SAE *The Engineering Society*
For Advancing Mobility
Land Sea Air and Space®
I N T E R N A T I O N A L®
400 Commonwealth Drive, Warrendale, PA 15096-0001

AEROSPACE RECOMMENDED PRACTICE

SAE **ARP4761**

Issued   1996-12

GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SAE ARP4761

ACKNOWLEDGMENTS

The leadership of the S-18 Committee would like to thank the actively contributing committee members, and their sponsoring companies, for the time, effort, and expense expended during the years of development of this document. Without the experience, cooperation and dedication of these people, development of this document would not have been possible.

Thanks to the following committee members.

1.   SCOPE:

This document describes guidelines and methods of performing the safety assessment for certification of civil aircraft. It is primarily associated with showing compliance with FAR/JAR 25.1309. The methods outlined here identify a systematic means, but not the only means, to show compliance. A subset of this material may be applicable to non-25.1309 equipment. The concept of Aircraft Level Safety Assessment is introduced and the tools to accomplish this task are outlined. The overall aircraft operating environment is considered.

When aircraft derivatives or system changes are certified, the processes described herein are usually applicable only to the new designs or to existing designs that are affected by the changes. In the case of the implementation of existing designs in a new derivation, alternate means such as service experience may be used to show compliance.

1.1   Purpose:

This document presents guidelines for conducting an industry accepted safety assessment consisting of Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA).

This document also presents information on the safety analysis methods needed to conduct the safety assessment. These methods include the Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Failure Modes and Effect Analysis (FMEA), Failure Modes and Effects Summary (FMES) and Common Cause Analysis (CCA). [CCA is composed of Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), and Common Mode Analysis (CMA)].

1.2   Intended Users:

The intended users of this document include, but are not limited to, airframe manufacturers, system integrators, equipment suppliers and certification authorities who are involved with the safety assessment of civil aircraft and associated systems and equipment.

1.3   How To Use This Document:

The guidelines and methods provided in this document are intended to be used in conjunction with other applicable guidance materials, including ARP4754, RTCA/DO-178, RTCA SC-180 Document DO-(TBD), and with the advisory material associated with FAR/JAR 25.1309. (For engines and propeller applications, reference the applicable FAR/JAR advisory material.) The intent of this document is to identify typical activities, methods, and documentation that may be used in the performance of safety assessments for civil aircraft and their associated systems and equipment. The specific application of such activities needs to be established by the organization conducting the assessment and the appropriate recipient.

1.3   (Continued):

This document provides general guidance in evaluating the safety aspects of a design. The primary analytical methods and tools and the relationship of these are introduced. Users who need further information on a specific method or tool may obtain detailed information from appendices A through K. These appendices provide information on Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects Summary (FMES), Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA) and Common Modes Analysis (CMA). Appendix L provides an example of the safety assessment process for a hypothetical system. This contiguous example illustrates the relationships between the processes and methods in creating the overall safety evaluation of an aircraft or system as it develops through the design cycle.

NOTE: The appendices are not stand alone documents, but are intended to be used in conjunction with the information contained in the basic document. The user is cautioned not to use the appendices independent of the basic document. Further, the examples in the Appendix L "Contiguous Example" should not be used without making reference to the corresponding appendix and to the main body of this document.

Examples presented in this document, including documentation examples, are intended only as guidance. The examples should not be interpreted as an addition to or an amplification of any requirement.

Throughout this document and the appendixes, reference is made to using Fault Tree Analyses. It should be understood by the reader that Dependence Diagrams or Markov Analyses may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

ARP1834 and ARP926A contain information about Fault/Failure Analysis but are superseded by this document for purposes of civil aircraft safety assessment. They are being amended to reflect this supersession.

2.   REFERENCES:

2.1   Applied Documents:

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1   SAE Publications: Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

ARP4754   Certification Considerations for Highly-Integrated or Complex Aircraft Systems

2.1.2   U.S. Government Publications: Available from DODSSP, Subscription Services Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

MIL-HDBK-217   Reliability Prediction of Electronic Equipment, Reliability Analysis Center
MIL-HDBK-338   Reliability Engineering Handbook
MIL-HDBK-978   NASA Parts Application Handbook

2.1.3   FAR Publications: Available from FAA, 800 Independence Avenue, SW, Washington, DC 20591

FAR 25.1309   Airworthiness Standards: Transport Category Airplanes, Federal Aviation Regulations
AC 25.19

2.1.4   RTCA Publications: Available from RTCA Inc., 1140 Connecticut Ave., NW, Suite 1020, Washington, DC 20036

RTCA/DO-178   Software Considerations in Airborne Systems and Equipment Certification, RTCA Inc.
RTCA/DO-TBD   Design Assurance Guidance for Airborne Electronic Hardware (RTCA Special Committee -180)

2.1.5   Other References:

JAR 25.1309   Large Aeroplanes, Joint Aviation Requirement
AC 25.1309-1A   System Design and Analysis, Advisory Circular, FAA
AMJ 25.1309   System Design and Analysis, Advisory Material Joint, JAA
NUREG-0492   Fault Tree Handbook, U.S. Nuclear Regulatory Commission
RAC NPRD   Nonelectronic Parts Reliability Data
RAC FMD-91   Failure Mode/Mechanism Distribution
GIDEP   Government Industry Data Exchange Program
Rome Laboratory   Reliability Engineers Toolkit

2.2   Definitions:

   NOTE: An effort has been made to maintain consistency between the definitions in ARP4754 and those in this document.

   AIRWORTHINESS: The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.

   ANALYSIS: An evaluation based on decomposition into simple elements.

   APPROVAL: The act of formal sanction of an implementation by a certification authority.

   APPROVED: Accepted by the certification authority as suitable for a particular purpose. (ICAO)

   ASSESSMENT: An evaluation based upon engineering judgement.

   ASSUMPTION: Statements, principles and/or premises offered without proof.

   ASSURANCE: The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements. (RTCA DO 178B)

   "AT RISK" TIME: The period of time during which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.

   AUTHORITY: The organization or person responsible within the State (Country) concerned with the certification of compliance with applicable requirements.

   AVAILABILITY: Probability that an item is in a functioning state at a given point in time.

   CERTIFICATION: The legal recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or other documents as required by national laws and procedures.

   CERTIFICATION AUTHORITY: Organization or person responsible for granting approval on behalf of the nation of manufacture.

   COMMON CAUSE: Event or failure which bypasses or invalidates redundancy or independence.

   COMMON CAUSE ANALYSIS: Generic term encompassing Zonal Analysis, Particular Risks Analysis and Common Mode Analysis.

   COMMON MODE FAILURE: An event which affects a number of elements otherwise considered to be independent.

2.2   (Continued):

COMPLEXITY: An attribute of systems or items which makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

COMPLIANCE: Successful performance of all mandatory activities; agreement between the expected or specified result and the actual result.

COMPONENT: Any self-contained part, combination of parts, subassemblies or units, which perform a distinct function necessary to the operation of the system.

CONFORMITY: Agreement of physical realization of the item with the defining document.

CRITICALITY: Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone, in combination or in combination with external events.

DEFECT: State of an item consisting of the non-performance of specified requirements by a characteristics of the item. A defect may, but need not, lead to a failure.

DEMONSTRATION: A method of proof of performance by observation.

DERIVED REQUIREMENTS: Additional requirements resulting from design or implementation decisions during the development process. Derived requirements are not directly traceable to higher level requirements; though derived requirements can influence higher level requirements.

DESIGN: The result of the design process.

DESIGN PROCESS: The process of creating a system or an item from a set of requirements.

DEVELOPMENT ASSURANCE: All those planned and systematic actions used to substantiate, to an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable certification basis.

DEVELOPMENT ERROR: A mistake in requirements determination or design.

ERROR: (1) An occurrence arising as a result of an incorrect action or decision by personnel operating or maintaining a system. (JAA AMJ 25.1309) (2) A mistake in specification, design, or implementation.

EVENT: An occurrence which has its origin distinct from the aircraft, such as atmospheric conditions (e.g., wind gusts, temperature variations, icing, lighting strikes), runaway conditions, cabin and baggage fires. The term is not intended to cover sabotage. (JAA AMJ 25.1309) Note: This definition, as it is stated here, describes an "External Event". There are other uses of "event" that covers other aspects (e.g., FTA events).

2.2   (Continued):

EXCHANGED FUNCTION: Interdependencies between functions.

EXPOSURE TIME: The period of time between when an item was last known to be operating properly and when it will be known to be operating properly again.

FAILURE: A loss of function or a malfunction of a system or a part thereof. Note: This differs from the ARP 4754 definition and conforms to the AC/AMJ 25.1309 definition.

FAILURE CONDITION: A condition with an effect on the aircraft and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions. A Failure Condition is classified in accordance to the severity of its effects as defined in FAA AC 25.1309-1A or JAA AMJ 25.1309.

FAILURE EFFECT (FE): A description of the operation of a system or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of a system or an item.

FAILURE MODE (FM): The way in which the failure of an item occurs.

FAILURE RATE: The gradient of the failure distribution function divided by the reliability distribution function at time t. $\lambda t = F'(t)/(1-F(t))$

If the failure distribution function is exponential, the failure rate is constant and the failure rate can be approximately calculated by dividing the number of failures within a hardware item population, by the total unit operating hours. Note: Failure rate could also be expressed in terms of failures per flight hour or per cycle.

FAULT: An undesired anomaly in an item or system.

FUNCTIONAL HAZARD ASSESSMENT (FHA): A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity.

GUIDELINES: Recommended procedures for complying with regulations.

HARDWARE: An object that has physical being. Generally refers to LRUs, circuit cards, power supplies, etc.

HAZARD: A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof.

IMPLEMENTATION: The act of creating a physical reality from a specification.

INDEPENDENCE: (1) A design concept which ensures that the failure of one item does not cause a failure of another item. (Derived from JAA AMJ 25.1309.) (2) Separation of responsibilities that assures the accomplishment of objective evaluation.

2.2   (Continued):

INSPECTION: An examination of an item against a specific standard.

INTEGRATION: (1) The act of causing elements of an item to function together. (2) The act of gathering a number of separate functions within a single implementation.

ITEM: One or more hardware and/or software elements treated as a unit.

LATENT FAILURE: A failure which is not detected and/or annunciated when it occurs.

MALFUNCTION: The occurrence of a condition whereby the operation is outside specified limits.

NOVELTY: Applicable to systems using new technology and to systems using a conventional technology not previously used in connection with the particular function in question.

PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA): A systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items.

PRODUCT: An item generated in response to a defined set of requirements.

REDUNDANCY: Multiple independent means incorporated to accomplish a given function.

RELIABILITY: The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time.

REQUIREMENT: An identifiable element of a specification that can be validated and against which an implementation can be verified.

RISK: The frequency (probability) of occurrence and the associated level of hazard.

SEGREGATION: The maintenance of independence by means of a physical barrier between two hardware components.

SEPARATION: The maintenance of independence by means of physical distance between two hardware components.

SIMILARITY: Applicable to systems similar in characteristics and usage to systems used on previously certified aircraft. In principle, there are no parts of the subject system more at risk (due to environment or installation) and that operational stresses are no more severe than on the previously certified system.

SOFTWARE: Computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system.

SPECIFICATION: A collection of requirements which, when taken together, constitute the criteria which define the functions and attributes of a system, or an item.

2.2   (Continued):

SYSTEM: A combination of inter-related items arranged to perform a specific function(s).

SYSTEM SAFETY ASSESSMENT (SSA): A systematic, comprehensive evaluation of the implemented system to show that the relevant requirements are met.

SYSTEM SAFETY ASSESSMENT PROCESS: The complete process applied during the design of the system to establish safety objectives and to demonstrate compliance with FAR/JAA 25.1309 and other safety related requirements.

VALIDATION: The determination that the requirements for a product are sufficiently correct and complete.

VERIFICATION: The evaluation of an implementation to determine that applicable requirements are met.

2.3   Acronyms:

AC	Advisory Circular
A/C	Aircraft
ACJ	Advisory Circular Joint
AMJ	Advisory Material Joint
ARP	Aerospace Recommended Practice (SAE)
CCA	Common Cause Analysis
CMA	Common Mode Analysis
CMR	Certification Maintenance Requirement (FAA AC 25-19)
DD	Dependence Diagram
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FC	Failure Condition
FC&C	Failure Conditions and Classifications
FE	Failure Effects
FHA	Functional Hazard Assessment
FM	Failure Modes
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes and Effects Summary
FTA	Fault Tree Analysis
H/W	Hardware
HIRF	High Intensity Radiated Fields
JAA	Joint Aviation Authorities
JAR	Joint Aviation Requirements
LRU	Line Replacement Unit
MA	Markov Analysis
MRB	Maintenance Review Board
MSG-3	Maintenance Steering Group 3
PRA	Particular Risks Analysis
PSSA	Preliminary System Safety Assessment

2.3   (Continued):

      RTCA   (Previously) Radio Technical Commission for Aeronautics
      SAE   Society of Automotive Engineers, Inc.
      SSA   System Safety Assessment
      S/W   Software
      ZSA   Zonal Safety Analysis

3.   SAFETY ASSESSMENT PROCESS:

3.1   Safety Assessment Overview:

The safety assessment process includes requirements generation and verification which supports the aircraft development activities. This process provides a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards have been properly addressed. The safety assessment process is qualitative and can be quantitative

The safety assessment process should be planned and managed to provide the necessary assurance that all relevant failure conditions have been identified and that all significant combinations of failures which could cause those failure conditions have been considered.

The safety assessment process for integrated systems should take into account any additional complexities and interdependencies which arise due to integration. In all cases involving integrated systems, the safety assessment process is of fundamental importance in establishing appropriate safety objectives for the system and determining that the implementation satisfies these objectives.

Figure 1 diagrams a top-level view of the safety assessment process (Functional Hazard Assessment, Preliminary System Safety Assessment, and System Safety Assessment) and how the safety assessment methods relate to that process. The development process is iterative in nature. The safety assessment process is an inherent part of this process. The safety assessment process begins with the concept design and derives the safety requirements for it. As the design evolves, changes are made and the modified design must be reassessed. This reassessment may create new derived design requirements. These new requirements may necessitate further design changes. The safety assessment process ends with the verification that the design meets the safety requirements. A typical development cycle timeline is shown across the top to show the chronological relationship of the safety process to the development process. Safety processes that are linked in the design process are grouped in boxes to highlight this relationship.

A Functional Hazard Assessment (FHA) is conducted at the beginning of the aircraft/system development cycle. It should identify and classify the failure condition(s) associated with the aircraft functions and combinations of aircraft functions. These failure condition classifications establish the safety objectives. These objectives are outlined in Table 1.

Typical Development Cycle
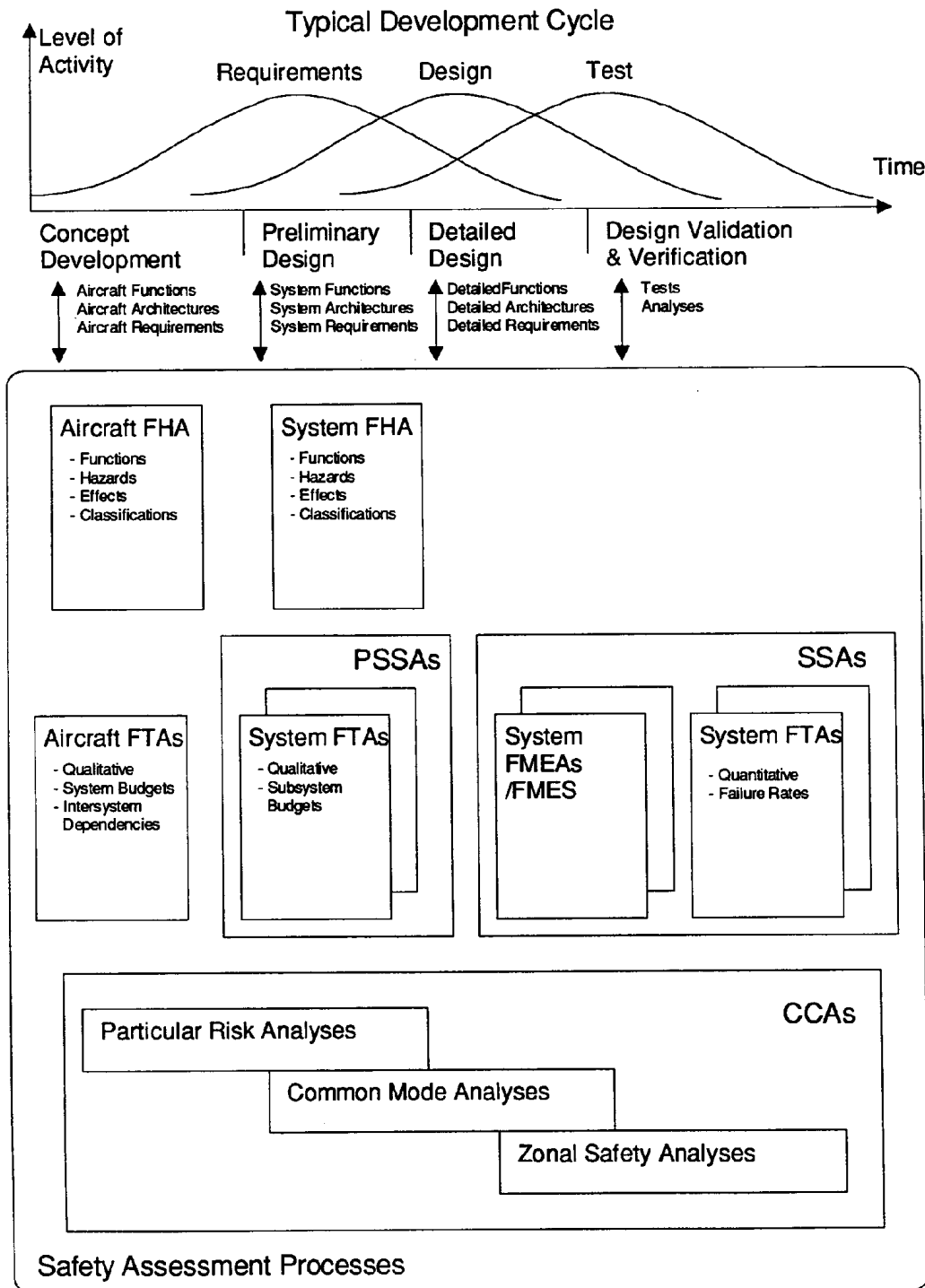
FIGURE 1 - Overview of the Safety Assessment Process

TABLE 1 - Failure Condition Severity as Related to Probability Objectives and Assurance Levels

Probability (Quantitative)		1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
				Per flight hour		
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants		- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A

Note: A "No Safety Effect" Development Assurance Level E exists which may span any probability range.

3.1   (Continued):

The goal in conducting the FHA is to clearly identify each failure condition along with the rationale for its classification. After aircraft functions have been allocated to systems by the design process, each system which integrates multiple aircraft functions should be re-examined using the FHA process. The FHA is updated to consider the failure of single or combinations of aircraft functions allocated to a system. The output of the FHA is used as the starting point for conducting the Preliminary System Safety Assessment (PSSA).

The PSSA is a systematic examination of the proposed system architecture(s) to determine how failures can cause the functional hazards identified by the FHA. The objective of the PSSA is to establish the safety requirements of the system and to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the FHA.

The PSSA is also an interactive process associated with the design definition. The PSSA is conducted at multiple stages of the system development including system, item, and hardware/software design definitions. At the lowest level, the PSSA determines the safety related design requirements of hardware and software. The PSSA usually takes the form of an FTA (DD or MA may also be used) and should also include common cause analysis.

The System Safety Assessment (SSA) is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the FHA and derived safety requirements from the PSSA are met. The SSA is usually based on the PSSA FTA (DD or MA may also be used) and uses the quantitative values obtained from the Failure Modes and Effects Summary (FMES). The SSA should verify that all significant effects identified in the FMES are considered for inclusion as primary events in the FTA. The FMES is a summary of failures identified by the FMEA(s) which are grouped together on the basis of their failure effects. The SSA must also include applicable common cause analysis results.

Each system architecture establishes the structure and boundaries that the specific system design has implemented. A Common Cause Analysis (CCA) should support the development of the specific system architecture and that of related systems by evaluating the overall architecture sensitivity to common cause events. These common cause events are evaluated by performing the following analyses: Particular risk analysis, zonal safety analysis, and common mode analysis. The results of aircraft level common cause analyses are fed into the PSSA and SSA for each system.

When conducting FTAs for either the PSSA or SSA, both the failure detection means allocated to maintenance tasks and related exposure times used in the analysis must be consistent with the maintenance tasks and intervals used by the maintenance program for the aircraft. In many cases, failure detection means are provided by flight deck effects or are inherent within the system (e.g., being provided by self-test, power up tests, etc.).

Dependence Diagrams are essentially equivalent to FTAs and the selection of one over the other is left to the personal preference of the analyst. Markov Analysis techniques are often useful when dealing with deferred maintenance scenarios. Appendixes D, E, and F list some of the advantages of using FTA, DD, and MA respectively.

3.1   (Continued):

The safety assessment process is more than just quantitative. It includes consideration of such qualitative issues as Development Assurance Levels, HIRF and lightning strike, etc. Much of this is included in the Common Cause Analysis (Appendixes I, J, and K).

The safety assessment process is complete when the SSA results are verified against the system level and aircraft level FHAs.

3.2   Functional Hazard Assessment (FHA):

A Functional Hazard Assessment is defined as a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity. An FHA is usually performed at two levels. These two analyses are known as an aircraft level FHA and a system level FHA.

The aircraft level FHA is a high level, qualitative assessment of the basic functions of the aircraft as defined at the beginning of aircraft development. An aircraft level FHA should identify and classify the failure conditions associated with the aircraft level functions. However, if separate systems use similar architectures or identical complex components and introduce additional aircraft level failure conditions involving multiple function, then the FHA should be modified to identify and classify these new failure conditions. The classification of these failure conditions establishes the safety requirements that an aircraft must meet. The goal in conducting this FHA is to clearly identify each failure condition along with the rationale for its severity classification.

The system level FHA is also a qualitative assessment which is iterative in nature and becomes more defined and fixed as the system evolves. It considers a failure or combination of system failures that affect an aircraft function. Assessment of any particular hardware or software item is not the goal of the system level FHA. However, if separate systems use similar architectures or identical complex components and introduce additional system level failure conditions involving integrated multiple functions, then the FHA should be modified to identify and classify these new failure conditions. The Development Assurance Level of an aircraft function depends on the severity of the effects of failures or development errors of that function on the aircraft, crew, or occupants. The Development Assurance Level of each item depends on both the system architecture and the resulting failure effects of the item on the functions performed by the system.

After aircraft functions have been allocated to systems by the design process, each system which integrates multiple aircraft functions should be re-examined using the system level FHA process.

3.2   (Continued):

The output of the aircraft level and/or system level FHAs is the starting point for the generation and allocation of safety requirements. An FTA (DD or MA) can be used to derive the lower level requirements from those identified in the FHAs (aircraft fault trees for the aircraft FHA and PSSA fault trees for system FHA). These derived requirements should be captured as requirements in aircraft and system specifications. Figure 2 shows the overall relationship between the FHA/FTA/FMEA. The figure shows an example of how the FHAs generate the top level events in the FTAs. The figure also highlights how the quantitative results from FMEA and FTA feed back into the system level and aircraft level FTAs to show compliance with numerical safety requirements from FHAs.

For details in performing the FHA, refer to Appendix A.

3.3   Preliminary System Safety Assessment (PSSA):

A PSSA is used to complete the failure conditions list and the corresponding safety requirements. It is also used to demonstrate how the system will meet the qualitative and quantitative requirements for the various hazards identified. The PSSA process identifies protective strategies, taking into account fail safe concepts and architectural attributes which may be needed to meet the safety objectives. It should identify and capture all derived system safety requirements (e.g., protective strategies such as partitioning, built-in-test, dissimilarity, monitoring, safety related tasks and intervals, etc.). The PSSA outputs should be used as inputs to the SSA and other documents, including, but not limited to, system requirements, hardware requirements and software requirements.

The PSSA is an iterative analysis imbedded within the overall development. It is an on-going process starting in the early phases of the design with the allocation of aircraft functions and their requirements to the system level. System level requirements are then allocated to items and finally item requirements will be allocated to hardware and software. Allocation of risk to items will determine hardware reliability requirements and development assurance requirements for both hardware and software (see ARP4754). These requirements and assurance levels are captured in item specifications.

The PSSA should identify failures contributing to the failure conditions from the system FHA. Possible contributing factors leading to failure conditions may be identified by using FTA, DD, MA, or other analysis methods. Hardware failures and possible hardware/software errors, as well as faults arising from common causes, should be included in the PSSA to show their contribution and to derive what system and item safety requirements are needed. Care should be taken to account for potential latent faults and their associated exposure times.
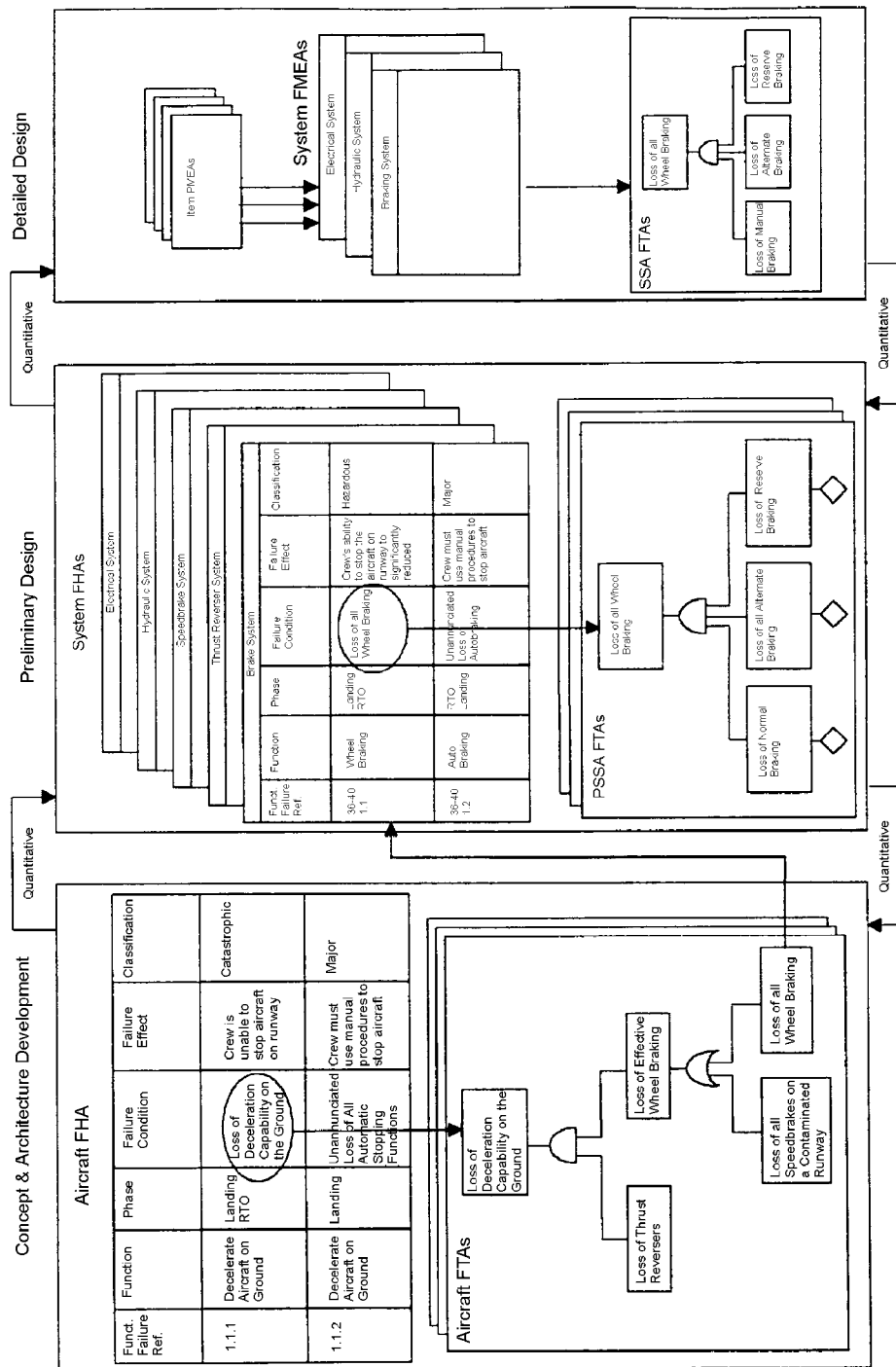
FIGURE 2 - Example of the Relationship Between FHAs and FTA/FMEAs

3.3   (Continued):

The inclusion of hardware and software errors in a qualitative manner in this analysis shows their contribution to the various failure conditions and can provide valuable information on deriving the Development Assurance Levels (refer to ARP4754). The PSSA can also identify the specific safety related requirements for software such as containment boundary definitions, partitioning strategies, and specific verification strategies. The existence of such requirements should be captured as part of the system requirements.

The left side of the Safety Assessment Diagram, Figure 3, indicates the recommended sequence of steps in the PSSA process. Not all the steps will be needed for every assessment, but each must be considered for applicability. The following two paragraphs describe the left side of Figure 3. Note that wherever FTA is shown it can be replaced by an equivalent analysis method such as DD or MA.

The PSSA process has two main inputs, the system FHA and the aircraft FTA. The system FHA yields failure conditions and classifications necessary for the next steps. The aircraft FTA determines the functional failures of concern. The aircraft FTA is supplemented by the Common Cause Analysis (CCA) to generate the top failure effects for the system FTA. The CCA also establishes the systems requirements such as redundancy, separation and independence of functions needed to be implemented by the design of the system.

The CCA at the system level supplements the output of the system FTA to yield the top failure effects at the item level for use in the item FTA. The item CCA also supplements the item FTA to further establish the design requirements, Development Assurance Levels, and hardware reliability requirements. These established requirements are used as the design specification requirements for the hardware and software of individual items. The output of the PSSA is intended to identify hardware failure effects, development error effects of hardware and software, reliability budgets, and Development Assurance Levels. The PSSA should also establish protective strategies and architectural features necessary to meet safety objectives.

Safety requirements generated from the base events of the PSSA fault tree should be provided to the FMEA analyst. This information may take the form of failure effects and failure rate budgets to assure that specific failure effect are addressed in the FMEA. This information helps the FMEA analyst determine the emphasis and depth of analysis of the FMEA.

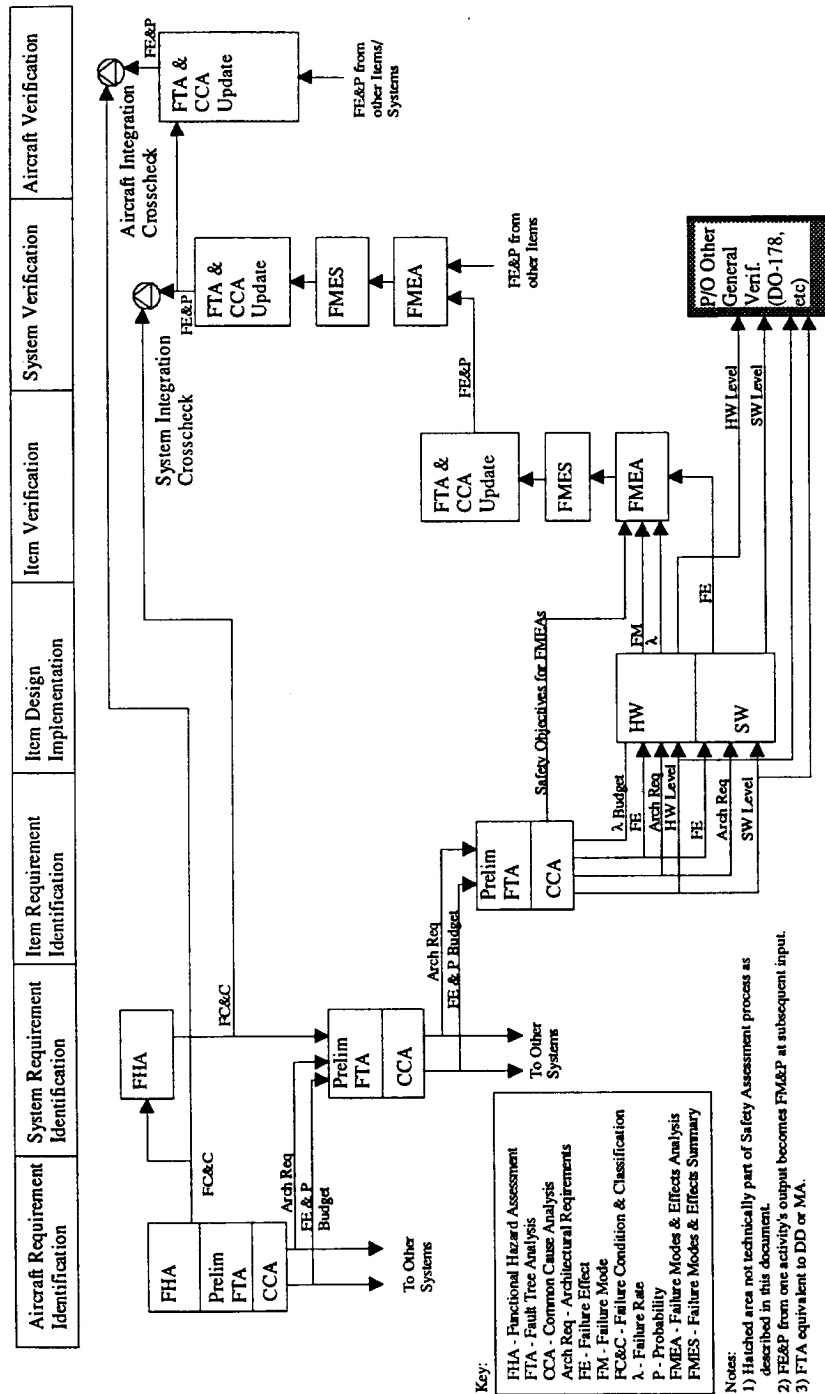For details in performing the PSSA, refer to Appendix B.

FIGURE 3 - Safety Assessment Diagram

3.4   System Safety Assessment (SSA):

A System Safety Assessment is a systematic, comprehensive evaluation of the implemented system to show that relevant safety requirements are met. The analysis process will be similar to the activities of the PSSA but different in scope. The difference between a PSSA and an SSA is that a PSSA is a method to evaluate proposed architectures and derive system/item safety requirements; whereas the SSA is a verification that the implemented design meets both the qualitative and quantitative safety requirements as defined in the FHA and PSSA.

The SSA integrates the results of the various analyses to verify the safety of the overall system and to cover all the specific safety considerations identified in the PSSA. The SSA process documentation includes results of the relevant analyses and their substantiations as needed. This may include the following information.

a. List of previously agreed upon external event probabilities
b. System description
c. List of failure conditions (FHA, PSSA)
d. Failure condition classification (FHA, PSSA)
e. Qualitative analyses for failure conditions (FTA, DD, FMES)
f. Quantitative analyses for failure conditions (FTA, DD, MA, FMES, etc.)
g. Common Cause Analyses
h. Safety related tasks and intervals (FTA, DD, MA, FMES, etc.)
i. Development Assurance Levels for hardware and software (PSSA)
j. Verification that safety requirements from the PSSA are incorporated into the design and/or testing process
k. The results of the nonanalytic verification process (i.e., test, demonstration and inspection activities)

The right side of the Safety Assessment Process Diagram, Figure 3, indicates the recommended sequence of steps in the SSA process. Not all the steps will be needed for every assessment, but each must be considered for applicability. The following two paragraphs describe the right side of Figure 3. Note that wherever FTA is shown, it can be replaced by an equivalent safety assessment analysis method such as a DD or MA.

The SSA process flow is generally represented through succeeding levels of verification. Through these upward hierarchical verification levels, hardware reliability requirements, architectural requirements and hardware and software Development Assurance Levels are verified against the safety requirements delineated in the PSSA process. The lower level of design is again evaluated to determine compliance with derived requirements. DO-178 procedures should be used to verify that the software implementation meets the required Development Assurance Levels. The applicant should establish appropriate development assurance procedures for hardware with the agreement of the Certification Authorities. The hardware Development Assurance Level is verified via procedures that are to be defined by RTCA SC-180.

3.4   (Continued):

An item level FMEA is performed and is summarized into the item FMES to support the failure rates of the failure modes considered in the item FTA/CCAs. The system FMEA is summarized into the system FMES to support the failure rates of the failure modes considered in the system FTA. The system is reviewed via FTA/CCA to identify the failure modes and probabilities used in the aircraft FTA. The aircraft FTA/CCA is used to establish compliance with the aircraft level failure conditions and probabilities by comparison with the aircraft FHA. As items are integrated into systems and systems are integrated into the aircraft, the failure effects are compared with the failure conditions identified in the FHA. This comparison is called an "Integration cross-check" in Figure 3.

For details in performing the SSA, refer to Appendix C.

3.5   Verification Means Used for Aircraft Certification:

For each failure condition, it should be determined how the aircraft/system will satisfy the safety objective. The flowchart depicted in Figure 4 provides guidance in defining a verification plan for the failure conditions in a given system. The most difficult category to determine a course of assessment for is the Major category. The flow chart provides some guidance on how to approach verification of failures categorized as Major.

4.   SAFETY ASSESSMENT ANALYSIS METHODS:

4.1   Fault Tree Analysis/Dependence Diagram/Markov Analysis (FTA/DD/MA):

Fault Tree Analysis (FTA), Dependence Diagram (DD), and Markov Analysis (MA) are top-down analysis techniques. These analyses proceed down through successively more detailed (i.e., lower) levels of the design.

After identifying the failure conditions in the FHA, the FTA/DD/MA can be applied as part of the PSSA to determine what single failures or combinations of failures can exist (if any) at the lower levels that might cause each failure condition. When an FMEA/FMES is performed, a comparison should be accomplished to ensure all significant effects identified are in the FTA/DD/MA as Basic Events. The FTA/DD/MA Basic Events get their failure rates from the FMEAs and/or FMESs.

For details in performing the FTA, refer to Appendix D. For details in performing the DD, refer to Appendix E. For details in performing the MA, refer to Appendix F.

4.1.1   Applications of the FTA/DD/MA: The completed FTA/DD/MA facilitates technical and management assessments and reviews because it identifies only the failure events which could individually or collectively lead to the occurrence of the undesired top event. In contrast, an FMEA lists only single failures, including some which may be of no concern.

The FTA/DD/MA facilitates subdivision of system level events into lower level events for ease of analysis.

System FHA Failure Conditions

Is Condition Hazardous or Catastrophic?

Yes

No

Is Condition Major?

No

Yes

Is System Complexity High?

Yes

No

Is Service Experience Relevant?

No

Yes

Qualitative and Quantitatve Analyses

*

Qualitative Analyses

FHA Summary
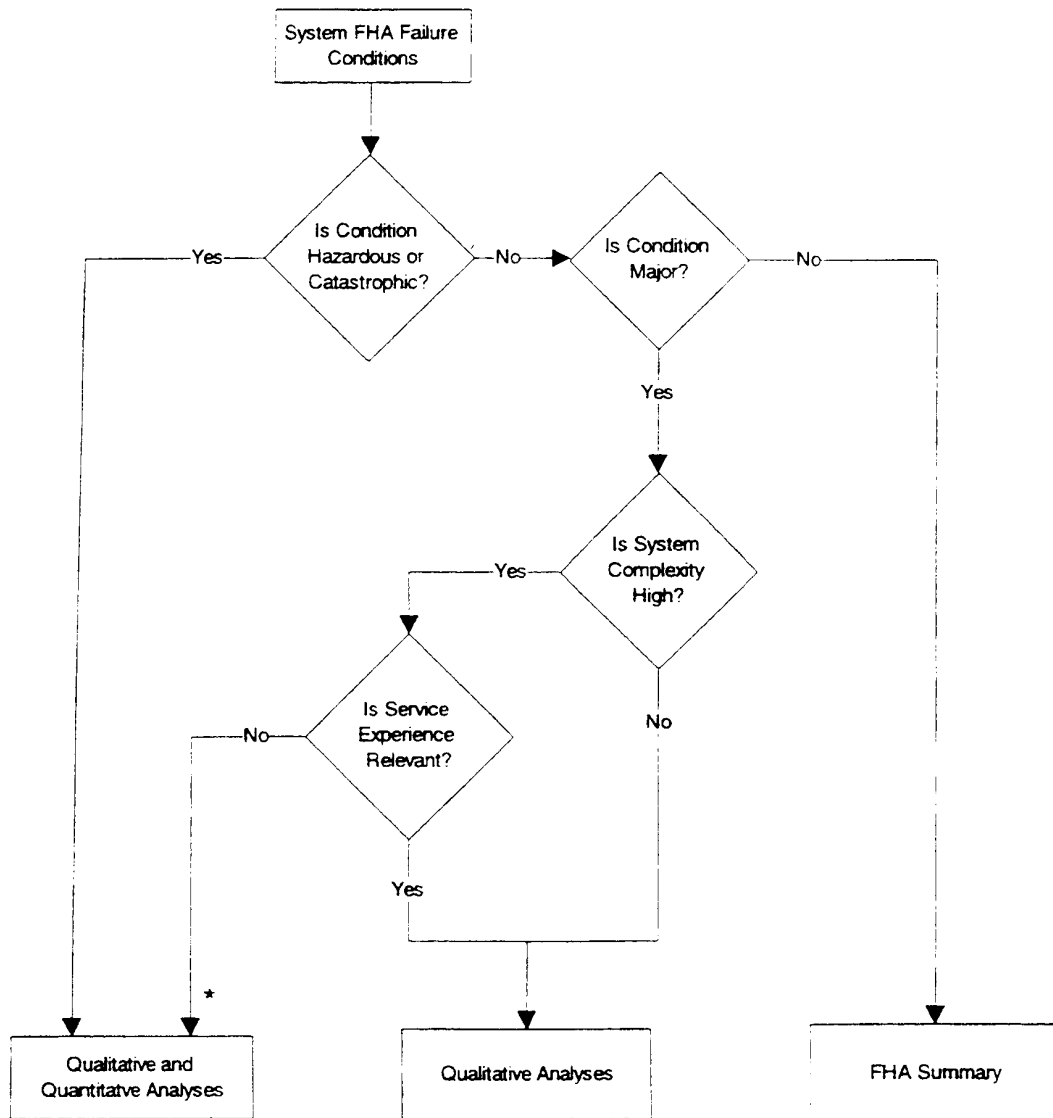
* Major Failure Conditions may be satisfactorily analysed with methods that are less rigorous and complete than those for Catastrophic or Hazardous Failure Conditions (e.g. FMEA containing failure rates)

FIGURE 4 - Safety Objective Verification Approach

4.1.1   (Continued):

The FTA/DD/MA may be used to:

a. Quantify probability of occurrence for the top event.
b. Evaluate proposed system architecture attributes to establish hardware reliability budgets and Development Assurance Levels for hardware and software during the PSSA process.
c. Assess the impact of a design modification.
d. Identify the need for a design modification and/or identify unique situations that require special attention.
e. Show compliance with qualitative and/or quantitative safety objectives as part of the SSA.
f. Provide a visual aid to qualitatively illustrate the significance of the software with respect to the failure condition classification of a top level event.
g. Establish crew and maintenance tasks and intervals necessary to meet the requirements of the safety assessment.

A Fault Tree Analysis uses Boolean logic gates to show the relationship of failure effects to failure modes. The two most common logic gates are the AND-gate and the OR-gate. An AND-gate represents a condition in which the coexistence of all inputs is required to produce an output representing the higher level event. An OR-gate represents a condition in which one or more inputs produce an output representing the higher level event.

The DD replaces the FTA logic gates by paths to show the relationship of the failures; parallel paths are equivalent to the AND-gates and series paths are equivalent to the OR-gates.

An MA calculates the probability of the system being in various states as a function of time. A state in the model represents the system status as a function of both the fault-tree and faulty components and the system redundancy. A transition from one state to another occurs at a given transition rate, which reflects component failure rates and redundancy. A system changes state due to various events such as component failure, reconfiguration after detection of a failure, completion of repair, etc. Each state transition is a random process which is represented by a specific differential equation. The differential nature of the model limits the computation at any point in the analysis to the probability of transitioning from any defined state to another state. The probability of reaching a defined final state can be computed by combinations of the transitions required to reach that state.

4.1.2   Software in FTA/DD/MA: Embedded software may be qualitatively included in the FTA/DD/MA for certain systems and items. In particular, FTA/DD/MA may be necessary to provide adequate analytic visibility of software safety issues for complex systems, especially when credit is taken for the following safety attributes.

a. Systems and items which provide fail-safe protection against software errors (The protection may be provided either via other software or via hardware alone.)
b. Systems and items in which software provides fail-safe protection against hardware errors or hardware faults
c. Systems and items in which software provides protection against latent hardware faults.

SAE ARP4761

4.1.2   (Continued):

When software is included in fault trees, the relationship between the top level hazards and specific software anomalous behaviors should be clearly established. It is important to explicitly identify the affected functions and to identify how the specified intended functions are affected. Specific protective strategies can be determined from the various potential cause factors associated with the specific software anomalous behaviors. These protective strategies can include architectural mechanisms in hardware or software and/or specific verification activities as part of a safety directed development (see ARP4754).

The occurrence of software errors are probabilistic but not in the same sense as hardware failures. Unlike hardware failures, these probabilities cannot be qualified. Therefore numerical and categorical probabilities should not be indicated for software errors in fault trees. Any software analysis in an FTA should be expressed in terms of development assurances to protect against software errors. The analysis should be evaluated for compliance on a purely qualitative basis.

4.1.3   Average Exposure Time Probability: When conducting quantitative FTA/DD/MA, the probabilities are estimated from the failure rates and exposure times of the events. Probability calculations for civil aircraft certifications are based on average probabilities calculated for all the aircraft of the same type. For the purpose of these analyses, the failure rates are usually assumed to be constant over time and are estimates of mature failure rates after infant mortality and prior to wear-out. If wearout or infant mortality is a consideration then other methods would need to be employed, for example life limitations or enhanced burn-in. Failing that, other distribution functions (e.g., Weibull) have to be applied or Monte Carlo simulation could be used. But this is beyond the scope of this document. These analyses should calculate average probability of occurrence per flight hour for the failure condition assuming a typical flight of average duration and considering the appropriate exposure and at risk times. A more detailed discussion of the proper determination of exposure and at risk times is contained in Appendices D and F.

When developing a new aircraft, the average flight time is usually determined from the customer requirements for the aircraft. This is an assumed value. When modifying an existing aircraft, the actual average flight time, based on in-service data, could be used.

4.2   Failure Modes and Effects Analysis (FMEA):

An FMEA is a systematic, bottom-up method of identifying the failure modes of a system, item, or function and determining the effects on the next higher level. It may be performed at any level within the system (e.g., piece-part, function, blackbox, etc.). Software can also be analyzed qualitatively using a functional FMEA approach. Typically, an FMEA is used to address failure effects resulting from single failures.

The scope of an FMEA should be coordinated with the user requesting it. The analysis may be a piece part FMEA or functional FMEA. If the failure rates derived from a functional FMEA allow the PSSA probability budgets to be met, a piece part FMEA may not be necessary. FMEAs typically include the following information.

4.2   (Continued):

    a. Identification of component, signal, and/or function
    b. Failure modes and associated hardware failure rates (numerical or categorical)
    c. Failure effects (directly and/or at the next higher level)
    d. Detectability and means of detection

    FMEAs may also include the following information.

    a. Compensating actions (i.e., automatic or manual)
    b. Phase of flight in which the failure occurs
    c. Severity of failure effects

    An FMEA may be used in conjunction with probabilistic techniques such as the FTA or DD to produce a quantitative analysis. Furthermore, an FMEA may be used to supplement the FTA/DD by providing a complementary list of failure effects from the bottom up.

    For details in performing an FMEA, refer to Appendix G.

4.3   Failure Modes and Effects Summary (FMES):

    An FMES is a grouping of single failure modes which produce the same failure effect (i.e., each unique failure effect has a separate grouping of single failure modes). An FMES can be compiled from the aircraft manufacturer's, system integrator's or equipment supplier's FMEAs. Furthermore, an FMES should be coordinated with the user to adequately address the need for inputs to higher level FMEAs and/or System Safety Assessment FTAs.

    For details in completing the FMES, refer to Appendix H.

4.4   Common Cause Analysis (CCA):

    Independence between functions, systems or items may be required to satisfy the safety requirements. Therefore, it is necessary to ensure that such independence exists, or that the risk associated with dependence is deemed acceptable. Common Cause Analysis (CCA) provides the tools to verify this independence, or to identify specific dependencies.

    In particular the CCA identifies individual failure modes or external events which can lead to a catastrophic or hazardous/severe-major failure condition. Such common cause events must be precluded for catastrophic failure conditions and must be within the assigned probability budget for hazardous/severe-major failure conditions.

    The safety analysis must given special attention to analyzing common-cause faults [AC/AMJ 25.1309]

4.4   (Continued):

CCA is subdivided into three types of analysis.

   a. Zonal Safety Analysis
   b. Particular Risks Analysis
   c. Common Mode Analysis

4.4.1   Zonal Safety Analysis (ZSA): A Zonal Safety Analysis should be performed on each zone of the aircraft. The objective of the analysis is to ensure that the equipment installation meets the safety requirements with respect to:

   a. Basic Installation. (The installation should be checked against the appropriate design and installation requirements.)

   b. Interference Between Systems. (The effects of failures of equipment should be considered with respect to their impact on other systems and structure falling within their physical sphere of influence.)

   c. Maintenance Errors. (Installation maintenance errors and their effects on the system or aircraft should be considered.)

When an effect which may affect safety identified, it will be highlighted in the Zonal Safety Analysis. This will either result in a redesign or will be shown to be acceptable in the appropriate safety assessment.

For details in performing the ZSA, refer to Appendix I.

4.4.2   Particular Risks Analysis (PRA): Particular risks are defined as those events or influences which are outside the system(s) and item(s) concerned, but which may violate failure independence claims. Some of the example risks shown here require analysis because of airworthiness regulations, while others arise from known external threats to the aircraft or systems.

Typical risks include, but are not limited to the following.

   a. Fire
   b. High Energy Devices
   c. Leaking Fluids
   d. Hail, Ice, Snow
   e. Bird Strike
   f. Tread Separation from Tire
   g. Wheel Rim Release
   h. Lightning
   i. High Intensity Radiated Fields
   j. Flailing Shafts

4.4.2   (Continued):

Having identified the appropriate risks with respect to the design under consideration, each risk should be the subject of a specific study to examine and document the simultaneous or cascading effect(s) of each risk.

The objective is to ensure that any safety related effects are either eliminated or the risk is shown to be acceptable.

For details in performing the PRA, refer to Appendix J.

4.4.3   Common Mode Analysis (CMA): A Common Mode Analysis is performed to verify that ANDed events in the FTA/DD and MA are independent in the actual implementation. The effects of design, manufacturing, maintenance errors and failures of system components which defeat their independence should be analyzed. Considerations should be given to the independence of functions and their respective monitors. Item with identical hardware and/or software could be susceptible to generic faults which could cause malfunctions in multiple items.

Common mode faults can fall into several categories which should be analyzed. The following are some examples of common mode faults.

    a. Hardware Error
    b. Software Error
    c. Hardware Failure
    d. Production/Repair Flaw
    e. Situation Related Stress (e.g., abnormal flight conditions or abnormal system configurations)
    f. Installation Error
    g. Requirements Error
    h. Environmental Factors (e.g., temperature, vibration, humidity, etc.)
    i. Cascading Faults
    j. Common External Source Faults

For details in performing the CMA, refer to Appendix K.

5.   SAFETY RELATED MAINTENANCE TASKS AND INTERVALS:

The calculation of event probability associated with a failure condition must take into account the time during which a latent failure can persist without being detected.

In many cases, the failures are detected by normal flight crew observation or during periodic power-up or self test routines. The latent period for these failures is short. In some cases, however, the exposure time for latent failures is associated with equipment shop tests or specific aircraft maintenance tasks. In these cases the latent period can be considerable amount of time.

5.   (Continued):

Maintenance tasks and time intervals which are identified during the PSSA and SSA by the use of the FTA, DD, MA or other similar analyses are potential Candidate Certification Maintenance Requirements (CCMRs). Where detection is accomplished by an aircraft maintenance task, the time interval required to meet the safety objective must be transferred to the appropriate maintenance department for implementation of required maintenance procedures and time intervals. Some maintenance checks associated with safety requirements compliance may be designated Certification Maintenance Requirements (CMRs). A CMR is a mandatory periodic task, required to maintain the safety of the aircraft, established during the design certification of the airplane as an operating limitation of the type certificate. These checks are established in accordance with AC 25-19 "Certification Maintenance Requirements".

It is important to note that CMRs are derived from a fundamentally different analysis process than the maintenance tasks and intervals that result from the Maintenance Steering Group (MSG-3) analysis associated with Maintenance Review Board (MRB) activities. MSG-3 analysis activity produces maintenance tasks that are performed for safety, operational or economic reasons, involving preventive maintenance tasks, which are performed before failure occurs (and are intended to prevent failures), as well as failure-finding tasks. CMRs on the other hand, are failure-finding tasks only, and exist solely to limit the exposure to otherwise hidden failures.

CMRs are designed to verify that a certain failure has or has not occurred, and do not provide any preventive maintenance function.

The MSG-3 process examines failure paths by using the "Next Failure" criteria. (e.g., what is the next worst thing that can happen, given the first failure has occurred?) Once the MSG-3 process is complete, the minimum maintenance required is established in the Maintenance Review Board document, or MRB.

Before becoming a CMR, a potential CMR, known as a Candidate CMR (CCMR), is reviewed by a Certification Maintenance Coordination Committee (CMCC), which will decide if the candidate will become a CMR. Details of this process are delineated in AC 25-19.

Once established, CMRs are required maintenance tasks and must be accomplished by the operator at the prescribed intervals, derived from the safety analysis, to maintain the airworthiness certificate of the aircraft.

Where the detection method is identified to be provided by test, assurance must be provided that the test procedures in fact detect the latent failures of concern.

The underlying goal of any system design should be an absolute minimum number of CMRs, with none as the ideal situation.

6.   TIME LIMITED DISPATCH (TLD):

The following section contains a discussion of a method currently being used to define and control dispatchability requirements for Full Authority Digital Engine Control (FADEC) based aircraft propulsion control. It is included here only to provide background for the concept.

The concept of TLD allows advantage to be taken of any redundancy available to permit the airlines to schedule maintenance actions at specific intervals, rather than possibly incurring delays and/or cancellations if it were required that all faults be rectified prior to the next flight. TLD operation is conditional upon average safety levels being maintained. The recommended process for approval of TLD operations requires additional criteria for the abatement of risks in particular dispatch configurations.

An example of engine related applications which utilize this concept is discussed below. In principle it could be applied to any system which has been designed to include redundancy.

The FAR/JAR 25.1309 Harmonization Working Group is addressing the issue of TLD. The result of that discussion will determine the future course of the use of TLD tools in aircraft design and operations.

6.1   FADEC Application:

The concept has been applied to dual channel engine FADEC (Full Authority Digital Engine Control) systems with regard to the failure condition of LOTC (Loss of Thrust Control) of a single engine.

TLD operation is conditional upon the resultant system operation and reliability being adequate to satisfy the requirements of the certification authorities. A list showing which faults appear in each dispatchable class and the allowable dispatch times must be agreed upon with the certification authorities.

An Aerospace Recommended Practice (ARP) document on Time Limited Dispatch of aircraft which use engines with electronic control systems is being prepared by SAE Committee E-36. This document will describe the use of MA and analytic calculations to determine the periods of time during which an aircraft can be dispatched with known inoperative engine control system items

PREPARED BY SAE COMMITTEE S-18,
SAFETY ASSESSMENT FOR AIRBORNE SYSTEMS AND EQUIPMENT

APPENDIX A
FUNCTIONAL HAZARD ASSESSMENT (FHA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

A.1   INTRODUCTION:

The objectives of the FHA is to consider functions at the most appropriate level and to identify failure conditions and the associated classifications while considering both loss of functions and malfunctions. The FHA should identify the failure conditions for each phrase of flight when the failure effects and classifications vary from one flight phase to another. The FHA also establishes derived safety requirements needed to limit the function failure effects which affect the failure condition classification. The requirements may include such things as design constraints, annunciation of failure conditions, recommended flight crew or maintenance action, etc. Furthermore, these requirements may involve single or multiple systems. All safety requirements should be traceable and validated at each level of derivation. A good way to accomplish this is to create a table of derived requirements based on design decisions. Once the high level requirements have been identified, they may be used to generate lower level requirements as part of the PSSA process for the systems or items. This process is continued, with reiteration, until the design process is complete.

There are two levels of FHA, the Aircraft level FHA and the System level FHA. FHAs carried out at these two levels use the same principles.

Generation of the FHA at the highest appropriate level is dependent upon overall knowledge and experience and may require consultation of numerous specialists. Table A1 is an example of the high level functions and their associated failure conditions that may be considered.

TABLE A1

Function	Failure Condition
Control Flight Path	Inability to control Flight Path
Control Touchdown and Roll Out	Inability to control Touchdown and Roll Out
Control Thrust	Inability to control Thrust
Control Cabin Environment	Inability to control Cabin Environment
Provide Spatial Orientation	Inability to provide Spatial Orientation
Fire Protection	Loss of Fire Protection

A.1   (Continued):

These failure conditions can be further broken down through the use of FHAs and Fault Trees. The following are some examples.

a.   Inability to Control Flight Path
    (1) Loss of trim
        (a) Loss of manual trim
        (b) Loss of fuel trim
        (c) etc.
    (2) Inadvertent trim
    (3) Loss of all hydraulics
    (4) Loss of flight control
    (5) Flight Control Malfunction
        (a) Elevator Hardover

Eventually, the failure conditions associated with safety should be defined together with their respective safety objectives and the proposed means for demonstrating compliance. For aircraft level safety requirements, methods for demonstrating compliance should be shown in the aircraft level FHA. For system level requirements, methods for demonstrating compliance should be shown using the PSSA.

The aircraft level FHA should be used to support identification of possible multiple system failure conditions which could have a higher failure condition classification than would be expected based on independent system analysis.

It is desirable to establish an aircraft level general hazard list to be used on future projects so that known hazards are not overlooked. If such a list already exists, it should be used as a cross-check in the development of the aircraft level FHA.

A.2   REQUIREMENT TO PERFORM AN FHA:

The FHA is the first step in a safety assessment process that is performed on new or modified aircraft programs. The FHA establishes the safety requirements for the new or modified design.

A.3   FHA PROCESS:

The FHA process is a top down approach for identifying the functional failure conditions and assessing their effects. This assessment is made in accordance with the following processes.

a.   Identification of all the functions associated with the level under study (internal functions and exchanged functions)

b.   Identification and description of failure conditions associated with these functions, considering single and multiple failures in normal and degraded environments

c.   Determination of the effects of the failure condition

SAE ARP4761

A.3   (Continued):

   d. Classification of failure condition effects on the aircraft (Catastrophic, Severe-Major/Hazardous, Major, Minor and No Safety Effect)

   e. Assignment of requirements to the failure conditions to be considered at the lower level

   f. Identification of the supporting material required to justify the failure condition effect classification

   g. Identification of the method used to verify compliance with the failure condition requirements

   Figures A1 and A2 describe the process flow for the Aircraft level and System level FHA.

A.3.1   Function Identification:

   All the functions associated with the level under study, both internal functions and exchanged functions, should be identified. These functions are identified by obtaining the necessary source data and then creating the function list.

A.3.1.1   Obtain the Necessary Source Data: The first step in performing the FHA process is to obtain the necessary source data

   The aircraft level FHA inputs are as follows.

   a. The list of the top-level aircraft functions (e.g., lift, thrust, etc.)
   b. The aircraft objectives and customer requirements (e.g., number of passengers, range, etc.)
   c. Initial design decisions (e.g., number of engines, conventional tail, etc.)

   The System level FHA inputs are as follows.

   a. The list of the main functions to consider
   b. A functional diagram showing external interfaces
   c. The list of functions created in the higher design level FHAs
   d. The list of the failure conditions identified in the higher design level FHAs
   e. The requirements defined in design requirements and objectives documents
   f. The design options chosen at the upper level and their rationale

Aircraft FHA

AIRCRAFT LEVEL
FUNCTIONAL
ANALYSIS
A.3.1

UPPER LEVEL REQUIREMENTS
(Aircraft specification - Regulations)

Aircraft Main
Functions &
Flight Phases

Aircraft Main Failure Conditions
and Associated Requirements
A.3.1.1

DESCRIPTION OF
AIRCRAFT LEVEL
FUNCTIONS (INTERNAL
AND EXCHANGED) AND
FLIGHT PHASES
A.3.1.2

EMERGENCY AND
ENVIRONMENTAL
CONFIGURATIONS
TO CONSIDER AT
AIRCRAFT LEVEL
A.3.2.1

AIRCRAFT LEVEL
FUNCTIONAL FAILURE
ANALYSIS
A.3.2.2

DETERMINATION AT
AIRCRAFT LEVEL OF

- ASSOCIATED FAILURE
  CONDITION (A.3.2.2)
- EFFECTS (A.3.3)
- FAILURE CONDITION
  CLASSIFICATION (A.3.4)
- DETECTION (CREW/GROUND)
- CREW ACTIONS
- JUSTIFICATION MATERIAL
- FUNCTION DEVELOPMENT
  ASSURANCE LEVEL

AIRCRAFT LEVEL
EXCHANGED
FUNCTIONS LIST
A.3.1.2b

AIRCRAFT LEVEL
FUNCTION LIST
A.3.1.2a

FLIGHT PHASES

Lower or upper level
activity

Process external to the
FHA but at the same level

Process belonging to the
FHA

REQUIREMENTS AND FAILURE CONDITION LIST TO CONSIDER
IN AIRCRAFT DESIGN AND IN LOWER LEVEL ACTIVITIES
(SYSTEM FHA)
- CLASSIFICATION OF FAILURE CONDITIONS (A.3.4)
- QUALITATIVE AND QUANTITATIVE REQUIREMENTS (A.3.5)
- FUNCTIONS DEVELOPMENT ASSURANCE LEVEL
- LIST OF JUSTIFICATION MATERIAL AND FOLLOW UP (A.3.6 & A.3.7)

TRANSMISSION OF FHA REQUIREMENTS FOR THE DESIGN PROCESS (INTERFACE DOCUMENTS)

| REQUIREMENTS FOR AIRCRAFT LEVEL AND LOWER LEVELS qualitative and quantitative, development assurance level, etc. | COMMON CAUSE ANALYSES | JUSTIFICATION MATERIALS | GROUND TESTS | FLIGHT TESTS | ETC. |

AIRCRAFT LEVEL REQUIREMENTS

VALIDATION ACTIVITIES

FIGURE A1 - Aircraft Level Functional Hazard Assessment

System FHA

AIRCRAFT LEVEL
FUNCTIONAL ANALYSIS
A.3.1

UPPER LEVEL REQUIREMENTS
(System functional specification - including specific system
regulations, and derived aircraft FHA requirements)

System Main Functions & Flight Phases   System Main Failure Conditions and Associated Requirements   A.3.1.1

SYSTEM LEVEL
FUNCTIONAL ANALYSIS
A.3.1

DESCRIPTION OF SYSTEM
LEVEL FUNCTIONS
(INTERNAL AND
EXCHANGED) AND FLIGHT
PHASES
A.3.1.2

EMERGENCY AND
ENVIRONMENTAL
CONFIGURATIONS
TO CONSIDER AT
SYSTEM LEVEL
A.3.2.1

SYSTEM LEVEL FUNCTIONAL
FAILURE ANALYSIS
A.3.2.2

SYSTEM LEVEL
EXCHANGED
FUNCTIONS LIST
A.3.1.2b

DETERMINATION AT
AIRCRAFT LEVEL OF

- ASSOCIATED FAILURE
  CONDITION (A.3.2.2)
- EFFECTS (A.3.3)
- FAILURE CONDITION
  CLASSIFICATION (A.3.4)
- DETECTION (CREW/GROUND)
- CREW ACTIONS
- JUSTIFICATION MATERIAL
- FUNCTION DEVELOPMENT
  ASSURANCE LEVEL

SYSTEM LEVEL
FUNCTION LIST
A.3.1.2a

FLIGHT PHASES

Lower or upper level
activity

Process external to the
FHA but at the same level

Process belonging to the
FHA

REQUIREMENTS AND FAILURE CONDITION LIST TO CONSIDER
IN SYSTEM DESIGN AND IN LOWER LEVEL ACTIVITIES (PSSA &
SSA)
- CLASSIFICATION OF FAILURE CONDITIONS (A.3.4)
- QUALITATIVE AND QUANTITATIVE REQUIREMENTS (A.3.5)
- FUNCTIONS DEVELOPMENT ASSURANCE LEVEL
- LIST OF JUSTIFICATION MATERIAL AND FOLLOW UP (A.3.6 & A.3.7)

TRANSMISSION OF FHA REQUIREMENTS FOR THE DESIGN PROCESS (INTERFACE DOCUMENTS)

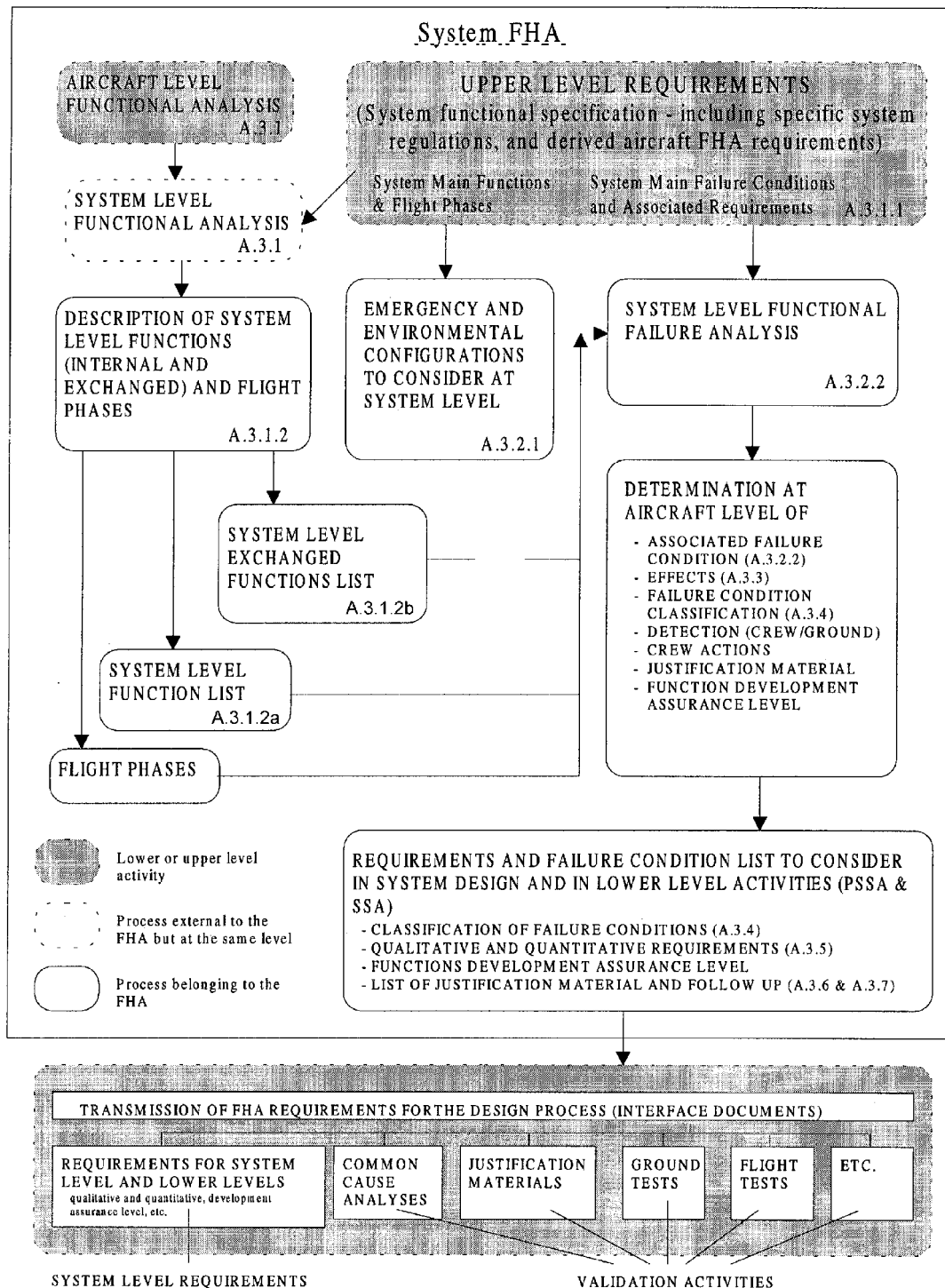| REQUIREMENTS FOR SYSTEM LEVEL AND LOWER LEVELS qualitative and quantitative, development assurance level, etc.	COMMON CAUSE ANALYSES	JUSTIFICATION MATERIALS	GROUND TESTS	FLIGHT TESTS	ETC.

SYSTEM LEVEL REQUIREMENTS   VALIDATION ACTIVITIES

FIGURE A2 - System Level Functional Hazard Assessment

A.3.1.2   Create a Function List: The FHA list of functions is made by starting with the expected function list and considering the source data inputs.

When, at the aircraft or system level, the functions are allocated to hardware or software, it is necessary to list the new functions introduced by this architectural design decision. This is done by listing all the hardware or software functions and by checking that all these functions are included in the aircraft or system level function list. During this process, two types of functions are identified.

   a.   Functions internal to the considered level (Internal Functions)

      (1)   At the aircraft level these are main functions of the aircraft and functions exchanged between the internal systems of the aircraft.
      (2)   At the system level these are functions of the considered system and functions exchanged between the internal equipment of the system.

   b.   Functions external to the considered level (Exchanged Functions)

      (1)   At the aircraft level, these are functions that interface with other aircraft or with ground systems.
      (2)   At the system level, for any given system, these are functions which are either provided by other systems or provided to other systems (including other aircraft systems or with ground systems).

A.3.2   Identification and Description of "Failure Conditions":

The failure conditions identification process begins with creating an environmental and emergency configuration list. Next, the analyst considers all the items of the internal function list, the exchanged function list, and the environmental and emergency/abnormal configuration list. The analyst then creates a list of failure conditions for the aircraft/system considering single and multiple failures in normal and degraded environments. To generate these failure conditions and assumptions, the analyst needs to understand the possible failure modes. The failure conditions should be subdivided into flight phases when the severity of the condition changes with different flight phases.

A.3.2.1   Environment and Emergency Configuration List: In addition to the list of functions of A.3.1.2, it is necessary to list the environmental conditions which need to be considered when determining the failure effects. Examples of environmental conditions to be considered at the aircraft level include the following.

   a.   Weather
   b.   HIRF
   c.   Volcanic Ash

A.3.2.1 (Continued):

It is also necessary to list the aircraft configurations resulting from emergency/abnormal conditions which need to be considered when determining the failure effects. Examples of emergency/abnormal conditions at the aircraft/system level include the following:

a. Ditching
b. Engine Out
c. Loss of Communications
d. Depressurization

For the system level FHA, this list is derived from the corresponding list coming from the aircraft level FHA or upper level FHA(s) and from architectural design decisions made during the initial concept design phase.

Examples of emergency/abnormal conditions to be added to the above list at the system level include the following:

a. Hydraulic System Loss
b. Electrical System Loss
c. Equipment Cooling Loss

A.3.2.2 Failure Condition Determination Considering Single and Multiple Failures: The creation of the single failure list involves examining the original list created in the previous steps and, in addition, applying an analysis of the concept design created in the initial design process. The creation of the multiple failure list is more difficult as it requires an understanding of the integration of the system components and the interaction of the system being analyzed with other systems on the aircraft. This process is aided by an understanding of the aircraft and system architecture. Multiple failures have to be considered, especially when the effect of a certain failure depends on the availability of another system.

Typical single failure conditions include the following:

a. Loss of Function
b. Unannunciated Loss of Function
c. Malfunction

Typical multiple failure conditions include the following:

a. Loss of two hydraulic systems where three systems exist on the aircraft
b. Loss of communication and loss of navigation

A.3.3   Determine the Effects of the Failure Condition:

The analyst must determine the effect of failure conditions on the aircraft, crew and occupants. The analyst should consult people with operational experience to aid in classifying the failure condition effects. This can be accomplished directly at the aircraft level FHA. In the case of the system level FHA, the aircraft level effect may be the same as the system level effect, or the analyst may have to consider combined effects of other systems which accomplish the same aircraft function in order to determine the effect of the system failure condition.

A.3.4   Determine the Classification of the Failure Condition Effects:

The determination of the classification is accomplished by analyzing accident/incident data, reviewing regulatory guidance material, using previous design experience, and consulting with flight crews, if applicable. The classifications are: Catastrophic, Severe-Major/Hazardous, Major, Minor and No safety effect. (Reference Table 1 in the main body of this document)

Documentation of supporting materials (analyses/studies, tests, etc.) used in determining the effects and classification of failure conditions should be preserved to ensure traceability for future reference.

A.3.5   Assignment of Probability Requirements to Failure Conditions to be Considered at the Lower Level:

For each failure condition, the analyst must assign probability requirements and applicable qualitative design requirements. These requirements take the form of written requirements in specifications (aircraft requirements, system requirements, and item requirements).

A.3.6   Identification of the Supporting Material Required to Justify the Failure Condition Effect Classification:

For those failure condition effects that are not well understood, additional supporting material (e.g., simulation, studies, flight tests) should be defined to validate the chosen classification.

A.3.7   Identification of the Method Used to Verify Compliance with the Failure Condition Requirements:

For each failure condition the analyst should determine how the aircraft/system will satisfy the safety objective. The flowchart depicted in Figure 3.5-1 in the main body of this document provides guidance in defining the necessary safety objective verification approach for the relevant failure condition.

A.3.8   Previous Experience:

When the list of failure conditions and their classifications has been produced, it may be worth checking how the list compares with lists from previous similar projects as an extra aid to guard against overlooking some of the less encountered failure conditions. Furthermore, it may also be worth creating and maintaining a generic list, as a checklist, to be used during the review process of the FHA.

A.4   FHA OUTPUTS:

A.4.1   Documentation:

The results of the FHA process should be documented so that there is traceability of the steps taken in developing the FHA report. The following information should be documented during the FHA process.

   a.   FHA input function list
   b.   Environmental and Emergency Configuration List
   c.   Derived safety requirements for the design at each level
   d.   FHA Report which contains the following
       (1) Function Description
       (2) Failure Conditions
       (3) Phase of Operations
       (4) Effect of the Failure Condition on the Aircraft, Crew and Occupants
       (5) Classification of the Failure Condition
       (6) Reference to Supporting Material
       (7) Verification Method (for the design solution chosen to meet the safety objective)

A.4.2   Link Between FHA and PSSA:

The results of the aircraft FHA and associated aircraft fault trees are the inputs to the system FHAs. The results of the system FHA are the inputs to the PSSA process.

The depth of the PSSA process will vary, depending on the design, complexity and failure condition classification related to the system analyzed.

The depth of the PSSA study is directed by the system FHA (i.e., failure condition classification) and the proposed design solution (complexity, novelty and integration). As the severity and/or design complexity increases, the depth of assessments/analyses increases.

APPENDIX B
PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

B.1   INTRODUCTION:

The Preliminary System Safety Assessment (PSSA) process is a systematic examination of a proposed system architecture(s) to determine how failures can lead to the functional hazards identified by the Functional Hazard Assessment (FHA), and how the FHA requirements can be met. The PSSA process is interactive and associated with the design definition. Just as the design process is iterative, the PSSA process is iterative. The PSSA process is continuous throughout the design cycle.

For each system analyzed, the PSSA addresses all significant Failure Conditions identified in the FHA(s). The methods of analysis may be either qualitative or quantitative.

There can be more than one level of PSSA. The highest level of PSSA is developed from the aircraft level and/or system level FHAs. Lower level PSSAs are developed from the output of higher level PSSAs.

Throughout this Appendix, reference is made to using Fault Tree Analyses. It should be understood by the reader that Dependence Diagrams or Markov Analyses may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

B.2   REQUIREMENT TO PERFORM THE PSSA:

The decision to conduct a PSSA is dependent upon the design of the architecture, complexity, the severity of the failure condition (or failure effect), and type of function performed by the system being analyzed. The requirement for a PSSA should have been established from the output of the aircraft level or system level FHA according to the verification approach defined in Figure 4 of the main body of this document.

B.3   PSSA PROCESS:

The PSSA is a top down approach to determine how failures can lead to the functional hazards identified by the FHA, and how the FHA requirements can be met. This assessment is made in accordance with the following processes.

B.3   (Continued):

   a.   Complete the list of aircraft and system level safety requirements.

   b.   Determine whether this architecture, and the planned concept design, can reasonably be
        expected to meet the safety requirements and objectives.

   c.   Derive the safety requirements for the design of lower level items (hardware and software),
        aircraft installation, other systems and operations (flight and maintenance tasks).

   Figure B1 describes the process flow for the PSSA.

B.3.1   Complete the List of Aircraft and System Level Safety Requirements:

   The aircraft FHA/CCA process creates an initial set of safety requirements for the design of the
   aircraft. Similarly, the system FHA/CCA process creates an initial set of safety requirements for
   the systems. By combining these initial sets of safety requirements with design/architecture
   decisions made in the PSSA process, a complete set of system requirements is generated.

B.3.1.1   Obtain the Necessary Source Data: The PSSA inputs are the aircraft and/or system level
          FHA, preliminary Common Cause Analysis (CCA), and the description of each system
          architecture under consideration in the PSSA. For each architecture option, these inputs may
          include:

   a.   Failure conditions and requirements identified in the aircraft and/or system level FHA.
   b.   The system architecture description and the rationale for this choice.
   c.   The list and functions of system equipment.
   d.   The system interfaces and relations with other systems.
   e.   Preliminary Common Cause Analyses.
        (1) ZSA findings
        (2) PRA external threats
        (3) CMA findings

   The assumptions made during the aircraft/system level FHAs should be confirmed to be
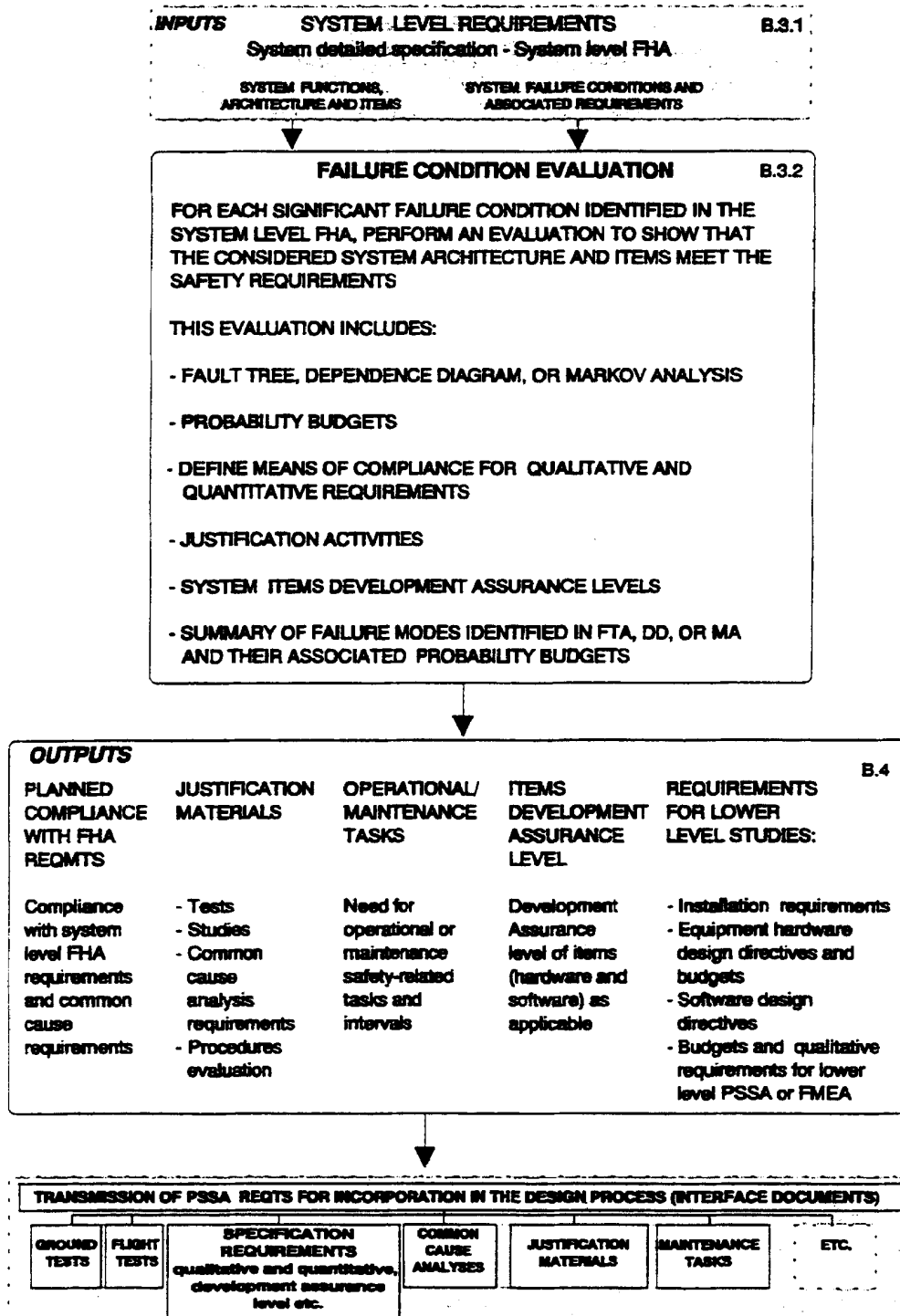   applicable to each architecture under consideration in the PSSA.

INPUTS   SYSTEM LEVEL REQUIREMENTS   B.3.1

System detailed specification - System level FHA

SYSTEM FUNCTIONS, ARCHITECTURE AND ITEMS   SYSTEM FAILURE CONDITIONS AND ASSOCIATED REQUIREMENTS

FAILURE CONDITION EVALUATION   B.3.2

FOR EACH SIGNIFICANT FAILURE CONDITION IDENTIFIED IN THE SYSTEM LEVEL FHA, PERFORM AN EVALUATION TO SHOW THAT THE CONSIDERED SYSTEM ARCHITECTURE AND ITEMS MEET THE SAFETY REQUIREMENTS

THIS EVALUATION INCLUDES:

- FAULT TREE, DEPENDENCE DIAGRAM, OR MARKOV ANALYSIS

- PROBABILITY BUDGETS

- DEFINE MEANS OF COMPLIANCE FOR QUALITATIVE AND QUANTITATIVE REQUIREMENTS

- JUSTIFICATION ACTIVITIES

- SYSTEM ITEMS DEVELOPMENT ASSURANCE LEVELS

- SUMMARY OF FAILURE MODES IDENTIFIED IN FTA, DD, OR MA AND THEIR ASSOCIATED PROBABILITY BUDGETS

OUTPUTS   B.4

PLANNED COMPLIANCE WITH FHA REQMTS	JUSTIFICATION MATERIALS	OPERATIONAL/ MAINTENANCE TASKS	ITEMS DEVELOPMENT ASSURANCE LEVEL	REQUIREMENTS FOR LOWER LEVEL STUDIES:
Compliance with system level FHA requirements and common cause requirements	- Tests - Studies - Common cause analysis requirements - Procedures evaluation	Need for operational or maintenance safety-related tasks and intervals	Development Assurance level of items (hardware and software) as applicable	- Installation requirements - Equipment hardware design directives and budgets - Software design directives - Budgets and qualitative requirements for lower level PSSA or FMEA

TRANSMISSION OF PSSA REQTS FOR INCORPORATION IN THE DESIGN PROCESS (INTERFACE DOCUMENTS)

GROUND TESTS	FLIGHT TESTS	SPECIFICATION REQUIREMENTS qualitative and quantitative, development assurance level etc.	COMMON CAUSE ANALYSES	JUSTIFICATION MATERIALS	MAINTENANCE TASKS	ETC.

FIGURE B1 - System Level PSSA Process

B.3.1.2 Completion of Safety Requirements for the System: The implementation of functions in a system architecture, in items (hardware or software), or integration of functions may result in new functions which have to be considered in the FHA to derive new failure conditions. The implementation may also derive new requirements (e.g., separation requirements and operational requirements). These new requirements and new failure conditions may require additional justification material within the PSSA or FHA.

B.3.2 Evaluate Design/Architecture Decisions Against Generated Safety Requirements and Objectives:

After the completion of the system FHA requirements, each identified Severe-Major/Hazardous and Catastrophic failure condition must be evaluated as shown in Figure 4 of the main body of this document. The evaluation should:

a. Show, using Fault Tree Analysis or similar method, how item failures combine to lead to the considered failure condition.

b. Identify all requirements associated with independence claims made in the Fault Tree Analyses by identifying:

   (1) All separation/segregation requirements and associated verification requirements during Common Cause Analysis investigations.
   (2) Tests (ground or flight test) to verify independence.
   (3) Common cause failures (Zonal Analysis, Particular Risks Analysis, Common Mode Analysis).

c. Show, using Fault Tree Analysis or similar method, that qualitative and quantitative requirements and objectives associated with the failure condition can be met by the proposed system architecture and the budgeted failure probabilities.

d. Determine the "Not to Exceed" interval for maintenance tasks driven by latent failures considered in the Fault Tree Analysis. (Latent failures which can exist for the design life of the aircraft, or the system/item in question without exceeding FTA numerical allowances, will not drive "Not to Exceed" maintenance intervals.)

e. Determine the Development Assurance Level of items considered in the Fault Tree Analysis.

(NOTE: Major and Minor failures conditions may be evaluated using the above techniques as necessary.)

This evaluation is made at a time in the design process when the results of the detailed studies at the item level are not yet fully available. Consequently, the PSSA failure condition evaluation must rely in part on engineering judgement and on in-service experience with similar designs. This process is of an iterative nature and becomes more complete during the evolution of the design.

B.3.3   Derive the Safety Requirements for the Design of Lower Level Items:

Each design safety requirement derived at the system level must be allocated to the items making up the system. These allocations include:

    a.   An updated failure condition list which includes the rationale for how the safety requirements (qualitative and quantitative) can be met with the chosen architecture.

    b.   The safety requirements (qualitative and quantitative) allocated to items (both hardware and software).

    c.   Requirements for the design of the installation (segregation, separation, protection, etc.).

    d.   The hardware and software Development Assurance Levels.

    e.   The safety maintenance tasks and associated "Not to Exceed" times.

Failure modes and associated probability budgets identified in PSSA Fault Tree Analysis should be used as requirements to drive the lower level detailed studies.

B.4   PSSA OUTPUTS:

B.4.1   Documentation:

The results of the PSSA process should be documented so that there is traceability of the steps taken in developing the PSSA reports. Some of the information which may be valuable to preserve includes the following.

    a.   Planned compliance method with FHA requirements
    b.   Updated FHAs
    c.   Material supporting the classification list
    d.   A failure condition list
    e.   Lower level safety requirements (Including Development Assurance Levels)
    f.   Qualitative FTAs
    g.   Preliminary CCAs
    h.   Operational requirements (flight and maintenance)

B.4.2   Outputs to Lower Level PSSA:

The PSSA may be performed at levels below the system level. The inputs to lower level PSSAs are the failure effects of concern, qualitative requirements, budgeting probabilities and Development Assurance Levels identified during a higher level FHA/PSSA. After the inputs are received, the PSSA lower level process is equivalent to that described in the above sections.

B.4.3   Link Between PSSA and System Safety Assessment (SSA):

The outputs of the PSSA are the inputs for the SSA process.

APPENDIX C
SYSTEM SAFETY ASSESSMENT (SSA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

C.1 INTRODUCTION:

The System Safety Assessment (SSA) is a systematic examination of the system, its architecture and its installation to show compliance with the safety requirements. For each PSSA carried out at a different level, there should be a corresponding SSA. The highest level SSA is the system level SSA. For each system analyzed, the SSA summarizes all significant failure conditions and their effects on the aircraft. The methods of analysis used to show compliance may be either qualitative or quantitative.

Throughout this appendix, reference is made to using Fault Tree Analyses. It should be understood by the reader that Dependence Diagrams or Markov Analyses may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

C.2 REQUIREMENT TO PERFORM THE SSA:

The requirement to perform an analysis may vary depending on the design, complexity, and type of function performed by the system being analyzed. This should have been established from the associated PSSA

C.3 SSA PROCESS:

The SSA process is a bottom up approach for verifying that the design safety requirements and objectives have been met. Figure C1 describes the process flow for the system level SSA. This assessment accomplishes the following:

a. Verification that the design requirements established in the System Level FHA are met

b. Validation that the classification established for the aircraft level effects are justified

c. Verification that the safety requirements called out in, or derived from aircraft design requirements and objectives are met

d. Verification that the design requirements identified in the CCA process are met

e. Linkage of the System level SSA to the aircraft level FHA.

INPUTS   SYSTEM LEVEL REQUIREMENTS   C.3.1
System detailed specification - System level FHA and PSSA

SYSTEM FUNCTIONS,   SYSTEM FAILURE CONDITIONS AND
ARCHITECTURE AND ITEMS   ASSOCIATED REQUIREMENTS

FAILURE CONDITION EVALUATION   C.3.2

FOR EACH FAILURE CONDITION IDENTIFIED IN THE SYSTEM
LEVEL FHA/PSSA, PERFORM AN EVALUATION TO SHOW
THAT THE SYSTEM ARCHITECTURE AND ITEMS MEET THE
SAFETY REQUIREMENTS

THIS EVALUATION INCLUDES:

- FAULT TREE, DEPENDENCE DIAGRAM, OR MARKOV
  ANALYSIS

- PROBABILITY CALCULATIONS

- INFORMATION SHOWING COMPLIANCE WITH
  QUALITATIVE AND QUANTITATIVE REQUIREMENTS

- JUSTIFICATION ACTIVITIES

- SYSTEM ITEMS DEVELOPMENT ASSURANCE LEVEL

- SUMMARY OF FMEA/FMES CONSIDERED IN FTA, DD, OR
  MARKOV ANALYSIS AND THEIR ASSOCIATED FAILURE
  RATE

RESULTS OF   C.3.1
OF FHA/PSSA
REQUIREMENTS

- JUSTIFICATION
  MATERIALS

- COMMON CAUSE
  ANALYSES

- LOWER LEVEL
  FMEA/FMES

- OPERATIONAL/
  MAINTENANCE
  TASKS

- DEVELOPMENT
  ASSURANCE LEVEL
  APPLICATION
  RESULTS

- RESULTS OF
  LOWER LEVEL
  REQUIREMENT
  APPLICATION AND
  TRACEABILITY

OUTPUTS   C.4

COMPLIANCE WITH FHA/PSSA REQUIREMENTS	JUSTIFICATION MATERIALS AND STATUS	OPERATIONAL/ MAINTENANCE TASKS	ITEMS DESIGN ASSURANCE LEVEL	SUMMARIES OF LOWER LEVEL STUDIES:
Compliance with system FHA/PSSA requirements and traceability	- Tests - Studies - Common cause analyses - Procedures	Operational/ Maintenance safety-related tasks and intervals. Cross references with operational and maintenance documents	Application results of design assurance levels to hardware and software	Summaries showing lower level requirements have been met

FIGURE C1 - System Level SSA Process

C.3.1   FHA Design Requirements Verification:

C.3.1.1 Obtain the Necessary Source Data: Inputs to the SSA are as follows.

    a.   System architecture description and the associated design rationale

    b.   Systems interfaces and their interactions with the items of the adjacent systems

    c.   Requirements and failure conditions identified in the System Level FHA/PSSA

    d.   List of functions and the associated rationale from the System Level FHA

    e.   Common Cause Analyses results

       (1) ZSA results
       (2) PRA external threats
       (3) CMA results

    f.   Results of all the supporting materials and lower level studies required in the FHA/PSSA. (FMEA/FMES from the item suppliers, results of flight tests, studies, etc.)

C.3.2   Failure Condition Evaluation:

Each failure condition identified in the FHA has to be evaluated in accordance with Figure 4 of the main body of this document. Selecting from the following techniques, the evaluation should be performed to:

    a.   Show, using Fault Tree Analysis, how items' failures combine to lead to the considered Failure Condition.

    b.   Show, using Fault Tree Analysis, that qualitative and quantitative requirements and objectives associated with the failure condition are met.

    c.   Inspect the maintenance documentation to verity that the "Not to Exceed" interval for maintenance tasks driven by latent failures considered in the Fault Tree Analyses have been included for the MRB. (Not all latent failures drive "Not to Exceed" maintenance intervals.)

    d.   Verify that the Development Assurance Level of items derived from the Fault Tree Analysis have been met.

    e.   Test the condition to assure compliance with requirements.

    f.   Demonstrate that the aircraft performs as expected with the given failure conditions.

C.3.2.1 Validation of Failure Condition Classification: Traceability should be demonstrated between requirements established in the FHA/PSSA and the documents in which these requirements are specified. These documents include the following items.

    a. Aircraft design requirements and objectives documentation
    b. System requirements documentation
    c. Test plans (ground tests, flight tests, etc.)
    d. Maintenance manual
    e. Common Cause Analyses documents

On method of accomplishing this task would be to create a matrix showing the requirements and the substantiation of their corresponding validations.

C.3.2.2 Verification that the Safety Requirements Identified in the Aircraft Requirement Document(s) are Met: The aircraft requirement document(s) contain all the requirements for the design of the aircraft. This includes all FAR/JARs and all company requirements. The verification of these requirements is accomplished by one or more of the four standard means, (i.e., test, analysis, demonstration and inspection).

C.3.2.3 Verification that the Design Requirements Identified in the CCA are Met: The CCA documentation contains requirements regarding system and component separation and segregation (from the Zonal Analysis), external threats (from the Particular Risk Analysis) and common mode failures (from the Common Mode Analysis). These requirements must be verified by one or more of the four standard means, (i.e., test, analysis, demonstration and inspection).

C.4 SSA OUTPUTS:

C.4.1 Documentation:

The results of the SSA process should be documented so that there is traceability of the steps taken in developing the SSA report. Some of the information which may be valuable to preserve includes:

    a. The updated failure condition list or FHA which includes the rationale showing compliance with safety requirements (qualitative and quantitative).

    b. Documentation showing how requirements for the design of the system items' installation (segregation, protection, etc.) have been incorporated.

    c. The materials used to validate the failure condition classification.

    d. The safety maintenance tasks and associated "Not to Exceed Time".

    e. Documentation showing how the system and items (including hardware and software) have been developed in accordance with assigned development assurance levels.

C.4.2   Linkage of the System Level SSA to the Aircraft Level FHA:

In order to close out the safety assessment process, each SSA must be reviewed against the basic requirement in both the system level and aircraft level FHA. The failure effect and its probability of occurrence at the aircraft level should be verified against the failure conditions and classifications of the aircraft level FHA.

APPENDIX D
FAULT TREE ANALYSIS

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

D.1   INTRODUCTION:

A Fault Tree Analysis (FTA) is a deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, a Fault Tree Analysis is a "top-down" system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated. The analyst begins with an undesired top level hazard event and systematically determines all credible single faults and failure combinations of the system functional blocks at the next lower level which could cause this event. The analysis proceeds down through successively more detailed (i.e., lower) levels of the design until a Primary Event is uncovered or until the top level hazard event requirement has been satisfied. A Primary Event is defined as an event which for one reason or another has not been further developed (i.e., the event does not need to be broken down to a finer level of detail in order to show that the system under analysis complies with applicable safety requirements). A Primary Event may be internal or external to the system under analysis and can be attributed to hardware failures/errors or software errors.

The analyst is encouraged to discontinue the FTA analysis when sufficient detail to satisfy the top level hazard requirement has been identified.

The fault tree graphical representation is hierarchical and takes its name from the branching that it displays. It is this format which makes this analysis a visibility tool for both engineering and the certification authority. As one of a family of safety assessment techniques for assuring that the system/equipment will accomplish its intended safety functions, fault tree analysis is concerned with ensuring that design safety aspects are identified and controlled.

FTA usage includes:

a. Facilitation of technical/certification authority assessments and reviews. (The completed fault tree displays only the failure events which could individually or collectively lead to the occurrence of the undesired top event.)

b. Assessment of a design modification with regards to its impact on safety.

c. Quantification of the top event probability of occurrence.

d. Allocation of probability budgets to lower-level events.

D.1   (Continued):

    e.   Visibility into the contribution of development errors by providing a format for mixed quantitative and qualitative assessment.

    f.   Assessment of single and multiple-fault effects.

    g.   Assessment of exposure intervals, latency, and "at-risk" intervals with regard to their overall impact on the system.

    h.   Visibility of potential common-cause boundaries.

    i.   Assessment of common-cause fault sources.

    j.   Assessment of fail-safe design attributes (fault-tolerant and error-tolerant).

D.2   SCOPE:

This fault tree analysis appendix contains the background information and procedural guidelines necessary for an experienced engineer to perform a fault tree analysis for the first time. Although this appendix contains the basic information on FTAs, the reader may also wish to refer to "Fault Tree Handbook" (U.S. Nuclear Regulatory Commission, document no. NUREG-0492) and other published material for a detailed discussion of FTA structure and mathematical evaluation techniques.

D.3   ROLE OF FTA IN SAFETY ASSESSMENT:

Fault tree analysis should be performed during system conception (part of the PSSA process, see main body 3.3) or after a system concept has been formed (part of the SSA process, see main body 3.4); a "top-down" analysis like FTA allows for its level of detail to match the proposed or current level of design detail respectively.

FTA revisions after design freeze are dictated by the level of the design change. Since the FTA's Primary Event failure rates are based on the Failure Modes and Effects Summary (FMES), the FTA will require updating if the hardware design change causes a failure rate change to be reflected in the FMES. The fault tree analyses should be reviewed again during the latter stages of the aircraft flight program; FTAs which include any equipment design changes resulting from the aircraft test program are usually required as part of the equipment certification supporting documentation.

Figure D1 shows one example of a typical FTA timeline. Note that this figure is an example only; all parties involved in developing a civil airborne system should decide on a specific timeline for FTA generation at the beginning of the safety assessment process.
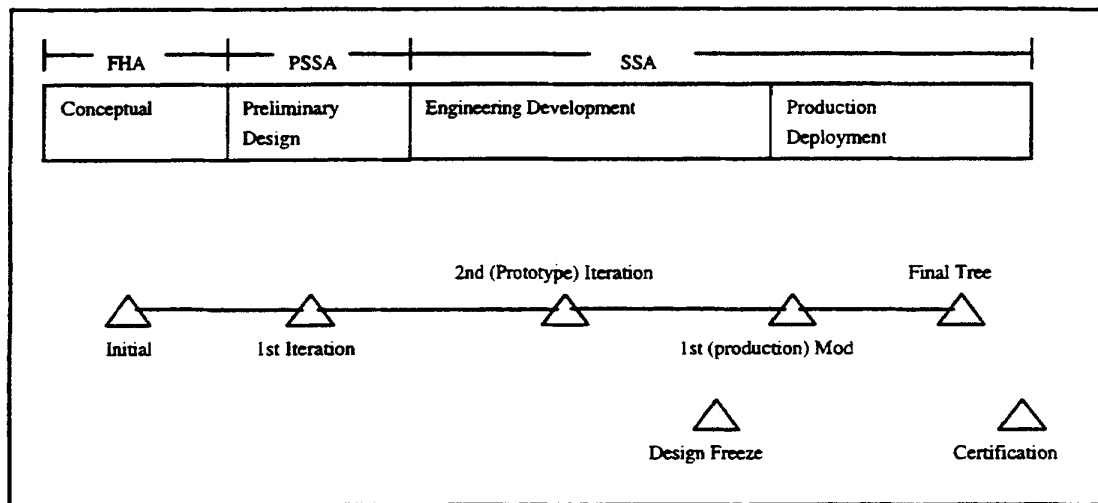
FIGURE D1 - Example of a Typical FTA Timeline

D.3   (Continued):

In the above example:

a.   The "Initial" FTA is performed as part of the FTA process to determine combinations of system failures and allocation of probability budgets to systems.

b.   The "1st iteration" may include fault tree changes due to rework or clarification of some of the analyst's initial assumptions as a result of the requirement validation process. This FTA is performed as part of the system architecture selection process. It is here that the allocation of risk and probability budgets to lower level events occurs.

c.   The "2nd (Prototype) iteration" includes fault tree changes resulting from knowledge gained during hardware or software detailed design. It is at this stage of the program, where 1) the failure rate information from a failure modes and effects summary (FMES) or other source is inserted into the fault tree Primary Events, 2) the top level event failure probability is calculated, and 3) this failure probability is compared to the applicable safety requirement as part of the equipment design verification process. This version of the fault tree becomes part of the supporting documentation needed to successfully complete the "Design Freeze" program milestone.

d.   The "1st (Production) Modification" includes fault tree changes based on hardware or software design changes resulting from problems uncovered during prototype testing.

D.3   (Continued):

   e.   The analyst then creates the "Final Tree" by incorporating any fault tree changes resulting
        from flight test based corrective actions to either hardware or software. This version of the
        fault tree then becomes part of the system safety assessment documentation needed to
        complete the "Certification" program milestone.

D.4   FAULT TREE SYMBOLS AND DEFINITIONS:

All fault trees are composed of two kinds of symbols, logic and event. The general rule with
regard to symbols is, keep it simple; the fewer the different symbol types used the easier it will be
for a person reviewing the fault tree to understand it. Logic symbols are used to tie together the
various branches of the fault tree. Logic symbols should not be directly connected together in the
fault tree, their inputs and outputs should always be events.

The two main logic symbols used are the Boolean logic AND-gates and OR-gates. The analyst
selects an AND-gate when the undesired top level event can only occur when all the next lower
conditions are true. The OR-gate is used when the undesired event can occur if any one or more
of the next lower conditions are true. The analyst may also use other Boolean logic gates if the
system architecture warrants the use of these gate types.

Event symbols most commonly used include a rectangle, triangle, oval, circle, house, and
diamond (see Figure D2). A rectangle contains the description of a logic symbol output or an
event. A triangle indicates a transfer of information and is composed of two types. A triangle with
a vertical line from its top represents a fault tree section (events and their corresponding
probability of occurrence) which is "transferred in". A triangle with a horizontal line from its side
indicates that the event the triangle is tied to is "transferred out" to another branch of the tree. The
oval represents a Conditional Event which defines a necessary condition for a failure mode to
occur (usually used in conjunction with PRIORITY AND and INHIBIT gates). For example,
"monitor fails first" is a Conditional Event because it is necessary before corrupt data can be
propagated through the system undetected.

The circle, house, and diamond all represent types of Primary Events. A circle signifies a Basic
Event. A Basic Event is defined as an event which is internal to the system under analysis,
requires no further development (i.e., has the capability of causing a fault to occur), and for
hardware elements only, can be assigned a failure rate budget or an actual failure rate from an
FMES or other source necessary for quantitative evaluation.

A house event is an event which is normally expected to occur. This event has the following two
possible states.

a.   The event has occurred.
b.   The event will not occur during the period under investigation.

A house functions like a switch and is used to include or exclude parts of the fault tree, which may
or may not apply to certain situations.
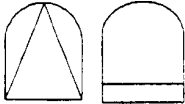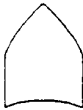
Symbol	Name	Definition
▭	Description Box	Description of an output of a logic symbol or of an event
⌓	AND-Gate	Boolean Logic gate - event can occur when all the next lower conditions are true
⌓⌓	Priority AND-Gate	Boolean Logic gate - event can occur when all the next lower conditions occur in a specific sequence (sequence is usually represented by a conditional event)
⌂	OR-Gate	Boolean Logic gate - event can occur if any one or more of the next lower conditions are true
⬡	Inhibit	Output fault occurs if the (single) input fault occurs in the presence of an enabling conditional event.
△	Transfer	Indicates transfer of information
○	Basic Event	Event which is internal to the system under analysis, requires no further development
⌂	House	Event which is external to the system under analysis, it will or will not happen (Pf=1 or Pf=0)
◇	Undeveloped Event	Event which is not developed further because it has little impact on the top level event or because the details necessary for further event development are not readily available
⬭	Conditional Event	A condition which is necessary for a failure mode to occur

FIGURE D2 - Fault Tree Symbols

D.4   (Continued):

A diamond signifies an Undeveloped Event. An Undeveloped Event is defined as an event which is not developed further because it has negligible impact on the top level event or because the details necessary for further event development are not readily available. Often these types of events are added to a fault tree in order to make the fault tree "complete" from a qualitative model point of view. Software related Primary Events usually take the form of an Undeveloped Event.

Many FTA computer software packages also have additional symbols which are usually unique to that particular FTA software package. The analyst may use other symbols which do not appear in Figure D2 if the symbols are properly defined.

Mathematical symbols that are used in the appendix include:

λ failure rate per hour (usually per hour of flight, but can be per hour of operation)

T   check interval

t   the exposure time or "at risk time" associated with the particular primary event

P or P_t probability of the event or failure occurring during the time t

D.5   OVERVIEW OF PERFORMANCE OF FAULT TREE ANALYSIS:

Performing a fault tree analysis requires six basic steps.

1.   Define the goal and depth of analysis for the FTA.

Be specific -- Will the fault tree be used to determine failure event budgets (part of a PSSA process)? Will it be used to verify system design compliance with established safety requirements (part of the SSA process)? Will the fault tree be evaluated qualitatively, quantitatively, or both? Defining the FTA goal helps the analyst determine the scope of the FTA.

2.   Define the analyst level required.

How deep (i.e., to what level) into the system will the analyst go to do the analysis? Will the system be subdivided in order to perform multi-level FTAs? Knowing the depth of the analysis is important for determining the scope of the FTA and for defining how the FTA results will be reported (i.e., tie in closely with Step 5). Section D.6 contains more information on the analysis definition.

D.5 (Continued):

3. Define the undesired event.

This undesired event can either by tied directly to an FHA or it can be tied to a Primary Event in another fault tree if the system has been subdivided into multiple levels (i.e., alignment of boundaries in multi-level FTAs). If the undesired event is a subdivision of a larger event, then care should be taken when combining the sub trees back together. All sub trees so combined must be reviewed for independence before combining them in a new fault tree. The probability of failure budget for the undesired event is also stated. (Note: budgets are numerical even if the analysis is qualitative.) Section D.7 contains more information on defining undesired events.

4. Gather the most complete system data available at the time and analyze it to determine the possible fault and failure events and event combinations which lead to the top event.

Section D.8 contains more information on this step.

5. Construct the fault tree associated with the undesired event from Step 3.

Section D.9 contains information on fault tree construction.

6. Analyze and summarize the FTA results.

Sections D.10 through D.13 contain more information on analyzing fault trees and summarizing their results.

D.6 FTA ANALYSIS DEFINITION:

The fault tree can be used to accomplish the main goals listed below.

1. In the PSSA process

a. Allocate the probability of failure (P_f) (also known as P_f budgeting) when working with P_f quantitative objectives. Budgeted failure probabilities in a PSSA fault tree can be tighter (i.e., a lower probability) than the probability number required by the tree mathematics.

b. Establish system architecture design requirements when working with fail-safe qualitative objectives.

D.6   (Continued):

    2.   In the SSA process

        a.   Verify compliance with established PSSA FTA objectives.

The analyst can work either goal at any indenture level within the system. An indenture level is defined as any one level within a multi-level FTA. The analyst will need to determine the boundary for the FTA. The boundary will be subjectively based on what the analyst wants or needs to accomplish by performing the FTA. Table D1 lists several possible indenture levels and their potential boundaries. Note that the information presented in the "FTA Boundary" column indicates one potential boundary of the analysis (i.e., the lowest level of design detail that the analyst will consider when performing the "top-down" FTA). The analyst should choose the boundaries based on the scope of analysis. The following item may be considered: what are the system inputs and outputs, what support system detail should be included, should human error be included, should software error be included, etc.

The selected FTA boundary ties in closely with how the fault tree evaluation results are reported.

D.7   UNDESIRED TOP LEVEL EVENT DETERMINATION:

The analyst should compile a list undesired events. Each undesired event will become the top level event in a fault tree. Depending on the system indenture level the analyst is dealing with, these top level events can have different origins. Table D2 describes some of the sources based on the safety assessment process diagram presented in the main body of this document.

D.8   SYSTEM INFORMATION COLLECTION:

The analyst should gather the most complete and current system data available. The analyst should analyze the data to determine the possible failure events and combinations which lead to the top event. The analyst will obtain the information from two main sources:

a.   System functional flow block diagrams
b.   Design description documentation or design requirement documentation

Remember that in order for the FTA to be an effective tool for establishing system safety criteria, the analysis should be performed as the design is being developed and not as an afterthought.

D.8.1   Review the System Functional Flow Block Diagram:

The analyst should review the system functional flow block diagram. The system functional flow block diagram will provide information on flight success criteria and system inter-dependencies. The word "system" in this context can refer to any grouping of aircraft or support equipment; e.g., propulsion system, engine subsystem, or autopilot LRU. The analyst must have intimate knowledge of the "system" to be analyzed in order to determine the single failures and combinations of failures which could cause the top level event for that particular tree to occur.

TABLE D1 - Examples of FTA Boundaries

FTA Indenture Level	FTA Boundary	Characteristics of FTA at This Indenture Level
A/C	A/C block diagram	FHA/PSSA: P$_f$ budgeting to the various major systems composing an A/C level function.
		FHA/PSSA: Identification of failure effects causing or contributing to A/C level failure conditions.
System	System block diagram	FHA/PSSA: P$_f$ budgeting to the Items within the system.
		SSA: Use of Item failure rates (taken directly from Item reliability prediction analysis) for Primary Event quantitative evaluation.
Item	Item functional block diagram	PSSA: P$_f$ budgeting to the various functional blocks within the item (i.e., allocation to hardware and software functions).
		SSA: Use of failure rates for specific groups of circuitry of interest (e.g., failure rate of core processor function -- CPU, oscillators, memory, etc.) when the entire item failure rate is too large to demonstrate compliance with safety requirements during a quantitative evaluation.
Item Functional Block	Item schematics	PSSA: P$_f$ budgeting to the various functional circuitry and their respective monitors, within the item functional blocks. Allocation of Design Assurance Levels to software functional elements.
	Software functional elements	SSA: Use of failure rates for specific components of interest (e.g., failure rate of ARINC 429 receiver) when the failure rate for a group of circuitry causes non-compliance with safety requirements during a quantitative evaluation. The analyst is able to take advantage of hardware component failure modes and their percentage of occurrence.

TABLE D2 - Sources of Top Level Events

FTA Indenture Level	Origin of Top Level Events
Aircraft	Aircraft Function FHA
System	System FHA and/or Aircraft Function FHA and/or Aircraft Function FTA
Item	System FTA
Item Functional Block	Item FTA

D.8.2   Review Design Description/Requirement Documentation:

The analyst should gather all existing system data and analyze it to determine the possible failure events and combinations which could lead to the top level event for that particular tree. Possible sources include the system architecture description documents, the various system, hardware, and software design specifications and description documents, and the designer/analyst's own intimate knowledge of the system.

D.9   FAULT TREE CONSTRUCTION:

The following four steps should be followed for constructing a fault tree.

1.   State the undesired top level event (and its probability of failure objective or failure rate objective if applicable) in a clear, concise statement.

2.   Develop the upper and intermediate tiers of the fault tree, determine the intermediate failures and combinations which are minimum, immediate, necessary, and sufficient to cause the top level event to occur and interconnect them by the appropriate fault tree logic symbols. Extend each fault event to the next lower level.

3.   Develop each fault event down through successively more detailed levels of the system design until the root causes are established or until further development is deemed unnecessary.

4.   Establish probability of failure budgets or failure rate budgets, evaluate the ability of the system to comply with the safety objectives, and redesign the system if deemed necessary (PSSA process).

OR

Evaluate the fault tree in either a qualitative and/or quantitative manner (SSA process).

D.9.1   State the Fault Tree's Undesired Top Level Event:

This section addresses the first fault tree construction step.

1.   State the undesired top level event (and its probability of failure objective if applicable) in a clear, concise statement.

The analyst will enter the fault tree top level event into a description box. This statement should identify what the undesired event is and when it occurs. For a majority of the fault trees, this top level event is already identified in an FHA or in another higher-level fault tree and just needs to be copied into the rectangular event symbol. In other cases, the analyst will need to clarify the undesired event statement before placing it into the description box.

The undesired top level event must be clearly and concisely stated because it sets the tone for the series of questions the analyst will ask when constructing the various fault tree levels. Table D3 provides some examples of poorly worded and revised top level event statements for SSA FTAs. During PSSA, the type of information stated in the "Revised Statement" column may not be available.

TABLE D3 - Examples of Undesired Event Statements

Poorly Worded Statement	Problem with Statement	Revised Statement
Loss of airspeed indication	Too vague as to "What" the fault is -- does it mean loss of primary airspeed, loss of secondary airspeed, or loss of both?	Loss of all airspeed display in the cockpit.
Display of misleading approach data without annunciation of failure	Too vague as to where the fault occurs -- is it on both navigation displays or only one?	Display of misleading approach data on both navigation displays without annunciation of failure.
Display of misleading attitude on a single pilots primary flight display, without annunciation of failure	States "what" but not "when" -- if considered during all flight phases, this event has a failure condition classification of major. If considered during take off after rotation, this event has a failure condition classification of Hazardous/Severe-Major. "When" defines the time period used with respect to P_f during a quantitative evaluation.	Display of misleading attitude on a single pilots primary flight display, without annunciation of failure during takeoff after rotation.

D.9.2   Develop the Upper and Intermediate Tiers of the Fault Tree:

This section addresses the second fault tree construction step.

2.   Develop the upper and intermediate tiers of the fault tree, determine the intermediate failures and combinations which are minimum, immediate, necessary, and sufficient to cause the top level event to occur and interconnect them by the appropriate, conventional fault tree logic symbols. Extend each fault event to the next lower level.

The analyst should construct the upper tiers of the fault tree (see Figure D3). Each fault tree will start with a top level event for that particular fault tree which is a previously defined event (see D.9.1). The analyst will expand the tree to each lower level by considering the following questions.

a.   Are there any single failures which will cause the listed event to be true?

b.   Are there any multiple failure combinations which will cause the listed event to be true?
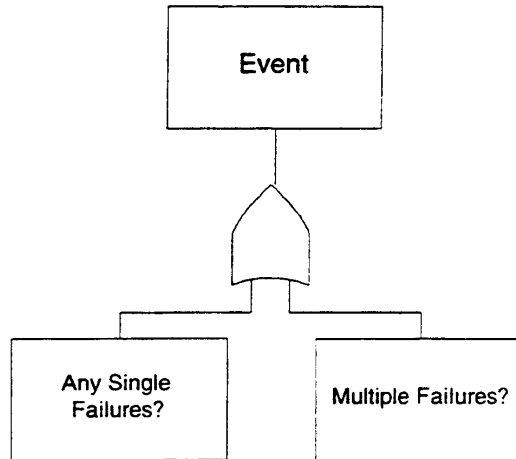
FIGURE D3 - Upper Tier of Fault Tree Based on Initial Questions

D.9.2   (Continued):

If there are not any single failures but there are multiple failure combinations, then the fault tree's first tier might be drawn like Figure D4.
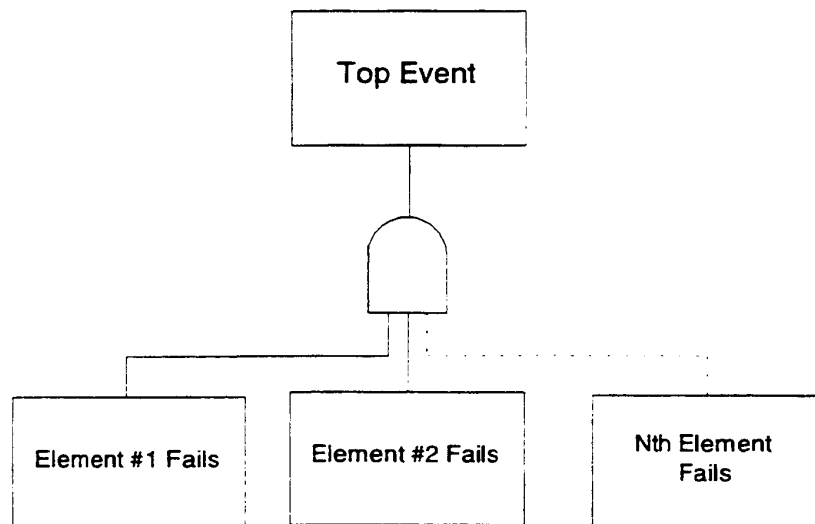
FIGURE D4 - Upper Tier of Fault Tree without Single Thread in the System

D.9.2 (Continued):

Multiple failure combinations may be dependent on a specific order in which they fail. These events are then defined as failure order dependent events (also known as sequential events). Failure order dependent events should be drawn as inputs into an AND-gate from left to right in the order in which they must fail. If, in the above figure, the first and second elements of the system must fail prior to the Nth element in order for the EVENT to occur, then the AND-gate may include another Undeveloped Event input which represents the probability that the "n" elements will fail in that order. Another way to represent failure order events dependent events is to use a PRIORITY AND-gate along with a Conditional Event. For details see also D.11.1.4.

For example, assume the above system has three elements. The fault tree's first tier would be drawn as in Figure D5.
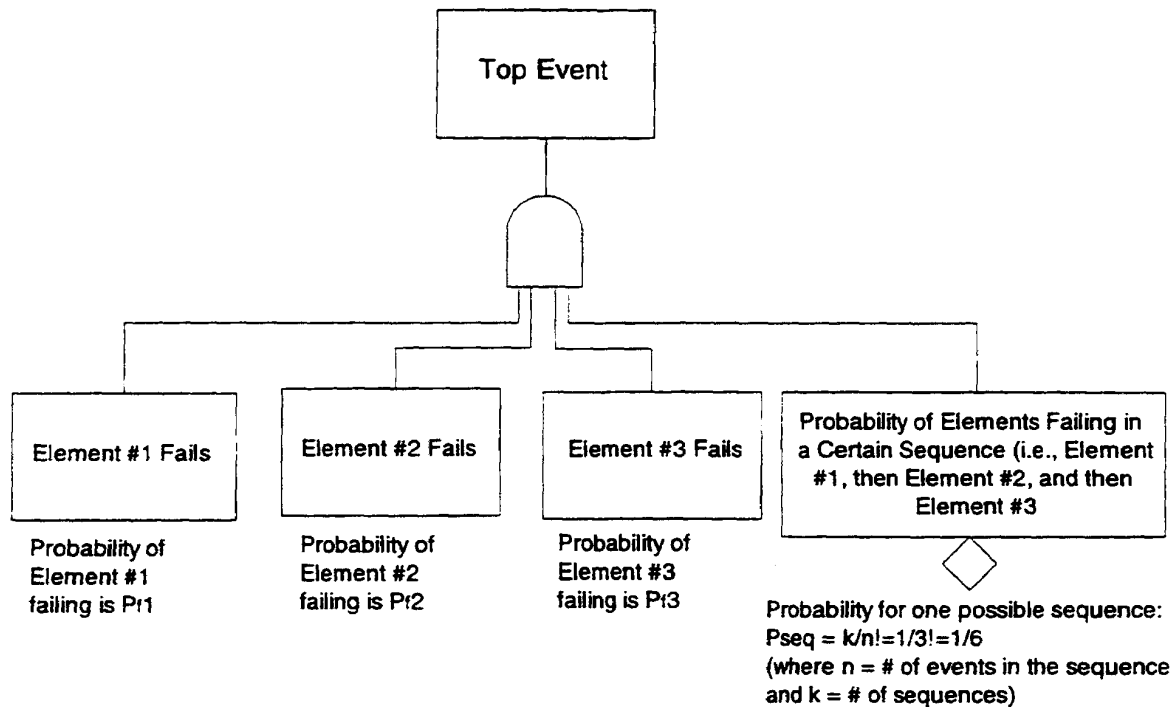
FIGURE D5 - Upper Tier of Fault Tree Considering Failure Sequence

D.9.2 (Continued):

The n! (factorial) term represents the number of event sequences which could occur. For this example, the possible event sequences are $P_f1P_f2P_f3$, $P_f1P_f3P_f2$, $P_f2P_f3P_f1$, $P_f2P_f1P_f3$, $P_f3P_f1P_f2$, and $P_f3P_f2P_f1$.

Next, the analyst will expand the tree by working "top-down" while considering the above questions for the event or failure effect, as it is also referred to, at each new level. When considering fail-safe events based on multiple failures, the analyst should consider contributions from incorrect outputs and inoperative protective or reconfiguration mechanisms as shown in Figure D6.
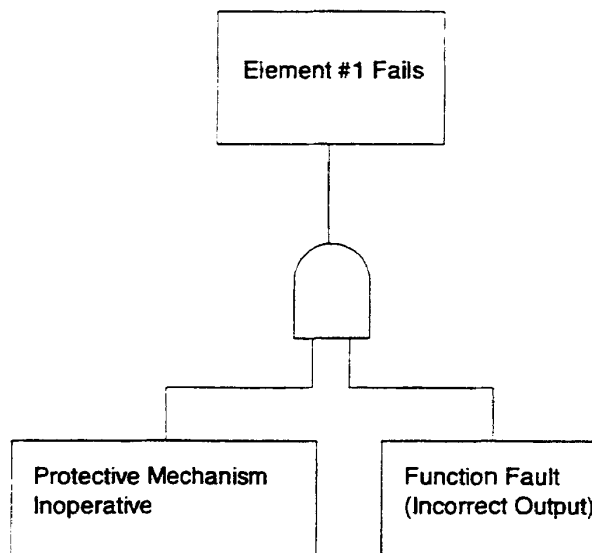
FIGURE D6 - Expanding a Fault Tree Event with Respect to Fail-Safe System Elements

Throughout the fault tree construction effort, the analyst must make sure that a pre-defined naming convention is followed so everyone working on a given system creates the fault trees in the same manner. When selecting a naming convention, the analyst should keep in mind three things.

a. The naming convention must prevent conflicts between events; i.e., no two different events can have the same name and identical events must have the same name. This is crucial for proper Boolean Algebra reduction.

b. The naming convention should not be too cryptic or someone looking at the tree will have to constantly refer to some sort of table in order to decipher the name.

D.9.2   (Continued):

    c.   The naming convention must be maintainable; i.e., set up the naming convention with ample growth potential so that you do not have to go back and re-name all events because your convention does not allow you to add several new events at a later date.

    If a software FTA package is used to construct the trees, this pre-defined naming convention must be compatible with the software package. Some software packages require gates to be named in order to identify the intermediate events which are outputs of logic gates.

D.9.3   Extend the Top Event Branches Down to the Primary Events:

    This section addresses the third fault tree construction step.

    3.   Develop each fault event down through successively more detailed levels of the system design until root causes are established or until further development is deemed unnecessary.

    The analyst should further develop and complete the fault tree by extending the fault tree branches down to the Primary Events (i.e., Basic Events, External Events, and Undeveloped Events). These Primary Events are the root causes of the first level fault events.

    The root cause will be hardware failure/error or software error broken down to a level of detail necessary to demonstrate system design compliance with safety objectives. Here is where the goal of the FTA becomes apparent with its impact on the FTA scope. If the FTA goal is a qualitative evaluation, gathering further information on the Primary Event is not necessary (unless the analyst determines that a further detailed qualitative analysis is required). If the FTA goal is a quantitative evaluation, the analyst should gather more detailed information on the Primary Event (hardware failure rates and "at-risk" or exposure times).

    In this appendix, four particular examples are developed to show typical fault tree representations which include basic events with or without latency and required order factors. The detailed mathematical calculations are further explained in D.11.1.5.

D.9.3.1   Example When Two Item Failures Cause a Loss of a Function: The first example fault tree shown in Figure D7 shows the simple failure case where the top event is caused by the loss of both items during the same flight. Both items are known to be operating at the start of the flight and neither fail latent. The two failures can occur in either order.
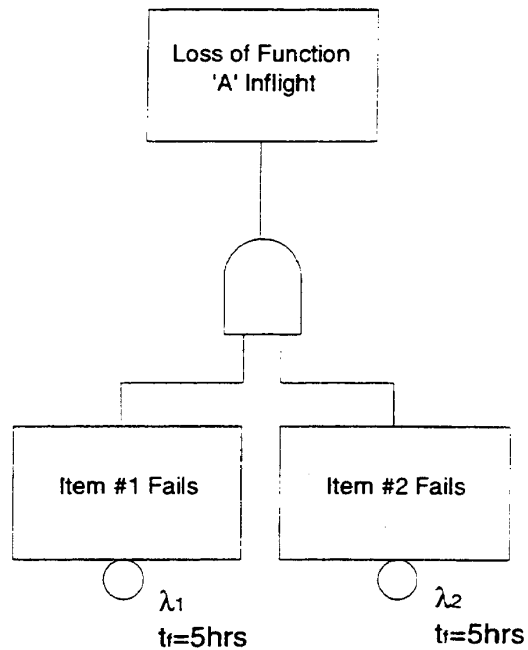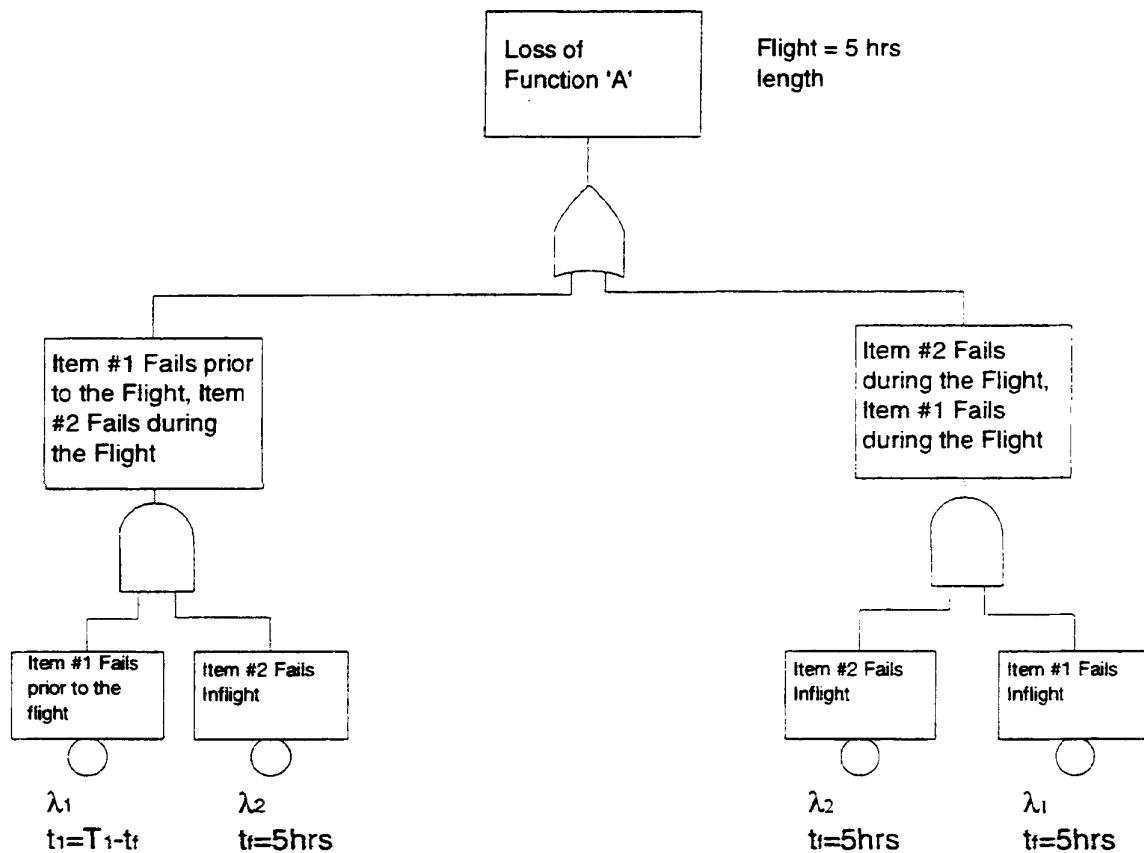
FIGURE D7 - Example of a Fault Tree Structure When Two Item Failures
Cause a Loss of a Function

D.9.3.2 Example When Two Item Failures Cause a Loss of a Function Where an Item Could Fail
Latent: In the second example, Item 1 can fail at any point between when it is checked (time
= zero) and when it is next checked (time = T). Item 2 is known to be operating at the start of
each flight and never fails latent. The order of failure does not matter. An example fault tree is
shown in Figure D8.

Loss of
Function 'A'

Flight = 5 hrs
length

Item #1 Fails prior
to the Flight, Item
#2 Fails during
the Flight

Item #2 Fails
during the Flight,
Item #1 Fails
during the Flight

Item #1 Fails
prior to the
flight

Item #2 Fails
Inflight

Item #2 Fails
Inflight

Item #1 Fails
Inflight

λ_1
$t_1 = T_1 - t_f$

λ_2
$t_f = 5hrs$

λ_2
$t_f = 5hrs$

λ_1
$t_f = 5hrs$

FIGURE D8 - Example of a Fault Tree Structure When Two Item Failures
Cause a Loss of a Function Where an Item Could Fail Latent

D.9.3.3 Example When Two Item Failures Cause a Loss of a Function Where each Item Could Fail
Latent: In the third example, either item could fail latent, but if both fail, this would be detected
by virtue of it causing the top event. Therefore, at least one of the items must be operating at
the start of each flight. An example fault tree is shown in Figure D9. Three things should be
noted about this figure.

1. An undeveloped event for failure order (i.e., ROF = k/n! as shown in Figure D5 and further
described in D.11.1.4) is not required because failure order dependence is built into the
tree structure via the latency period ($t_n = T_n - t_f$). This is representative of a failure during the
latency period before the flight.

2. The right-most AND-gate is necessary to cover the case that both items fail during the
flight without a required sequence.
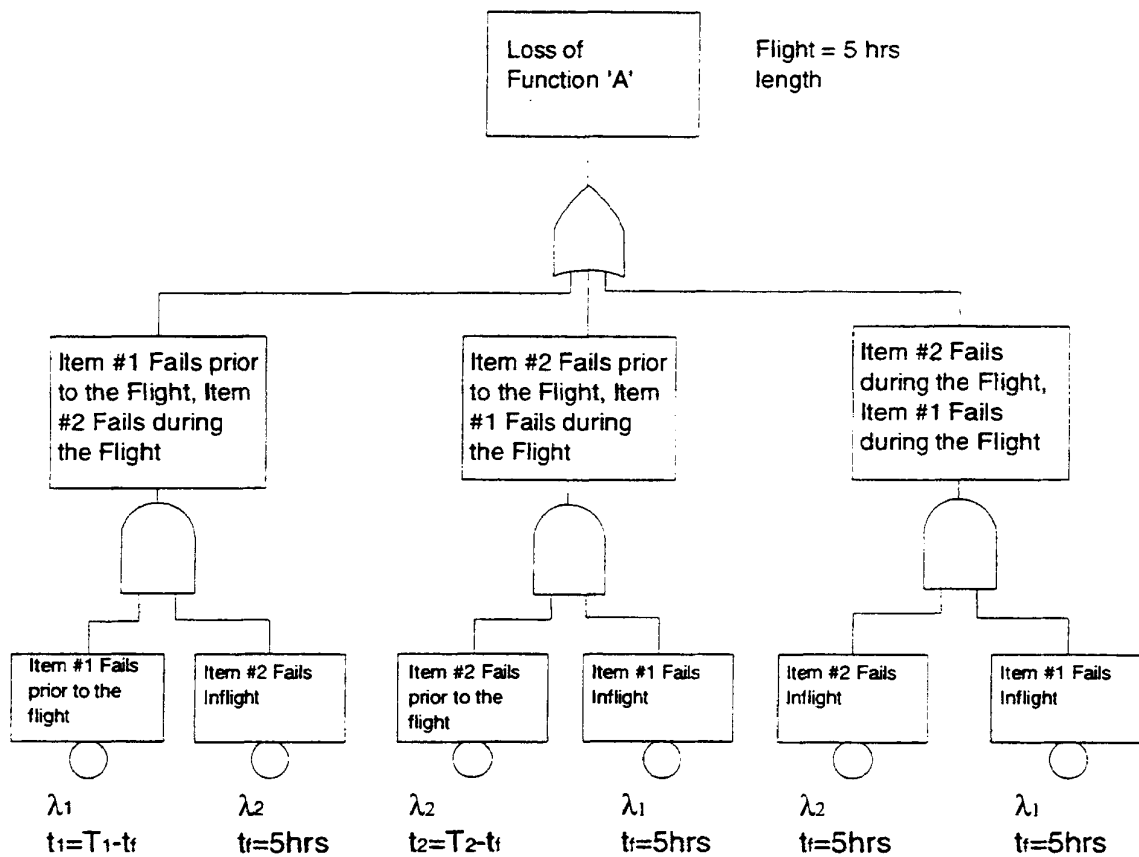
FIGURE D9 - Example of a Fault Tree Structure When Two Item Failures Cause
a Loss of a Function Where each Item Could Fail Latent

D.9.3.3 (Continued):

3. The right-most AND-gate is often omitted and the exposure times set equal to the
inspection intervals, for cases where t_f is much less than the inspection intervals.

D.9.3.4 Example When Two Item Failures Cause a Top Event and One Item Could Fail Latent and
Failures are Order Dependent: In the fourth example, item one (the latent one) must fail prior
to item two or the top event does not result. Item two is known to be operational at the start of
the flight. This is typical of a failure/monitor situation where the top event is an erroneous
output rather than a loss of function. An example involving the transmission of incorrect data is
provided in Figure D10.

The required order factor (ROF) is used per D.11.1.4.

Erroneous Output of Function 'A' Inflight

Flight = 5 hrs length

Item #1 Fails prior to the Flight, Item #2 Fails during the Flight

Item #1 Fails prior to Item #2 and both fail during the Flight

Item #1 Fails prior to the flight

Item #2 Fails Inflight

Item #1 Fails Inflight

Item #2 Fails Inflight

Required Order Factor

λ_1
$t_1 = T_1 - t_f$

λ_2
$t_f = 5hrs$

λ_1
$t_f = 5hrs$

λ_2
$t_f = 5hrs$

1/2
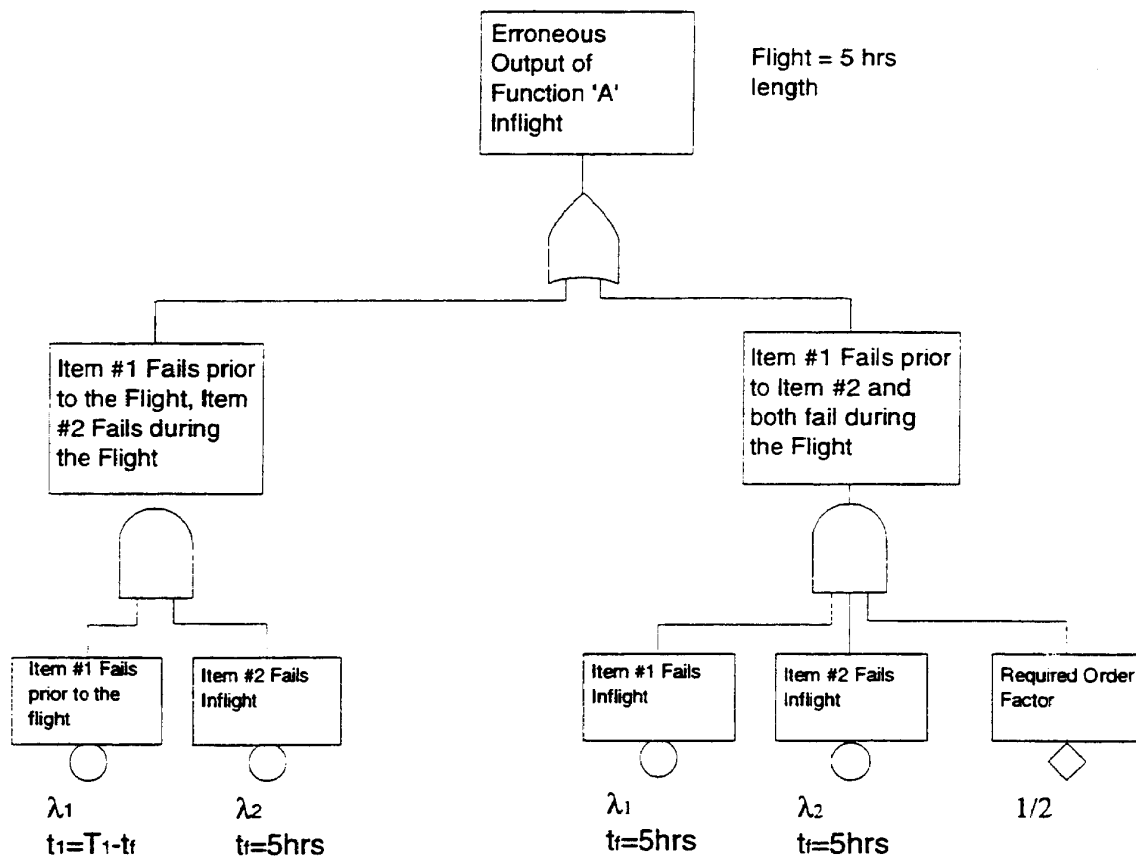
FIGURE D10 - Example of a Fault Tree Structure When Two Item Failures Cause a Top Event and One Item can Fail Latent and Failures are Order Dependent

D.9.4   Evaluate the Fault Tree for Compliance with Safety Objectives:

This section addresses the fourth fault tree construction step.

4.   Evaluate the fault tree in either a qualitative or quantitative manner.

Fault trees are qualitative models by nature of their construction. Depending on the goal of the FTA, the analyst will evaluate the fault tree in a qualitative or qualitative and quantitative fashion (when the fault tree contains hardware failures and development errors (hardware and software), the analyst's quantitative evaluation will actually be a combination of the two methods). Table D4 summarizes the results of the two evaluation methods. The analyst should find this table useful when determining the FTA goal. Qualitative evaluation and quantitative evaluation are further described in Section D.10 and D.11 respectively.

TABLE D4 - Summary of Qualitative Versus Quantitative FTA Evaluation
Techniques and Results

Qualitative	Quantitative
MINIMAL CUT SETS	NUMERIC PROBABILITIES
Combination of component failures causing system failure	Probabilities of system and cut set failures
QUALITATIVE IMPORTANCE	QUANTITATIVE IMPORTANCE
Qualitative ranking of contributions to system failures, direct cause vs. contributory via fail-safe	Quantitative ranking of contributions to system failure
COMMON CAUSE POTENTIALS	SENSITIVITY EVALUATIONS
Minimal cut sets potentially susceptible to a single failure cause	Effects of changes in models and data, errors determinations

D.10 QUALITATIVE FAULT TREE EVALUATION:

The qualitative fault tree evaluation produces minimal cut sets. These can be used to determine the qualitative importance and to evaluate common-cause potentials.

The following sections provide only the minimal amount of information needed to understand the subject manner. For a more detailed and complete explanation of these techniques, refer to "Fault Tree Handbook" (NUREG-0492) or one of many similar books on the subject of fault tree evaluation.

D.10.1 Fault Tree Minimal Cut Set Determination:

A fault tree minimal cut set is a smallest set of Primary Events which must all occur in order for the undesired top level event to occur.

The analyst must be aware of the potential lack of independence between two or more Primary Events in order to avoid serious errors in qualitative and quantitative analysis. This lack of independence can occur whenever the same event appears in more than one location in the fault tree or when certain single failures can result in more than one failure event simultaneously. When dependence is known, it is modeled by the same event (or gate) appearing at more than one place in the fault tree and is handled correctly by the application of Boolean algebra to generate the cut sets. Care should be taken when in a high level tree (where the primary events are derived as top level events from separate fault tree analyses), an event can appear in more than one of those separate fault trees. If this happens, the dependence will not be visible in the high level tree and the probability calculation for the high level tree will be incorrect. To obtain accurate calculations in this case, it is necessary to replace the derived primary events with their corresponding detailed fault tree structure. This allows the common events to be correctly modeled throughout the high level fault tree so that accurate cut set listings and probability calculations can be obtained.

D.10.1 (Continued):

The analyst may use "direct analysis" on the fault tree when the various Primary Events only appear once in that given tree. However, for most civil airborne systems this is not the case. The logic symbol dictates how the calculation will be performed based on the following Probability Calculus basic rules. (NUREG-0492 addresses this subject in greater detail.)

a. The probability of obtaining an outcome A is denoted by P(A), outcome B by P(B), and so on for other outcomes.

b. The probability that A AND B occur is denoted by P(AB).

c. The probability that A OR B occurs is denoted by P(A+B).

d. If A and B are two independent events with the probabilities P(A) and P(B), then the probability that both events will occur is the product:

P(AB) = P(A) * P(B) -- applies to two input AND-gates.

e. If A, B, and C are three independent events with the probabilities P(A), P(B), and P(C), then the probability that all three events will occur is the product:

P(ABC) = P(A) * P(B) * P(C) -- applies to three input AND-gates

f. The same logic can be carried to four or more independent events.

g. If the two independent events can occur simultaneously, the probability that either A OR B or both A AND B will occur is:

P(A+B) = P(A) + P(B) - [P(A) * P(B)] -- applies to two input OR-gates.

h. If the three independent events can occur simultaneously, the probability that A OR B OR C, or any combination of these three will occur is:

P(A+B+C) = P(A) + P(B) + P(C) - [P(A) * P(B)] - [P(A) * P(C)] -

[P(B) * P(C)] + [P(A) * P(B) * P(C)] -- applies to three input OR-gates.

The same logic can be carried to four or more independent events.

D.10.1 (Continued):

    i.   If the two events are mutually exclusive so that when one occurs the other cannot occur, the equation for a two input OR-gate simplifies to:

       $P(A+B) = P(A) + P(B)$ Furthermore, $P(AB) = 0$

       This equation is also good approximation for two non-mutually exclusive events with low probabilities (errs on the conservative side).

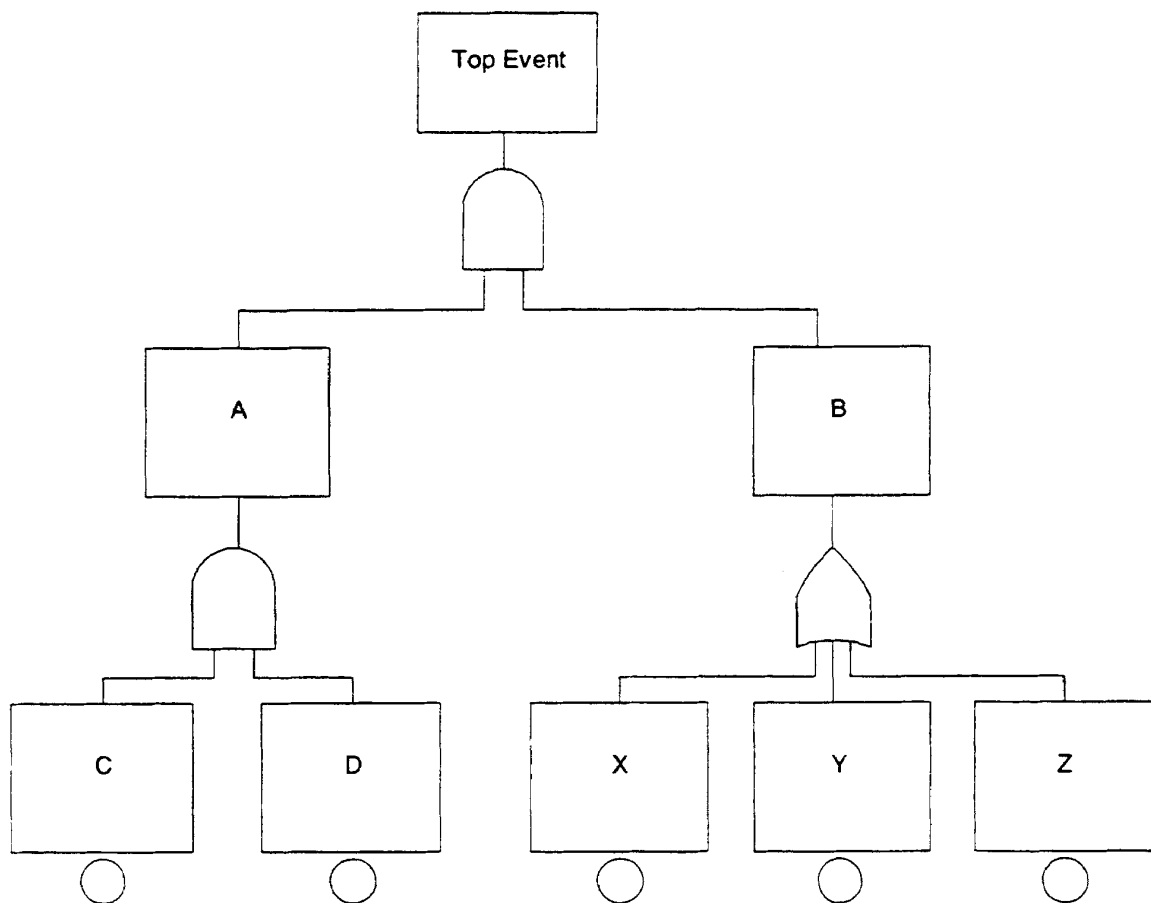For a "direct analysis" example, consider the tree in Figure D11.

FIGURE D11 - Tree to Demonstrate Direct Analysis Techniques

D.10.1 (Continued):

From Figure D11:

P(A) = P(C) * P(D) [C and D are independent events]

P(B) = P(X) + P(Y) + P(Z) [X,Y, and Z are mutually exclusive events]

P(top) + P(A) * P(B) = [P(C) * P(D)] * [P(X) + P(Y) + P(Z)]

The analyst must perform Boolean Analysis on the tree structure if Primary Events occur more than once in that given tree. Based on the location of these identical Primary Events within the tree, "direct analysis" without first reducing the tree via Boolean Analysis will lead to an undesired top level event probability which is either greater than or less than the event's true probability.

As an example of fault tree reduction via Boolean Analysis, consider the tree structure in Figure D12.
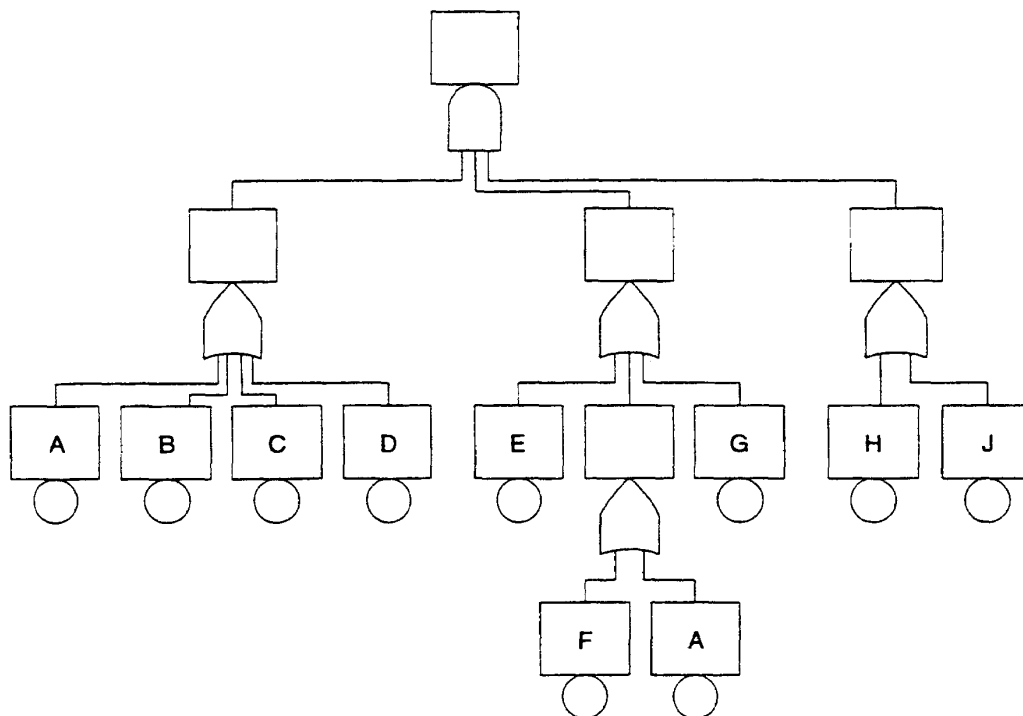
FIGURE D12 - Tree to Demonstrate Boolean Reduction Techniques

D.10.1 (Continued):

The Boolean reduction follows the following steps.

a. Use "direct analysis" to determine the apparent "top". The term apparent is used because event A is located in two branches of the fault tree.

top = (A+B+C+D) * (E+F+A+G) * (H+J)

b. Multiple out the above equation in order to get terms separated by "+" signs.

top = AEH + AFH + AAH + AGH + BEH + BFH + ABH + BGH + CEH + CFH + ACH + CGH + DEH + DFH + ADH + DGH + AEJ + AFJ + AAJ + AGJ + BEJ + BFJ + ABJ + BGJ + CEJ + CFJ + ACJ + CGJ + DEJ + DFJ + ADJ + DGJ

c. Apply the following Boolean Logic rules to the expanded FTA equation:

(1) A + A = A, (2) A * A = A, (3) A + AK = A, (4) AAK + AK

By applying the above logic, the fault tree minimal cut set is determined by reducing the number of elements in a term and reducing the number of total terms. Applying Boolean Logic to the equation from Step 2:

top = ~~AEH~~ + ~~AFH~~ + AAH + ~~AGH~~ + BEH + BFH + ~~ABH~~ + BGH + CEH + CFH + ~~ACH~~ + CGH + DEH + DFH + ~~ADH~~ + DGH + ~~AEJ~~ + ~~AFJ~~ + AAJ + ~~AGJ~~ + BEJ + BFJ + ~~ABJ~~ + BGJ + CEJ + CFJ + ~~ACJ~~ + CGJ + DEJ + DFJ + ~~ADJ~~ + DGJ

Rewriting this equation results in the fault tree minimal cut set. Notice that twelve terms were eliminated and two terms went from 3 to 2 elements within the term.

top = AH + BEH + BFH + BGH + CEH + CFH + CGH + DEH + DFH + DGH + AJ + BEJ + BFJ + BGJ + CEJ + CFJ + CGJ + DEJ + DFJ + DGJ

d. Draw the reduced fault tree by first combining terms within the minimal cut set equation (optional step). The reduced fault tree is shown in Figure D13.

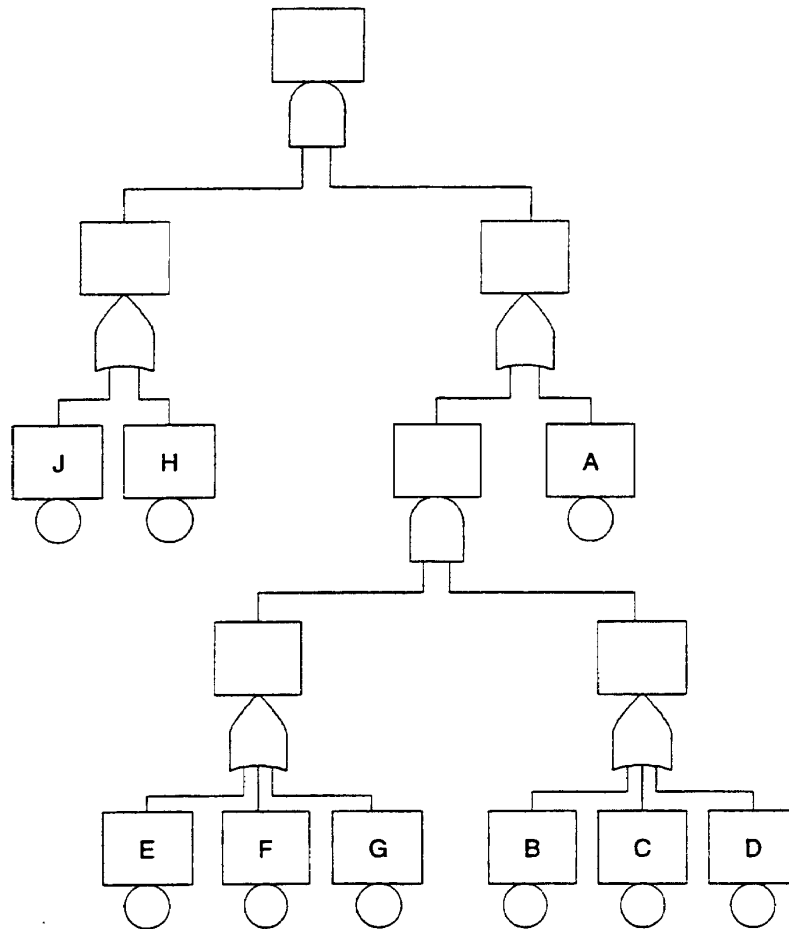top = (J+H) * [A + (E+F+G) * (B+C+D)]

FIGURE D13 - Reduced Fault Tree

D.10.1 (Continued):

Many commercially available fault tree analysis software packages will generate the cut sets automatically when given the proper commands. Once the reduced tree is drawn, the analyst must verify that all AND-gates indicate a true combination of independent events. This step is very important before performing the FTA numerical calculations.

D.10.2 Qualitative Importance Determination:

In order to get some idea of how the various cut sets impact the undesired top level event, the analyst can evaluate the fault tree using a method known as Qualitative Importance. Qualitative Importance is simply ranking the cut sets in ascending order based on the number of Primary Events in the cut set. This method allows the analyst to see the various Primary Events relative importance with respect to top level event occurrence based on how many times the Primary Event appears in the cut sets and in what combination with other Primary Events. This FTA evaluation technique works well with hardware failure/development error, software development error, and a combination of the two in the same tree.

Assume that the analyst wants to evaluate a fault tree via qualitative importance. First, the cut set is ranked as described above. This ranking gives the analyst knowledge of whether the top level event has any associated single point failures and how often any one Primary Event helps cause the top event to occur.

Furthermore, by assuming a standard failure rate value (e.g., 1E-06) and a standard exposure time (e.g., 100 hours) for all hardware component related Basic Events, the analyst can get a gross estimate of a cut set's relative importance. For example, using the values provided in the previous sentence, a cut set with two Basic Events has a probability of failure (P_f) of 1E-08, a cut set of three Basic Events has a P_f of 1E-12. Using this gross estimating technique, the analyst can quickly conclude that cut sets with five or more Basic Events have very little relative impact on the top level event probability of failure.

The drawbacks associated with this evaluation method are as follows.

a. If the analyst has hardware related Basic Event at indenture levels higher than the component level, an additional reliability analysis should be performed in order to get a respectable failure rate number for the P_f estimate.

b. Basic Event exposure times can vary greatly from one Basic Event to another because of such factors as monitor cycle times, monitor exposure times, maintenance intervals, etc. Consequently, the estimated failure probabilities used to weigh relative importance of one cut set to another are no better than gross estimates. Exposure time variations can mean two or three orders of magnitude difference between the estimated failure probabilities and quantitatively obtained failure probabilities.

D.10.3 Common Cause Vulnerability:

Fault trees can also be qualitatively evaluated using a method known as Common Cause Susceptibility resulting in a list of Common Cause Potentials. Common Cause Susceptibility is based on the fact that cut sets provide a finite listing of Primary Event combinations which will cause the top level event to occur. The analyst can get an idea of how susceptible the top level event is to common cause failures by examining each cut set. A single failure must cause more than one Primary Event in the cut set to occur in order to be classified as a common cause failure. Therefore, a cut set having similar Primary Events is more likely to be susceptible to common cause failures than a cut set having dissimilar Primary Events.

D.10.3 (Continued):

For example, suppose cut set #1 has three Primary Events, all of which are the same CPU part number in a triple similar redundancy configuration system. Suppose cut set #2 also has three Primary Events, all of which are different CPU part numbers in triple dissimilar redundancy configuration system. By examining these two cut sets, the analyst can readily determine that cut set #1 has a higher potential for a common cause fault like a generic microcode error, than cut set #2.

Each potential for a common cause failure should be examined to determine if a single cause really exists which will cause these failure combinations to occur and cause the listed event. These common-cause faults are analyzed for their likelihood and should be placed in the fault tree only if they cannot be designed out of the system.

Common cause analysis should address common cause faults and generic errors. Appendices I, J, and K contain detailed information on performing common cause analyses.

D.10.4 Hardware and Software Development Assurance Level Determination:

The minimal cut sets of the fault tree can be used to assist in the determination of the appropriate Development Assurance Levels for hardware and/or software as part of the PSSA.

The principles described in ARP4754 should be used if system architecture is to be considered when determining the Development Assurance Level of hardware and/or software, to assign a level which is different from that associated with the failure condition category of the top event.

When hardware and/or software items are associated with more than one top event in a safety analysis, the Development Assurance Level should be the highest which results from the review of each fault tree. An example of a fault tree which includes the consideration of hardware and software errors is provided in Section D.12.

D.11 QUANTITATIVE FAULT TREE EVALUATION:

Quantitative fault tree evaluation techniques produce three types of results: (1) numerical probabilities, (2) quantitative importance, and (3) sensitivity evaluations. All three results can be obtained from minimal cut sets as described in Section D.10. Other methods exist which may be more efficient for some fault trees. The following sections provide only the minimal amount of information needed to understand the subject matter and have been restricted to elementary examples which are based on the assumption of constant failure rates and small λt. For a more detailed and complete explanation of these techniques, refer to "Fault Tree Handbook" (NUREG-0492) or one of many similar books on the subject of fault tree evaluation.

The methods of fault tree quantification other than those described in this section, which can be shown to be logically and mathematically correct, may be used at the discretion of the analyst.

D.11.1 Numerical Probability Calculations:

The quantitative evaluation technique for determining a fault tree level event probability of failure (P_f) using cut sets has five major steps.

1. Determine the fault tree minimal cut sets.
2. Determine the failure rates of the Basic Events.
3. Determine the exposure times and "at risk" times of the Basic Events.
4. Establish any relevant Required Order Factors.
5. Perform the FTA numerical calculations.

These five steps are described further in the subsequent subsections. Note that the analyst cannot perform quantitative analysis on minimal cut sets containing development errors. Fault trees containing development errors should be evaluated using a qualitative evaluation method described in Section D.10. Fault trees containing both hardware failures and hardware and software development error primary events require the analyst to only perform quantitative analysis on the hardware failure related primary events. Section D.12 describes incorporation of the development errors into the fault trees in greater detail.

D.11.1.1 Determine the Fault Tree Minimal Cut Sets: The process of determining minimal cut sets for quantitative FTA evaluation is exactly the same as the process used for qualitative evaluation. Refer to D.10.1.

D.11.1.2 Determine the Failure Rates of the Basic Events: A failure rate for each hardware related Basic Event in the fault tree should be determined. Failure rates should be determined whenever possible from failure rate date of similar equipment already in field use. Other industry wide sources of failure rates and/or mode distributions include MIL-HDBK-217, MIL-HDBK-338, MIL-HDBK-978, Rome Laboratory's "Reliability Engineer's Toolkit", Reliability Analysis Center (RAC) "Nonelectronic Parts Reliability Data" (NPRD) GIDEP (Government Industry Data Exchange Program) and RAC "Failure Mode/Mechanism Distribution" (FMD). While these documents provide a basis for failure rate prediction of some component types, there will be many device types that are not included in these documents. This is especially true for complex digital integrated circuits (ICs) which need to be considered in a part by part basis. Determining the failure modes of digital devices generally require engineering judgment and it is unlikely that all of the failure modes can be determined for a complex digital IC.

When performing an FTA as part of an SSA, the failure rates for the Basic Events may be obtained from the applicable FMEA/FMES if available. Reference to FMES may be explicitly made in each Basic Event for traceability purposes.

D.11.1.3 Determine the Exposure Times and At Risk Times of the Basic Events: The analyst must determine the Exposure Time or At Risk Time associated with each Basic Event in the fault tree. Some of the different types of basic events are listed below.

    a. Basic Event associated with loss or malfunction of a function of an item which is used throughout the entire flight.

    b. Basic Events associated with loss or malfunction of a function of an item only during particular phases of the flight.

    c. Basic Events associated with latent failure of an item that performs a function

    d. Basic Events associated with loss or malfunction of a protective element (e.g., fault monitors)

The paragraphs that follow describe how to determine the exposure times associated with each of these types of events.

D.11.1.3.1 Loss or Malfunction of a Function of an Item Used Throughout the Entire Flight: In this case, the item being analyzed is used throughout the entire flight. When the item fails or malfunctions, it results in the undesired failure effect. The At Risk Time for this case is equal to the estimated average flight duration.

D.11.1.3.2 Loss or Malfunction of a Function of an Item Used Only During a Particular Phase of a Flight: There are two main subcases associated with the loss or malfunction of an item which is used only during particular phases of flight. In the first subcase, the At Risk Time is equal to the time elapsed from the beginning of the flight to the end of the phase in question. For example, assume the event in question is "Gear Down" and the equipment item used to lower the gear is known to be operating properly via on-ground test. The At Risk Time for the equipment required to lower the landing gear is the time period from the ground test to the end of the "Gear Down" phase of the flight.

In the second subcase, the item is known to be working just prior to using it and is again only used during a particular phase of the flight. For this subcase, the At Risk Time, is equal to the time elapsed from the function checkout to the end of the phase in question. For example, assume the event in question is "Autoland" and the equipment item used to automatically land the plane is known to be operating properly via an initiated test run at mode engagement. The At Risk Time for this scenario is the time period from the initiated test to when the aircraft touches the ground.

D.11.1.3.3 Latent Failures: Latent failures disable protective mechanisms or reduce safety margins thereby increasing the risk of hazards due to subsequent conditions or failures. Latent failures, by themselves, do not constitute a hazard (i.e., by themselves they have no effect which would make them noticeable, otherwise they would not be latent, by definition). Usually latent failures affect only functions which are not relied upon in normal operation, but which provide fail-safe coverage and/or protection against abnormal conditions.

Latent failures can persist for a time interval which is either greater than or shorter than the flight time. This time interval is known as exposure time and is defined as the time between when an item was last known to be operating properly and when it will be known to be operating properly again. Proper operation may be verified during acceptance tests, maintenance checks, monitor cycle times, power-up tests, etc. The key to latent failure management is to detect and repair the applicable failed state quickly in order to reduce the exposure time.

In the case where a function is being monitored, the exposure time of the function is linked to the monitor exposure time.

D.11.1.3.4 Failure Detection Coverage and Exposure Times: Failure detection may be accomplished through dedicated hardware circuitry, software code, or various test methods. For the purposes of this section, these failure detection methods are referred to as monitors.

There are two subtle assumptions typically made when monitors are included in fault trees. They are:
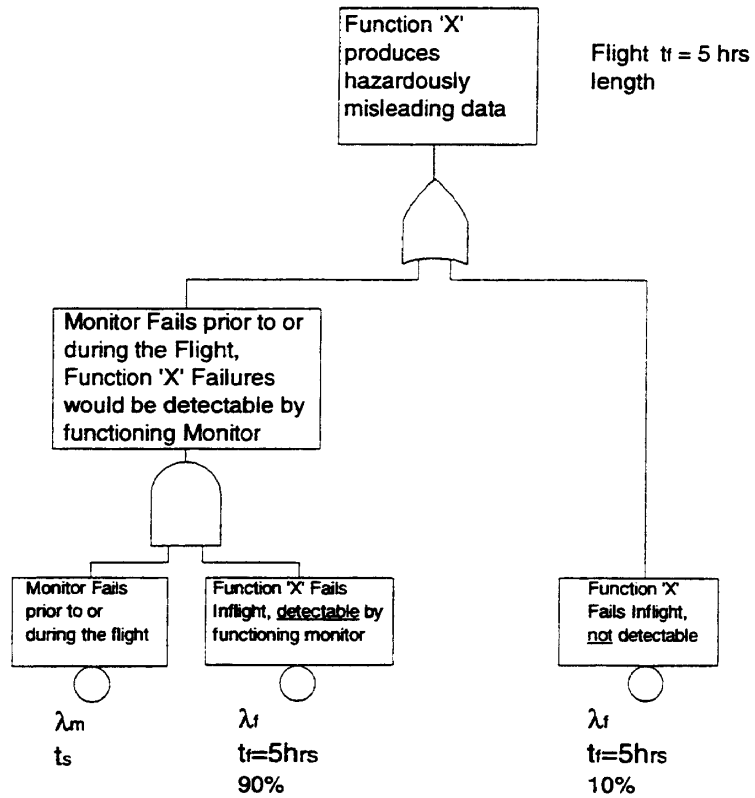
a. The monitor provides 100% failure detection coverage of the item performing the function, and

b. The monitor verification ("scrub") operation verifies that the monitor is fully operational (i.e., the "scrub" operation provides 100% coverage of the monitor).

Unfortunately, real life monitors may not provide 100% coverage. The analyst should consider fine tuning the FTA to account for imperfect coverage.

Figure D14 models a system where a monitor detects only 90% of Function "X" circuitry failures whenever the monitor is exercised. In this fault tree, 100% verification of monitor operation is achieved. The remaining 10% of Function "X" circuitry failures are not detected until a return to service test is performed on the item. This simplified tree provides a conservative result because the left branch of the tree does not consider required failure order between monitor and function failures in the same flight.

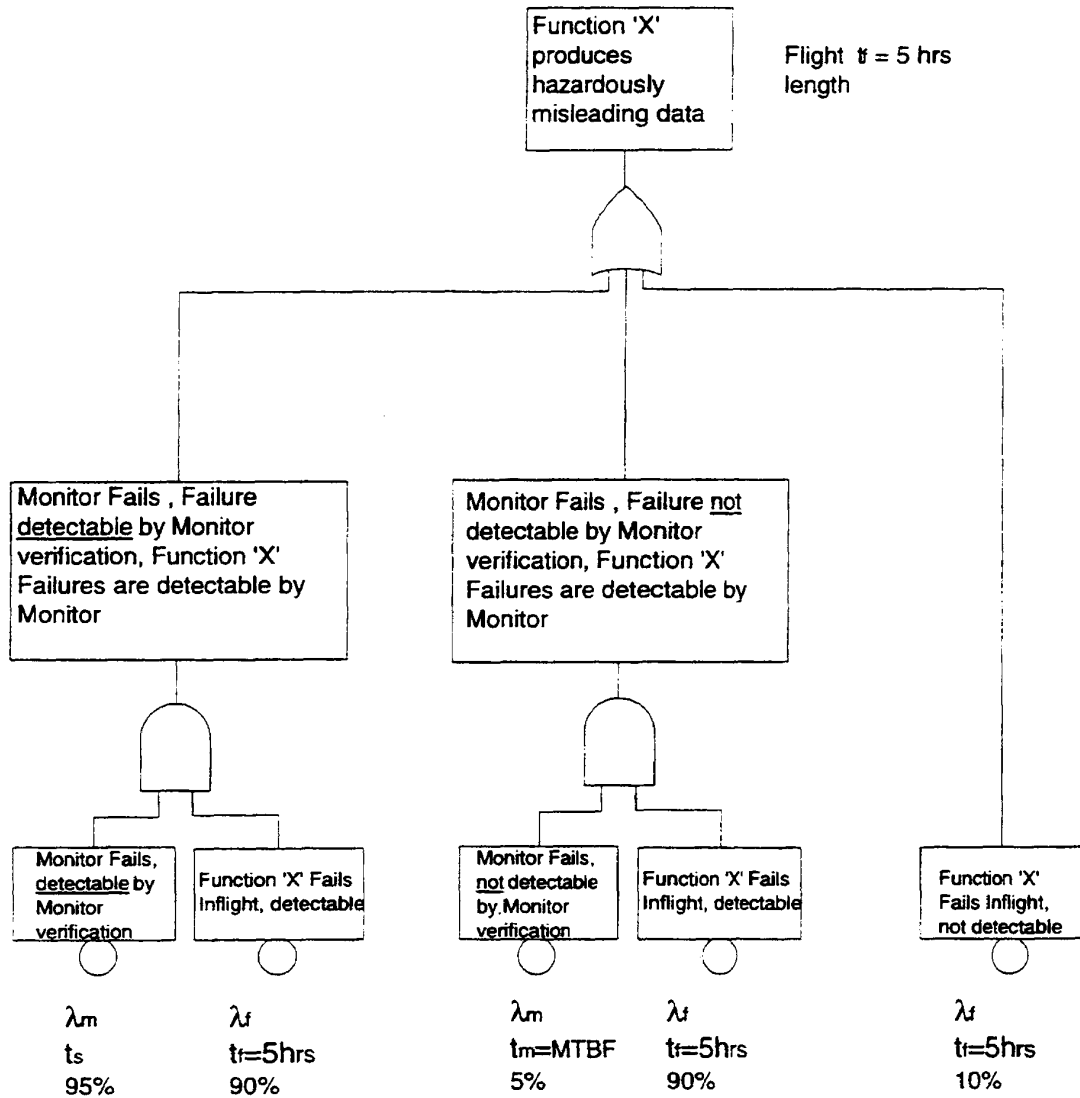Figure D15 models the above system when it is only possible to achieve 95% verification of monitor operation.

Function 'X'
produces
hazardously
misleading data

Flight tf = 5 hrs
length

Monitor Fails prior to or
during the Flight,
Function 'X' Failures
would be detectable by
functioning Monitor

Monitor Fails
prior to or
during the flight

Function 'X' Fails
Inflight, detectable by
functioning monitor

Function 'X'
Fails Inflight,
not detectable

λ_m
t_s

λ_f
t_f=5hrs
90%

λ_f
t_f=5hrs
10%

t_s= Monitor 'scrub' (verification) time

$P_f=0.9\lambda_m\lambda_f t_s t_f + 0.1\lambda_f t_f$

FIGURE D14 - An Example of a Fault Tree Structure When the Monitor
Detects 90% of Function 'X' Failures

Function 'X' produces hazardously misleading data

Flight tf = 5 hrs length

Monitor Fails , Failure detectable by Monitor verification, Function 'X' Failures are detectable by Monitor

Monitor Fails , Failure not detectable by Monitor verification, Function 'X' Failures are detectable by Monitor

Monitor Fails, detectable by Monitor verification

Function 'X' Fails Inflight, detectable

Monitor Fails, not detectable by Monitor verification

Function 'X' Fails Inflight, detectable

Function 'X' Fails Inflight, not detectable

λ_m
ts
95%

λ_f
tf=5hrs
90%

λ_m
tm=MTBF
5%

λ_f
tf=5hrs
90%

λ_f
tf=5hrs
10%

ts= Monitor 'scrub' (verification)

$P_{f\ flight}=0.9*0.95\lambda_m\lambda_f t_s t_f+0.9*0.05\lambda_m\lambda_f t_m t_f+0.1\lambda_f t_f$

$P_{f\ hour} = P_{f\ flight}/t_f$

FIGURE D15 - An Example of a Fault Tree Structure When the Monitor Detects 90% of Function 'X' Failures and the Monitor Verification is 95%

D.11.1.3.4 (Continued):

Many methods of failure detection may be required to effectively verify proper operation of a function, test, or monitor. Each of these detection layers may have different exposure times and must be accounted for accordingly. Some of the more common detection methods include the following.

a. Real time self test
b. Power up self test
c. Preflight self test
d. Scheduled maintenance testing
e. Initial production test
f. Return to service test

D.11.1.4 Establish any Relevant Required Order Factors: An AND-gate in a fault tree implies no specific order of the faults present. In some cases, this may be unrealistic. An example is a failure combination where a monitor is used to detect failures of functional circuitry that can cause the top level event. If the monitor fails first, the failure may remain latent until the monitor is next checked. If the function X circuitry fails first, the top level event does not occur because the monitor annunciates the failure.

When dealing with failure order dependent events, a factor may be incorporated into the fault tree to make the calculated probabilities less conservative. This factor is known as the Required Order Factor (ROF) or the Sequencing Factor. For small λt the probability of the two events occurring in either order (given that they both fail) is approximately 1/2 of the total probability and therefore the ROF for each order is 1/2. In general, if there are n events in an AND-gate there are n! possible orders in which they could fail. If only k of those possible orders lead to the top event, then ROF = k/n! This approximation is only valid for events with the same exposure time or events with different exposure times where $(\lambda_1 + \lambda_2)T_{(Max)}$ is less than 0.2. For all other cases, ROF should be calculated. An example using ROF is shown in Figure D10.

When a fault tree contains multiple ROFs, it is more accurate to apply the ROF to the minimal cut sets when performing probability calculations. An example is shown in Figure D16.

The ROF can only be applied when all inputs to the AND-gate have the same exposure time.
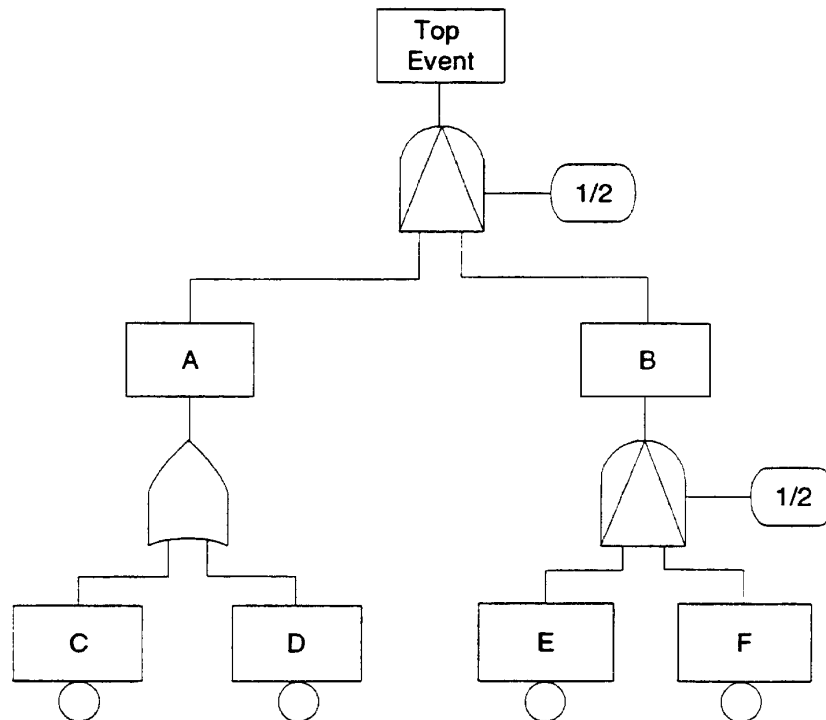
FIGURE D16 - An Example of a Fault Tree Structure Which Includes PRIORITY AND-Gates and ROF

D.11.1.4 (Continued):

From Figure D16, a minimal cut set would be $1/2(P_fC*1/2*P_fE*P_fF) = 1/4* P_fC*P_fE*P_fF$. This answer is incorrect as described in the next paragraph.

a. The analyst should generate the same cut set from Figure D16 ignoring the ROFs (i.e., $P_fC*P_fE*P_fF$). Next it is necessary to calculate k/n! by considering how many of the possible combinations would satisfy the required orders. There are 3! (i.e., six) possible orders which are CEF, CFE, ECF EFC FCE and FEC. The order CEF clearly satisfies the required order and ECF may also satisfy it. More knowledge of the actual system is required to establish this. Therefore, k could equal 1 or 2 and k/n! may equal 1/6 or 1/3. The complete and most correct mathematical solution for the probability of this cutset is therefore either $1/6 P_fC*P_fE*P_fF$ or $1/3 P_fC*P_fE*P_fF$. This illustrates that using the ROFs in the cutset analysis can be incorrect and can be either optimistic or pessimistic.

D.11.1.5 Perform the FTA Numerical Calculations: After the above steps are completed, the probability of failure for the top level event [P_f(top)] is calculated by performing the Boolean Algebra mathematics. The methods used for combining probabilities in AND-gates and OR-gates are described in 10.1.

When dealing with constant failure rates (i.e., the equipment is operating in the flat portions of the Reliability Bathtub Curve), the Basic Event Probability of Success (also referred to as Basic Event Reliability) is given by the following equation:

$$P_s = R = e^{-\lambda t} \qquad \text{(Eq. D1)}$$

where:

P_s = Probability of Success
R = Reliability
e = natural logarithm base
λ = Base Event failure rate
t = Base Event Exposure or "At Risk" Time

In reliability terms, we know component survival and component failure are complementary and mutually exclusive. Consequently, for any given time period:

$$P_s + P_f = R + Q = 1 \qquad \text{(Eq. D2)}$$

or

$$P_f = Q = 1 - e^{-\lambda t} \qquad \text{(Eq. D3)}$$

where:

P_f = Probability of Failure
Q = Unreliability

When $\lambda t \leq 0.1$, Equation D3 can be simplified to $P_f = Q = \lambda t$.

The FTA numerical calculations should be performed using P_f because the electronic based systems of today have such high reliability (R = 0.9999....) that Q is less sensitive to round-off errors and thus produces a more accurate P_f(top). In other words, FTA numerical calculations should deal with the Probability of Failure terms instead of Probability of Success terms.

D.11.1.5 (Continued):

The case in which two latent failures cause system failure is approximately correct providing $n\lambda t_f$ is small for both failure mechanisms, but is inaccurate if $n\lambda t_f$ is large. The reason is that if both components in a dual component system fail latent, then the failure must be manifest. Therefore, there is an implicit assumption that both components have not failed at the beginning of the mission. Since this case is not included in the calculations, the result may be higher than necessary when $n\lambda t_f$ is large (n is the number of missions between maintenance periods). A correct mathematical result can be obtained by the use of Boolean manipulation or Markov Analysis.

In D.11.1.5.1 through D.11.1.5.4, the four particular examples in D.9.3 are developed further to show typical fault tree calculations which include basic events with or without latency and required order factors. The methodology presented here shows the probability for the worst case flight as well as the average probability per flight of the top event, for double failures. Different methods could be applied to calculate the average probability per flight in cases where the problem is straightforward. Distinct formulas would need to be developed to deal with more than two failures or where some of the above described assumptions are not valid. To calculate the probability per flight hour, refer to Section D.13. A conservative analysis using the worst case flight probabilities may be submitted to show compliance without the complication of computing the average probability. Caution is required with the use of fault tree software packages which may automatically select either worst case or average probabilities.

D.11.1.5.1 Fault Tree Calculation When Two Item Failures Cause a Loss of a Function and Neither Item Failure is Latent: This is the simple failure case where the top event is caused by the loss of both items during the same flight. Both items are known to be operating at the start of the flight and neither fail latent. Since neither failure is latent, the average and worst case probabilities are identical. The two failures can occur in either order. An example is shown in Figure D17.

Loss of Function
'A' Inflight

Item #1 Fails

Item #2 Fails

λ_1
t_f=5hrs

λ_2
t_f=5hrs

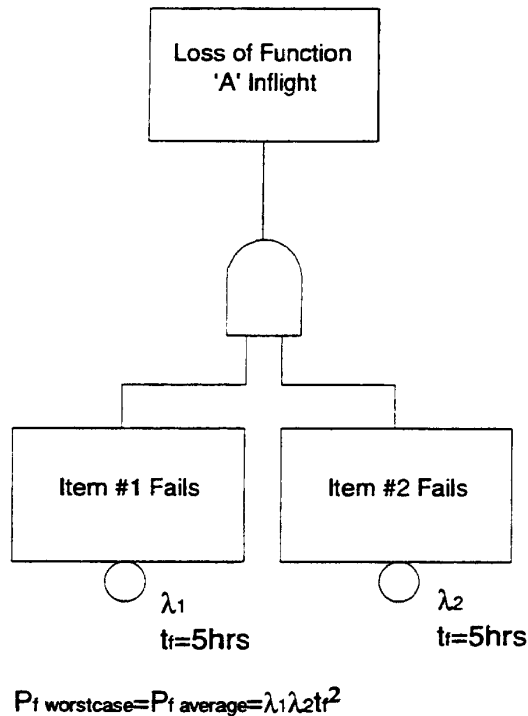P_f worstcase=P_f average=$\lambda_1\lambda_2 t_f^2$

FIGURE D17 - An Example of a Fault Tree Calculation When Two Item
Failures Cause a Loss of a Function

D.11.1.5.2 Fault Tree Calculation When Two Items Cause a Loss of a Function and One of the Items
Can Fail Latent but the Other Cannot Fail Latent, No Sequencing: In this case, Item 1 can
fail at any point between when it is checked (time = zero) and when it is next checked (time
= T). Item 2 is known to be operating at the start of each flight and never fails latent. The
order of failure does not matter. In this case there is a difference between the average
probability of the top event per flight and the probability of the top event for the worst case
flight. Consider that there are n flights of t_f hours, i.e., $T = nt_f$.

Using the approximation of $P_f = \lambda t$ for small λt, gives the following which is shown pictorially
in Table D5.

a. Probability of both failures occurring in the first flight after the inspection check = $\lambda_1\lambda_2 t_f^2$.

b. Probability of item one failing in either of the first two flights after the inspection check
and item two failing in the second flight = $2\lambda_1\lambda_2 t_f^2$.

c. Probability of item one failing in any of the first i flights and item two failing in the ith flight
= $i\lambda_1\lambda_2 t_f^2$.

TABLE D5 - Pictorial Representation of Average Probability Calculation for a
Two Failure Case - One Latent and One Active

Case #	Current Flight	A Non-Latent Failure on Current Flight And a Latent Failure On 1st Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure On 2nd Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure On ith Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure On Next to Last Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure On Last Flt of Latency Period	Total Probability for This Case
1	1st Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$					$\lambda_1 \lambda_2 t_f^2$
2	2nd Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$				$2\lambda_1 \lambda_2 t_f^2$
i.	ith Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$			$i\lambda_1 \lambda_2 t_f^2$
n-1	Next to Last Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$		$(n-1)\lambda_1 \lambda_2 t_f^2$
n	Last Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$n\lambda_1 \lambda_2 t_f^2$

D.11.1.5.2 (Continued):

    d. Probability of item one failing in any of n flights and item two failing in the final (nth) flight $= n\lambda_1\lambda_2 t_f^2$. (This is the probability for the worst case flight.)

    e. The average probability per flight equals the sum of the probabilities for each flight, divided by n, the number of flights in the latency period.

$$
\begin{aligned}
P_{f\ Average} &= 1/n * \Sigma i\lambda_1\lambda_2 t_f^2 \text{ for } i = 1 \text{ to } n \qquad\text{(Eq. D4)}\\
&= (\lambda_1\lambda_2 t_f^2)/n * \Sigma i \text{ for } i = 1 \text{ to } n\\
&= (\lambda_1\lambda_2 t_f^2)/n * (n * (n+1))/2\\
&= \tfrac{1}{2} * \lambda_1\lambda_2 t_f(nt_f + t_f)\\
&= \tfrac{1}{2} * \lambda_1\lambda_2 t_f(T + t_f)
\end{aligned}
$$

D.11.1.5.2 (Continued):

The factor of ½ appears as a result of calculating the average probability that the function will fail on any single flight within the latency period and not from using a mean exposure time of T/2.
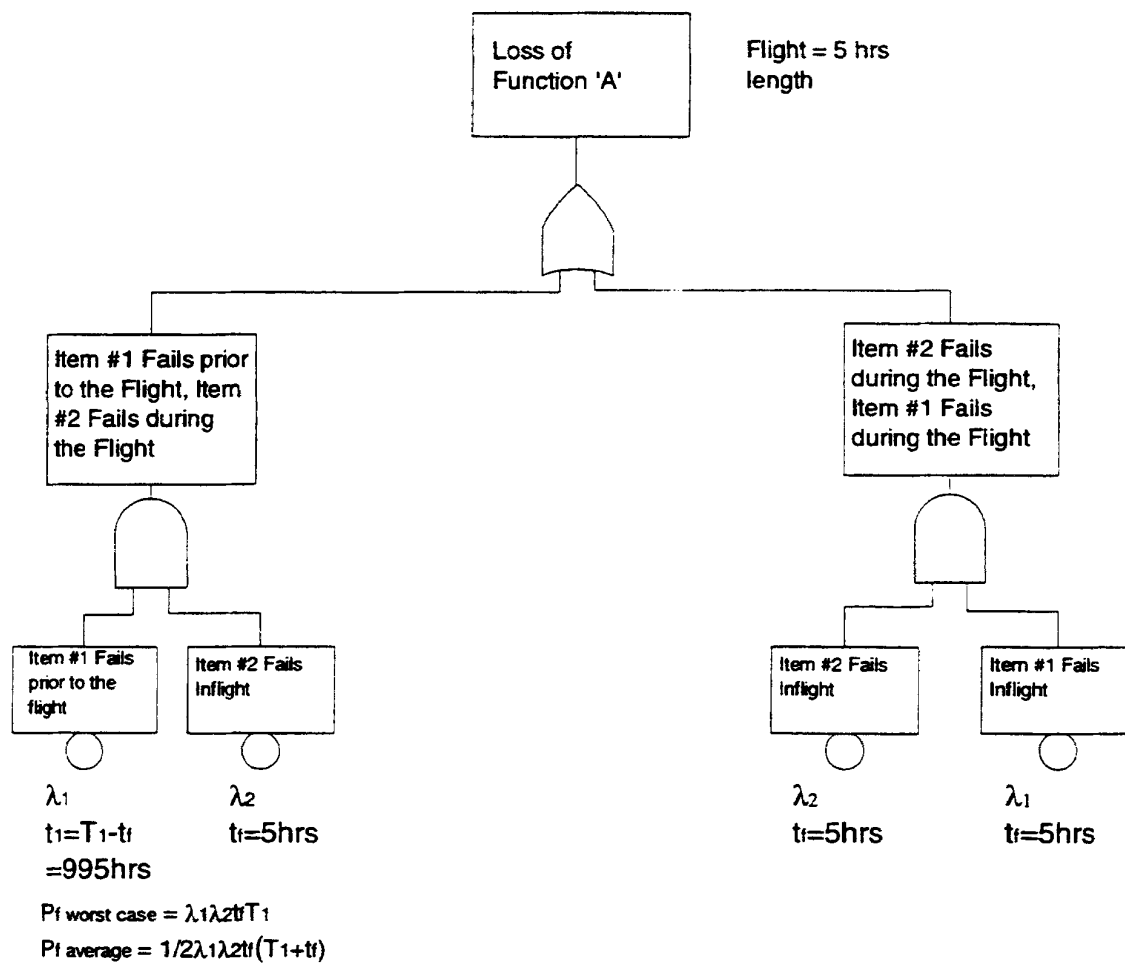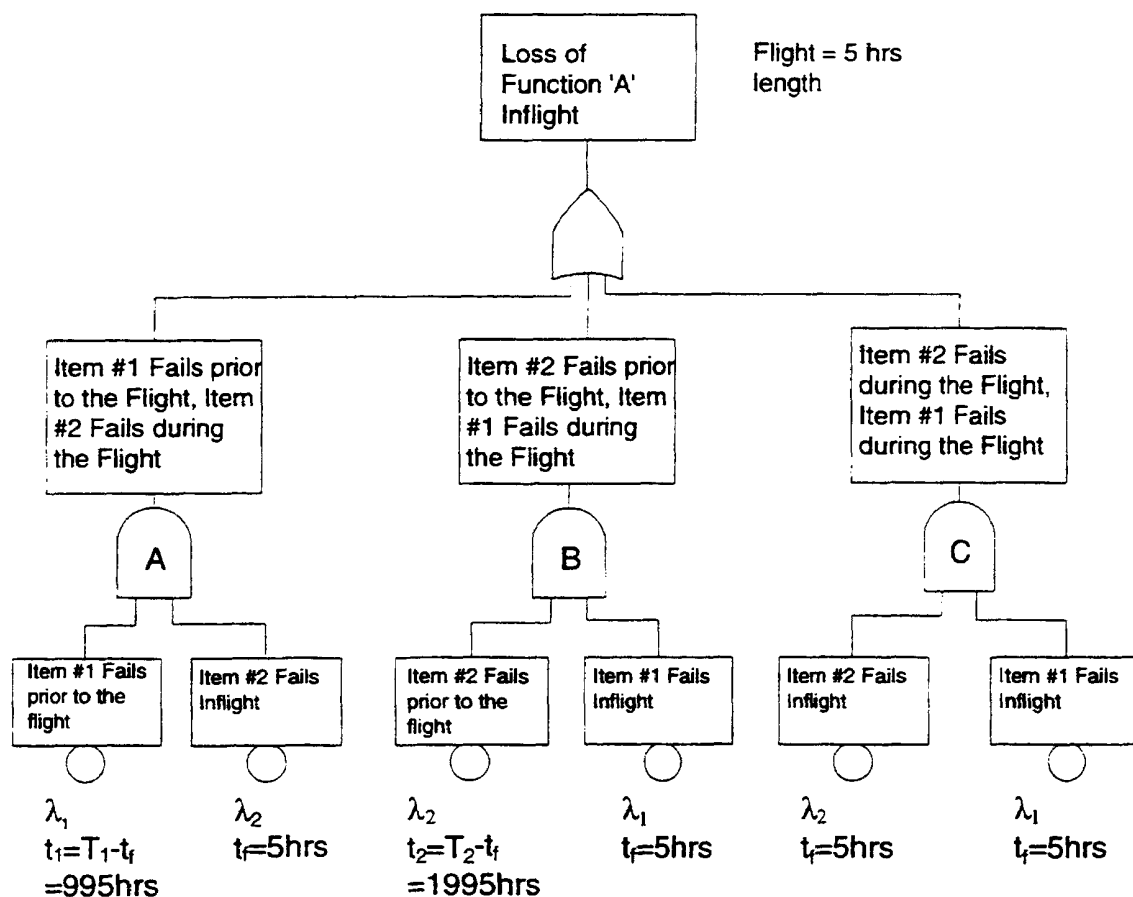
An example is shown in Figure D18.

Pf worst case $= \lambda_1\lambda_2 t_f T_1$

Pf average $= 1/2\lambda_1\lambda_2 t_f (T_1+t_f)$

FIGURE D18 - An Example of a Fault Tree Calculation When Two Item Failures
Cause a Loss of a Function Where Item #1 Could Fail Latent

D.11.1.5.3 Fault Tree Calculation When Two Items Cause a Loss of a Function and Each Item Could Fail Latent - No Sequencing: In this case, either item could fail latent, but if both fail, this would be detected by virtue of it causing the top event. Therefore at least one of the items must be operating at the start of each flight. An example is shown in Figure D19.

Loss of Function 'A' Inflight

Flight = 5 hrs length

Item #1 Fails prior to the Flight, Item #2 Fails during the Flight

A

Item #2 Fails prior to the Flight, Item #1 Fails during the Flight

B

Item #2 Fails during the Flight, Item #1 Fails during the Flight

C

Item #1 Fails prior to the flight

λ_1
$t_1 = T_1 - t_f$
$= 995$hrs

Item #2 Fails Inflight

λ_2
$t_f = 5$hrs

Item #2 Fails prior to the flight

λ_2
$t_2 = T_2 - t_f$
$= 1995$hrs

Item #1 Fails Inflight

λ_1
$t_f = 5$hrs

Item #2 Fails Inflight

λ_2
$t_f = 5$hrs

Item #1 Fails Inflight

λ_1
$t_f = 5$hrs

Pf worst case $= \lambda_1 \lambda_2 t_f (T1 + T2 - t_f)$
Pf average $= 1/2 \lambda_1 \lambda_2 t_f (T1 + T2)$

FIGURE D19 - An Example of a Fault Tree Calculation When Two Item Failures Cause a Loss of a Function Where each Item Could Fail Latent

D.11.1.5.3 (Continued):

       Three things should be noted about Figure D19. First, an undeveloped event for failure order (i.e., ROF = k/n! as described in D.11.1.4) is not required because failure order dependence is built into the tree structure via the latency period ($t_n = T_n - t_f$), which is representative for a failure before the flight. Second, the rightmost AND-gate is necessary to cover the case that both items fail during the flight without a required sequence. Third, the rightmost AND-gate is often omitted and the exposure times set equal to the inspection intervals, for the case where t_f is much less than the inspection intervals.

    a. The probability of the worst case flight is calculated as below, with reference to Figure D19:

$$P_f A = \lambda_1(T_1-t_f) \lambda_2 t_f \quad \text{(Eq. D5)}$$
$$P_f B = \lambda_2(T_2-t_f) \lambda_1 t_f \quad \text{(Eq. D6)}$$
$$P_f C = \lambda_1 t_f \lambda_2 t_f \quad \text{(Eq. D7)}$$

$$P_{f\text{worst case}} = P_f A + P_f B + P_f C \quad \text{(Eq. D8)}$$
$$= \lambda_1 \lambda_2 t_f(T_1-t_f + T_2 - t_f + t_f)$$
$$= \lambda_1 \lambda_2 t_f(T_1 + T_2 - t_f)$$

    b. For the average probability calculation as described in D.11.1.5.5, the result is:

$$P_{f\text{ average}} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f(T_1 + T_2) \quad \text{(Eq. D9)}$$

D.11.1.5.4 Fault Tree Calculation When the Failure of Both Items Cause a Top Event and One can Fail Latent and a Required Order is Needed: In this case, item one (the latent one) must fail prior to item two or the top event does not result. Item two is known to be operational at the start of the flight. This is typical of a failure/monitor situation where the top event is an erroneous output rather than a loss of function. An example involving the transmission of incorrect data is provided in Figure D20.

       The required order factor (ROF) is used per D.11.1.4.

    a. The probability of the worst case flight is calculated as below with reference to Figure D20:

$$P_f A = \lambda_1(T_1-t_f)\lambda_2 t_f \quad \text{(Eq. D10)}$$
$$P_f B = 1/2\lambda_1 \lambda_2 t_f^2 \quad \text{(Eq. D11)}$$

$$P_{f\text{worst case}} = P_f A + P_f B \quad \text{(Eq. D12)}$$
$$= \lambda_1(T_1-t_f)\lambda_2 t_f + (\lambda_1 \lambda_2 t_f^2)/2$$
$$= \lambda_1 \lambda_2 t_f(T_1-t_f/2)$$

    b. For the average probability calculation, as described in D.11.1.5.5, the result is:

$$P_{f\text{average}} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f T_1 \quad \text{(Eq. D13)}$$

Loss of
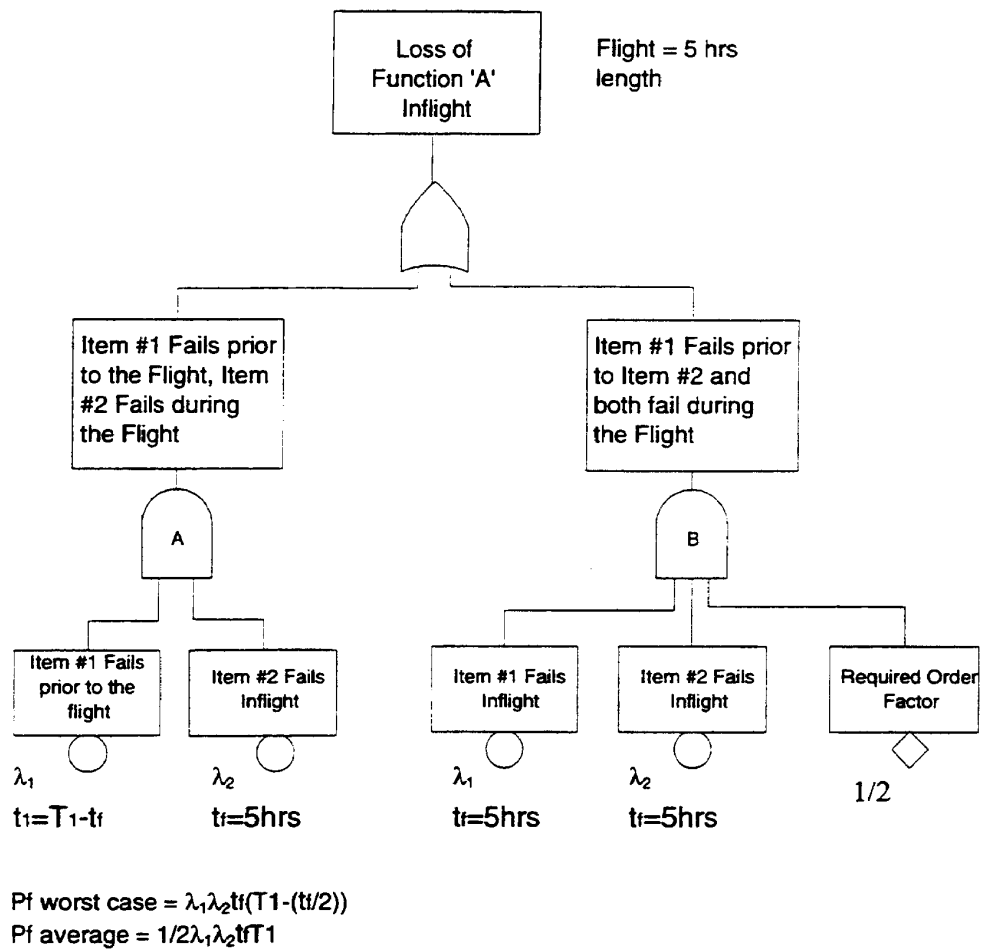Function 'A'
Inflight

Flight = 5 hrs
length

Item #1 Fails prior
to the Flight, Item
#2 Fails during
the Flight

Item #1 Fails prior
to Item #2 and
both fail during
the Flight

A

B

Item #1 Fails
prior to the
flight

Item #2 Fails
Inflight

Item #1 Fails
Inflight

Item #2 Fails
Inflight

Required Order
Factor

λ_1

$t_1 = T_1 - t_f$

λ_2

$t_f = 5hrs$

λ_1

$t_f = 5hrs$

λ_2

$t_f = 5hrs$

$1/2$

Pf worst case = $\lambda_1 \lambda_2 t_f (T_1 - (t_f/2))$
Pf average = $1/2 \lambda_1 \lambda_2 t_f T_1$

FIGURE D20 - An Example of a Fault Tree Calculation When Two Item Failures Cause
a Top Event and One Item Can Fail Latent and Failures are Order Dependent

D.11.1.5.5 Examples of Calculation of the Average Occurrence Probability of a Double Failure for an Average Flight Time: The following example considers the general case of a double failure F_1 and F_2 with two different failure rates, λ_1 and λ_2, and two latencies, T_1 and T_2, with the assumptions:

$$T_1 \leq T_2, T_2 = NT_1 \text{ and } t_f \text{ is the average flight time} \qquad \text{(Eq. D14)}$$

We have:
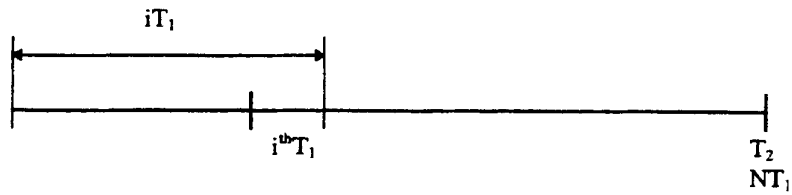
FIGURE 21

D.11.1.5.5.1 Probability of Occurrence for the ith T_1: This probability is composed of two cases, Case A and Case B.

    a. Case A: F_2 occurs before F_1

        (1) This case is composed of two subcases:

            (a) A1: F_2 occurs before the ith T_1 and F_1 occurs during T_1
            (b) A2: F_2 occurs before F_1 during the ith T_1

$$P_A = P_{A1} + P_{A2} = \lambda_2(i-1)T_1\lambda_1T_1 + (\lambda_1T_1\lambda_2T_1/2) \qquad \text{(Eq. D15)}$$
$$(\text{note: } /2 \text{ term for sequencing } F_2 \text{ before } F_1 \text{ during } T_1.)$$

$$P_A = \lambda_1\lambda_2T_1{}^2(i-1+1/2) = \lambda_1\lambda_2T_1{}^2(i-1/2)$$

    b. Case B: F_1 occurs before F_2

        (1) In this case the latency of F_1 is T_1, and the double failure occurs if F_1 occurs before F_2 during T_1.

$$P_B = (\lambda_1T_1\lambda_2T_1)/2 \qquad \text{(Eq. D16)}$$
$$(\text{note: } /2 \text{ term for sequencing } (F_1 \text{ before } F_2) \text{ during } T_1.)$$

The total probability of occurrence for the ith T_1 is:

$$P = P_A + P_B = \lambda_1\lambda_2T_1{}^2[(i-1/2) + 1/2] = \lambda_1\lambda_2T_1{}^2i \qquad \text{(Eq. D17)}$$

D.11.1.5.5.2 Probability of Occurrence for the T_2 Periods: The global occurrence probability for the T_2 period is:

$$P_G = \Sigma (P_A + P_B); \text{ for } i = 0 \text{ to } i = N \qquad \text{(Eq. D18)}$$

$$P_G = \lambda_1 \lambda_2 T_1^2 [(N(N+1)/2 - N/2) + (N/2)]$$

$$P_G = \lambda_1 \lambda_2 T_1^2 [(N^2/2 + N/2 - N/2) + N/2]$$

$$P_G = \lambda_1 \lambda_2 T_1^2 [N^2/2 + N/2)$$

$$\text{Replaces } NT_1 \text{ by } T_2$$

$$P_G = \tfrac{1}{2}\lambda_1 \lambda_2 T_2 (T_1 + T_2)$$

D.11.1.5.5.3 Probability of Occurrence Per Flight: P_G is the average occurrence probability for a period of T_2 hours. To have the average occurrence probability per flight, it is necessary to divide P_G by T_2 to have the average occurrence probability per hour of flight and to multiply by t_f, which is the average time of a flight.

This results in the general formula:

$$P_{ft} = P_G * t_f/T_2 \qquad \text{(Eq. D19)}$$

$$P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f (T_1 + T_2)$$

Where P_{ft} = probability per flight of the double failure

D.11.1.5.5.4 Derivation of Current Cases: From the P_{ft} general formula from D.11.1.5.5.3 above, one can derive several current cases of double failures:

a. Two latent failures, F_1 and F_2, with two different latency periods, T_1 and T_2.

$$\text{No sequence: } P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f (T_2 + T_1) \qquad \text{(Eq. D20)}$$

$$\text{Sequence } F_2 \text{ before } F_1: P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f T_2$$

$$\text{Sequence } F_1 \text{ before } F_2: P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f T_1$$

b. Two latent failures, F_1 and F_2, with the same latency periods, $T_1 = T_2 = T$.

$$\text{No sequence: } P_{ft} = \lambda_1 \lambda_2 t_f [(T + T)/2] = \lambda_1 \lambda_2 t_f T \qquad \text{(Eq. D21)}$$

$$\text{Sequence } F_2 \text{ before } F_1: P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f T$$

$$\text{Sequence } F_1 \text{ before } F_2: P_{ft} = \tfrac{1}{2}\lambda_1 \lambda_2 t_f T$$

D.11.1.5.5.4 (Continued):

   c. One latent failure, F_2 and one active failure, F_1, with latency periods, $T_2 = T$ and $T_1 = t_f$

$$\text{No sequence: } P_{ft} = \tfrac{1}{2}\lambda_1\lambda_2 t_f(T + t_f) \qquad \text{(Eq. D22)}$$

Sequence F_2 before F_1: $P_{ft} = \tfrac{1}{2}\lambda_1\lambda_2 t_f T$
(case of command and monitoring system)

Sequence F_1 before F_2: $P_{ft} = \tfrac{1}{2}\lambda_1\lambda_2 t_f t_f = \tfrac{1}{2}\lambda_1\lambda_2 t_f^2$

   d. Two active failures, F_1 and F_2, $T_1 = T_2 = t_f$

$$\text{No sequence: } P_{ft} = \lambda_1\lambda_2 t_f[(t_f + t_f)\,/2] = \lambda_1\lambda_2 t_f^2 \qquad \text{(Eq. D23)}$$

Sequence F_2 before F_1: $P_{ft} = \tfrac{1}{2}\lambda_1\lambda_2 t_f t_f = \tfrac{1}{2}\lambda_1\lambda_2 t_f^2$

Sequence F_1 before F_2: $P_{ft} = \tfrac{1}{2}\lambda_1\lambda_2 t_f t_f = \tfrac{1}{2}\lambda_1\lambda_2 t_f^2$

D.11.2 Quantitative Sensitivity Evaluation:

Sensitivity evaluations can be broken into two categories (refer to NUREG-0492 for a detailed discussion of this subject).

   a. Variations of models or data
   b. Formal error analysis

The analyst can use data or fault tree model variations to determine how sensitive a system design is to a particular aspect of individual Primary Events. By inserting different failure rates in a particular Primary Event, the analyst can decide whether a higher reliability item/component is worth the additional cost. By inserting different exposure times, the analyst provides input to help establish equipment maintenance intervals.

The analyst can use formal error analysis to determine how sensitive the FTA result is to Primary Event variability, i.e., variability in component failure rates and maintenance intervals. The Monte Carlo method is one such technique which is adaptable to fault tree analysis. Since error analyses are based on statistical and probabilistic techniques which are beyond the scope of this appendix, the reader should refer to textbooks on this subject matter.

Quantitative Importance is similar to Qualitative Importance (see D.10.2) in that both evaluation methods simply rank the cut sets for determining their relative importance with respect to top level event occurrence.

Quantitative Importance can take various forms. Several methods are provided here. The analyst receives a different type of information from each method.

D.11.2 (Continued):

Method #1: A simple ranking of cut sets in descending order based on each cut sets actual probability of failure (i.e., highest to lowest P_f).

This method is closely related to qualitative importance. The analyst can accurately determine cut set ranking as opposed to only being able to get a gross estimate of cut set ranking using the qualitative importance method.

Method #2: ith Cut Set Importance -- provides a percentage of cut set failure probability with respect to the top level event failure probability.

$$\%(i) = \frac{P_f(i)}{P_f(top)} \qquad \text{(Eq. D24)}$$

Method #3: Fussell-Vesley (FV) Importance -- provides the risk associated with an individual Primary Event (i.e., provides a relative indication on how much a Primary Event is contributing to the top level event P_f).

$$FV = \frac{P_f(top) - P_f(top/A = 0)}{P_f(top)} \qquad \text{(Eq. D25)}$$

where P_f (top/A=0) is defined as the probability that the top event occurs given event A never occurs; i.e., P_f (A) = 0.

Method #4: Birnbaum Importance -- provides the increase in risk associated with a Primary Event. That is, this method provides the difference in top level event P_f when a Primary Event occurs (i.e., P(A) = 1) and when a Primary Event does not occur (i.e., P(A) = 0).

$$Birnbaum = P_f(top/A = 1) - P_f(top/A = 0) \qquad \text{(Eq. D26)}$$

D.12 USING FAULT TREES TO SHOW CONTRIBUTION OF ERRORS:

Fault trees can provide a means to illustrate the contribution of potential hardware and software errors to the undesired events being analyzed. This is accomplished by including hardware and software error events in the fault tree. These events are included in a purely qualitative manner and do not enter into the calculation of the probability for the top level event which can only be performed for hardware failures.

By including potential hardware and software errors in the fault tree, the analyst can assess the development assurance necessary to ensure that common mode errors cannot degrade the safety level achieved by protecting against random hardware faults.

D.12 (Continued):

The following example shows how including potential hardware and software errors in a fault tree can guide the analyst in assessing the development assurance that must be achieved.

The example is shown for two identical displays. For simplicity, the source of data to the displays is excluded from the analysis and it is assumed that the monitoring is contained within each display. The initial fault tree is shown in Figure D22. In this initial fault tree, it is assumed that all hardware failures are independent. Compliance with a 1E-9 safety level appears to be quite easily achieved because four independent hardware failures must occur.
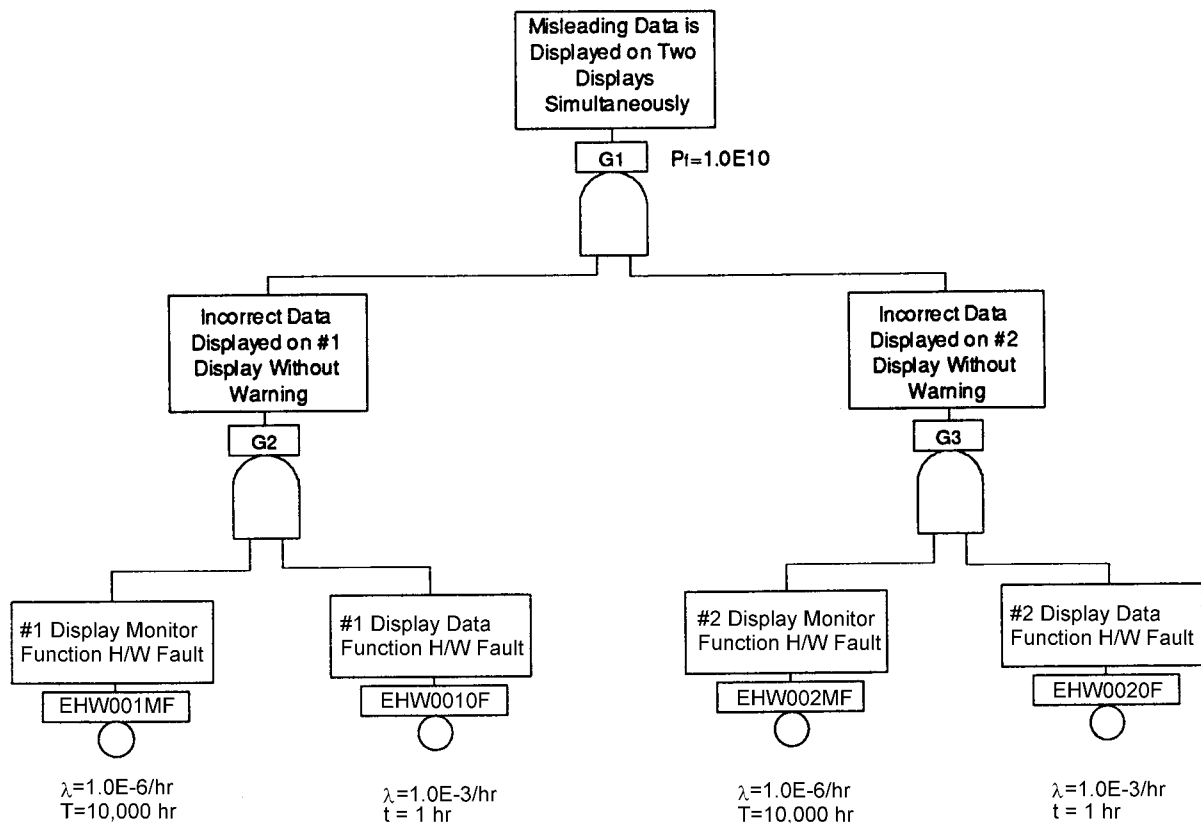
FIGURE D22 - Example Fault Tree, Working Basis for Incorporation of Design Errors

D.12 (Continued):

The analyst can easily determine that the minimal cutset for the tree is (EHW0010F)(EHW001MF)(EHW0020F)(EHW002MF). Now the analyst must determine if common cause faults can affect the calculations performed on the cutset. The fault trees (Figure D23 pages 1-4) on the following pages add the potential common cause faults to provide visibility to their possible effects. The potential common cause faults shown are: "EXTERNAL COMMON CAUSE FAULTS (POWER, ENVIRONMENT, ETC.)", "CONTRIBUTION OF ERRORS IF DATA AND MONITOR ARE INDEPENDENT", and "CONTRIBUTION OF H/W AND S/W ERRORS IF DATA AND MONITOR ARE NOT INDEPENDENT". The external common cause faults are included for completeness but will not be addressed further here.

Because the displays are identical, the worst case assumption is made that a software or hardware error will affect both of them simultaneously. Within each display, there are two functions under analysis, the data generation function and monitor function. If the data generation design and the monitor design are independent, the fault sequences shown under the event, "CONTRIBUTION OF ERRORS IF DATA AND MONITOR ARE INDEPENDENT" guide the assignment of the development assurance of the software and hardware that perform these functions. In this case, combinations of hardware and software errors and random hardware faults play a role in causing the top level event.

If the data generation and monitor functions are not designed to be independent, then the fault sequence shown under the event, "CONTRIBUTION OF ERRORS IF DATA AND MONITOR ARE NOT INDEPENDENT" guides the assignment of the necessary development assurance. If the functions are not independent, hardware and software errors are the major contributor to the top level event.

The analyst can now look at 5.4 of ARP4754 for guidance on the Development Assurance Levels that need to be assigned for the alternate potential designs. If the data and monitor functions are not independent, the hardware and software involved in both of these functions will need to be developed to Level A. If the functions are independent, it may be possible to reduce the level of one or both of the functions.

Including the potential of hardware and software errors into the fault tree provides valuable insight into the questions that need to be asked regarding independence and ultimate, when those questions are answered, insight into the development assurance that must be applied.
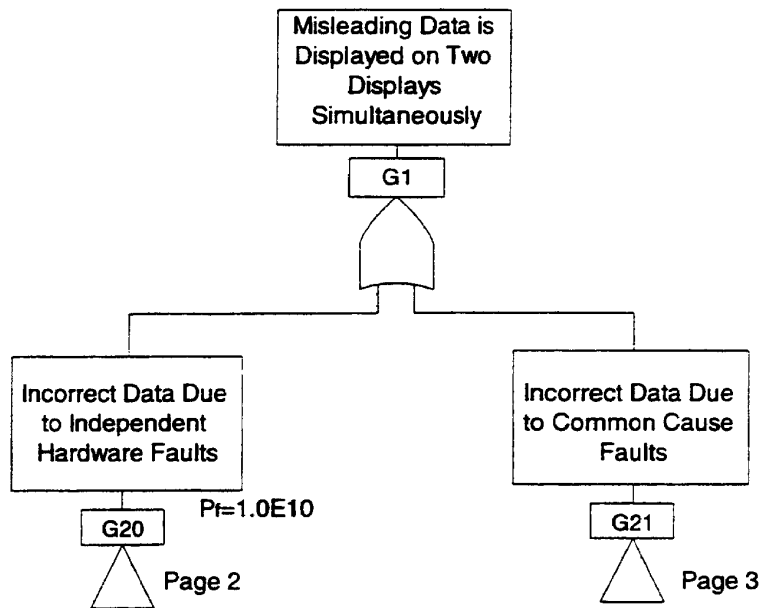
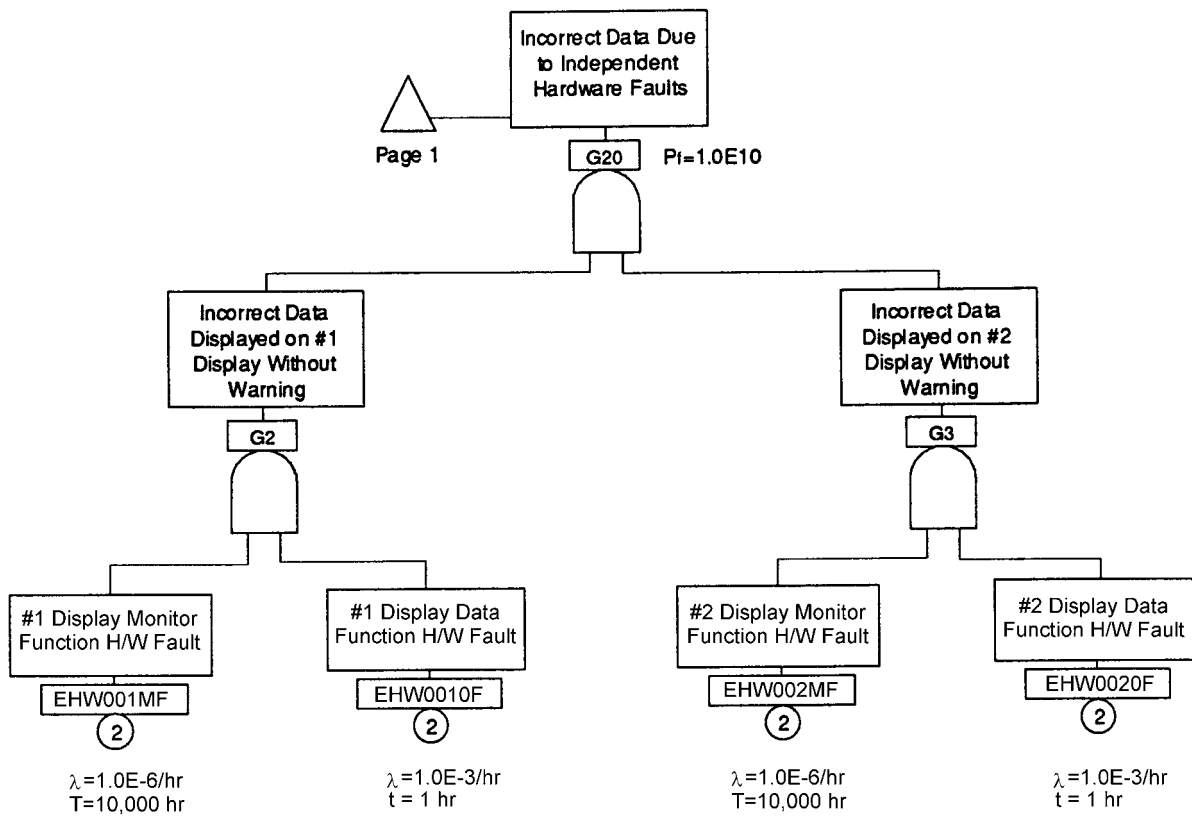FIGURE D23 - Consideration of Common Cause Faults (Error) - (Pages 1 of 4)

Incorrect Data Due to Independent Hardware Faults

Page 1

G20 Pf=1.0E10

Incorrect Data Displayed on #1 Display Without Warning

G2

Incorrect Data Displayed on #2 Display Without Warning

G3

#1 Display Monitor Function H/W Fault

EHW001MF

②

λ=1.0E-6/hr
T=10,000 hr

#1 Display Data Function H/W Fault

EHW0010F

②

λ=1.0E-3/hr
t = 1 hr

#2 Display Monitor Function H/W Fault

EHW002MF

②

λ=1.0E-6/hr
T=10,000 hr

#2 Display Data Function H/W Fault

EHW0020F

②

λ=1.0E-3/hr
t = 1 hr

FIGURE D23 (Continued) - (Page 2 of 4)

Page 1 — Incorrect Data Due to Common Cause Faults — G21

Contribution of Errors if Data and Monitor are Independent — G25

External Common Cause Faults (Power, Environment, etc)

Contribution of Errors if Data and Monitor are Not Independent — G24

Errors Cause Misleading Data - Data an Monitor are Independent — G9

Combination of H/W Faults and Errors Cause Misleading Data Display — G10 — Page 4

Hardware Error

Software Error

Data Errors — G11

Monitor Errors — G12

Data Function H/W Error — EHW1620E — (2)

Data Function S/W Error — ESW1620E — (2)

Monitor Function H/W Error — EHW0020F — (2)

Monitor Function S/W Error — EHW0020F — (2)

FIGURE D23 (Continued) - (Pages 3 of 4)

Combination of H/W Faults and Errors Cause Misleading Data Display — G10

Page 3

Data H/W Faults and Monitor Errors — G13

Monitor H/W Faults and Data Errors — G14

Data H/W Fault in #1 and #2 Displays — G15

Monitor Errors — G16

Monitor H/W Fault in #1 and #2 Displays — G17

Data Errors — G18

#1 Display Data Function H/W fault — EHW0010F (2)

#2 Display Data Function H/W fault — EHW0020F (2)

#1 Display Monitor Function H/W fault — EHW001MF (2)

#2 Display Monitor Function H/W fault — EHW002MF (2)

Monitor Function H/W Error — EHW162ME (2)

Monitor Function S/W Error — ESW162ME (2)

Data Function H/W Error — EHW162DE (2)

Data Function S/W Error — ESW162DE (2)

FIGURE D23 (Continued) - (Page 4 of 4)

D.13 ANALYZE AND SUMMARIZE THE FTA RESULTS:

After the tree is constructed, the analyst will need to normalize and then summarize the fault tree data, and document whether the current architecture is adequate to meet the top level event requirement.

D.13.1 Fault Tree Data Analysis -- Normalizing the FTA Numerical Calculation:

The certificate authority states its safety requirements in terms of "Probability of Failure per Flight Hour". If the system under analysis has these types of requirements, the analyst must "normalize" the undesired top event Probability of Failure number.

When P_f(top) is calculated on a per flight basis, the analyst normalizes P_f(top) by dividing the top event probability by the flight time, or other appropriate time and thus reports the Probability of Failure per flight hour.

D.13.2 Summarizing Fault Tree Analysis Results During SSA Process:

One method for summarizing the FTA data is to construct an FTA Data Summary Chart. This chart uses a columnar format which provides an engineering management or a certification authority reviewer with easy access to all the pertinent FTA results. The following table contains an example of this type of chart.

TABLE D6 - Example of a System Indenture Level FTA Data Summary Chart

Safety Design Criteria	Safety Design Criteria	Safety Design Criteria	Analysis Results	Analysis Results	Analysis Results
List of Top Level Events (from FHA)	List of Top Level Events (from FHA)	Corresponding Maximum Allowable Probability	System's Probability of Occurrence	Compliance (Yes or No)	Corrective Action
Funct #	Description				
4A1	Loss of all Altitude Display in the cockpit	1E-9	5E-9	No	Redesign Air Data System or add more detail to the LRU FTA
4A2	Loss of primary altitude on both pilot PFDs	1E-7	1E-7	Yes	None
.		.	.		
.		.	.		
.		.	.		

Note that the numbers entered into the "Corresponding Maximum Allowable Probability" column are based on the Failure Condition Classification for the given top level event.

Now we can see the tie between FTA boundaries and summarizing FTA results. Table D6 indicates that Function #4A1 does not meet its top level event safety requirement at the system indenture level and the apparent corrective action is to increase the FTA scope by enlarging the FTA boundaries down to the LRU indenture level. Assuming that Function #4A1B55 is the Primary Event in the Function #4A1 system indenture level FTA, Table D7 provides an example of a summary table for an LRU indenture level FTA.

TABLE D7 - Example of an LRU Indenture Level FTA Data Summary Chart

Safety Design Criteria	Safety Design Critiera	Safety Design Criteria	Analysis Results	Analysis Results	Analysis Results
List of Top Level Events (from System FTA)	List of Top Level Events (from System FTA)	Corresponding Maximum Allowable Probability	System's Probability of Occurrence	Compliance (Yes or No)	Corrective Action LRU Functional Block FTA or HW/SW Change
Funct #	Description				
4A1B55		1.0E-9	1.0E-8	No	Perform LRU Functional Block FTA
4A1B56		1.0E-5	1.0E-7	Yes	None
.		.	.		
.		.	.		
.		.	.		

APPENDIX E
DEPENDENCE DIAGRAMS

NOTE: The basic ARP4761 document contains information which places the information in this
appendix in context. This appendix should be used in conjunction with the main body of the
document.

E.1   INTRODUCTION:

Dependence Diagrams (DD) may be used as an alternate method of representing the data in
Fault Tree Analyses (FTAs). This provides an alternate pictorial representation of combinations of
failures for the purpose of probability analysis. The processes and methods explained and
described in Appendix D for FTAs also generally apply to DDs. The principle differences between
FTAs and DDs are that DDs have no additional logic symbols, because they show the logic by
serial or parallel arrangement of boxes, and that DDs do not show intermediate events which
would appear in FTAs as descriptions of the output of a logic symbol. The DD is analytically
identical to the FTA and the role of the DD in the safety assessment process is the same as the
role of FTAs. The guidance in this appendix deals with DD unique issues not covered by the FTA
process in Appendix D.

E.2   SCOPE:

This Appendix explains the basic logic arrangements, the basic analysis procedure and the
pictorial representation of several, different types of events. Variations and additions on the event
representations may be applied as necessary to support a specific analysis. This Appendix should
enable an engineer experienced in fault tree analysis to apply the Dependence Diagram method.

E.3   BASIC LOGIC ARRANGEMENT:

Each Dependence Diagram represents a Failure Condition (unwanted top event). It is constructed
utilizing rectangular boxes, which represent fault events leading to the top event. These boxes are
arranged in series or parallel formation. Series chains are OR situations, while parallel chains
represent AND situations.
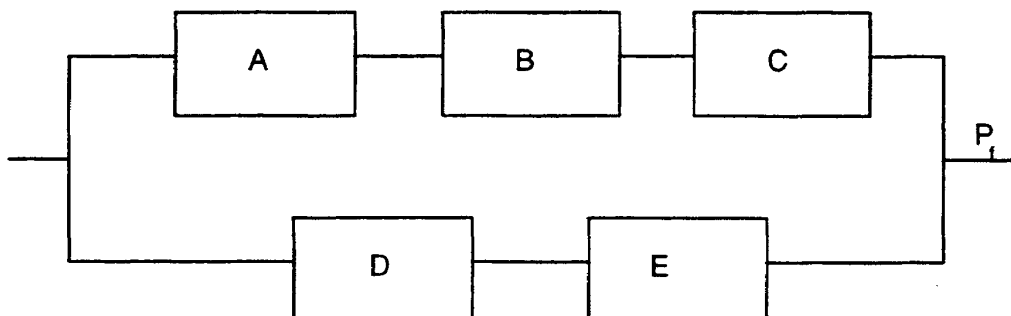
FIGURE E1 - Series/Parallel Combinations

E.3   (Continued):

The probability of the overall Failure Condition P_f in the DD shown in Figure E1 is approximately given by:

$$P_f = (P_fA + P_fB + P_fC) * (P_fD + P_fE) \text{ per flight} \qquad \text{(Eq. E1)}$$

The arrangement shown is simplistic in order to introduce the reader to the basic philosophy. The dependence diagrams can become quite complex and may involve the multiple use of single failures throughout the diagram, in which case the application of Boolean algebra will be required in order to complete the probabilistic calculations and generate the minimal cut sets.

All the qualitative and quantitative evaluations using minimal cut sets are identical to those made with the Fault Tree cut sets (see the following paragraphs of Appendix D).

a.   Qualitative importance determination (D.10.2)

b.   Common cause vulnerability (D.10.3)

c.   Quantitative evaluation: Probabilistic calculations and associated formulas are the same as those used for Fault Tree evaluations (Section D.11).

Errors can be incorporated into Dependence Diagrams in the same way as in Fault Trees (see Appendix D, Section D.12).

E.4   PICTORIAL REPRESENTATIONS OF EVENTS:

Dependence Diagrams are usually constructed utilizing rectangular boxes. Variations in the form of the boxes can be used to depict different conditions, similar in manner to the variety of shapes used in Fault Trees. Examples are described in the following paragraphs.

E.4.1   Failure Modes:

The "solid line" box depicts a failure mode which is internal to the system being analyzed and which needs no further development. This is comparable to a circle representation in Fault Trees. In the PSSA, the box should contain a description of the failure mode and the budgeted failure rate with associated risk time and/or exposure time. In the SSA, the budgeted failure rate may be replaced by the actual failure rate and may include the source reference from the FMES. Figure E2 is an example from an SSA Dependence Diagram.

```
┌─────────────────────────────┐
│  Loss of speed signal       │
│                             │
─│  Ref.:    FMES 7.4          │─
│                             │
│  Failure Rate:    1E-6      │
│  Risk Time:       5 min     │
│  Exposure Time:  N/A        │
└─────────────────────────────┘
```
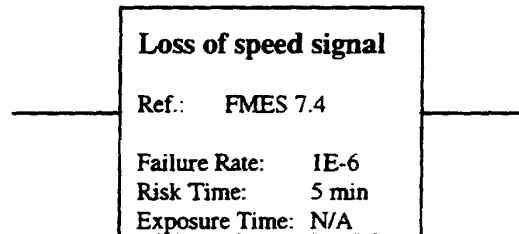
FIGURE E2 - Fully Developed Failure Mode Internal to the System

E.4.1   (Continued):

This example indicates that the failure "Loss of Speed Signal" is referenced back to the FMES, with a failure rate of 1E-6 and the risk time for that failure of 5 min.

E.4.2   Failure Condition:

A box drawn with "dashed" lines depicts another failure condition of the system under investigation or failure condition of another system. This is comparable to a sub-tree in fault tree analysis.

```
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
│  Loss of Busbar 1XPI  │
│                       │
─│  Ref.:    SSA 24.4.3  │─
│                       │
│  Failure Rate:   1E-5 │
│  Risk Time:      1h    │
│  Exposure Time:  N/A   │
└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```
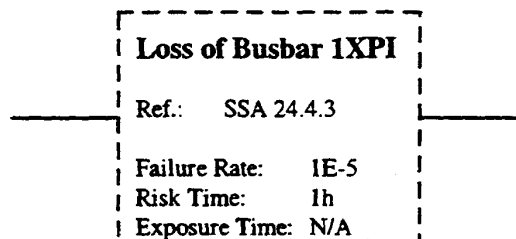
FIGURE E3 - Undeveloped Failure Mode Internal to the System or External Failure Mode

The example in Figure E3 above indicates that "Loss of Busbar 1XPI" can be found in the referenced SSA.

A box which has a diagonal cross depicts a failure mode for which the probability of failure cannot be directly derived from its stated λ and t. This box may be a further subset dependence diagram in its own right, and has to be referred to directly in order to determine its probability of failure. This box is shown in Figure E4.
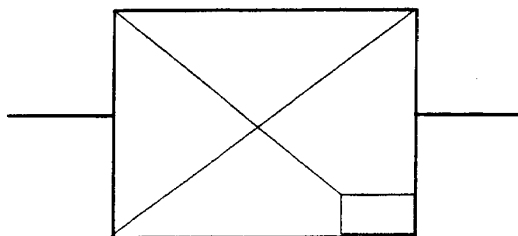
FIGURE E4 - Indirect Probability

E.4.2   (Continued):

Care should be taken when using these failure condition boxes in the probability calculation of the Dependence Diagram. They only show the top level of another Dependence Diagram which could contain common elements with the Dependence Diagram under investigation. They may also contain exposure times different from the ones considered in the original Dependence Diagram.

Calculations should always be performed with the complete dependence diagram structure for the failure condition of concern; and not by simply using the probability of that failure condition in the calculation.

E.4.3   External Events:

A "dotted" line box depicts an event which is external to the aircraft, for example icing conditions.
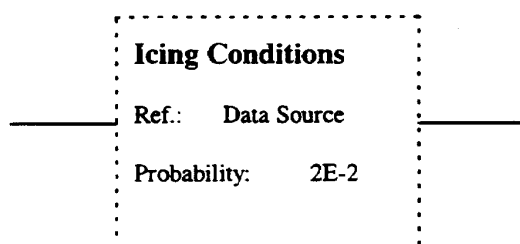
FIGURE E5 - Failure or Event External to the Aircraft

The example in Figure E5 above indicates that Icing Conditions exist with a probability of 2E-2 per flight and the reference for the probability.

APPENDIX F
MARKOV ANALYSIS (MA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

F.1   INTRODUCTION:

This appendix presents an intuitive understanding of Markov analysis without the complexity of the underlying mathematics. A Markov model (chain) represents various system states, and relationships among them. The states can either be operational or non-operational. The transition rate from one state to another is a function of the failure or repair rate. Since one can know the status of the system at the start of the time period, one can initialize the probability value of that particular state of the system to be 1 and probability of all other states of the system to be zero. At some time, t, there is a finite probability of being in any state of the Markov chain. The sum of the probabilities of being in all possible states must be equal to 1. The state probabilities are derived by solving a set of differential equations which are derived from the Markov chain. Each state is mutually exclusive because at any given time, the system can be in only one of the states. Final failure state is generally the state in which all redundancy of the system has been exhausted or there are no more operational states.

F.1.1   Background:

The complexity and size of the systems are rapidly increasing with new advances in technology. Aircraft systems are relying more and more on fault tolerant systems. Such systems hardly ever fail completely because of continuous monitoring of their condition and instantaneous reconfiguration of the systems. This is true unless external events override the operation. Given this scenario of fault tolerances, the safety assessment process and evaluation of such system may be more appropriately achieved by the application of the Markov technique.

For civil airborne systems and equipment, end users may take advantage of the available redundancy to schedule maintenance activities. This scheduling is possible because the redundancy provides equipment safety levels for longer periods of time.

FTA and DD have been widely used for safety assessment because they are conceptually simple and easy to understand. For these reasons, FTAs and DDs should be used whenever possible, recognizing the following limitations.

a.   It is difficult to allow for various types of failure modes and dependencies such as near-coincident-faults, transient and intermittent faults and standby systems with spares.

b.   A fault tree is constructed to assess cause and probability of a single top event. If a system has many failure conditions, separate fault trees may need to be constructed for each one of them.

F.1.1   (Conditions):

In some situations it may be difficult for a fault tree to represent the system completely; such as repairable systems and systems where failure/repair rates are state dependent.

Markov Analyses (MAs) do not possess the above indicated limitations. The sequence-dependent events are included naturally, therefore they can cover a wide range of system behaviors.

In MAs, one can more easily include the scenarios pertaining to the user operational environments; e.g., airline maintenance policies, dispatch requirements and safety considerations. MAs are also capable of handling several phases of a flight, state dependent failure rates, common mode failures, performability and performance-reliability dependence, physical interconnection dependence, time dependent transitions and above all, the imperfect coverage. Imperfect coverage can result from latent failures and less than 100% detectability. However, the disadvantage of performing Markov analysis is that, the size of a Markov model may grow exponentially with the number of components. For a system with 'n' components the corresponding Markov chain may have up to 2^n states in the simplest case, although it usually is a lot less when system operation is considered. If more than two states are associated with any component, the number of states may even be larger. Techniques have been developed to effectively deal with this problem.

Definitions of selected terms used in Markov Models are given in Table F1.

TABLE F1 - Definitions of Terms Used in Markov Analysis

Absorbing State:	A system enters the state and remains there. This means there are no outgoing transitions from this state. If absorbing states are present in a Markov chain, eventually the probability of being in one of these states will be unity.
Ergodic Process:	In addition to being homogeneous, the final value of the probability of being in any state is independent of the initial condition.
ESPN (Extended Stochastic Petri Nets):	A FEHM model for detailed analysis of system recovery from a fault of any type.
FEHM (Fault and Error Handling Models):	These are the models which describe the system behavior on occurrence of a fault. The models output the probability of fault detection, Coverage (C), probability of non-detection and hence system failure called Single point failure (S), probability of system failure due to a near coincident fault, probability (N), and probability of restoring the system from a fault, (R). There are six FEHM's which are popularly used and they are Histogram, Probabilities & Distributions, Means & Standard Deviations, CARE III, ARIES and Extended Stochastic Petri Nets (ESPN).

TABLE F1 (Continued)

Homogeneous Markov processes:	State transitions are memory-less and state holding time is exponentially distributed. Components do not 'age' and state transitions occur at a constant transition rate.
Homogeneous Process:	All transition probabilities and transition rates are constant.
Non-Homogeneous process:	Relaxes the exponential holding time restriction.
Performability:	This measure is the combination of reliability and performance of a system. Performance could be in terms of throughput of the system, average job completion time, average fuel consumption, etc.
Semi-Absorbing State:	A system enters the state as an outcome of continuous transition and remains there until repair which is the outcome of a discrete probability interchange.
Semi-Markov process:	The transition rates can be functions of state specific (local) clocks and not global clocks. The state holding times can be non-exponential and can depend on the next state.
State Space:	Set of all possible states that a system can attain.
State:	A state represents a status of the system.
Stiff Markov Chain:	Contains both, slow and fast transitions whose transition rates differ by orders of magnitude.
Stochastic Processes:	Cannot predict system behavior beforehand but the probabilities of different states at a particular time can be specified.
Transition Times:	The time at which a transition takes place from one state to another state. This transition can take place on a continuous or discrete time scale.
Transitions:	Movement from state to state with certain finite probability or a transition rate. Transition from state i to state j depends only on state i and state j and not on the history. This is the reason why Markov chains are called memory-less systems.

F.2 THEORY:

Markov analysis of any system consists of two parts: Observing the system behavior by writing down the equations associated with the transitions and states in the system, and solving these equations using standard techniques. The state equations for any system can be constructed by inspection of the Markov chain. However, due to mathematical complexity this manual method can lead to errors and omissions even for simple systems. Therefore, some form of automated model generation is recommended. In general, the change in the probability of a state is due to the flows leaving and entering that state. The flows along a transition are the product of the transition rate along that transition and the probability of the state at the origin of that transition. A negative sign represents the rate at which the system is leaving that particular state, while a positive sign implies the rate at which the system is entering that new state.

To illustrate, consider the following scenario:
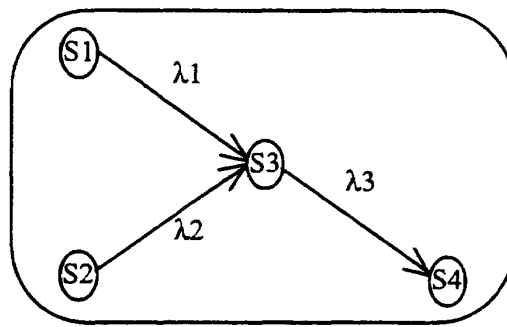
FIGURE F1 - An Example of Input/Output Transitions In/Out of a State in a Markov Chain

In this system, state S_3 has a time dependent probability value of $P_3(t)$. It has two input arcs from states S_1 and S_2 and one output arc to state S_4. Time dependent probability values of S_1 and S_2 are $P_1(t)$ and $P_2(t)$ respectively. Transition rates into the state S_3 from S_1 and S_2 are λ_1 and λ_2 respectively. Transition rate out of the state is λ_3. The rate of change of state probability of S_3 can be written in terms of state probabilities $P_1(t)$, $P_2(t)$, $P_3(t)$ and transition rates λ_1, λ_2, and λ_3 and that equation is given below:

$$\frac{dP_3(t)}{dt} = \lambda_1 P_1(t) + \lambda_2 P_2(t) - \lambda_3 P_3(t) \tag{Eq. F1}$$

Similarly, differential equations can be written for all other states of this Markov chain. These set of differential equations can be solved using mathematical techniques such as Laplace Transforms. However, as the system becomes more complicated, it is a very laborious and time consuming process to manually solve the set of differential equations. Hence, the analyst should use one of the tools given in Section F.4 (e.g., HARP) to solve the Markov chain. Detailed examples are shown in the following subsections.

F.2.1   Series Systems:

F.2.1.1   A Series System: Non-repairable: As an example, one can consider a system of two components in series. Component A has a failure rate of λ_a failures/hour and component B has a failure rate of λ_b failures/hour. Also there is a common failure mode by which both components A and B fail simultaneously and this rate is given by λ_c failures/hour. (This should not be confused with the logical AND of the independent failures of component A and B.) A Markov model for this system is shown in Figure F2. The model is constructed by considering all possible failure combinations (states) at each failure level. For instance, at the zero failure level (0F) there is only one state: A and B are good, and at the one failure level (1F) there are two states, one where A has failed and the other where B has failed. At (2F) level, there is a common mode failure and both components are failed.
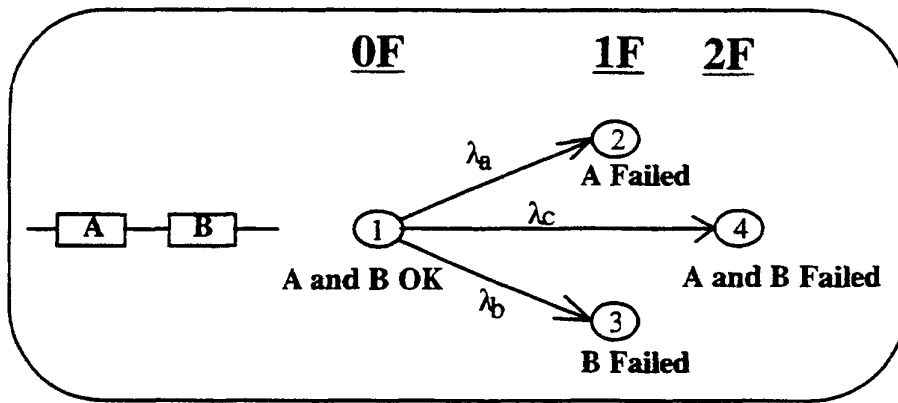
FIGURE F2 - Markov Model of a Simple Non-repairable Series System

The state equations for the system represented in Figure F2 are:

$$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t)$$

$$\frac{dP_4(t)}{dt} = \lambda_c P_1(t)$$

(Eq. F2)

where $P_i(t)$ is the probability of being in state i at time t. For constant failure rate and an initial condition of $P(0) = [1\ 0\ 0\ 0]^T$ (T stands for transpose), the state equations can be integrated to obtain closed form expressions for all the probability values. They are given by:

F.2.1.1   (Continued):

$$P_1(t) = e^{-(\lambda_a + \lambda_b + \lambda_c)t}$$

$$P_2(t) = \frac{\lambda_a}{\lambda_a + \lambda_b + \lambda_c} \times \left(1 - e^{-(\lambda_a + \lambda_b + \lambda_c)t}\right)$$

$$P_3(t) = \frac{\lambda_b}{\lambda_a + \lambda_b + \lambda_c} \times \left(1 - e^{-(\lambda_a + \lambda_b + \lambda_c)t}\right) \qquad \text{(Eq. F3)}$$

$$P_4(t) = \frac{\lambda_c}{\lambda_a + \lambda_b + \lambda_c} \times \left(1 - e^{-(\lambda_a + \lambda_b + \lambda_c)t}\right)$$

For large times, $P_1(t)$ goes to zero, $P_2(t)$ approaches $\lambda_a/(\lambda_a + \lambda_b + \lambda_c)$, $P_3(t)$ approaches $\lambda_b/(\lambda_a + \lambda_b + \lambda_c)$ and $P_4(t)$ approaches $\lambda_c/(\lambda_a + \lambda_b + \lambda_c)$. The probability of system failure is equal to the sum of $P_2(t)$, $P_3(t)$ and $P_4(t)$.

This is the same solution which one would obtain when using any combinatorial method as shown below:

At time t,

P (A failing) = $1 - e^{-\lambda_a t}$

P (B failing) = $1 - e^{-\lambda_b t}$

P (A and B failing) = $1 - e^{-\lambda_c t}$ (common mode failure)

Now, from combinatorial techniques:

P (A or B failing) = 1 - P (A and B both not failing)

Therefore,

P (A or B) = $1 - e^{-(\lambda_a + \lambda_b + \lambda_c)t}$

Notice that this is same as $P_2(t) + P_3(t) + P_4(t)$ as derived from the Markov chain.

Similarly,

P (A and B not failing) = $e^{-(\lambda_a + \lambda_b + \lambda_c)t}$

Notice that this equation is same as $P_1(t)$ obtained using the Markov techniques above.

F.2.1.2   A Series System - Repairable: As an example, once again consider the same system of two components in series. Component A has a failure rate of λ_a failures/hour and component B has a failure rate of λ_b failures/hour. Also there is a common failure mode by which both components A and B fail simultaneously and this rate is given by λ_c failures/hour. (This should not be confused with the logical AND of the independent failures of component A and B.) In addition to failures, both components A and B are assumed to be repaired at a constant rate of μ. In most of the aviation cases, repair is done at the end of the check interval and hence is a discrete repair process. However, the modeling in F.2.2.1 and F.2.2.2 approximate the discrete repairs by a continuous time Markov process. This approximation is valid when $\lambda \ll \mu$. In case the repair is a stochastic process, this model represents a correct solution. Examples of discrete repair modeling are given in F.5.1 and F.5.2. When both components are failed, repair rate is assumed to be μ_c. By choosing different values for μ_c, one can simulate different scenarios like single repairmen, multiple repairmen, etc. A Markov model for this system is shown in Figure F3. All the repairs are shown as dotted lines in the figure.
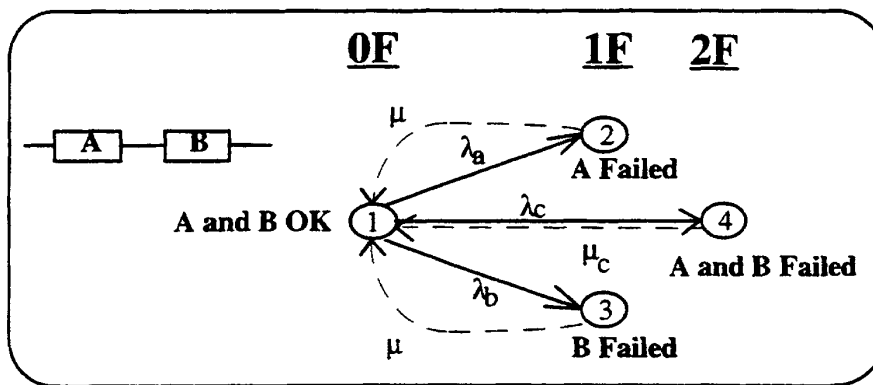
FIGURE F3 - Markov Model of a Simple Repairable Series System

The state equations for the system represented in Figure F3 are:

$$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)P_1(t) + \mu(P_2(t) + P_3(t)) + \mu_c P_4(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - \mu P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - \mu P_3(t)$$ (Eq. F4)

$$\frac{dP_4(t)}{dt} = \lambda_c P_1(t) - \mu_c P_4(t)$$

F.2.1.2   (Continued):

where $P_i(t)$ is the probability of being in state i at time t. For constant failure and repair rate and an initial condition of $P(0) = [1\ 0\ 0\ 0]^T$ (T stands for transpose), the state equations can be integrated (similar to the procedure shown in F.2.1.1) to obtain closed form expressions for all the probability values. For simplicity, they are not shown here.

F.2.2   Parallel Systems:

F.2.2.1   A Parallel System - Non-repairable: The Markov model of the parallel system is given in Figure F4 in which system failure is defined to be the failure of components A and B. Because of the nature of the Markov method, order dependencies can be easily included in the Markov chain; i.e., states 4 and 5. States 4 and 5 in the Markov chain distinguish between the two possible orders of component failure leading to a system loss.
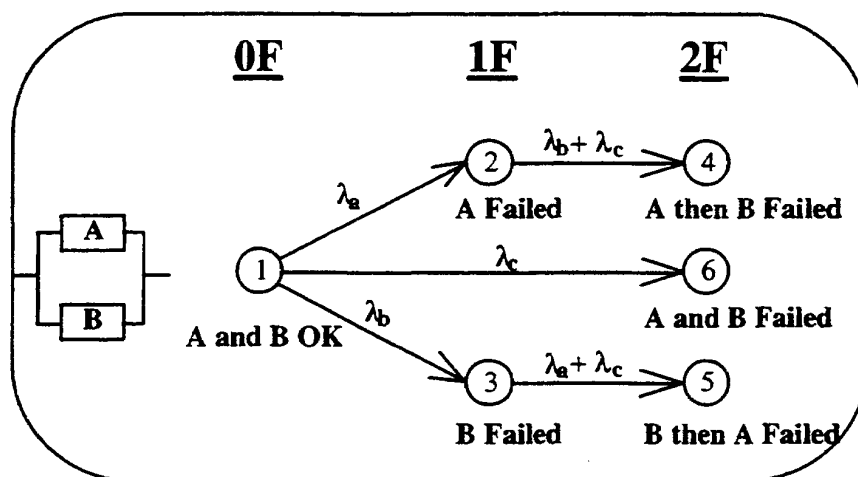
FIGURE F4 - Markov Model of a Simple Parallel System

Assuming the failure rates of components A and B to be λ_a and λ_b respectively, common mode failure rate to be λ_c, and $P_i(t)$ being the probability of system being in state 'i' at time 't', the state equations for this system are:

F.2.2.1   (Continued):

$$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - (\lambda_b + \lambda_c)P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - (\lambda_a + \lambda_c)P_3(t)$$

$$\frac{dP_4(t)}{dt} = (\lambda_b + \lambda_c)P_2(t)$$ (Eq. F5)

$$\frac{dP_5(t)}{dt} = (\lambda_a + \lambda_c)P_3(t)$$

$$\frac{dP_6(t)}{dt} = \lambda_c P_1(t)$$

For constant failure rate and an initial condition of $P(0) = [1\ 0\ 0\ 0\ 0\ 0]^T$ the state probabilities are:

$$P_1(t) = e^{-(\lambda_a + \lambda_b + \lambda_c)t}$$

$$P_2(t) = e^{-(\lambda_b + \lambda_c)t}\left(1 - e^{-\lambda_a t}\right)$$

$$P_3(t) = e^{-(\lambda_a + \lambda_c)t}\left(1 - e^{-\lambda_b t}\right)$$

$$P_4(t) = \frac{\lambda_a}{\lambda_a + \lambda_b + \lambda_c} - e^{-(\lambda_b + \lambda_c)t} + \frac{\lambda_b + \lambda_c}{\lambda_a + \lambda_b + \lambda_c}e^{-(\lambda_a + \lambda_b + \lambda_c)t}$$ (Eq. F6)

$$P_5(t) = \frac{\lambda_b}{\lambda_a + \lambda_b + \lambda_c} - e^{-(\lambda_a + \lambda_c)t} + \frac{\lambda_a + \lambda_c}{\lambda_a + \lambda_b + \lambda_c}e^{-(\lambda_a + \lambda_b + \lambda_c)t}$$

$$P_6(t) = \frac{\lambda_c}{\lambda_a + \lambda_b + \lambda_c}\left(1 - e^{-(\lambda_a + \lambda_b + \lambda_c)t}\right)$$

$P_2(t)$ and $P_3(t)$ give the probability of the system being in a degraded mode; i.e., A has failed and B is operational and vice-versa. The probability of system failure is equal to the sum of $P_4(t)$, $P_5(t)$, and $P_6(t)$. In this case also, one can show that the probability equations derived from combinatorial techniques are similar to the ones obtained above using the same argument as given in the previous section.

F.2.2.2 A Parallel System - Repairable: The Markov model for a repairable parallel system is given in Figure F5.
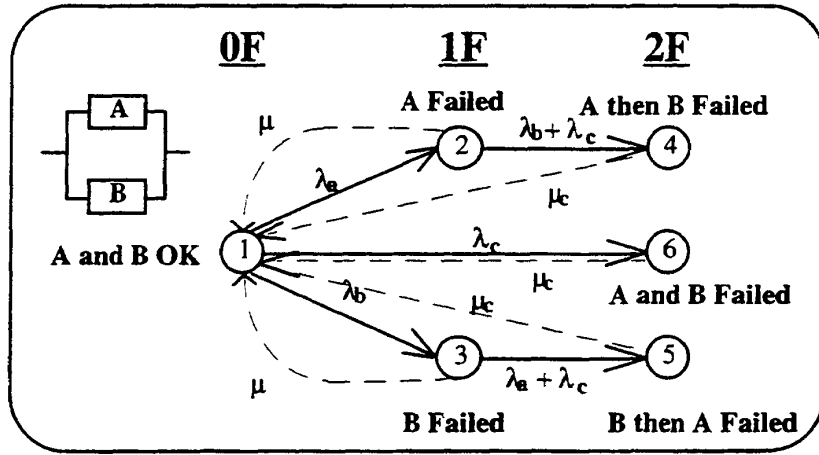
FIGURE F5 - Markov Model of a Simple Repairable Parallel System

The repair rates are assumed to be μ and μ_c from states where there is only one component failure and two component failures respectively. They are shown as dotted lines in Figure F5. Assuming the failure rates of components A and B to be λ_a and λ_b respectively, common mode failure rate to be λ_c, and $P_i(t)$ being the probability of system being in state 'i' at time 't', the state equations for this system are:

$$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)P_1(t) + \mu(P_2(t) + P_3(t)) + \mu_c(P_4(t) + P_5(t) + P_6(t))$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - (\lambda_b + \lambda_c - \mu)P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - (\lambda_a + \lambda_c - \mu)P_3(t)$$

(Eq. F7)

$$\frac{dP_4(t)}{dt} = (\lambda_b + \lambda_c)P_2(t) - \mu_c P_4(t)$$

$$\frac{dP_5(t)}{dt} = (\lambda_a + \lambda_c)P_3(t) - \mu_c P_5(t)$$

$$\frac{dP_6(t)}{dt} = \lambda_c P_1(t) - \mu_c P_6(t)$$

One can derive the exact state probabilities by integrating the above equations as was done in the previous section.

- 117 -

F.2.3   Fault and Error Handling Models (FEHM) in Markov Analysis:

Usually, faults in a system occur at a very low rate. The time to detect and handle a fault will be very short, usually in the order of seconds or less. This many orders of magnitude difference in fault occurrence and detection times, make the Markov chain very stiff and the solution time of the reliability model may be very large. To reduce this time, the solution method can be broken down into two parts: The first part deals with the conditions for system to fail and the repair strategy involved, and is called the Fault Occurrence and Repair Model (FORM). The system behavior is described by means of fault trees or Markov chains. The second part defines the system behavior after a fault occurs. This model, Fault and Error Handling Model (FEHM), computes four probabilities which are defined below:

R   =   probability that the system perceives the occurred fault as a transient and recovers from this transient fault.
C   =   probability that the system perceives the occurred fault as a permanent fault and successfully completes permanent reconfiguration with resulting loss in module redundancy.
S   =   probability that the system fails due to its inability to detect, isolate, and/or recover from the occurred fault.
N   =   probability that the system fails due to the occurrence of a second (near-coincident) fault while handling the first fault.

In Figure F6, several FEHM modes are shown which can be used to define these complex actions and interactions in the system upon occurrence of a fault.
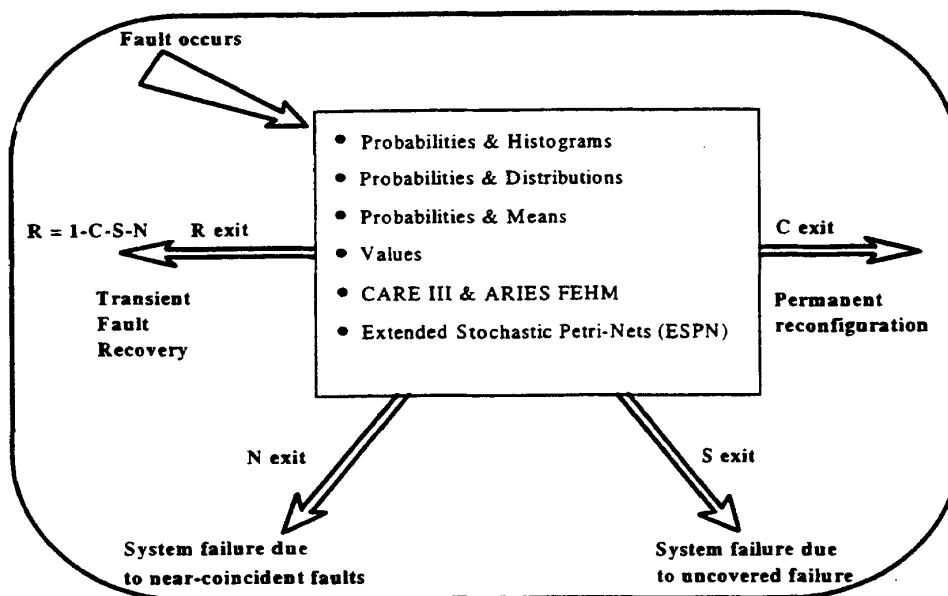
FIGURE F6 - A List of Generic Fault Error Handling Models (FEHM)

F.2.3 (Continued):

Here the 'C' exit is taken if the fault in the system is detected and the system successfully reconfigures into a degraded mode. The 'R' exit is taken if the system is able to detect the failure and is able to diagnose the fault and recover from it. In this case, the system behaves as if no fault has occurred previously. The 'S' exit is taken if the system fails to recognize the fault and this fault leads to system failure. The 'N' exit is taken if a second fault occurs in the system while it is trying to reconfigure from the earlier fault. In this situation, the system is always assumed to go to a failure state. These FEHM models are "canned" models which deal with a variety of error recovery scenarios in real life. For example, the ARIES FEHM model deals with system recovery from a fault in phases which might reflect different retries upon a soft/transient fault in the system. Similarly, the CARE III FEHM model defines error recovery in terms of detection and isolation rates and is ideal for modeling error recovery procedures in fault tolerant memory. It is always possible to define a new FEHM model which might reflect the error recovery process more accurately. This is possible by a direct input of the recovery Markov chain. Further details of the FEHM models are given in the HARP manual. It should be understood that FEHM modeling is only one of the solution techniques and is not the only solution technique available. The Analyst can use any technique as long as the validity of the methodology is explained and understood properly.

F.2.3.1 Use of FEHM in Modeling: In a simple 3-Processor/2-Bus system as illustrated in Figure F7, the system fails when all three processors have failed or when both buses have failed. The failure rates of each processor and each bus are assumed to be λ_1 and λ_2 respectively.
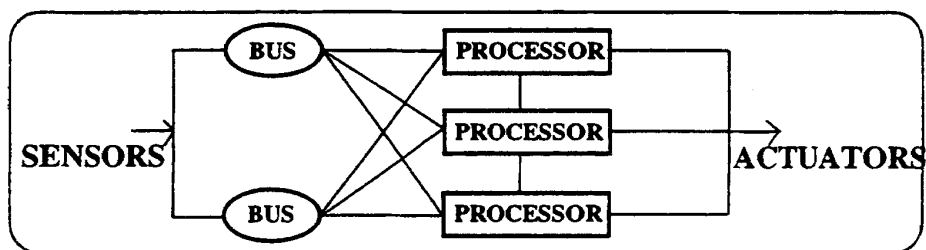

FIGURE F7 - Signal Flow Representation of a 3-Processor/2-Bus System

One can show FEHM modeling through the use of the above example. In the first case, one can solve the system without including any FEHM. In this case, it is assumed that the system can detect any fault 100% of the time and can reconfigure to a degradable mode within no time. In the second case, imperfect coverage is assumed. In this case, upon a failure, there could be several decisions to be made such as: fault detected, fault isolated, system reconfigured, system repaired and system failure due to near coincident fault. All these scenarios can be modeled using FEHM.

F.2.3.2 System Modeling Without FEHM (Coverage = 1.0): The Markov chain for this system is shown in Figure F8. The state tuple is given by two variable set: (X,Y) where X is the number of functional processors in the system and Y is the number of functional buses in the system. In the case of perfect coverage, one can assume that when a processor or a bus has failed, the system always successfully transitions to the next redundant (degraded) level (i.e., from state (3,2) to state (2,2) or from (3,2) to (3,1) upon a processor or a bus failure respectively (see Figure F8)).
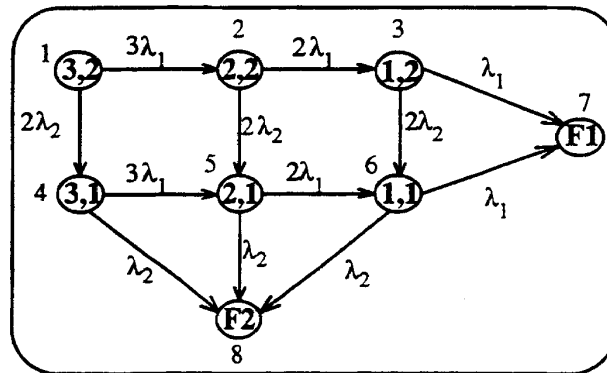
FIGURE F8 - Markov Chain Representation of a 3-Processor/2-Bus System without Coverage

Assuming $P_i(t)$ represents the probability that the system is in state 'i' at time 't', the state equations for this example are constructed by inspecting the Markov chain and are given below:

F.2.3.2   (Continued):

$$(3,2) \quad \frac{dP_1(t)}{dt} = (-3\lambda_1 - 2\lambda_2)P_1(t)$$

$$(2,2) \quad \frac{dP_2(t)}{dt} = 3\lambda_1 P_1(t) - (2\lambda_1 + 2\lambda_2)P_2(t)$$

$$(1,2) \quad \frac{dP_3(t)}{dt} = 2\lambda_1 P_2(t) - (\lambda_1 + 2\lambda_2)P_3(t)$$

$$(3,1) \quad \frac{dP_4(t)}{dt} = 2\lambda_2 P_1(t) - (3\lambda_1 + \lambda_2)P_4(t)$$

$$(2,1) \quad \frac{dP_5(t)}{dt} = 2\lambda_2 P_2(t) + 3\lambda_1 P_4(t) - (2\lambda_1 + \lambda_2)P_5(t)$$

$$(1,1) \quad \frac{dP_6(t)}{dt} = 2\lambda_2 P_3(t) + 2\lambda_1 P_5(t) - (\lambda_1 + \lambda_2)P_6(t)$$

$$(F1) \quad \frac{dP_7(t)}{dt} = \lambda_1 P_3(t) + \lambda_1 P_6(t)$$

$$(F2) \quad \frac{dP_8(t)}{dt} = \lambda_2 P_4(t) + \lambda_2 P_5(t) + \lambda_2 P_6(t)$$

(Eq. F8)

F.2.3.3   System Modeling with FEHM (Coverage < 1): If the 3-Processor/2-Bus system contains imperfect coverage (i.e., presence of latent failures and less than 100% fault detectability) or could face transient, intermittent or near coincident failures, one can model these scenarios by using some type of Fault and Error Handling Models (FEHM). When a fault occurs, the system can recover from the fault without declaring it as a permanent fault. Figure F6 shows six generic FEHM which are available in Hybrid Automated Reliability Predictor (HARP). Figure F9 shows a Markov chain with coverage being employed to handle the system faults. When a fault occurs, there is some probability, C, which is less than 1, that the system will reconfigure to the next lower redundant (or degraded) level. The fault can also be undetected and so severe that it will cause the entire system to fail. The probability of such a failure is denoted as Failure due to Single Point Fault (FSPF). Another failure mode which is considered in this Markov chain is that, while a fault is being recovered, a second fault occurs almost at the same time or before reconfiguration can take place to cause Failure due to a Near-Coincident Fault (FNCF).
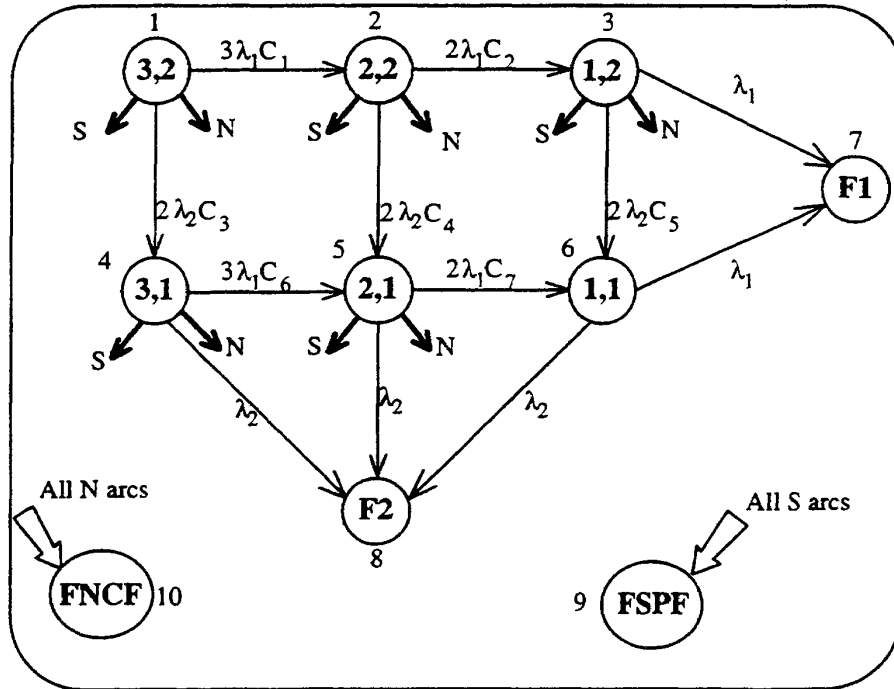
FIGURE F9 - Markov Chain Representation of a 3-Processor/2-Bus System with Imperfect Coverage
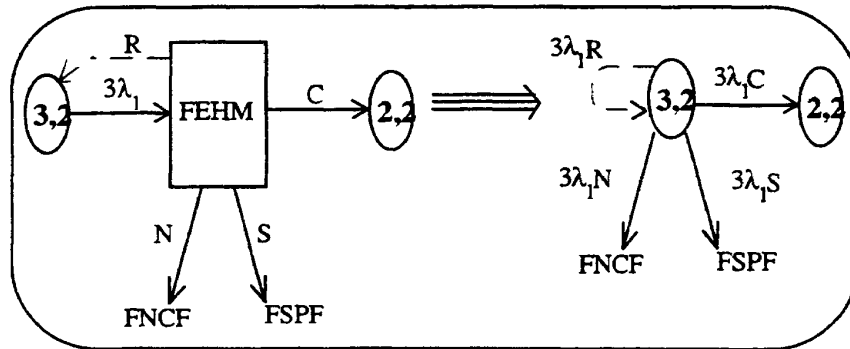

FIGURE F10 - Effect of Using FEHM Models in Markov Chain Representation

F.2.3.3   (Continued):

Here, from a state (3,2) the system enters FEHM with a failure rate of $3\lambda_1$. From this FEHM, the system can take four exits (each corresponding to the system behavior under fault condition).

a.   It can go to a state (2,2) with a finite probability given by the imperfect coverage value, C.

b.   The system diagnoses the fault and returns back to the (3,2) state with probability given by the restoration factor, R.

c.   The fault might go undetected and lead to a system failure with a probability, S.

d.   Before the system can reconfigure from the first fault, there might be a second fault in the system with probability, N and this double fault in the system leads to a near coincident failure.

As shown in Figure F10, each state in the Markov chain is modified by inserting C, R, S, and N values and then solving the Markov chain. These values are directly provided by the user or are calculated from the distributions for these exits given by the user. The HARP tool has the capability to modify the Markov chain accordingly, once the user provides the FEHM.

In the SURE tool, the FEHM concept is included in the form of functions. Whenever a component fails, a function is used to define the mean time to reconfigure the system to a degraded state with less redundancy. Similarly, other functions are used to define the near coincident faults. The advantage of the SURE program lies in the fact that these functions can be any distribution functions and not limited to exponential functions alone.

F3   STATE SPACE REDUCTION TECHNIQUES FOR MARKOV MODELS:

Markov models can become very large and complex. For this reason it may be necessary to explore techniques for reducing the size of the models.

F.3.1   State Aggregation:

State aggregation is one method of reducing the size of the Markov chain. This technique aggregates two states with identical failure rates into a single state. The example below shows the concept of state aggregation. This system contains three processors with failure rates of λ_1, λ_2, and λ_3. The System is assumed to be failed if all the processors fail. Figure F11 shows the Markov chain of the system.
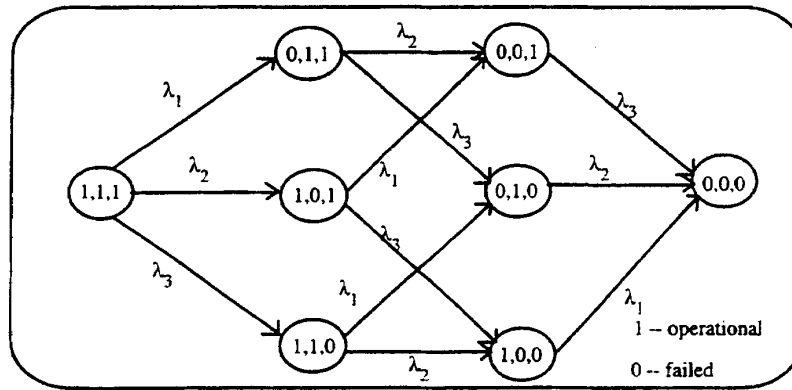
FIGURE F11 - Markov Chain Representation of Three Processor System

F.3.1   (Continued):

To illustrate state aggregation, assume that all processors are identical. Hence the failure rates of all components are given by λ. The Markov chain equivalent in this case can be reduced by combining all the states which are within the same column in Figure F11. The reduction was possible by noticing that any pair of transitions between two columns are identical and this reduces the Markov chain to the one shown in Figure F12.
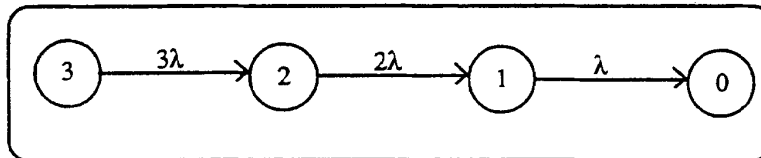
FIGURE F12 - Reduced State Space of Three Processor System Using State Aggregation

One can observe that three states in one column of Figure F11 have been aggregated into one state in Figure F12. This reduces the total number of states from 8 in Figure F11 to 4 in Figure F12.

These states are hardware equivalent since the faults which define the states are equally likely. They are also transition equivalent since the ongoing system reliability when further faults occur is also identical. States which are hardware equivalent are not necessarily transition equivalent and vice-versa. It is transitional equivalence only which is valid for model reduction.

F.3.2   Model Truncation:

Model truncation reduces the Markov chain by terminating the process of generation of the Markov chain in the direction in which the state probabilities will be very small. Another form of truncation is to terminate the generation of the Markov chain after a certain number of failures have occurred in the system. This assumes that the probability of finding the system with a number of failures greater than the truncation limit is very small. Using the same example shown in Figure F12, assume that the model is to be truncated after 2 failures. Then the Markov chain is further reduced and is shown below:
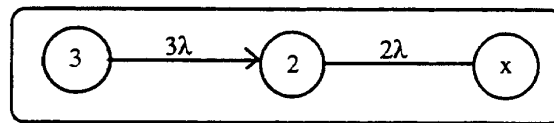

FIGURE F13 - Reduced State Space of Three Processor System Using Model Truncation

By solving these models one can determine/verify that the exact unreliability from the full model lies between the upper and lower bounds obtained from the truncated model. The analyst has to decide about the required level of truncation by evaluating the spread between the upper and the lower bounds. Upper bounds on system reliability are obtained by assuming that all truncated states are operational states. Similarly, lower bounds on system reliability are obtained by assuming that all truncated states are failed states. This computation is done by many tools such as HARP, SURE and others which are discussed later.

F.3.3   Hierarchical Modeling:

One method of reducing the size of a Markov chain is to break a large model into many independent sub-models. This can be achieved if each sub-model is independent. To illustrate an example of this scenario, consider the earlier defined system consisting of three processors (failure rate: λ_1) and two buses (failure rate: λ_2). The system is assumed to fail if all three processors fail or both buses fail. One can develop sub-models for the processor system and bus system and then solve them separately before combining their results. Figure F14 shows the sub chains for both the processor and bus system. A word of caution here is that the independence of sub-models should be evaluated very carefully in such cases; in the current fault tolerant systems where there are component dependencies and repairs involved, breaking the model into independent sub-models may not always be possible.
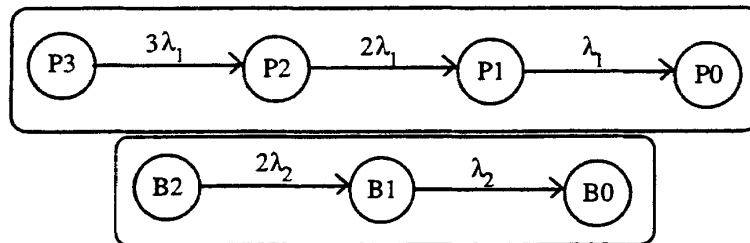
FIGURE F14 - Separate Sub-chains for Processor and Bus System

F.3.3   (Continued):

The probability of system failure, from simple combinatorial techniques is given by:

P (all Processors or all Buses failure)
  = probability of all processors failure (prob. (P0))
  + probability of all buses failure (prob. (B0))
  – prob. (P0)*prob. (B0)

This equation follows from the assumption of independence between the processor and bus sub-models.

F.4   TOOLS AVAILABLE:

Numerous Markov model solvers are available. The following three computer based Markov tools (SURE, SHARPE, and HARP) have been successfully applied to many large and complex problems. There are other tools (SPNP, REST, SURF, ASSURE) which deal with the reliability and availability issues but all of those tools can be categorized into these three tool sets. SURE was developed at NASA Langley whereas HARP was developed at Duke and Clemson Universities under NASA grant. Both of these tools are available from NASA Langley. SHARPE was developed at Duke University.

F.4.1   SURE - Semi-Markov Unreliability Range Evaluator and ASSIST:

The SURE program uses two bounding theorems to compute the upper and lower bounds on system reliability. The advantage of the SURE technique is that the bounds are algebraic in form and, consequently, are computationally efficient. The SURE program divides the transitions into fast and slow paths where fast paths define system recovery from a fault and slow paths refer to the system failures. Once the paths are defined SURE builds a path list leading from the starting state to the final undesired state and computes the probability of traversing this path given the mean and distribution of the transition function for each branch in the path. This program enables the solution of large and complex Markov models. Since SURE can handle a general distribution of recovery time, the overall fault-handling process can be captured in a single transition. The output contains the following information.

F.4.1   (Continued):

   a.   The upper and lower bounds on the probability of the total system failure

   b.   The probability bounds for each undesired event in the model

   c.   The list of every path in the model and its probability of traversal

An associated program called "ASSIST" can generate Markov models in a format compatible with SURE. However, one has to learn the ASSIST language to input data. Due to the limitations of bounding algorithms, steady state solution or fleet average probabilities cannot be computed using SURE.

F.4.2   SHARPE - Symbolic Hierarchical Automated Reliability/Performance Evaluator:

SHARPE enables the user to construct hybrid and hierarchical system models. Hybrid modeling combines the flexibility of Markov models and the efficiency of combinatorial methods. The built-in model types are: reliability block diagram, fault tree, reliability graphs, Markov chains, acyclic or irreducible semi-Markov chains, single and multiple-chain product-form queuing networks, (which are cascade of Markov chains), generalized stochastic Petri Mets (finite state machine description of the system), and series-parallel task graphs. Hierarchical modeling aggregates the predefined sub-models, thereby avoiding both the large state space and stiffness problems.

The Ease of use and efficiency of SHARPE make it a very useful tool for the preliminary design process.

F.4.3   HARP - The Hybrid Automated Reliability Predictor:

The main approach for reducing the state space in HARP is behavioral decomposition. The reliability model is divided into two types of models: slow and fast. The Fault Occurrence Repair Models (FORM) are analyzed separately. The FORM contain information about the structure of hardware redundancy repair procedures, and can be specified either as a fault tree or Markov chain. The coverage model (FEHM) allows modeling of the recovery procedure necessary for the three types of faults; permanent, intermittent and transient faults. Seven different types of FEHM are available to the user. HARP accepts a nominal value and a variance of all input parameters. Additionally, HARP supports the modeling of time dependent failure rates associated with the Weibull failure distribution. This capability applies only to the non-repairable systems. The output file contains information about the probability of user-specified states. HARP provides automatic generation of Markov chains for non-repairable systems if the input is a fault tree.

With fault tolerant systems, components may or may not be operational at the start of a flight. Components are maintained at different scheduled times, per the airline's maintenance plans. Therefore, it is possible that one or more redundant components may have failed (latently or otherwise) before the start of a flight. Another scenario deals with different phases of a flight where the components can have different failure rates or a different set of components is operational.

F.5   EXAMPLES:

Some of the Markov modeling examples which have great significance in aviation systems are given below. Any tool can be used to generate and solve the equations. For the sake of brevity, the equations are not shown here.

The Markov models shown below present a methodology for modeling latent faults. The results can be processed to derive the worst case failure probabilities and the average failure probabilities. The models provide a vector of failure probabilities where each vector corresponds to the system failure probability per flight Using these values, the worst case estimate of failure probability is computed by taking the failure probability of the last flight. To compute the average value of failure probability over the duration of the maintenance check interval, one can sum up all the failure probability values at the end of each flight and divide by the number of flights.

F.5.1   Latent Fault Modeling Using Discrete Repair Process:

If a component is known to be working at the start of a flight, then the reliability calculation is based on an exposure time equal to the flight length. Some aircraft systems include components which are not inspected every flight. Failures of this type of component are called latent because they are not detected unless another failure occurs or a scheduled inspection is performed. There are several possible scenarios depending on whether both the active and standby systems are latent or monitored events and if fault sequencing is important or not. The dashed repair arcs in Figures F15 through F18 represent discrete repairs at fixed intervals. Repairs from system failure states, F, are not shown because these depend on maintenance policy (i.e. the repairs could be partial or full.). Some of the important scenarios along the Markov representation for these scenarios are given below.

a.   Scenario I: A system comprising a component and a monitor

The component is checked before each flight to confirm that it is working, and repaired if necessary. The monitor is not checked before each flight but is regularly checked at a maintenance interval. Thus failure of the monitor can be latent. In reliability analysis, we need to distinguish between a monitored failure and unmonitored failure of the component because the implications of unmonitored failure are likely to be more severe. In this discussion we examine only the computation of probability of an unmonitored failure. An unmonitored failure occurs only if the monitor fails before the component. The Markov representation of this scenario is shown in Figure F15. End of flight inspections and repairs if required are represented as dotted lines with m_t as the parameter in Figure F15. Scheduled inspection and repairs if required are shown as dotted lines with m_T as the parameter in Figure F15. This is true in all the subsequent Markov models shown through Figures F16 to F18. In Figure F15, λ is the failure rate of the component and β of the monitor.
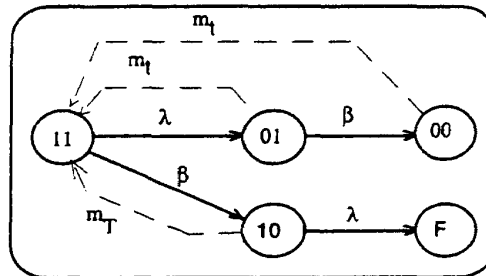
FIGURE F15 - Markov Chain for a Component and a Latent Failing Monitor System

F.5.1   (Continued):

    b.   Scenario II: A system comprising a component and a backup

The component is checked each flight and repaired if found defective. The backup is checked only at a maintenance interval. System failure occurs if the backup component has failed at the time that the component fails or if the backup fails on the same flight as the component. This differs from scenario I in that failure of the monitor after failure of the component but on the same flight would not comprise an unmonitored failure. Markov representation of this scenario is shown in Figure F16. In Figure F16, λ is the failure rate of the component and β of the backup.
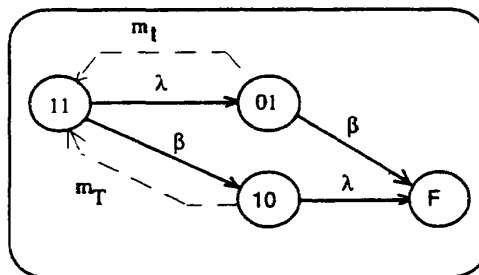

FIGURE F16 - Markov Chain for a Component and a Latent Failing Backup System

    c.   Scenario III: A system comprising two component

When one component of a two component system fails, the backup takes over, but there is no indication that this has happened. The system is checked each flight to ensure that the system is operational. This check ensures that at least one of the two components is working. The individual components are checked at a fixed maintenance interval. Markov model representation for this scenario is shown in Figure F17. Both components are repaired at the end of scheduled inspection interval as shown by dotted lines in the model. 'F' state probability at the end of every flight is adjusted to zero to take into account the fact that the system is operational at the start of any flight with at least one component functional.
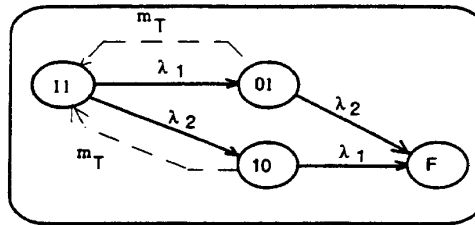
FIGURE F17 - Markov Chain for a Two Component System, Both Failing Latently

F.5.1   (Continued):

   d.   Scenario IV: A system comprising n component

When one component of an n-component system fails, then a backup takes over, but there is no indication that this has happened. The system is checked each flight to ensure that the system is operational. This check ensures that at least one of the n components is working. The individual components are all checked at a fixed maintenance interval T. The Markov chain representation for a three component system is shown in Figure F18. All the repair intervals in the model are the scheduled inspection interval of all the components. At the end of each flight, the fail state probability is adjusted to zero to take into account the fact that the system is operational at the start of any flight with at least one component functional.
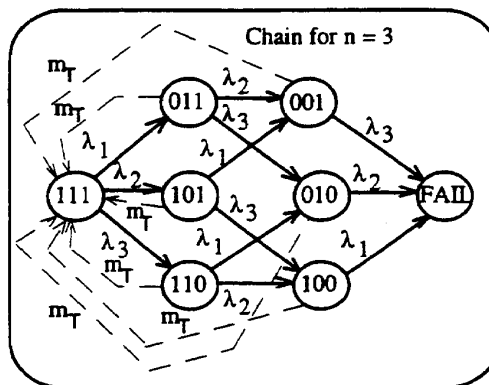

FIGURE F18 - Markov Chain for a Three Component System, All Failing Latently

F.5.2   A Scheduled Maintenance Example:

As an example, consider a two engine system, left and right engines, where each engine has two controllers as illustrated in Figure F19. The system fails when the functionality in all four controllers is lost (state 9 in the Markov chain). The system is functionally degraded when one or more of the controllers are dead. It may be in a non-dispatch state as per regulations when both controllers for one engine are lost. In the figure, all states shown to the left of dotted line are dispatchable states. However, the failure definitions (scenarios) can be modified to account for the Minimum Equipment List (MEL). It is assumed in this example that the system has a different failure rate from each state.

If the left engine is repaired at the end of a flight, then one can know for sure that both controllers in that engine will be fully operational at the start of the next flight. In other words, in the Markov chain at the start of the next flight, the probability of a controller for the left engine failure should be zero. This results in the probabilities of states 3, 4, 6, 7, 8, 9 (shaded in the Figure F20) being initialized to zero at the start of the next flight. The user should be aware that this redistribution of state probabilities may be computerized in a modified version of HARP. The user has to specify that the left engine is being brought up to a fully operational state and the program does the rest.
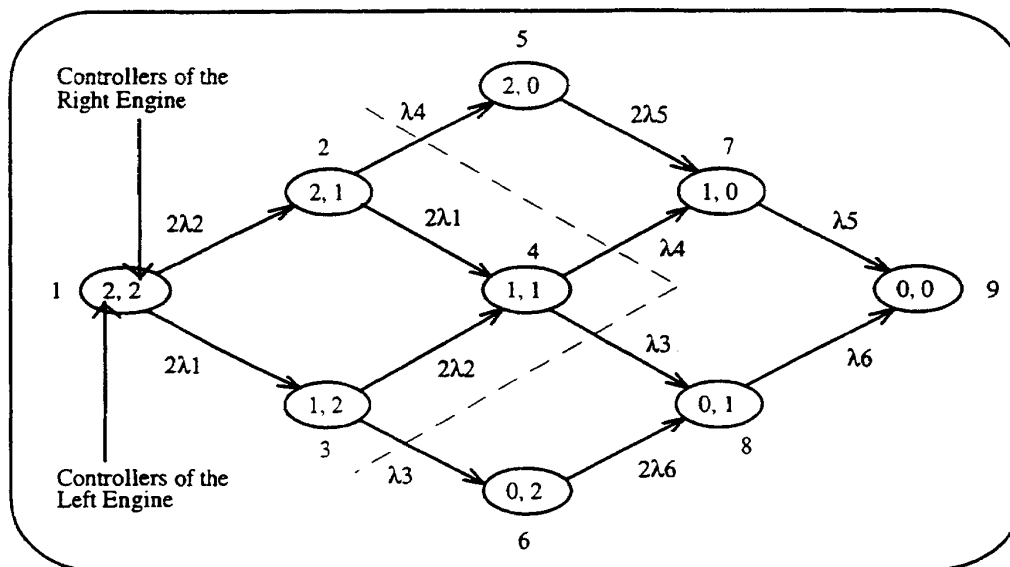

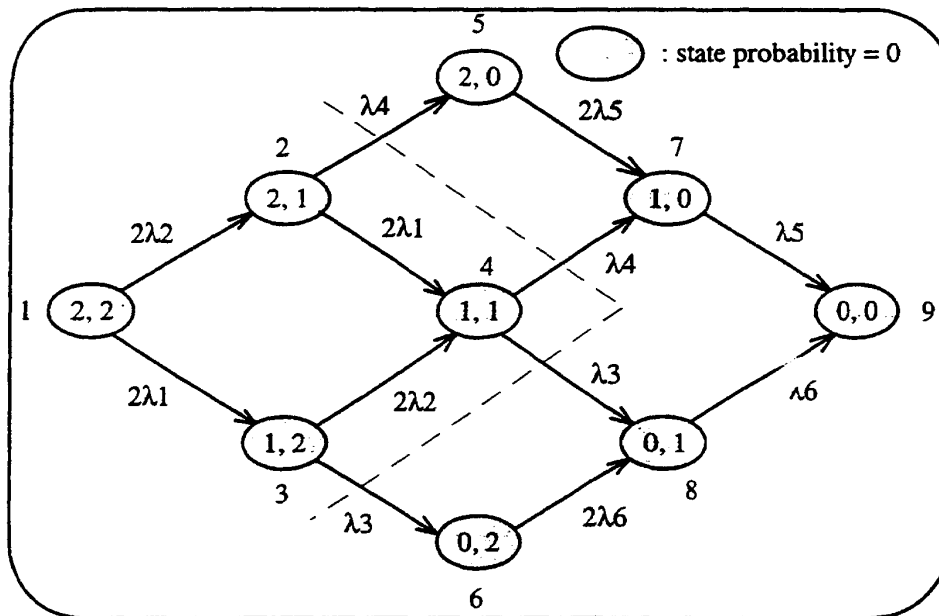FIGURE F19 - Markov Chain for the Two Engine Example

FIGURE F20 - Markov Chain Modification When Left Engine is Brought
to Fully Operational State at the Start of the Next Flight

F.5.2   (Continued):

Similarly, when the right engine is repaired at the end of a flight, then one can know for sure that both controllers in that engine will be fully operational at the start of the next flight. In other words, in the Markov chain at the start of the next flight, the probability of a controller for the right engine failure should be zero. This results in the probabilities of states 2, 4, 5, 7, 8, 9, (shaded lightly in the Figure F21) being initialized to zero at the start of the next flight.

This example shows the usefulness of Markov modeling as it allows the user to specify different maintenance scenarios.
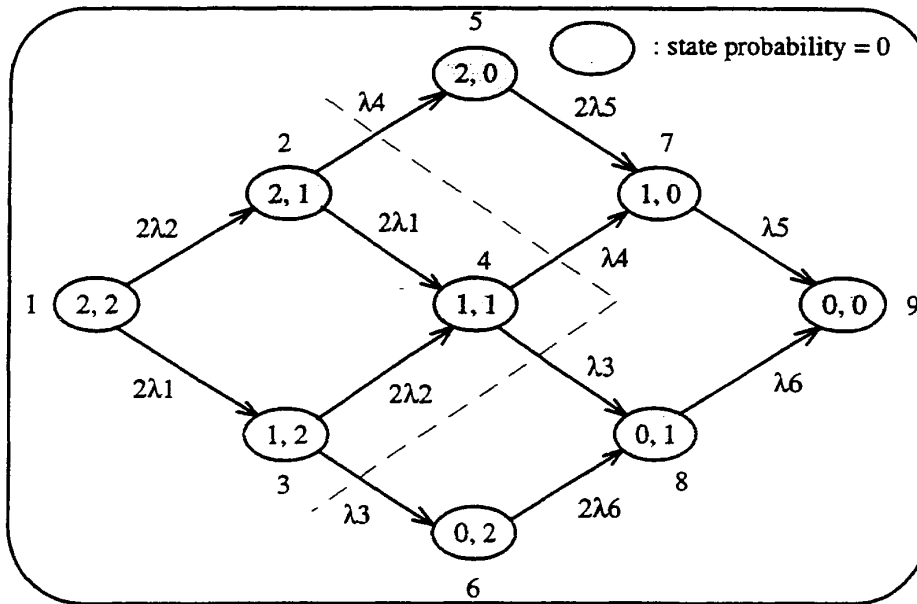
FIGURE F21 - Markov Chain Modification When Right Engine is Brought
to Fully Operational State at the Start of the Next Flight

F.5.3 A Multi-Phase Example:

Consider the same example of two engines as given in the previous section. The system is assumed to be of two phases. In the first phase, the system starts in a state where two controllers on both engines are working perfectly. Now assume that in the second phase, knowing that two controllers on the left engine have failed, one needs to estimate the specific risk of the system. Here specific risk is the subsequent risk on a flight given a known dispatch inoperative condition (i.e., both controllers on left engine have failed). Knowing this, one needs to know how long the system can operate safely, while the aircraft lands at the nearest airport within specified duration.

The phase 1 Markov chain is the same as that shown in Figure F19. In phase 2, since the left engine is assumed to have failed, there are only three states in the system: in the right engine either two, one or zero controllers are working. The resultant Markov chain for phase 2 is shown in Figure F22. The system is assumed to be operational as long as at least one controller on the right engine is working. Since, one is already assuming that left engine has failed at the start of phase 2, states 1, 2, 3, 4, 5 and 7 are initialized to zero at the start of phase 2. The results at the end of phase 2 give the specific risk of the system given the fact that one started a phase in a degraded configuration (left engine being failed).
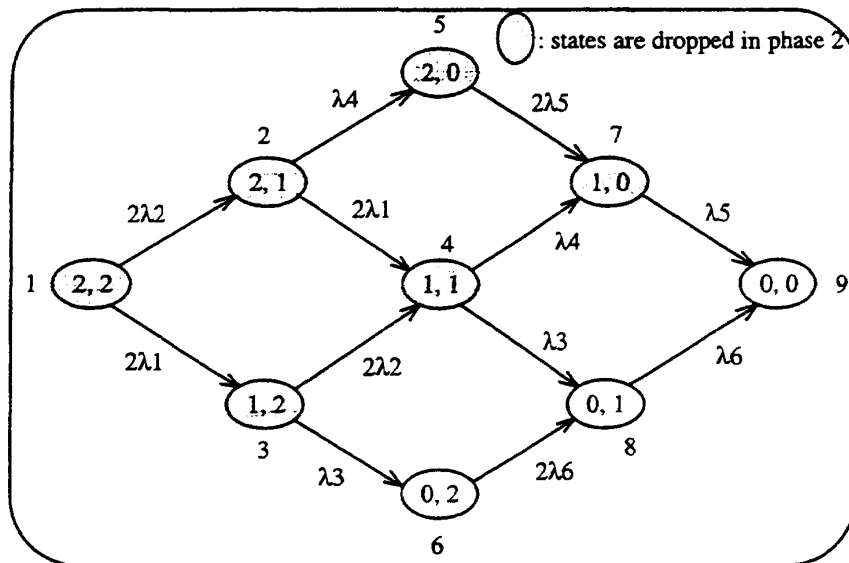
FIGURE F22 - Markov Chain Modification for Phase 2 Configuration
In Phase 2, Shaded States are Dropped from the Markov Chain

F.5.3   (Continued):

The software tools HARP and SURE can be modified to include multi-phase analyses and scheduled maintenance scenarios.

APPENDIX G
FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

G.1   INTRODUCTION:

A Failure Modes and Effects Analysis (FMEA) is a systematic method of identifying the failure modes of a system, item, function, or piece-part and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic or mechanical systems). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode. The results of an FMEA may be used to generate the Failure Modes and Effects Summary (FMES) and are usually used to support the other analysis techniques of the System Safety Assessment (SSA) process such as Fault Tree Analysis (FTA), Dependence Diagram (DD), or Markov Analysis (MA). Combinations of failures are not usually considered as part of the FMEA.

G.2   SCOPE:

An FMEA is performed at a given level (system, item, etc.), by postulating the ways the chosen level's specific implementation may fail. The effect of each failure mode is determined at the given level and usually the next higher level for each operating mode of the equipment. Sometimes an FMEA may be focused toward a specific operating scenario as required to support a top down FTA, DD, or MA.

The FMEA must account for all safety related effects and any other effects identified by the requirements. In cases where it is not possible to identify the specific nature of a failure mode, the worst case effect must be assumed. If the worst case is unacceptable for the fault tree, the failure modes must be examined at the next lower indenture level. (i.e., If the FMEA is being conducted at the functional level, drop to the piece-part level and exclude components with no effect on the event under consideration. If the analysis is being conducted at a piece-part level, drop to consider specific failure mechanisms within the part. Another option is to redesign to improve redundancy or add monitoring.)

Regardless of the level the FMEA is to be performed to, the major steps of an FMEA include preparation, analysis, and documentation.

G.3 FMEA PROCESS:

G.3.1 FMEA Preparation:

The preparation of an FMEA includes determining the customer requirements, obtaining current documentation, and understanding the operation of the function.

It is important to know the customer's expectations and requirements for the FMEA before beginning. If the FMEA requirements are not known, the FMEA may not meet the needs of the requestor and may have to be redone.

Requirements for an FMEA usually originate from a PSSA activity such as an FTA, DD, MA. The analyst needs to know the analysis level (functional versus piece-part), safety related effects, other failure effects and operational modes of interest. An FMEA is used to support the safety assessment process by providing failure rates to quantify the basic event of the FTA, DD, or MA. An FMEA may also be used to support verification of the FTA through a comparison of the FMEA failure modes with the basic events of the fault tree.

The final step before beginning to perform the analysis is to obtain the following information which may be necessary to complete the analysis, or may simplify the analysis activity.

a. FMEA requirements including safety related and requested failure effects and specific operating modes of interest

b. Specifications

c. Current drawings or schematics

d. Parts lists for each system or item

e. Functional block diagrams

f. Explanatory materials including the theory of operation

g. An applicable list of failure rates (G.3.2)

h. The FMEA on the previous generation or similar function

i. Any design changes and revisions that have not yet been included on the schematic (NOTE: Designs may change frequently and having the most up to date material will reduce FMEA updates.)

j. Preliminary list of component failure modes from previous FMEAs, if applicable

NOTE: For FMEAs performed early in the design stage, some of the above information will not be available and assumptions or estimates may have to be made. Detailed documentation of these assumptions must be maintained for traceability and to simplify future updates.

G.3.2 Performing the Analysis:

The analyst needs to review and understand the information gathered during the preparation stage previously described. The analyst will also find it useful to understand the functions that the design being analyzed performs within the next higher level. After the analyst has gained sufficient knowledge, failure modes are identified. Every feasible hardware failure mode is postulated at the level of the design being analyzed. Consideration is given to failure modes of the components or functions that make up the given level. Information to aid in determining the failure modes of the functions or components is provided in G.3.2.1 and G.3.2.2.

Every identified failure mode is analyzed to determine its effect on the given level and usually on higher levels as well. Failure effect categories are created for each different type of effect and a code may be assigned to each effect category. Defining these codes simplified the FMEA worksheet by moving the description of each effect from the worksheet to the body of the report. The FMEA worksheet provides a list of failure modes, effects and rates. Examples of FMEA worksheets are provided in the following sections. Each effect category must have only one higher level effect, otherwise the effect categories must be defined in more detail. For example, if the effect category is originally defined as "causes signal xyz to be out of specification" but an out of specification high condition causes a different effect from an out of specification low condition, then the effect category should be split to "... out of specification high" and "... out of specification low". Similarly if the failure mode is found to cause two higher level effects (e.g., "Loss of signal A" and "Loss of signal B") then these two should be combined to form a new effect category "Loss of both signal A and B".

The means by which the failure is detected is usually determined and documented within the FMEA worksheets. Examples of detection methods include detection by hardware or software monitors, flight crew detection, power up tests, and maintenance checks.

For a quantitative FMEA, a failure rate is assigned to each failure mode. Whenever possible, failure rates should be determined from failure data of similar equipment already in field use. Industry sources of failure rates including MIL-HDBK-217, MIL-HDBK-338, RAC "Nonelectronic Parts Reliability Data". (NPRD) and GIDEP (Government Industry Data Exchange Program), MIL-HDBK-978, and Rome Laboratory's "Reliability Engineer's Toolkit" can also be used. The total failure rate for each failure effect category may be detailed in a summary sheet or is summarized in the Failure Modes and Effects Summary (FMES) (see Appendix H).

There are two basic types of FMEAs, functional and piece-part. Functional FMEAs are typically performed to support the safety analysis effort with piece-part FMEAs performed as necessary to provide further refinement of the failure rate. Piece-part FMEAs are typically done when the more conservative failure rates from a functional FMEA will not allow the system or item to meet the FTA probability of failure budget. A piece-part FMEA may also be useful for systems that rely on redundancy, since a functional FMEA may not reveal single component failures affecting more than one redundant element. Piece-part FMEAs are also useful for safety analysis of mechanical items and assemblies.

G.3.2.1 Functional FMEA: A functional FMEA may be performed at any indenture level. The appropriate level of subdivision is determined by the complexity of the system and the objectives of the analysis. If the required analysis is on a section of circuitry or mechanical devices larger than a particular function, it should be broken down into functional blocks. From an aircraft or system level, this may mean defining each LRU or item as a functional block. From the system or lower levels it may involve breaking down an item into many blocks. The FMEA task is simplified if each block has as few outputs as possible. Once the functional blocks have been determined, a functional block diagram should be created and each block labeled with its functional name. For each functional block, internal and interface functions should be analyzed relative to system operation.

The next step is postulating the failure modes for each functional block. Determine the failure modes by thinking about the intent of the functional block and trying to determine how that function might fail regardless of the specific parts used. The analyst must know the operation of the functional block well enough to be positive that no significant failure modes have been overlooked, including single component failures that could affect more than one redundant functional block. Often, given a clear description of the block's function, many of the failure modes will become apparent.

Following is a simple example of functional failure modes:

The power supply circuitry that generates the 5V can be called a functional block. Some examples of functional failure modes would be as follows.

a. Loss of 5V
b. Voltage less than 5V
c. Voltage greater than 5V
d. Noise on 5V
e. Short to ground or other voltage

There may be other failure modes based on circuit implementation.

The effect of each failure mode is determined by considering how the function fits into the overall design. Failure effect categories are generally created for each effect type and a failure effect category code is assigned. All failure modes that cause this identical effect are assigned to the effect category. The effect category code can then be entered into the FMEA worksheet for each failure, as shown in Table G1. Software and fault monitoring must be considered when determining failure effects and means of detection. As part of this analysis, the analyst must also verify that the monitoring can indeed detect the failure mode. In order to properly perform this analysis, the analyst must have detailed knowledge of the system requirements and software design including internal fault management techniques as applicable.

If a quantitative analysis is being performed, a failure rate is assigned to each failure mode. One technique is to perform a failure rate prediction for each block and apportion the failure rate across the various failure modes based on past experience of similar functions or other sources allowing determination of probability of occurrence. Guidance for failure distribution of component parts is provided in G.3.2.2.1.

TABLE G1 - Functional FMEA Worksheet

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

System:	FMEA Description:	Date:
Subsystem:		Sheet of
Item ATA:	FTA References:	File:
	Author:	Rev:

FUNCTION NAMES	FUNCTION CODE	FAILURE MODE	MODE FAILURE RATE	FLIGHT PHASE	FAILURE EFFECT	DETECTION METHOD	COMMENTS

Note: May be revised to fit analysis level and program needs.

G.3.2.1   (Continued):

The results of the functional FMEA are recorded in a worksheet similar to Table G1. This example table can be modified to meet program needs. Different requirements may result in addition or deletion of some of the information. The analyst should ensure that the FMEA form and content meets the specific needs of the requester before beginning the analysis.

As the analysis progresses, the following should be informally recorded for future maintenance of the FMEAs and to assist in resolving questions regarding the FMEA.

a.   Justification of each failure mode
b.   Rationale for the assigned failure rate
c.   Rationale assigning a particular failure to a failure effect category
d.   Documentation of any assumptions made

This documentation is usually not included in the FMEA report but is retained for reference.

G.3.2.2   Piece-Part FMEA: A piece-part FMEA is similar to a functional FMEA except that instead of analyzing at the functional or block diagram level, the failure modes of each individual component contained in the item or function are analyzed. A piece-part FMEA can be used to determine the failure effects of potential electrical, electronic, or mechanical failures. For example, the effect of failures of a resistor or a motor shaft can be considered as part of a piece-part FMEA. Piece-part FMEAs on electronic equipment are usually performed only as necessary when the more conservative results of a functional FMEA will not allow the item to meet the FTA probability of failure budget. This is due in part to the difficulty in determining the failure modes for complex components.

The first step in a piece-part FMEA is to create a list of all components to be covered by the FMEA. The next step is to determine the failure modes of each component type. This is the most difficult part of the piece-part FMEA, particularly FMEAs performed on electronic items containing complex integrated circuits. Determining all the failure modes of any but the simplest components (where industry data is available) is extremely difficult and sometimes impossible. When in doubt the worst case assumptions of part failure modes must be made. Information to assist in determining component failure modes is contained in G.3.2.2.1.

Once a component's piece-part failure modes have been determined, they are entered into the FMEA worksheet as shown in Table G2. This example worksheet can be modified to meet individual needs. Different requirements may result in addition or deletion of some of the information in the worksheet. The analyst should ensure that the FMEA form and content meets the specific needs of the requester before beginning the analysis.

TABLE G2 - Piece-Part FMEA Worksheet

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

System:		FMEA Description:		Date:
Subsystem:				Sheet of
Item ATA:		FTA References:		File:
Function:		Author:		Rev:

PART NUMBER	PART TYPE	FAILURE MODE	MODE FAILURE RATE	FLIGHT PHASE	FAILURE EFFECT	DETECTION METHOD	COMMENTS

Note: May be revised to fit analysis level and program needs.

G.3.2.2 (Continued):

The next step is to determine the effect of the failure on the next higher level assembly and assign a failure effect category to the failure. Failure effect codes may be assigned to each category to simplify the table. The detailed description of each failure effect category can then be included in the text of the report. All failure modes that cause this identical effect are assigned to the effect category. The effect category code can then be entered into the FMEA worksheet for each failure, as shown in Table G2. Software and fault monitoring must be considered when determining failure effects and means of detection. As part of this analysis, the analyst must also verify that the monitoring can indeed detect the failure mode. In order to properly perform this analysis, the analyst must have detailed knowledge of the system requirements and software design including internal fault management techniques as applicable.

If a quantitative analysis is being performed, a failure rate is assigned to each failure mode. Guidance for failure distribution of component parts is provided in G.3.2.2.1.

As the analysis progresses, the following should be informally recorded for future maintenance of the FMEAs and to assist in resolving questions regarding the FMEA.

a. Justification of each failure mode
b. Rationale for the assigned failure rate
c. Rationale assigning a particular failure to a failure effect category
d. Documentation of any assumptions made

This documentation is usually not included in the FMEA report but is retained for reference.

G.3.2.2.1 Determining Piece-Part Failure Modes and Failure Distributions: When conducting piece-part FMEAs, it may be necessary to further break down the failure rates for components to identify percentages of failure rates applicable to specific failure modes. Guidance for this may be obtained from industry documents such as RAC "Failure Mode/Mechanism Distributions" (FMD), MIL-HDBK-978, and Rome Laboratory's "Reliability Engineer's Toolkit" which provide this information for many component types.

Typical failure modes to consider include, but are not limited to, the following:

a. Open
b. Short
c. Parameter shifts
d. Out of adjustment
e. Dielectric breakdown
f. Intermittent operation
g. Inoperative
h. Spurious operation
i. Wear
j. Mechanical failure
k. Sticking
l. Loose
m. Fracture

In general, the function of the component must be considered and all potential ways that the component can fail to perform that function correctly must be considered for inclusion in the list of component failure modes. Unintended function of the component must also be considered. The documents referenced above provide a good basis to allow the analyst to determine potential failure modes of the components being analyzed. Engineering judgment is a necessary part of the failure mode determination process.

While the failure rate and mode source documents provide a basis for failure modes of some component types, there will be many device types that are not included in these documents. This is especially true for complex digital ICs which need to be considered on a part by part basis. Determining the failure modes of digital devices generally requires engineering judgment and it is unlikely that all of the failure modes can be determined for a complex digital IC.

A method for estimating the failure modes of complex digital devices is to model the digital devices under consideration with constituent functional blocks for which a better definition of failure modes may exist. Identify the pin level effects of possible failures of the functional blocks as the device failure modes if possible. Some faults may affect multiple pins and various combinations of pins. Particular attention must be paid to potential component failure modes that may lead to the FTA basic events.

G.3.2.2.1 (Continued):

Trying to determine the actual failure mechanisms and the associated effects through a physics of failure approach is not recommended for ICs as it forces the analyst to perform an "FMEA" on each digital IC. This "FMEA" may be more complex than the higher level FMEA being completed and may not even be possible for complex ICs. In addition, an undisclosed design enhancement by the chip manufacturer could render the entire effort obsolete. Complex IC failure modes can include intermittent faults and various fault combinations possibly affecting multiple pins.

Failure modes of other component types are more readily available than for ICs. However, a look at several sources will yield different failure mode distributions for the same component type and sometimes even different failure modes. This points out that even for simple components it is difficult to determine which potential failure modes are valid and which ones cannot happen.

G.3.2.3 Substantiation: If the analytical method of determining failure effects for a failure mode is difficult, laboratory verification should be performed if possible. It is desirable for all significant failure effects to be verified by test. For electrical or electronic systems, faults can be inserted by opening leads or shorting leads together or to ground. If device outputs can be tri-stated, logic combinations can be easily inserted. Unfortunately, the most difficult failure modes to analyze are sometimes difficult to confirm through testing. For example, it is impossible to insert all faults for most ICs. Computer aided design software may also be used to simulate failures. This software allows the equivalent of the fault to be inserted into the circuit simulation and the failure effect determined.

Analysis of failures during testing and in actual use can also be used to substantiate the results of the FMEA. This failure data can also be used to create a library of failure modes for future FMEAs.

G.4 DOCUMENTATION:

G.4.1 FMEA Report:

The report for an FMEA should include:

a. A document number allowing the report to be referenced by the FMES, FTA or similar analysis.

b. An introduction containing a brief statement about the purpose and the objective of the FMEA.

c. A brief overview of operation and a block diagram.

d. A section describing the analysis approach. (This section should include a description of how the analysis was performed, definitions of the levels used, and a listing of pertinent assumptions.)

G.4.1(Continued):

    e. A complete listing of the results of the FMEA. (FMEA forms similar to the examples included in G.3.2.1 and G.3.2.2 can be used.)

    f. Identifying part numbers and revision status of hardware, software and firmware analyzed.

    g. Appendices should also include the following items.

        (1) Drawings or schematic diagrams

        (2) Any failure mode distributions for lower level components defined during analysis or obtained from other sources (Include justification for all modes considered.)

        (3) A list of failure rates and failure rate source used in the analysis

G.4.2 FMEA Checklist:

The following checklist will ensure that the correct steps are taken in the proper order to perform a cost effective and accurate FMEA.

    1. Obtain written specification of requirements, if possible, from customer or requester defining:

        (a) failure effects of interest,
        (b) outputs to be considered,
        (c) allowable failure detection methods,
        (d) final report format,
        (e) schedule.

    2. Prepare for the analysis by:

        (a) obtaining and understanding documentation,
        (b) generating parts lists,
        (c) partitioning equipment into sub levels and documenting the partitioning,
        (d) collecting failure modes of components if a piece-part analysis is required.

    3. Perform detailed analysis by:

        (a) determining failure modes and assigning failure effect codes,
        (b) avoiding poorly defined failure modes so that confusion will not occur when going from the current level to higher levels,
        (c) determining detection means, if required, for each failure effect category,
        (d) making detailed notes documenting why a failure category was assigned.

    4. Verify analysis conclusions (with lab or aircraft data if possible) for any issues in question.

    5. Write the final report.

G5. DETECTION COVERAGE ANALYSIS FOR TEST PROCESSES AND MONITORING:

This type of analysis is useful to determine how effective various test processes are at the detection of latent faults.

The method used to accomplish this involves an examination of the applicable failure modes to determine whether or not their effects are detected, and to determine the percentage of failure rate applicable to the failure modes which are detected. The possibility that the detection means may itself fail latent should be accounted for in the coverage analysis as a limiting factor (i.e., coverage cannot be more reliable than the detection means availability).

Inclusion of the detection coverage in the FMEA can lead to each individual failure that would have been one effect category now being a separate effect category due to the detection coverage possibilities. Another way to include detection coverage is for the FTA to conservatively assume that no holes in coverage due to latent failure in the detection method affect detection of all failures assigned to the failure effect category of concern. The FMEA can be revised is necessary for those cases where this conservative assumption does not allow the top event probability requirements to be met.

APPENDIX H
FAILURE MODES AND EFFECTS SUMMARY (FMES)

NOTE: The basic ARP 4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

H.1   INTRODUCTION:

A Failure Modes and Effects Summary (FMES) is a summary of lower level failure modes with the same effects from the Failure Modes and Effects Analyses (FMEAs). The FMES is used as an input to the Fault Tree Analysis (FTA) or other analyses. The failure effects from the FMEA are failure modes for the FMES. The higher level effect is listed in the effect column of the FMES. Identical failure effects from the FMEA are categorized as one mode in the FMES.

The failure rate for each failure mode in the FMES is the sum of the failure rates coming from the failure modes of the individual FMEA(s). An FMES need not necessarily be a separate analysis; it can be done as a part of an FMEA. The FMES is an aid to simplify the FTAs (reduce the number of OR-gates at the lowest level) and to combine the effects of item failures and failures of the installation that have the same effect as one single event. For calculation of failure rates, it should be remembered that an FMEA considers single failures, whereas an FTA considers both single failures and combinations of failures.

The relationship between the FMEAs and FMES is shown in Figure H1.

H.2   SCOPE:

This FMES appendix contains the background information and procedural guidelines necessary for an analyst to perform an FMES and to provide visibility of the benefits of compiling an FMES.

H.3   FMES PROCESS:

H.3.1   FMES Preparation:

The preparation for the FMES includes determining the customer requirements, obtaining applicable FMEA data and understanding the operation of the system or item being analyzed. It is important to know and understand the customer requirements for the FMES. Furthermore, all FMEA(s) and the relevant supporting material (drawings, parts lists, etc.) have to be available.

Circuit X FMEA

Failure Mode	Failure Rate	Failure Effect
R5 Open	A	Loss of +5V
R5 Short	B	5V tied to GND

Circuit Y FMEA

Failure Mode	Failure Rate	Failure Effect
C5 Short	C	5V tied to GND
C5 Open U58 P2 Open	D	

Item FMES

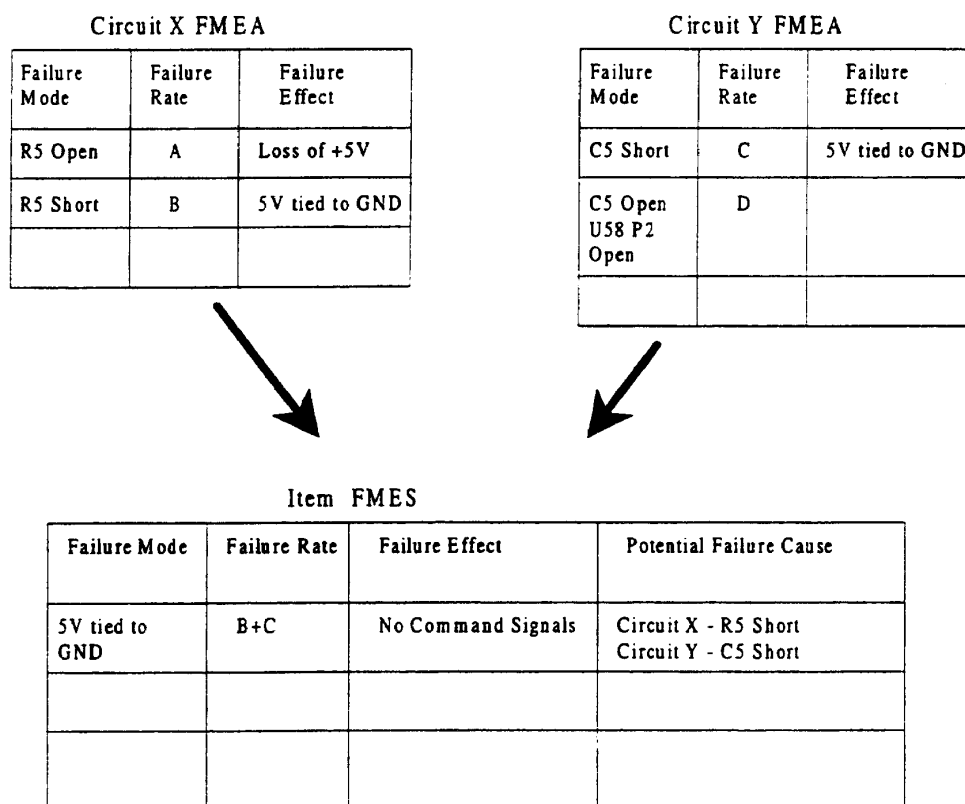| Failure Mode	Failure Rate	Failure Effect	Potential Failure Cause
5V tied to GND	B+C	No Command Signals	Circuit X - R5 Short Circuit Y - C5 Short

FIGURE H1 - Example of FMEAs and FMES Relationship

H.3.2   Performing an FMES:

The analyst should review the existing FMEA(s), and check all failure effects for consistency, (i.e., is the same failure effect always described with the same wording and does different wording for the failure effect always mean a different failure?). This check should be done with special care when an FMES on the system level is performed (i.e., summarizing effects from installation failure modes and item failure modes). The failure effect from the FMEAs is entered in the "FAILURE MODE" column of the FMES form similar to the example shown in Table H1. Note that the FMES form may be altered to add or delete specific data entries as necessary to support the specific FMES customer requirement and the specific FMEA format being used.

Identify all failure modes having the same failure effect and sum their individual failure rates. The calculated failure rate is entered in the "FAILURE RATE" column of the FMES. The references to the individual failure mode in the FMEA may be identified in the FMES "CAUSAL FAILURE" columns. The effect of the failure mode on the next higher level, the systems of that failure and the relevant phase of flight may also be entered in the relevant columns of the FMES form.

TABLE H1 - FMES Worksheet

FAILURE MODES AND EFFECTS SUMMARY (FMES)

Aircraft:
ATA:
System:
Subsystem or Unit:

FMES-No.:
Supplier:
Supplier's Part Number/
Supplier's Drawing Ref:

Date:
Sheet   of
Rev:
Prepared by:

REF	FAILURE MODE	FAILURE RATE	PHASE	EFFECTS ON SYSTEM	SYMPTOMS 1. Flight Crew 2. Ground Crew	1. CAUSAL FAILURE 2. REMARKS	CAUSAL FAILURE REF	CHECK REF	FAILURE CONDITION REF

Note: May be revised to fit analysis level and program needs.

SAE ARP4761

H.4 DOCUMENTATION:

Each FMES report should include the following information.

a. A brief description of the system or item being analyzed, giving design philosophy, including monitoring devices and principle design features (This should be supported by suitable diagrams, schematics, and block diagrams.)

b. A listing of primary and secondary system or item functions

c. A list of references, part numbers, and revision identification to identify the hardware and software releases analyzed

d. A section containing a concise description of the results of the analysis

e. A list of failure rate sources

f. References to FMEAs used to generate the FMES

The results are documented in FMES tables providing an uncluttered overview of the results of the FMEA. See Table H1 for an example FMES Worksheet format. The summary should present top level failure effects and means of detection. Also included are flight phase information and detection method.

APPENDIX I
ZONAL SAFETY ANALYSIS (ZSA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

I.1   INTRODUCTION:

Historically, the system safety analysis was conducted purely on the basis of system schematics. This approach did not sufficiently recognize the implications of the physical installation of the system hardware which could significantly impair the independence between items. Therefore, an analysis was defined which allows consideration of installation aspects of individual systems/items and the mutual influence between several systems/items installed in close proximity on the aircraft. This analysis is called the Zonal Safety Analysis (ZSA).

A ZSA should be carried out for each zone of the aircraft. The partitioning of an aircraft into zones is a task which is accomplished in order to perform the ZSA, and also to evaluate maintenance operations. Figure I1 shows an example of such aircraft zoning.

The ZSA should be carried out during the whole development process of a new aircraft or of any major modification to an existing aircraft. Initially, basic design and installation guidelines are generated, and drawings or models are analyzed. As the project progresses the analysis is based on mock-ups and then the aircraft. The analysis will generally be performed by the airframe manufacturer. The conclusions of the ZSAs should provide inputs to the relevant SSAs for the aircraft and complement the lower level analyses in the SSA. This appendix presents a representative ZSA process. The ZSA section of appendix L gives examples of associated guidelines, and checklists.

The Common Mode Analysis, the Zonal Safety Analysis and the Particular Risk Analysis constitute the Common Cause Analysis.

Crown-ECS–Distribution
Flight Deck-Flight Deck-Panels & Modules
Passenger Compartment-Payloads–Linings

Floors-Elec–Wiring Installation
E/E Bay-Elec–Panels & Cargo Handling

Cargo Compartment-Payloads–Systems
A/C & Mix Bay-ECS–A/C, Temp Control, etc.
Landing Gear-Mech/Hyd Systems–Landing Gear Actuation
Wings/Wheel Well-Mech/Hyd Systems–Hydraulic Installation
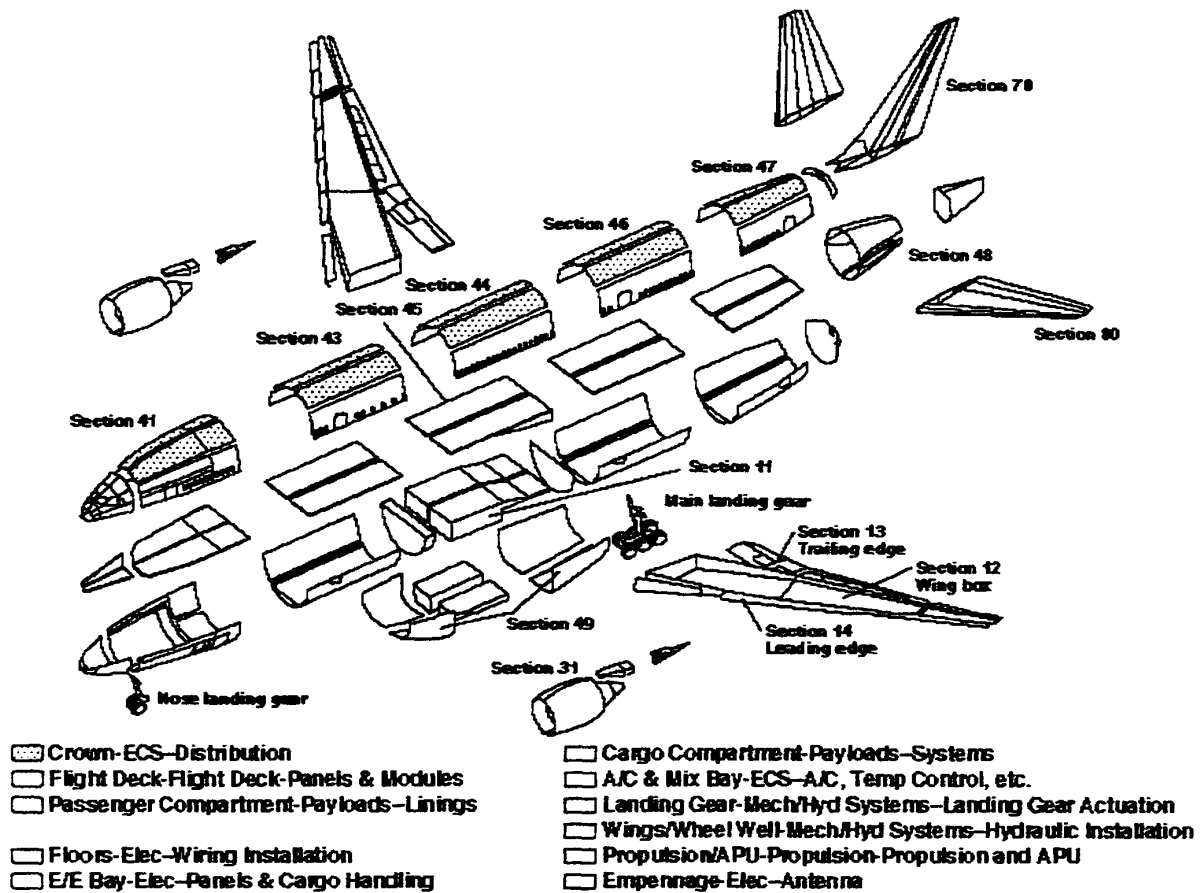Propulsion/APU-Propulsion-Propulsion and APU
Empennage-Elec–Antenna

FIGURE I1 - Example of Aircraft Zones

I.2   SCOPE:

This appendix contains the information and procedural guidelines necessary for an experienced
engineer to establish an adequate set of design and installation guidelines and to perform a ZSA.

I.3   ZSA PROCESS:

The objective of the Zonal Safety Analysis is to ensure that the system design and installation meets safety objectives with respect to:

a.   The basic standards of design and installation.
b.   The effect of failures on the aircraft.
c.   The implication of maintenance errors.
d.   The verification that the design meets the FTA event independence claims.

The analysis can use the aircraft zones defined for maintenance purposes. Figure I2 shows which tasks should be done for such an analysis.

The Zonal Safety Analysis is primarily a qualitative analysis which comprises three separate main tasks.

I.3.1   Preparation of Design and Installation Guidelines:

The first task, which is independent of the zone itself, is the preparation of design and installation guidelines for each new aircraft project. For derivative aircraft modifications, the guidelines of the baseline aircraft should be used as much as possible.

The design and installation guidelines should consider aircraft level requirements and considerations from the PSSAs. Maintenance errors should also be considered. The guidelines can be grouped into general guidelines, system specific design and installation guidelines or zone specific design and installation guidelines. All these types of guidelines should be generated by the appropriate group responsible for the design, and approved by all organizations involved.

I.3.2   Inspection of the Installation in the Zone:

The second task is to inspect each zone of the aircraft against these guidelines for conformity to the guideline recommendations. The results should be recorded for future reference on the program and for an example for future programs.

I.3.3   Inspect for Systems/Items Interference:

The third task starts with the preparation of a list of systems/items within each zone of the aircraft. This list can be based on installation drawings, mock-ups, or the aircraft depending on the phase of the project. For these systems/items, a list of failure modes which could have an effect on other systems/items installed in the vicinity (systems/items external failure modes) should be established. This list can be based on the FMEAs and FMESs of the systems/items, and on the knowledge of systems/items intrinsic hazards.

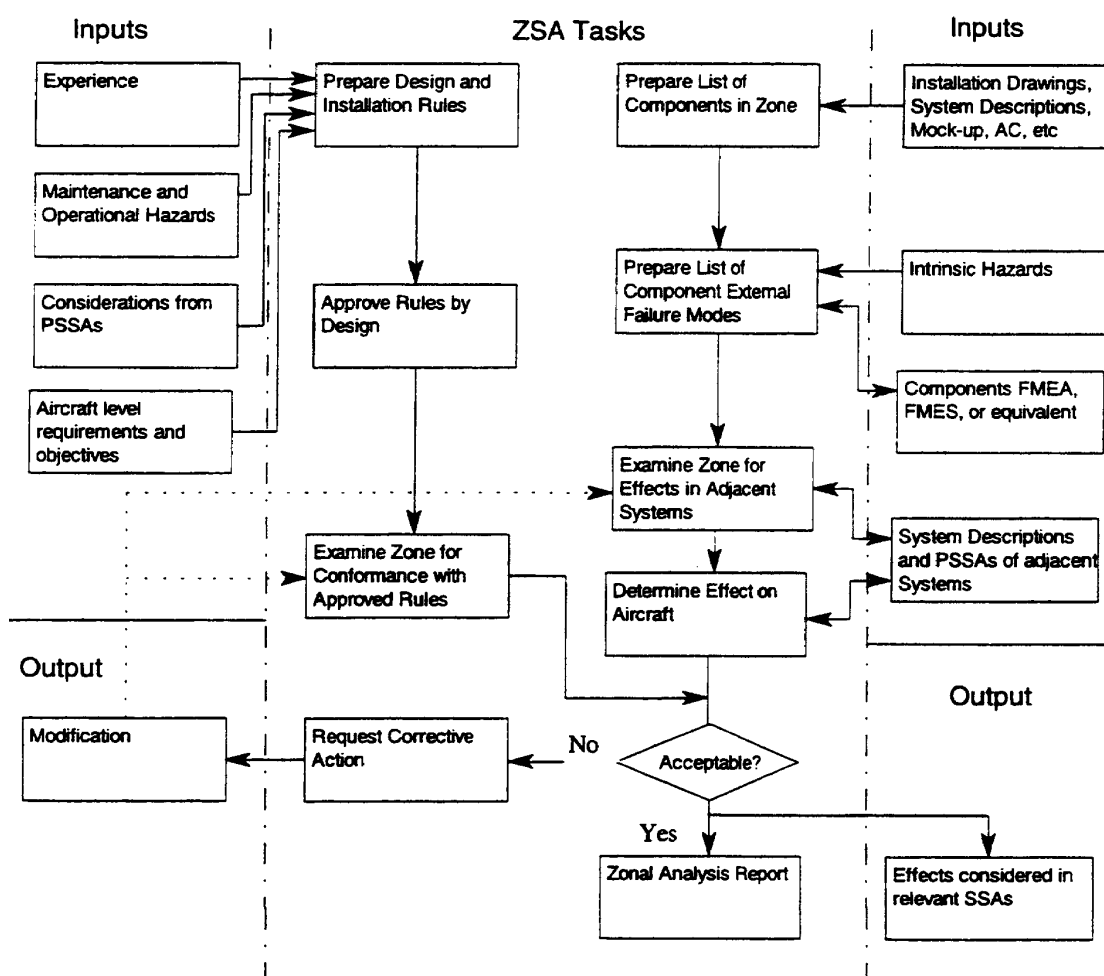Inputs | ZSA Tasks | Inputs

Experience → Prepare Design and Installation Rules

Maintenance and Operational Hazards

Considerations from PSSAs → Approve Rules by Design

Aircraft level requirements and objectives

Prepare List of Components in Zone ← Installation Drawings, System Descriptions, Mock-up, AC, etc

Prepare List of Component External Failure Modes ← Intrinsic Hazards

Components FMEA, FMES, or equivalent

Examine Zone for Effects in Adjacent Systems

Examine Zone for Conformance with Approved Rules

Determine Effect on Aircraft

System Descriptions and PSSAs of adjacent Systems

Output

Modification ← Request Corrective Action ← No ← Acceptable?

Yes ↓

Zonal Analysis Report

Output

Effects considered in relevant SSAs

FIGURE I2 - Zonal Safety Analysis Process

I.3.3   (Continued):

The failure modes of the systems/items, the external failure effect, and the resulting effect on the aircraft should be considered by an FMEA-type analysis. The effect of these failure modes on the adjacent systems should be judged based on the system description, PSSA or equivalent. The described effect on the aircraft should be compatible with the relevant SSA. The SSA should consider the system/item external failure effects as a common cause failure in different systems. The FTA is one method for accomplishing this task.

I.3.3   (Continued):

The results of the inspection of the zone against the design and installation guidelines and the resulting effects on aircraft of systems/items external failures should be documented in the ZSA report. Any acceptable results should be used in the relevant SSAs. Any deviation from the design guidelines should be seen as a candidate for design change. Deviations should result in a design change or justification of the deviation.

I.4   DOCUMENTATION:

Records of the analysis should be made on a day to day basis. In addition to working systematically through the checklist, the following details should be included.

a. How, when and by whom the assessment was made (i.e., mock-ups, aircraft, etc.)

b. The correct identification of any equipment that is highlighted as a potential problem

c. Any deviations from the guidelines, or any significant failures resulting from later interaction of systems or maintenance errors

d. The manner in which problems highlighted by the analysis have been resolved (giving reference to associated documents)

The system/item external failures and their implications should be analyzed and listed. References should be given for the source of the failure mode, the rationale for the failure effect on the adjacent system and the reference to the relevant SSA which describes the effect on the aircraft.

Any problem or deviation should be brought to the attention of the responsible design organization and should be considered for design change.

The preliminary results of each section of analysis should be submitted to the relevant departments of the project organization. The ZSA report should be prepared from the "day to day" records and should summarize the above data. As it is a living document and provides an input to the SSA of the aircraft, it should be reissued periodically throughout the design cycle.

APPENDIX J
PARTICULAR RISKS ANALYSIS (PRA)

NOTE: The basic ARP4761 document contains information which places the information in this
        appendix in context. This appendix should be used in conjunction with the main body of the
        document.

J.1   INTRODUCTION:

Particular risks are events or influences which are outside the system(s) concerned but which
may violate event independence claims. These particular risks may also influence several zones
at the same time, whereas the Zonal Safety Analysis (ZSA) is restricted to each specific zone.
Some of the risks may be subject to specific airworthiness requirements (e.g., engine non-
contained rotor failures, tire burst, etc.).

Typical risks would include, but are not limited to the following.

a. Fire
b. High energy devices (non-containment):
    (a) Engine
    (b) APU
    (c) Fans
c. High pressure bottles
d. High Pressure Air Duct Rupture
e. High Temperature Air Duct Leakage
f. Leaking fluids: (Usually examined as part of the Zonal Safety Analysis, but may sometimes
    require specific additional assessment)
    (1) Fuel
    (2) Hydraulic
    (3) Battery acid
    (4) Water
g. Hail, ice, snow
h. Bird strike
i. Tire burst, flailing tread
j. Wheel rim release
k. Lightning strike
l. High Intensity Radiated Fields
m. Flailing shafts
n. Bulkhead rupture

Having identified the appropriate risks with respect to the design under consideration, each risk
should be subject to a separate study based on this appendix. The objective of the relevant
analysis is to ensure that any safety related effects are either designed out or shown to be
acceptable.

J.1   (Continued):

The Particular Risk Analysis (PRA) should be carried out throughout the aircraft development process for a new aircraft. It should also be carried out for any major modification to the aircraft. Initially, drawings or models should be analyzed, but as the project progresses, the analysis should be based on mock-ups and then the actual aircraft. The analyses will usually be performed by the airframe manufacturer.

The Common Mode Analysis, the Zonal Safety Analysis and the Particular Risk Analysis constitute the Common Cause Analysis.

J.2   SCOPE:

This appendix contains the information and procedural guidelines necessary to enable an experience engineer to develop an adequate failure model for the particular risk under investigation, define the affected zones and review the consequences of the particular risk.

J.3   PRA PROCESS:

The PRA is usually performed on a risk by risk basis. It is primarily a qualitative analysis which is performed by doing the following:

a.   Define the details of the particular risk to be analyzed. (e.g., tire/wheel burst)

b.   Define the failure model to be used for the analysis. (e.g., tire burst model and wheel burst model)

c.   List the requirements to be fulfilled. (e.g., FAR/JAR 729(f))

d.   Define the affected zones/areas. (e.g., landing gear bays)

e.   Define the affected systems/items. (cross-check with ZSA)

f.   Define the design and installation precautions taken. (cross-check with design and installation guidelines used in the ZSA)

g.   Review the consequences of the particular risk on the affected items. (cross-check with FMEA/PSSAs)

h.   Review the effect of the particular risk on the aircraft due to failure modes of items or their combinations. (cross-check with SSAs)

J.3   (Continued):

  i.   Determine if the consequences are acceptable.

     (1) If yes, prepare justification for certification and use in the SSA or other specific certification documentation.
     (2) If no, initiate a design change.

J.4   DOCUMENTATION:

The review of the consequences for each particular risk is documented in a format which should include the following information:

a.   The description of the analyzed particular risk.
b.   The items which are affected by the particular risk.
c.   The zones where the items are installed.
d.   The failure modes caused by the particular risk under investigation.
e.   The resulting effect on the aircraft and the classification of that effect.

The effect on the aircraft should be cross-checked with the relevant PSSA/SSA. Furthermore, ensure that the PRA and PSSA/SSA "Effect on Aircraft" and "Classification" entries are in agreement. The PRA results should be included in the relevant PSSAs/SSAs.

Additionally the following details should be included:

a.   Any deviations from the initial assumptions.

b.   The manner in which problems highlighted by the analysis have been resolved.

References should be made to the specific documentation which describes the effect of the external threat on the aircraft.

Any problem uncovered during the PRA process should be brought to the attention of the responsible design organization.

APPENDIX K
COMMON MODE ANALYSIS (CMA)

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

K.1   INTRODUCTION:

The Common Mode Analysis (CMA) is performed throughout the safety assessment process. The CMA is a qualitative analytical tool used to ensure the "goodness" of a design. Design experience is used to inspect the integration of components in a logical way. This practice is carried out at all levels from item design to aircraft level design. The analysis includes an evaluation of the components within an item (Component/Item level CMA) and of how they fit into the larger system (System/Aircraft level CMA).

This document describes CMAs as being performed based on inputs from the FHA and PSSA, and to provide substantiation for the SSA. Given this precondition, CMAs are performed to verify that ANDed events in the Fault Tree Analysis (FTA), Dependence Diagrams (DD) and Markov Analysis (MA) are truly independent. The effects of design implementation, manufacturing and maintenance errors, and failures of system components which defeat redundant design principles should be analyzed. Generally speaking, the CMA contributes to the verification that independence principles have been applied when necessary. For example, considerations should be given to the independence of functions and their respective monitors. Also, items with identical hardware and/or software could be susceptible to generic faults which could cause malfunctions in multiple items.

The Common Mode Analysis, the Zonal Safety Analysis and the Particular Risk Analysis constitute the Common Cause Analysis.

K.2   SCOPE:

This appendix provides guidance on conducting a CMA. The process described may be used at item, system or aircraft levels.

K.3   COMMON MODE ANALYSIS PROCESS:

The following four steps summarize the CMA process as shown in Figure K1.

1.   Establish program specific checklists (specific Common Mode Types, Sources, and Failure/Errors checklist) (see K.3.1).

2.   Identify the CMA requirement (see K.3.2).

3.   Analyze the design to ensure it meets the requirements identified in step 2 above (see K.3.3).

4.   Document the results of the first three steps of the CMA process (see K.4).

Figure K1 describes the general process to perform a CMA at a System/Aircraft level. The process may be adapted to provide guidance for CMA at a Component/Item level.

K.3.1   List/Checklist:

The CMA process is based on analyzing design and implementation for elements that may defeat the redundancy or independence of functions within the design. This analysis is performed by the application of checklists. Wherever required redundancy or independence is compromised, justification for the acceptability or elimination of the compromise is required.

The following common modes are examples of those which should be considered in this activity.

a.   Software development errors
b.   Hardware development errors
c.   Hardware failures
d.   Production/repair flaw
e.   Stress related events (e.g., abnormal flight conditions, abnormal system configurations)
f.   Installation errors
g.   Requirement errors
h.   Environmental factors (e.g., temperature, vibration, humidity, etc.)
i.   Cascading faults
j.   Common external source faults

K.3.1.1   General Common Mode Types, Sources and Failures/Errors Checklist: There are many elements which may be considered by the CMA. Table K1 provides examples of general common mode types, example sources, and example failures/errors which should be considered. Project specific CMA checklists should be derived based on the example data and previous experience (common knowledge or experience in similar aircraft). The level of detail of these checklists depends upon the degree of complexity or novelty of the technology or system under study.
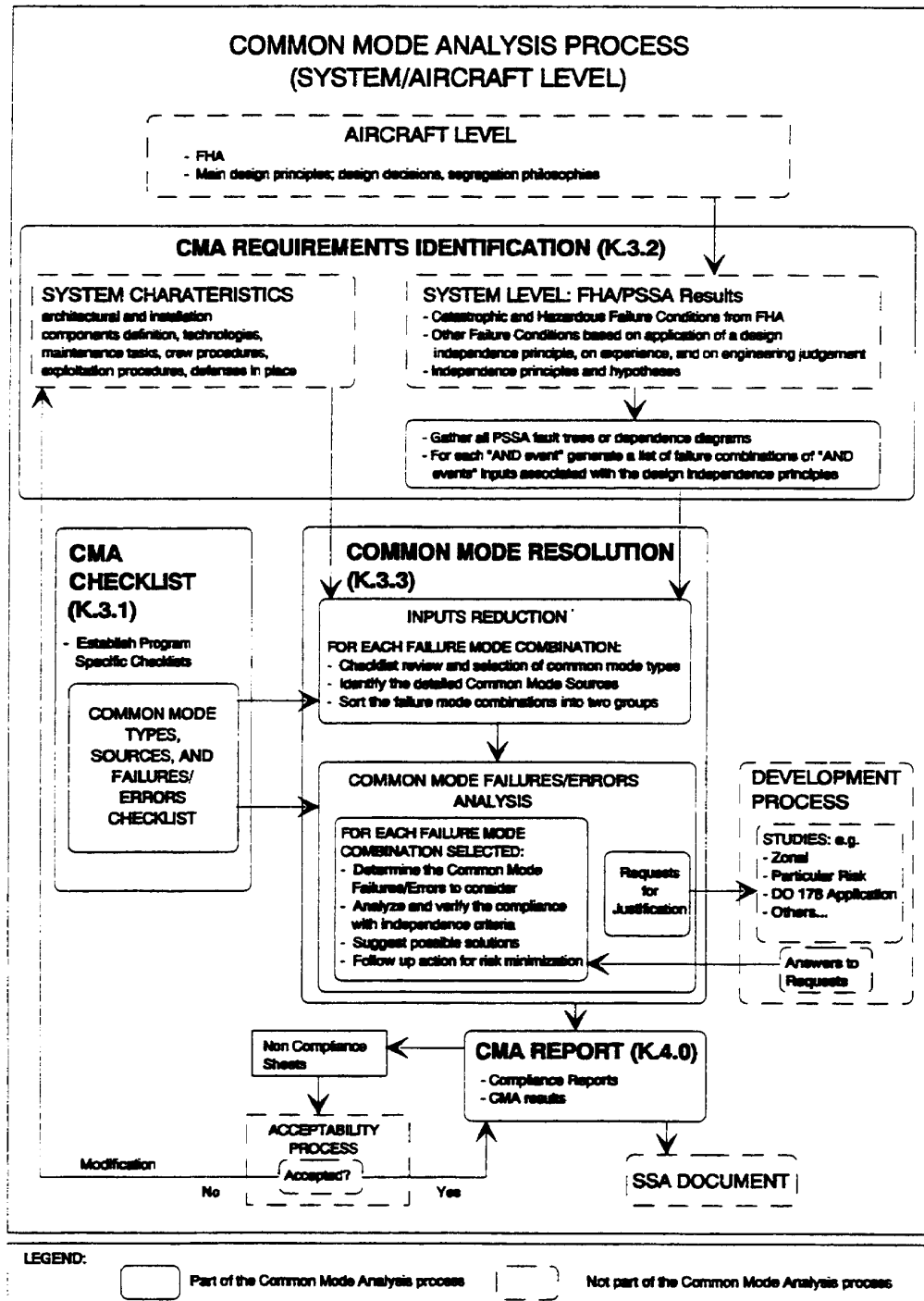
COMMON MODE ANALYSIS PROCESS
(SYSTEM/AIRCRAFT LEVEL)

AIRCRAFT LEVEL
- FHA
- Main design principles; design decisions, segregation philosophies

CMA REQUIREMENTS IDENTIFICATION (K.3.2)

SYSTEM CHARATERISTICS
architectural and installation
components definition, technologies,
maintenance tasks, crew procedures,
exploitation procedures, defenses in place

SYSTEM LEVEL: FHA/PSSA Results
- Catastrophic and Hazardous Failure Conditions from FHA
- Other Failure Conditions based on application of a design independance principle, on experience, and on engineering judgement
- Independance principles and hypotheses

- Gather all PSSA fault trees or dependence diagrams
- For each "AND event" generate a list of failure combinations of "AND events" inputs associated with the design independence principles

CMA CHECKLIST (K.3.1)
- Establish Program Specific Checklists

COMMON MODE TYPES, SOURCES, AND FAILURES/ ERRORS CHECKLIST

COMMON MODE RESOLUTION (K.3.3)

INPUTS REDUCTION
FOR EACH FAILURE MODE COMBINATION:
- Checklist review and selection of common mode types
- Identify the detailed Common Mode Sources
- Sort the failure mode combinations into two groups

COMMON MODE FAILURES/ERRORS ANALYSIS
FOR EACH FAILURE MODE COMBINATION SELECTED:
- Determine the Common Mode Failures/Errors to consider
- Analyze and verify the compliance with independence criteria
- Suggest possible solutions
- Follow up action for risk minimization

Requests for Justification

DEVELOPMENT PROCESS
STUDIES: e.g.
- Zonal
- Particular Risk
- DO 178 Application
- Others...

Answers to Requests

Non Compliance Sheets

CMA REPORT (K.4.0)
- Compliance Reports
- CMA results

ACCEPTABILITY PROCESS
Accepted?
Modification No Yes

SSA DOCUMENT

LEGEND: Part of the Common Mode Analysis process | Not part of the Common Mode Analysis process

FIGURE K1 - CMA Process

TABLE K1 - Example of a General Common Mode Types, Sources and Failures/Errors Checklist

Common Mode Types	Common Modes Sub-types	Examples of Common Mode Sources	Examples of Common Mode Failures/Errors
CONCEPT AND DESIGN	DESIGN ARCHITECTURE	Common discharge header	Common discharge failure
		Common external sources (ventilation, electrical power, ...)	Failure of common sources (ventilation, electrical power, ...)
		Equipment Protections	Designer failure to predict an event, ...
		Operating Characteristics (normally running, standby, ...)	...
		Others	...
	TECHNOLOGY, MATERIALS, EQUIPMENT TYPE	New/ Sensible technology	General design error, ...
		Component type (size, material, ...)	Hardware error, ...
		Common Software	Software error, ...
		Component Use	...
		Internal Conditions (temperature or pressure ranges, ...)	Usage out of operating ranges, ...
		Initial Conditions	...
		Others	...
	SPECIFICATIONS	Specification Origin	Origin error (human), lack of specific protection in equipment design, ...
		Same Specification	Defective specification, ...
		Others	...
MANUFACTURING	MANUFACTURER	Common Manufacturer	Common error due to manufacturer, error due to inadequately trained personnel, ...
		Others	...
	PROCEDURES	Same Procedure	Incorrect procedure, ...
		Others	...
	PROCESS	Same Process	Incorrect process, Inadequate manufacturing control, inadequate inspection, inadequate testing, ...
		Other	...

TABLE K1 (Continued)

Common Mode Types	Common Modes Sub-Types	Examples of Common Mode Sources	Examples of Common Mode Failures/Errors
INSTALLATION/ INTEGRATION AND TEST	FITTER	Common Fitter	Installation error due to fitter, ...
		Others	...
	PROCEDURES	Installation phase	Common error due to phase, ...
		Others	...
	LOCATION	Same zone	Local failure or event, ...
		Others	...
	ROUTING	Same Routing	Local event, ...
		Others	...
OPERATION	STAFF	Common Staff	Error due to inadequately trained personnel, over stressed or disabled operator, ...
		Others	...
	PROCEDURES	Same Procedure	Faulty operating procedures, misdiagnosis (following wrong procedure), omission of action, incorrect or inadequate commission of action, ...
		Others	...
MAINTENANCE	STAFF	Common Staff	Error due to inadequately trained personnel, incorrect human action, ...
		Others	...
	PROCEDURES	Same Procedure	Failure to follow repair procedures, defective repair procedure, lack of repair procedures, ...
		Others	...
TEST	STAFF	Common Staff	Error due to inadequately trained personnel, incorrect human action, ...
		Others	...
	PROCEDURES	Same Procedure	Faulty test procedure, ...
		Others	...
CALIBRATION	STAFF	Common Staff	Error due to inadequately trained personnel, ...
		Calibration Tools	Inadequate tools adjustment, ...
		Others	...

TABLE K1 (Continued)

Common Mode Types	Common Modes Sub-Types	Examples of Common Mode Sources	Examples of Common Mode Failures/ERrors
	PROCEDURES	Same Procedure	Failure to follow calibration procedures, defective calibration procedure, lack of calibration procedures, ...
		Others	...
ENVIRONMENTAL	MECHANICAL AND THERMAL	Temperature	Fire, lightning, welding, etc., cooling system faults, electrical short circuits, ...
		Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, ...
		Impact	Pipe whip, water hammer, missiles, structural failure, ...
		Vibration	Machinery in motion, earthquake, ...
		Pressure	Explosion, out of tolerance system changes (pump overspeed, flow, blockage), ...
		Humidity	Steam pipe breaks, ...
		Moisture	Condensation, pipe rupture, rainwater, ...
		Stress	Thermal stress at welds of dissimilar metals, thermal stresses, ...
		Others	...
	ELECTRICAL AND RADIATION	Electromagnetic	Welding equipment, rotating electrical machinery, lightning, ...
		Radiation	Gamma radiation, charged particle radiation, ...
		Conducting Medium	Moisture, conductive gases, ...
		Out-of-tolerance	Power surge voltage, short circuit, power surge current, ...
		Others	...
	CHEMICAL	Corrosion (acid)	Leak of acid used in maintenance for removing rust and cleaning, ...
		Corrosion (oxidation)	Moisture around metals
	MISCELLANEOUS	Other Chemical Reactions	Galvanic corrosion, complex interactions of fuel cladding, water, oxide fuel, ...
		Biological	Poisonous gases, animate causes (mussels in heat exchanger), ...
		Others	...

K.3.2   CMA Requirements Identification:

In order to perform a CMA, the analyst needs to know and understand the subject system characteristics with regard to system operation and installation. These characteristics include such things as the following:

a.   Design architecture and installation plan
b.   Equipment and components characteristics
c.   Maintenance and test tasks
d.   Crew procedures
e.   Systems, equipment and software specifications

Additionally, the analyst needs to know system characteristics with regard to safeguards utilized to eliminate or minimize common mode effects. These include the following:

a.   Diversity (dissimilarity, redundancy, etc.) and barriers
b.   Testing and preventive maintenance programs
c.   Design control and design quality level
d.   Review of procedures or specifications
e.   Training of personnel
f.   Quality control

With the above system background, the analyst must next determine the specific CMA analysis requirements for the product under investigation. There are two distinct processes used to develop CMA requirements as identified in the following discussion. Usually both processes must be followed to establish complete application specific CMA requirements.

K.3.2.1   CMA Requirements from FTA, DD and MA: These requirements are derived by examining the analyses that support the FHA and PSSA. The process is described below.

a.   For each Hazardous or Catastrophic event documented in the FHA and/or PSSA, identify each AND event (AND-gate in fault tree) and determine the associated design independence principle.

b.   Examine the AND events from the previous step to determine which failure combinations must be assured to be independent.

c.   Document all derived CMA requirements resulting from the above analysis.

K.3.2.2   Other CMA Requirements: There are likely to be CMA requirements not derivable from the FTA, DD, or MA, these requirements stem from the specific product CMA checklists (see K.2.1), and product or engineering experience. These requirements are derived by reviewing the checklists against the design process, design detail, selected components, manufacturing processes, installation processes, and maintenance processes in use. As this review and evaluation progresses, each identified condition which could contribute to a common mode event is reduced to a CMA requirement and documented in the requirement listing. Examples of CMA requirements which may not be apparent from the fault trees are generic failures in complex components, environmental considerations, physical component locations, etc.

K.3.3   Common Mode Failure/Error Resolution:

For each CMA requirement in K.3.2, the following CMA process steps are followed:

a.   Determine the potential common mode failures/errors associated with each source.

b.   Analyze each potential common mode failure/error to verify compliance with independence criteria.

c.   In case of non acceptance at CMA level, suggest possible solutions and initiate design correction.

d.   Follow up on corrective actions, determine acceptability of resultant design.

K.4   DOCUMENTATION:

The output of a Common Mode Analysis is the CMA Report. This report is expected to include the following:

a.   Reference documents, drawings, and support material used in the analysis.

b.   List of derived requirements guiding the CMA

c.   Description of system/component analyzed

d.   Rationale for compliance with CMA requirements

e.   Identification of problems/concerns identified during analysis if applicable.

f.   Resolution of identified problems/concerns (corrective action or justification for acceptance)

g.   Conclusion/result of CMA

K.4.1   Link With FHA, PSSA and SSA:

The Common Mode Analysis uses results of FHA/PSSA assessments such as list of Catastrophic Failure Conditions, Independence Criteria considered in the design, and any directives for CMA performance. A summary of the results of the common mode analysis is included in the SSA. Any remaining common modes should be included in the relevant FTA, DD or MA reports.

K.4.2   Link With Zonal Safety and Particular Risk Analyses:

Particular Risk Analysis and Zonal Safety Analysis are not specifically part of the CMA. However, it is impossible to ignore potential common mode effects from these sources. Where Zonal Safety or Particular Risk Analysis identify potential common mode concerns, the CMA analyst should, where possible, ensure that the concerned Particular Risk or Zonal Safety Analysis covers the identified problem.

APPENDIX L
CONTIGUOUS SAFETY ASSESSMENT PROCESS EXAMPLE

NOTE: The basic ARP4761 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body and the other appendices of the document.

L.1   INTRODUCTION:

L.1.1   Scope:

This appendix describes, in detail, a contiguous example of the safety assessment process for a fictitious aircraft design. In order to present a clear picture, a function was broken down into a single item of a single system. A function was chosen which had sufficient complexity to allow use of all the methodologies, yet was simple enough to present a clear picture of the flow through them. This function/system/item was analyzed using all the methods and tools described in the rest of this ARP document. Each method was employed to show how it may be applied. In practice, for example, one might choose FTA, DD or MA to aid in determining potential causes of functional faults. However, all three methods are employed here to give the reader an understanding of their similarities and differences. The methodologies applied here are an example of one way to utilize the principles defined in the document. Other formats may be used to accomplish the documentation, so long as the principles outlined in the text of this ARP are followed.

This example contains references to all documentation that a company may use to assure itself of the safety of its products. Some of these documents are submitted to the regulatory agencies for the purpose of certification (e.g., the Wheel Brake System FHA). Other documents are internal to the company and not required for certification (e.g., the S-18 Design Requirements Document). No implication is made that these documents should all be submitted to a regulatory agency and none should be implied. Safety and Certification are not synonymous terms. We are trying to show here the process for safety assessment, including those processes that go beyond certification requirements.

L.1.2   Acronym List for Appendix L Example:

ACCU	Accumulator
ALT	Alternate
APU	Auxiliary Power Unit
AS	Anti Skid
B	Blue Hydraulic System
BSCU	Brake System Control Unit
C	Capacitor
CMD	Command
COMP	Computation
CSMG	Constant Speed Motor Generator
ECS	Environmental Control System
ELEC	Electric

L.1.2   (Continued):

    EMI   Electromagnetic Interference
    HIRF   High Intensity Radiated Fields
    HYD   Hydraulic
    IC   Integrated Circuit
    I/O   Input/Output
    CAT IIIb   Category 3b All Weather Landing System
    CPU   Central Processing Unit
    F.R.   Failure Rate
    G   Green Hydraulic System
    L or LH   Left or Left Hand
    LRU   Line Replaceable Unit
    MLG   Main Landing Gear
    MON   Monitor
    MT   Periodic Maintenance Task
    NLG   Nose Landing Gear
    NORM   Normal
    PCU   Power Control Unit
    POS   Position
    P/S   Power Supply
    PTU   Power Transfer Unit
    PWM   Pulse Width Modulator
    PWR   Power
    R or RH   Right or Right Hand
    R   Resistor
    REF   Reference
    RTO   Rejected Takeoff
    STBY   Standby
    SYS   System
    VDC   Volts Direct Current
    V1   Speed from which the aircraft cannot be safely stopped on remaining runway
    WBS   Wheel Brake System

L.1.3   Outline:

The function chosen is analyzed using the methods described in the appendices. The order of the methods presented represents a nominal course of their development through the design cycle. However, the CCA activity is shown at the end of this example, whereas in the process flow, it occurs throughout the process. (See Figures 1, 2 and 3 of the ARP4761 Main document).

The outline of the example is as follows.

   a. Aircraft FHA
      (1) Preliminary Aircraft FTA
   b. Wheel Brake System (WBS) FHA
   c. PSSA

L.1.3   (Continued):

      (1) WBS FTA, DD, MA
      (2) BSCU FTA, DD, MA
    d. SSA
      (1) BSCU FMEA
      (2) BSCU FMES
      (3) BSCU CMA
      (4) BSCU FTA, DD, MA
      (5) WBS FMES
      (6) WBS FTA, DD, MA
      (7) WBS Integration Cross-Check
    e. CCA (the BSCU CMA is addressed under SSA section to improve continuity of the example)
      (1) ZSA (Wheel Well Zone)
      (2) PRA (Tire Burst)
      (3) WBS CMA

As each new section begins, please read at the top of the page the "NOTE" which will change to describe that particular section. In this way, the reader will always be able to tell exactly where he/she is in the safety assessment process. For example:

NOTE: Aircraft FHA
NOTE: PSSA, BSCU FTA

Each section of the Example will be written to look like a submittable document. Although many different formats may be acceptable to the certification authorities, our examples will use the following format:

1.0   Introduction
2.0   References
3.0   Function/System Description
4.0   Analysis
4.1   (As required to support analysis write-up)
4.2   (As required to support analysis write-up)
4.2.1 (As required to support analysis write-up)
4.2.2 (As required to support analysis write-up)
5.0   Conclusion

Editorial comments are provided in italics. Where necessary, the reader will be directed to the appropriate appendix for further guidance on the process involved.

L.1.4   Description of the Example Function:

The aircraft function analyzed is: "Decelerate aircraft on the ground (stopping on the runway)". This example concentrates on the aircraft braking system, the details of which are evolved through the following example approximately as they would in a real life situation.

L.1.5   List of Figures for Appendix L:

L.1.5   (Continued):

L.1.5   (Continued):

NOTE: Aircraft FHA

Aircraft Functional Hazard Assessment (FHA) for the S18 Aircraft

1.0   INTRODUCTION

This analysis comprises the functional hazard assessment of the functions of the "S18" aircraft. This is a fictitious aircraft which was created for this document. The operation of all systems employed to accomplish the functions of the aircraft were considered.

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable FHA appendix paragraph.)

Aircraft FHA Paragraph #	Appendix A Paragraph #
4.1	A.3.1
4.2	A.3.2
4.3	A.3.3
4.4	A.3.4, A.3.6
4.5	A.3.7
4.6	A.4

2.0   REFERENCES

1) S18 Aircraft Design Requirements Document
2) FAR/JAR 25.1309
3) ARP4754 "Certification Considerations for Highly-Integrated or Complex Aircraft Systems"
4) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"

3.0   DESCRIPTION SUMMARY

The S18 aircraft is a four engine passenger aircraft designed to carry 300 to 350 passengers up to 5000 nautical miles at .86 mach. The average flight length is 5 hours.

(Editor's Note: The other initial features defining this aircraft would be included in this paragraph, but are not described for the sake of brevity. These features are generally developed from the marketing and business decisions made during the initial marketing effort.)

4.0   RESULTS OF THE AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (FHA)

4.1   Identified Functions

Figure 4.1-1 depicts the Aircraft functions in a simple tiered hierarchy format.

(Editor's Note: The "Control Aircraft on the Ground" function is broken down in this example. From this decomposition, the "Decelerate Aircraft on the Ground" function is pursued in the Aircraft FHA example. The function being analyzed is identified in column (1) of an example FHA form shown in Table 4.1-1.)

FIGURE L1

NOTE: Aircraft FHA
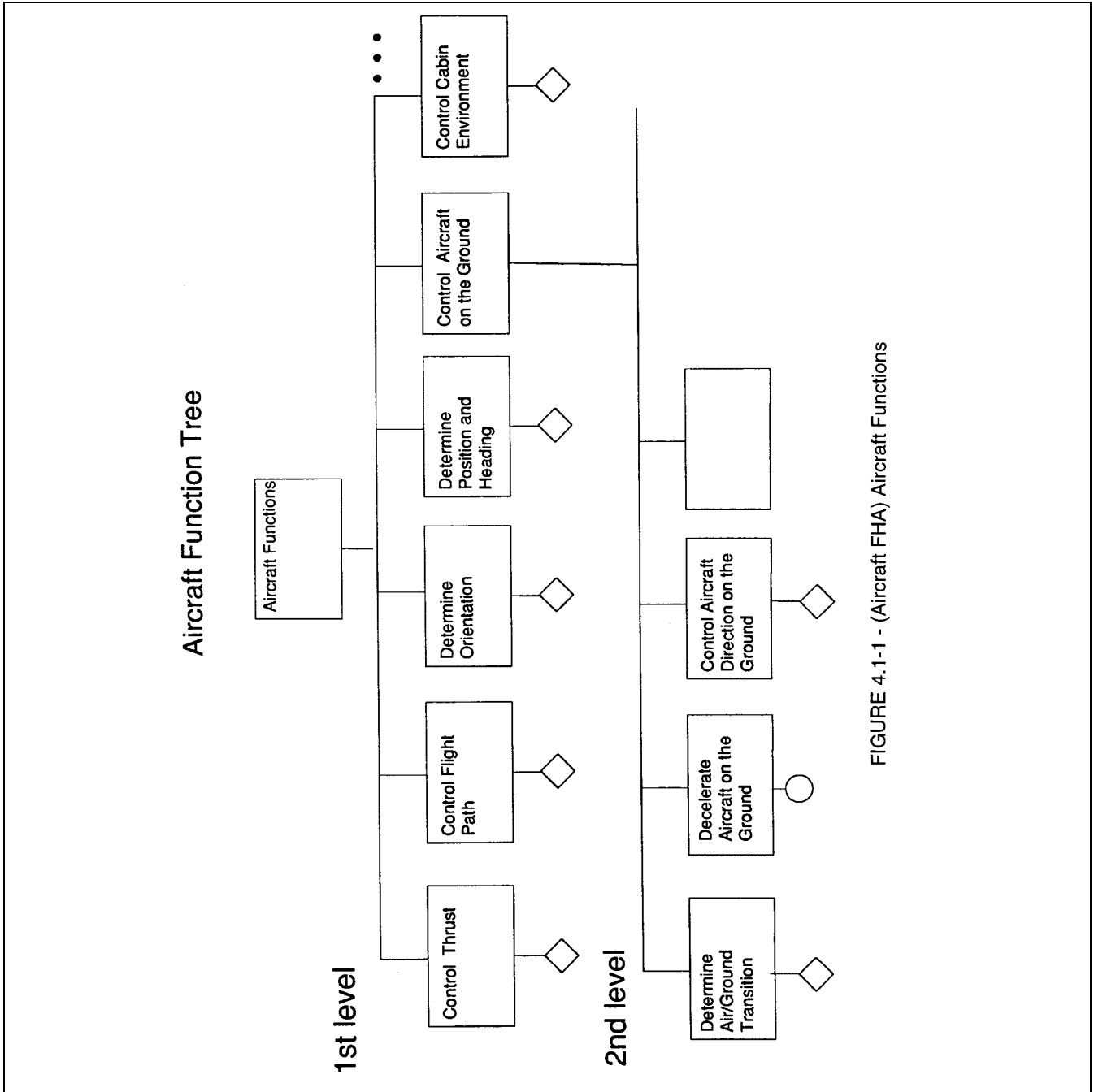
FIGURE 4.1-1 - (Aircraft FHA) Aircraft Functions

FIGURE L1 (Continued)

SAE ARP4761

NOTE: Aircraft FHA

4.2 Identified Failure Conditions

For the function "Decelerate Aircraft on the Ground" the following set of failure conditions and assumptions for the assessment were determined.

4.2.1 Functional Failure Conditions

    a. Loss of all deceleration capability
    b. Reduced deceleration capability
    c. Inadvertent deceleration
    d. Loss of all auto stopping features
    e. Asymmetrical Deceleration

4.2.2 Environmental and Emergency Configurations and Conditions

    a. Runway Conditions (Wet, icy, etc.)
    b. Runway Length
    c. Tail/Cross Wind
    d. Engine Out
    e. Hydraulic System Loss
    f. Electrical System Loss

4.2.3 Applicable Phases

    a. Taxi
    b. Takeoff to Rotation
    c. Landing Roll
    d. Rejected Takeoff (RTO)

4.2.4 Interfacing Functions

    a. Air/Ground Determinations
    b. Crew Alerting (Crew warnings, alerts, messages)

Columns (2) and (3) of Table 4.1-1 show that part of the FHA form which contains the formulated failure conditions for this given function.

4.3 Effects of Failure Condition on the Aircraft, Crew and Occupants

For each failure condition, the effects of the failure condition on the aircraft and crew are shown in column (4) of Table 4.1-1.

FIGURE L1 (Continued)

NOTE: Aircraft FHA

4.4   Classify/Justify the Effects the Failure Condition has on the Aircraft and Crew

For each failure condition, the classification of the failure condition is defined in Columns (5) and (6) of Table 4.1-1.

4.5   Plan for the Verification of Safety Objectives

For each failure condition, the plan for the verification of safety objectives is defined in Column (7) of Table 4.1-1. This column lists the references to requirements, fault trees, analyses, and or tests.

FIGURE L1 (Continued)

NOTE: Aircraft FHA

TABLE 4.1-1 - Aircraft FHA *(Partial - addresses only "Decelerate Aircraft on the Ground")*

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
Decelerate Aircraft on the Ground	Loss of Deceleration Capability	Landing /RTO/ Taxi	See Below			
	a. Unannunciated loss of deceleration capability	Landing /RTO	Crew is unable to decelerate the aircraft, resulting in a high speed overrun.	Catastrophic		S18 Aircraft Fault Tree
	b. Annunciated loss of deceleration capability	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun.	Hazardous	Emergency landing procedures in case of loss of stopping capability	S18 Aircraft Fault Tree
	c. Unannunciated loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.	Major		
	d. Annunciated loss of deceleration capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No Safety Effect		
	Inadvertent Deceleration after V1 (Takeoff/RTO decision speed)	Takeoff	Crew is unable to takeoff due to application of brakes at the same time as high thrust settings, resulting in a high speed overrun.	Catastrophic		S18 Aircraft Fault Tree

FIGURE L1 (Continued)

NOTE: Aircraft FHA

TABLE 4.1-1 - Aircraft FHA (Cont.) *(Partial - addresses only "Decelerate Aircraft on the Ground")*

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
	Partial loss of Deceleration Capability	Landing /RTO	See Below			
	a. Unannunciated partial loss of deceleration capability	Landing /RTO	Crew is unable to completely decelerate the aircraft before the end of the runway resulting in a potential overrun.	Hazardous		S18 Aircraft Fault Tree
	b. Annunciated partial loss of deceleration capability	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun.	Major		
	c. Unannunciated partial loss of deceleration capability	Taxi	Crew may not be able to adequately stop the aircraft before obstacle, resulting in low speed collision.	Minor		
	d. Annunciated partial loss of deceleration capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No Safety Effect		
	Loss of automatic stopping capability	Landing /RTO	See below			

FIGURE L1 (Continued)

NOTE: Aircraft FHA

TABLE 4.1-1 - Aircraft FHA (Cont.) *(Partial - addresses only "Decelerate Aircraft on the Ground")*

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
	a. Unannunciated loss of automatic stopping capability	Landing /RTO	Crew arms automatic stopping features for landing/RTO. Upon landing/RTO the automatic stopping features fail to operate. Crew recognizes situation and manually activates stopping capability. Crew reaction time results in potential overrun.	Major		
	b. Annunciated loss of automatic stopping capability	Landing /RTO	Crew manually activates stopping capability upon landing or RTO.	No Safety Effect		
	Asymmetric Deceleration	Landing /RTO	See Below			
	a. Unannunciated asymmetric deceleration	Landing /RTO	Crew is not prepared for asymmetric deceleration and reacts too late to maintain directional control, resulting in an offside excursion from the runway.	Major		
	b. Annunciated asymmetric deceleration	Landing	Crew is prepared for asymmetric deceleration and counters with appropriate rudder & nose wheel steering inputs.	Minor		
	c. Asymmetric deceleration	Taxi	Aircraft diverts slightly from intended course	No Safety Effect		

FIGURE L1 (Continued)

NOTE: Preliminary Aircraft FTA

4.6   Aircraft FHA Outputs

(Editor Note: The aircraft level FHA and associated fault tree give a preliminary set of failure conditions and associated requirements to consider at the system level. These failure conditions and requirements will be validated and updated during the system level FHA.)

Based on the FHA safety objectives, architectural decisions were made during the conceptual design phase. These architectural decisions are the basis for the preliminary aircraft fault tree shown in Figure 4.6-1.

The requirement of 1E-9 per flight hour for "Unannunciated loss of deceleration capability" results from the failure condition classification of catastrophic. This requirement is equivalent to a requirement of 5E-9 per flight, since the average flight length is 5 hours.

The requirements of 5E-7 per flight for "Unannunciated loss of all speed brakes on contaminated runway" and for "Unannunciated loss of all wheel brakes" result from the classification of these failure conditions as Hazardous (this classification is equivalent to 1E-7 per flight hour). These classifications are based on knowledge and experience with these system failures conditions. These requirements result in a requirement probability of 1E-6 per flight (i.e., 2x5E-7 per flight hr.) at the next higher level of "Unannunciated loss of effective wheel braking".

As shown in Figure 4.6-1, the allocation of the above requirements allows the budget for "Unannunciated loss of thrust reversers" to be set at 5E-3 per flight. This is 5E-9 divided by 1E-6.

Figure 4.6-1 also shows a fault tree leg associated with inadvertent deceleration after V1. Three aircraft systems can exhibit failure conditions that cause an inadvertent deceleration after V1. Each of the failure conditions is classified as Catastrophic and must meet 1E-9 per flight hour or 5E-9 per flight.

However, since they are only catastrophic during a specific phase of flight operation, their "per hour" requirements need to be factored. The factor is the average flight length of 5 hours divided by the at risk time (15 seconds would be a conservative estimate of the time from V1 to rotation).

Hence, the hourly failure rate requirement for each is 1E-9/flt hr * 5 flt hrs/flt * 1 flt/0.25 min * 60 min/1 hr = 1.2E-6/hr

The probability requirements after converting them to failure rate requirements would read as follows:

a. Inadvertent Thrust Reverse after V_1 1.2E-6 per hour
b. Inadvertent spoiler deployment after V_1 1.2E-6 per hour
c. Inadvertent wheel braking after V_1 1.2E-6 per hour
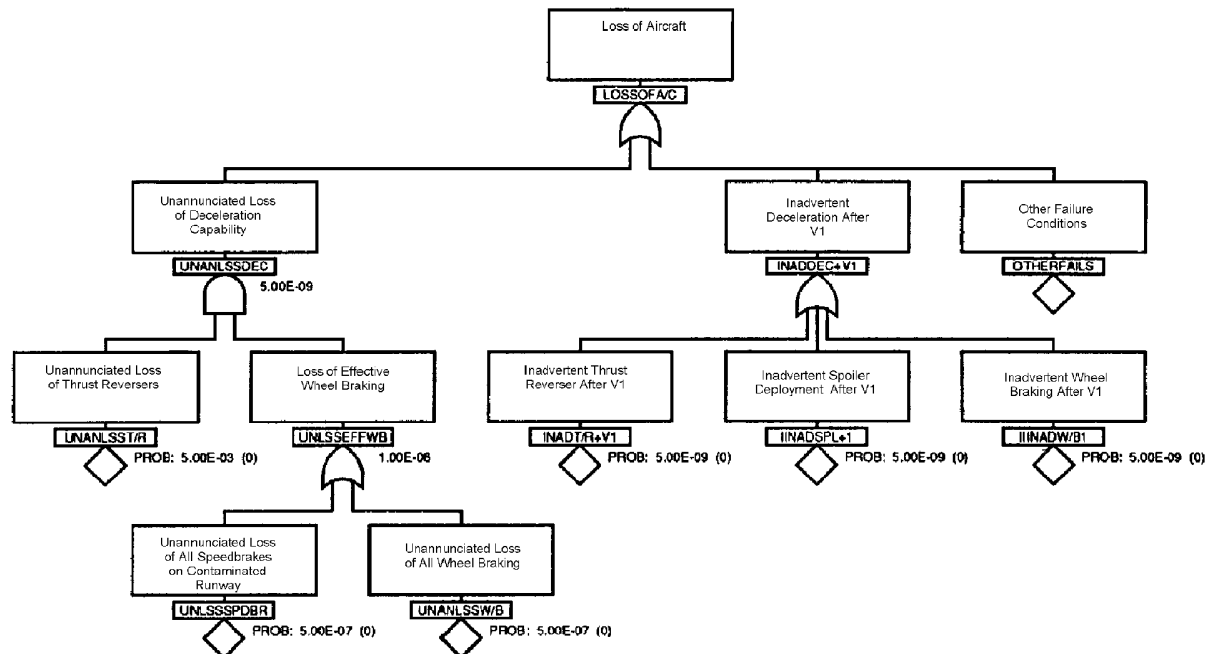
FIGURE L1 (Continued)

NOTE: Preliminary Aircraft FTA

FIGURE 4.6-1 (Aircraft FHA) Preliminary Aircraft Fault Tree

FIGURE L1 (Continued)

NOTE: System FHA

Wheel Brake System Functional Hazard Assessment (FHA)

1.0   INTRODUCTION

This analysis comprises the functional hazard assessment for the Wheel Brake System of the S18 aircraft. The Wheel Brake System must meet two safety design objectives based on the architectural design decisions made in conjunction with the development of the aircraft level FHA. These are stopping the wheel rotation on the ground and stopping wheel rotation in the wheel well.

(Editor's Note: The function of stopping wheel rotation on the ground is analyzed in this example because it corresponds with the aircraft function to decelerate the aircraft on the ground.)

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable FHA appendix paragraph.)

System FHA Paragraph #	Appendix A Paragraph #
4.1	A.3.1
4.2	A.3.2
4.3	A.3.3
4.4	A.3.4, A3.6
4.5	A.3.7
4.6	A4.0

2.0   REFERENCES

1) Aircraft Functional Hazard Assessment for the S18 Aircraft
2) Preliminary S18 Aircraft FTA
3) S18 Aircraft Design Requirements and Objectives Document

3.0   SYSTEM DESCRIPTION

The primary purpose of the wheel braking system is to decelerate the aircraft on the ground without skidding the tires. The wheel braking system performs this function automatically upon landing or manually upon pilot activation. In addition to decelerating the aircraft, the wheel braking system is used for directional control on the ground through differential braking, stopping the main landing gear wheel rotation upon gear retraction, and preventing aircraft motion when parked.

FIGURE L2

NOTE: System FHA

4.0   RESULTS OF THE WHEEL BRAKE SYSTEM FUNCTIONAL HAZARD ASSESSMENT

4.1   Identified Wheel Brake System Functions

The wheel brake system performs the following functions.

a. Decelerate the wheels on the ground
    (1) Manual activation
    (2) Automatic activation
    (3) Antiskid
b. Decelerate the wheels on gear retraction
c. Differential braking for directional control
d. Prevent aircraft from moving when parked

(Editor's Note: For the purpose of this example, the "Decelerate the wheels on the ground" function is analyzed. The function is identified in column (1) of an example FHA form shown in Table 4.1-1.)

4.2   Identified Failure Conditions

For the function "Decelerate the wheels on the ground", the following set of failure conditions and assumptions for the assessment were determined.

4.2.1   Functional Failure Conditions

    a. Total Loss of Wheel Braking
    b. Partial Symmetrical Loss of Wheel Braking
    c. Asymmetrical Loss of Wheel Braking
    d. Inadvertent Application of Wheel Braking

4.2.2   Environmental and Emergency Configurations and Conditions

    a. Runway Conditions (Wet, icy, etc.)
    b. Runway Length
    c. Tail/Cross Wind
    d. Engine Out
    e. Hydraulic System Loss
    f. Electrical System Loss

4.2.3   Phases - (ground phases)

    a. Taxi
    b. Takeoff to Rotation
    c. Landing Roll
    d. Rejected Takeoff (RTO)

FIGURE L2 (Continued)

NOTE: System FHA

4.2.4   Interfacing Functions

   a. Crew Alerting (Crew warnings, alerts, messages)
   b. Rudder/Nose Wheel Steering for directional control

   Columns (2) and (3) of Table 4.1-1 show that part of the FHA form which contains the formulated failure conditions for this given function.

4.3   Effects of Failure Condition on the Aircraft, Crew and Occupants

   For each failure condition, the effect of the failure condition on the aircraft, crew and occupants is shown in column (4) of Table 4.1-1.

4.4   Classify/Justify the Effects of the Failure Condition on the Aircraft, Crew and Occupants

   For each failure condition, the classification of the failure condition is defined in columns (5) and (6) of Table 4.1-1.

4.5   Plan for the Verification of Safety Objectives

   For each failure condition, the plan for the verification of safety objectives is defined in Column (7) of Table 4.1-1. This column lists the references to requirements, fault trees, analyses, and or tests.

4.6   WBS FHA Summary

   The following set of significant safety requirements extracted from this WBS FHA will be provided as inputs to the WBS PSSA.

   1) Loss of all wheel braking during landing or RTO shall be less than 5E-7 per flight.
   2) Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be less than 5E-7 per flight.
   3) Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.
   4) Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.
   5) Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.

FIGURE L2 (Continued)

NOTE: System FHA

TABLE 4.1-1 - Wheel Brake System FHA
(Partial - addresses only "Decelerate the Wheels on the Ground")

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
Decelerate Aircraft using Wheel Braking	Total loss of wheel braking	Landing or RTO	See Below			
	a. Unannunciated loss of wheel braking	Landing or RTO	The crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers maximum extent possible. This may result in a runway overrun.	Hazardous		S18 Aircraft FTA
	b. Annunciated loss of wheel braking	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun. Crew uses spoilers and thrust reversers to the maximum extent possible.	Hazardous	Crew procedures for loss of normal and reserve modes	S18 Aircraft FTA
	Partial Symmetrical loss of wheel braking	Landing or RTO	See below			

FIGURE L2 (Continued)

NOTE: System FHA

TABLE 4.1-1 - Wheel Brake System FHA (Cont.)
(Partial - addresses only "Decelerate the Wheels on the Ground")

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
	a. Unannunciated partial symmetrical loss of wheel braking	Landing or RTO	The crew detects the failure when the brakes are used. Crew uses available wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. Temperature on wheels of the loaded brakes increases and could reach point where wheel/tire failure occurs. Depending on number of brakes lost result could be an overrun.	Major to Hazardous	Additional study required to determine classification	TBD
	b. Annunciated partial symmetrical loss of wheel braking	Landing	The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking, spoilers and thrust reversers to maximum extent to decelerate the aircraft. Temperature on wheels of the loaded brakes increases and could reach point where wheel/tire failure occurs. Depending on number of brakes lost result could be an overrun.	Major		
	Asymmetrical loss of wheel braking	Landing or RTO	See below			

FIGURE L2 (Continued)

NOTE: System FHA

TABLE 4.1-1 - Wheel Brake System FHA (Cont.)
(Partial - addresses only "Decelerate the Wheels on the Ground")

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
	a. Asymmetric loss of wheel braking - brake system failure only	Landing or RTO	Decrease in braking performance. Tendency to veer off the runway. For braking performances and brake temperature the effects are the same as partial brake loss above. The crew keeps the aircraft on the runway by using rudder at high speed and nose wheel steering at low speed. Consequences are TBD pending the results of the justification studies.	TBD	Additional studies required to determine classification	
	b. Asymmetrical loss of wheel braking and loss of rudder or nose wheel steering	Landing	Decrease in braking performance. Tendency to veer off the runway. For braking performances and brake temperature the effects are the same as partial brake loss above. The crew cannot maintain runway centerline and results in an offside excursion.	Hazardous		S18 Aircraft FTA
	Inadvertent wheel brake application		See below			
	a. Inadvertent wheel brake application without wheel locking	Takeoff Before V1	The crew stops the aircraft on the runway	Minor		

FIGURE L2 (Continued)

NOTE: System FHA

TABLE 4.1-1 - Wheel Brake System FHA (Cont.)
(Partial - addresses only "Decelerate the Wheels on the Ground")

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
	b. Inadvertent wheel brake application with all wheels locked	Takeoff Before V1	Potential burst of all tires and loss of braking efficiency	Hazardous		S18 Aircraft FTA
	c. Inadvertent wheel brake application with all wheels locked or not locked	Takeoff After V1	Crew cannot takeoff or safely RTO resulting in a high speed overrun.	Catastrophic		S18 Aircraft FTA
	d. Undetected inadvertent wheel braking on one wheel without locking of the wheel	Takeoff	Crew cannot detect the failure by the asymmetry which is very small. Brake temperature can reach very high temperature. Crew retract gear resulting in possible wheel fire or tire failure	Catastrophic		S18 Aircraft FTA
	e. Inadvertent application on one wheel without locking of the wheel coupled with detected high brake temperature	Takeoff	Crew cannot detect the failure by the asymmetry which is very small. Brake temperature can reach very high temperature. Crew detects high brake temperature and leave gear extended to cool brake	Minor	Crew procedure for leaving the gear down in case of detected hot brake temperatures	
etc.	etc.					

FIGURE L2 (Continued)

NOTE: PSSA - Wheel Brake System

Wheel Brake System PSSA

1.0   INTRODUCTION

This PSSA is a compendium of the assessments and analyses performed in the concept and preliminary design phases of the wheel braking system. The purpose of this PSSA is to complete the list of safety requirements, determine the proposed design can reasonably satisfy the requirements, and derive the safety requirements to be considered in the design of lower level items and installations.

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable appendix paragraph.)

System PSSA Paragraph #	Appendix B Paragraph #
4.1.1	B.3.1.1
4.1.2	B.3.1.2
4.2	B.3.2
4.2.1	Appendix D
4.2.2	Appendix E
4.2.3	Appendix F
4.3.2	B.3.3

2.0   REFERENCES

1) S18 Aircraft FHA
2) S18 Wheel Braking System FHA
3) S18 Aircraft Preliminary CCA Results - PRA, CMA, ZSA *(Editor's Note: The PRA, CMA and ZSA are referenced because they provide the methods for determining independence requirements.)*
4) Relevant Airworthiness requirements

3.0   SYSTEM DESCRIPTION SUMMARY

The Wheel Brake System is installed on the two main landing gears. Braking on the main gear wheels is used to provide safe retardation of the aircraft during taxiing and landing phases, and in the event of a rejected take-off. The wheel brake system is shown in Figure 3.0-1. The wheel brakes also prevent unintended aircraft motion when parked, and may be used to provide differential braking for aircraft directional control. A secondary function of the wheel brake system is to stop main gear wheel rotation upon gear retraction.

Braking on the ground is commanded either manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The Autobrake function allows the pilot to pre-arm the deceleration rate prior to takeoff or landing. Autobrake is only available with the NORMAL braking system.

FIGURE L3

NOTE: PSSA - Wheel Brake System

3.0   (Continued):

The eight main gear wheels have multi-disc carbon brakes. Based on the requirement that loss of all wheel braking is less probable than 5E-7 per flight, a design decision was made that each wheel has a brake assembly operated by two independent sets of hydraulic pistons. One set is operated from the GREEN hydraulic supply and is used in the NORMAL braking mode. The Alternate Mode is on standby and is selected automatically when the NORMAL system fails. It is operated independently using the BLUE hydraulic power supply and is backed by an accumulator which is also used to drive the parking brake. The accumulator supplies the ALTERNATE system in the EMERGENCY braking mode, when the BLUE supply is lost and the NORMAL mode is not available. Switch-over is automatic under various failure conditions, or can be manually selected. Reduction of GREEN pressure below a threshold value, either from loss of GREEN supply itself or from its removal by the BSCU due to the presence of faults, causes an automatic selector to connect the BLUE supply to the ALTERNATE brake system. An anti-skid facility is available in both the NORMAL and ALTERNATE modes, and operates at all speeds greater than 2 meters per second.

In the NORMAL braking mode, all eight wheels are individually braked from their own servo valves, which are also used to apply anti-skid. In the ALTERNATE mode, a dual metering valve provides a low pressure hydraulic braking input via four servo valves which provide the antiskid function to four pairs of wheels. Operation of the ALTERNATE system is precluded when the NORMAL system is in use.

In the NORMAL mode, the brake pedal position is electrically fed to a braking computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical aircraft and system states, to provide correct brake functions and improve system fault tolerance, and generates warnings, indications and maintenance information to other systems. This computer is accordingly named the Braking System Control Unit (BSCU). It automatically provides the following functions.

a. Takeover of manual braking (brake pedals), or automatic controls (engagement of Autobrake, autopilot commands during CAT IIIb landing)

b. Control of interfaces with other aircraft systems
   (Editor's Note: Interfaces with other systems may include the hydraulic system, the brake temperature monitoring system, etc.)

c. Generation of braking commands, according to commands received and the status of the system

d. Braking regulation in order to avoid skidding of the main wheels

e. Transmission of information (indications, lights, warnings, etc.) to the flight deck and to the various aircraft computers concerning the BSCU status

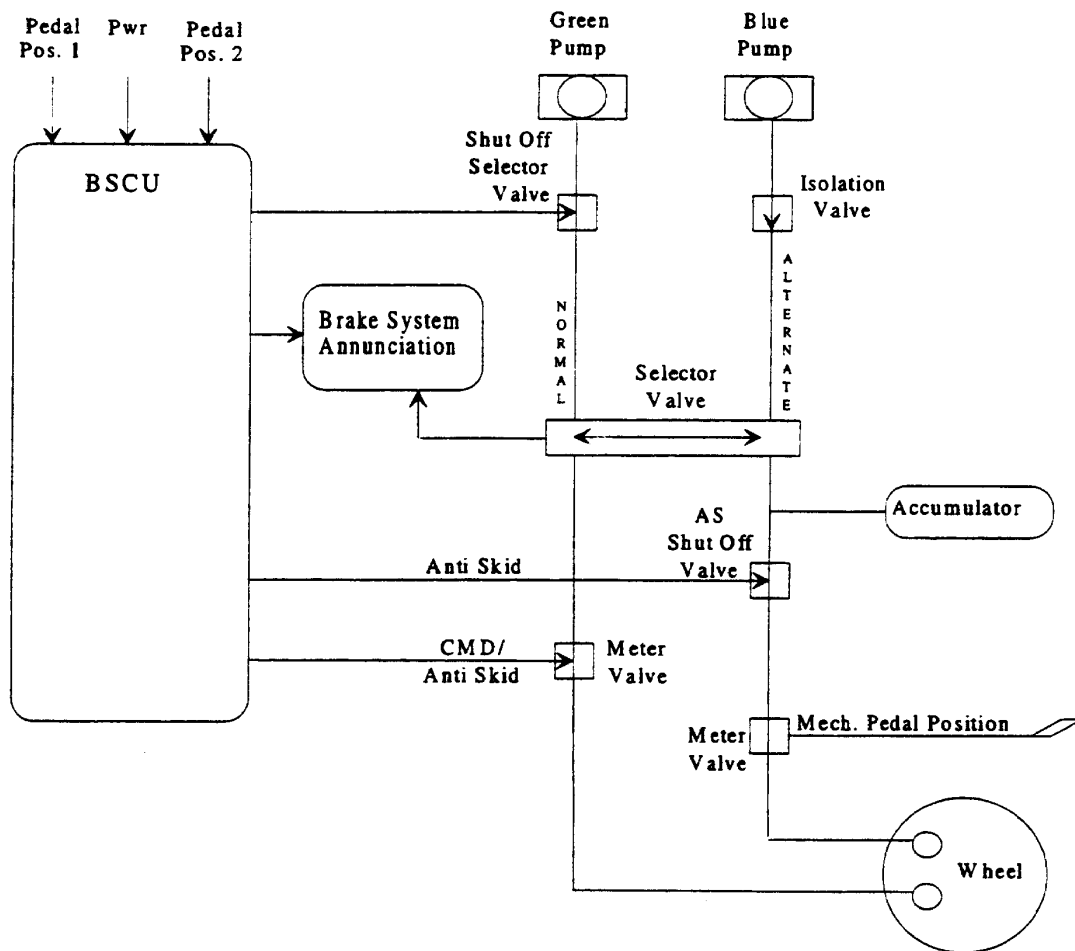FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System

FIGURE 3.0-1 - (PSSA - Wheel Brake System)
Preliminary Wheel Brake System Diagram

FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System

4.0   RESULTS OF WHEEL BRAKING SYSTEM PSSA

4.1   Wheel Braking System Safety Requirements

4.1.1   PSSA Inputs

The following set of safety (availability, integrity, installation) requirements were derived from the aircraft and system FHAs and Common Cause Analyses based on an average flight duration of 5 hours.

1) Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be less than 5E-7 per flight.
2) Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5E-7 per flight.
3) Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.
4) Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.
5) Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.
6) The wheel braking system and thrust reverser system shall be designed to preclude any common threats (tire burst, tire shred, flailing tread, structural deflection, etc).
7) The wheel braking system and the thrust reverser system shall be designed to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).

The Wheel Brake System design features satisfying the safety requirements are documented in Table 4.1.1-1.

FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System

TABLE 4.1.1-1 - (PSSA - Wheel Brake System) Wheel Brake
System Safety Requirements/Design Decisions

Safety Requirement	Design Decisions	Remarks
1. Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be less than 5E-7 per flight.	More than one hydraulic system required to achieve the objective (service experience). Dual channel BSCU and multimode brake operations.	The overall wheel brake system availability can reasonably satisfy this requirement. See PSSA FTA below.
2. Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5E-7 per flight.	Separate the rudder and nose wheel steering system from the wheel braking system. Balance hydraulic supply to each side of the wheel braking system.	The wheel braking system will be shown to be sufficiently independent from the rudder and nose wheel steering systems. System separation between these systems will be shown in the zonal safety analysis and particular risk analysis.
3. Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.	None	Requirement 4 is more stringent and hence drives the design.
4. Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.	No single failure shall result in this condition.	None
5. Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.	No single failure shall result in this condition.	None

4.1.2   Derived Safety Requirements

The design decisions described in Table 4.1.1-1 lead to a primary and secondary system to perform the wheel braking function. As a result of these design decisions, the following set of safety (availability, integrity, installation) requirements were derived.

1) The primary and secondary system shall be designed to preclude any common threats (e.g., tire burst, tire shred, flailing tread, structural deflection).
2) The primary and secondary system shall be designed to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).

FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System

TABLE 4.1.2-1 - (PSSA - Wheel Brake System) Wheel Brake System Derived Safety Requirements

Safety Requirement	Design Decisions	Remarks
1. The primary and secondary system shall be designed to preclude any common threats (tire burst, tire shred, flailing tread, structural deflection).	Install hydraulic supply to the brakes in front and behind the main gear leg.	Compliance will be shown by ZSA and PRA. *(Editor's Note: In this example only for the main gear bay zone and the tire burst particular risk.)*
2. The primary and secondary system shall be designed to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).	Choose two different hydraulic systems to supply the brakes, emergency braking without electrical power.	Compliance will be shown by CMA.

FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System - FTA

4.2   Failure Condition Evaluation

The failure conditions identified from the aircraft and system FHAs are listed below. A preliminary assessment and budgets will be developed for each of these failure conditions.

1)   Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be less than 5E-7 per flight.
2)   Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during shall be less than 5E-7 per flight.
3)   Inadvertent wheel braking with all wheels locked during takeoff roll after V1 shall be less than 5E-7 per flight.
4)   Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.
5)   Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.

4.2.1   Fault Tree Analysis for PSSA

(Editor's Note: This section would normally contain the fault trees for all significant failure conditions. This example shows the evaluation of "Unannunciated loss of all wheel braking" only.)

The high level PSSA Fault Tree shown in Figure 4.2.1-1 reflects the top level requirement of the braking system and depicts the three braking sub systems and budgets for the unannunciated loss of each.

FIGURE L3 (Continued)

NOTE: PSSA - Wheel Brake System - FTA

4.2.1   (Continued):

The Fault Tree in Figure 4.2.1-2 depicts the next level of system development and assessment. This tree includes recognition of the fact that loss of all braking is considered hazardous and a design decision was made to cover all possible loss regardless of annunciation. This is reflected by the addition of the "Loss of Annunciation Capability" event which is ANDed with the "Loss of All Wheel Braking" event shown in Figure 4.2.1-1. The probability of "Loss of Annunciation Capability" is set to 1.0. Design decisions were also made requiring the "Normal" and "Alternate" Brake systems to meet the availability and integrity requirements without dependence or contribution from the "Emergency Standby System", this is denoted by the probability of failure of that system being set to 1.0. This results in an increased integrity budget for the "Normal" and "Alternate" brake system functions.

Figure 4.2.1-2 also shows the downward development of the "Normal Brake" system design by budgeting failure rates to the identified contributors to "Normal Brake System Does Not Operate" (Loss of Hydraulic Supply, Loss of Hydraulic Components, and Loss of BSCU Ability to Command Braking). The Loss of BSCU Ability to Control Braking event is further broken down into the two major elements of BSCU Failure and Loss of Power to BSCU with applicable budgets for aircraft power failures included and the resultant requirement for BSCU failure budget of 6E-6 per hour was reverse calculated to allow satisfaction of the higher level Loss of BSCU budget. This integrity budget was passed to the BSCU supplier as a design requirement for the system.

The BSCU supplier's experience indicated that the 6.6E-6 failure rate budget was not realistic for a design of the complexity of the BSCU function, and thus the supplier derived a requirement for redundant BSCU computations in order to meet the failure rate budget. The Fault Tree in Figure 4.2.1-3 depicts the evolution of the design showing the redundant BSCUs with their ANDed configuration and the resultant per channel failure rate per hour budget of 1.15E-3.

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - FTA

Editor's Note: A decision to provide two means of applying wheel brakes to
affect a complete stop is made. These means are the Normal and Alternate brake
systems. A parking brake is necessary for normal operation of the aircraft on
the ground and a decision to allow it to act as an emergency brake is made.
This fault tree reflects initial allocations of probability budgets to each of
the three systems. The normal system is given the most stringent allocation.

Unannunciated Loss
of All Wheel Braking

UNANLSSW/B

5.00E-07
Requirement is per
5 hour flight

Normal Brake System
Does Not Operate -
No Annunciation

LSSNORMWB

PROB: 5.00E-03 (0)
Budgeted Prob.

Alternate Brake
System Does Not
Operate - No
Annunciation

LOSSALTWB

PROB: 1.00E-02 (0)
Budgeted Prob.

Emergency Brake
System Does Not
Operate - No
Annunciation

LOSSEMRWB

PROB: 1.00E-02 (0)
Budgeted Prob.

FIGURE 4.2.1-1 - (PSSA - Wheel Brake System - FTA)
Unannunciated Loss of All Wheel Braking Fault Tree (Original)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - FTA

Editor's Note: Since unannunciated and annunciated loss of wheel braking are each considered hazardous failure conditions, a decision is made to include all failures of the wheel braking system that result in loss regardless of whether or not they are annunciated.
- A decision is made that the Normal and Alternate systems will meet the requirement without relying on the emergency (parking) brake at all.
- Discussions with potential BSCU vendors reveal that a 6.6E-6/hour failure rate is not feasible with a single item. A decision is made to require 2 BSCUs. This decision is reflected in the fault tree on the following page.
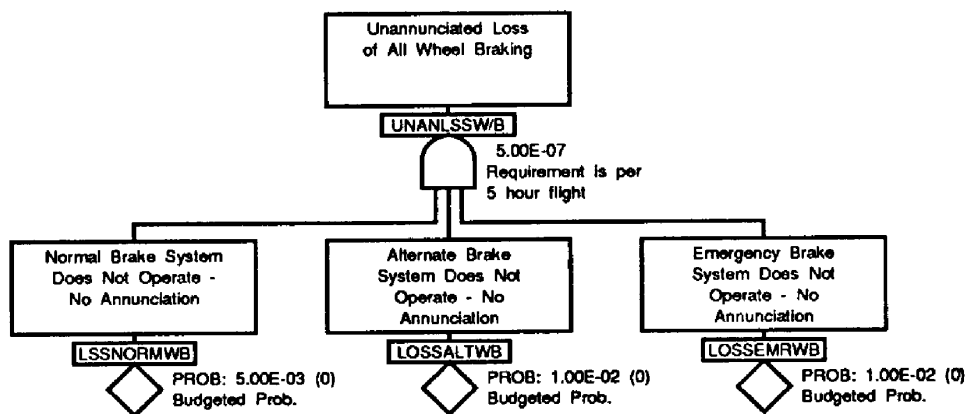

FIGURE 4.2.1-2 - (PSSA - Wheel Brake System - FTA)
Unannunciated Loss of All Wheel Braking Fault Tree (Revision A)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - FTA

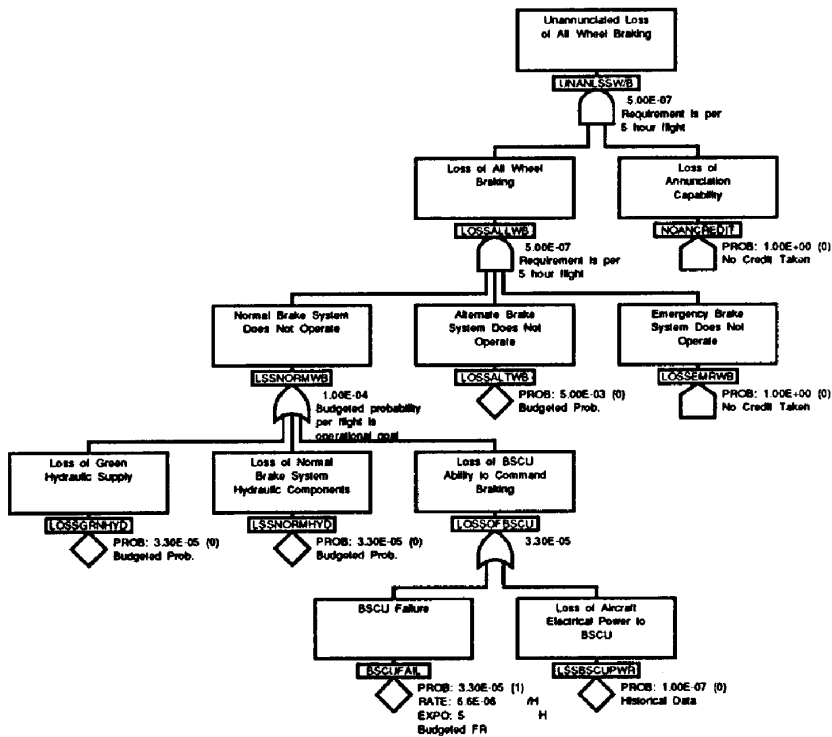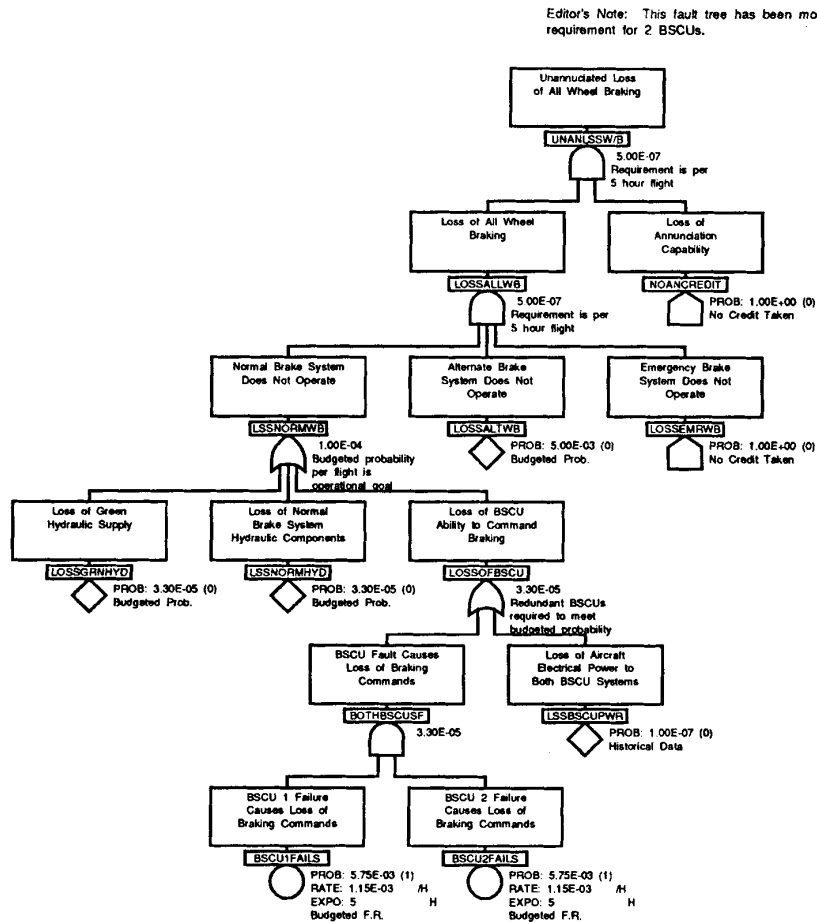Editor's Note: This fault tree has been modified to accommodate the requirement for 2 BSCUs.

FIGURE 4.2.1-3 - (PSSA - Wheel Brake System - FTA)
Unannunciated Loss of All Wheel Braking Fault Tree (Revision B)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - DD

4.2.2   DD for a PSSA (Qualitative/Budgeted System)

(Editor's Note: For details of the DD process, refer to Appendix E.)

(Editor's Note: Normally textual description of development of the DD would be included in the analysis. This text would be similar to that included in the preceding FTA example)
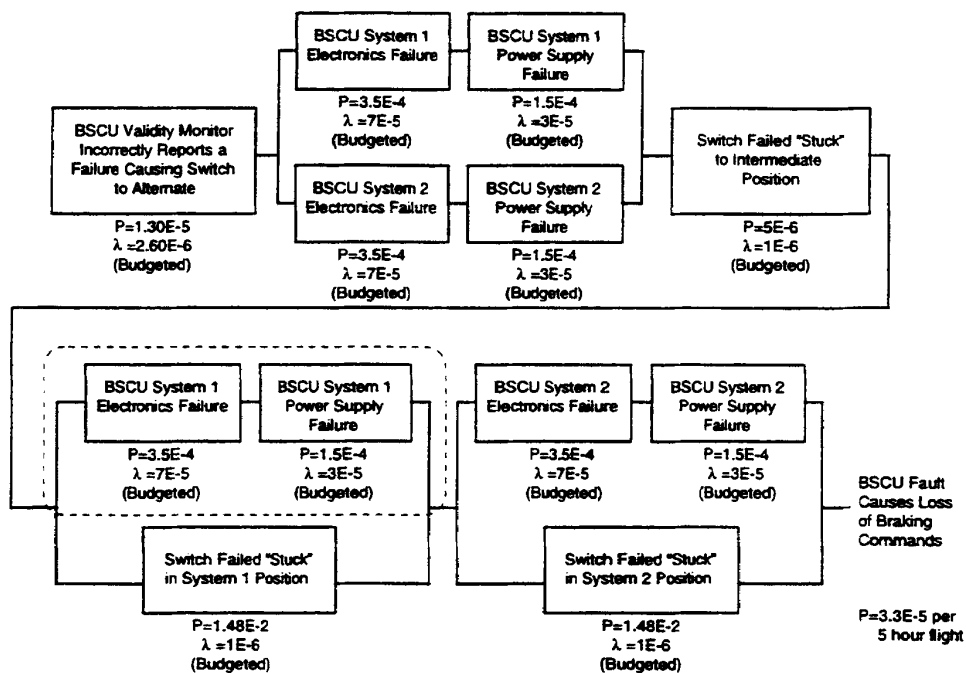
BSCU System 1 Electronics Failure
P=3.5E-4
λ =7E-5
(Budgeted)

BSCU System 1 Power Supply Failure
P=1.5E-4
λ =3E-5
(Budgeted)

BSCU Validity Monitor Incorrectly Reports a Failure Causing Switch to Alternate
P=1.30E-5
λ =2.60E-6
(Budgeted)

BSCU System 2 Electronics Failure
P=3.5E-4
λ =7E-5
(Budgeted)

BSCU System 2 Power Supply Failure
P=1.5E-4
λ =3E-5
(Budgeted)

Switch Failed "Stuck" to Intermediate Position
P=5E-6
λ =1E-6
(Budgeted)

BSCU System 1 Electronics Failure
P=3.5E-4
λ =7E-5
(Budgeted)

BSCU System 1 Power Supply Failure
P=1.5E-4
λ =3E-5
(Budgeted)

BSCU System 2 Electronics Failure
P=3.5E-4
λ =7E-5
(Budgeted)

BSCU System 2 Power Supply Failure
P=1.5E-4
λ =3E-5
(Budgeted)

BSCU Fault Causes Loss of Braking Commands
P=3.3E-5 per 5 hour flight

Switch Failed "Stuck" in System 1 Position
P=1.48E-2
λ =1E-6
(Budgeted)

Switch Failed "Stuck" in System 2 Position
P=1.48E-2
λ =1E-6
(Budgeted)

FIGURE 4.2.2-1 - (PSSA - Wheel Brake System - DD) Unannunciated Loss of All Wheel Braking Dependence Diagram (Original)

(Editor's Note: A decision to provide two means of applying wheel brakes to affect a complete stop is made. These means are the Normal and Alternate brake systems. A parking brake is necessary for normal operation of the aircraft on the ground and a decision to allow it to act as an emergency brake is made. This dependence diagram reflects initial allocations of probability budgets to each of the three systems. The normal system is given the most stringent allocation.)

FIGURE L3 (Continued)
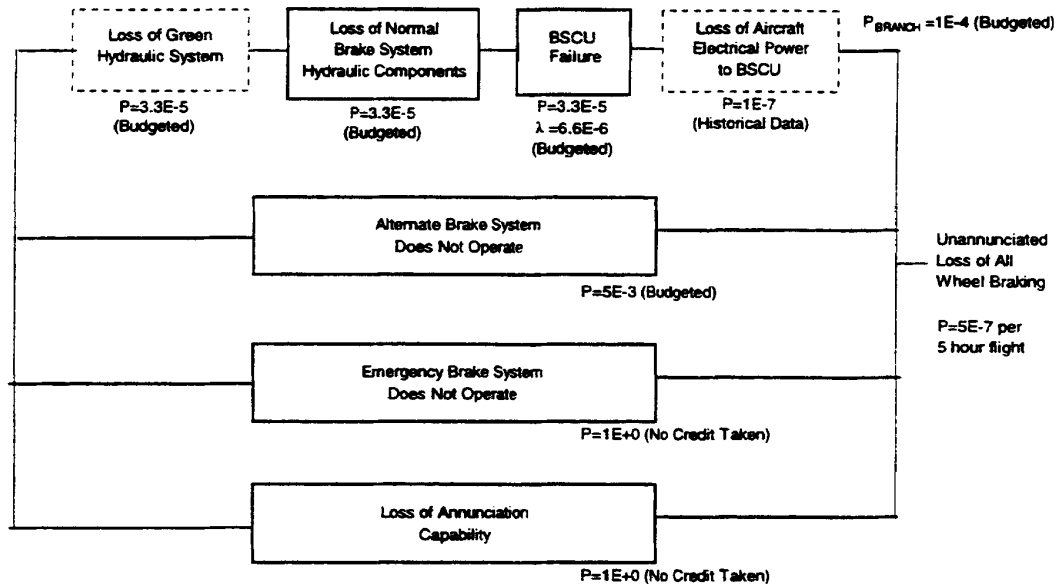
NOTE: PSSA Wheel Brake System - DD

FIGURE 4.2.2-2 - (PSSA - Wheel Brake System - DD) Unannunciated Loss of All Wheel Braking Dependence Diagram (Revision A)

4.2.2   (Continued):

(Editor's Note: The failure condition being investigated in this Wheel Brake System DD is unannunciated loss of wheel braking because it contributes to the catastrophic failure condition, unannunciated loss of deceleration capability. Since unannunciated and annunciated loss of wheel braking are each considered hazardous failure conditions, a decision is made to include all failures of the wheel braking system that result in loss regardless of whether or not they are annunciated. This decision is represented on the DD by including an event for loss of annunciation capability with a probability of 1.

A decision is made to design the system so that the Normal and Alternate systems are able to meet the requirement without relying on the emergency (parking) brake at all.

An operational objective of a normal braking system with a failure rate no greater than 1E-4 per flight is imposed.

Discussions with potential BSCU vendors reveal that a 6.6E-6 per hour failure rate is not feasible with a single item. A decision is made to require two BSCUs. This decision is reflected in the DD on the following page.)

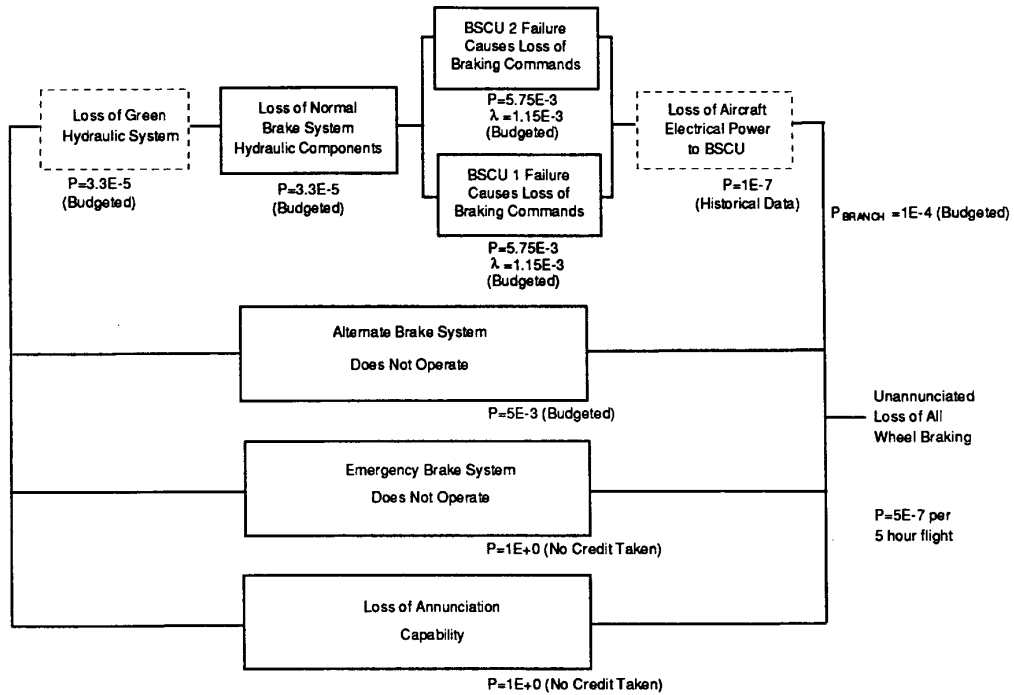FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - DD

FIGURE 4.2.2-3 - (PSSA - Wheel Brake System - DD) Unannunciated Loss of All Wheel Braking Dependence Diagram (Revision B)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - MA

4.2.3   Markov Analysis for PSSA

(Editor's Note: This section would normally contain the Markov analyses for all significant failure conditions. This example shows the evaluation of "Unannunciated Loss of Wheel Braking" only.)

In the example S18 Aircraft, the λ_1, which is the NORMAL braking system failure rate, is expanded to do a detailed Markov analysis. This analysis might involve design iterations.

Editor's Note: In this example ALTERNATE (λ_2) and EMERGENCY (λ_3) systems are assumed to be developed events and hence no further analysis to derive the failure rates for these events is given.)

The Markov chain representation of the wheel braking system is shown in Figure 4.2.3-1. It shows the Markov chain for three different systems which provide braking commands: NORMAL, ALTERNATE and EMERGENCY. Each state in the Markov chain is defined by a three tuple showing the status of the NORMAL, ALTERNATE and EMERGENCY braking systems. A "1" in the state represents a normally working system and a "0" in the state represents a failed system. For example, state (0 1 1) represents a system condition in which the NORMAL braking system is failed while both the ALTERNATE and EMERGENCY braking systems are operational. λ_1, λ_2, and λ_3 are the failure rates of the NORMAL, ALTERNATE and EMERGENCY braking systems in number of failures per hour. The Wheel Braking System is assumed to be failed when all three NORMAL, ALTERNATE and EMERGENCY systems are failed. This is represented by state (0 0 0). Some states in the Markov chain show the maximum state probabilities which are the allocated budgets for the NORMAL, ALTERNATE and EMERGENCY braking systems.

FIGURE L3 (Continued)
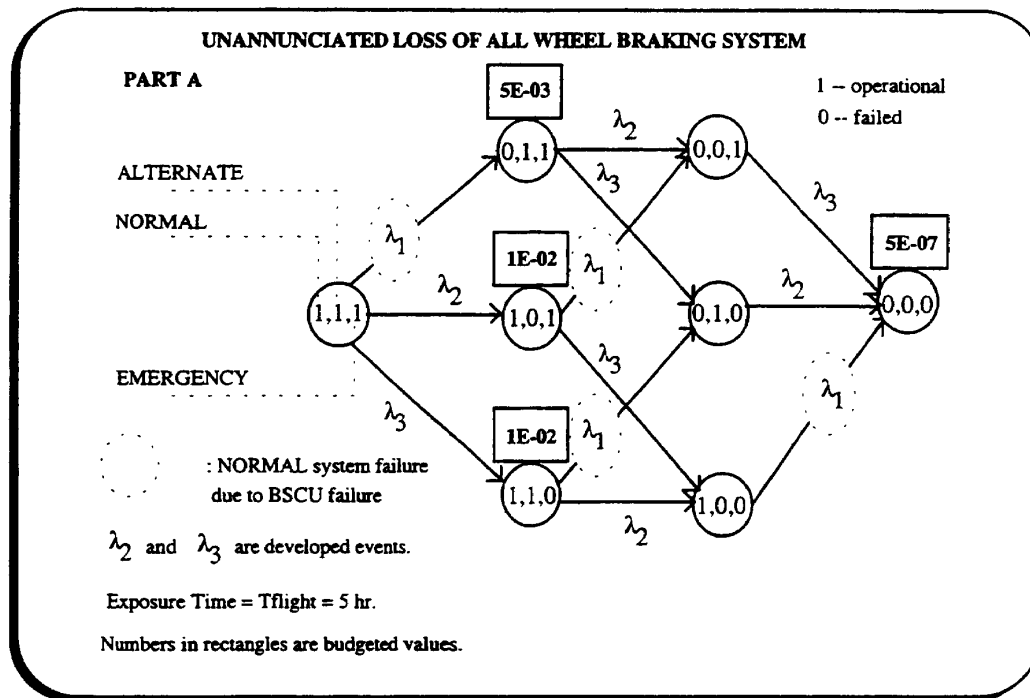
NOTE: PSSA Wheel Brake System - MA

FIGURE 4.2.3-1 - (PSSA Wheel Brake System - MA) Unannunciated Loss of All Wheel Braking (Original)

4.2.3   (Continued):

Figure 4.2.3-2 (Part A) is the same as Figure 4.2.3-1 except that no credit has been taken for the EMERGENCY brake system. Figure 4.2.3-2 (Part B) shows the detailed Markov chain for the BSCU computer which controls the NORMAL braking system. All the dotted circles in of Figure 4.2.3-1 are replaced with the analysis results of Part B of Figure 4.2.3-2. Figure 4.2.3-2 (Part B) shows the NORMAL braking system as an OR function of three components: the BSCU, the GREEN hydraulic system and the Normal brake system hydraulic components.

In Figure 4.2.3-2, the BSCU is designed as a single item. After discussions with potential BSCU manufacturers, it was concluded that two BSCUs are required to meet the safety requirements. This modified target design of the BSCU is shown in Figure 4.2.3-3. To meet the safety requirements, two BSCUs are shown in Figure 4.2.3-3 (Part C). In this Markov chain, each state is represented by a two-tuple (A, S) where "A" is the status of the active BSCU, which could be either BSCU 1 or BSCU 2 and "S" is the status of the standby BSCU. Each component is assumed to be in an operational or failed state. Failed states are represented by a bar on top of the symbol. The BSCU system is assumed to be failed when both BSCUs fail or the electrical power to both BSCUs is lost.

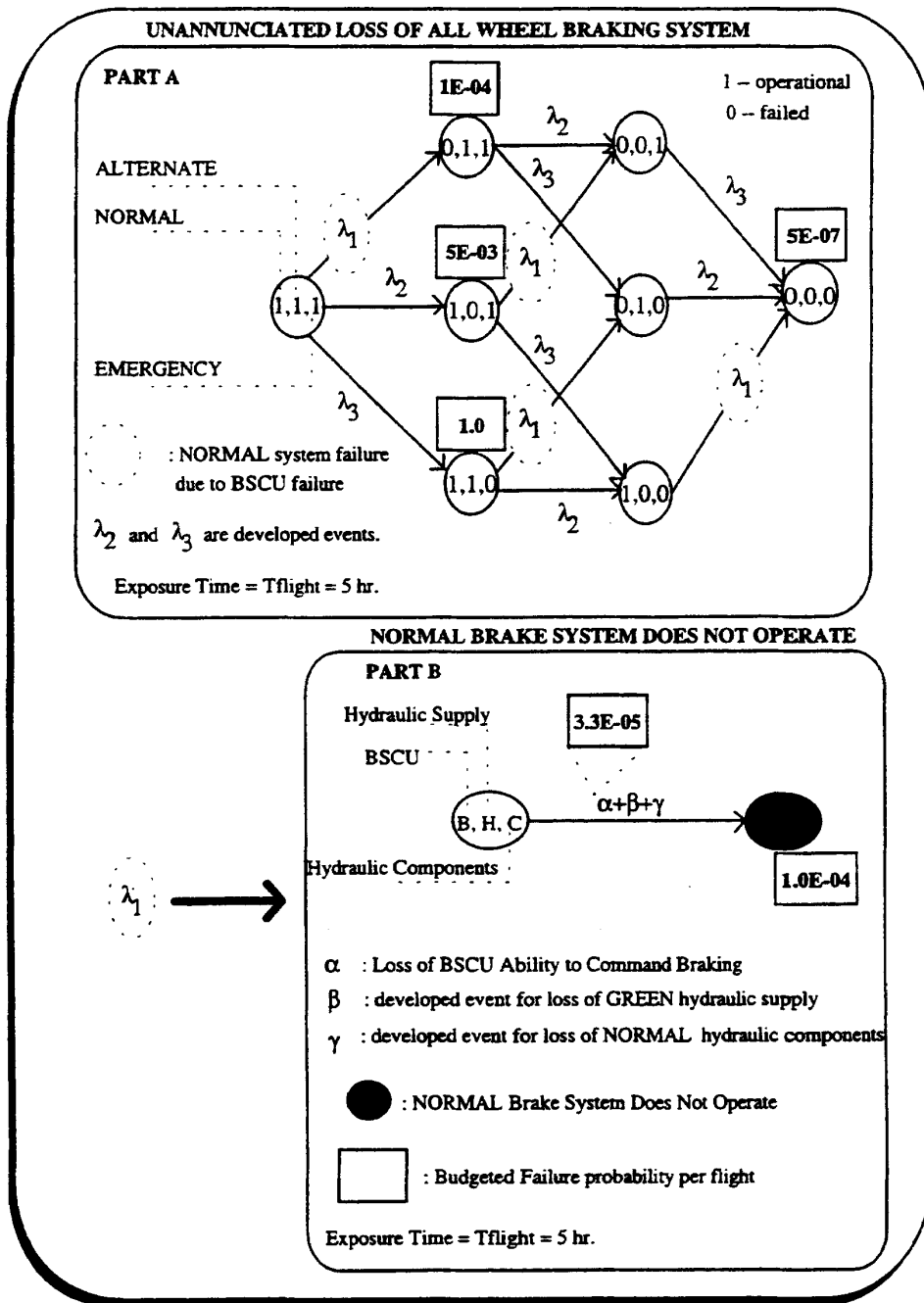FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System - MA

FIGURE 4.2.3-2 - (PSSA Wheel Brake System - MA) Unannunciated Loss of All Wheel Braking (Revision A)
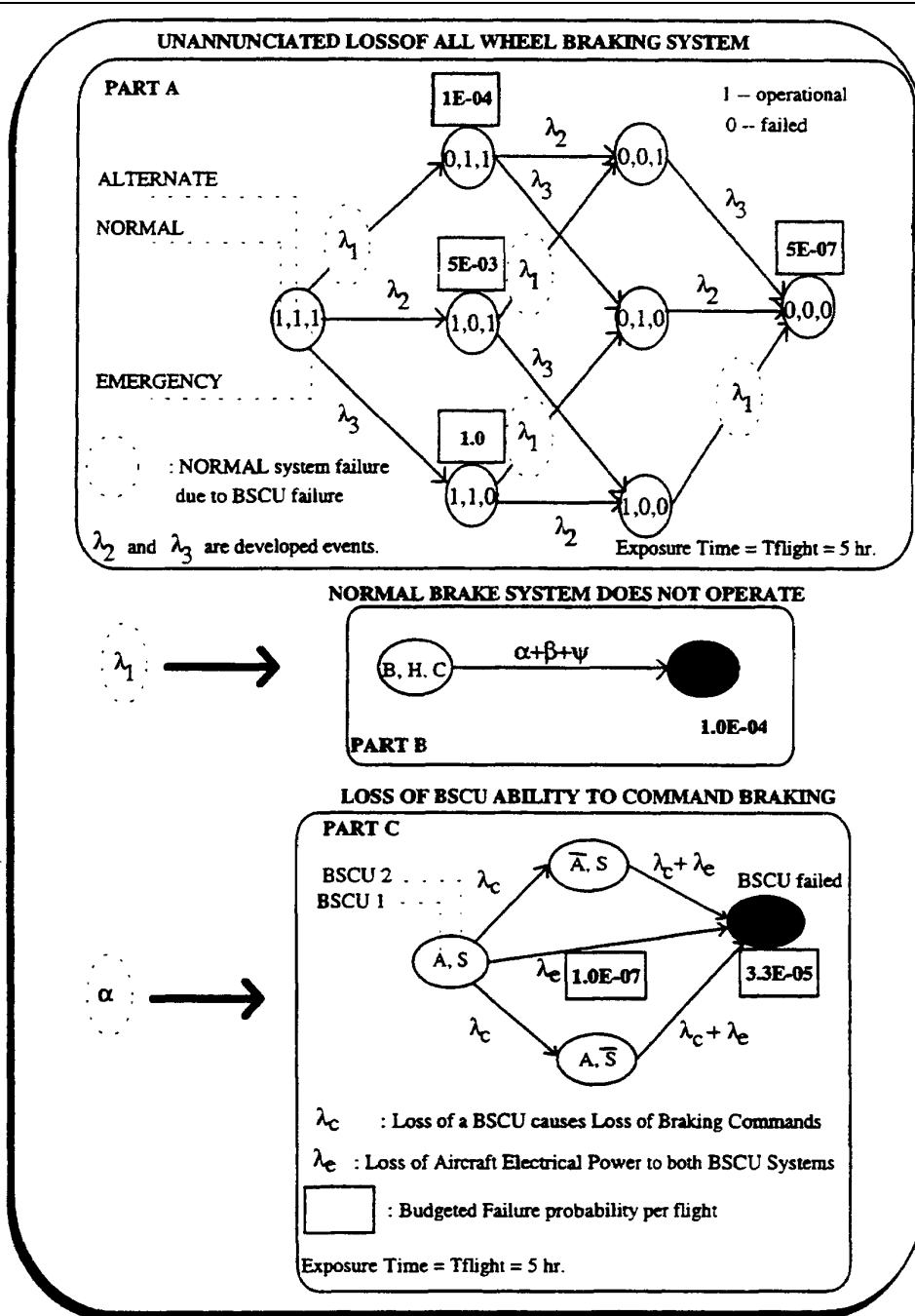
FIGURE L3 (Continued)

NOTE: Wheel Brake System - MA

FIGURE 4.2.3-3 - (PSSA Wheel Brake System - MA) Unannunciated Loss of All Wheel Braking (Revision B)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System

4.3   Requirements Established

From the requirements determined and listed in section 4.1 the following lower level requirements have been derived

4.3.1   Installation Requirements

Primary and secondary hydraulic supply system shall be segregated and verification shall be done in ZSA and PRA.

(Editor's Note: Additional installation requirements are developed from the fault trees but they are not shown here for brevity.).

4.3.2   Item Level Requirements

1) The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight.
2) The probability of "Loss of a single BSCU" shall be less than 5.75E-3 per flight.
3) The probability of "Loss of Normal Brake System Hydraulic Components" shall be less than 3.3E-5 per flight.
4) * The probability of "Inadvertent braking due to BSCU" shall be less than 2.5E-9 per flight.
5) No single failure of the BSCU shall lead to "Inadvertent braking".
6) The BSCU shall be designed to Development Assurance Level A based on the catastrophic classification of "Inadvertent braking due to BSCU".

(*Editor's Note: This requirement was determined from a fault tree which was not shown in this example.)

4.3.3   Requirements on Other Systems

The probability of "Loss of Green Hydraulic supply to the Normal brake system" shall be less than 3.3E-5 per flight.

(Editor's Note: Additional system requirements on other systems are developed from those fault trees but they are not shown here for brevity.)

FIGURE L3 (Continued)

NOTE: PSSA Wheel Brake System

4.3.4   Safety Maintenance Requirements

A failure of the ALTERNATE braking mode is latent because the NORMAL braking mode operates when it contains no failures. Therefore it is necessary to generate a maintenance task to functionally check the ALTERNATE braking mode. Determine the periodicity of that check so that the requirement "Alternate braking does not operate is less than 5E-3 per flight" is met.

(Editor's Note: Additional maintenance requirements may be developed from those fault trees but they are not shown here for brevity.)

5.0   CONCLUSION

The design as known now can satisfy the safety requirements determined in the FHA and the previous CCAs. Further requirements on installation, lower level items, other systems and maintenance tasks to be performed have been identified and are passed on to the responsible design authority.

FIGURE L3 (Continued)

NOTE: PSSA BSCU

BSCU PSSA

1.0 INTRODUCTION

This PSSA documents the assessments and analyses performed in the preliminary design phases of the Brake System Control Unit. The purpose of this PSSA is to complete the list of safety requirements, determine the proposed design can reasonably satisfy the requirements and derive hardware and software requirements.

(Editor's Note: The following Cross Reference Table provides linkage from each example to the applicable PSSA appendix paragraph.)

Item PSSA Paragraph #	Appendix B Paragraph #
4.1.1	B.3.1.1
4.2	B.3.2
4.2.1	Appendix D
4.2.2	Appendix E
4.2.3	Appendix F
4.3	B.3.3

2.0 REFERENCES

1) S18 Wheel Brake System PSSA
2) BSCU Specification

3.0 DESCRIPTION SUMMARY

The requirements imposed on the BSCU for availability and integrity led to the proposal that the BSCU consist of two independent systems to meet the availability requirements and the proposal that each system contain a command and monitor channel to meet the integrity requirements. A block diagram of the proposed BSCU architecture is shown in Figure 3.0-1.

Each BSCU system generates necessary voltages in its own power supply. A power supply monitor is provided to detect out of specification voltage conditions. Brake pedal inputs are provided to the command and monitor channels which compute the necessary braking commands. The commands generated by each channel are compared and if they do not agree, a failure is reported. The results of the power supply monitor and the comparator are provided to a System Validity Monitor. A failure reported by either system in a BSCU will cause that system to disable its outputs and set the System Validity Monitor to invalid. Each BSCU System Validity Monitor is provided to an overall BSCU Validity Monitor. Failure of both System 1 and System 2 will cause the selector valve to select the Alternate Brake System.

In normal operation, BSCU system 1 provides the brake and anti-skid commands to the wheel brakes. When System 1 reports a failure via its System Validity Monitor, the output of System 2, if valid, is switched in to provide the commands. In the event that System 2 subsequently fails, all BSCU outputs are disabled and the BSCU Validity Monitor is set to invalid.

FIGURE L4
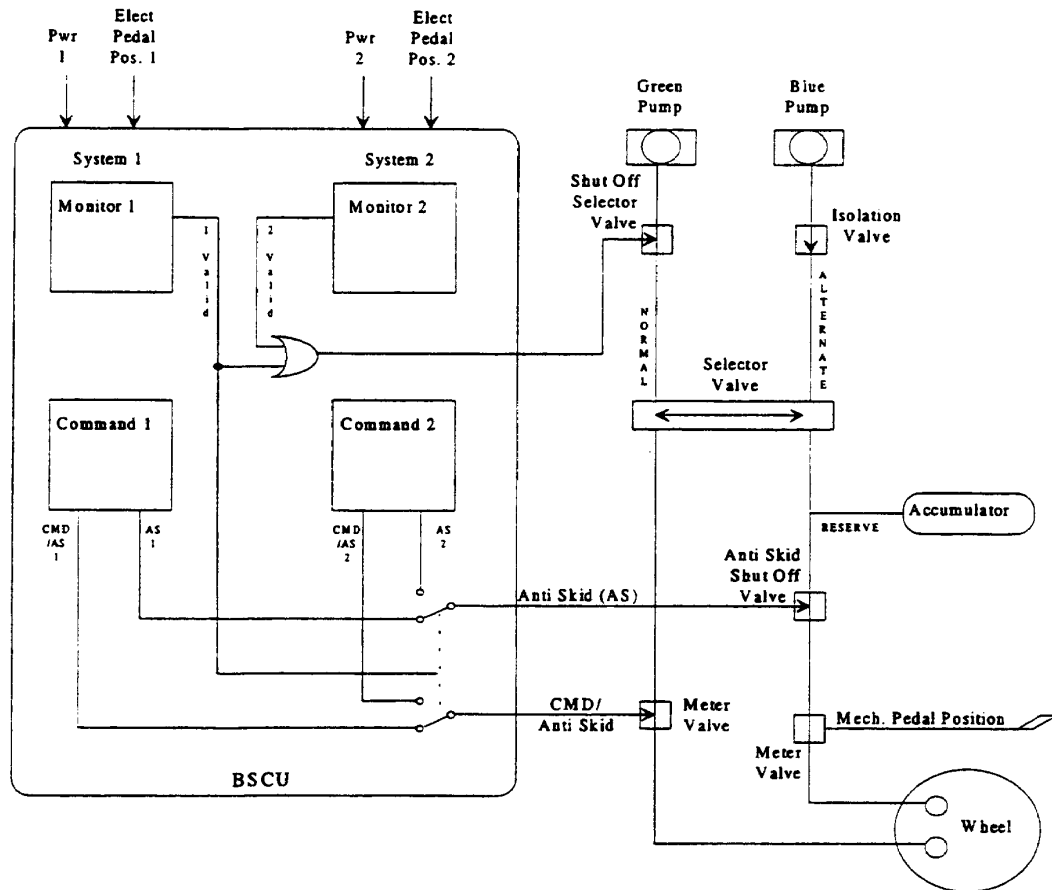
NOTE: PSSA BSCU

FIGURE 3.0-1 - (PSSA BSCU) Proposed BSCU Architecture

FIGURE L4 (Continued)

NOTE: PSSA BSCU

4.0   BSCU PSSA

4.1   BSCU Safety Requirements

4.1.1   PSSA Inputs

The following set of safety requirements were derived from the Wheel Brake System PSSA.

1)   The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight.
2)   The probability of "Loss of a single BSCU" shall be less than 5.75E-3 per flight.
3)   The probability of "Inadvertent braking due to BSCU" shall be less than 2.5E-9 per flight.
4)   No single failure of the BSCU shall lead to "Inadvertent braking".
5)   The BSCU shall be designed to Development Assurance Level A based on the catastrophic classification of "Inadvertent Braking Due to BSCU".

The following aircraft operational considerations were provided by the airframe manufacturer.

a.   Average flight length - 5 hours
b.   Average power-up interval - 100 hours
c.   Aircraft life - 100,000 hours
d.   Time between V1 and rotation - 15 seconds (.004167 hour)

The plan for showing how the BSCU will comply with the safety requirements is shown in Table 4.1.1-1.

FIGURE L4 (Continued)

NOTE: PSSA BSCU

TABLE 4.1.1-1 - (PSSA BSCU) BSCU Safety Requirements/Design Decisions

Safety Requirement	Design Decisions	Remarks
1. The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight.	Dual channel BSCU design	The overall BSCU system availability can reasonably satisfy this requirement. See FTA in Figure 4.2.1-1.
2. The probability of "Loss of a single BSCU" shall be less than 5.75E-3 per flight.	Design for adequate reliability	None
3. The probability of "Inadvertent braking due to BSCU" shall be less than 2.5E-9 per flight.	Each BSCU system contains independent command and monitor channels.	BSCU integrity can achieve this requirement. See FTA in PSSA BSCU FTA Figure 4.2.1-2.
4. No single failure of the BSCU shall lead to "Inadvertent braking".	No single failure shall result in this condition.	Perform CMA and FMEA as necessary.
5. The BSCU shall be designed to Development Assurance Level A.	Develop command channel to Development Assurance Level A and the monitor channel to Level B.	Development Assurance Levels assigned according to guidance in Section 5.4 of SAE ARP 4754.

4.2   Failure Condition Evaluation

Fault trees for the failure conditions, loss of BSCU and inadvertent braking due to BSCU were developed and evaluated to determine the feasibility of the proposed BSCU design. Probability allocations were made based on all available information about the design and past experience.

(Editor's Note: The failure condition of inadvertent wheel braking is re-introduced here because it provides a better example for demonstrating the BSCU common mode analysis and failure modes and effects analysis.)

FIGURE L4 (Continued)

NOTE: PSSA BSCU - FTA

4.2.1   PSSA of BSCU System - Fault Tree Analysis

The fault tree in Figure 4.2.1-1 addresses the loss of BSCU failure condition. The BSCU supplier has determined that BSCU redundancy may be accomplished through inclusion of two independent BSCU systems within a single BSCU LRU, with a monitor/switching arrangement selecting a valid BSCU command for delivery to the Brake System. As depicted in the Fault Tree, loss of all BSCU operation occurs if the BSCU Validity Monitor fails such that it incorrectly reports both BSCUs failed (BSCU Validity Monitor Incorrectly Reports Dual Failures), if BSCU systems 1 and 2 both experience failures within the same flight (BSCU Systems 1 AND 2 do not Operate), or if a specific switch failure in conjunction with the selected channel failure occurs (Switch Failure Contributes to Loss of BSCU Braking Commands). The fault tree further depicts the combinations of BSCU switch failure possibilities and the accompanying BSCU System failures leading to Loss of Braking. The tree also shows the breakdown and failure rate budgeting for a single system BSCU failure contribution from either the computation channel or the power supply.

The fault tree in Figure 4.2.1-2 addresses inadvertent wheel braking caused by the BSCU. The BSCU can cause inadvertent braking only when the Normal Braking System is in use. This fault tree does not deal with this aircraft level aspect of the analysis. The fault tree assumes that there are no undetectable BSCU failures that can cause an inadvertent brake command. In order to meet the requirements, this assumption should be proven correct via FMEA and/or CMA. The other branch of the fault tree deals with combinations of monitored BSCU failures and monitor failures. Detectable BSCU failures are power supply failures that cause out of spec voltages detected by the power supply monitor and command channel I/O or CPU failures that cause an inadvertent brake command which are detected by the comparator. Monitor I/O and CPU failures are not included in the fault tree because the monitor channel does not provide brake commands. Monitor channel failures will cause the comparator to report a failure and switch brake commands to the other BSCU System if the comparator is working. If the comparator is not working, a monitor channel failure still does not cause inadvertent braking.

Since the BSCU System 1 is the normally active channel, the fault tree (page 2) demonstrates that System 1 undetected power supply failures may contribute to inadvertent braking, as may computation channel failures. The fault tree in page 3 contains the same BSCU failure information relative to BSCU System 2, however System 2 cannot be applied to the brakes unless the monitor/select switch is activated; thus the event of the switch being in position 2 is ANDed with the System 2 failures. Two conditions may result in switch activation, a previous detected failure of System 1, or an independent monitor/switch failure.

FIGURE L4 (Continued)

NOTE: PSSA BSCU - FTA

Editor's Note: The "Loss of All Wheel Braking" FTA was used by the airframe manufacturer to produce BSCU vendor requirements. The BSCU vendor reviewed the requirement for two BSCUs and determined that one BSCU with two systems inside would be adequate. The BSCU vendor generated the following BSCU PSSA Fault Tree starting with the basic event, "BSCU Fault Causes Loss of Braking Commands" from the Wheel Brake System PSSA FTA.

An exposure time of 14,750 hours was budgeted for the latent switch failures. This is the maximum exposure time which allows the top level probability requirement to be met.
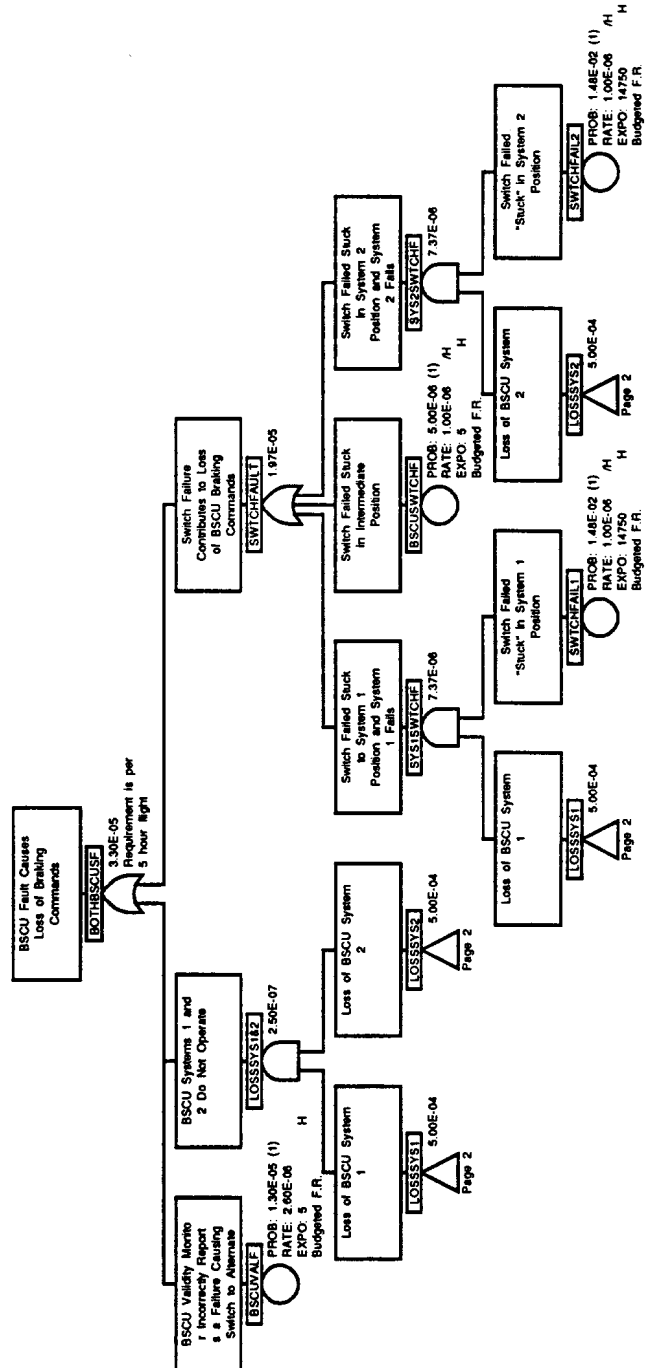
FIGURE 4.2.1-1 - (PSSA BSCU - FTA)
BSCU Fault Causes Loss of Braking Commands Fault Tree (Page 1)

NOTE: PSSA BSCU - FTA

Editor's Note: This level of detail would not normally appear in this fault tree because it is possible to show that the requirements are met using the total failure rate of the BSCU. Detail about BSCU failure modes is included in this example to allow a feature of Markov Analysis to be illustrated.
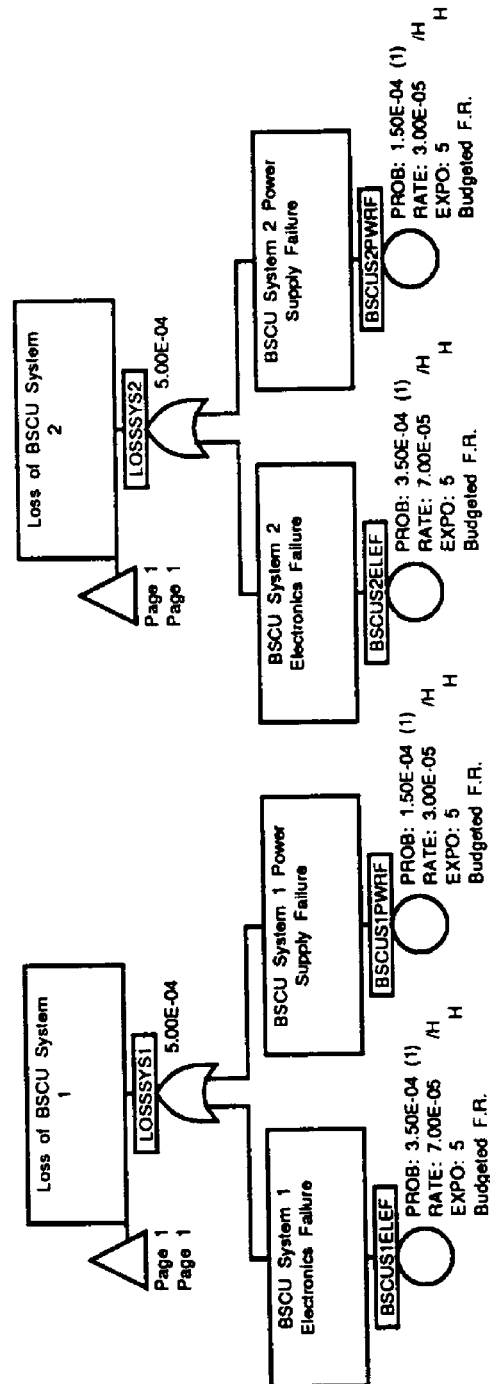
FIGURE 4.2.1-1 (PSSA BSCU - FTA)
BSCU Fault Causes Loss of Braking Commands Fault Tree (Page 2)

FIGURE L4 (Continued)
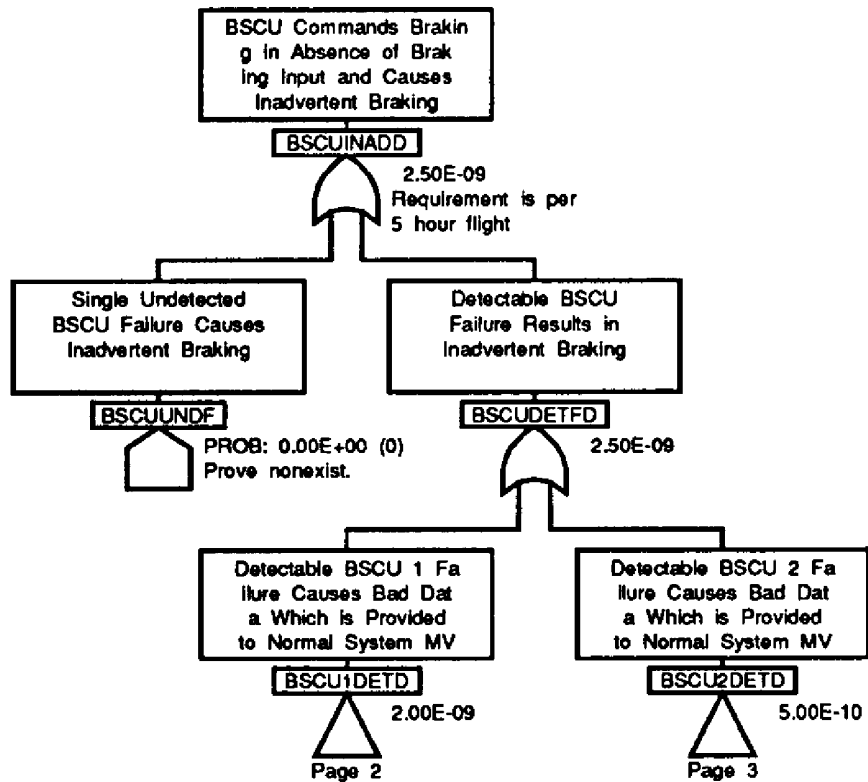
NOTE: PSSA BSCU - FTA

FIGURE 4.2.1-2 - (PSSA BSCU - FTA)
BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking Fault Tree (Page 1)

FIGURE L4 (Continued)
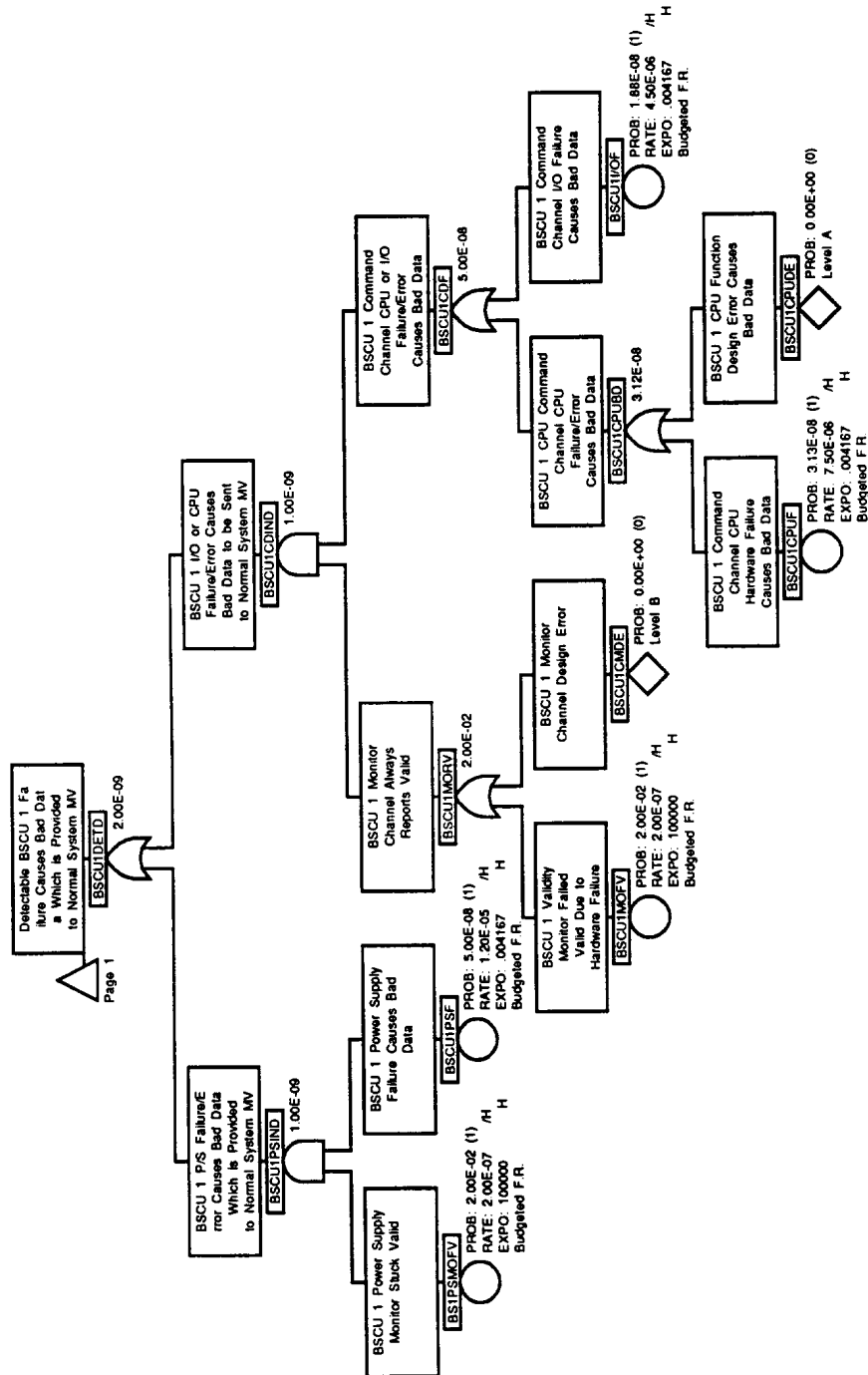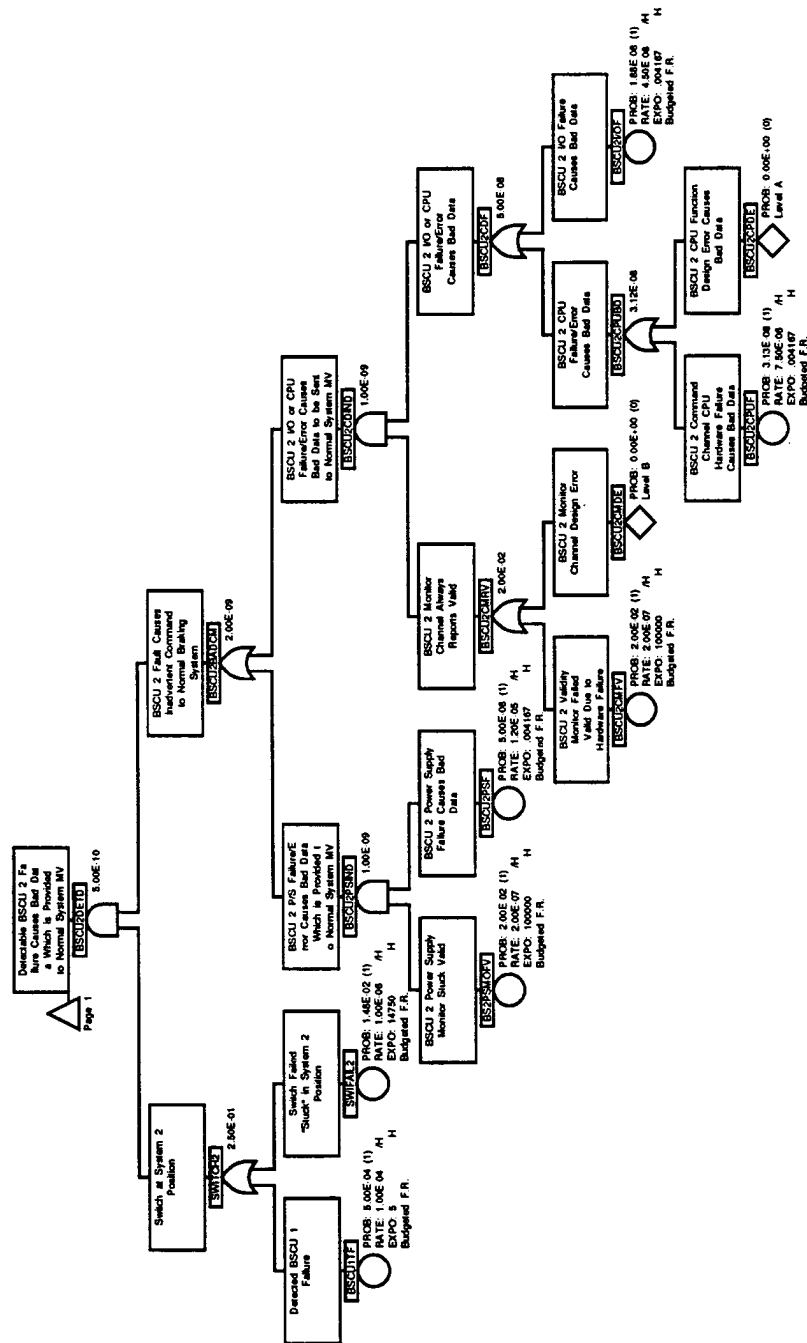
NOTE: PSSA BSCU - FTA

FIGURE 4.2.1-2 - (PSSA BSCU - FTA)
BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking Fault Tree (Page 2)

FIGURE L4 (Continued)

NOTE: PSSA BSCU - FTA

FIGURE 4.2.1-2 - (PSSA BSCU - FTA)
BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking Fault Tree (Page 3)

FIGURE L4 (Continued)

NOTE: PSSA BSCU - DD

4.2.2   PSSA of BSCU System - Dependence Diagram Analysis

(Editor's Note: Normally textual description of development of the DD would be included in the analysis. This text would be similar to that included in the preceding FTA example.)

The dependence diagram in Figure 4.2.2-1 addresses the loss of BSCU failure condition. Loss of all BSCU operation occurs if the BSCU Validity Monitor fails such that it incorrectly reports both BSCUs failed or if BSCU systems 1 and 2 experience failures.

The dependence diagram in Figure 4.2.2-2 addresses inadvertent wheel braking caused by the BSCU. The BSCU can cause inadvertent braking only when the Normal Braking System is in use. This dependence diagram does not deal with this aircraft level aspect of the analysis. The dependence diagram assumes that there are no undetectable BSCU failures that can cause an inadvertent brake command. In order to meet the requirements, this assumption should be proven correct via FMEA and/or CMA. The dependence diagram deals with combinations of monitored BSCU failures and monitor failures.

FIGURE L4 (Continued)
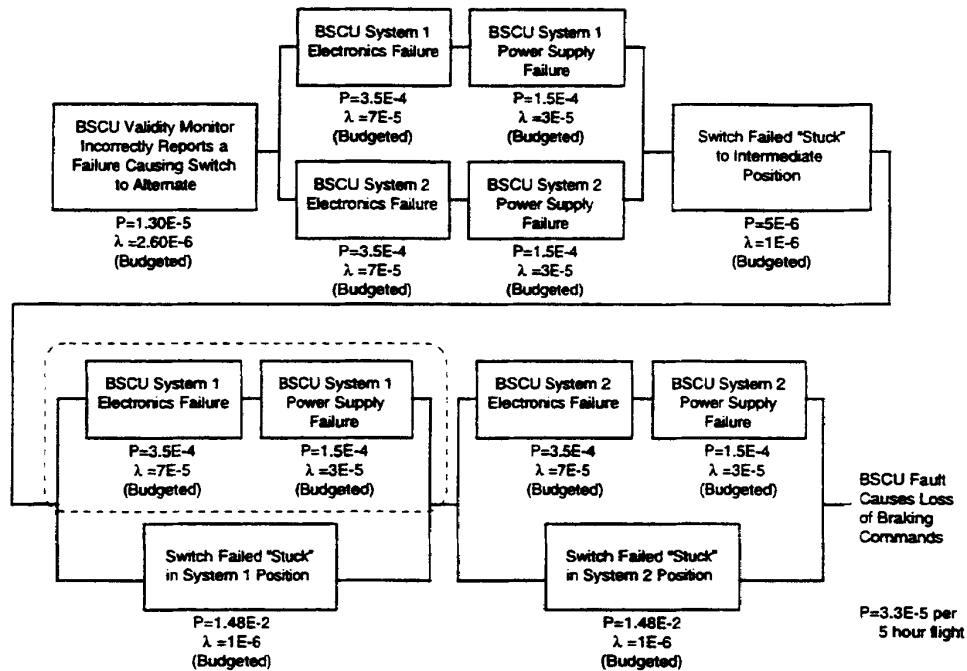
NOTE: PSSA BSCU - DD

FIGURE 4.2.2-1 - (PSSA BSCU - DD) BSCU Fault Causes Loss of Braking Commands
Dependence Diagram

4.2.2   (Continued):

(Editor's Note: The "Loss of All Wheel Braking" DD was used by the airframe manufacturer to produce BSCU vendor requirements. The BSCU vendor reviewed the requirement for two BSCUs and determined that one BSCU with two systems inside would be adequate. The BSCU vendor generated the following BSCU PSSA DD starting with the basic event. "BSCU Fault Causes Loss of Braking Commands" from the Wheel Brake System PSSA DD.

An Exposure time of 14,750 hours was budgeted for latent switch failures. This is the maximum exposure time which allows the top level probability requirement to be met.

This level of detail would not normally appear in this DD cause it is possible to show that the requirements are met using the total failure rate of the BSCU. Detail about BSCU failure modes is included in this example to allow a feature of Markov analysis to be illustrated.)

FIGURE L4 (Continued)

NOTE: PSSA BSCU - DD

Single Undetected BCSU Failure Causes Inadvertent Braking
P=0E+0
Assumed until CMA Completed

BSCU 1 Power Supply Monitor Stuck Valid
P=1E-2
λ =2E-7
(Budgeted)

BSCU 1 Power Supply Failure Causes Bad Data
P=5E-8
λ =1.2E-5
(Budgeted)

BSCU 1 Validity Monitor Failed Valid Due to H/W Failure
P=1E-2
λ =2E-7
(Budgeted)

BSCU 1 Command Channel CPU H/W Failure Causes Bad Data
P=3.13E-8
λ =7.5E-6
(Budgeted)

BSCU 1 Monitor Channel Design Error
P=0E+0
Assumed due to Level A development

BSCU 1 CPU Function Design Error Causes Bad Data
P=0E+0
Assumed due to Level B development

BSCU 1 Command Channel I/O Failure Causes Bad Data
P1.88E-8
λ =4.5E-6
(Budgeted)

Detected BSCU 1 Failure
P=5E-4
λ =1E-4
(Budgeted)

Switch Failed "Stuck" in System 2 Position
P=1.48E-2
λ =1E-6
(Budgeted)

BSCU 2 Power Supply Monitor Stuck Valid
P=1E-2
λ =2E-7
(Budgeted)

BSCU 2 Power Supply Failure Causes Bad Data
P=5E-8
λ =1.2E-5
(Budgeted)

BSCU 2 Validity Monitor Failed Valid Due to H/W Failure
P=1E-2
λ =2E-7
(Budgeted)

BSCU 2 Command Channel CPU H/W Failure Causes Bad Data
P=3.13E-8
λ =7.5E-6
(Budgeted)

BSCU 2 Monitor Channel Design Error
P=0E+0
Assumed due to Level A development

BSCU 2 CPU Function Design Error Causes Bad Data
P=0E+0
Assumed due to Level B development

BSCU 2 I/O Failure Causes Bad Data
P=1.88E-8
λ =4.5E-6
(Budgeted)

BSCU Commands Braking in Absence of Brake Input and Causes Inadvertent Braking
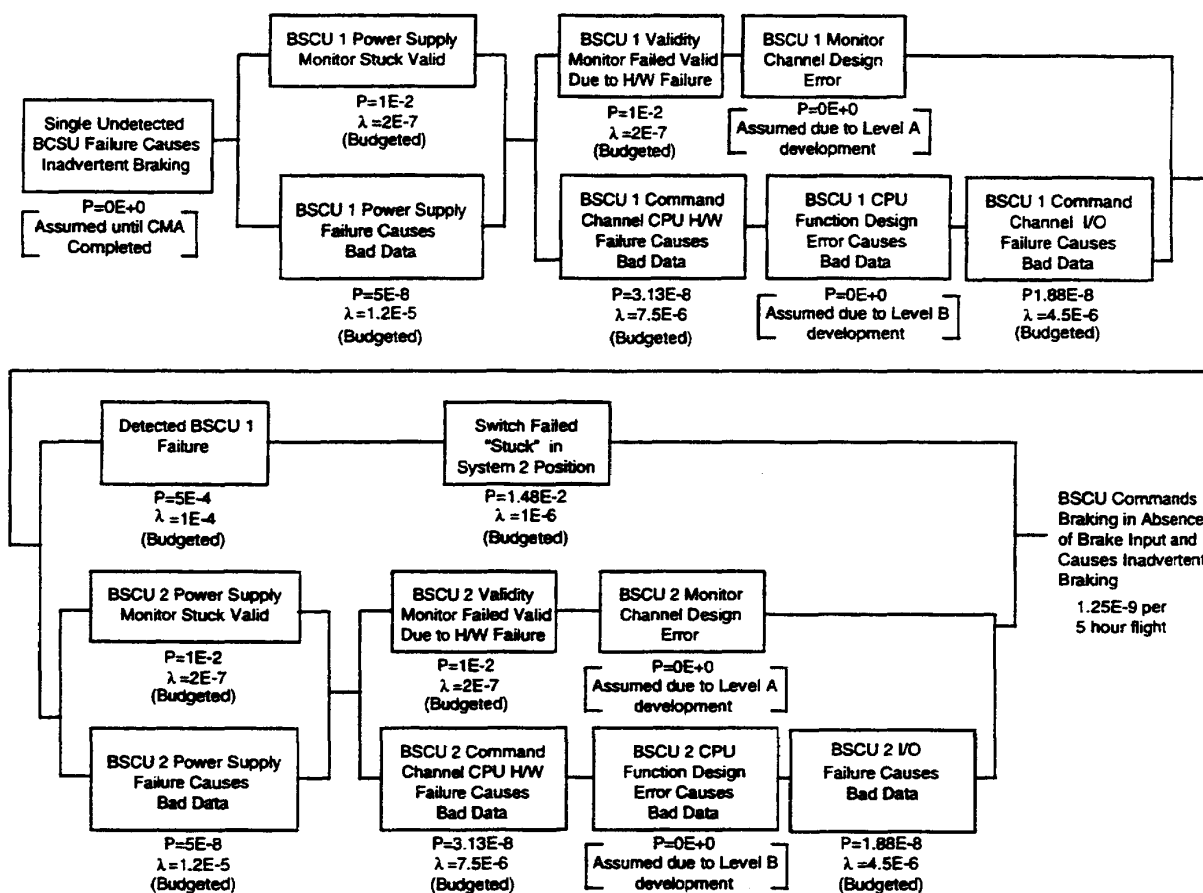1.25E-9 per 5 hour flight

FIGURE 4.2.2-2 - (PSSA BSCU - DD) BSCU Commands Braking in Absence of Brake Input and Causes Inadvertent Braking DD

FIGURE L4 (Continued)

NOTE: PSSA BSCU - MA

4.2.3   PSSA of BSCU System - Markov Analysis

The Markov Analysis for "BSCU Fault Causes Loss of Braking Commands", including the switching mechanism, is shown in Figure 4.2.3-1 (Part A). In the Markov chain, each state is represented by a three-tuple (A, S, SW) where "A" is the status of the active BSCU computer, which could be either BSCU 1 or BSCU 2, "S" is the status of the standby BSCU computer and "SW" is the status of the switch. Each component is assumed to be in an operational or failed state. Failed states are represented by a bar on top of the symbol. Both the active and standby BSCU computers can fail in only one mode. The switching system can fail in two different modes, either stuck to the active BSCU computer or stuck open (not connected to either of the BSCU computers). The BSCU system is assumed to be failed when either both BSCU computers fail or the switching system fails to switch from the active to the standby system when the active system fails in a flight. Figure 4.2.3-1 (Part B) shows the expanded Markov model for a BSCU system failure. The BSCU system is assumed to be failed whenever the BSCU electronics fail or the BSCU power supply fails. Failure of both of these units is represented by a single transition in the Markov chain of Figure 4.2.3-1 (Part B).

Figure 4.2.3-2 shows "Detectable BSCU Failure Results in Inadvertent Braking". Inadvertent braking occurs when both the monitor and active system fail in either BSCU system. Inadvertent braking due to BSCU system 1 failure is shown in Figure 4.2.3-3. In this case, each state is represented by a four tuple (A, B, C, D). The first and third tuple in each state correspond to the BSCU system CPU & I/O and power supply. The second and fourth tuple in each state correspond to the CPU & I/O monitor and power supply monitor. Inadvertent braking occurs when both the CPU and its monitor fail or when the power supply and its monitor fail. The budgeted probability value of inadvertent braking due to BSCU system 1 failure is 2E-9.

Inadvertent braking due to BSCU system 2 and switching mechanism failure is shown in Figure 4.2.3-4. The Markov model in Figure 4.2.3-4 is same as the Markov model for BSCU system 1 (Figure 4.2.3-3) except that a new failure mode is added to the model to account for the switching mechanism. This is the failure of switching mechanism shown in the figure with a failure probability of 2.5E-1. Hence the total budgeted probability for Inadvertent braking due to BSCU system 2 failure is (2E-9)x(2.5E-1) = 5E-10.

FIGURE L4 (Continued)

NOTE: PSSA BSCU - MA

BSCU FAULT CAUSES LOSS OF BRAKING COMMANDS

PART A

system 2

system 1

switching

$2\lambda_c$

A, S, SW

λ_c

λ_{sw}

A, S, SW

A, S, $\overline{SW}$

Switch Stuck

λ_{sw}

λ_{sw}

λ_c

A, S, $\overline{SW}$

Switch Stuck

λ_{sw}

λ_c

BSCU failed

3.3E-05

● : BSCU and NORMAL system failure due to
BSCU system 1 and system 2 failure

X: System Operational
  (X is either BSCU System1 or BSCU System2 or Switching)

$\overline{X}$: System Failed

[ ] : Budgeted Failure probability per flight

Exposure Time = Tflight = 5 h (for BSCU System).

Exposure Time = 14750 h (for Switch System).

LOSS OF A BSCU SYSTEM

λ_c →

E, P

$\xi + \psi$

5.0E-04

Power Supply

Electronics

[ ] : Budgeted Failure probability per flight

Exposure Time = Tflight = 5 hr.

ξ : BSCU System Electronics Failure Rate

ψ : BSCU System Power Supply Failure Rate
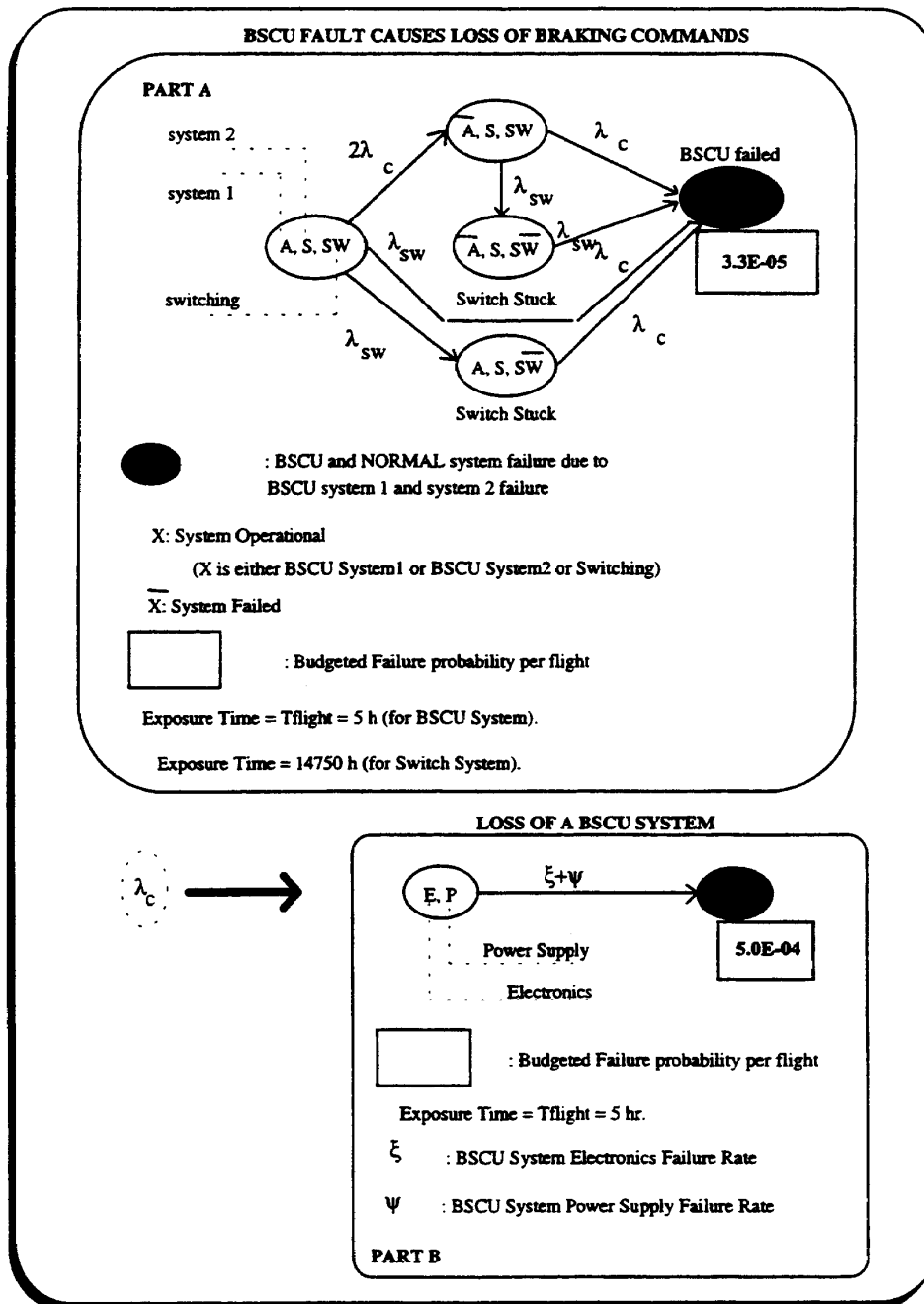
PART B

FIGURE 4.2.3-1 - (PSSA BSCU - MA) BSCU Fault Causes Loss of Braking Commands MA

FIGURE L4 (Continued)
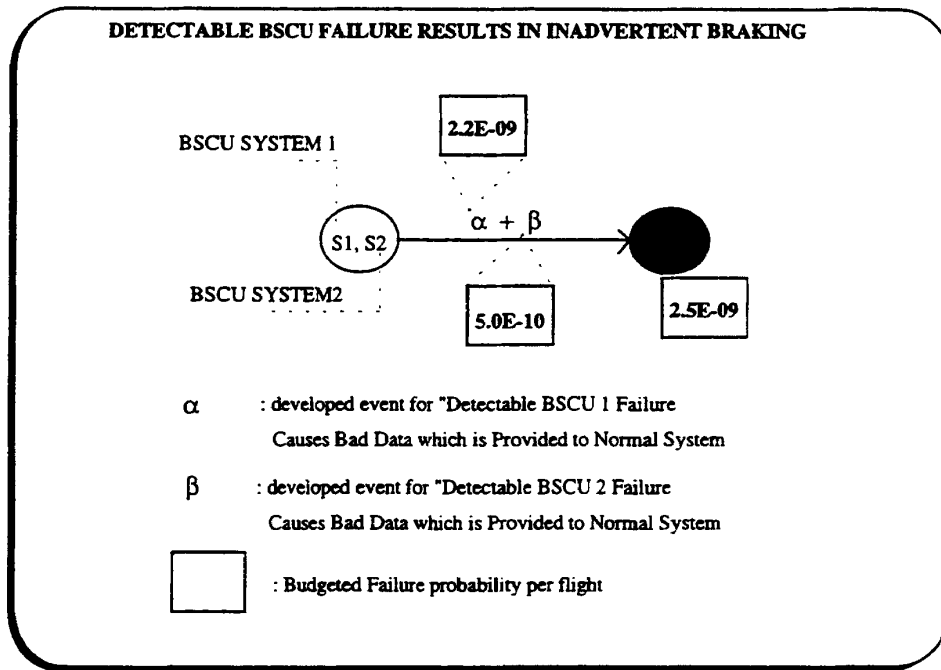
NOTE: PSSA BSCU - MA

FIGURE 4.2.3-2 - (PSSA BSCU - MA) Detectable BSCU Failure Results in Inadvertent Braking MA
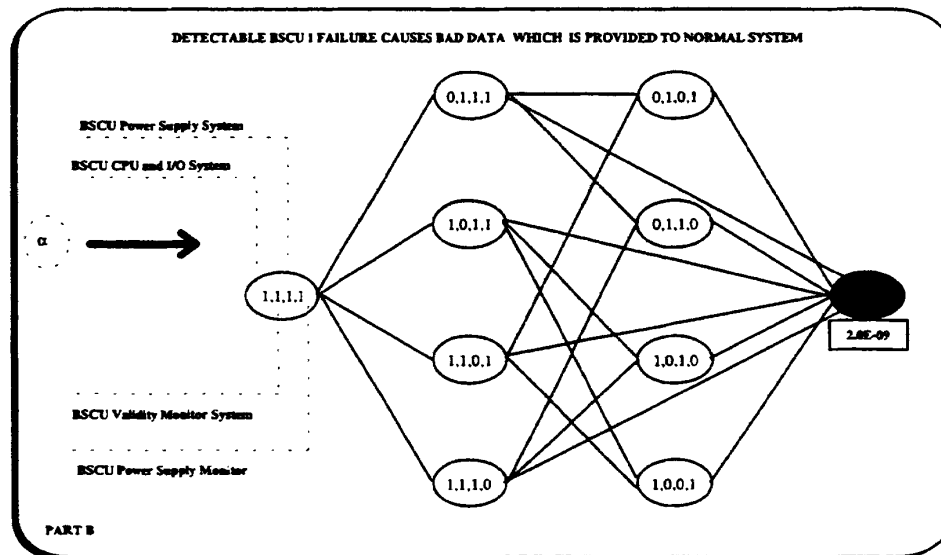

FIGURE 4.2.3-3 - (PSSA BSCU - MA) Inadvertent Braking Due to BSCU System 1 Failure MA

FIGURE L4 (Continued)

NOTE: PSSA BSCU - MA

DETECTABLE BSCU 2 FAILURE CAUSES BAD DATA WHICH IS PROVIDED TO NORMAL SYSTEM

BSCU Power Supply System

BSCU CPU and I/O System

β

BSCU Validity Monitor System

BSCU Power Supply Monitor

PART C

0,1,1,1   0,1,0,1

1,0,1,1   0,1,1,0

1,1,1,1

1,1,0,1   1,0,1,0
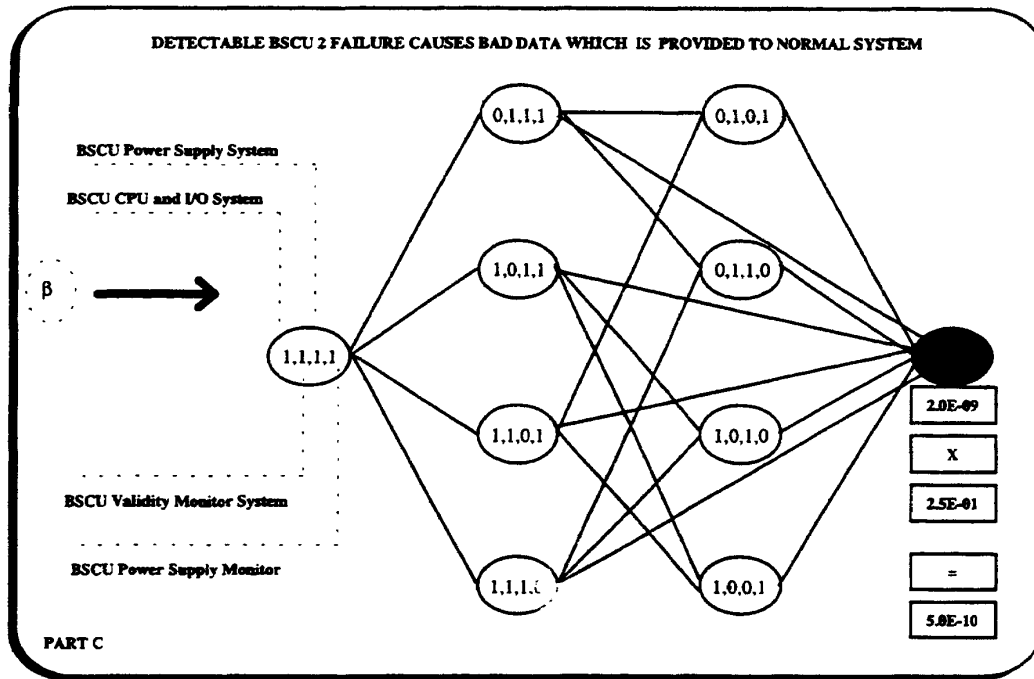
1,1,1,1   1,0,0,1

2.0E-09

X

2.5E-01

=

5.0E-10

FIGURE 4.2.3-4 - (PSSA BSCU - MA) Inadvertent Braking Due to BSCU System 2 Failure and Switching Mechanism Failure MA

FIGURE L4 (Continued)

NOTE: PSSA BSCU

4.3   Requirements Established

As a result of the failure condition evaluation, the following lower level requirements have been derived.

4.3.1   Installation Requirements

Each BSCU System requires a source of power independent from the source supplied to the other system.

4.3.2   Hardware and Software Requirements

The following BSCU hardware and software requirements have been derived and must be satisfied in order to meet the overall safety objectives.

1) Each BSCU system will have a target failure rate of less than 1E-4 failures per hour.
2) The targeted probabilities for the fault tree primary failure events shown in Figures 4.2.1-1 and 4.2.1-2 have to be met. Note: Any events that do not meet these target probabilities must be approved by the system engineering group before proceeding with the design.
3) There must be no undetectable BSCU failures that can cause inadvertent braking.
4) There must be no common mode failures of the command and monitor channels of a BSCU system that could cause them to provide the same incorrect braking command simultaneously.
5) * The monitor channel of a BSCU system shall be designed to Development Assurance Level A.
6) * The command channel of a BSCU system may be designed to Development Assurance Level B.

(Editor's Note: These allocations could have been switched, designing the command channel to Development Assurance Level A and the monitor channel to Level B.)

4.3.3   Safety Maintenance Requirements

The switch that selects between system 1 and system 2 must be checked on an interval not to exceed 14,750 hours.

5.0   CONCLUSION

The design as known now appears to be able to satisfy the safety requirements imposed by the Wheel Brake System PSSA. Further requirements on installation, hardware and software and maintenance tasks to be performed have been identified and are passed on to the responsible design authority. Failure Modes and Effects Analyses and Common Mode Analyses are required to verify that this design meets the requirements.

FIGURE L4 (Continued)

NOTE: SSA BSCU - FMEA

(Editor's Note: At this point in the example, it is assumed that the PSSA is sufficiently developed to enable detail design implementation. The example resumes following detail design implementation and develops the SSA to support certification. As described in Figure 3 of the main body of this document, the SSA process begins as a bottom up analysis at the item level.)

BSCU Power Supply Failure Modes and Effects Analysis (FMEA)

(Editor's Note: This FMEA example is simplified by limiting the FMEA to the BSCU power supply. In reality an FMEA may be requested at any level from an entire system to a small portion of circuitry performing one function inside an LRU.)

1.0   INTRODUCTION

(Editor's Note: For the purpose of this example it is assumed that the FMEA was chosen to support the SSA FTA. The process and format of the FMEA may require minor alterations to support DD or MA methodologies; however the basic steps and principles carry forward.)

This FMEA addresses the BSCU power supply in support of the basic events and safety objectives identified in the "INADVERTENT WHEEL BRAKING AFTER V1" preliminary FTA as requested in Reference 2.

This FMEA report provides quantification of the final FTA by providing failure rates for the basic events. The FTA basic events supported by this FMEA are "BSCU Power Supply Failure Causes Bad Data", "BSCU Power Supply Monitor Failed Valid" and the power supply contribution to "Undetected BSCU Failure Causes Inadvertent Braking". This analysis was performed against released and final documentation of the BSCU design and production drawings. This FMEA will be part of the supporting documentation for both the BSCU and wheel brake system SSAs.

The required FMEA was performed in two parts. A functional FMEA was performed on the Power Supply and a piece part FMEA was performed on the Power Supply Monitor portion of the power supply. The piece part FMEA was performed after the conservative results of the functional FMEA did not meet the safety objectives.

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable FMEA appendix paragraph.

Item FMEA Paragraph #	Appendix G Paragraph #
4.1	G.3.2.1
4.2	G.3.2.2

FIGURE L5

NOTE: SSA BSCU - FMEA

2.0   REFERENCES

(*Editor's Note: The information contained in these references provides a substantial portion of the documentation required before beginning an FMEA. See Section G.2.1)*

1) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"

2) Internal memo requesting FMEA support for "Inadvertent Braking after V1" fault tree for the S18 Aircraft incorporating the BSCU System

3) BSCU released design and production documentation

4) MIL-HDBK-217F "Reliability Prediction of Electronic Equipment"

5) Internal memo stating component failure modes to be used for BSCU FMEA.

6) Results of lab analysis of "Loss of or Reduced Filtering"

3.0   POWER SUPPLY DESCRIPTION

(*Editor's Note: Part of the Preparation for an FMEA is understanding the operation of the function. A brief overview of the operation should be included in the report as outlined in G2.1)*

The implementation of the BSCU power supply, as documented in Reference 3 was reviewed. The design and implementation of the BSCU 1 and 2 power supplies were found to be identical. Implementation is through identical power supply designs, located on physically separated areas of the BSCU circuit card assembly as depicted in architectural diagram of the BSCU in Figure 3.0-1. Within each BSCU System, the power supply and power supply monitor functions are physically independently located.

The power supply design is depicted in the block diagram provided in Figure 3.0-2. A detailed schematic of the +5 volt monitor design is provided in Figure 3.0-3.

The BSCU power supply is of standard design and is described in the BSCU Hardware Description document.

The power supply monitors are window comparators. Both +5 and ±15 volts are monitored for over and under voltage conditions. The outputs are ANDed together so that if any voltage exceeds the trip point, high or low, the monitor output is pulled low.

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

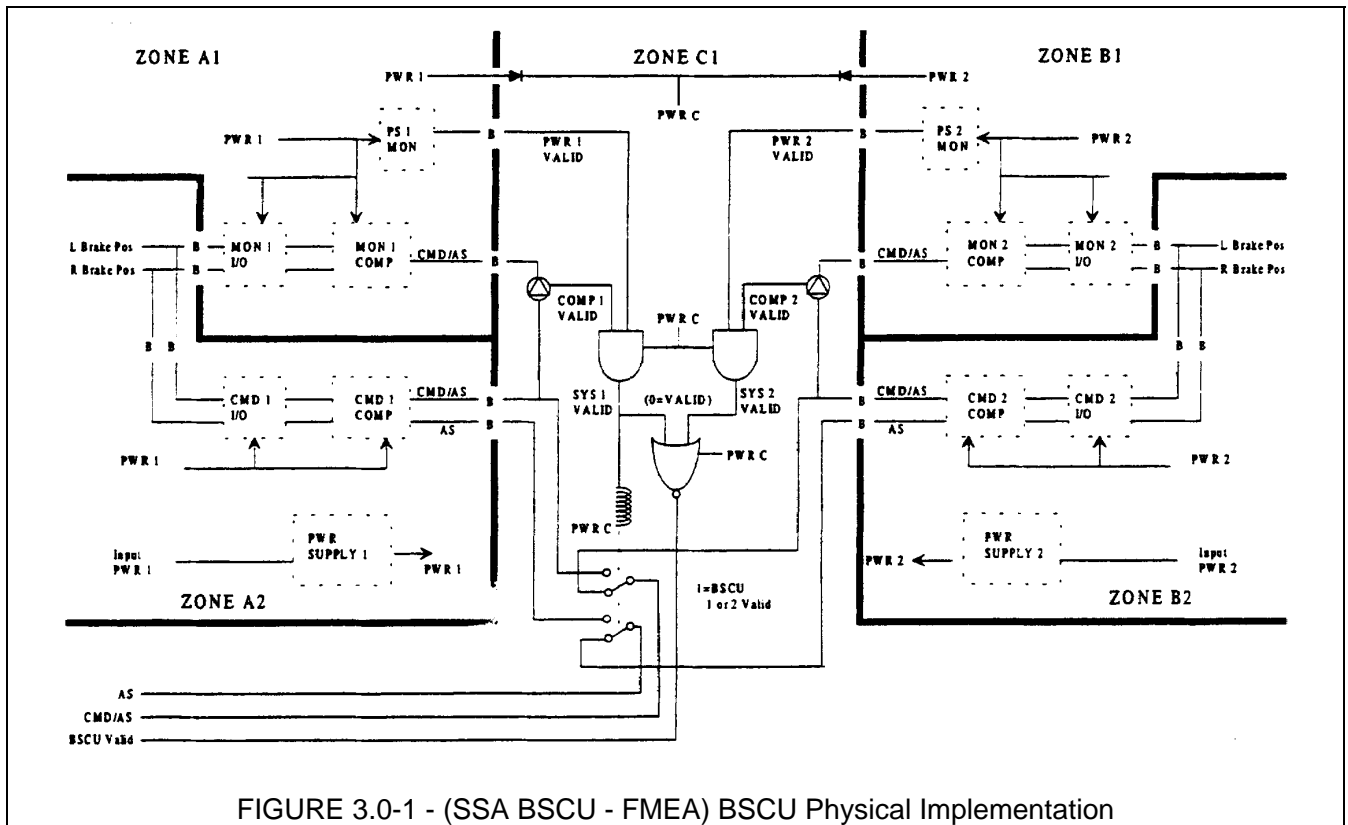FIGURE 3.0-1 - (SSA BSCU - FMEA) BSCU Physical Implementation
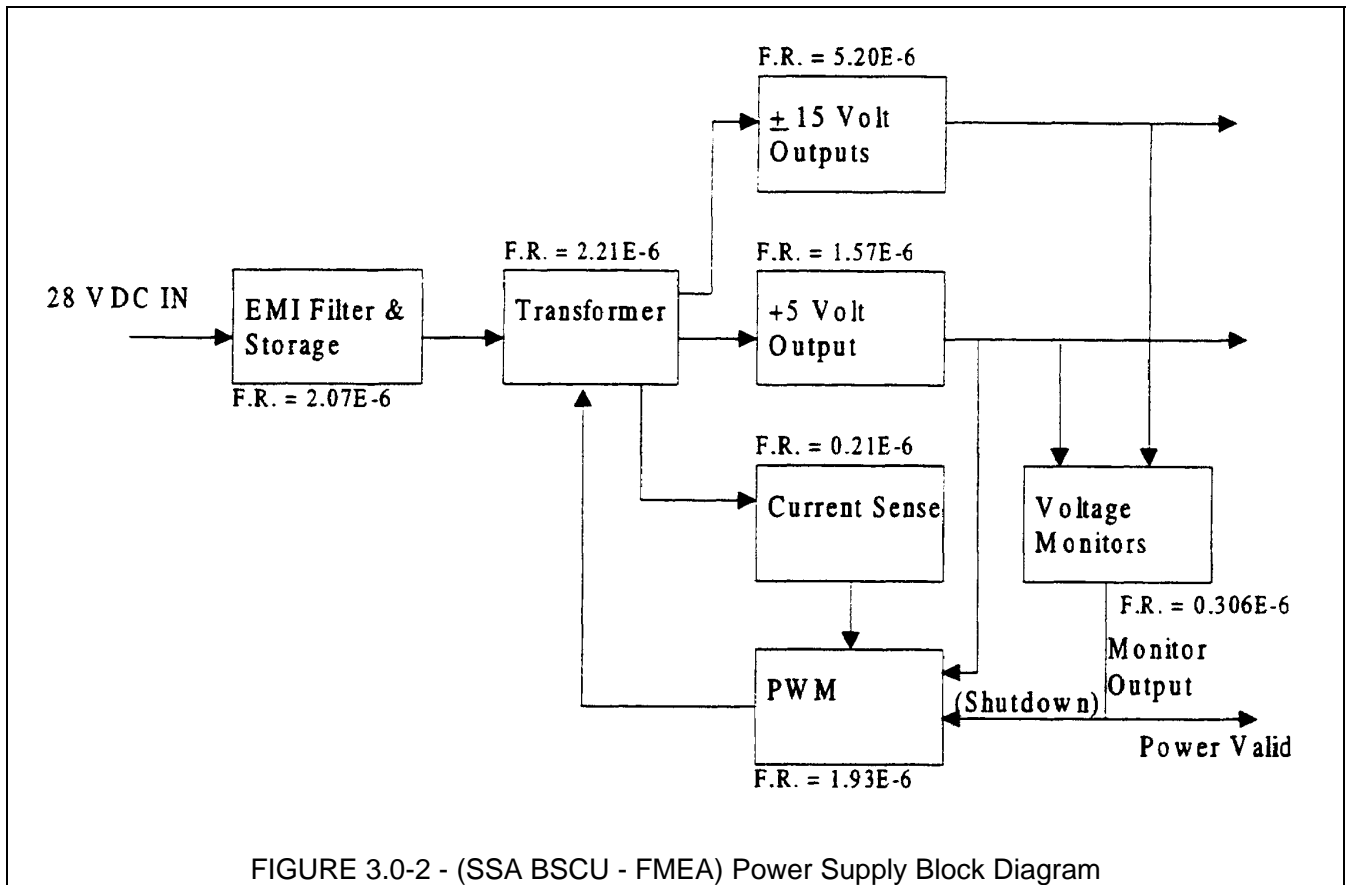
FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

FIGURE 3.0-2 - (SSA BSCU - FMEA) Power Supply Block Diagram
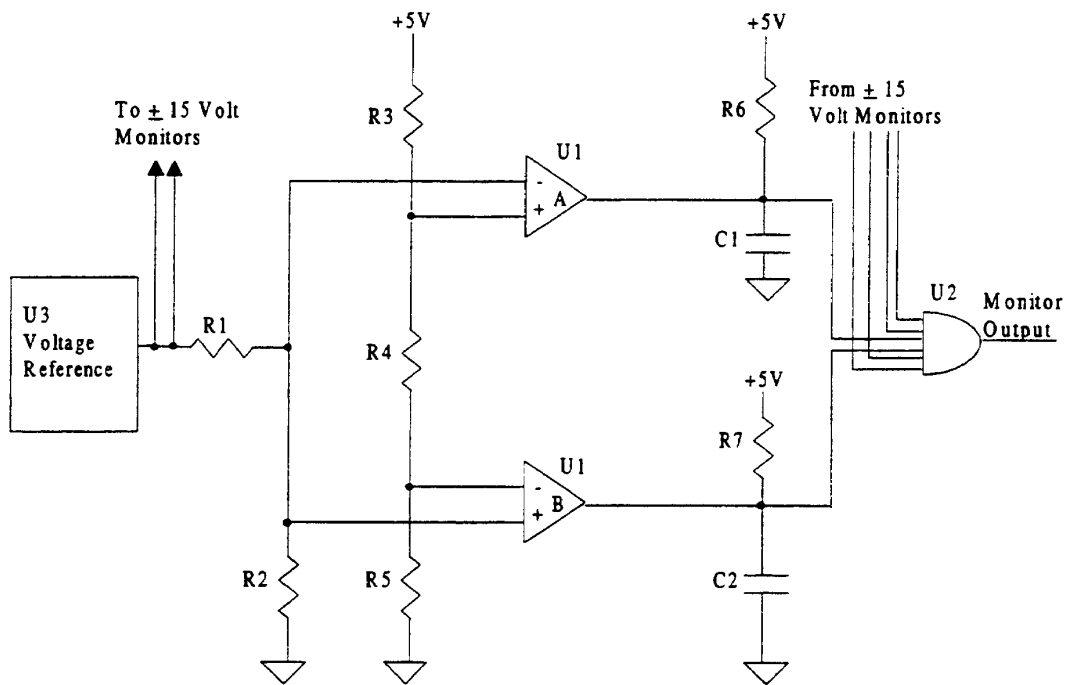
FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

FIGURE 3.0-3 - (SSA BSCU - FMEA) Schematic of Power Supply Monitor

NOTE: ±15 volt monitor uses same reference voltage and monitoring scheme.

4.0   POWER SUPPLY DETAIL ANALYSIS AND RESULTS

This FMEA contains two sections. Section 4.1 is the functional FMEA performed on the entire power supply. The functional FMEA on the power supply monitor has been deleted from the functional FMEA section since it is superseded by the piece part FMEA found in section 4.2.

4.1   Functional FMEA

Initial analysis of the power supply was conducted by computing the total power supply failure rate based on parts counts and failure rates. Conservative analysis did not meet the budget for Undetectable power supply failure causes inadvertent braking. Therefore a functional FMEA was performed to provide better resolution into the failure rates of the various failure modes. The only failure that may cause bad data and may not be detected by a properly functioning power supply monitor is "Loss of/reduced filtering". This failure mode may cause increased ripple on the output voltages that may be at such a level and frequency that it is not detected by the monitor. Table 4.1-1 documents the Functional FMEA results.

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

4.1   (Continued):

(Editor's Note: Only the analysis of the +5 volt block is shown in detail. The results of an FMEA on the remainder of the Power Supply are included in the summary. This is done to remove pages of tables unnecessary to give a representative example of a functional FMEA.)

TABLE 4.1-1 - (SSA BSCU FMEA)
Functional Failure Modes and Effects Analysis for BSCU Power Supply

Function Name	Failure Mode	Failure Rate (E-6)	Flight Phase	Failure Effect	Detection Method	Comments
+5 Volt	+5V out of spec.	0.2143	All	Possible P/S shutdown	Power Supply Monitor trips, shuts down supply and passes "invalid power supply (P/S)" to other BSCU system	BSCU channel fails
	+5V short to ground	0.2857	All	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
	Loss of / reduced filtering	0.3571	All	Increase Ripple	May pass out of spec voltage to rest of BSCU if ripple is such that it is not detected by the P/S monitor	May cause spurious P/S monitor trip
	+5V open	0.5714	All	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
	No Effect	0.1429	All	No Effect	None/No Effect	No Effect
Total Failure Rate of +5V Supply		1.5714				

FIGURE L5 (Continued)

SAE ARP4761

NOTE: SSA BSCU - FMEA

4.2   Power Supply Monitor Piece Part FMEA

Initial analysis of the power supply monitor was conducted by computing the total power supply monitor failure rate based on parts counts and failure rates. It was found that the total failure rate of the power supply monitor was 3.06E-7 failures per hour thus not complying with the budgeted failure rate of 2.0E-7 for monitor fails valid. A detailed piece part FMEA was conducted to provide better resolution into the probability of a "Monitor Fails Valid" condition. Table 4.2-2 documents this piece part FMEA. Five general Failure Code categories were included to enhance summary failure classification. These Failure Effect Codes are defined in Table 4.2-1.

TABLE 4.2-1 - (SSA BSCU - FMEA) Failure Effect Categories

Failure Effect Code	Failure Effect Category
1.	Monitor Stuck Valid
2.	Nuisance Monitor Trip
3.	Monitor Stuck Tripped/Supply Shutdown
4.	Monitor Sensitivity Shifts
5.	No Effect

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

TABLE 4.2-2 - (SSA BSCU - FMEA) Piece Part Failure Modes
and Effects Analysis for BSCU Power Supply Monitor

Component ID	Part type	Failure Mode	Failure Mode Rate (E-6)	Failure Effect Code	Failure Effect	Detection Method
C1	Ceramic Capacitor	short	.0073	3	Under voltage monitor stuck tripped	P/S shut down by monitor
		open	.0013	2	Loss of delay, spurious monitor trips	P/S shutdown
		low cap.	.0019	2	Decrease delay to trip	
C2	Ceramic Capacitor	short	.0073	3	Over voltage monitor stuck tripped	P/S shut down by monitor
		open	.0013	2	Loss of delay, spurious monitor trips	P/S shutdown
		low cap	.0019	2	Decrease delay to trip	
U1A	Comparator IC	output open	.0124	1	Under volt monitor stuck valid	bench test
		output grounded	.0056	3	Under volt monitor trips	P/S shutdown
		high offset voltage	.0062	4	loss of monitor sensitivity	bench test
U1B	Comparator IC	output open	.0124	1	Over volt monitor stuck valid	bench test
		output grounded	.0056	3	Over volt monitor trips	P/S shutdown
		high offset voltage	.0062	4	loss of monitor sensitivity	bench test

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

TABLE 4.2-2 - (SSA BSCU - FMEA) Piece Part Failure Modes
and Effects Analysis for BSCU Power Supply Monitor (Continued)

Component ID	Part type	Failure Mode	Failure Mode Rate (E-6)	Failure Effect Code	Failure Effect	Detection Method
R1	Film Resistor	open	.0009	3	over volt monitor trips	P/S shutdown
		increase resistance	.0005	4	trip window shifts down	
		decrease resistance	.0004	4	trip window shifts up	
R2	Film Resistor	open	.0009	3	under volt monitor trips	P/S shutdown
		increase resistance	.0005	4	trip window shifts up	
		decrease resistance	.0004	4	trip window shifts down	
R3	Film Resistor	open	.0009	3	under volt monitor trips	P/S shutdown
		increase resistance	.0005	4	trip window shifts up	
		decrease resistance	.0004	4	trip window shifts down	
R4	Film Resistor	open	.0009	1	monitor stuck valid	bench test
		increase resistance	.0005	2	trip window tightens	bench test
		decrease resistance	.0004	1	trip window widens, may cause monitor stuck valid	bench test
R5	Film Resistor	open	.0009	3	over volt monitor trips	P/S shutdown
		increase resistance	.0005	4	trip window shifts down	
		decrease resistance	.0004	4	trip window shifts up	

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

TABLE 4.2-2 - (SSA BSCU - FMEA) Piece Part Failure Modes
and Effects Analysis for BSCU Power Supply Monitor (Continued)

Component ID	Part type	Failure Mode	Failure Mode Rate (E-6)	Failure Effect Code	Failure Effect	Detection Method
R6	Film Resistor	open	.0009	3	under volt monitor stuck tripped	P/S shutdown
		increase resistance	.0005	5	no effect	
		decrease resistance	.0004	5	no effect	
R7	Film Resistor	open	.0009	3	over volt monitor stuck tripped	P/S shutdown
		increase resistance	.0005	5	no effect	
		decrease resistance	.0004	5	no effect	
U2	AND gate	stuck high	.0108	1	monitor stuck valid	bench test
		stuck Low	.0054	3	monitor stuck tripped	P/S shutdown
U3	Voltage Reference	inop	.0110	3	overvolt monitor trip	P/S shutdown
		out of spec	.0058	4	window shift	
		short	.0026	3	monitor trip	P/S shutdown
		open	.0245	3	overvolt monitor trip	P/S shutdown
:	:	:	:	:	:	:

NOTE: Failures in failure effect category 4 may cause monitor effectiveness to be reduced.

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

4.2   (Continued):

(Editor's Note: For the purposes of this example, failure modes and failure rates for the ±15 volt monitors are assumed to be identical to the +5 volt monitor. In an actual FMEA the same detailed analysis would have to be completed on the ±15 volt monitors to determine the actual failure modes and rates.)

4.3   FMEA Summary

The BSCU level effect of "Loss of/reduced filtering" was unknown and might have contributed to "Undetectable BSCU failure causes inadvertent braking". It is extremely conservative to assume that all failures in this category will be undetectable and capable of causing "Undetectable BSCU failure causes inadvertent braking". Therefore a separate laboratory analysis of the effect on the system was performed. This analysis (reference 6) shows that none of the failures in the "Loss of/reduced filtering" effect category can cause inadvertent braking.

(Editor's Note: Laboratory analysis may be required in some instances to determine the actual effect of a failure mode. See Section G.2.2.3)

All other failure effect categories except "No effect" may contribute to "BSCU power supply failure caused bad data". These failures will be detected by a properly functioning power supply monitor. Table 4.3-1 summarizes the results of the power supply and power supply monitor FMEAs.

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMEA

TABLE 4.3-1 - (SSA BSCU FMEA)
BSCU Power Supply and Power Supply Monitor Failure Modes and Effects Summary

Failure Modes	Failure Rate (E-6)	BSCU Effect	Potential Failure Cause	Detection Method	Comments
Power Supply (P/S) Shutdown	8.21	BSCU system fails	+5 out of spec +5 short to gnd +5 volt open +15 out of spec ...	"Power valid" to other BSCU set invalid	BSCU System 2 provides braking command
Increased Ripple from P/S	1.86	Unknown	Loss/reduced filtering: +5 volts +15 volts -15 volts ...	Possibly undetected	Laboratory analysis was performed that indicates this mode does not cause inadvertent braking.
Properly Operating P/S Monitor cannot shut down P/S	0.57	P/S does not shut down following P/S failure	PWM input from voltage monitor stuck valid	Card level test only	Power valid signal shuts down BSCU 1 outputs. No obvious BSCU effect.
P/S Monitor Fails Valid	0.1429	Possible erroneous operation following P/S failure	U1A open U1B open R4 Open R4 decreased R U2 high ...	Bench test	Latent failure
P/S Monitor Tripped	0.1578	BSCU system fails	C1 short C1 open C2 short C2 open ...	"Power valid" to other BSCU set invalid	
No Effect (NE)	2.5554	None	+5 volt output NE R6 increase R R6 decrease R ...	None	None

FIGURE L5 (Continued)

SAE ARP4761

NOTE: SSA BSCU - FMEA

5.0 CONCLUSION

The FMEA of the power supply was necessary to verify the design implementation meets the budget of 1.2E-5 failures per hour for "BSCU Power Supply Failure Causes Bad Data". The actual failure rate for "BSCU Power Supply Failure Causes Bad Data" is 1.06E-5 failures per hour.

The FMEA of the power supply monitor was necessary to verify the design implementation meets the budget of 2E-7 failures per hour for failure of the power supply monitors where the failure mode of concern is "Power Supply Monitor Fails to Detect Power Supply Failure". The actual failure rate for "Power Supply Monitor Fails to Detect Power Supply Failure" is 1.429E-7 failures per hour.

The BSCU power supply meets the requirement for loss of power supply, undetectable failure that causes inadvertent braking, and power supply monitor fails to detect a power supply failure.

FIGURE L5 (Continued)

NOTE: SSA BSCU - FMES

FMES for the BSCU System

1.0   INTRODUCTION

This FMES provides a summary of the results of all BSCU FMEAs.

(Editor's Note: Results of other FMEAs that may have been performed are also included to provide a more extensive list of failure effects.)

(Editor's Note: For details on FMES process refer to Appendix H.)

2.0   REFERENCES

The following references were utilized in performing this analysis.

1) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"
2) Internal memo documenting FMEAs results relative to the BSCU System
3) BSCU released design and production documentation

3.0   BSCU DESCRIPTION

(Editor's Note: Normally a system description would be included here. However, since it's included elsewhere in Appendix L, it is not repeated here.)

4.0   FMES DATA

The failure effects from the FMEAs from Reference 2 were examined and summarized as shown in Table 4.0-1.

FIGURE L6

NOTE: SSA BSCU - FMES

TABLE 4.0-1 - (SSA BSCU - FMEA) FMES of BSCU Output Level Failure Effects

Failure Mode	Failure Rate	Potential Failure Cause *(source of failure)*	Detectability	Comments
Loss of braking command from system 1	4.35 E-5	-System 1 P/S shutdown - System 1 P/S monitor trips - System 1 command failed	- signal to crew alerting system	System 2 provides braking command
Loss of braking command from system 2	4.35 E-5	- System 2 P/S shutdown - System 2 P/S monitor trips - System 2 command failed	- signal to crew alerting system	System 1 provides braking command
Loss of Braking command from both system 1 and 2	1.6 E-9	-BSCU validity monitor stuck invalid - BSCU switch failed in intermediate position	Indication on system display "Loss of normal braking"	Discrete provided
Inadvertent brake command from system 1 or 2	0.85 E-9	-failures 3,5,9 of CMD1 I/O, CMD2 I/O *(FMEA BSCU)*	Obvious by effect	
Asymmetrical brake command from system 1 or 2	1.6 E-8	-failures 6,11,12 of CMD1COMP, CMD2COMP *(FMEA BSCU*	Obvious by effect	

(Editor's Note: Not all failures mentioned in the "Potential Failure Cause" column can be found in the FMEA in this example appendix, but it shows the principle of the FMES to summarize all failures with the same effect to get one failure mode for the next higher level of analysis.)

FIGURE L6 (Continued)

NOTE: SSA BSCU - CMA

Common Mode Analysis (CMA) for the BSCU

CMA of the BSCU Design Implementation (Item/Component Level CMA)

(Editor's Note: The processes and methods described in Appendix K should be utilized to develop an LRU CMA report similar to the following. The format of the report is left to the analyst, however the specific content should reflect the expected content as described in Appendix K and this example. This example depicts one format of a completed Item Common Mode Analysis.)

1.0   INTRODUCTION

This report documents the Brake System Control Unit (BSCU) Common Mode Analysis assuring that no single failures exist within the BSCU which can initiate a hazardous or catastrophic event. The BSCU provides redundant high integrity braking and anti-skid control for the S18 aircraft.

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable CMA appendix paragraph.)

Item CMA Paragraph #	Appendix K Paragraph #
4.1	K.3.1
4.2	K.3.2
4.3	K.3.3, K.4

2.0   REFERENCES

The following references were utilized in performing this analysis:

1) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process for Civil Airborne Systems and Equipment"
2) "Loss of All Wheel Braking" and "Inadvertent Wheel Braking" fault trees for the S18 Aircraft incorporating the BSCU System
3) Aircraft Functional Hazard Assessment for the S18 Aircraft
4) Preliminary Safety Assessment for the S18 Aircraft
5) BSCU design and production documentation
6) "Safety Segregation Design Guidelines for LRUs in Safety Critical Systems"

FIGURE L7

SAE ARP4761

NOTE: SSA BSCU - CMA

3.0   FUNCTION/SYSTEM DESCRIPTION

The BSCU is the LRU which provides the Normal brake system commands and the Anti Skid commands to the Normal and Alternate brake systems. The Normal system brake commands have the potential to initiate Inadvertent Braking, and reduce the availability of the Normal brake system relative to Loss of Wheel Braking; thus analysis of this function is required. The Anti Skid commands cannot engage the brakes, they can only remove a brake command generated elsewhere, therefore the Anti Skid design does not contribute to inadvertent braking. Given that Anti-skid does not contribute to the Reserve Braking system, it does not contribute to Total Loss of Wheel Braking. Analysis of Anti Skid functions is therefore not required.

The selected architecture for the BSCU is a Dual-Dual configuration consisting of two independent systems (System 1 and 2) each having two independent computation channels (command and monitor). Each System interfaces through a dedicated LRU connector (P1 or P2). The BSCU operates as an Active/Standby device where System 1 is normally active and System 2 is a standby system which is automatically switched on line upon System 1 failures detected by the System 1 in line monitoring. In line monitoring of both System 1 and System 2 combine to provide a Normal System shutdown and automatic reversion to Alternate Braking System when both BSCU systems are inoperative. Figure 3.0-1 depicts the BSCU architecture and its interfaces with other brake system elements.

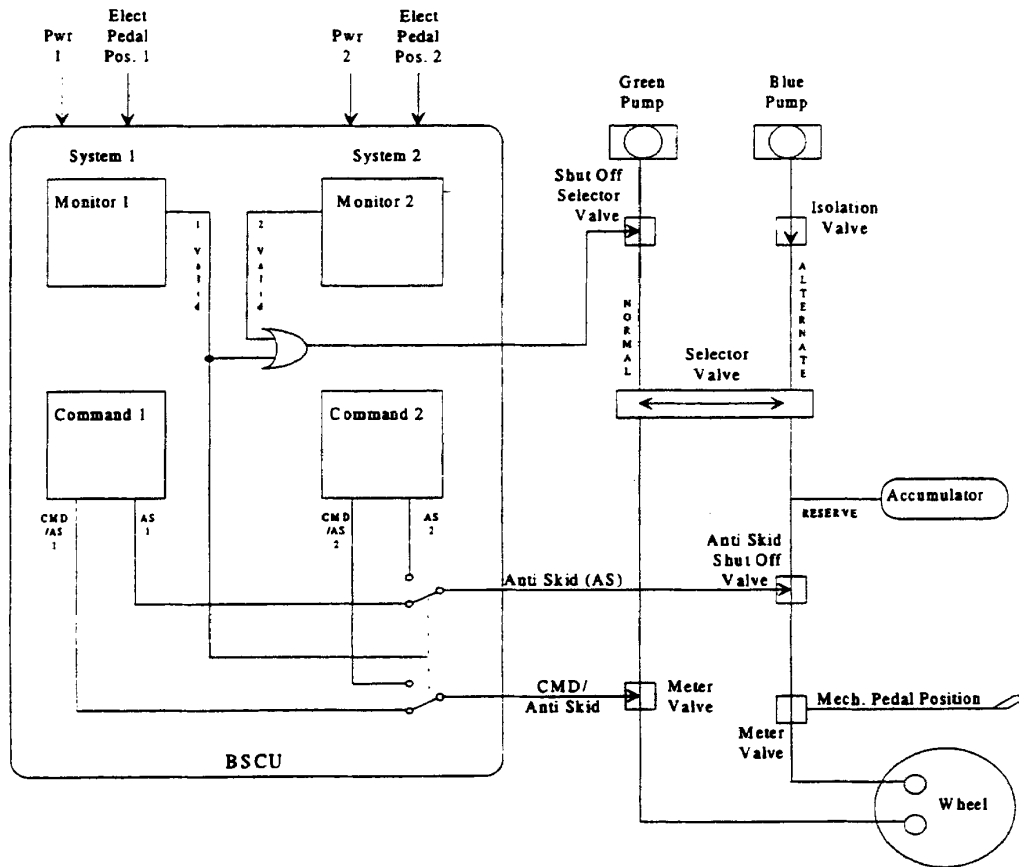FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

FIGURE 3.0-1 - (SSA BSCU - CMA) BSCU Architecture Diagram

FIGURE L7 (Continued)

SAE ARP4761

NOTE: SSA BSCU - CMA

4.0   BSCU CMA DETAIL

4.1   Common Mode Types, Sources and Failures/Errors Checklist

(Editor's Note: Appendix K section 2.1 provides guidance for establishing the Common Mode Types, Sources, and Failures/errors checklists.)

The common mode error/failure source listings in Appendix K of Reference 1 were reviewed to identify common mode sources applicable to the BSCU. The following error/failure sources were identified as relevant to the BSCU common mode analysis.

a.   Design considerations

(1) Common external sources to redundant functions
(2) Common electrical interfaces (connectors) within the redundant systems
(3) Generic Development Errors within redundant systems (hardware or software)
(4) Common failures effecting computation and monitoring functions

b.   Manufacturing considerations

(1) Inappropriate component substitution
(2) Improper assembly
(3) Common manufacturer of components
(4) Installation considerations
(5) Incomplete installation (connectors not mated)
(6) Incorrect installation (connectors interchanged)

c.   Environmental considerations

(1) Non-compliance with environmental requirements
(2) Non-compliance with electrical and radiation requirements

The above identified potential common mode error/failure sources are expected to be mitigated by one of the following Means of Acceptance.

a.   Design analysis/test
b.   Production testing
c.   Approved/controlled manufacturing processes
d.   Approved/controlled repair processes
e.   Certification/qualification testing

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

4.2   Analysis Requirements

(Editor's Note: Appendix K sections 3.2 (FHA/PSSA inputs) and section 3.3 provide guidance for establishing the analysis requirements.)

The BSCU CMA analysis requirements were identified by reviewing references 2, 3, and 4 and identifying Fault Tree AND-gates implemented within the BSCU and contributing to hazardous or catastrophic condition. Various BSCU functions were found to contribute to hazardous Loss of Wheel Braking, and catastrophic Inadvertent Wheel Braking events. Independence of these functions must be shown in order to assure absence of common mode faults due to Development Error. The following BSCU independence requirements were derived from the fault tree review.

1.   Loss of Wheel Braking

Loss of all wheel braking requires loss of Normal brake system, AND loss of Alternate brake system AND loss of Emergency/Reserve brake systems. The BSCU brake command output contributes only to the Normal system. The Anti Skid command output can contribute to loss of both the Normal and Alternate brake systems due to its ability to remove a brake command from other sources. No element of the BSCU contributes to the Emergency/Reserve braking system, therefore there can be no common mode BSCU failures which can inhibit all wheel braking. However; loss of the redundant BSCU systems can reduce availability of Normal braking as depicted in the fault tree.

2.   Inadvertent Wheel Braking

Any of the individual braking systems can contribute to inadvertent wheel braking, therefore it must be shown that the BSCU contains no common mode failures which may inadvertently activate the Normal braking system while the Normal system is active.

The Inadvertent Wheel Braking fault tree was analyzed to identify BSCU related failures and establish BSCU independence requirements. The following BSCU functions must be shown to be independent and free of common mode failures in order to validate the Inadvertent Wheel Braking fault tree.

1)   Failures of BSCU system computation must be independent from failures of the associated validity monitors and command switching outputs. This assures that single failures cannot cause an improper command and simultaneously inhibit monitor and removal of the command.

2)   Failures of each BSCU system's command and monitor channels must be independent to assure that single failures cannot impact both channels similarly, defeating the cross channel comparison monitor.

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

4.2   (Continued):

3)   Failures of each BSCU power supply and the associated power supply monitors must be independent to assure that no single failure can cause anomalous power supply operation and defeat the power supply monitor. (Since the power supply is common to the command and monitor channels of a given system, a power supply failure could similarly affect both channels, defeating the comparator.)

4)   Generic hardware or software errors in elements common to the command or monitor channels, or the validity/comparison monitors must be considered.

5)   Manufacturing considerations including common components within BSCU systems 1 and 2 and Manufacturing quality control must be considered.

6)   The installation must consider common mode errors such as connections, inspections, etc.

7)   The BSCU shall be designed considering environmental conditions for HIRF and lightning.

4.3   Common Mode Analysis

With the knowledge of intended operation as described in section 3.0, the actual implementation was reviewed relative to the independence requirements identified in section 4.2 and the segregation guidelines identified in reference 6. A number of factors were considered and are addressed individually in the following analysis.

Figure 4.3-1 depicts physical BSCU segregation zones separating the functions for which independence must be provided. Analysis was conducted by reviewing printed circuit wiring board documentation and other production assembly documentation. The design intent is that BSCU System 1 be entirely constrained within zone A while BSCU System 2 is constrained within zone B, assuring independence of systems 1 and 2. Each system is further divided into additional zones 1 and 2. This division provides independence of the MONITOR COMP and the POWER SUPPLY MONITOR functions in zone 1 from the COMMAND COMP and the POWER SUPPLY functions in zone 2, respectively. The "VALIDITY" and "SWITCHING" functions are within a unique zone, zone C, to provide independence from common element of both systems 1 and 2. This segregation design assures independence of the elements within each of these functions. The actual implemented design was reviewed to assure that the intent of the segregation was satisfied.

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

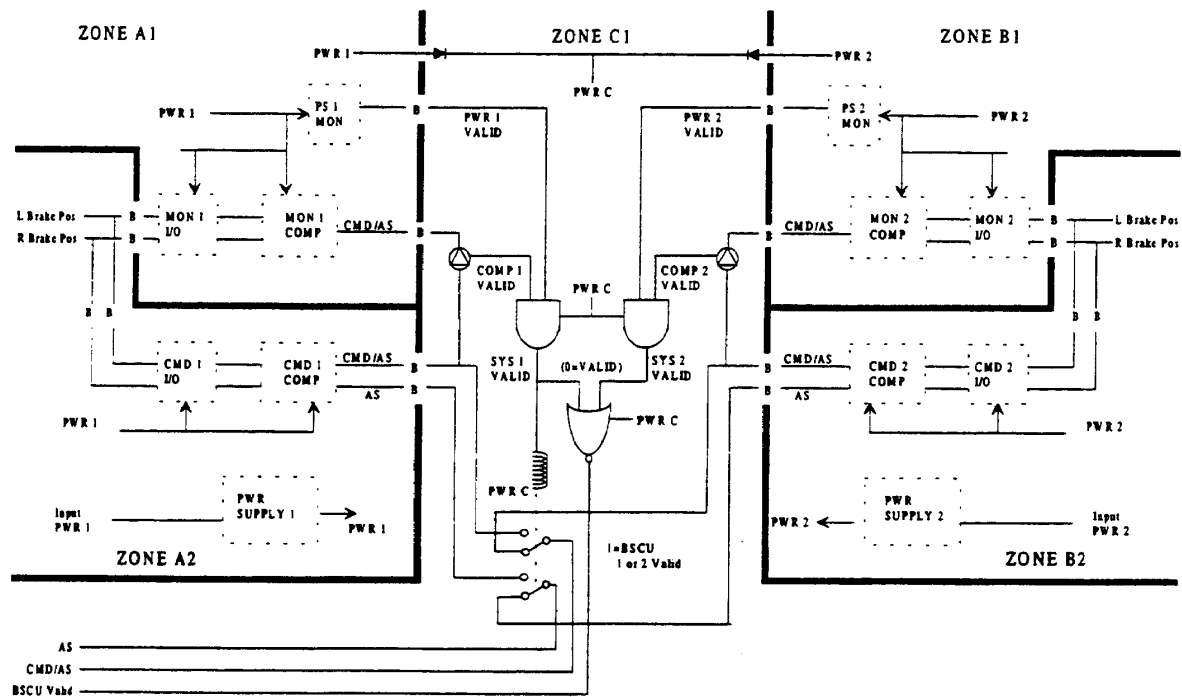FIGURE 4.3-1 - (SSA BSCU CMA) BSCU Physical Implementation

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

4.3   (Continued):

Analysis began at the inputs to the BSCU and flowed through each segregation zone to identify any unintended violations of the function segregation. The following list signals violated the segregation zones. These signals were further analyzed to assure they were acceptable and anticipated interconnections, and that appropriate buffering to prevent fault propagation was provided.

Power supply voltages were common to all elements in each System (however each system's power supply voltages were found to be independent). This is acceptable given the independent power monitor input to system validity.

The Monitor and Command computation channel Command/Anti Skid outputs and the Command computation channel Anti Skid output passed from their respective segregation zones into the validity/monitor zone. The comparison and command switching between systems functions is implemented within the validity/monitor segregation zone. The command signals must pass into that zone to be switched to the output as appropriate. Adequate buffering is provided to prevent fault propagation between zones. Thus these violations are acceptable.

System 2 BSCU Validity, Anti Skid, and Command/Anti Skid outputs passed from System 2 into System 1's validity/monitor channel. As with the similar violations of the System 1 commands, this is an anticipated violation given that the selection of which of the two systems is directed to the output is functionally implemented within System 1's validity/monitor zone. Again adequate buffering for fault propagation was present in the design.

Power and pedal inputs for each System were routed through independent system oriented connectors, keyed differently to preclude inadvertent interchanges of inputs to the two systems. All outputs from the BSCU are routed through the System 1 connector. Output functions and System 1 input functions are separated by grounded connectors pins, eliminating undetectable inadvertent shorts between input or power and brake command or validity outputs. The validity and command outputs are also isolated from each other within the connector.

Independence requirements 1, 2 and 3 of section 4.2 are satisfied by the segregation of functionality provided within the design implementation. The requirements in 4, 5, 6 and 7 of section 4.2 are satisfied as follows.

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

4.3   (Continued):

Requirement 4, Generic Failures in Components to Multiple Channels or Systems, is dealt with as follows.

a. Components (including software elements) common to multiple channels and/or systems were reviewed from the standpoint of assuring that a generic failure is either not possible, will not produce similar failure effects in multiple channels/systems, or will not affect both outputs and monitors of the respective outputs. The software elements are common to both BSCU Systems. The computation and monitor channel software has been developed and rigorously verified to Development Assurance Level A and B respectively, using DO-178 compliant processes, thus precluding design flaws of concern.

b. All components used in the BSCU design are common and relatively simple industry components used widely in similar systems in the past. Based on the extensive industry experience with these components, no adverse failure conditions are anticipated. This process sufficiently demonstrates the absence of generic type development errors in this device.

Requirement 5, Manufacturing Considerations, is dealt with as follows.

Manufacturing errors which could invalidate independence of the BSCU functions are controlled by a combination of controlled manufacturing processes, inspection of sequential assembly processes, and end product predelivery testing of each unit produced.

Requirement 6, Installation Considerations, is dealt with as follows.

Installation and maintenance related common mode errors are controlled by established maintenance procedures backed up by specific return to service testing. Additionally, unique connector keying eliminates reversing BSCU connectors.

Requirement 7, Environmental Considerations, is dealt with as follows.

Environmental considerations relative to common failure modes are eliminated through extensive qualification and certification testing conducted in accordance with DO-160 Environmental Standards.

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

4.4   LRU Level CMA Summary

Table 4.4-1 summarizes the results of the BSCU Common Mode Analysis.

TABLE 4.4-1 - (SSA BSCU - CMA) BSCU Common Mode Analysis Summary

Failure Condition	Common Mode Source	Design Justification	Ref. 4.2 Req. #
Loss of all Wheel Braking	BSCU failure	BSCU is associated only with Normal Brake system commands and has no brake command inputs to Alternate or Emergency systems.	Not Applicable
Reduction of availability of Normal braking system	Simultaneous BSCU System 1 & 2 failure	No common functions except output switching and validity which are appropriately buffered.	1
Inadvertent Braking due to common failures in BSCU command and monitor channels	Violation of Command and Monitor Segregation Zones	Common functions limited with buffering protection provided in accordance with segregation guidelines.	2
Inadvertent Braking due to inappropriate Power Supply Monitor Independence in the presence of anomalous system power supply outputs	Violation of Power Supply & Monitor Segregation Zones or inappropriate power monitor design	Common functions limited with buffering protection provided in accordance with segregation guidelines. Monitor outputs biased to invalid in absence of power or invalid power supplies.	3&4
Generic Common Component Failures	Violation of any required independence or generic development errors	Components used have either industry accepted integrity or have been exposed to special design verification processes.	5

FIGURE L7 (Continued)

NOTE: SSA BSCU - CMA

TABLE 4.4-1 - (SSA BSCU - CMA) BSCU Common Mode Analysis Summary (Continued)

Failure Condition	Common Mode Source	Design Justification	Ref. 4.2 Req. #
Manufacturing Considerations	Manufacturing errors violating independence	Certification Authority approved manufacturing & quality assurance processes in use. Final test and inspections preclude manufacturing errors.	6
LRU Test Deficiencies	Failure to detect latent failures at bench test	LRU bench test has been analyzed to assure coverage of safety critical latent failures.	6
Installation Considerations	Improper installation and/or maintenance on aircraft	Post maintenance "return to service" testing required prior to dispatch verifies system interfaces and operation.	7
Environmental Conditions	Environmental Induced Common Failures	Precluded by Extensive Environmental Qualification testing.	8

5.0 CONCLUSION

No BSCU common mode failures which could result in loss of wheel braking or inadvertent wheel braking were identified.

FIGURE L7 (Continued)

NOTE: SSA BSCU - FTA, DD, MA

BSCU - FTA (DD or MA) Report

1.0   INTRODUCTION

This report documents the Brake System Control Unit (BSCU) Fault Tree Analysis (Dependence Diagram or Markov Analysis) results.

(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to the applicable appendix paragraph.)

Item SSA Paragraph #	Appendix
4.0	C.3.1.1
5.0	C.3.1.2, 3.3
5.1	Appendix D
5.2	Appendix E
5.3	Appendix F

2.0   REFERENCES

  1) BSCU PSSA
  2) BSCU Specification
  3) BSCU FMEA
  4) BSCU FMES
  5) BSCU CMA
  6) BSCU Reliability Prediction Report

3.0   DESCRIPTION SUMMARY

(Editor's Note: The description for this example is the same as found in the BSCU PSSA section 3.0.)

4.0   SUMMARY OF BSCU ANALYSIS RESULT

FTA's (DDs or MAs) for significant BSCU undesired events were generated during the preliminary system safety assessment of the BSCU. This report formalizes those analyses with actual failure rates and exposure times.

Failure Effect	Requirement	Analysis Result
BSCU fault causes loss of braking commands	< 3.3 E-5/flight	1.5 E-6/flight
BSCU fault causes inadvertent braking after V1	< 2.5 E-9/flight	6.16 E -10/flight

FIGURE L8

NOTE: SSA BSCU - FTA, DD, MA

5.0   DETAIL OF BSCU ANALYSIS RESULTS

BSCU Fault Causes Loss of Braking Commands Analysis

Figures 5.1-1, 5.2-1, or 5.3-1 (FTA, DD, MA, respectively) show the final analysis for "BSCU Fault Causes Loss of Braking Commands". The total failure rate of the BSCU was used for "BSCU System 1(2) Failure". The system selection switch is tested every power up for ability to switch to both positions and the exposure time to the latent switch failures is 100 hours.

BSCU Fault Causes Inadvertent Braking After V1 Analysis

Figures 5.1-2, 5.2-2, or 5.3-2 (FTA, DD, MA, respectively) show the final analysis for "BSCU Commands Braking in Absence of Brake Input and Causes Inadvertent Braking". The BSCU CMA identified the power supply as a potential single point failure causing inadvertent braking commands from the active BSCU System. A FMEA was performed on the BSCU and determined that there are no single failures that can cause this fault.

Fault sequences involving failure of a monitor and failure of brake command circuitry are sequence dependent. The monitor must fail first. The power supple monitor and BSCU system validity monitors are only checked during off aircraft testing. An exposure time of 100,000 hours, the life of the aircraft is assigned to these failures to be conservative.

The fault tree shows that the software involved in the BSCU system validity monitor function was developed to Development Assurance Level B. The software involved in generating braking commands in the command channel was developed to Level A.

FIGURE L8 (Continued)

NOTE: SSA BSCU - FTA

5.1   BSCU Fault Tree Analyses

The BSCU fault trees are identified as follows.

a. Figure 5.1-1 BSCU Fault Causes Loss of Braking Commands

b. Figure 5.1-2 BSCU Commands Braking in Absence of Brake Input and Causes Inadvertent Braking

FIGURE L8 (Continued)
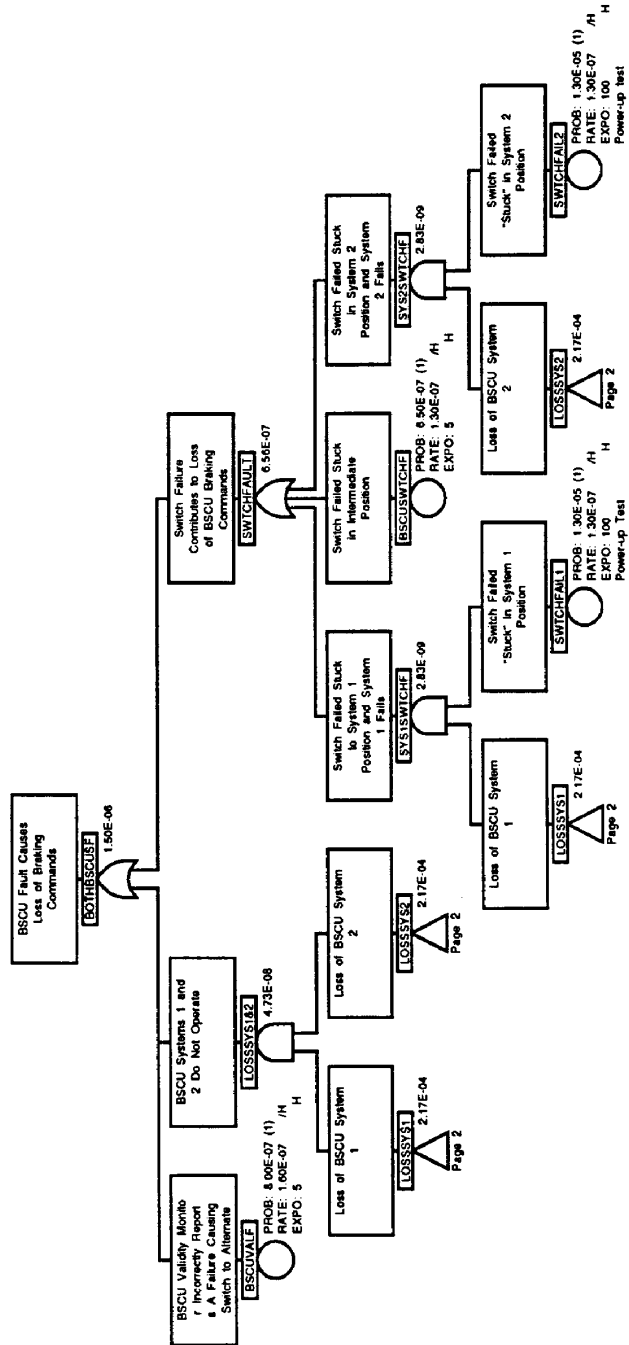
NOTE: SSA BSCU - FTA

FIGURE 5.1-1 - (SSA BSCU - FTA)
BSCU Fault Causes Loss of Braking Commands (Page 1)
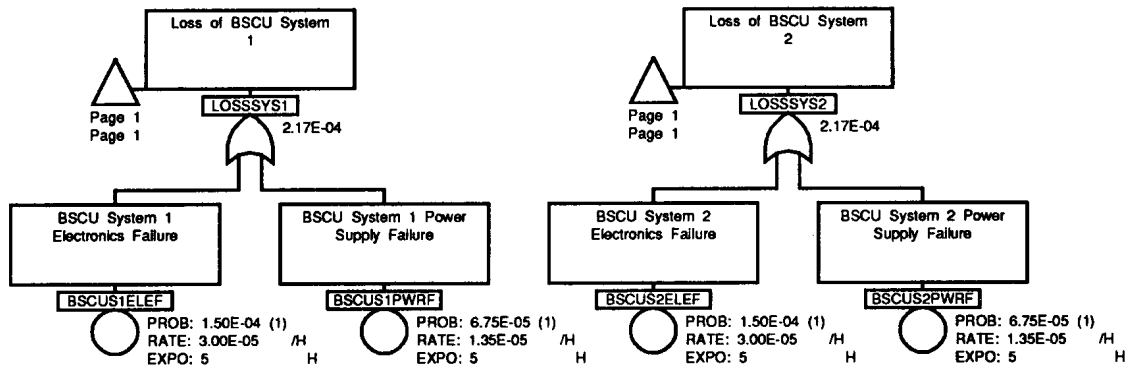
FIGURE L8 (Continued)

NOTE: SSA BSCU - FTA

FIGURE 5.1-1 - (SSA BSCU - FTA) BSCU Fault Causes Loss of Braking Commands (Page 2)

FIGURE L8 (Continued)

NOTE: SSA BSCU - FTA

FIGURE 5.1-2 - (SSA BSCU - FTA) BSCU Commands Braking in Absence of Brake Input and Causes Inadvertent Braking (Page 1)

FIGURE L8 (Continued)

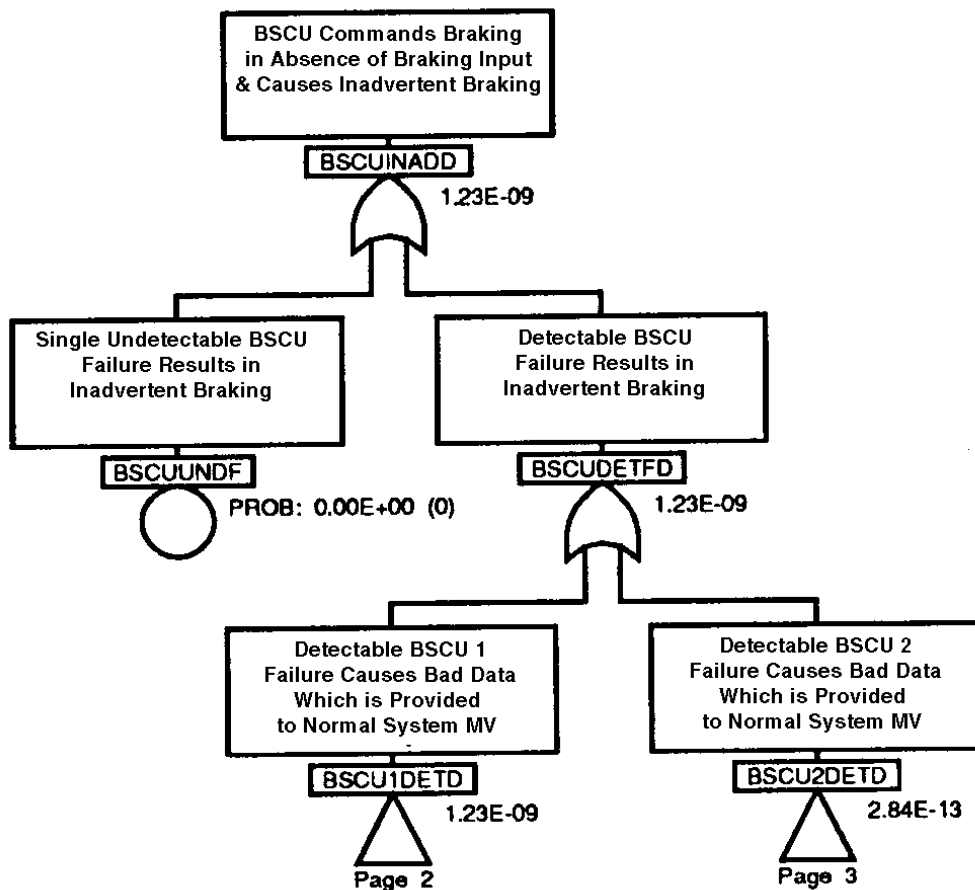NOTE: SSA BSCU - FTA

FIGURE 5.1-2 - (SSA BSCU - FTA)
BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking (Page 2)

FIGURE L8 (Continued)

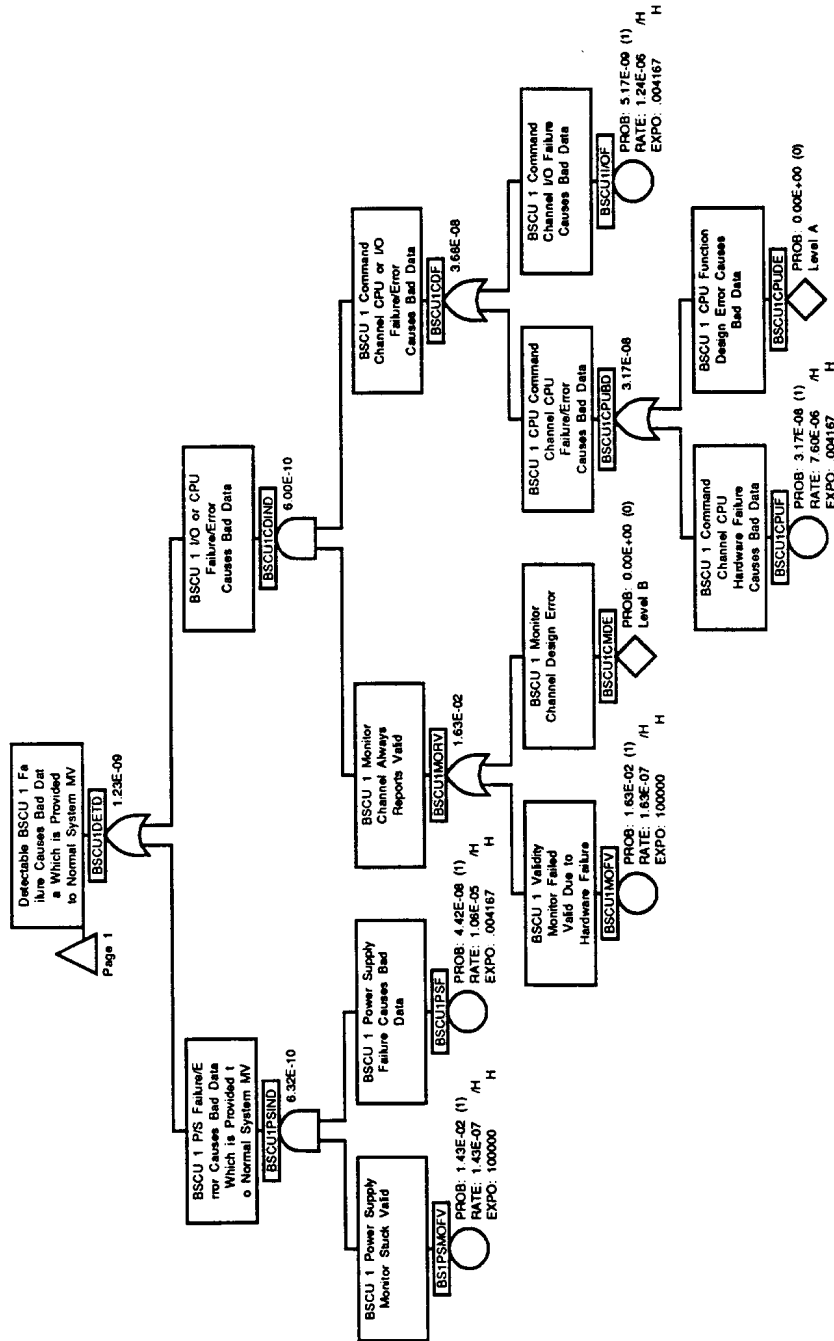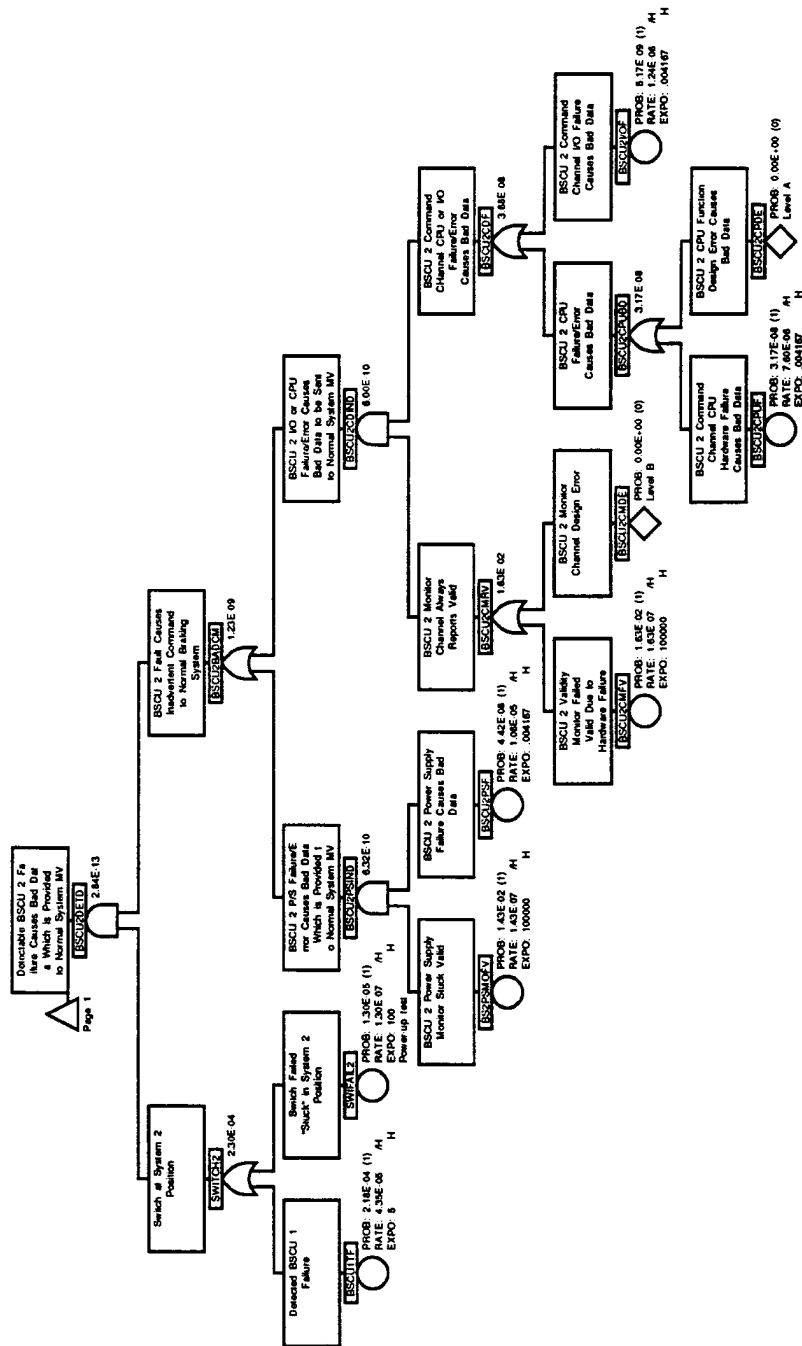NOTE: SSA BSCU - FTA

FIGURE 5.1-2 - (SSA BSCU - FTA)
BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking (Page 3)

FIGURE L8 (Continued)

NOTE: SSA BSCU - DD

5.2   BSCU Dependence Diagrams

(Editor's Note: Normally textual description of development of the DD would be included in the analysis. This text would be similar to that included in the preceding FTA example.)

The satisfactory compliance of the BSCU with its design objectives and failure rate budgets for the events of Loss of Braking and Inadvertent Braking is shown in the dependence diagrams included in Figures 5.2-1 and 5.2-2 respectively. These dependence diagrams are the same diagrams derived in the PSSA for the BSCU. However in the SSA diagrams, the failure rate budgets have been replaced with the actual failure rates derived through the FMES or various FMEAs conducted on the actual design as documented for production.
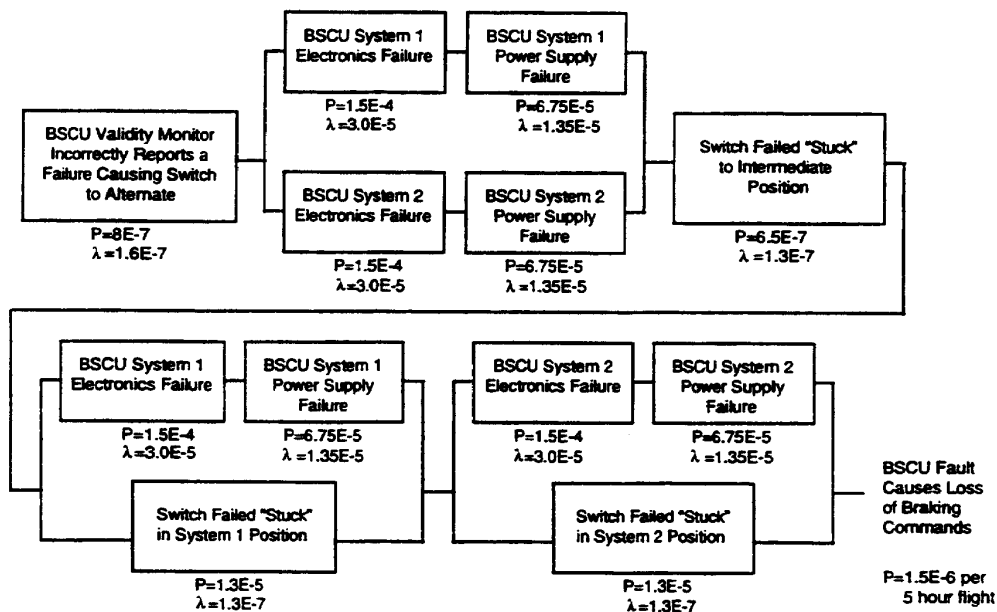

FIGURE 5.2-1 - (SSA BSCU - DD) BSCU Fault Causes Loss of Braking Commands
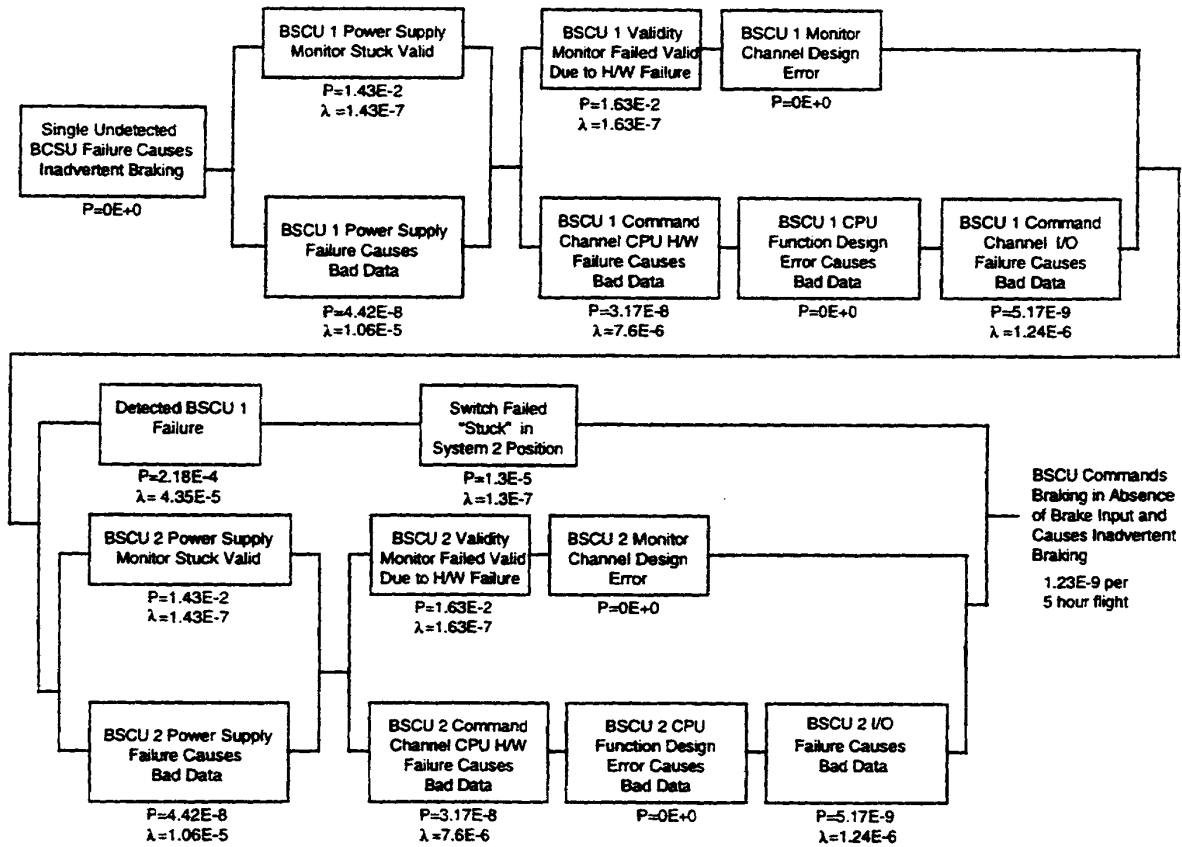
FIGURE L8 (Continued)

NOTE: SSA BSCU - DD

FIGURE 5.2-2 - (SSA BSCU - DD) BSCU Commands Braking in Absence of Brake Input
and Causes Inadvertent Braking

FIGURE L8 (Continued)

NOTE: SSA BSCU - MA

5.3   BSCU MARKOV ANALYSES

(Editor's Note: Normally textual description of development of the MA would be included in the analysis. This text would be similar to that included in the preceding FTA example.)

The satisfactory compliance of the BSCU with its design objectives and failure rate budgets for the events of Loss of Braking and Inadvertent Braking is shown by the analyses included in Figures 5.3-1 and 5.3-2 respectively. These analyses are the same ones derived in the PSSA for the BSCU. However in the SSA analyses, the failure rate budgets have been replaced with the actual failure rates derived through various FMEA analyses conducted on the actual design as documented for production.

The Markov Analyses for "BSCU Fault Causes Loss of Braking Command" is shown in Figure 5.3-1. There are three distinct components in the model. The first two components are BSCU System 1 and System 2 and the third component is Switching System. BSCU System 1 and System 2 have monitors in them and hence no single failure of any component within a BSCU System can cause loss of the wheel braking function. BSCU System 1 and System 2 are checked at the start of every flight. On the other hand, a single fault of the Switching System can cause loss of the NORMAL braking function. This can happen if the Switch fails:

a.   stuck to a failed BSCU System (sequence dependent),
b.   stuck open so that none of the BSCU systems are providing braking commands.

The Switching System is checked every maintenance check of T hours which is assumed to be 100 hrs. for this analysis. The BSCU System will fail in a flight if:

a.   both BSCU Systems fail in the same flight,
b.   the switching system failure is followed by the failure of a BSCU system to which the switching system is connected (sequence dependent),
c.   the switching system is stuck open and cannot provide any braking commands.

Figures 5.3-2 through 4 show the MA for inadvertent braking due to a monitor and an active failure in both BSCU systems. This Markov model is similar to the one used in the PSSA of the BSCU system, except that a sequence of failures is introduced. In the model shown in Figure 5.3-3, for example, a BSCU system is assumed to be failed only when the monitor of a system fails before the failure of an active item. Hence the BSCU CPU & I/O system fails only when the CPU & I/O monitor fails before the CPU & I/O fails in a flight. Similarly, the power monitor has to fail before a power supply for the power system to fail.

FIGURE L8 (Continued)
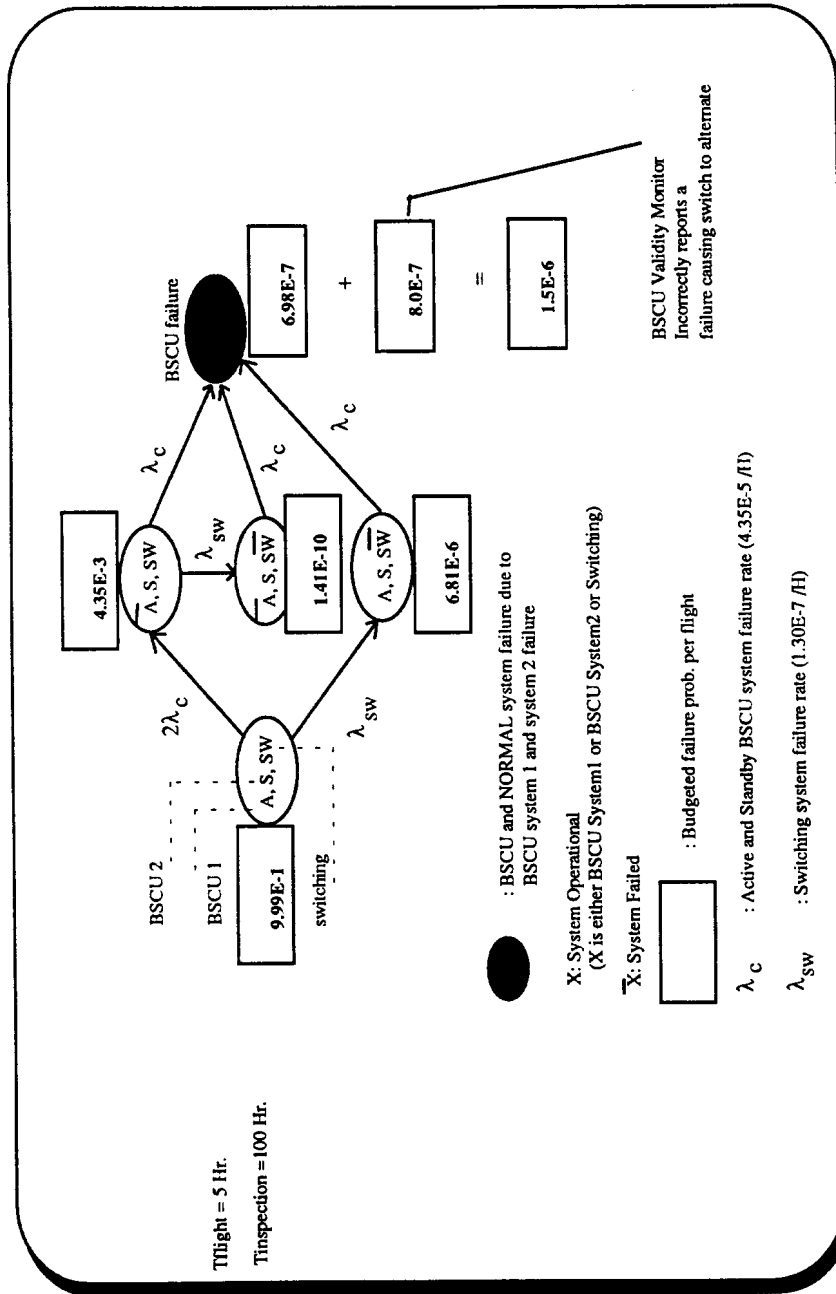
NOTE: SSA BSCU - MA

FIGURE 5.3-1 - (SSA BSCU - MA)
BSCU Fault Causes Loss of Braking Command

FIGURE L8 (Continued)

NOTE: SSA BSCU - MA

FIGURE 5.3-2 - (SSA BSCU - MA) Inadvertent Braking Due to Failure
of Both BSCU Systems and Their Monitors

FIGURE 5.3-3 - (SSA BSCU - MA) Inadvertent Braking Due to BSCU System 1 Failure
(Component repairs are not shown for clarity)

FIGURE L8 (Continued)

NOTE: SSA BSCU - MA

DETECTABLE BSCU 2 FAILURE CAUSES BAD DATA WHICH IS PROVIDED TO NORMAL SYSTEM

BSCU Power Supply System

BSCU CPU and I/O System

β

1.69E-1   1,1,1,1

0,1,1,1
3.57E-8

1,0,1,1
1.59E-2

1,1,0,1
4.28E-8

1,1,1,0
1.39E-2

0,1,0,1
1.58E-15

0,1,1,0
5.14E-10

1,0,1,0
2.29E-4

1,0,0,1
7.04E-10

1.22E-9

X

2.3E-04

=

2.81E-13

BSCU Validity Monitor System

BSCU Power Supply Monitor

PART C

FIGURE 5.3-4 - (SSA BSCU - MA) Inadvertent Braking Due to BSCU System 2 Failure and Switching Mechanism Failure (Component repairs are not shown for clarity)

FIGURE L8 (Continued)

NOTE: SSA Wheel Brake System

System Safety Assessment (SSA) for the Wheel Brake System

1.0   INTRODUCTION

The Wheel Brake System SSA is a compendium of the assessments and analyses performed in the development and verification phases of the design process for this system. These assessments and analyses include inputs from the Wheel Brake System PSSA. The purpose of the SSA is to provide a record of how the Wheel Brake System design meets the safety requirements established for it during the PSSA process.

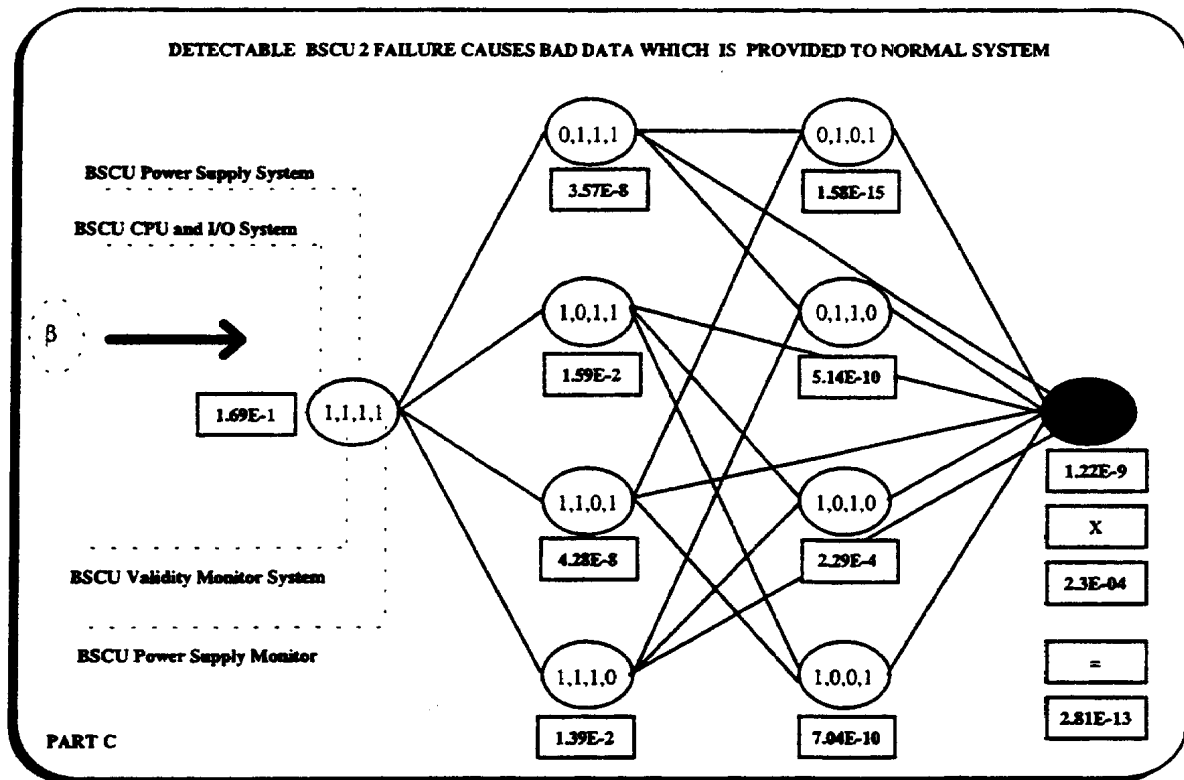*(Editor's Note: The following Cross Reference Table provides linkage from each example paragraph to applicable appendix paragraph.)*

System SSA Paragraph #	Appendix
4.0	C.3.1.1
5.0	C.3.3,
5.1	Appendix H
5.2	Appendix D
5.3	Appendix E
5.4	Appendix F
5.5	C.3.4, Appendix I, J & K

2.0   REFERENCES

1)   S18 Aircraft FHA
2)   Wheel Braking System PSSA (including system FHA)
3)   S18 Aircraft CMA
4)   Wheel Brake System CMA
5)   BSCU CMA
6)   S18 Particular Risk Analysis
7)   S18 Zonal Safety Analysis
8)   BSCU FMEA/FMES
9)   BSCU FTA
10) FAR/JAR 25.1309
11) ARP4754 "Certification Considerations for Highly-Integrated or Complex Aircraft Systems"
12) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"
13) S18 "Design Requirements and Objectives Document" (S18 Design Specification)

3.0   DESCRIPTION SUMMARY

(Editor's Note: For the purpose of this guideline, see the PSSA example for the Brake System Description. In the case of a real SSA, the updated and final description would also appear here.)

FIGURE L9

NOTE: SSA Wheel Brake System

4.0   WHEEL BRAKING SYSTEM SAFETY REQUIREMENTS

The following safety requirements will be satisfied by the S18 aircraft.

1)   Loss of all wheel braking during landing or RTO shall be less than 5E-7 per flight.
2)   Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5E-7 per flight.
3)   Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.
4)   Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.
5)   Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.
6)   The Normal, Alternate and Emergency systems shall be designed to preclude any common threats (e.g., tire burst, tire shred, flailing tread, structural deflection).
7)   The Normal, Alternate and Emergency systems shall be designed to preclude any common mode failures (e.g., hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).
8)   No single failure of the BSCU shall lead to inadvertent braking.
9)   The BSCU shall be designed to Development Assurance Level A.

5.0   SAFETY REQUIREMENTS VERIFICATIONS

The safety requirements identified in section 4.0 were determined to be correct and complete for the Wheel Brake System. The matrix shown in Table 5.0-1 identifies how each requirement was verified.

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System

TABLE 5.0-1 - (SSA Wheel Brake System) Wheel Brake System Safety
Requirements Verification Matrix

Safety Requirement	Results	Verification Method & Remarks
1. Loss of all wheel braking during landing or RTO shall be less than 5E-7 per flight.	Passed (3.2E-8)	Analysis See WBS SSA FTA 5.2-1
2. Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing shall be less than 5E-7 per flight.	Passed (4E-7)	Analysis See WBS SSA FTA 5.2-X (Editor's Note: This analysis is not shown in this example.)
3. Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight.	Passed (3E-7)	Analysis See WBS SSA FTA 5.2-Y (Editor's Note: This analysis is not shown in this example.)
4. Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.	Passed (4E-9)	Analysis See WBS SSA FTA 5.2-Z (Editor's Note: This analysis is not shown in this example.) See WBS CMA
5. Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight.	Passed (3E-9)	Analysis See WBS SSA FTA 5.2-AA (Editor's Note: This analysis is not shown in this example.) See WBS CMA
6. The Normal, Alternate and Emergency systems shall be designed to preclude any common threats. (tire burst, tire shred, flailing tread, structural deflection, etc.).	Passed	Analysis See Tire Burst -PRA

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System

TABLE 5.0-1 - (SSA Wheel Brake System) Wheel Brake System Safety
Requirements Verification Matrix (Continued)

Safety Requirement	Results	Verification Method & Remarks
7. The Normal, Alternate and Emergency system shall be design to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).	Passed	Analysis See WBS CMA
8. No single failure of the BSCU shall lead to inadvertent braking.	Passed	Analysis See BSCU CMA
9. The BSCU shall be designed to Development Assurance Level A.	Passed	Procedures/Audit See suppliers guidelines

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FMES

5.1   Failure Modes and Effects Summary

This report provides a Summary of the Wheel Braking System failure mode as identified by the FMEAs conducted on the various items within the Wheel Braking System.

The Wheel Braking System FMEAs were reviewed from the perspective of combining all identified failure modes that have the same Wheel Braking System top level failure effect. The composite failure rates for these effects were calculated by summing the individual failure rates contributing the failure effect. Table 5.1-1 documents the result of the summarization.

TABLE 5.1-1 - (SSA Wheel Brake System - FMES) FMES of Braking Failure Effects

Failure Mode	Failure Rate	Potential Effect on Braking System	Potential Failure Cause *(source of failure)*	Detectability	Comments
Loss of a single BSCU command channel	8.70E-5	None	- loss of brake command from channel 1 or 2 *(see BSCU FMES)*	by BITE, failure stored in BSCU	Redundant channel commands braking
Loss of both BSCU command channels	4.0E-7	Loss of Normal Braking mode	- failure of the BSCU *(see BSCU FMES)* - failure of brake pedal transducers *(see FMEA of pedal transducers)* - loss of power supplied to BSCU *(see SSA electrical system)*	Indication on system display: "Loss of normal braking"	Alternate braking is used. Autobrakes no longer available.
Inadvert-ent brake command	2.85E-8	Brakes are applied	- failure of the BSCU *(see BSCU FMES)* - failure of brake pedal transducers *(see FMEA of pedal transducers)*	Obvious by effect	Aircraft may over run available runway at high speed

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FMES

TABLE 5.1-1 - (SSA Wheel Brake System - FMES) FMES of Braking Failure Effects (Continued)

Failure Mode	Failure Rate	Potential Effect on Braking System	Potential Failure Cause (source of failure)	Detectability	Comments
Asym-metrical brake command	3.6E-8	Brakes applied asym-metrically between two landing gear	- failure of the BSCU (see BSCU FMES) - failure of brake pedal transducers (see FMEA of pedal transducers)	Obvious by effect	Aircraft may not track runway centerline
Loss of Green Hydraulic System		Loss of Normal Braking mode			Alternate braking is used. Autobrakes no longer available
Loss of Blue Hydraulic System		Loss of Alternate Braking mode			Normal braking is used.
...					
...					
...					

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FTA

5.2   Braking System Fault Tree Analyses

The satisfactory compliance of the WBS with its design objectives and failure rate budgets for the event of Loss of Braking is shown by the fault trees included in Figures 5.2-1. The fault tree is the same tree derived in the PSSA for the WBS, however in the SSA trees, the failure rate budgets have been replaced with the actual failure rates derived through various FMEA analyses conducted on the actual design as documented for production.

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FTA

Figure 5.2-1 - (SSA Wheel Brake System - FTA) Loss of All
Wheel Braking Fault Tree (Page 1)

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FTA

FIGURE 5.2-1 - (SSA Wheel Brake System - FTA)
Loss of All Wheel Braking Fault Tree (Page 2)

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - FTA

Loss of BSCU System 1

Page 2
Page 2

LOSSSYS1   2.17E-04

BSCU System 1 Electronics Failure

BSCUS1ELEF   PROB: 1.50E-04 (1)
RATE: 3.00E-05 /H
EXPO: 5 H

BSCU System 1 Power Supply Failure

BSCUS1PWRF   PROB: 6.75E-05 (1)
RATE: 1.35E-05 /H
EXPO: 5 H

Loss of BSCU System 2

Page 2
Page 2

LOSSSYS2   2.17E-04

BSCU System 2 Electronics Failure

BSCUS2ELEF   PROB: 1.50E-04 (1)
RATE: 3.00E-05 /H
EXPO: 5 H

BSCU System 2 Power Supply Failure

BSCUS2PWRF   PROB: 6.75E-05 (1)
RATE: 1.35E-05 /H
EXPO: 5 H

FIGURE 5.2-1 - (SSA Wheel Brake System - FTA) Loss of All Wheel Braking Fault Tree (Page 3)

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - DD

5.3   Braking System Dependence Diagrams

(Editor's Note: This section comprises a direct replacement for section 5.2 "Wheel Brake System FTA" in the SSA example.)

The satisfactory compliance of the WB with its design objectives and failure rate budgets for the events of Loss of Braking is shown by the dependence diagram included in Figures 5.3-1. This dependence diagram is the same one derived in the PSSA for the WBS. However in the SSA, the failure rate budgets have been replaced with the actual failure rates derived through various FMEAs conducted on the actual design as documented for production.

This report contains inputs from the Braking System FMES and the BSCU DD.
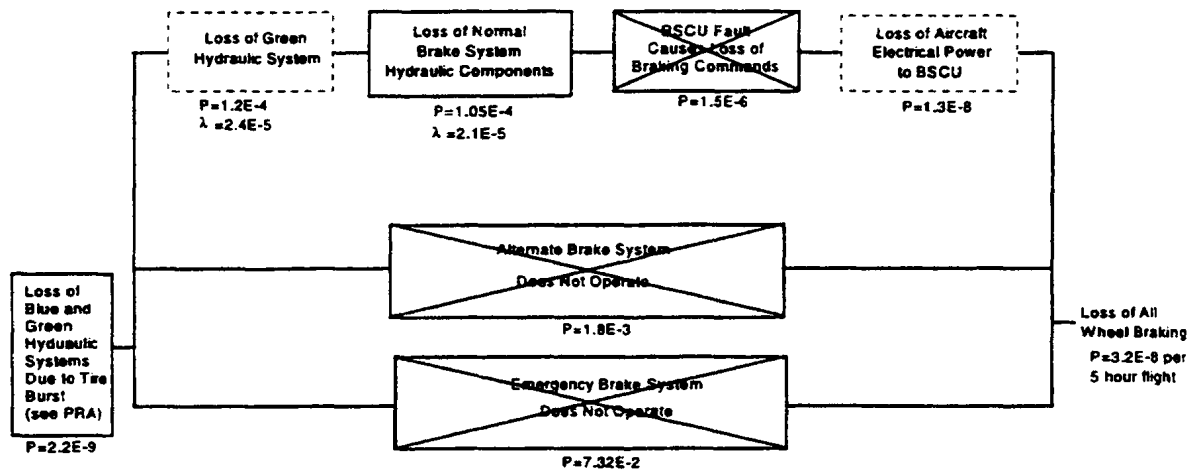
FIGURE 5.3-1 - (SSA Wheel Brake System - DD) Loss of All Wheel Braking

Editor's Note: The above dependence diagram is similar in structure to the Wheel Brake System PSSA DD except for the addition of the basic event, "Tire Burst" and a slight modification to accommodate the actual implementation of the BSCU. A single failure can cause loss of both BSCU systems which was not accounted for in the iteration of the "Unannunciated Loss of All Wheel Braking" PSSA DD. The single failure case does not prevent the implementation from meeting the requirements and so it is not necessary to re-design. It is necessary to account for the failure.)
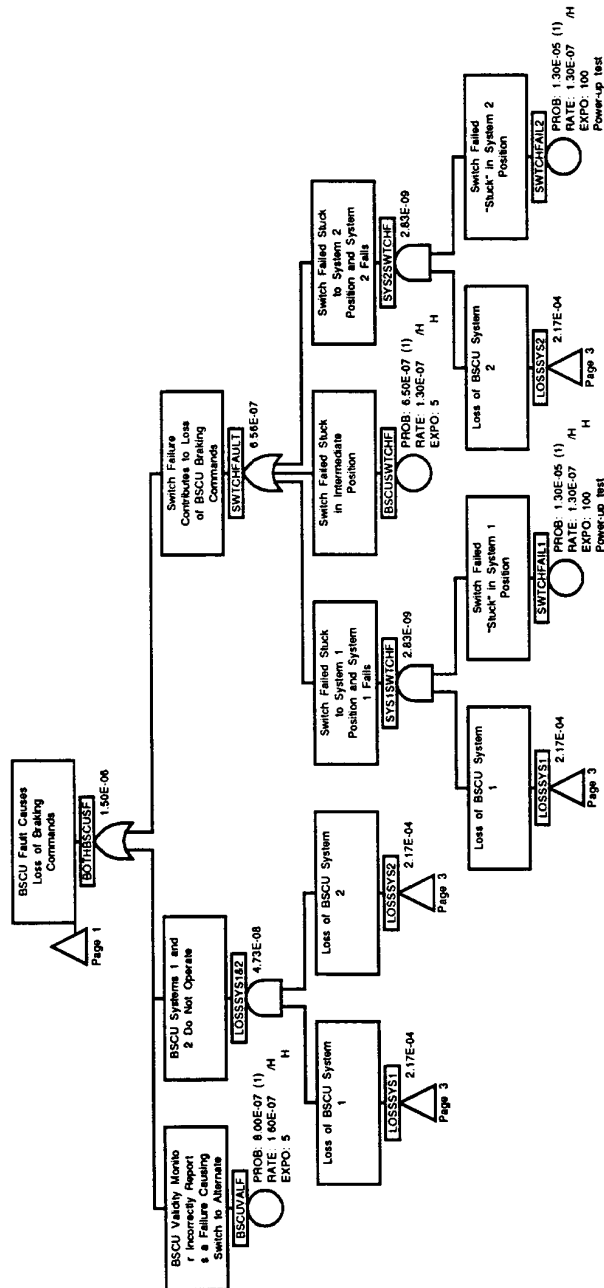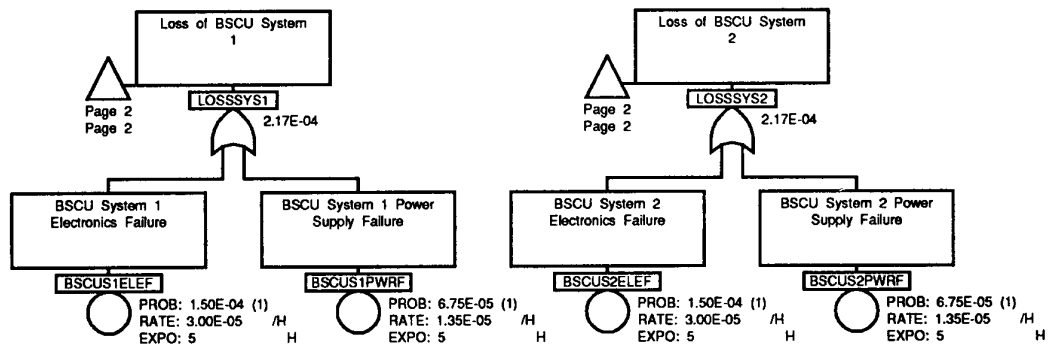
FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - MA

5.4   Braking System Markov Analysis

(Editor's Note: This section comprises a direct replacement for section 5.2 "Wheel Brake System FTA" in the SSA example.)

The Markov Analysis for "Loss of All Wheel Braking" involves the following two steps. First, the BSCU Mean Time Between Critical Failure (MTBCF) is calculated. The Markov chain shown in Figure 5.4-1 can be used to calculate the MTBCF of BSCU as a whole. Then, the MTBCF results can be incorporated into the System SSA Model. The MTBCF values calculated in the first step are used to calculate the NORMAL braking system failure rate. The NORMAL braking system failure rate is equal to 1/MTBCF of the BSCU dual channel system, plus the failure rate of the Green hydraulic supply, plus the failure rate of the NORMAL brake system hydraulic components.

The NORMAL braking system failure rate (λ_1) is 4.52E-5 per hour. The Markov chain shown in Figure 5.4-1 is solved to calculate the flight average probability of "Loss of All Wheel Braking". Failure rates used for ALTERNATE and EMERGENCY system are 3.6E-4 and 1.44E-2 failures per hour respectively. Average state probabilities per flight are shown in the Markov chain of Figure 5.4-1. The average probability of loss of all three braking functions is 2.98E-8 per 5 hour flight. This, when added with "Loss of Blue and Green Hydraulic Systems Due to Tire Burst" (probability 2.2E-9 per 5 hour flight), results in an average failure probability for "Loss of All Wheel Braking" of 3.2E-8 per 5 hour flight. This is well within the safety budgets of 5E-7 per flight probability of "Loss of All Wheel Braking".
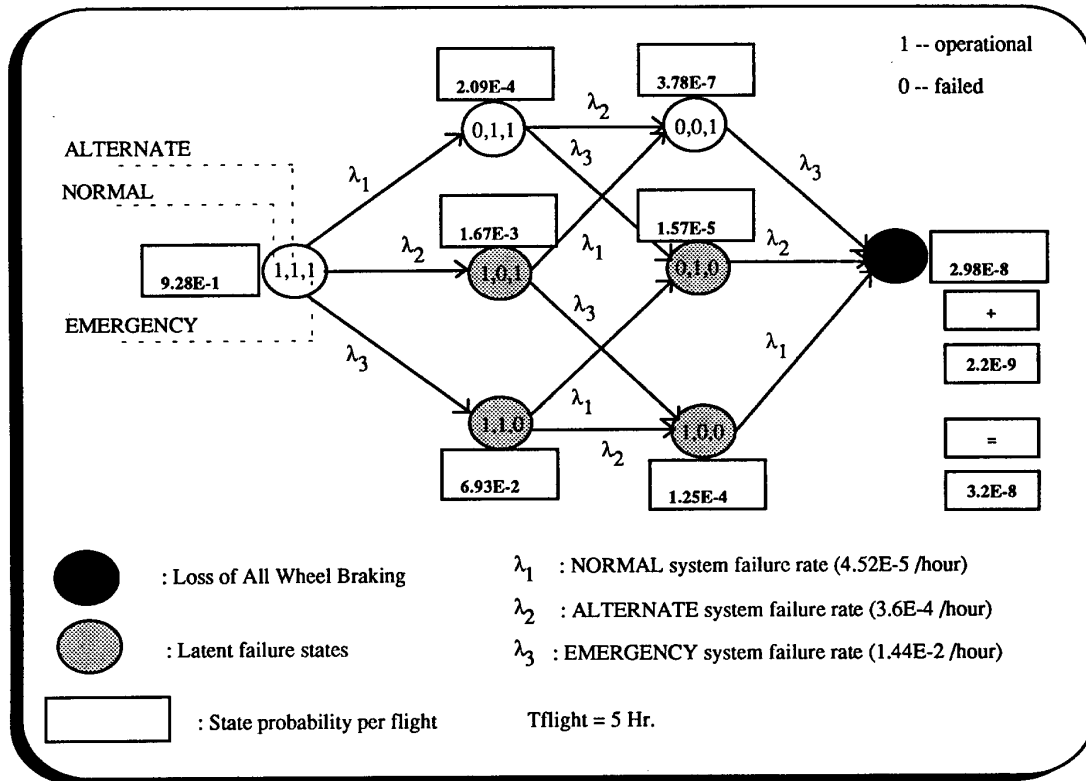
FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - MA

FIGURE 5.4-1 - (SSA Wheel Brake System - MA) Loss of All Wheel Braking

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - CCA

5.5   Braking System CCA, Summary of Results

5.5.1   Summary of the S18 Aircraft Zonal Safety Analysis Results, Relevant for the Braking System

The Zonal Safety Analysis No. YYY for the S18 aircraft shows that the Braking System installation complies with the installation guidelines and that no unacceptable common cause failure are expected from the installation.

Component failures with an effect external to the component have been considered in the fault tree.

5.2.2   Summary of the S18 Aircraft Particular Risk Analyses, Revelant for the Braking System

The following analyses have been performed for the S18 aircraft and are relevant for the Braking System.

1) Particular Risk Analysis No. XYZ S18 Aircraft
2) Particular Risk Analysis No. ZZZ for the S18 Aircraft, Fire, Tire burst, Lightning

(Editor's Note: Other analyses would have been performed for the S18 aircraft, but they are not shown here for brevity.)

The worst failure effect resulting from a particular risk is the "Total loss of wheel braking" due to tire burst. This failure has been considered in the FTA.

5.5.3   Summary of the S-18 Aircraft Common Mode Analysis for the Wheel Braking Function

The Common Mode Analysis for the Wheel Braking Function, No. ZXY and the Common Mode Analyses No. ZZZ for the Electrical System and No. WWW for the Hydraulic *System (Editor's Note: Which are not shown in this example)* showed that:

a. no event resulting from common mode type error has been identified which has a catastrophic effect.
b. those common mode type errors which could lead to a hazardous effect are restrained by special tests, manufacturing processes, quality assurance means or are acceptable because of their probability.

5.5.4   Common Mode Analysis for Main Items of the Braking System

A common mode analysis has been performed for the BSCU which shows, that no common mode failure of the BSCU exists, which could result in loss of wheel braking or inadvertent wheel braking.

FIGURE L9 (Continued)

NOTE: SSA Wheel Brake System - CCA

5.5.5   Braking System Safety Maintenance Task and Intervals

The following safety maintenance tasks and intervals have been identified.

1)   Operational Check of the alternate braking system interval: MT2
2)   Operational Check of Power Supply Monitors A and B interval: MT1

FIGURE L9 (Continued)

NOTE: SSA WBS Integration Crosscheck

5.6 System Integration Cross-check

Table 5.6-1 provides a compliance matrix assuring that the wheel brake system design analyzed within the SSA meets the objectives identified in the system level FHA paragraphs 4.6.

This matrix demonstrates acceptable compliance to the FHA objectives.

TABLE 5.6-1 - (SSA Wheel Brake System-Integration Cross-Check)
System Integration Cross-Check Compliance Matrix

FHA REQUIREMENT			DESIGN RESULTS FROM SSA		
No.	Condition	Objective	Event	Prob.	Reference
1	Loss of all braking during landing or RTO	5E-7	Loss of all wheel braking	3.2E-8	SSA FTA Fig. 5.2-1
2	Asymmetrical loss of wheel braking & loss of rudder or nose steering	5E-7	*(Editor's Note: Not developed in this example)*		
3	Inadvertent wheel braking during takeoff or landing rollout	5E-7	*(Editor's Note: Not developed in this example)*		
4	Inadvertent wheel braking during takeoff before V1	5E-9	*(Editor's Note: Not developed in this example)*		
5	Undetected inadvertent wheel braking during takeoff	5E-9	*(Editor's Note: Not developed in this example)*		

FIGURE L9 (Continued)

SAE ARP4761

NOTE: SSA - CCA - ZSA

A Zonal Safety Analysis (ZSA) for the S18 Aircraft

Main Landing Gear Bay ZSA

(Editor's Note: For details on the ZSA process, refer to Appendix I.)

1.0   INTRODUCTION

This analysis comprises the zonal safety analysis for the main landing gear bay of the S18 aircraft. The S18 aircraft must achieve the requirement that no event resulting from a single failure due to installation leads to a catastrophic failure condition *(Editor's Note: In this example "loss of deceleration capability")* and that failure conditions with hazardous failure effects have an adequately low probability.

(*Editor's Note: A ZSA document could include more than one zone, the example "main landing gear bay" was chose because a lot of systems are installed here which could affect either wheel braking and/or thrust reversers.)*

2.0   REFERENCES

1) S18 Aircraft FHA
2) Wheel Brake System FHA
3) Hydraulic System FHA
4) Thrust Reverser System FHA
5) Ground Spoiler System FHA
6) Design Guidelines, General S-18 Aircraft
7) Design Guidelines, Hydraulic Installation
8) Design Guidelines, Electrical Installation

3.0   DESCRIPTION

This zonal safety analysis (ZSA) example covers the Main landing gear bay. A detailed description of the zone is provided in section 4.2.1. The purpose is to show that a hazard to the aircraft and/or the occupants cannot be caused by the systems installed in this zone. The analysis has been performed on the first production aircraft using all relevant design and installation guidelines. Non-compliance's with these guidelines and their status are compiled in section 4.2.2 of this analysis. The analysis of the component-external failure modes and their effects on the relevant system itself and adjacent systems are shown in section 4.3.2.

Consideration of external events, e.g., engine non-containment and tire burst or wheel rim release, will be covered by separate Particular Risk Analyses.

FIGURE L10

NOTE: SSA - CCA - ZSA

4.0   ANALYSES TASKS

4.1   Preparation of the Design and Installation Guidelines

During the PSSA, relevant design guidelines and checklists are developed and utilized for the design and installation of all relevant systems. These are used during the ZSA for the SSA to show that the systems installation complies with those requirements.

(Editor's Note: The checklists provided in this example are only short versions. They will be developed usually only once for a specific project and can contain further guideline for specific zones such as fire zones.)

4.1.1   Example of General Design and Installation Guidelines

The following guidelines are examples which support an adequate installation of systems. This list should be enlarged and revised and developed in accordance with those design and installation guidelines applied by the user of this document.

a.   Equipment Installation (Including Pipes, Ducts, Hoses, Wires, Cables, etc.)

(1) The installation should ensure that no unacceptable stress is imposed.
(2) Attachments to moving parts should be mounted in such a way as to minimize stress.
(3) Attachments to moving parts should be positioned so that they do not obstruct and are not obstructed by adjacent structure or equipment.
(4) Pneumatic pipes and hoses should be installed so as to minimize water accumulation.
(5) The segregation of primary and secondary systems should be shown to be satisfactory with regard to the failure of one system affecting the other and failure of a separate system affecting both.

b.   Component Removal and Replacement

(1) A change of similar but not identical components should not have an unacceptable effect on system performance.
(2) Any component which could be installed in an incorrect orientation should not produce a problem. (e.g., cause a significant reduction in clearance or cause unacceptable stress on any connecting wire, cable, hose, etc.)
(3) Cross connection of connectors, pipes, etc., shall be prevented.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.1.1   (Continued):

    c. Maintenance and Servicing

       (1) All ground service connection points should be identified and/or arranged such that it is obvious which fluids should be used or which equipment connected.
       (2) Where possible, the design should allow replacement of items without removal of other equipment, in particular, equipment in other systems. If not, a check of all the involved systems should be made if a risk exists.
       (3) Consideration should be given to any possible hazards that might result from tools, bolts, etc., being inadvertently left on the aircraft.

    d. Drainage

       (1) Consideration should be given to implications on drainage of incorrect component/equipment installation.
       (2) There should be drainage in those areas or components where accumulation of liquid would be dangerous.

    NOTE: Fluids to be considered include water, chlorinated water, fuel, hydraulic fluid, cleaning and de-icing fluids, oil, sewage waste, etc.

4.1.2   Example of Specific Design and Installation Guidelines, by System

Specific design and installation guidelines for each system or ATA-chapter should be derived from experience, in-service data, the relevant PSSA and aircraft level requirements and objectives. As far as possible their origin shall be traceable and they should be agreed all partners concerned. The following guidelines are taken from ATA chapter 29 and are intended as examples.

    a. ATA 29 - Hydraulics

       (1) The air conditioning piping should normally be routed above the hydraulics.
       (2) When proximity of hydraulic and air conditioning systems is unavoidable a protective shielding is necessary. The ducting used for cabin air should be inert to hydraulic and other toxic or reactive contaminants likely to come in contact with it.
       (3) It should be possible to manually operate valves without use of special tools or dismantling.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.2   Check of the Installation Against Design and Installation Guidelines

The suitability and durability of materials used in the components, installation or structure is considered to be fundamental to the design.

The following items are considered to be fundamental to the design.

a. The effect of thermal variation
b. Structural Deflection
c. Pressure Variation
d. Build Tolerance
e. "g" effect
f. Vibration
g. Electrolytic incompatibility
h. Materials and Finishes
i. Effects of fluid contamination
j. Smoke emission, flame resistance and fire propagation

If obvious or suspected errors concerning the items are revealed as a result of Zonal Safety Analysis, a Query Sheet should be raised. External events, when appropriate, should be considered in conjunction with all other guidelines where applicable.

4.2.1   Zone Description

The Main Landing Gear Bay extends from frame C42 to frame C46/47 in the non-pressurized zone. It includes the main gear doors and houses the main gear when retracted.

At the left-hand side between frame C46/47 and C50 a part of the hydraulic system and the APU bleed air duct are located in the non-pressurized zone. This will be considered as part of the Main Landing Gear Bay.

4.2.1.1   Partitioning

Ceiling:	Class I (limit of pressurized zone)
Frame C42:	Limit of the Hydraulic bay: There are holes in this partition for ventilation purpose; center box; center tank.
Lower part:	Keel beam, main gear doors and fuselage structure of the belly fairing
Frame C46/47:	Class I (limit of pressurized zone)
Lateral partitions:	Fuselage structure of the belly fairing
Lateral partitions between frame C47 and C50:	Fuselage structure of the belly fairing and the pressurized fuselage

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.2.1.2   System Installation

The following systems/components are installed in the main landing gear bay.

a.   Blue hydraulic system pipes on the left hand side
b.   Yellow hydraulic system pipes on the right hand side
c.   Green hydraulic system pipes in the lower part
d.   Reservoir of green system
e.   Manifold green system equipped
f.   Power Transfer Unit (PTU)
g.   Manifolds
h.   Maintenance lights
i.   Brake system components
j.   Main Landing Gear
k.   Main Landing Gear free fall system
l.   Proximity sensors
m.   Slat drive power control unit (PCU)
n.   Flap drive power control unit (PCU)
o.   Flap drive transmission shafts
p.   Gearbox for slat and flap drive shafts
q.   Constant speed motor generator (CSMG) driven by hydraulic power
r.   Auxiliary Power Unit (APU) bleed duct
s.   APU Fuel line

The following systems/components are installed in the unpressurized area between frame C47 and C50.

a.   Ground service panel of green hydraulic system
b.   Ground service panel of blue hydraulic system
c.   Reservoir of blue system
d.   APU bleed air duct
e.   Trim air valve aft cargo compartment heating
f.   Trim air pressure regulator valve aft cargo compartment heating
g.   Electrical cables
h.   Hydraulic pipes

4.2.1.2.1   Fuel System

The shrouded APU fuel feed line is located in the left-hand side box. When the APU does not run, the fuel pipe is not under pressure and contains only a limited quantity of fuel. A fuel drainage pipe is installed on the right-hand side of the secondary keel beam. Other components like the valve and APU pump are sealed.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.2.1.2.2   Hydraulic System

The hydraulic system pipes are segregated. The blue ones are located on the left-hand side at frame C46/C47. The yellow hydraulic system pipes are placed on frame C42 on both sides and at frame C46/C47 on right hand side (see Figure 4.2.1.2.2-1). The routing of the yellow pipes from frame C42 to C45 is located above the pressure sealing.

The reservoir of the green system is installed on frame C42 whereas the other green system components and pipes are placed in the middle beneath the ceiling of the compartment (see Figure 4.2.1.2.2-2).

All hydraulic pipes in this region are manufactured from titanium alloy or stainless steel. No aluminum alloy is applied.

In the area between frame C46/C47 and C50 the pressure hydraulic pipe is installed below the APU bleed air duct and the optional cargo compartment hot air duct.

FIGURE L10 (Continued)
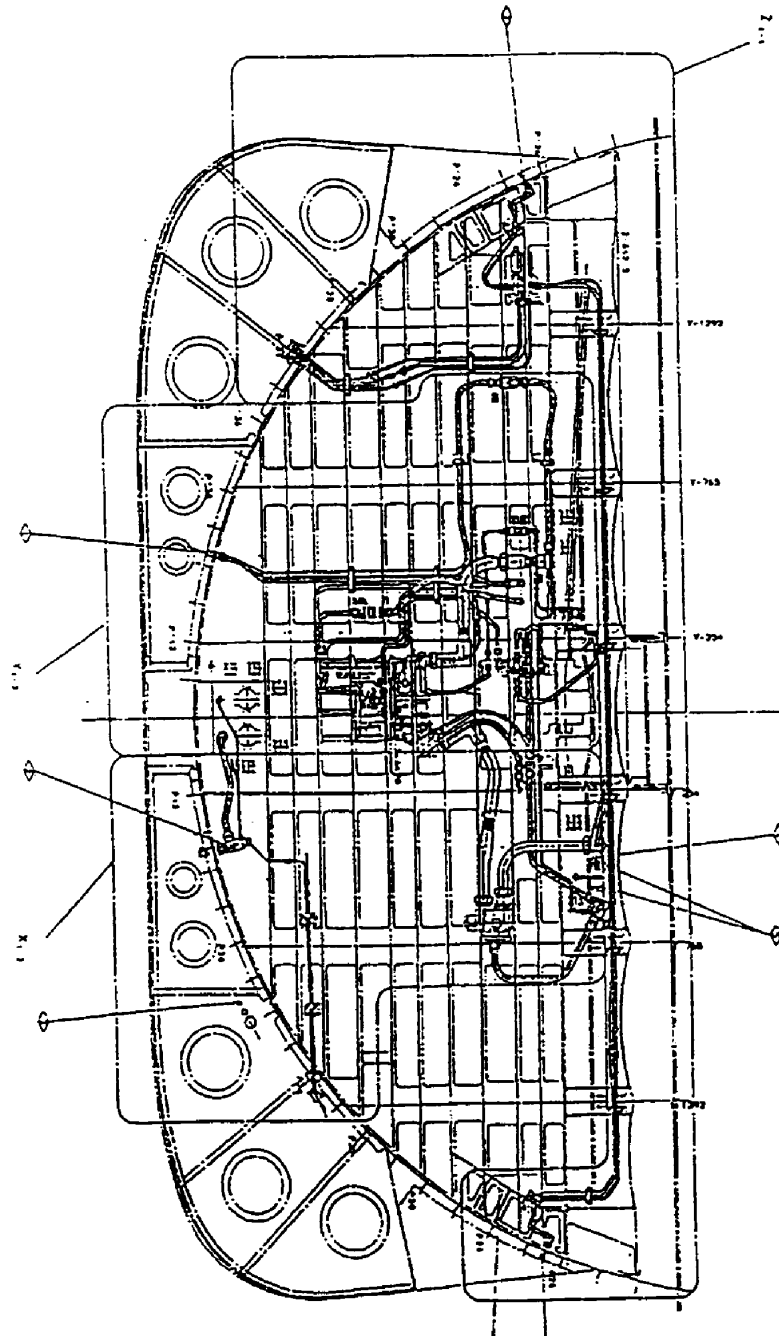
NOTE: SSA - CCA - ZSA

FIGURE 4.2.1.2.2-1 - (CCA - ZSA) Hydraulic Pipe Installation in Frame C46/47
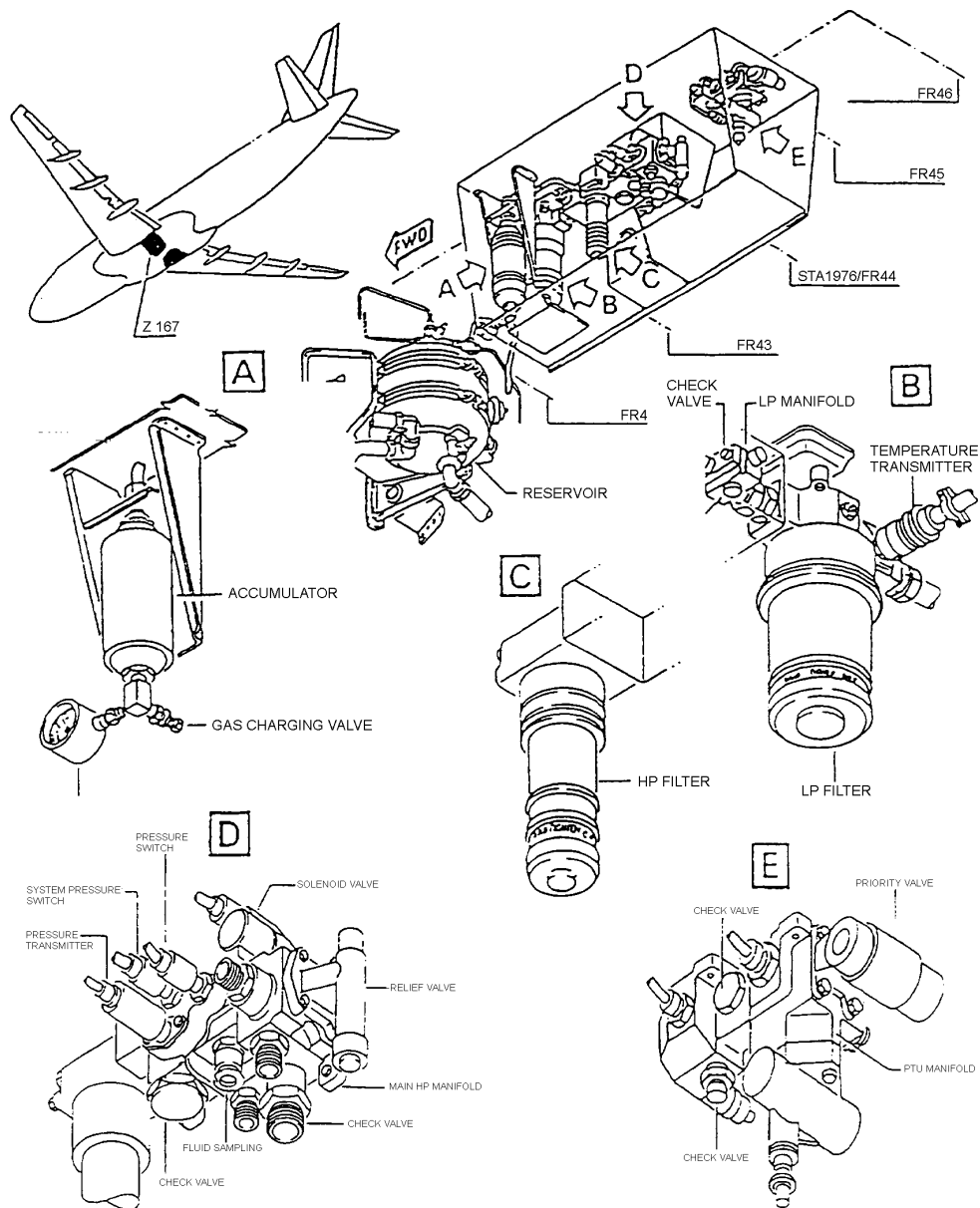
FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

FIGURE 4.2.1.2.2-2 - (CCA - ZSA) Green Hydraulic System Components

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.2.1.3   Zone Specific Design Considerations

4.2.1.3.1   Hot Surfaces

The tires are rated for a maximum temperature of 120°C. This temperature is not exceeded on the brake's outer surface areas.

The bleed air temperature can be up to 260°C under normal maximum system operating conditions or under single failure conditions of operation. The bleed air duct is manufactured from titanium. It is insulated with two layers of glass wool and a sealed with a kevlar outer skin.

The optional trim air pressure regulator valve, the venturi and the trim air valve are not insulated and can have a surface temperature up to 205°C.

4.2.1.3.2   Electrical Cables and Equipment

Cables are rated for continuous operation with a maximum temperature of 200°C. Cable bundles are installed in conduits. Cable bundles leading to the wings are installed in special conduits for lightning strike protection reasons.

Partition feed-through and connections are sealed. There is no discontinuity in the electrical wiring routed on the ceiling (no connection bars).

The emergency generator is placed on the keel beam.

4.2.1.3.3   Design Precautions to Minimize the Risk of Fire

The flap and slat PCU, the CSMG and the PTU are seal drained and the reservoir of the green system has an overflow to avoid hydraulic fluid leakage.

The APU fuel feed line is shrouded and drained.

The fuel valves and the APU pump are so designed that a fuel leakage to main landing gear bay is not probable.

Any leaking flammable fluid is drained overboard and any vapor will be scavenged by the ventilating airflow.

Brake overheat is detected via the brake temperature and monitoring system.

No aluminum alloy hydraulic pipes are used.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

4.2.1.3.3   (Continued):

The flap transmission shafts in front of frame C46 are safe guarded by retainers in case of shaft rupture.

A dual loop air leak detection system is installed.

In case of duct rupture a pressure relief is ensured by louvers in the main landing gear bay and over pressure breakout panels in the left hand part.

4.2.1.3.4   Ventilation

Figure 4.2.1.3.4-1 illustrates the main landing gear bay ventilation zone. On the ground, this bay is open and external conditions prevail. In-flight, fresh air flows in via the connection tubes from the ECS bay. A part of the air flows overboard via cooling exit louvers and the remainder flows into the hydraulic bay.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

CABIN

WING BOX

ACTUATOR

CONNECTION TUBE

WHEEL
WELL

AIR
CONDITIONING
BAY

EXCHANGER

NACA INTAKE

VARIABLE ANGLE RAMPS

EXIT - CONTROL FLAP

COOLING INTAKE - LOUVRES

VENTILATION SLOTS

HYDRAULIC BAY

FULLY SEALED U/C DOOR

COOLING EXIT - LOUVRES

INFLIGHT

CABIN

WING BOX

ACTUATOR

CONNECTION TUBE

WHEEL
WELL

AIR
CONDITIONING
BAY

ACTUATOR

EXCHANGER

NACA INTAKE

VARIABLE ANGLE RAMPS

EXIT - CONTROL FLAP

COOLING INTAKE - LOUVRES

VENTILATION SLOTS

HYDRAULIC BAY

COOLING EXIT - LOUVRES

ON GROUND

FIGURE 4.2.1.3.4-1 - (CCA - ZSA) Main Landing Gear (MLG) Bay Ventilation

FIGURE L10 (Continued)

SAE ARP4761

NOTE: SSA - CCA - ZSA

4.2.1.3.5   Drainage

The shroud of the APU fuel feed line is drained via the drain mast located between frame C46 and C47. Any fluids will be drained overboard via the belly fairing trough drain holes and small gaps in the seals of the undercarriage bay doors. As this zone is not pressurized, drainage is constant in flight and on ground.

4.2.2   Results of the Check of the Installation Against Design and Installation Guidelines

The results of the check of the installation against design and installation guidelines are summarized in Table 4.2.2-1.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

TABLE 4.2.2-1 - (CCA - ZSA) Zonal Safety Analysis Summary Sheet

ZONAL SAFETY ANALYSIS SUMMARY SHEET

Aircraft Type/Standard:		Zone: **Main Landing Gear Bay**	Complied by:	Sheet: 01	of:
				01	
			Date:	Issue: 01	
Query Sheet No.	**Reason for non Compliance**		**Action Taken**	**Remarks**	
27.01	Flight control bolt installed head down.			Query Sheet OPEN.	
92.01	Long bonding strips.			Query Sheet OPEN.	
92.02	Chafing of conduits.		Installation drawing modified.	Query Sheet CLOSED.	
92.04	Missing drain holes in several conduits.			Query Sheet OPEN.	

FIGURE L10 (Continued)

SAE ARP4761

NOTE: SSA - CCA - ZSA

4.3 Check for Component-External Failure Modes and Their Effects on Systems Installed in the Main Landing Gear Bay.

4.3.1 Checklist for Interaction of Systems

Failures in a system may only have a limited effect on aircraft safety due to the way in which they change the operation of that system. Some failures however, may have a significant effect on aircraft safety by interacting with another adjacent system. The effects of such interactions are considered, by usage of an FMEA-type analysis, based on the list of installed components in the relevant zone, in the Zonal Safety Analysis and the relevant PSSA/SSA. Examples of failures external to components and their possible interactions are:

a. flailing broken torque shafts producing secondary damage to hydraulic lines, control cables, wiring, fuel pipes, etc.
b. leaks from oxygen pipe unions in close proximity to electrical equipment or combustible material.
c. equipment disconnection or failure, including detachment of nuts and bolts, etc., resulting in the possibility of subsequent jams to control runs.
d. debris from high energy rotating equipment failure causing secondary damage to aircraft system(s) or structure.
e. air leaks from engine bleed or air-conditioning line may generate high pressure in enclosed areas and/or generate high temperatures.
f. accumulator burst may cause secondary damage.
g. tire tread debris can damage structure and systems.
h. smoke generated from failed or overheated electrical equipment may affect crew operation.
i. leakage of any fluid (hot air, oxygen, fuel, water, hydraulic fluid, etc.) in close proximity to electrical equipment.
j. leakage of flammable fluid close to heat sources.
k. leakage of fluid (fuel, oil, hydraulic fluid, etc.) able to contaminate air conditioning system.
l. water waster system affecting other systems by internal or external leaks.

Some of those risks are also addressed as particular risks.

4.3.2 Results of the Check for Component-External Failure Modes and Their Effects on Systems Installed in the Main Landing Gear Bay

Table 4.3.2-1 lists the component external failure modes and their effects on the systems installed in the main landing gear bay.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

TABLE 4.3.2-1 - (CCA - ZSA) Component-External Failures and Implementation

ZONAL SAFETY ANALYSIS, COMPONENT-EXTERNAL FAILURES AND IMPLICATIONS

Aircraft:		System: Flight Controls Zone: Main Landing Gear Bay	Issue: 1 Date: Oct. 94	Prepared by: Page: 1 of 4
Ref.	Component Failure Mode	Effect on Aircraft	Symptoms to: 1. flight crew 2. ground crew	1. crew corrective action 2. aircraft condition after crew action
1	Slat power control unit leakage	Hydraulic leakage is drained overboard. Hydraulic vapor is ventilated overboard. PCU is seal drained. Effects on ATA 27 (slat system) or ATA 29 (hydraulics) see SSA of ATA 27 or ATA 29.	1. Hydraulic pressure (possible). 2. Damage will be detected by a maintenance action or zonal inspection.	See ATA 27 (slat system) and ATA 29 (hydraulics) SSA.
2	Flap power control unit leakage	Hydraulic leakage is drained overboard. Hydraulic vapor is ventilated overboard. PCU is seal drained. Effects on ATA 27 (flap system) or ATA 29 (hydraulics) see SSA of ATA 27 or ATA 29.	1. Hydraulic pressure (possible). 2. Damage will be detected by a maintenance action or zonal inspection.	See ATA 27 (flap system) and ATA 29 (hydraulics) SSA.
3	Flap shaft broken (left hand)	Broken shaft may damage green hydraulics lines at rear wall. Loss of green hydraulic system.	1. Flaps inoperable (Loss of green hydraulic pressure.)	See ATA 27 (flap system) and ATA 29 (hydraulics) SSA.
4	Flap shaft broken (right hand)	Broken shaft may damage yellow hydraulics lines at rear wall. Loss of yellow hydraulic system.	1. Flaps inoperable (Loss of yellow hydraulic pressure.)	See ATA 27 (flap system) and ATA 29 (hydraulics) SSA.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

TABLE 4.3.2-1 - (CCA - ZSA) Component-External Failure and Implementation (Continued)

ZONAL SAFETY ANALYSIS, COMPONENT-EXTERNAL FAILURES AND IMPLICATIONS

Aircraft:	System: Fuel System	Issue: 1	Prepared by:
	Zone: Main Landing Gear Bay	Date: Oct. 94	Page: 2 of 4
Ref.	Failure Component Mode	Effect on Aircraft	Symptoms to: 1. flight crew 2. ground crew	1. crew corrective action 2. aircraft condition after crew action
1	Center tank rear wall leakage	Fuel leakage will be drained overboard. Vapors are extracted by ventilation.	2. Damage will be detected by a maintenance action or a zonal inspection.	1. None
2	Leakage or rupture of drainage pipe	This pipe will carry fuel only in case of center tank leakage or leakage of the wing tanks entering the wing center box. Leakage will be drained overboard.	2. Damage will be detected by a maintenance action or a zonal inspection.	1. None
3	APU feeder pipe leakage	Pipe only under pressure if APU is running. Pipe is shrouded. fuel leakage will be drained overboard.	2. Damage will be detected by a maintenance action or a zonal inspection.	1. None

FIGURE L10 (Continued)

SAE ARP4761

NOTE: SSA - CCA - ZSA

TABLE 4.3.2-1 - (CCA - ZSA) Component-External Failure and Implementation (Continued)

ZONAL SAFETY ANALYSIS, COMPONENT-EXTERNAL FAILURES AND IMPLICATIONS

| Aircraft: | System: Hydraulic System | | Issue: 1 | Prepared by: |
| | Zone: Main Landing Gear Bay | | Date: Sept. 94 | Page: 3 of 4 |
Ref.	Failure Component Mode	Effect on Aircraft	Symptoms to: 1. flight crew 2. ground crew	1. crew corrective action after crew action 2. aircraft condition after crew action
1	Hydraulic pipe leakage or rupture	One hydraulic system inoperable (blue, green or yellow). Hydraulic leakage is drained overboard. Hydraulic vapor is ventilated overboard.	1. Loss of hydraulic pressure reservoir level indication	See ATA 29 (hydraulic system) SSA.
2	Hydraulic component leakage	One hydraulic system inoperable (blue, green or yellow). Hydraulic is drained overboard. Hydraulic vapor is ventilated overboard. Emergency generator and power transfer unit are seal drained.	1. Reduced hydraulic pressure.	See ATA 29 (hydraulic system) SSA.
3	Hydraulic accumulator burst (green system)	Green hydraulic system inoperable. Hydraulic leakage is drained overboard. Hydraulic vapor is ventilated overboard. Debris contained by kevlar wrapping. Effects on brake system see SSA.	1. Loss of hydraulic pressure.	See ATA 29 (hydraulic system) SSA.
4	Hydraulic accumulator burst (brake system)	Hydraulic leakage is drained overboard. Hydraulic vapor is ventilated overboard. Debris contained by kevlar wrapping.	1. Brake hydraulic pressure.	See Brake system SSA.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

TABLE 4.3.2-1 - (CCA - ZSA) Component-External Failure and Implementation (Continued)

ZONAL SAFETY ANALYSIS, COMPONENT-EXTERNAL FAILURES AND IMPLICATIONS

| Aircraft: | System: Bleed Air System | Issue: 1 | Prepared by: |
	Zone: Main Landing Gear Bay	Date: Sept. 94	Page: 4 of 4
Ref.	Failure Component Mode	Effect on Aircraft	Symptoms to: 1. flight crew 2. ground crew	1. crew corrective action 2. aircraft condition after crew action

1	Leakage of APU bleed air duct (in keel beam)	Hot bleed air will flow through keel beam ventilation holes.
		The overheat detection system will shut off the LH bleed air system.
			1. Overheat detection warning	1. Shut off of LH pack
				2. Only one bleed air
				   system is available.
				   Wing deicing system is
				   not operable.

2	Rupture of APU bleed air duct (in keel beam)	Hot bleed air will flow through keel beam ventilation holes.
		The overheat detection system will shut off the LH bleed air system.
		Pressure is restricted by louvers.
			1. Overheat detection warning	1. Shut off of LH pack
				2. Only one bleed air
				   system is available.
				   Wing deicing systems is
				   not operable.

FIGURE L10 (Continued)

NOTE: SSA - CCA - ZSA

5.0   CONCLUSION

This report describes the systems installation in the zone under investigation. It highlights the potential problems and their effects on the aircraft. If the effect on the aircraft has been considered to be not acceptable, according to the ZSA guidelines and checklists, this problem was discussed with the relevant design responsible and a modification has been initiated if necessary. This ensures that the installation of the systems provides an adequate safety level.

FIGURE L10 (Continued)

NOTE: SSA - CCA - PRA

A Particular Risk Analysis (PRA) for the S18 Aircraft

Tire Burst Failure Assessment

(Editor's Note: For details on the PRA process, refer to Appendix J.)

1.0   INTRODUCTION

This analysis covers the Particular Risk Analysis for the risk of a tire burst.

(Editor's Note: For brevity, this example covers only the burst of the main landing gear tires with the gear extended. A complete analysis would also consider nose wheel tires, gear retracted, etc.)

This analysis shall demonstrate that no tire burst could lead to a catastrophic failure condition *(Editor's Note: In this example "loss of deceleration capability")* and that the probability of hazardous failure conditions are acceptable *(Editor's Note: In this example, "loss of all wheel braking").*

2.0   REFERENCES

   1) S18 Aircraft FHA
   2) S18 Wheel Brake System FHA/PSSA
   3) S18 Flight Control System FHA/PSSA
   4) S18 Thrust Reverser System FHA/PSSA

Additionally, the Airworthiness Requirements applicable to tire failures are:

   5) FAR/JAR 25.729(f) which covers the protection of equipment on the landing gear and in the wheel wells from the effects of a single tire failure.
   6) FAR/JAR 25.1309 which covers equipment, systems and installations in general.
   7) FAR 25.963 (e) which covers prevention of debris penetration of fuel tank access or inspection hole covers.

3.0   DESCRIPTION

The purpose of this report is to describe the consequences of tire failures on the extended Main Landing Gear of the S18 aircraft in order to demonstrate compliance with applicable airworthiness regulations. The S18 aircraft is fitted with twin-wheel nose landing gear and four wheel bogie main landing gear (see Figure 3.0-1).

FIGURE L11

SAE ARP4761

NOTE: SSA - CCA - PRA

3.0   (Continued):

The analysis uses a standardized tire failure model, agreed upon with the airworthiness authorities, to assess the adequacy of the design and construction of the aircraft to protect against such failures. Test evidence or service experience on similar aircraft types is referenced where appropriate.

All event probabilities stated within the analysis are per flight.

3.1   Landing Gear Description

The S18 is equipped with a three element landing gear system which is retracted by hydraulic means during flight.

The Nose Landing Gear (NLG) is of twin-wheel type and retracts forwards into a bay in the forward fuselage. After retraction the profile of the fuselage is restored by three mechanically operated doors linked to the landing gear structure and two doors attached to the fuselage and operated by two hydraulic actuators.

The Main Landing Gear (MLG) are of four wheel bogie design and retract inboard about wing located pintles. After retraction of the MLG, four doors (two to each MLG) mechanically linked to the landing gear structure, restore the wing under-surface profile. The fuselage belly profile is restored by two hydraulically operated doors, one to each MLG.

All the landing gear legs are normally retracted and extended using power supplied by the green hydraulic system. If hydraulic power is not available the landing gear cannot be retracted, and if already retracted can only be extended using the battery powered Gravity Extension system. This electro-mechanical system unlocks the Nose and Main gear door and gear uplocks allowing the gear to fall to the downlocked position.
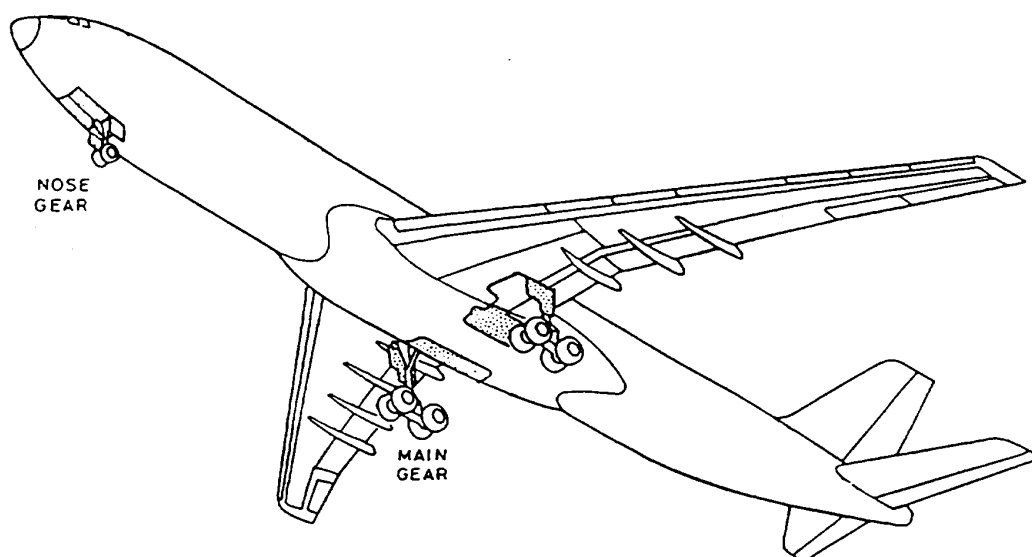
FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

FIGURE 3.0-1 - (CCA - PRA) S18 Aircraft Nose and Main Landing Gears

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.0 ANALYSIS

4.1 Tire Failure Model

4.1.1 General

In order to have a standardized set of conditions for the evaluation of the consequences of tire failures a failure model has been derived from a study of occurrence reports and previous practice adopted for certification of previous aircraft.

Within the model all failure probabilities are quoted per wheel per flight.

The conditions defined by the model were used as the basis for all tire particular risk assessments. Six failure modes were considered which are applicable to the S18 landing gear.

(Editor's Note: This example uses only one mode dealing with tire failures on the extended gear.)

4.1.2 Tire Burst Gear Extended

Tire burst occurring when the wheel is in contact with the ground produces tire treat debris. This may be projected in the wheel plane between 45° and 180° measured from ground horizontal plane in rearward direction. There is assumed to be a uniform risk of debris projection over this 135° arc.

In addition, tire pieces may be projected at up to 15° either side of the wheel plane, spread on a Gaussian distribution. Thus the probability of an item being struck by debris is dependent on the area of the item presented to the debris and its position relative to the tire. A chart or "window diagram" can be constructed from drawings for each wheel defining the area over which damage can occur. From these diagrams the probability of an item being struck can be calculated.

The following two sizes of tread debris are considered.

a. A large piece with dimensions WxW and a small piece 0.5Wx0.5W where W is the tire tread width.

b. In 10% of cases the failure of the first tire is considered to provoke the bursting and tread shed of a second tire due to overloading.

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.2   Method of Compliance

The effects of an impact by a single large or small debris piece on equipment in the wheel bays and on the landing gears legs are assessed to demonstrate compliance with FAR/JAR 25.729(f).

An assessment of the consequences of an impact by a single debris piece on structure, or systems outside the wheel bays; or double impacts on any location is made to demonstrate compliance with FAR/JAR 25.1309.

The effects of a single impact by either debris piece on fuel tank access panels are assessed to demonstrate compliance with FAR 25.963(e).

The means of assessment is analysis supported by test evidence.

4.3   Definition of Affected Zones/Areas

The analysis of the effects of tread shed is assessed by the locations noted below. For illustration see Figures 4.3-1 through 4. Damage from any individual debris piece will in most cases be able to strike only a single target location due to the geometry of the areas at risk and hence for this analysis damage to any single location only is considered.

a. MLG leg fairing and hinged door.
b. MLG leg and dressings
c. Lower wing skin
d. Access panels 541AB, BB, CB, DB/641AB, BB, CB, DB
e. Access panels 573DB/673DB
f. Fixed underwing panel
g. Shroud box
h. Overwing panel
i. Inner Rear Spar
j. Inboard flap
k. No. 2 Flap track and fairing
l. No. 1 Slat
m. No. 1 Spoiler
n. Lower forward fuselage
o. Belly fairing
p. Rear fuselage

FIGURE L11 (Continued)
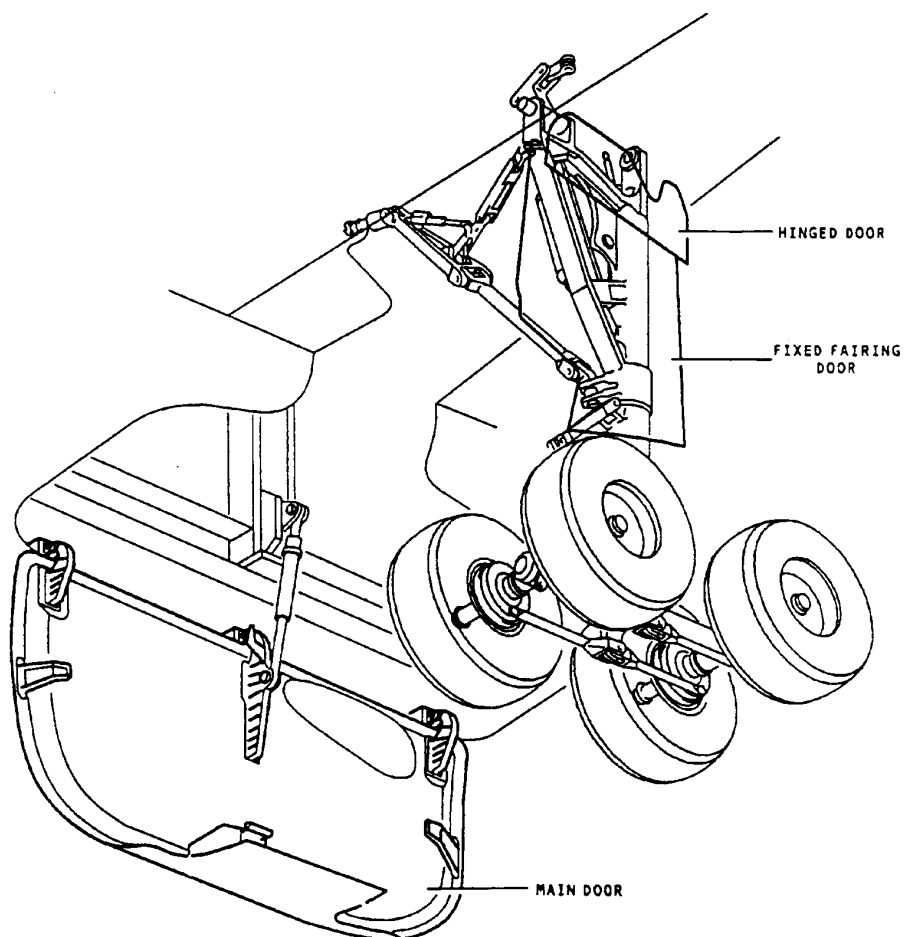
NOTE: SSA - CCA - PRA

FIGURE 4.3-1 - (CCA - PRA) Main Landing Gear Bay

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

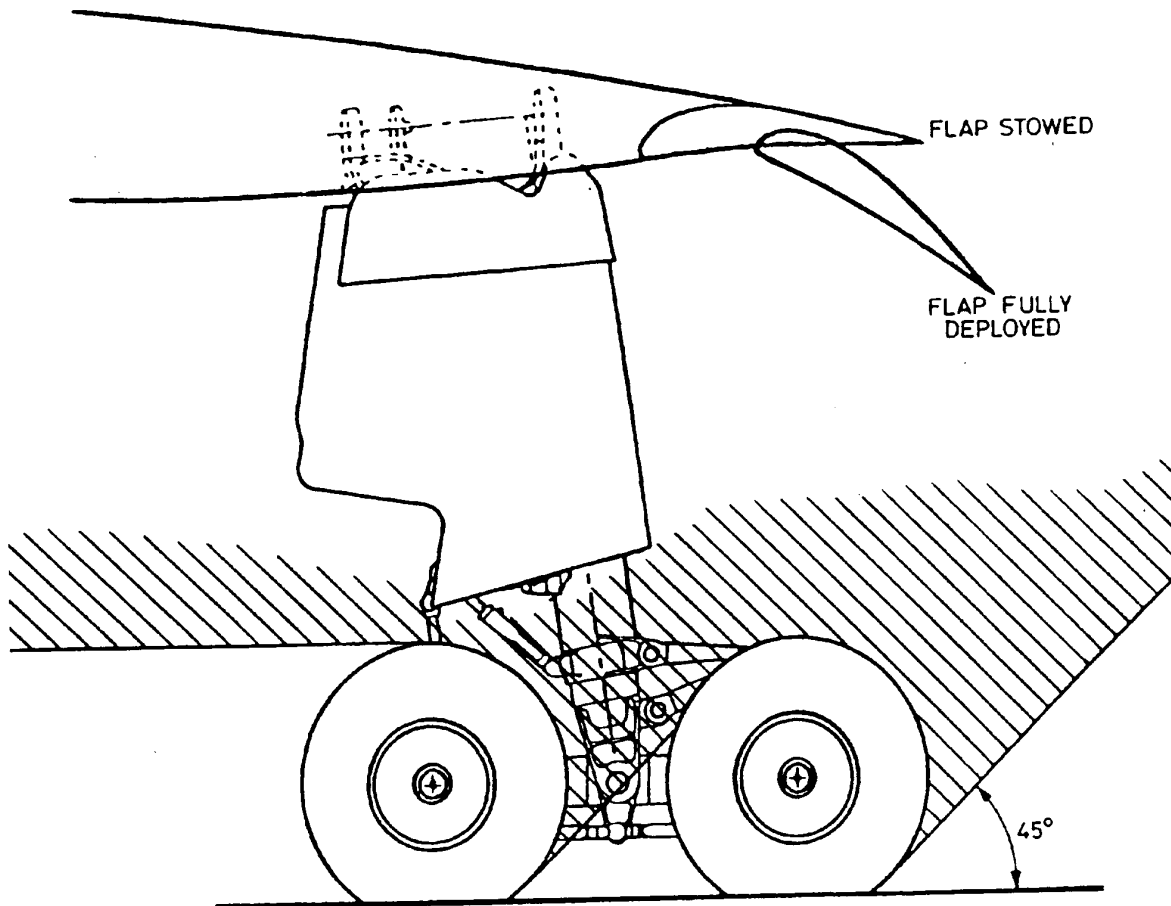FLAP STOWED

FLAP FULLY
DEPLOYED

45°

FIGURE 4.3-2 - (CCA - PRA) Tire Burst Area Side View
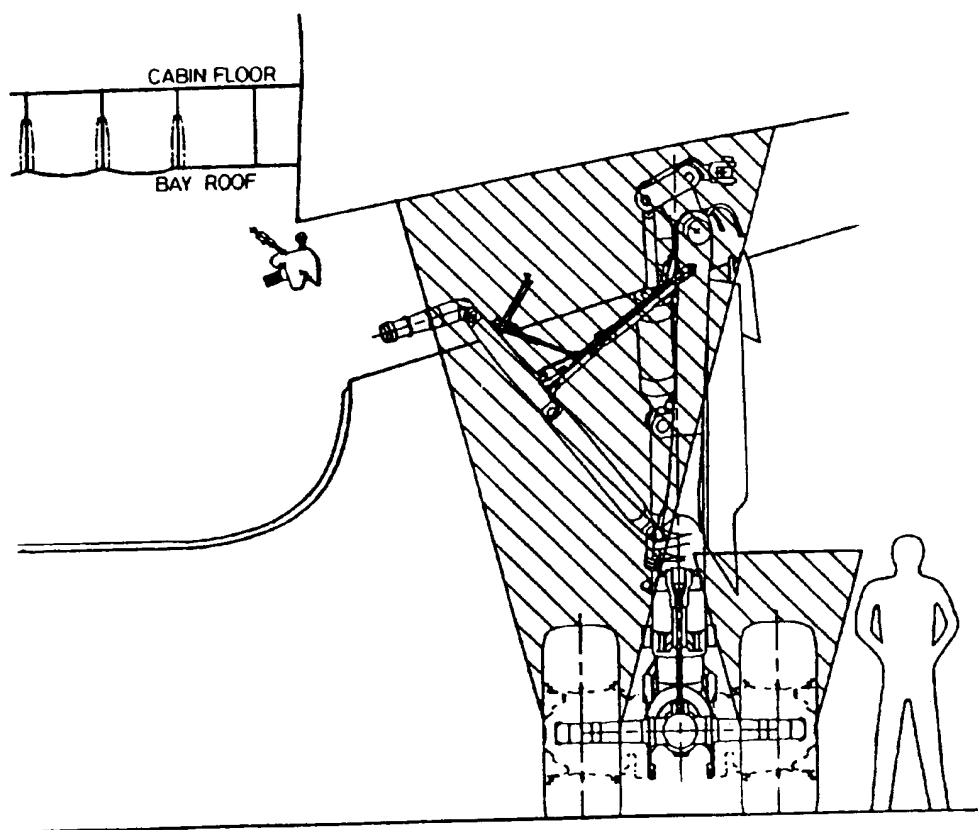
FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

FIGURE 4.3-3 - (CCA - PRA) Tire Burst Zone Area - Front View

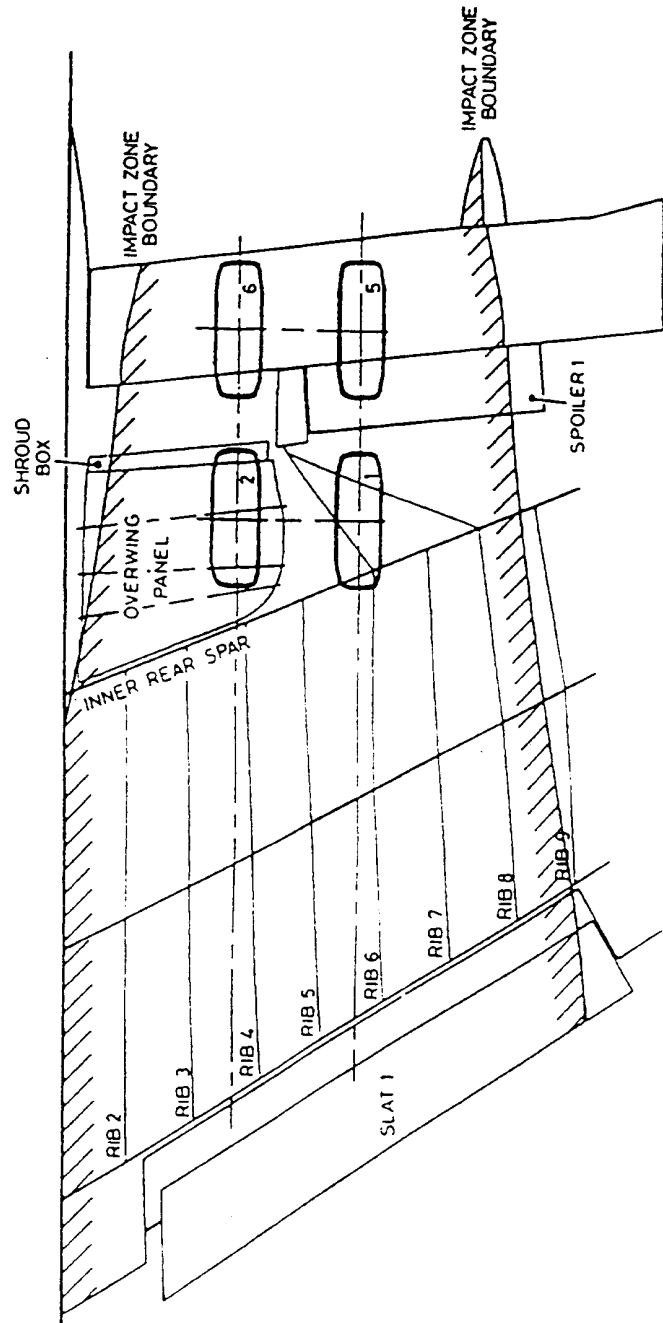FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

FIGURE 4.3-4 - (CCA - PRA) Tire Burst Zone Area - Top View

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.4   Definition of Affected Systems

The tire burst only affects the hydraulic and electric systems.

(Editor's Note: Normally the detailed information in the following chapters would be available in other PSSAs/SSAs and only the failure condition classification and a reference to theses PSSAs/SSAs would be needed here. The information here is to allow a complete example without the other analyses being available.)

4.4.1   General

This analysis considers that rigid and flexible hydraulic pipes are severed if struck by wheel or tire debris. The probable outcome of such an event is loss of the associated hydraulic system. For reference the consequences of such a hydraulic system loss on the major systems of the aircraft are given below, along with the Failure Condition Classification. For the identification of the control surfaces see Figure 4.4.1-1.

FIGURE L11 (Continued)
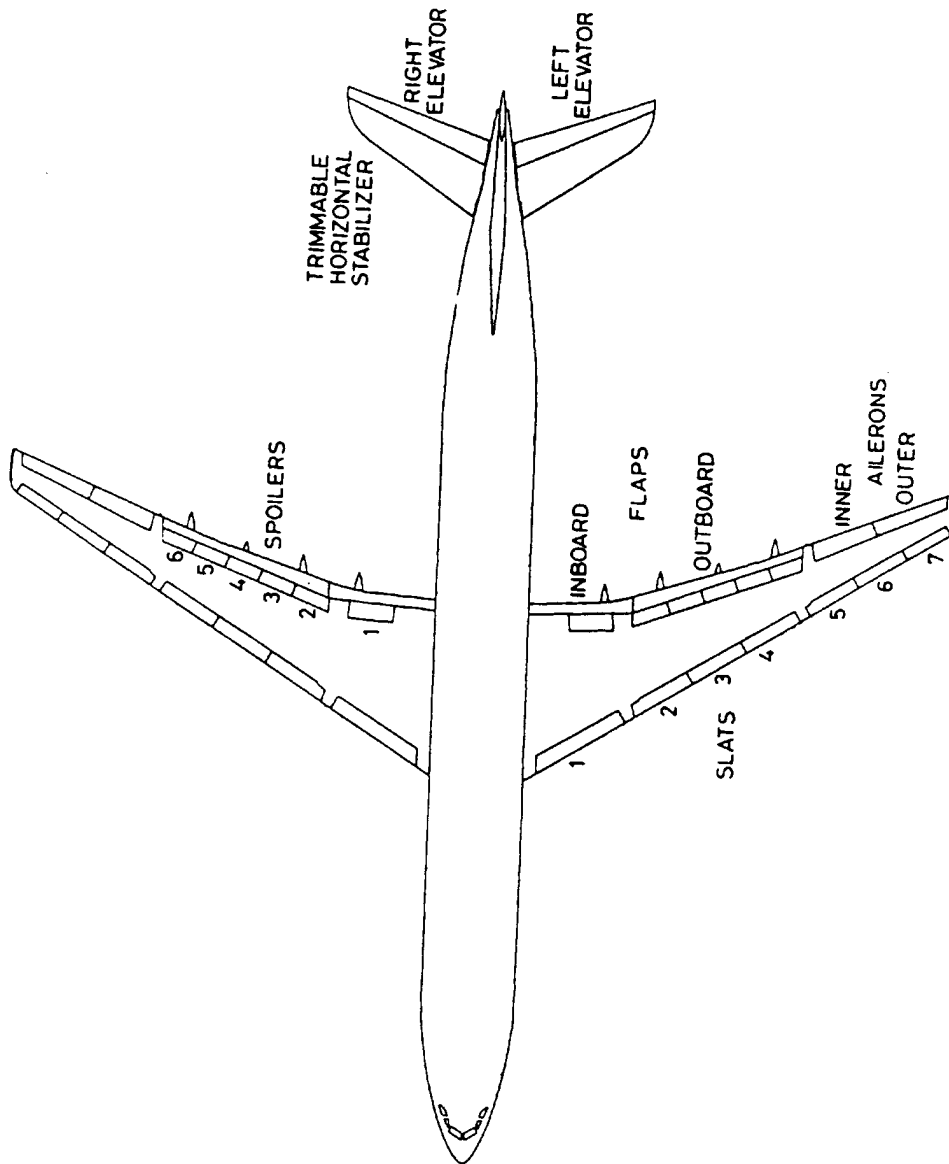
NOTE: SSA - CCA - PRA

FIGURE 4.4.1-1 - (CCA - PRA) S18 Aircraft Flight Control Surfaces

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.4.2   Hydraulic System Losses

    a. Loss of Green Hydraulics

        (1) ATA 27

            (a)   Flaps half speed operation
            (b)   Slats half speed operation
            (c)   Loss of spoiler 1 and 5 operation (both wings)

        (2) ATA 32

            (a)   Loss of normal brake system, automatic change-over to alternate (blue) brake system
            (b)   Loss of nose wheel steering
            (c)   Loss of landing gear retraction (if gear down)
            (d)   Gravity gear extension (if gear up)

        (3) ATA 78

            (a)   Loss of thrust reverser number 2

   Failure Condition Classification - MINOR

    a. Loss of Blue Hydraulics

        (1) ATA 27

            (a)   Slat half speed operation
            (b)   Loss of spoiler 2 and 3 operation (both wings)

        (2) ATA 32

            (a)   Loss of alternate brakes. Emergency braking by accumulator (blue) without antiskid remains if blue brake pipes are not severed.

        (3) ATA 78

            (a)   Loss of thrust reverser number 3

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.4.2 (Continued):

Failure Condition Classification - MINOR

a. Loss of Yellow Hydraulics

(1) ATA 27

(a) Flaps half speed operation
(b) Loss of spoiler 4 and 6 operation (both wings)

(2) ATA 78

(a) Loss of thrust reversers number 1 and 4

Failure Condition Classification - MINOR

a. Loss of Green and Blue Hydraulic

(1) ATA 27

(a) Loss of slat operation
(b) Flaps half speed operation
(c) Loss of spoiler 1, 2, 3 and 5 operation (both wings)
(d) Loss of inner aileron operation

(2) ATA 32

(a) Loss of normal and alternate brakes. Emergency braking by accumulator (blue) without antiskid remains if blue brake pipes are not severed, downstream of the accumulator.
(b) Loss of nose wheel steering
(c) Gravity gear extension (if gear up)

(3) ATA 78

(a) Loss of thrust reversers number 2 and 3

FIGURE L11 (Continued)

SAE ARP4761

4.4.2   (Continued):

Failure Condition Classification - MAJOR, (If all brakes lost - HAZARDOUS)

a. Loss of Green and Yellow Hydraulics

    (1) ATA 27

        (a)   Loss of flap operation
        (b)   Slats half speed operation
        (c)   Loss of spoiler 1, 4, 5 and 6 operation (both wings)
        (d)   Loss of right elevator operation
        (e)   Loss of outer aileron operation
        (f)   Loss of yaw damper operation

    (2) ATA 32

        (a)   Loss of normal brake system, automatic change-over to alternate (blue) brake system
        (b)   Loss of nose wheel steering
        (c)   Loss of landing gear retraction (if gear down)
        (d)   Gravity gear extension (if gear up)

    (3) ATA 78

        (a)   Loss of thrust reversers number 1, 2 and 4

Failure Condition Classification - MAJOR

a. Loss of Blue and Yellow Hydraulics

    (1) ATA 27

        (a)   Flaps half speed operation
        (b)   Slats half speed operation
        (c)   Loss of spoiler 2, 3, 4 and 6 operation (both wings)
        (d)   Loss of trimmable horizontal stabilizer operation

    (2) ATA 32

        (a)   Loss of alternate brakes. Emergency braking by accumulator (blue) without antiskid remains if blue brake pipes are not severed.

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.4.2   (Continued):

      (3) ATA 78

        (a)   Loss of thrust reversers number 1, 3 and 4

Failure Condition Classification - MAJOR

  a. Loss of Green, Blue and Yellow Hydraulics

     (1) ATA 27

       (a)   Complete loss of flight control operation

Failure Condition Classification - CATASTROPHIC

4.4.3   Electrical System Loss Consequence

4.4.3.1   General

This analysis considers that rigid and flexible electrical conduits are severed if struck by wheel or tire debris. The probable outcome of such an event is loss of the associated electrical control or monitoring signals.

To safeguard operation of all major systems of the aircraft at least two independent and segregated electrical systems and controlling computers are employed. All monitoring sensors are duplicated, although of necessity these may be mounted close together at the point to be monitored.

4.4.3.2   Single Electrical System Losses

Control and monitoring circuits are themselves subject to continuity monitoring by the associated controlling computer.

In the event of wheel or tire failure causing loss of multiple electrical systems the operation of vital aircraft systems will be by alternate emergency system in most cases, such as:

a. Hydro-mechanical control of alternate braking (without antiskid).
b. Gravity extension of nose and main landing gear.

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

TABLE 4.6-1 - (CCA - PRA) Tire Failure Particular Risk Analysis Summary

TIRE FAILURE STUDY TREAD SHED, TIRE BURST	MAIN LANDING GEAR - EXTENDED			
FAR/JAR 25 NO.	AFFECTED ITEMS	CONSEQUENCES	FAILURE CONDITION CLASSIFICATION	RISK	REPORT PARA.
729(f)	**MLG LEG FAIRING DOOR** LEG FAIRING DOOR PANEL	Attachments broken, fairing door (36kg) departs airframe and strikes inboard flap and passes below horizontal stabilizer (impact energy at flap less than bird strike)	MINOR		2.1
729(f)	**MLG HINGED DOOR** HINGED DOOR PANEL	Attachments broken, hinged door (15kg) departs airframe (as above)	MINOR		
729(f)	**MLG LEG AND DRESSINGS** ELEC.: 2M tachometer data HYD: Blue (or Green) to 2 brakes	Loss of brakes on 3 wheels of affected bogie	MAJOR		
1309	**LOWER WING SKIN** ELEC: 1M fuel pump 2M power supply	Loss of pumping to one engine. Engine runs down unless crossfeed manually selected	MINOR	1.8E-6	

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

TABLE 4.6-1 - (CCA - PRA) Tire Failure Particular Risk Analysis Summary (Continued)

TIRE FAILURE STUDY — **MAIN LANDING GEAR - EXTENDED**

TREAD SHED, TIRE BURST

FAR/JAR 25 NO.	AFFECTED ITEMS	CONSEQUENCES	FAILURE CONDITION CLASSIFICATION	RISK	REPORT PARA.
963(e) (FAR only)	**ACCESS PANELS 541/641 AB, BB, CB, DB** FUEL TANK ACCESS PANELS	Denting	NONE		
1309	**ACCESS PANELS 573/673DB** ELEC.: 1M to wing 2M and MLG 1S NORMAL 2S BRAKING HYD: Blue to flight control STRUCTURE: assess panel, assembly	Alternate braking without anti-skid	MAJOR	2.0E-7	2.1
		Loss of Blue hydraulics	MINOR		
		Release of panel (1.7Kg)	MINOR		
1309	**FIXED UNDERWING PANEL** underwing panel, assembly	Release of panel (5.1Kg)	MINOR	8.0E-8	

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

TABLE 4.6-1 - (CCA - PRA) Tire Failure Particular Risk Analysis Summary (Continued)

TIRE FAILURE STUDY TREAD SHED, TIRE BURST	MAIN LANDING GEAR - EXTENDED			
FAR/JAR 25 NO.	AFFECTED ITEMS	CONSEQUENCES	FAILURE CONDITION CLASSIFICATION	RISK	REPORT PARA.
729(f) 1309	**SHROUD BOX** HYD: Green to wing MECH.: Flap transmission STRUCTURE: Shroud box assembly	Loss of hydraulics Loss of flap operation Release of small debris pieces	MINOR MINOR MINOR		
729(f) 1309	**OVERWING PANEL** ELEC.: 1M to MLG HYD: Green to MLG STRUCTURE: Overwing panel assembly	Alternate braking without anti-skid Loss of Green hydraulics Puncture of panel release of small debris pieces	MINOR MINOR MINOR		

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

TABLE 4.6-1 - (CCA - PRA) Tire Failure Particular Risk Analysis Summary (Continued)

TIRE FAILURE STUDY TREAD SHED, TIRE BURST		MAIN LANDING GEAR - EXTENDED			
FAR/JAR 25 NO.	AFFECTED ITEMS	CONSEQUENCES	FAILURE CONDITION CLASSIFICATION	RISK	REPORT PARA.
729(f)	**INNER REAR SPAR** ELEC.: 1M to WING 2M and WING 1S ALTERNATE 2S BRAKING	Loss of inner aileron operation Loss of spoiler 1, 2, 3, 5 operation Loss of navigation lights Half speed flap operation	MAJOR MAJOR MINOR MINOR MINOR		2.1
729(f)	HYD: Blue to wing OR Green to MLG downlock	Loss of Blue hydraulics or Loss of Green hydraulics after gear up selection	MINOR		
1309	**INBOARD FLAP** Inboard flap panel	Local damage to bottom Skin, release of small debris pieces	MINOR	1.2E-5	
1309	**NO. 2 FLAP TRACK FAIRING** flap track fairing	Local damage and release of debris pieces	MINOR	5.0E-8	
1309	**NO. 1 SLAT** no. 1 Slat panel	Local damage and release of small debris pieces	MINOR		

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

TABLE 4.6-1 - (CCA - PRA) Tire Failure Particular Risk Analysis Summary (Continued)

TIRE FAILURE STUDY		MAIN LANDING GEAR - EXTENDED			
TREAD SHED, TIRE BURST					
FAR/JAR 25 NO.	AFFECTED ITEMS	CONSEQUENCES	FAILURE CONDITION CLASSIFICATION	RISK	REPORT PARA.
1309	**NO. 1 SPOILER**				
	no. 1 Spoiler panel	Release of debris pieces	MINOR	2.96E-6	
	no. 1 Spoiler actuator	Loss of Green hydraulics	MINOR	1.20E-7	
1309	**FUSELAGE**				
	SECTION 13 AND 14 upper lateral shell below window line	Skin dents and paint Scratches	MINOR	3.4E-8	2.1
	SECTION 15/21 belly fairing	Punctured, release of small debris pieces	MINOR	7.0E-8	
	SECTION 16 upper lateral shell below window line	Skin dents and paint Scratches	MINOR	1.4E-8	

FIGURE L11 (Continued)

NOTE: SSA - CCA - PRA

4.4.3.2   (Continued):

In some cases the electrical control systems can have a limited control function with tolerance of loss of all channels of monitoring data for certain parameters, such as:

a. Landing gear hydraulic extension after loss of both channels of "landing gear doors closed" data.

4.5   Design Precautions taken

The hydraulic systems supplying the brakes, and the necessary sensor and control wiring are installed with one circuit on the front and the other circuit on the rear of the main landing gear leg.

(Editor's Note: Other design precautions in accordance with the design and installation guidelines may apply, but they are not shown here for brevity.)

4.6   Review of Consequences

The combined debris impact zones of all eight MLG tires give extensive coverage of the bottom wing skin in the wing root region. Included within this region is the uncovered MLG wing bay. Consequently a considerable number of events with a Minor failure condition classification can occur, typically loss of a single hydraulic circuit, electrical channel or minor structural damage. Prominent examples of these are given in Table 4.6-1.

A number of events cause loss of two circuits in combination resulting in loss of; inner aileron and spoiler 1, 2, 3 and 5 operation; or loss of brakes on 3 wheels of the affected bogie; or alternate braking having a "Major" failure condition classification.

No event caused by a single debris piece having a failure condition classification worse than "Major" has been identified. Therefore JAR 25.729(f) is satisfied and the failure condition classification for a single debris piece is "Major".

In 10% of cases a second debris piece is specified by the Wheel and Tire model. In the event of two debris pieces striking the Blue and Green braking circuits independently then all braking is lost, which is assigned a "Hazardous" failure condition classification. Therefore the failure condition classification for two debris pieces is "Hazardous" and the associated probability is 2.2E-9 per flight.

FIGURE L11 (Continued)

SAE ARP4761

NOTE: SSA - CCA - PRA

5.0   CONCLUSIONS

The general assumption adopted for this analysis was that electrical and hydraulic systems are ruptured by debris impact. Thus all the effects described represent the worst case.

a. No event resulting from tire failures has been identified as a CATASTROPHIC Failure Condition.

b. One event resulting from tire failures has been identified as a HAZARDOUS Failure Condition. This event is total loss of braking caused by tire debris pieces from two MLG wheels impacting the Blue and Green brake hydraulic supply pipes within the MLG wing bay region. The probability of occurrence of this event has been assessed as EXTREMELY REMOTE (2.2E-9 per flight).

c. No other event has been identified by the analysis which has a Failure Condition Classification worse than MAJOR. An inverse relationship between the severity of systems or structural damage and the probability of occurrence has been demonstrated in accordance with the FAR/JAR 25.1309 advisory material.

d. Essential equipment located on the landing gear or in wheel wells has been shown to be protected from single tire failures with a Failure Condition Classification worse than MAJOR. FAR/JAR 25.729(f) is therefore satisfied.

e. Fuel tank access covers located in areas considered to be at risk from tire fragments or bursting have been shown to minimize penetration and deformation. FAR 25.963(e) is therefore satisfied.

The aircraft has been shown by analysis to be capable of continued safe flight and landing after any single failure or combination of failures caused by wheel or tire debris events that are not shown to be extremely improbable. FAR/JAR 25.671(c) is therefore satisfied.

FIGURE L11 (Continued)

SAE ARP4761

NOTE: SSA - CCA - CMA (Aircraft)

**Common Mode Analysis (CMA) for Aircraft
for the Wheel Braking System**

(Editor's Note: for details on the CMA process, refer to Appendix K.)

1.0   INTRODUCTION

This analysis covers the common mode analysis (CMA) at the aircraft level for the wheel braking function. The analysis assures that no single and common events or failures occurring at the aircraft level can produce a catastrophic effect. This example covers only the independence between the normal and alternate systems, considering the emergency brake as part of the alternate.

(Editor's Note: A complete analysis at the aircraft level would also consider other (in)dependencies (e.g., between wheel braking and thrust reverser system), but they are omitted for brevity.)

2.0   REFERENCES

The following references were used in performing the CMA at aircraft/system level.

1) ARP4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"
2) PSSA fault tree "Loss of All Wheel Braking" for the S18 Aircraft.
3) Zonal Analysis No. YYY for the S18 Aircraft.
4) Particular Risks Analyses No. ZZZ for the S18 Aircraft: Fire, Tire burst, Lightning
5) Common Mode Analysis No. ZZZ of the Electrical Power Distribution and Generation System for the S18 Aircraft
6) Common Mode Analysis No. WWW of the Hydraulic Power Distribution and Generation System for the S18 Aircraft
7) System Safety Assessment for the wheel braking system

3.0   DESCRIPTION SUMMARY

(Editor's Note: For the purpose of this guideline, see the PSSA example for the Brake System Description. In the case of a real CMA an updated description summary would appear here.)

FIGURE L12

SAE ARP4761

NOTE: SSA - CCA - CMA (Aircraft)

4.0   ANALYSIS

4.1   Check-lists

The following checklist delineates common sources and failure modes to be considered in the common mode analysis.

COMMON MODE TYPES, SOURCES AND FAILURES CHECKLIST

DESIGN ARCHITECTURE

    External source: Electrical Power Supply
    External source: Hydraulic Power Supply
    Operating Characteristics
    Location
    Pipes and Wires Routing

TECHNOLOGY, EQUIPMENT

    Technology, Component/Equipment Type

SPECIFICATION

    Technical Specification and its Origin

INSTALLATION

    Procedures and Fitter

MANUFACTURING

    Manufacturer and Manufacturing Process

OPERATION

    Crew actions and Procedures

CORRECTIVE MAINTENANCE

    Procedures and Staff

ENVIRONMENTAL FACTORS

    Lightning,
    Pollution due to water, slush, etc.

FIGURE L12 (Continued)

SAE ARP4761

NOTE: SSA - CCA - CMA (Aircraft)

4.2   Independence Requirements

(Editor's Note: The example chosen is based on the AND Gate associated with the "Loss of All Wheel Braking" element considered in the PSSA fault tree (refer to reference 2).)

The inputs to this gate are the following failures: Loss of the Normal Brake System, the Alternate Brake System and the Emergency (Reserve) Brake System.

The independence requirement associated with this gate is the independence between the Normal and the Alternate systems. Emergency brake system has to be considered as a part of the Alternate system.

(Editor's Note: Other independence requirements may be derived from the PSSA, but they are not analyzed nor shown here for brevity.)

4.3   Common Mode Analysis

To show compliance with the requirement listed above, the brake system design and implementation have been reviewed for vulnerability to common mode errors. Component failures which could lead to a loss all wheel braking have been analyzed in Table 4.3-1.

(Editor's Note: Table 4.3-1 addresses the applicable portions of Table K.3.2.1.1-1 and summarizes the results of these investigations. Possible common mode sources, common mode errors and justification/protections have been considered.)

FIGURE L12 (Continued)

NOTE: SSA - CCA - CMA (Aircraft)

TABLE 4.3-1 - (CCA - CMA (Aircraft)) Wheel Brake Function Common Mode Analysis

REQUIREMENT: NORMAL AND ALTERNATE BRAKING SHALL BE INDEPENDENT

COMMON MODE SOURCE	COMMON MODE ERROR	JUSTIFICATION
DESIGN ARCHITECTURE External source: Electrical Power Supply	Common point in the electrical supply leading to a complete loss of power for control and monitoring of the Normal and Alternate brake systems.	Normal system equipment (e.g., BSCU, servo valve) is electrically supplied by Main Bus 1 and 2. Alternate system equipment (e.g., metering valve, servo valves) is electrically supplied by the Emergency bus. A Common Mode Analysis of the electrical power distribution and generation system has been performed to verify the functional independence between both bus bars.
External source: Hydraulic Power Supply	Common point in the hydraulic supply leading to a complete loss of hydraulic power to Normal and Alternate Brake Systems.	Normal system is supplied by the GREEN Hydraulic circuit. Alternate System is supplied by the BLUE Hydraulic System. A Common Mode Analysis of the hydraulic power distribution and generation system has been performed to verify the functional independence between GREEN and BLUE hydraulic system. The tire burst analysis shows that two tire bursts are necessary to lead to this failure and that the probability is acceptable (ref. 4).
Operating Characteristics	Common operating characteristics violating independence.	Normal brake system is the nominal one. It is normally in standby mode operation during flight phase and demanded at each end flight. Alternate brake system is a backup system. I' always in standby mode and demanded, by th operation of an automatic selector, when Normal brake system is off or fails off. Alternate system is tested periodically. Both systems have different operating characteristics (one system is demanded when the other fails)

FIGURE L12 (Continued)

NOTE: SSA - CCA - CMA (Aircraft)

TABLE 4.3-1 - (CCA - CMA (Aircraft)) Wheel Brake Function Common Mode Analysis (Continued)

REQUIREMENT: NORMAL AND ALTERNATE BRAKING SHALL BE INDEPENDENT		
COMMON MODE SOURCE	COMMON MODE ERROR	JUSTIFICATION
Location	Local event leading to total loss of wheel braking.	Main equipment of both systems is located at the landing gear zone. Physical segregation of electrical wires and hydraulic paths.
Pipes and Wires Routing	Local event affecting electrical routes or hydraulic circuits.	Independent electrical routes are used. Each route has its dedicated connectors. Physical barrier ensures the independence of both hydraulic circuits all along the main landing gear zone. Zonal analysis verifies the independence between electrical routes and hydraulic circuits.
TECHNOLOGY, EQUIPMENT Technology, Component/Equipment Type	Development Error	Conventional technology is used on components. Different type of components and assemblies are installed in both systems except for the servo valves. Previous experience on servo valves and qualification tests after manufacturing and installation phases assures correct operation.
SPECIFICATION Technical Specification and its Origin	Defective specification or origin error	Different technical specifications for the equipment installed. Independent technical review of the specifications prevents origin errors.
INSTALLATION Procedures and Fitter	Installation error	Installation quality: double inspection. After installation phase, visual inspection and operational tests of the Normal, Alternate and Emergency systems are performed.

FIGURE L12 (Continued)

SAE ARP4761

NOTE: SSA - CCA - CMA (Aircraft)

TABLE 4.3-1 - (CCA - CMA (Aircraft)) Wheel Brake Function Common Mode Analysis (Continued)

REQUIREMENT: NORMAL AND ALTERNATE BRAKING SHALL BE INDEPENDENT		
COMMON MODE SOURCE	COMMON MODE ERROR	JUSTIFICATION
MANUFACTURING Manufacturer and Manufacturing Process	Faulty manufacture affecting similar equipment installed in both systems	Same manufacturer for servo valves (normal/alternate) and components. Manufacturer's quality process is certified.
OPERATION Crew actions and Procedures	Faulty operation procedure or Crew incorrect action leading to the disconnection of both brake systems.	Normally, at the end of a flight, crew uses the autobrake system. Crew has previously selected the adequate level of braking. The Alternate system is used when the NORMAL system is off. Crew action consists on depressing the brake pedals. There is an independence between both operation procedures as they are performed in different conditions and using different means.
CORRECTIVE MAINTENANCE Procedures and Staff	Faulty maintenance procedure or maintenance error	Maintenance errors are detected by the operational test and visual inspections performed after each maintenance action. These tests assure correct equipment operation. When corrective maintenance on normal brake system is performed, the alternate one is switched off. When corrective maintenance on alternate brake system is performed, the Normal one is switched off. In both cases, final tests performed in both systems detect all possible maintenance errors.

FIGURE L12 (Continued)

- 330 -

NOTE: SSA - CCA - CMA (Aircraft)

TABLE 4.3-1 - (CCA - CMA (Aircraft)) Wheel Brake Function Common Mode Analysis (Continued)

REQUIREMENT: NORMAL AND ALTERNATE BRAKING SHALL BE INDEPENDENT		
COMMON MODE SOURCE	COMMON MODE ERROR	JUSTIFICATION
ENVIRONMENTAL FACTORS Lightning, Pollution due to water, slush, etc.	Environmental factor effecting simultaneously the Normal and the Alternate brake systems operation.	Normal and Alternate brake systems are protected against lightning effects. Equipment is qualified to sustain runway pollution. Extensive environmental testing, only one brake system operating, the other is in stand-by, normally different operating time.

5.0   CONCLUSION

The analysis shows that:

a. no even resulting from a common mode type error has been identified which has a catastrophic effect.
b. those common mode type errors which could lead to a hazardous effect are restrained by special tests, manufacturing processes, quality assurance means or are acceptable because of their probability.

FIGURE L12 (Continued)