M-494.4

U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

FILE
Obsolete

Subject: SYSTEM DESIGN ANALYSIS

Date: 9/7/82
Initiated by: ANM-110

AC No: 25.1309-1
Change:

1. PURPOSE. This advisory circular provides guidance material for acceptable means, but not the only means, of demonstrating compliance with the requirements of Part 25 of the Federal Aviation Regulations which includes probabilistic terms, as introduced by Amendment 25-23, for airplane equipment, systems, and installations.

2. REFERENCE REGULATION. Section 25.1309 of the Federal Aviation Regulations, as amended through Amendment 25-41.

3. BACKGROUND.

a. For a number of years, aircraft systems were evaluated by the Federal Aviation Administration to the "single fault" criteria contained in § 4b.606 of the Civil Air Regulations, recodified and later amended as § 25.1309 of the Federal Aviation Regulations. The term "single fault" was a misnomer because additional cases of the hidden fault and the consequential fault also had to be considered (§ 4b.606-1 of the Civil Aeronautics Manual). With the development of more complex systems and the increasing criticality of those systems, the Federal Aviation Administration revised the rules in 1970 to require consideration of single and multiple faults in the system under study. The consequences of faults in separate systems which perform different functions are also to be considered if the simultaneous loss of functions performed by these systems creates a hazard to the airplane. Because of the growth in airplane system complexity, it is difficult in certain cases to make a responsible engineering judgment regarding the effects of certain system failures based on conventional analysis, tests, and historical data. However, the need for making a valid judgment has increased with the increasing criticality of certain systems.

b. To better understand the effects of complex airplane system failures, it may be desirable to use analytical techniques which can assist in identifying failure conditions and their potential consequences. This advisory circular identifies various analytical approaches, both qualitative and quantitative, which may be used to assist airplane manufacturers and FAA personnel in determining compliance with the referenced regulation and provide guidance for determining when, or if, a particular analysis should be conducted. Numerical values are assigned to the probabilistic terms included in the referenced regulation for use in those cases where the effects of system faults are examined by quantitative methods of analysis.

c. A finding of compliance with the requirements of FAR 25.1309 is based on the technical judgment of FAA pilots and engineers. The structured methods of analysis described by this advisory circular are intended to assist FAA personnel in finding compliance with the requirements in those cases where a design review cannot readily determine the impact of failures on the safety of the airplane. These analytical tools are intended to supplement, but not replace, the judgment of the FAA certification personnel.

4. DISCUSSION.

a. Section 25.1309 of Part 25 of the Federal Aviation Regulations, subsequent to Amendment 25-23, requires substantiation by analysis and, where necessary, by appropriate ground, flight, or simulator tests that the probability of a failure condition is expected to remain within limits which are related to the consequence of the failure condition. The requirements in the referenced regulation are intended to assure an orderly and thorough evaluation of systems considered separately and in relation to other systems. It is important to recognize that some systems (functions) have conventionally received such an evaluation to show compliance with other specific regulations or special conditions and thereby may be shown to meet the intent of FAR 25.1309 without a need for extensive additional analyses.

b. The probability of the occurrence of a failure condition may be considered within three classifications: probable, improbable, and extremely improbable. These classifications may be related to failure conditions which have increasingly more severe impact on safety. Airplane functions may be divided in the following manner:

(1) NON-ESSENTIAL--Functions whose failures would not contribute to or cause a failure condition which would significantly impact the safety of the airplane or the ability of the flight crew to cope with adverse operating conditions. Airplane conditions which result from improper accomplishment or loss of non-essential functions may be probable.

(2) ESSENTIAL--Functions whose failures would contribute to or cause a failure condition which would significantly impact the safety of the airplane or the ability of the flight crew to cope with adverse operating conditions. Failure conditions which result from improper accomplishment or loss of essential functions must be improbable.

(3) CRITICAL--Functions whose failure would contribute to or cause a failure condition which would prevent the continued safe flight and landing of the airplane. Failure conditions which result from improper accomplishment or loss of critical functions must be extremely improbable.

c. In order to show compliance with FAR 25.1309(b), FAR 25.1309(d) requires an analysis which must consider:

(1) Possible modes of failure, including malfunctions and damage from external sources.

(2) The probability of multiple failures and undetected failures.

(3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and

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

d. An analysis to identify failure conditions should be qualitative. An assessment of the probability of a failure condition can be qualitative or quantitative. An analysis may range from a simple report which interprets test results or presents a comparison between two similar systems to a fault/failure analysis which may (or may not) include numerical probability data. An analysis may make use of previous service experience from comparable installations in other airplanes.

e. The depth of this analysis will vary, depending on the design complexity and type of functions performed by the system being analyzed. Section 6 of this advisory circular identifies various analytical approaches and provides guidelines for determining when each should be used.

5. DEFINITIONS. For the purpose of conducting or evaluating an analysis, the following terms and numerical values should apply:

a. CONTINUED SAFE FLIGHT AND LANDING--This phrase is used in the regulation to require that an airplane be capable of continued controlled flight and landing, possibly using emergency procedures and without exceptional pilot skill or strength, after any failure condition which has not been shown to be extremely improbable. There may be failure conditions which are not extremely improbable for which it is necessary to assure that continued safe flight and landing is possible by appropriate analysis and/or tests.

b. DEDUCTIVE--The term used to describe those analytical approaches involving the reasoning from a defined unwanted event or premise to the causative factors of that event or premise by means of a logical methodology (the "top-down" or "how could it happen" approach). A deductive approach will postulate a particular failure condition and attempt to determine what system and equipment failure modes, errors, and/or environmental conditions will contribute to the failure condition.

c. ERROR--A mistake in specification, design, production, maintenance, or operation which causes an undesired performance of a function.

d. EVENT--An occurrence which causes a change of state. NOTE: The Regulatory Authorities of some countries use a more specific definition.

e. EXPOSURE TIME--The period (in clock time or cycles) during which a system, subsystem, unit or part is exposed to failure, measured from when it was last verified functioning to when its proper performance is or may be required.

f. FAILURE--The inability of a system, subsystem, unit or part to perform within previously specified limits. Note that some failures may have no effect on the capability of the airplane and therefore are not failure conditions.

g. FAILURE ANALYSIS--The logical, systematic examination of a system, subsystem, unit or part, to identify and analyze the probability, causes, and consequences of potential and real failures.

h. FAILURE CONDITION--A consequential airplane state which has an impact on the functional capability of the airplane or the ability of the crew to cope with adverse operating conditions, or which would prevent continued safe flight and landing. NOTE: A failure condition can result from the occurrence of a specific single event or a combination of related faults, failures, errors, operating conditions or environments. Postulated failure conditions are assessed for their impact on safety and assigned an appropriate probability classification. A defined failure condition provides the criteria for classifying system functions as non-essential, essential or critical and for showing compliance with 25.1309(b) in accordance with this advisory circular.

i. FAILURE EFFECT(S)--The consequence(s) of a failure mode on the system, subsystem, unit or part's operation, function, or status.

j. FAILURE MODE--The manner in which a system, subsystem, unit, part or function can fail.

k. FAULT--An undesired anomaly in the functional operation of a system, subsystem, unit or part.

l. FAULT TREE ANALYSIS--A top down deductive analysis identifying the conditions and functional failures necessary to cause a defined failure condition. The fault tree, when fully developed, may be mathematically evaluated to establish the probability of the ultimate failure condition occurring as a function of the estimated probabilities of identified contributory events.

m. FLIGHT TIME (Block Time)--The time from the moment the aircraft first moves under its own power for the purpose of flight until the moment it comes to rest at the next point of landing.

n. PROBABILITY CLASSIFICATIONS--Three probability classifications are defined below. Quantitative ranges are also provided as a common point of reference if numerical probabilities are used in assessing compliance with FAR 25.1309 or other applicable regulations. The quantitative ranges given for these classifications represent goals and are considered to overlap due to the inexact nature of probability estimates. When assessing the acceptability of a failure condition using a quantitative analysis, the numerical ranges given below should normally be interpreted to be the allowable risk for an hour of flight time based on a flight of mean duration for the airplane type. However, when assessing a function which is used only at a specific time during a flight, the probability of the failure condition should be calculated for the specific time period and expressed as the risk for the flight condition; takeoff, landing, etc., as appropriate.

(1) PROBABLE--Probable events may be expected to occur several times during the operational life of each airplane. A probability on the order of 1×10^{-5} or greater.

(2) IMPROBABLE--Improbable events are not expected to occur during the total operational life of a random single airplane of a particular type, but may occur during the total operational life of all airplanes of a particular type. A probability on the order of 1×10^{-5} or less.

(3) EXTREMELY IMPROBABLE--Extremely improbable events are so unlikely that they need not be considered to ever occur, unless engineering judgment would require their consideration. A probability on the order of 1×10^{-9} or less.

NOTES: (a) If a quantitative analysis is used to help show compliance with Federal Aviation Regulations for equipment which is installed and required only for a specific operating condition for which the airplane is thereby approved, credit may not be taken for the fact that the operating condition does not always exist. Except for this limitation, appropriate statistical randomness of environmental or operational conditions may be considered in the analysis. (However, the applicant should obtain prior concurrence of the FAA when including such conditions in the analysis.) (b) The three probability terms defined in paragraph 5n above are intended to relate to an identified failure condition resulting from or contributed to by the improper operation or loss of a function or functions. These terms do not define the reliability of specific components or systems. (c) The range of numerical values assigned to each of the terms is intended to minimize differences in the interpretation of what these terms mean when used in § 25.1309 of the Federal Aviation Regulations. It is important to realize that these terms and others such as "reliable," "unlikely," and "remote" are used throughout the Federal Aviation Regulations. In many cases, these other terms were used prior to Amendment 25-23. Careful

judgement is necessary when interpreting the intent of any regulation using such terms. In all cases, the effect of the given failure conditions should be considered.

o. FUNCTION--Each particular purpose performed by a system, subsystem, unit or part.

p. INDUCTIVE--The term used to describe those analytical approaches involving the systematic evaluation of the defined parts or elements of a given system or subsystem to determine specific characteristics of interest (the "bottom-up," or "what happens if" approach). An inductive approach will assume an initiating event and attempt to determine the corresponding effect on the overall system.

q. HIDDEN FAILURE--A failure that is not inherently revealed at the time it occurs.

r. QUALITATIVE--The term used to describe those analytical approaches which are oriented toward relative, nonmeasurable or non-numerical and subjective values.

s. QUANTITATIVE--The term used to describe those analytical approaches which are oriented toward the use of numbers to express a measurable quantity.

t. REDUNDANCY--The existence of more than one independent means of accomplishing a given function.

u. RELIABILITY--The probability that a system, subsystem, unit or part will perform its intended function for a specified interval under stated operational and environmental conditions.

6. ACCEPTABLE TECHNIQUES.

a. The first step in determining compliance with FAR 25.1309(b) should be to determine the criticality of the system or installation to be certificated. This analysis may be conducted using service experience, engineering, or operational judgment, or by using a top-down deductive qualitative analysis which examines each function performed by the system. The analysis should determine the criticality of each system function, i.e., either non-essential, essential, or critical. Each system function should be analyzed with respect to functions performed by other aircraft systems. This is necessary because the loss of different but related functions provided by separate systems may affect the criticality category assigned to a particular system. This type of analysis, variously referred to as a preliminary hazard analysis, criticality categorization, or criticality assessment may contain a high level of detail in some cases, such as for an integrated electronic flight instrument system. However, many installations may only need an informal review of the system design by the applicant for the benefit of the FAA certification personnel to determine the criticality of the functions performed by the system. The purpose of the preliminary hazard analysis is to identify the critical and

esential functions and the systems which must operate properly to accomplish these functions. Once the criticality of a system has been established, additional techniques which might be useful in determining compliance with FAR 25.1309(b) are more easily identified.

b. Analysis of systems which perform non-essential functions.

(1) Although a preliminary hazard analysis has been accomplished, and it has been determined that a particular system performs only non-essential functions, this is not sufficient for demonstrating compliance with the requirements of FAR 25.1309(b). It is also necessary to determine if failures of the system could contribute to a failure condition involving any essential or critical function.

(2) In general, the installation of a non-essential system should be accomplished in a manner which insures its independence and isolation from other systems in the airplane which perform critical or essential functions. If a review of the design based on good engineering judgment determines that system faults cannot affect essential or critical functions, then no further analysis is necessary. If the installation does not have satisfactory isolation from systems which perform essential or critical functions, or if the system complexity is such that a design review alone cannot adequately establish that such isolation has been achieved, then the system should be analyzed using more rigorous methods, some of which are identified in paragraphs 6c and 6d, below.

(3) Special care must be taken with systems that perform non-essential functions which provide information for use by the flight crew, such as engine performance data systems. Systems of this type, which are not required by regulation and also are non-essential, may have hazardous failure modes which provide misleading information to the flight crew without warning. These systems may have to be analyzed as a system which performs an essential function.

(4) Typically, systems such as galleys, position lights, public address systems, and interior cabin lights, to name a few, should be certificated based on a design review alone without the need of a formal failure analysis. Note that some systems required by regulation may be found to perform non-essential functions using the criteria of this advisory circular. Equipment such as transponders, position and anticollision lights, altitude alerting systems and ground proximity warning systems, are required for various operations and airplanes by regulation for safe and expeditious use of the airspace, but loss of this type of equipment does not create a serious hazard to the airplane or prevent its continued safe flight and landing and may therefore be considered to perform non-essential functions.

c. Analysis for failure conditions involving systems which perform essential functions.

(1) Failure conditions which affect essential functions should be improbable. Satisfactory service history of the equipment under analysis or similar units will be acceptable for showing compliance. Compliance may also be shown by a quantitative reliability analysis using failure rates from an acceptable industry standard or actual equipment failure rate data. An

acceptable probability level within the defined improbable range should be agreed upon with the FAA for a particular failure condition. Determination of the acceptable probability level should be based on an inverse relationship between the probability of the failure condition and the severity of its effect on airplane safety. This is not meant to imply that a numerical analysis will always be required to show compliance with an agreed-to level.

(2) Many units which perform essential functions have dual or greater redundancy. If redundancy exists and there is some evidence to indicate the satisfactory reliability of the redundant subsystems, no further analysis is necessary. For complex systems, a failure modes and effects analysis may be necessary to verify that redundancy actually exists, and to show that the failure modes of the system do not have an adverse effect on other essential or critical functions. A complete quantitative safety analysis will not usually be necessary.

(3) If failure modes are found to exist which result in failure conditions, these failure conditions should be shown to be improbable or extremely improbable, depending upon the criticality of the affected function. However, failure conditions resulting from single faults will not usually be accepted as being extremely improbable. In unusual cases, a failure condition resulting from a single fault can be assessed as extremely improbable if it can be shown that based upon construction, installation and experience such a fault need not be considered as a practical possibility.

d. Analysis for failure conditions involving systems which perform critical functions.

(1) A quantitative safety analysis will generally be necessary for each failure condition identified by the preliminary hazard analysis that would prevent the continued safe flight and landing of the airplane. Such failure conditions should be extremely improbable. If a quantitative safety analysis is required, the analysis may include the following:

(i) FAULT TREE ANALYSIS

(ii) FAILURE MODES AND EFFECTS ANALYSIS--An inductive bottom up analysis which determines what happens to the system upon single failures of its individual parts. These failure modes are used as the bottom level events of the fault tree analysis.

(iii) PROBABILITY ANALYSIS--Determines the probability of the single faults used as bottom level events of the fault tree analysis from failure rate data and exposure times to both active and hidden failures. The probability of all event conditions in the fault tree analysis will then be calculated from this data. The fact that maintenance or flight crew checks will be performed throughout the life of the system is relevant to quantitative analysis. When exposure times applicable to probability calculations for critical functions are affected by flight crew checks or maintenence inspection intervals, these time intervals and check procedures should be clearly specified in appropriate documents. Required flight crew member actions should be

specified in the limitations section of the Airplane Flight Manual. Required maintenance procedures and inspection intervals should be included in the Airworthiness Limitations section of the Instructions for Continued Airworthiness. The required maintenance procedures and inspection intervals should also be made known to the FAA Maintenance Review Board (MRB) which develops the initial aircraft maintenance program. The specific data will be used in determining the initial maintenance requirements for inclusion in the MRB document. Changes to the Airworthiness Limitations section as service experience is gained on the airplane must be approved by the FAA Transport Airplane Certification Directorate. An owner or operator of the airplane may request that alternative inspection intervals and related procedures be set forth in an operations specification approved by the Administrator under Parts 121, 123, 125, 127 or 135 or in accordance with an inspection program approved under FAR 91.217(e). For very simple installations, it may be possible to successfully analyze a failure condition involving a critical function without using the detailed formal procedures outlined above. In general, the simultaneous failure of two reliable independent systems, each of which has dual redundancy, is expected to be extremely improbable.

(2) The increasing use of digital avionics systems in aircraft has focused attention on the probability of failure conditions caused by errors in the specification of system requirements or implementation of system design. Of particular concern are errors in the computer programs used by software based digital equipment. This advisory circular has outlined the use of quantitative safety analysis for evaluating some types of systems which perform critical and essential functions. At this time, valid quantitative methods for evaluating the probability of system errors have not been identified by the aviation industry or the Federal Aviation Administration. However, a design methodology for software based systems has been developed by the Radio Technical Commission for Aeronautics (RTCA). These recommendations are contained in RTCA Document DO-178, are accepted by the FAA, and should be followed for software based systems which perform essential and critical functions.

e. The analytical techniques outlined in this section provide acceptable techniques, but not the only technique for determining compliance with the requirements of FAR 25.1309(b). Other comparable techniques exist and may be proposed by an applicant for use in any certification program. However, these methods should be proposed to the FAA certificating office early in the program. Early agreement between the applicant and the Federal Aviation Administration should be reached on the methods of analysis to be used, identification of critical functions, and assumptions to be used in the acceptance of the proposed analysis.

f. The analysis should be clearly documented. All assumptions, sources of reliability data, failure rates, system functional type (critical, non-essential, essential), etc. should be concisely documented for ease of review. To the extent feasible, the analysis should be self-contained.

7. RECOMMENDATION. The purpose and intent of this advisory circular is to provide guidance. Terms and methods of analysis which may be utilized in

demonstrating compliance with FAR § 25.1309 are included. If additional explanation or discussion is desired, contact the Transport Airplane Certification Directorate, Aircraft Certification Division, Regulations and Policy Office, ANM-110, 17900 Pacific Highway South, C-68966, Seattle, Washington 98168, or phone 206-764-7051.

Charles R. Foster
Director, Transport Airplane Certification Directorate

APPENDIX 1. BACKGROUND INFORMATION FOR CONDUCTING FAILURE ANALYSES

1. INFORMATION SOURCES. For those unfamiliar with the concepts of systems analysis in general and fault tree analysis in particular, the U.S. Nuclear Regulatory Commission has published NUREG-0492, titled "Fault Tree Handbook." This document provides a detailed description of this method of analysis which has been used successfully by various manufacturers to determine the probability of a particular failure condition for FAA certification programs. The handbook also provides a bibliography of additional books, articles, and papers on the subject of reliability. The format of quantitative analyses which use NUREG-0492 as a guide will be acceptable to the FAA. Copies of this document can be obtained from the National Technical Information Service, or from:

GPO Sales
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

If an equipment manufacturer does not have an acceptable record of service experience necessary to estimate the reliability of an item of electronic equipment, MIL-HDBK-217 (Reliability Prediction of Electronic Equipment) may provide a satisfactory means to perform this estimate.

A manufacturer or operator may record service history information on the basis of hours of flight time (block hours), flying hours, operating hours, cycles, etc. This information may be converted into hours of flight time by the application of appropriate conversion factors.

2. IDENTIFICATION AND EVALUATION OF CRITICAL FUNCTIONS. The preliminary hazard analysis is noted in this advisory circular as a means of identifying critical and essential functions and the systems which must operate properly to accomplish these functions. Critical functions are generally those for which no satisfactory substitute is available and which must be accomplished for continued safe flight and landing of the airplane.

Examples of some systems which perform critical functions that have been identified on various transport category airplanes are listed below. This list is only provided to illustrate the types of functions which may be critical. Each airplane model must be examined to determine what functions are critical.

a. The primary flight control system.

b. Hydraulic power for airplanes with powered flight control systems and no manual reversion.

c. Secondary flight control systems, if failure of these systems can result in uncontrolled flight.

d. Engine control system elements that affect all engines simultaneously.

e. For airplanes certificated for flight in instrument meteorological conditions, the total systems and displays which provide the flight crew with any of the following:

(1) Attitude Information

(2) Altitude Information

(3) Airspeed Information

f. Automatic landing system for use in low visibility landings.

When determining the extent of the analysis to be conducted for failure conditions involving systems which perform critical functions, a number of factors should be considered. A failure modes and effects analysis should be performed on a system which performs critical functions if its complexity is such that the effects of its failure modes are not obvious. A quantitative analysis is normally needed only when systems which perform critical functions differ significantly in design or application, as listed below, from existing systems which satisfactorily perform these functions.

a. Technology

b. Interrelationship with other systems on the airplane.

c. Relationships between the system and critical characteristics of the airplane.

d. Complexity

For example, systems performing critical functions, such as a mechanical control cable system for primary flight controls with dual redundancy or a hydraulic power system with triple or quadruple redundancy used by a fully powered flight control system would not necessarily be the subject of a quantitative analysis. However, even if these systems were similar in design to those in current service, they would normally be the subject of a failure modes and effects analysis.

When it has been determined that a quantitative analysis should be conducted, the following should be considered:

a. Human errors in operation and maintenance. The design of systems which perform critical functions should be such that failure of the systems do not require flight crew action to prevent the failure condition beyond the tasks normally required to fly the airplane, or that system failures which require flight crew intervention provide a clear and unmistakable annunciation to alert the flight crew that the failure has occurred and the subsequent flight crew member actions necessary to prevent the failure condition can be satisfactorily accomplished. The failure annunciation and the required flight crew member actions should be evaluated by FAA flight test pilots to determine if the necessary actions can be satisfactorily accomplished in a timely manner without

exceptional pilot skill or strength. If satisfactory action by the flight crew is doubtful, then reliance on flight crew intervention should not be assumed in determining the probability of the failure condition. If the evaluation determines that satisfactory intervention can be expected from a properly trained flight crew, then the occurrence of the failure condition has been prevented.

In a similar manner, an assessment should be made of the design and of the maintenance instructions with the object of eliminating the possibility of maintenance errors which could result in a failure condition. Maintenance tasks which are required should be evaluated to determine if they can be reasonably accomplished. For the purposes of a quantitative analysis, the satisfactory accomplishment of identified maintenance tasks should be assumed to be one (1). The FAA believes that a numerical assessment of the probability of human error on the part of the flight crew or maintenance personnel is not appropriate for the purposes of conducting a design analysis.

b. System Independence and Redundancy. The most often encountered difficulty with quantitative analyses presented to the FAA has been the improper treatment of events which are not mutually independent. The probability of occurrence of two events which are mutually independent may be multiplied to obtain the probability that both events occur using the formula:

$$P(A \text{ and } B) = P(A)P(B).$$

This multiplication will produce an incorrect solution if A and B are not mutually independent. Often a quantitative analysis will be defective because a single failure will be included as a primary event at more than one location and then improperly combined with itself in computing the probability of the top event of a fault tree.

Another persistent problem is the identification of common failure modes which simultaneously affect the operation of two or more separate systems which otherwise are independent. The loss of electrical power, hydraulic power, or cooling may often result in common failure modes. A failure modes and effects analysis is often useful in identifying common failure modes.

U.S. Department
of Transportation

**Federal Aviation
Administration**

800 Independence Ave., S.W.
Washington, D.C. 20591

Official Business
Penalty for Private Use $300

RETURN POSTAGE GUARANTEED

Postage and Fees Paid
Federal Aviation
Administration
DOT 515

THIRD CLASS BULK RATE

★ U. S. GOVERNMENT PRINTING OFFICE : 1982 381-428/2295