Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

AEROSPACE RECOMMENDED PRACTICE

ARP1834™ REV. B

Issued 1986-08
Revised 1997-06
Reaffirmed 1992-09
Stabilized 2018-02

Superseding ARP1834A

Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

RATIONALE

ARP4761 provides updated methods and processes for use on civil aircraft safety assessment. When analyzing these types of systems, ARP4761 should be used in lieu of this ARP.

STABILIZED NOTICE

This document has been declared "Stabilized" by the SAE S-18 Aircraft and Sys Dev and Safety Assessment Committee and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2018 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit
http://standards.sae.org/ARP1834B

Documents Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

INTRODUCTION

Background:

A fault and failure analysis (F/FA) usually consists of one or more of the analysis processes depicted by Figure 1, "Family of Fault/ Failure Analysis Processes." Typically, these analysis techniques are for the purpose of:

a. Analyzing, assessing and documenting the effects of potential failures on a particular equipment item or system design;

b. Identifying those failures which affect operational success or safety, and determining their probability of occurrence;

c. Enabling quantification of fault/failure detection and isolation capability as it relates to equipment safety and maintainability.

Aerospace Recommended Practice ARP926A, "Fault/Failure Analysis Procedure", addresses the application of F/FA methods to parts, components and systems other than those of an essentially digital nature. The development of this separate ARP to address digital F/FA was initiated to recognize:

a. The expanding use of digital hardware in military, commercial, and consumer products;

b. The need to apply F/FA procedures to digital devices, components and systems;

c. The distinctive characteristics of digital equipment, having unique potential failure modes which, if not recognized and designed for, can result in either excessive downtime or erroneous output with severe ramifications.

Documents
Document Sharing Hub
Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

TABLE OF CONTENTS

INTRODUCTION 1

1. SCOPE 4

1.1 Use of ARP1834 Guidelines for Safety Certification 4

2. REFERENCES 5

2.1 Applicable Documents 5
2.1.1 SAE Publications 5
2.1.2 U.S. Government Publications 5
2.1.3 RTCA Publications 5
2.1.4 Other References 6
2.2 Glossary 6

3. POSSIBLE APPROACHES 8

3.1 Influences Versus System Types 10
3.1.1 Common to all System F/FAs 10
3.1.2 Non-Processor-Based System F/FAs 12
3.1.3 Processor-Based System F/FAs 12
3.2 F/FA Scope and Approach 13
3.2.1 Failure Consequences 13
3.2.2 Architecture 14
3.2.3 Fault Management 14
3.2.4 Maintainability Considerations 15
3.3 F/FA Approach Considerations 15
3.3.1 Program Phase 15
3.3.2 Level of Detail versus Cost 15
3.3.3 Skill Level, Expertise Required 16
3.3.4 Facility - Special Needs 16
3.3.5 Fault Management 17
3.3.6 Software Design 18
3.3.7 Safety Hazard Identification 19
3.3.8 Design Changes 19
3.4 F/FA Decision Tree 20

4. FAILURE MODES AND EFFECTS 20

4.1 Identification of General Needs 20
4.2 Failure Mechanisms 22
4.3 Modes and Effects 22
4.3.1 Device Failure Modes 22
4.3.2 Soft Failures 23
4.3.3 Latent Failures 23
4.3.4 Failure Mode Data Sources 24

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

TABLE OF CONTENTS (Continued)

4.4 Failure Rate Allocation 25
4.5 Custom LSI 25
4.6 Software Considerations 25

5. FAULT MONITORING METHODOLOGY 25

5.1 Reasons for Fault Monitoring 26
5.2 System Architecture vs Fault Monitoring 26
5.3 Types of Fault Monitoring 26
5.3.1 Processor Failure Detection 27
5.3.2 Data Transmission Error Detection 27
5.3.3 Data Validity 28
5.4 Fault Monitoring Effectiveness 29
5.5 Method of Fault Monitoring Analysis 29

6. ANALYSIS METHODS 29

6.1 Basic Methods and Elements 29
6.1.1 General 29
6.1.2 Sequence 30
6.1.3 F/FA Process Steps 31
6.2 Special Methods 38
6.2.1 Fault Insertion Using Hardware 38
6.2.2 Fault Insertion Using Emulation 39
6.2.3 Fault Insertion into a Computer Simulation of the Hardware Functions 39

APPENDIX A EXAMPLE - F/FA BASIC BOTTOM-UP APPROACH 41
APPENDIX B EXAMPLE - F/FA BASIC TOP-DOWN APPROACH 58
APPENDIX C 67

FIGURE 1 Family of Fault/Failure Analysis Processes 9
FIGURE 2 Typical Analysis Flow - Scope, Direction, and Responsibility 11
FIGURE 3 An Example of a F/FA Decision Tree 21

TABLE 1 F/FA Objective Versus Development Phase 8
TABLE 2 One Example of Categorizing Scope and Approach of Analysis 14
TABLE 3 Digital Systems Considerations of F/FA Approaches 16
TABLE 4 Typical Device Failure Modes 23

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

1. SCOPE:

ARP1834 provides general guidance for the selection, approach to, and performance of various kinds of F/FA of digital systems and equipment. Its prime objective is to present several industry-acceptable, cost-effective methods for identifying, analyzing, and documenting digital-equipment failure modes and their effects. The analysis techniques and considerations presented here are directed to digital-equipment hardware faults and failures exclusively.

ARP1834 is not intended as an exhaustive treatment of the enormously complex process involved in the analytical failure evaluation of complete digital systems, nor as a universally applicable, definitive listing of the necessary and sufficient steps and actions for such evaluation.

ARP4761 provides updated methods and processes for use on civil aircraft safety assessment. When analyzing these types of systems, ARP4761 should be used in lieu of this ARP.

ARP1834 addresses the following areas of consideration in the preparation and performance of F/FA's for digital equipment:

a. Possible Analysis Approaches: Top-Down and/or Bottom-Up (Section 3)
b. Fault/Failure Modes, as they affect equipment operation and performance (Section 4)
c. Fault Monitoring Methodology: Reasons for, types of, and effectiveness (Section 5)
d. Analysis Methods: Preparation for, types of, effectiveness and coverage (Section 6)

1.1 Use of ARP1834 Guidelines for Safety Certification:

If this document is used as guidance for analyses involved in achieving digital-equipment safety certification by a regulatory agency, early coordination with that agency should be initiated to establish the scope and level of analysis effort that will be required to show compliance. Specific applications of F/FA processes discussed herein (and quite possibly others omitted here) will need to be negotiated on a case-by-case basis between the applicant and the agency, and between the prime contractor and his subcontractor or equipment supplier.

For digital systems performing functions that are critical and/or essential (see 3.2.1), it may not be possible to demonstrate compliance with safety-certification requirements without the use of design techniques aimed at producing a fault-tolerant system. A goal for these design techniques is the possible reduction or elimination of the need for part-level FMEA. This consideration is of pivotal importance, because thorough, accurate and dependable FMEA of contemporary microcircuits is not a feasible undertaking (see 6.1.3.6.1). The depth of the F/FA required to show compliance will be strongly influenced by such techniques. Typical design techniques which may be used in various combinations include:

a. System Architecture

(1) Similar Redundancy
(2) Dissimilar Redundancy
(3) Signal Consolidation or "Voting"
(4) Hardware Functional Partitioning

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

1.1 (Continued):

b. Fault Detection and Isolation

(1) Comparison Monitoring between redundant elements
(2) In-line test and monitoring
(3) In-line reasonableness checks

c. Fault Response

(1) System reconfiguration
(2) Operational mode changing
(3) System shutdown

Although such design considerations are outside the scope of this document, they must be taken into account by system designers and analysts in meeting overall system-safety objectives and in establishing the level of effort required for the F/FA.

2. REFERENCES:

2.1 Applicable Documents:

The following publications contain information relative to applications of tail bumpers. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this specification and references cited herein, the text of this specification takes precedence. Nothing in this specification, 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.

ARP926A
ARP4761

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

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

RTCA Document No. DO-178

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

2.1.4 Other References:

AC 20-115
AC 25.1309-1
RAC
GIDEP (Government Industry Data Exchange Program)
McGough, J., Swern, F., "Measurement of Fault Latency in a Digital Avionics Miniprocessor," Flight Systems Division Bendix Corporation, NASA Contract NASI-15946, April, 1981.
Seshu, S. and Freeman, D. N., "The Diagnosis of Asynchronous Sequential Switching Systems", IRE Transactions on Electronic Computers, Vol. EC-11 No. 4 August, 1962, pp. 459-465.
Hardie, F. H., and Suhocki, R. J., "Design and Use of Fault Simulation for Saturn Computer Design", IEEE Transactions on Electronic Computers, Vol. EC-16, No. 4, August 1967, pp. 412-429.
Bertolino, L., Grefsrud, L. E., "Failure Analysis of Digital Systems Using Simulation", Proceedings; Reliability and Maintainability Symposium, 1977.

2.2 Glossary:

This glossary contains definitions of terms used in the text of this document.

ALGORITHM: An explicit set of rules, generally mathematical in nature, for solving a particular problem. When this set of rules is applied to identified inputs, the desired outputs will be obtained after a finite number of steps have been completed.

AVAILABILITY: Probability that an item is in an operable state when required.

(CPU) CENTRAL PROCESSING UNIT: The part of a computer that controls the interpretation and execution of instructions.

CERTIFICATION: The process of obtaining regulatory agency approval for a function, equipment, system or aircraft, by establishing that it complies with all applicable government regulations.

CHANGE CONTROL: The process of evaluating, approving, and documenting a system configuration and changes to the system.

COMPARISON MONITORING: The technique of comparing a set of computed variables with a corresponding set from an independent source.

Documents
Document Sharing Hub
Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

2.2 (Continued):

EMULATOR: Software run on a host computer that accepts the same input data, executes the same programs, and yields the same outputs as the target computer. The emulation software may execute on a host computer or on a computer similar to the computer that will actually be used in the system. Emulators replace the computer in the system to enable the computer/system interface to be tested, verified, and validated in an orderly fashion.

FAILURE: The inability to perform within specified limits.

FAULT: An undesired anomaly in the functional operation of an equipment or system.

FAULT ISOLATION: As used in reference to diagnostics or built-in-test equipment, the ability to identify the unit in which a fault has occurred.

FAULT MANAGEMENT: Those aspects of the system design which cover fault monitoring (detection), fault response, fault storage and fault annunciation, for both operational and maintenance purposes.

FIRMWARE: A computer program that is stored in a fixed or "firm" way, usually in a read-only memory.

FUNCTIONAL ISOLATION: The property of a system which provides effective separation of functions to minimize adverse interaction.

HOST COMPUTER: Any computer used to develop software for another (target) computer.

LINE REPLACEABLE UNIT (LRU): An assembly which forms part of a system, designed to be removed and replaced in the event of failure to improve maintainability of a vehicle.

PARTITIONING: The process of determining how the system requirements will be implemented either in hardware and its components or in software and its components. In software, partitioning is said to exist if co-resident tasks execute without any interdependency between them.

PROCESSOR BASED SYSTEM: A system which uses a processor to control the timing and execution of all functions in a pre-determined relationship.

REDUNDANCY: That feature of design architecture which provides more than one means to perform certain functions.

SIMULATION: The representation of physical systems and phenomena by computerized models, e.g., an imitative type of data processing in which specialized computer programs are used to mimic the behavior of a physical device or system.

STATE CHANGES: Conditions involving one or more bits changing from 0 to 1, or from 1 to 0.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

2.2 (Continued):

TARGET COMPUTER: The digital computer embedded in the operational equipment that executes the operational software.

VALIDATION: The process of demonstrating, through testing in the real environment, or an environment as real as possible, that the system satisfies the user's requirements.

VERIFICATION: The process of demonstrating the logical correctness of the software and showing that it performs according to its specifications.

VOLATILE MEMORY: A memory device which requires continuous power to retain data.

3. POSSIBLE APPROACHES:

The prime criterion for performing any of the F/FA processes depicted by Figure 1, should be to provide credible results in the most cost effective manner. Of the various factors and influences which affect success or failure per this criterion, the phase of development at which the F/FA is expected to be performed and the analysis objectives are probably the most significant. Table 1 reflects how the iterative nature of F/FA, as the design progresses, can help to accomplish these F/FA objectives in a cost effective manner.

TABLE 1 - F/FA Objective Versus Development Phase

Development Phase	Objective
Preliminary Design	To find design weaknesses, single point failures and potential hazards
Design/Development	To assess safety, reliability, maintainability and availability
Design Acceptance	To substantiate that equipment meets requirements

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

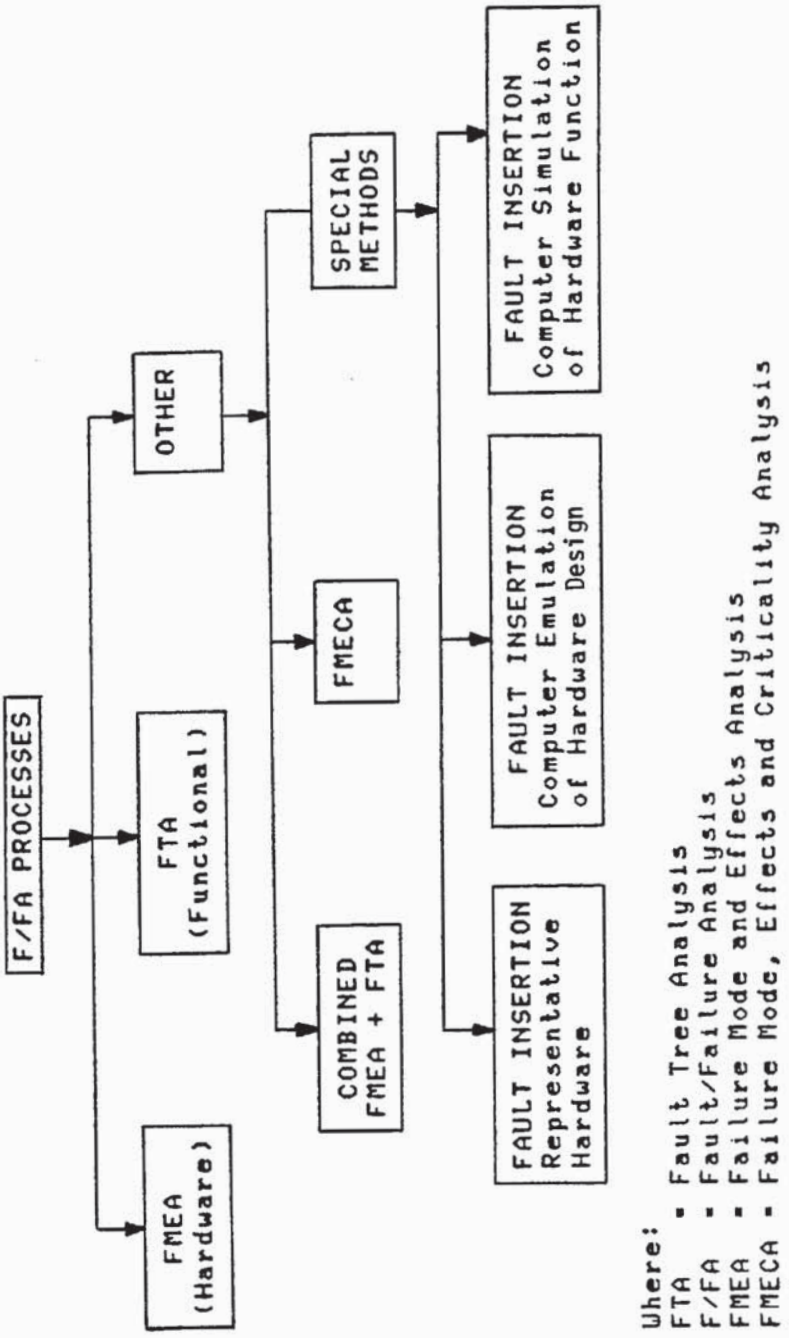


FIGURE 1 - Family of Fault/Failure Analysis Processes

Documents
Document Sharing Hub
Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3. (Continued):

Factors which influence the particular F/FA approach to be utilized in conjunction with digital equipment, can, for discussion purposes, be categorized under the following headings:

a. Influence Factors

(1) Common to all systems F/FAs
(2) Non-processor-based system F/FAs
(3) Processor-based F/FAs

b. Factors affecting scope and approach of F/FAs

c. Approach considerations and comparisons for digital system F/FAs

d. Decision tree for civil aircraft F/FAs

3.1 Influences Versus System Types:

3.1.1 Common to all System F/FAs: There are two basic approaches to performing any F/FA: the top-down approach and the bottom-up approach. (ARP926A calls these two the "functional approach" and the "hardware approach," respectively.) As shown in Figure 1, top-down or bottom-up analysis or both may be utilized in conjunction with any F/FA. Normally the choice of approach is based on considerations of clarity, emphasis, program phase, equipment-development life cycle, etc.

The top-down analysis is initiated at the system level, or top-assembly level, and proceeds downward through the hardware design (see Figure 2). Failure effects are identified in terms of malfunction of the system or equipment-item or of the loss of one of its functions, rather than in terms of lowest-level-failure impact. Having identified the undesirable effects, this analysis determines if failures can exist at the lower equipment levels that can cause the undesirable effects. Fault-Tree Analysis is an example of top-down analysis.

The bottom-up analysis is initiated at the electronic-part or component level or at a higher, intermediate equipment level and proceeds upward to the top equipment or system level as shown in Figure 2. At the initiated level, every credible hardware failure mode is postulated, and the failure effects of each such failure mode on the next-higher equipment level are identified. (In some such analyses, the failure rate and exposure time of each failure mode are also assigned.) Failure Modes and Effects Analysis (FMEA) is an example of a bottom-up analysis.

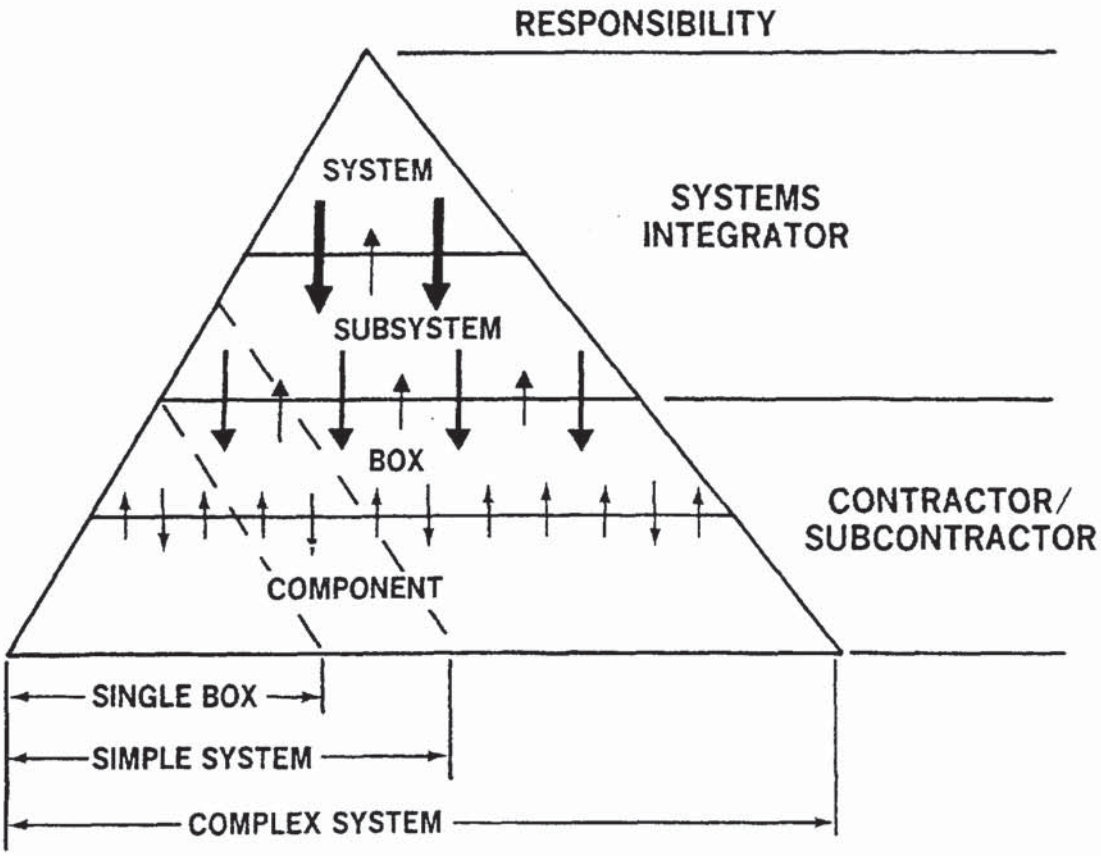
For any equipment employing microcircuits, completion of a bottom-up analysis initiated at the electronic-part level is not ordinarily achievable, because (as discussed in 6.1.3.6.1) a thorough, accurate, and dependable failure-mode analysis of most microcircuits is not feasible.

ARP926A contains examples illustrating the mechanics of certain basic analyses. Additional examples illustrating the use of these basic approaches on digital systems are provided in this document.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026



NOTES:

1. THE SIZE AND QUANTITY OF THE ARROWS REFLECT THE DEPTH AND SCOPE OF THE ANALYSIS
2. THE DIRECTION OF THE ARROWS INDICATES THE DIRECTION OF THE ANALYSIS (TOP DOWN, BOTTOM UP)
3. THE AREAS OF RESPONSIBILITY WILL GENERALLY OVERLAP MORE THAN INDICATED

FIGURE 2 - Typical Analysis Flow - Scope, Direction, and Responsibility

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.1.2 Non-Processor-Based System F/FAs: The basic approaches described in ARP926A may be used for simple, non-processor-based digital systems. The more complex non-processor-based digital systems will probably require the application of techniques described in this document.

3.1.3 Processor-Based System F/FAs: The basic F/FA approaches described for non-processor-based digital circuits may be extended to processor-based systems. Typically, analyses are performed using the functional approach. Where it is possible, the processor circuit is divided into various basic functional elements. The function failure effects are in either case, however, generalized as loss of function or incorrect function. In the latter situation, extreme care must be taken whenever an incorrect function is assigned to a processor-based system. The processor may generate new and possibly undesirable functions if left uncorrected.

The effect of these processor failure modes on the system is determined by evaluating the fault monitoring and response provisions in conjunction with software design and hardware implementation.

For processor-based systems, the functional approach may be effective if the effect on the system due to a failure is dependent on the fault monitoring, the effectiveness of which can be evaluated. With procuring or regulatory agency concurrence, it may not be necessary to perform analysis beyond the point of determining that critical and essential function failure modes are detectable by fault monitoring, plus verifying that the desired response will follow. It may be only necessary to initiate the hardware F/FA approach at the lowest level subject to analysis for those cases where critical and essential function effects are determined or where there is a need to quantify the probability of any undesired event.

Special methods may be needed to supplement the basic analytical hardware and functional F/FA approaches where the effects of failures are uncertain. These techniques may use actual hardware, an emulation of the hardware, or a simulation of the hardware functions. Failures may be simulated by one of the following methods:

a. In the target computer, replace functioning hardware with failed equivalent hardware which may contain individual failed gates, or

b. Inject faults at individual device pins in the target computer, either manually or automatically, or

c. Inject faults into a digital computer emulation of the target computer, or

d. Inject faults into a digital computer simulation of the function.

Section 6.2 contains a description of these special methods.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.2 F/FA Scope and Approach:

Factors that directly affect the required level and scope of analysis include:

a. Failure consequences

b. System Architecture (redundancy, function isolation),

c. Fault Management (monitoring techniques, effectiveness, comprehensiveness), and

d. Maintainability considerations.

Table 2 deals with different aspects of the scope of, and approach to, the analysis.

3.2.1 Failure Consequences: A fundamental principle applicable to all equipment is that the scope of the selected analysis approach should depend upon the severity of the worst possible failure consequences.

For commercial airborne systems and equipment, a categorization of function criticality was introduced by RTCA Document No. DO-178 for software, implied by Part 25.1309(b), of the Federal Aviation Regulations, recognized by Advisory Circulars AC 20-115 and AC 25.1309-1. The criticality categories with associated quantitative levels are shown in Table 2 and defined by the FAA in AC 25.1309-1 as:

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

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

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

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

TABLE 2 - One Example of Categorizing Scope and Approach of Analysis

Criticality Level	Analysis - Scope and Approach (may be required)	Associated Failure Condition Probability of Occurrence (Reference FAA AC 25.1309-1)
Critical	Prelim. Hazard Analysis Fault Tree Analysis FMEA Probability Analysis (supporting FTA)	Extremely Improbable (1×10^{-9} or less)
Essential	FTA FMEA	Improbable (1×10^{-5} or less)
Non-Essential	Analysis to determine that system performs only non-essential functions; determine if failure could contribute to a failure condition involving an essential or critical function.	May be probable (1×10^{-5} or greater)

3.2.2 Architecture: If the architecture (the arrangement and interrelationship of components) of the system is such that multiple outputs are (for the most part) isolated from each other by utilizing separated, independent circuits, the parts level F/FA task could be fairly simple and limited in scope. However, if the circuits are highly interactive, then the analysis task could be difficult and lengthy. This is particularly true when it is necessary, because of failure mode criticality, to tabulate and analyze every credible failure mode in the Line Replaceable Unit (LRU).

When the architecture of the system utilizes a higher degree of independent, non-interactive elements, the failure modes become easier to analyze.

3.2.3 Fault Management: Fault management includes: detection, response, storage and display.

There are a number of possible hardware and/or software means for implementing digital fault monitoring. In any given application, it is a design responsibility to select fault monitoring techniques which comply with the equipment specification safety requirements.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.2.3 (Continued):

If the system architecture is so configured as to rely heavily on in-line monitoring (as opposed to comparison of redundant signals) to reduce risk of adverse effects associated with failures, then some method of fail-safe monitoring may need to be employed. Any such special methodology will expand the scope of analysis required. If the fault monitoring is designed, however, to detect specific failures, a proportionate reduction in F/FA scope (that is, numbers of combinations of failures which need to be analyzed) can be achieved, provided that the fault monitoring is successfully shown to perform its intended function, and does not cause unnecessary loss of function. The effects of failures of fault monitoring must also be analyzed.

3.2.4 Maintainability Considerations: The scope of F/FA may be dictated by contractual requirements for minimum proven levels of fault detection coverage. These requirements are intended to reduce life cycle costs by correct identification of faulty assemblies at various levels of repair.

3.3 F/FA Approach Considerations:

Table 3 provides factors to be considered when selecting a F/FA approach. The following discussions are keyed to those considerations.

3.3.1 Program Phase: This refers to the design phase in which an approach may be initiated. The bottom-up approach cannot be started until the hardware/circuits are defined. The top-down or functional approach can be initiated earlier in the program; actually, anytime after a concept has been formed, including the basic design development through tradeoff analysis.

For processor-based digital hardware, software requirements become an additional consideration to be defined before the F/FA is started. The functional F/FA approach can be used in conjunction with a conceptual hardware design to help define the software safety checking requirements, in conjunction with system architecture and hardware fault monitoring.

3.3.2 Level of Detail versus Cost: For both the hardware and functional F/FA approaches, costs are related to the level of detail or depth of analysis. Processor based systems are time-based and, as such, exhibit operating state changes according to their internal clocking and state processor algorithms. Serious processing errors can occur as a result of one failure in a particular state lasting an extremely short interval of time in one of the thousands of active digital elements. Tasks being performed are so complex that some errors may be undetected for long periods of time. Therefore, it may not be possible to predict processor failure effects at its output pins or to define how these events may be manifested at the output ports.

The better the fault management in the design, the less detail required in the F/FA. It may be more cost-effective to use the functional F/FA approach initially and expand the analysis on failure modes determined to be critical. The expansion of the analysis would then use the hardware F/FA approach.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

TABLE 3 - Digital Systems Considerations of F/FA Approaches

Consideration	Bottom-Up Approach	Top-Down Approach
1. Program Phase	Circuit Description to Product Release	No limit - Conceptual Phase to Product Release
2. Level of Detail versus Cost	More exhaustive for components selected for Analysis	Relative to System Requirements
3. Skill Level, Expertise Required	Primarily in circuit design of technology utilized	Primarily in systems aspects of technology utilized
4. Facility Special needs	No special facilities required	No special facilities required
5. Fault Management	Assists in quantifying fault isolation	Assists in identifying need for fault isolation at intermediate levels
6. Software Design	Helps to evaluate Software implementation	Helps to evaluate Software scope
7. Safety Hazard Identification	Supports Analysis of Identified Hazards	Hazard identification at system level
8. Design Changes	Less Tolerant of changes; more likely to require amended F/FA	More Tolerant of changes; less likely to require amended F/FA

3.3.3 Skill Level, Expertise Required: The hardware F/FA approach requires a circuit design skill level comparable to the technology utilized. The functional F/FA approach requires system level expertise and an overall familiarity with the design objectives. For processor based digital hardware, these approaches require an overall knowledge of the design, software and fault management requirements.

3.3.4 Facility - Special Needs: The two basic F/FA approaches do not require any special facilities. Other methods, as described in Section 6, require special facilities.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.3.5 Fault Management: Modern systems, particularly processor based systems, usually include a significant amount of fault management. Fault management covers the various aspects of fault detection, fault response, fault storage, fault display, and possibly fault correction. A system with these built-in attributes can be analyzed in a completely different fashion than one without them, or with only rudimentary capabilities. The process becomes one of analyzing the effectiveness of the designed-in fault management capability rather than trying to postulate the effects of specific faults.

3.3.5.1 Fault Detection: Fault detection is basically performed by defining the allowable behavior at various points in the system in the non-faulted condition and then either monitoring continuously or testing at intervals, or on demand, that these conditions have not been violated. The analysis must confirm that failures are indeed detected.

In many cases, a localized bottom-up approach from postulated failure to the next higher detection node will be needed. However, the task is usually simplified because the specific behavior in the faulted condition is not of interest, only the fact that it is distinguishable from the non-faulted behavior. Usually, this may be accomplished by performing tests under known and controlled conditions. For example, an A-to-D converter can be tested at a time when it is off-line by inserting a known input and looking for the expected output. Any other output indicates a failure.

3.3.5.2 Fault Response: The built-in fault response, (i.e., the designed reaction to a detected fault) depends on the specific purpose. Requirements for fault detection usually fall into three categories: safety, operational, and maintenance:

a. Safety requirements will usually involve high level system operations; reconfiguration, signal selection, mode changing or even disconnect in some cases. Secondary safety responses may include relevant annunciations to the flight crew of primary responses.

b. Operational requirements most commonly involve system status indications required by the flight crew for making decisions such as: whether to dispatch or not; dispatch is allowed but only degraded operation is available; etc.

c. Maintenance requirements involve such functions as long term (non-volatile) storage and output (data bus or built-in display) of maintenance related data.

In each case, the analysis must confirm that:

a. The required response(s) to a specific detected fault does indeed occur, and

b. The designed response(s) to a specific detected fault is appropriate.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.3.5.3 Fault Storage and Display: In most cases, the system design will require short term (volatile) and/or long term (non-volatile) storage of fault data in order to implement the required responses.

Often local (built-in) or remote fault display is also required.

The analysis must include consideration of failures of the storage and display elements of the system.

3.3.6 Software Design: Software should be considered from three main aspects, which are:

1. How hardware failures can affect the execution of the operational program.
2. How hardware failures can affect the functional isolation of critical functions.
3. How the Fault Management is designed, particularly those features which are performed via the operational program.

3.3.6.1 Effects on Program Execution: A typical CPU breaks down into functional elements, as follows:

a. Arithmetic Logic Unit (ALU)

b. Read Only Memory (ROM)

c. Random Access Memory (RAM)

d. Interrupt Control

e. Timing and Control

A comprehensive analysis of the effects of all definable failure modes of the above elements on the system behavior under all conditions is impractical. However, the effects of some failures, under some conditions, can be analyzed.

For example, it may or may not be possible to completely trace all the effects of a failure which result in an incorrect state of one bit of a Program ROM. If the affected bit is part of a dedicated data constant, the resulting arithmetical errors may be analyzable; however, if the affected bit is part of an instruction, some of the effects will probably be unpredictable. In either case (or any other ROM bit failure), the resulting change in a ROM checksum is a predictable event.

For other failures, it may be necessary to rely on more indirect evidence that a failure affecting software execution has occurred.

Documents
Document Sharing Hub
Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.3.6.1 (Continued):

The use of built-in self test techniques, such as a periodic execution of specific instructions with controlled inputs, is one example. Another, in a wider sense, is the use of a Watch Dog Timer (sometimes referred to as a heart-beat monitor) to check the program execution time against an independent clock.

The analyst must determine whether failures of the hardware, which can affect program execution, do indeed result in effects which, although not necessarily predictable, are nevertheless detectable by one or more of the fault monitoring techniques applied.

Any residual postulated faults; i.e., possible faults for which detection is uncertain, will probably have to be subjected to testing by one of the special methods described in Section 6.2.

3.3.6.2 Effect of Failures on Functional Isolation: Functional isolation of operational program elements, so that they do not cross physical storage device boundaries, is fairly common in the implementation of digital systems.

Part of the software consideration for a F/FA consists of analyzing the functional relationships of various program segments and a comparison with the storage patterns in the physical devices to ensure that failures in a single storage device do not affect more than one critical function.

3.3.6.3 Fault Management Design: It is important that anyone analyzing a digital system be generally familiar with the system requirements and how these are satisfied by the software design. However, in one area, that of fault management, it is imperative that the analyst develop a good understanding in the detailed specific requirements and the step by step instructions which, when executed, implement the fault management design.

This knowledge is essential for a proper evaluation of:

a. Failure effects, including their detectability, and

b. The ability of the system to respond correctly.

3.3.7 Safety Hazard Identification: The functional approach provides the ability to identify potential hazards. The hardware approach may be required to support analysis of potential hazards, (identified by the functional approach) for meeting acceptable probability levels.

3.3.8 Design Changes: The validity of a completed F/FA analysis is sensitive to follow-on hardware or software changes, and depends on the analysis approach used. In general, the bottom-up F/FAs are more sensitive to design changes since they recognize changes in hardware elements, whereas the top-down F/FAs are based upon broader functional groups.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)

Downloaded from SAE International by Auburn University Libraries, Monday, April 13, 2026

3.4 F/FA Decision Tree:

Figure 3 is a flow chart depicting the key tasks and decisions involved in selecting the fault/failure analyses typically required for safety certification of aircraft digital electronic systems.

To minimize complexity, the chart does not address the situation where the completed analyses show that the system will not meet the safety criteria. It is likely, for example, that if the system lacks full redundancy, many essential systems and most critical systems will fail to meet the specified criteria. In that situation, system redesign with revised analyses would be necessary.

If system failures do not involve essential or critical functions, including providing misleading information to the flight crew, further analysis is normally not required.

If any of the system failures do involve essential or critical functions, the next question is whether sufficient redundancy is provided or other design techniques employed (see paragraph 1.1). If an FMEA can verify the redundancy, adequate failure detection and acceptability of the failure effects, then further analysis may not be required.

On the other hand, if either the redundancy or other design techniques are shown to be lacking or inadequate (by the hazard analysis) or the FMEA fails to verify that the failure effects are acceptable, then a fault tree or other analysis is also necessary. If the analysis shows that the probability of occurrence of each failure condition is acceptable (relative to the criticality category of the failure effect) then further analysis may not be required.

4. FAILURE MODES AND EFFECTS:

4.1 Identification of General Needs:

Performance of F/FAs typically involves a cause-and-effect analysis procedure. As a result, at some point in the analysis, the modes of failure (the "cause") must be considered. This section addresses the topic of failure modes of digital functions and devices.

The level at which a F/FA is started affects what is perceived to be a fault. The top level effect will always be the same, regardless of the level at which analysis is started. If a functional F/FA is to be performed, the modes of failure and their relative frequency of occurrence are hypothesized for each function at this particular equipment level. For a hardware approach at the lowest level subject to analysis, the failure modes themselves must be evaluated in terms of higher level effects. The analyst must guard against dealing with generalities and must recognize the unique aspects of each design.

Within this framework and with emphasis on digitally oriented time-based systems, the determination of basic "failure modes" may often prove difficult, if not impossible. As newer digitally oriented systems evolve, trends toward increasing computational power make it more difficult to identify specific, elementary, simplistic failure modes. Failure modes in this context are synonymous with what are often referred to as failure indicators of digital devices - the output or device package pin level indications of failure caused by internal failure mechanisms related to the chip or interconnect.

Documents
Document Sharing Hub

Full document details: Fault/Failure Analysis For Digital Systems and Equipment (Use ARP4761 for Aircraft Safety Assessment)