any interface aspects are properly considered and are easily understood. Where system and function interrelationships are more complex, a top-down approach, from an aeroplane-level perspective, should be taken in planning and conducting FHAs However, with the increasing integrated system architectures, this traditional top-down approach should be performed in conjunction with common-cause considerations (e.g. common resources) in order to properly address the cases where one system contributes to several aeroplane-level functions.

c. *Considerations When Assessing Failure Condition Effects*.

The requirements of CS 25.1309(b) 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.

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. Some of these factors include consequent or related conditions existing within the aeroplane that may affect the ability of the crew to deal with direct effects, such as the presence of smoke, acceleration effects, interruption of communication, interference with cabin pressurisation, etc. When assessing the consequences of a given failure condition, account should be taken of the failure information provided, 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 recommendations may need to be identified in some cases.

(1) The severity of failure conditions should be evaluated according to the following:

(i) Effects on the aeroplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a failure condition are difficult to assess, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.

(ii) Effects on the crewmembers, such as increases above their normal workload that would affect their ability to cope with adverse operational or environmental conditions or subsequent failures.

(iii) Effects on the occupants, i.e., passengers and crewmembers.

(2) For convenience in conducting design assessments, failure conditions may be classified according to the severity of their effects as 'no safety effect', 'minor', 'major', 'hazardous', or 'catastrophic'. Paragraph 7.a above provides accepted definitions of these terms.

(i) The classification of failure conditions does not depend on whether or not a system or function is the subject of a specific requirement or regulation. 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 auto-flight systems, may have the potential for 'major', 'hazardous', or 'catastrophic failure conditions'.

(ii) 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. It is particularly important to consider factors that would alleviate or intensify the severity of a failure condition. When flight duration, flight phase, or diversion time can adversely affect the classification of failure conditions, they must be considered to be intensifying factors. Other intensifying factors include conditions that are not related to the failure (such as weather or adverse operational or environmental conditions), and which reduce the ability of the flight crew to cope with 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. Another example of an alleviating factor is the ability of the flight crew to recognise the failure condition and take action to mitigate its effects. Whenever this is taken into account, particular attention should be paid to the detection means to ensure that the ability of the flight crew (including physical ability and timeliness of the response) to detect the failure condition and take the necessary corrective action(s) is sufficient. Refer to CS 25.1309(c) and paragraph 9.c of this AMC for more detailed guidance on crew annunciations and crew response evaluation. Combinations of intensifying or alleviating factors need to be considered only if they are anticipated to occur together.

11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS.

After the failure conditions have been identified and the severity of the effects of the failure conditions have been assessed, there is a responsibility to determine how to show compliance with the requirement and obtain the concurrence of EASA. Design and installation reviews, analyses, flight tests, ground tests, simulator tests, or other approved means may be used.

a. *Assessment of Failure Condition Probabilities*.

(1) The probability that a failure condition would occur may be assessed as probable, remote, extremely remote, or extremely improbable. These terms are defined in paragraph 7. Each failure condition should have a probability that is inversely related to the severity of its effects as described in paragraph 8.

(2) When a system provides protection from events (e.g., cargo compartment fire, gusts), its reliability should be compatible with the safety objectives necessary for the failure condition associated with the failure of the protection system and the probability of such events. (See paragraph 11g of this AMC and Appendix 4.)

(3) 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 severity of failure conditions, and whether or not the system is complex.

(4) Experienced engineering and operational judgement should be applied when determining whether or 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 and hardware item need not be a dominant factor in the determination of complexity at the system level.

b. *Single Failure Considerations.*

(1) According to the requirements of CS 25.1309(b)(1)(ii), a catastrophic failure condition must not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure conditions. In addition, there must be no common-cause failure, which could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures, which cannot be shown to be independent from each other. Common-cause failures (including common mode failures) and cascading failures should be evaluated as dependent failures from the point of the root cause or the initiator. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (including common mode failures) and cascading failures. They should, therefore, be assessed and mitigated in the frame of the common-cause and cascading failures consideration. Appendix 1 and the Document referenced in paragraph 3.b(3) describe types of common-cause analyses that may be conducted~~,~~ to assure that independence is maintained. Failure containment techniques available to establish independence may include partitioning, separation, and isolation.

(2) While single failures must normally be assumed to occur, there are cases where it is obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that a failure mode simply would not occur, unless it is associated with a wholly unrelated failure condition that would itself be catastrophic. Once identified and accepted, such cases need not be considered failures in the context of CS 25.1309. For example, with simply loaded static elements, any failure mode, resulting from fatigue fracture, can be assumed to be prevented if this element is shown to meet the damage tolerance requirements of CS 25.571.

c. *Common Cause Failure Considerations*.

An analysis should consider the application of the fail-safe design concept described in paragraph 6b and give special attention to ensure the effective use of design and installation techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel, more than one system performing operationally similar functions, or any system and an associated safeguard. When considering such common-cause failures or other events, consequential

or cascading effects should be taken into account. 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 (other than engines and propellers) or pressure vessels, pressure differentials, non-catastrophic structural failures, loss of environmental conditioning, disconnection of more than one subsystem or component by over temperature protection devices, contamination by fluids, damage from localised fires, loss of power supply or return (e.g. mechanical damage or deterioration of connections), excessive voltage, physical or environmental interactions among parts, errors, or events external to the system or to the aeroplane (see Document referenced in paragraph 3b(3)).

d. *Depth of Analysis*.

The following identifies the depth of analysis expected based on the classification of a failure condition.

(1) *No Safety Effect Failure Conditions*. An FHA, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these failure conditions. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(2) *Minor Failure Conditions*. An FHA, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these failure conditions. Combinations of failure condition effects, as noted in paragraph 10 above, must also be considered. If it is chosen not to do an FHA, the safety effects may be derived from the design and installation appraisal.

(3) *Major Failure Conditions*. Major failure conditions must be remote:

(i) If the system is similar in its relevant attributes to those used in other aeroplanes and the effects of failure would be the same, then design and installation appraisals (as described in Appendix 1), and satisfactory service history of the equipment being analysed, or of similar design, will usually be acceptable for showing compliance.

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

(iii) For complex systems without redundancy, compliance may be shown as in paragraph 11.d(3)(ii) of this AMC. To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional failure modes and effects analysis (FMEA) supported by failure rate data and fault detection coverage analysis.

(iv) An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative FMEA and qualitative fault tree analysis may be necessary to determine that redundancy actually exists (e.g. no single failure affects all functional channels).

(4) *Hazardous and Catastrophic Failure Conditions*.

Hazardous failure conditions must be extremely remote, and catastrophic failure conditions must be extremely improbable:

(i) Except as specified in paragraph 11.d(4)(ii) below, a detailed safety analysis will be necessary for each hazardous and catastrophic failure condition identified by the FHA. The analysis will usually be a combination of qualitative and quantitative assessment of the design.

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

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

e. *Calculation of Average Probability per Flight Hour (Quantitative Analysis)*.

(1) The average probability per flight hour is the probability of occurrence, normalised by the flight time, of a failure condition during a flight, which can be seen as an average over all possible flights of the fleet of aeroplane to be certified. The calculation of the average probability per flight hour for a failure condition should consider:

(i) the average flight duration and the average flight profile for the aeroplane type to be certified,

(ii) all combinations of failures and events that contribute to the failure condition,

(iii) the conditional probability if a sequence of events is necessary to produce the failure condition,

(iv) the relevant 'at risk' time if an event is only relevant during certain flight phases, and

(v) the exposure time if the failure can persist for multiple flights.

(2) The details how to calculate the average probability per flight hour for a failure condition are given in Appendix 3 of this AMC.

(3) If the probability of a subject failure condition occurring during a typical flight of mean duration for the aeroplane type divided by the flight's mean duration in hours is likely to be significantly different from the predicted average rate of

occurrence of that failure condition during the entire operational life of all aeroplanes of that type, then a risk model that better reflects the failure condition should be used.

(4) 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 wide line in Figure 1, and the expression 'on the order of' in the descriptions of the quantitative probability terms that are provided above. When calculating the estimated probability of each failure condition, this uncertainty should be accounted for in a way that does not compromise safety.

f. *Integrated Systems.*

Interconnections between systems have been a feature of aeroplane design for many years and CS 25.1309(b) recognises this in requiring systems to be considered in relation to other systems. Providing the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be demonstrated through a series of system safety assessments, each of which deals with a particular failure condition (or more likely a group of failure conditions) associated with a system and, where necessary, takes account of failures arising at the interface with other systems. This procedure has been found to be acceptable in many past certification programmes. However, where the systems and their interfaces become more complex and extensive, the task of demonstrating compliance may become more complex. It is therefore essential that the means of compliance be considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy. Aspects of the guidance material covered elsewhere in this AMC and which should be given particular consideration are as follows:

(1) planning the proposed means of compliance; this should include development assurance activities to mitigate the occurrence of errors in the design,

(2) considering the importance of architectural design in limiting the impact and propagation of failures,

(3) the potential for common-cause failures and cascade effects and the possible need to assess combinations of multiple lower-level (e.g. major) failure conditions,

(4) the importance of multidisciplinary teams in identifying and classifying significant failure conditions,

(5) effect of crew and maintenance procedures in limiting the impact and propagation of failures.

In addition, rigorous and well-structured design and development procedures play an essential role in facilitating a methodical safety assessment process and providing visibility to the means of compliance. Document referenced in paragraph 3b(2) may be helpful in the certification of highly integrated or complex aircraft systems.

g. *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 operations. However, Appendix 4 contains allowable probabilities, which may be assigned to various operational and environmental conditions for use in computing the average probability per flight hour of failure conditions without further

justification. Single failures, which, in combination with operational or environmental conditions, lead to catastrophic failure conditions, are, in general, not acceptable.

Limited cases that are properly justified may be considered on a case-by-case basis (e.g. operational events or environmental conditions that are extremely remote).

Appendix 4 is provided for guidance and is not intended to be exhaustive or prescriptive. At this time, a number of items have no accepted standard statistical data from which to derive a probability figure. However, these items are included for either future consideration or as items for which the applicant may propose a probability figure supported by statistically valid data or supporting service experience. The applicant may propose additional conditions or different probabilities from those in Appendix 4 provided they are based on statistically valid data or supporting service experience. The applicant should obtain early concurrence of EASA when such conditions are to be included in an analysis. 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.

h. *Justification of Assumptions, Data Sources and Analytical Techniques*.

(1) Any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, to show compliance with the requirements, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault independence, limitation of analytical methods, processes, and assumptions. The justification of the assumptions made with respect to the above items should be an integral part of the analysis. Assumptions can be validated by using experience with identical or similar systems or components with due allowance made for differences of design, duty cycle and environment. Where it is not possible to fully justify the adequacy of the safety analysis and where data or assumptions are critical to the acceptability of the Failure Condition, extra conservatism should be built into either the analysis or the design. Alternatively any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions are insensitive to that uncertainty.

(2) Where adequate validation data is not available (e.g., new or novel systems), and extra conservatism is built into the analysis, then the normal post-certification in-service follow-up may be performed to obtain the data necessary to alleviate any consequence of the extra conservatism. This data may be used, for example, to extend system check intervals.

12. OPERATIONAL AND MAINTENANCE CONSIDERATIONS.

This AMC addresses only those operational and maintenance considerations that are directly related to compliance with CS 25.1309; other operational and maintenance considerations are not discussed herein. Flight crew and maintenance tasks related to compliance with this requirement should be appropriate and reasonable. However, quantitative assessments of crew errors are not considered feasible. Therefore, reasonable tasks are those for which full credit can be taken because they can realistically be anticipated to be performed correctly when they are required or scheduled. In addition, based on experienced engineering and operational judgement, the discovery of obvious failures during normal operation or maintenance of the

aeroplane may be assumed, even though identification of such failures is not the primary purpose 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 information provided to the crew and the complexity of the required action should be considered. When considering the information provided to the flight crew, refer also to paragraph 9.c (compliance with CS 25.1309(c)). Credit for flight crew actions, and considerations of flight crew errors, should be consistent with relevant service experience and acceptable human factors evaluations. 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 both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance of the periodic checks required to demonstrate compliance with CS 25.1309(b) provided overall flight crew workload during the time available to perform them is not excessive and 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 Aeroplane Flight Manual in compliance with CS 25.1585. The applicant should provide a means to ensure that the AFM will contain the required flight crew actions that have been used as mitigation factors in the hazard classification or that have been taken as assumptions to limit the exposure time of failures.

b. Maintenance Action.

Credit may be taken for the correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments. The maintenance tasks needed to demonstrate compliance with CS 25.1309(b) should be established. In doing this, the following maintenance scenarios can be used:

(1) For failures known to the flight crew, refer to paragraph 12.d.

(2) Latent failures will be identified by a scheduled maintenance task. If this approach is taken, and the failure condition is hazardous or catastrophic, then a CCMR maintenance task should be established. Some latent failures can be assumed to be identified based upon return to service test on the LRU following its removal and repair (component mean time between failures (MTBF) should be the basis for the check interval time).

c. Candidate Certification Maintenance Requirements.

(1) By detecting the presence of, and thereby limiting the exposure time to significant latent failures that would, in combination with one or more other specific failures or events identified by safety analysis, result in a hazardous or catastrophic failure condition, periodic maintenance or flight crew checks may be used to help show compliance with CS 25.1309(b). Where such checks cannot be accepted as basic servicing or airmanship they become CCMRs. AMC 25.19 details the handling of CCMRs.

(2) Rational methods, which usually involve quantitative analysis, or relevant service experience should be used to determine check intervals. This analysis contains inherent uncertainties as discussed in paragraph 11e(3). Where periodic checks become CMRs these uncertainties justify the controlled escalation or exceptional short-term extensions to individual CMRs allowed under AMC 25.19.

d. *Flight with Equipment or Functions known to be Inoperative*.

An applicant may elect to develop a list of equipment and functions that need not be operative for flight, based on stated compensating precautions that should be taken, e.g. operational or time limitations, flight crew procedures, or ground crew checks. The documents used to demonstrate compliance with CS 25.1309, together with any other relevant information, should be considered in the development of this list. Experienced engineering and operational judgement should be applied during the development of this list. When operation is envisaged with equipment that is known to be inoperative, and this equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, limitations may be needed on the number of flights and/or the allowed operation time with such inoperative equipment. These limitations should be established in accordance with the recommendations contained in CS-MMEL.

13. ASSESSMENT OF MODIFICATIONS TO PREVIOUSLY CERTIFICATED AEROPLANES.

The means to assure continuing compliance with CS 25.1309 for modifications to previously certificated aeroplanes should be determined on a case-by-case basis and will depend on the applicable aeroplane certification basis and the extent of the change being considered. The change could be a simple modification affecting only one system or a major redesign of many systems, possibly incorporating new technologies. The minimal effort for demonstrating compliance to 25.1309 for any modification is an assessment of the impact on the original system safety assessment. The result of this assessment may range from a simple statement that the existing system safety assessment still applies to the modified system in accordance with the original means of compliance, to the need for new means of compliance encompassing the plan referred to in paragraph 9b. (STC applicants, if the TC holder is unwilling to release or transfer proprietary data in this regard, the STC applicant may have to create the System Safety Assessment. Further guidance may be found in paragraph 6 of Document referenced in paragraph 3b(2).) It is recommended that the Agency be contacted early to obtain agreement on the means of compliance.

[Amdt 25/2]
[Amdt 25/4]
[Amdt 25/8]
[Amdt 25/11]
[Amdt 25/12]
[Amdt 25/14]
[Amdt 25/19]
[Amdt 25/24]
[Amdt 25/27]

Appendix 1 – Assessment methods

ED Decision 2020/001/R

Various methods for assessing the causes, severity, and probability of 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. Probability assessments may be qualitative or quantitative. Descriptions of some types of analysis are provided below and in Document referenced in paragraph 3b(3).

a. *Design Appraisal.* This is a qualitative appraisal of the integrity and safety of the system design.

b. *Installation Appraisal.* This is a qualitative appraisal of the integrity and safety of the installation. 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.* This is 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. Document referenced in paragraph 3b(3) provides methodology and detailed guidelines, which may be used to perform this type of analysis. A FMEA could be apiece part FMEA or a functional FMEA. For modern microcircuit based LRUs and systems an exhaustive piece part FMEA is not practically feasible with the present state of the art. In that context, a FMEA may be more functional than piece part oriented. A functional oriented FMEA can lead to uncertainties in the qualitative and quantitative aspects, which can be compensated for by more conservative assessment such as:

   — assuming all failure modes result in the failure conditions of interest,

   — careful choice of system architecture,

   — taking into account the experience lessons learned on the use of similar technology.

d. *Fault Tree or Dependence Diagram Analysis.* Structured, deductive, top-down analyses that 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 may be used as the source document for those primary failures or other events.

e. *Markov Analysis.* A Markov model (chain) represents various system states and the relationships among them. The states can be either operational or non-operational. The transitions from one state to another are a function of the failure and repair rates. Markov analysis can be used as a replacement for fault tree/dependence diagram analysis, but it often leads to more complex representation, especially when the system has many states. It is recommended that Markov analysis be used when fault tree or dependence diagrams are not easily usable, namely to take into account complex transition states of systems which are difficult to represent and handle with classical fault tree or dependence diagram analysis.

f. *Common-Cause Analysis.* The acceptance of adequate probability of failure conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognise that such independence may not exist in the practical sense and specific studies are necessary to ensure that independence can either be assured or considered to be acceptable. These studies may also identify a combination of failures and effects that would otherwise not have been foreseen by FMEA or fault tree analysis.