SAE INTERNATIONAL

AEROSPACE RECOMMENDED PRACTICE

ARP4761™ REV. A

Issued 1996-12
Revised 2023-12

Superseding ARP4761

(R) Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment

RATIONALE

This SAE Aerospace Recommended Practice (ARP) provides updated and expanded guidelines for accomplishing the safety assessment process on civil aircraft, systems, and equipment.

PREFACE

Since the original publication of ARP4761, the civil aviation industry safety assessment process has evolved. Many practices that were in their infancy when the original document was published are now well established and have more defined processes. For example, the Aircraft Functional Hazard Assessment (AFHA) which was at that time starting to become common practice is now a standard element of the safety assessment process. The AFHA process and legacy methods have been updated, and the Preliminary Aircraft Safety Assessment (PASA), Aircraft Safety Assessment (ASA), and new safety analysis methods have been added in Revision A. In addition to the breakout of the aircraft-level processes, the Definitions section has undergone significant updates and Section 3 has been restructured, including major updates to the figures. This update represents the current industry best practices and is intended to help those developing new or modifying existing civil aircraft, systems, or equipment to have success in developing safe aircraft for the future. Terms no longer used in this document or cases where their dictionary definition applies have been deleted from the definitions.

TABLE OF CONTENTS

1. SCOPE 4
1.1 Purpose 4
1.2 Intended Users 4
1.3 How to Use This Document 4

2. REFERENCES 5
2.1 Applicable Documents 5
2.1.1 SAE Publications 5
2.1.2 U.S. Government Publications 6
2.1.3 FAA Publications 6
2.1.4 EASA Publications 6
2.1.5 RTCA Publications 7
2.1.6 EUROCAE Publications 7
2.1.7 Other References 7
2.2 Definitions 8
2.3 Acronyms 12

SAE Executive Standards Committee 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 © 2023 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

For more information on this standard, visit
https://www.sae.org/standards/content/ARP4761A/

Documents
Document Sharing Hub

Full document details: SAE ARP4761A

3. SAFETY ASSESSMENT PROCESS 14
3.1 Safety Assessment Process Overview 14
3.1.1 Safety Assessment Process Activities and Interactions 16
3.1.2 Safety Analysis Methods 17
3.2 Aircraft Functional Hazard Assessment (AFHA) 20
3.3 Preliminary Aircraft Safety Assessment (PASA) 20
3.4 System Functional Hazard Assessment (SFHA) 20
3.5 Preliminary System Safety Assessment (PSSA) 21
3.6 System Safety Assessment (SSA) 21
3.7 Aircraft Safety Assessment (ASA) 22
3.8 Determining Depth of Analysis for Failure Conditions 22
3.9 Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) Assignment 22
3.10 Considerations of Human Error in the Safety Assessment Process 22

4. SAFETY ANALYSIS METHODS 23
4.1 Fault Tree Analysis/Dependence Diagram/Markov Analysis/Model-Based Safety Analysis 23
4.1.1 Applications of the FTA, DD, MA, and MBSA 23
4.2 Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Summary (FMES) 25
4.3 Cascading Effects Analysis (CEA) 25
4.4 Zonal Safety Analysis (ZSA) 25
4.5 Particular Risk Analysis (PRA) 26
4.6 Common Mode Analysis (CMA) 26

5. SAFETY-RELATED MAINTENANCE TASKS AND INTERVALS 26
5.1 Certification Maintenance Requirements 26
5.2 Maintenance Steering Group 27

6. MASTER MINIMUM EQUIPMENT LIST (MMEL) 27

7. TIME-LIMITED DISPATCH (TLD) 27

8. IN-SERVICE SAFETY ASSESSMENT 28

9. NOTES 28
9.1 Contribution Acknowledgement 28
9.2 Contribution Acknowledgement 29
9.3 Revision Indicator 29

APPENDIX A AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA) 30

APPENDIX B PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA) 49

APPENDIX C SYSTEM FUNCTIONAL HAZARD ASSESSMENT (SFHA) 65

APPENDIX D PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) 84

APPENDIX E SYSTEM SAFETY ASSESSMENT (SSA) 97

APPENDIX F AIRCRAFT SAFETY ASSESSMENT (ASA) 104

APPENDIX G FAULT TREE ANALYSIS (FTA) 112

APPENDIX H DEPENDENCE DIAGRAM (DD) 167

APPENDIX I MARKOV ANALYSIS (MA) 172

AVA Documents Document Sharing Hub

Full document details: SAE ARP4761A

APPENDIX J FAILURE MODES AND EFFECTS ANALYSIS (FMEA) 242

APPENDIX K ZONAL SAFETY ANALYSIS (ZSA) 256

APPENDIX L PARTICULAR RISK ANALYSIS (PRA) 266

APPENDIX M COMMON MODE ANALYSIS (CMA) 274

APPENDIX N MODEL-BASED SAFETY ANALYSIS (MBSA) 290

APPENDIX O CASCADING EFFECTS ANALYSIS (CEA) 321

APPENDIX P FUNCTION AND ITEM DEVELOPMENT ASSURANCE ASSIGNMENT (FDAL/IDAL) 330

APPENDIX Q CONTIGUOUS SAFETY ASSESSMENT PROCESS EXAMPLE 351

Figure 1 Overview of safety assessment process 16
Figure 2 Safety assessment process interaction with a typical development process 18
Figure 3 General safety assessment process 19

Documents
Document Sharing Hub

Full document details: SAE ARP4761A

1. SCOPE

ARP4761A and its EUROCAE counterpart, ED-135, present guidelines for performing safety assessments of civil aircraft, systems, and equipment. They may be used when addressing compliance with certification requirements (e.g., 14 CFR/CS Parts 23, 25, 27, and 29 and 14 CFR Parts 33, 35, CS-E, and CS-P). ARP4761A/ED-135 may also be used to assist a company in meeting its own internal safety assessment standards. While the safety assessment processes described are primarily associated with civil aircraft, systems, and equipment, these processes may be used in many other applications. The guidelines herein identify a systematic safety assessment process, but other processes may be equally effective.

The processes described herein are usually applicable to the new designs or to existing designs that are affected by changes to design or functions. In the case of the implementation of existing design(s) in a derivative application, complementary means such as service experience in a similar application may be used in the safety assessment.

ARP4761A/ED-135 does not address safety assessment of in-service products but does include references to those processes. ARP5150A and ARP5151A contain processes for conducting in-service safety assessments.

This document does not include information on security threat considerations.

1.1 Purpose

This document presents guidelines for conducting an industry accepted safety assessment process consisting of the Aircraft Functional Hazard Assessment (AFHA), Preliminary Aircraft Safety Assessment (PASA), System Functional Hazard Assessment (SFHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Aircraft Safety Assessment (ASA) processes.

This document also presents information on the safety analysis methods that may be used to conduct the safety assessment process. These methods include Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Zonal Safety Analysis (ZSA), Particular Risk Analysis (PRA), and Common Mode Analysis (CMA).

1.2 Intended Users

The intended users of this document include, but are not limited to, aircraft, engine, and propeller 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 provided in this document are intended to be used in conjunction with other applicable documents (e.g., ARP4754B/ED-79B, RTCA DO-178C/ED-12C, RTCA DO-254/ED-80, and RTCA DO-297/ED-124), and also with the associated certification regulations and advisory material. These regulations/advisory materials include 14 CFR/CS Parts 23, 25, 27, and 29 (sections 1309, 1709, 2510, and other system safety requirements such as sections 671, 783, 901, 903, and 933, as applicable) and 14 CFR Parts 33 and 35, CS-E, and CS-P. Since the terminology used herein is directly aligned with ARP4754B/ED-79B, the application of ARP4761A/ED-135 in support of other development processes may require an understanding of the concepts in ARP4754B/ED-79B.

All the processes described in this document may not be applicable to all projects. The depth each process goes to in this document is an example and the level presented here may not be applicable to all projects. The safety program plan (or similar planning document) should draw from the list of processes depicted in this document, and describe how, and to what depth they will be used. The size and scope of the final process presented in this document may not be appropriate for the type and complexity of the product or STC activity. At a high level, the applicant is strongly encouraged to have the safety program plan (or similar planning document) include the depth to which each process will be applied, and where the results will show that the safety requirements are met. For information on planning documents, refer to ARP4754B/ED-79B. This document defines an overall safety assessment process and provides recommendations of process outputs. It identifies activities, methods, and inputs that may be used in the performance of safety assessments for civil aircraft and their associated systems and equipment. It is recognized that the safety process for a given program will be accomplished at multiple levels by multiple stakeholders.

AVA Documents
Document Sharing Hub
Full document details: SAE ARP4761A

General guidelines in evaluating the safety aspects of an aircraft, system, or equipment are provided in Section 3; the recommended processes and analytical methods, and the relationship between these, are introduced therein. Section 4 expands on some of these analytical methods. Section 5 provides information on the use of the analytical methods in this document by the manufacturer in determining maintenance tasks and intervals that provide for safe operation of the aircraft. Section 6 describes the relationship between the safety assessment process and the Master Minimum Equipment List (MMEL). Section 7 provides information on the Time Limited Dispatch (TLD) concept for Full-Authority Digital Engine Control (FADEC) systems which may be helpful in developing similar aircraft design solutions. Section 8 provides information on associated in-service safety assessment.

Users who need further information on a specific process or method may obtain detailed information from Appendices A through P. Appendix Q provides a contiguous example of the safety assessment process for a hypothetical system. This 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 standalone documents, but are intended to be used in conjunction with the information contained in this document's main body. The user is cautioned not to use the appendices independent of the document main body. Further, the contiguous example contained in Appendix Q should not be used without making reference to the document main body and corresponding appendices.

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

Throughout this document and appendices, reference is made to using FTA. It should be understood by the reader that other quantitative analysis methods—such as DD, MA, or MBSA—may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

ARP5580 contains information about FMEA, but ARP4761A/ED-135 takes precedence for purposes of civil aircraft safety assessment.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. 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 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 International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

AIR6219	Development of Atmospheric Neutron Single Event Effects Analysis for Use in Safety Assessments
ARP4754B	Guidelines for Development of Civil Aircraft and Systems
ARP5107C	Guidelines for Time-Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems
ARP5150A	Safety Assessment of Transport Airplanes in Commercial Service
ARP5151A	Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

2.1.2 U.S. Government Publications

Copies of these documents are available online at https://quicksearch.dla.mil.

MIL-HDBK-217F Reliability Prediction of Electronic Equipment

MIL-HDBK-338B Electronic Reliability Design Handbook

2.1.3 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

14 CFR 23.2510 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 25.1309 Airworthiness Standards: Transport Category Airplanes, Subpart F - Equipment; Equipment, Systems, and Installations (refer to AC 25.1309-1A)

14 CFR 27.1309 Airworthiness Standards: Normal Category Rotorcraft, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 29.1309 Airworthiness Standards: Transport Category Rotorcraft, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 25.1709 Airworthiness Standards: Transport Category Airplanes, Subpart H - Electrical Wiring Interconnection Systems (EWIS) - System Safety, EWIS

14 CFR 33 Airworthiness Standards: Aircraft Engines

14 CFR 35 Airworthiness Standards: Propellers

AC 20-155A Industry Documents to Support Aircraft Lightning Protection Certification

AC 20-158A The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment

AC 25-19A Certification Maintenance Requirements

AC 25.1309-1A System Design and Analysis*

*Note that, through the Equivalent Level of Safety (ELOS) process, the FAA may grant an applicant the use of the AC 25.1309 Draft ARSENAL which accompanies an ELOS finding on 14 CFR 25.1301 and 25.1309 that the Aviation Rulemaking Advisory Committee (ARAC) recommended in June 2002 ARAC report TAEsdaT2-5241996 (includes AC/AMJ 25.1309 Draft ARSENAL revised System Design and Analysis).

2.1.4 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu.

CS 23.2510 Certification Specifications for Normal-Category Aeroplanes, Subpart F - Equipment; Equipment, systems and installations

CS 25.1309 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart F - Equipment; Equipment, systems and installations

CS 27.1309 Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft, Subpart F - Equipment; Equipment, systems and installations

AVA Documents Document Sharing Hub

Full document details: SAE ARP4761A

CS 29.1309 Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft, Subpart F - Equipment; Equipment, systems and installations

CS 25.1709 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart H, System Safety, EWIS

CS-E Certification Specifications and Acceptable Means of Compliance for Engines

CS-MMEL Master Minimum Equipment List

CS-P Certification Specification for Propellers

AMC 25.1309 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart F - System Design and Analysis (contained within CS 25)

AMC 25-19 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Certification Maintenance Requirements (contained within CS 25)

2.1.5 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-178B Software Considerations in Airborne Systems and Equipment Certification

DO-178C Software Considerations in Airborne Systems and Equipment Certification

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

DO-297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

2.1.6 EUROCAE Publications

Available from EUROCAE Secretariat, 9-23 Rue Paul Lafargue, 93200 Saint-Denis, France, Tel: +33 1 40 92 79 30, https://www.eurocae.net/.

ED-12B Software Considerations in Airborne Systems and Equipment Certification

ED-12C Software Considerations in Airborne Systems and Equipment Certification

ED-79B Guidelines for Development of Civil Aircraft and Systems

ED-80 Design Assurance Guidance for Airborne Electronic Hardware

ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

ER-008 Development of Atmospheric Neutron Single Event Effects Analysis for use in Safety Assessments

2.1.7 Other References

MSG-3 Operator/Manufacturer Scheduled Maintenance Development

NUREG-0492 Fault Tree Handbook, U.S. Nuclear Regulatory Commission

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

2.2 Definitions

NOTE: The shared definitions in ARP4754B/ED-79B, ARP5150A, ARP5151A, and those in this document and ED-135 have been coordinated for consistency.

ANALYSIS: A detailed examination based on decomposition into simple elements.

ASSESSMENT: An evaluation process which may include one or more types of analysis and experience.

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

ASSURANCE: The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements (DO-178C/ED-12C, ARP4754B/ED-79B).

“AT RISK” TIME: The period of time during which the aircraft may be subject to the failure effect under analysis.

AVAILABILITY: Qualitative or quantitative attribute that a system or equipment is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system (equipment) not providing its output(s), i.e., unavailability.

CERTIFICATION: The legal recognition that a product complies with the applicable regulations.

CERTIFICATION AUTHORITY: Organization or person responsible for granting approval in accordance with applicable regulations.

COMMON CAUSE: A single failure, error, or event that can produce undesirable effects on two or more systems, equipment, items, or functions.

DERIVED REQUIREMENTS: Requirements that introduce behaviors or characteristics beyond those specified in higher-level requirements.

DEVELOPMENT ASSURANCE: All those planned and systematic actions used to substantiate, at an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable certification basis (derived from AC 25.1309 Draft ARSENAL revised and AMC 25.1309).

DEVELOPMENT ERROR: A mistake in requirements, design, or implementation.

EQUIPMENT: A physical object that can be installed and removed from the aircraft and performs one or more specific functions. Equipment contains one or more items.

ERROR: An omitted or incorrect action by a manufacturer, crew member, or maintenance person, or a mistake in requirements, design, or implementation (derived from AMC 25.1309).

EXPOSURE TIME: The period of time between when a specific system, equipment, or item, that can cause or contribute to the failure condition under analysis, was last known to be operating properly and when it will be known to be operating properly again.

EXTERNAL EVENT: An occurrence which has its origin distinct from the aircraft or the system being examined, such as atmospheric conditions (e.g., wind gusts/shear, temperature variations, icing, lightning strikes), operating environment (e.g., runway conditions, conditions of communication, navigation, and surveillance services), cabin and baggage fires, and bird-strike. The term is not intended to cover sabotage.

FAILURE: An occurrence which affects the operation of an aircraft, system, equipment, item, or piece-part such that it can no longer function as intended (this includes both loss of function and malfunction). Note: Errors may cause Failures but are not considered to be Failures.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

FAILURE CONDITION (FC): A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events (AMC 25.1309).

FAILURE CONDITION CLASSIFICATION: A discrete scale allowing categorization of the severity of the effects of a failure condition. Classification levels are defined in the applicable regulation and advisory material. For example, AC 25.1309 Draft ARSENAL revised and AMC 25.1309 define the following classifications; Catastrophic, Hazardous, Major, Minor, and No Safety Effect.

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

FAILURE MODE: A specific way in which a system, equipment, hardware item, or piece-part may fail.

FAILURE RATE: The expected frequency of occurrence of a specific failure mode over a period of time. The failure rate at time t may be calculated by dividing the failure density function f(t) by the reliability distribution function R(t) where:

$$R(t) = (1\text{-failure distribution function } F(t))$$

$$\lambda(t) = f(t)/(1-F(t))$$

Note that 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.

FAULT: A manifestation of an error in an item or system that may lead to a failure.

FUNCTION: Intended behavior of an aircraft, system, equipment, or item regardless of implementation.

FUNCTION DEVELOPMENT ASSURANCE LEVEL (FDAL): The level of rigor of development assurance tasks performed to Functions. Note: The FDAL is used to identify the ARP4754B/ED-79B objectives that need to be satisfied for the aircraft/system functions.

FUNCTIONAL FAILURE SET (FFS): A set of one, or more members that are considered to be independent from one another (not necessarily limited to one system), whose development error(s) leads to a top-level failure condition.

FUNCTIONAL INDEPENDENCE: See INDEPENDENCE.

GUIDANCE: Recommended procedures for showing compliance with regulations.

GUIDELINE: Supporting information that can be helpful but is not considered to be guidance.

HARDWARE: The physical realization of systems, equipment, or items. May refer to these objects individually or collectively.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

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

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

INDEPENDENCE: Specific types of independence include:

- FUNCTIONAL INDEPENDENCE: A characteristic that minimizes the likelihood of common development errors by using different functions.
- ITEM DEVELOPMENT INDEPENDENCE: A characteristic that minimizes the likelihood of common development errors by using different item designs.
- PHYSICAL INDEPENDENCE: A characteristic that minimizes the likelihood of common failures caused by physical failure, damage, or environmental effects by using physical separation or segregation between two or more things, e.g., hardware items, equipment, wiring, tubing.
- PROCESS INDEPENDENCE: A practice that minimizes the likelihood of development errors by using separation of responsibilities that assures the accomplishment of objective evaluation by someone other than the performer of the activity, e.g., validation activities are not performed solely by the developer of the requirement(s) of a system or item.

INDEPENDENCE PRINCIPLE: Features of an intended implementation where independence has been determined to be necessary.

INSPECTION: An examination of a system or item against a specific standard.

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

INTEGRITY: Qualitative or quantitative attribute of a system, equipment, or an item indicating that it can be relied upon to work as intended.

ITEM: A defined and bounded set of either (one or more) hardware elements or (one or more) software elements which are treated as a single entity for analytical purposes.

ITEM DEVELOPMENT ASSURANCE LEVEL (IDAL): The level of rigor of development assurance tasks performed on Item(s); e.g., IDAL is the appropriate software level in DO-178C/ED-12C, and design assurance level in DO-254/ED-80 objectives that need to be satisfied for an item.

ITEM DEVELOPMENT INDEPENDENCE: See INDEPENDENCE.

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

MALFUNCTION: A condition where the operation of a function is different than intended, excluding the loss of function.

MEAN TIME BETWEEN FAILURES (MTBF): The average elapsed time between consecutive failures of a repairable system, equipment, or hardware item during operation under stated conditions.

MEAN TIME TO FAILURE (MTTF): The average elapsed time to failure for a non-repairable system, equipment, or hardware item during operation.

MEMBER: An aircraft or system function or item that may contain a development error causing its loss of function or malfunction. (Used only with regard to a Functional Failure Set.)

MINIMAL CUT SET (MCS): A set of primary events where removing any single primary event no longer results in the top event.

MODEL: An abstract representation of a given set of aspects of a system/function/item that is used for its analysis, implementation, simulation, or code generation and that has unambiguous, well-defined syntax and semantics.

MONITORING: The act of detecting the effects of a failure. May or may not result in mitigation or corrective action of the adverse effects as defined by the analyzing organization.

AVA Documents
Document Sharing Hub
Full document details: SAE ARP4761A

PARTITIONING: The use of physical or logical boundaries to separate portions of a system or an item such that the portions may be considered independent.

PROCESS: A set of interrelated activities performed to produce a prescribed output or product.

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

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

RISK: The potential of an occurrence to cause harm defined by its probability and the severity of its consequence(s).

SAFETY: The state in which risk is acceptable.

SAFETY OBJECTIVE: A qualitative and/or quantitative attribute necessary to achieve the required level of safety for the identified failure condition, depending on its classification.

SAFETY REQUIREMENT: A requirement which is necessary to achieve either a safety objective or satisfy a constraint established by the safety process.

SEGREGATION: The use of a barrier to provide physical independence between hardware elements.

SEPARATION: The use of physical distance to provide independence between hardware elements.

SIGNIFICANT LATENT FAILURE: A latent failure which, in combination with one or more specific failures or events, would result in a Hazardous or Catastrophic failure condition (AC 25.1309 draft ARSENAL revised/AMC 25.1309).

SOFTWARE: Executable algorithm that runs on a computer. May refer to such elements individually or collectively.

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

SUBSYSTEM: A defined portion of a system that performs one or more specific functions.

SURVIVABILITY: The ability of an aircraft, system, or equipment to continue to function in a way that achieves safe aircraft operation after being affected by an outside influence, e.g., by a failure or environmental event external to the aircraft or system affected. Note that the subset crash survivability, aka crash resistance, refers to the ability of an aircraft design to protect the occupants (crew and passengers) from injury during/after a crash.

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

TRACEABILITY: The recorded relationship established between two or more elements of the development process. For example, between a requirement and its source or between a verification method and its requirement.

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

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

2.3 Acronyms

AC	Advisory Circular (FAA)
AFHA	Aircraft Functional Hazard Assessment
AFM	Aircraft Flight Manual
AMC	Acceptable Means of Compliance (EASA)
ARP	Aerospace Recommended Practice (SAE)
ASA	Aircraft Safety Assessment
CCMR	Candidate Certification Maintenance Requirement
CEA	Cascading Effects Analysis
CFR	Code of Federal Regulations
CMA	Common Mode Analysis
CMCC	Certification Maintenance Coordination Committee
CMR	Certification Maintenance Requirement
CoFFE	Combined Functional Failure Effects
COTS	Commercial Off-the-Shelf
CS	Certification Specification
CTMC	Continuous Time Markov Chain
DD	Dependence Diagram
EASA	European Union Aviation Safety Agency
ETOPS	Extended-Range Operations
EUROCAE	European Organisation for Civil Aviation Equipment
EWIS	Electrical Wiring Interconnection Systems
FAA	Federal Aviation Administration
FADEC	Full-Authority Digital Engine Control
FC	Failure Condition
FC&C	Failure Conditions and Classifications
FDAL	Function Development Assurance Level
FFBD	Functional Flow Block Diagram

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

FFS	Functional Failure Set
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes and Effects Summary
FPM	Failure Propagation Model
FTA	Fault Tree Analysis
HIRF	High-Intensity Radiated Fields
HW	Hardware
IDAL	Item Development Assurance Level
IMA	Integrated Modular Avionics
I/O	Input/Output
LH	Left Hand
LOTC	Loss of Thrust Control
LRU	Line Replaceable Unit
MA	Markov Analysis
MBSA	Model-Based Safety Analysis
MBSE	Model-Based System Engineering
MC	Markov Chain
MCS	Minimal Cut Set
MF&MS	Multifunction and Multisystem
MM	Markov Model
MMEL	Master Minimum Equipment List
MRB	Maintenance Review Board
MSG-3	Maintenance Steering Group 3
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
ODE	Ordinary Differential Equation
PASA	Preliminary Aircraft Safety Assessment

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RH	Right Hand
ROF	Required Order Factor
RTO	Rejected Takeoff
SEE	Single Event Effects
SEU	Single Event Upset
SFHA	System Functional Hazard Assessment
SSA	System Safety Assessment
SW	Software
TC	Type Certificate (or Certification)
TLD	Time-Limited Dispatch
TSF	Time Since Fault
ZSA	Zonal Safety Analysis

3. SAFETY ASSESSMENT PROCESS

3.1 Safety Assessment Process Overview

The safety assessment process is one of multiple processes integral to aircraft and system development. Other integral processes such as requirements management, configuration management, and process assurance are described in ARP4754B/ED-79B. The safety assessment process:

- Evaluates aircraft functions and the design of systems performing these functions.
- Identifies and classifies failure conditions associated with those functions and systems.
- Determines the minimum level of rigor to be applied to the associated development assurance activities according to the classification of those failure conditions.
- Identifies safety objectives and requirements.
- Hierarchically validates these safety requirements for completeness and correctness at each tier (e.g., aircraft, systems, and items).
- Confirms that the implementation satisfies its safety requirements and objectives.

The safety assessment process is iterative and both qualitative and quantitative in nature with its activities supporting the aircraft development process. Through these activities, the safety assessment process provides confidence that the likelihood of failures and errors that may lead to failure conditions has been minimized to a level commensurate with the severity of these failure conditions.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Figure 1 depicts a top-level view of a typical development cycle timeline and the relationship of the safety assessment process to a development process. The development process and safety assessment process are iterative in nature. The safety assessment process includes the following principal processes generally initiated in sequence, but not necessarily completed in sequence. These processes may include the production of reports documenting the results of these processes.

- Aircraft Functional Hazard Assessment (AFHA)

  A systematic, comprehensive evaluation of aircraft functions to identify and classify failure conditions (FCs) of those functions according to their severity, and provide a basis for aircraft-level safety objectives.

- Preliminary Aircraft Safety Assessment (PASA)

  A systematic, comprehensive evaluation of a proposed aircraft architecture to provide confidence that the safety objectives resulting from the failure condition classifications can be met by developing safety requirements pertaining to those failure conditions.

- System Functional Hazard Assessment (SFHA)

  A systematic, comprehensive evaluation of system functions to identify and classify failure conditions of those functions according to their severity and provide a basis for system-level safety objectives.

- Preliminary System Safety Assessment (PSSA)

  A systematic, comprehensive evaluation of a proposed system architecture and equipment/item designs to provide confidence that the safety objectives resulting from the failure condition classifications and system-level safety requirements from the PASA can be met by developing associated system-level, equipment-level, and item-level safety requirements pertaining to those failure conditions.

- System Safety Assessment (SSA)

  A systematic, comprehensive evaluation of the implemented system to verify that applicable safety objectives and requirements are met.

- Aircraft Safety Assessment (ASA)

  A systematic, comprehensive evaluation of the aircraft to verify that applicable safety objectives and requirements are met.

The safety assessment process reflects multiple system-level processes (SFHAs, PSSAs, and SSAs) for an aircraft's multiple systems. Note that a system could consist of one or more systems (sometimes called "subsystems"), thereby entailing the system-level processes for each of those systems and hierarchal interfaces with other safety assessment processes.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

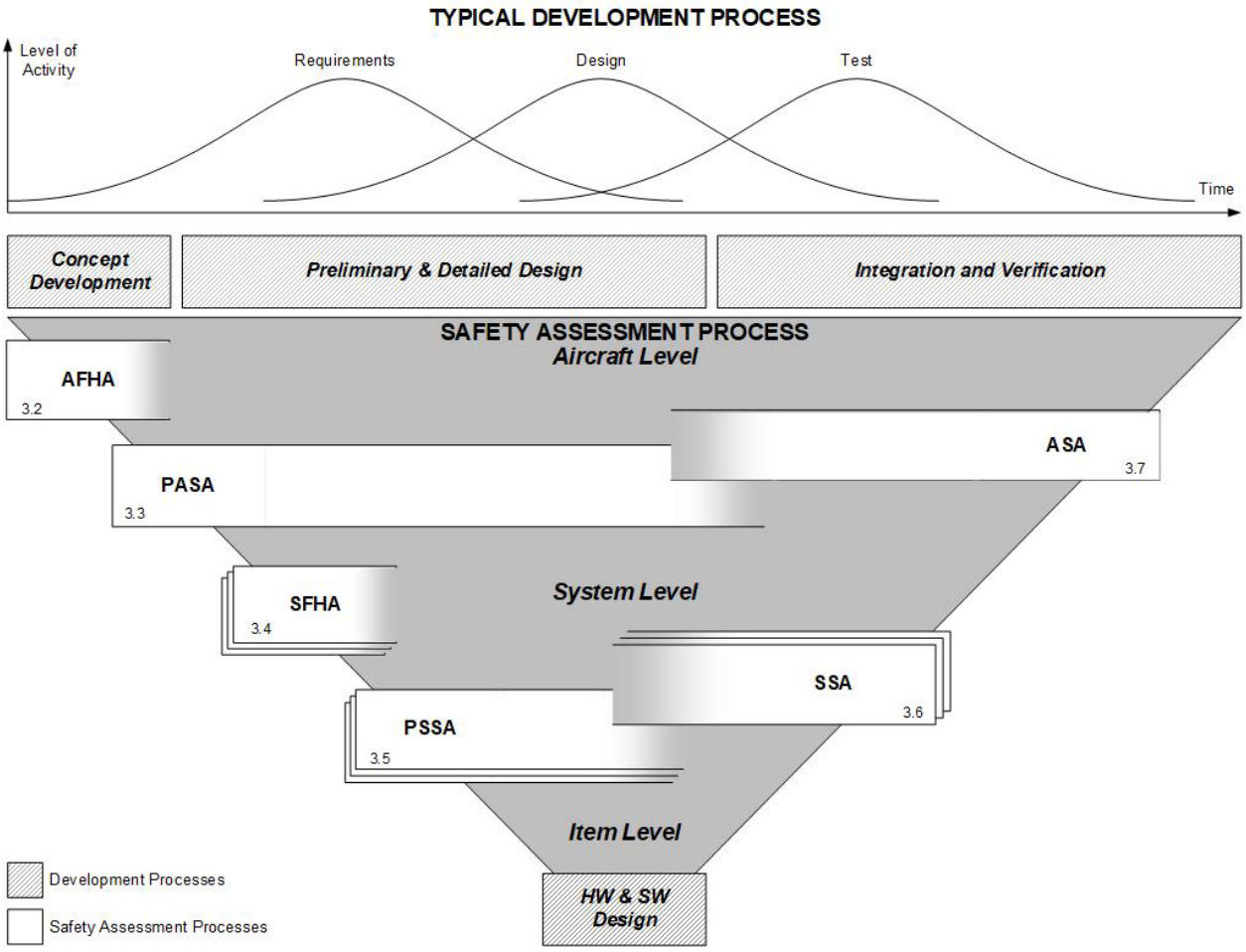


Figure 1 - Overview of safety assessment process

3.1.1 Safety Assessment Process Activities and Interactions

Safety assessment process activities are conducted in conjunction with the associated development process activities and should be described in a plan such as the safety program plan in ARP4754B/ED-79B. Figure 2 highlights the safety assessment principal processes' interactions with key development process activities, such as those in ARP4754B/ED-79B. Figure 3 summarizes the safety assessment process and highlights its safety activities and interactions. The activities shown in these two figures are conducted in parallel with multiple interactions between the processes, but are presented separately to provide graphical clarity.

The safety assessment process begins in the AFHA process with the review of aircraft-level functions from the development process and the determination of aircraft/system-level failure conditions. Safety objectives based on the classification of those failure conditions are provided for use in the PASA process. In the PASA process, the proposed aircraft architecture is evaluated to provide confidence that the safety objectives resulting from the AFHA failure condition classifications can be met. Safety requirements pertaining to safety objectives associated with those failure conditions are established and passed on to the development process for allocation to systems, subsystems, and items. Requirements are also passed on to the PSSA processes for the systems allocated such requirements along with assigned Function Development Assurance Levels (FDALs).

Similar to and usually following the aircraft-level AFHA and PASA processes, the SFHA and PSSA processes are executed to accomplish similar activities and objectives at the system level. The development process allocates functions to systems and the SFHA process evaluates associated failure conditions and classifications for those functions. Safety objectives are established from those failure condition classifications. The PSSA process identifies safety requirements to satisfy those safety objectives. These safety requirements are then passed to other systems, subsystems, and items for implementation.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

In some cases, the originator may flow safety objectives from the AFHA (SFHA) to the development process and the PASA (PSSA). In other cases, the originator may flow failure condition classifications to the development process and the PASA (PSSA) with safety objectives being established from these failure condition classifications within the PASA (PSSA) processes.

The SSA process verifies that the implemented system design meets the qualitative and quantitative safety objectives and requirements from the SFHA, PSSA, and PASA.

Similarly, the ASA process provides confirmation that aircraft-level analyses and SSAs' results verify the overall aircraft and systems design meets the qualitative and quantitative safety objectives and safety requirements from the AFHA and PASA.

Any change to the design or a principal assessment could precipitate a change to another principal assessment, e.g., a change to the PASA or SFHA could drive a change to the PSSA/SSA. As the design evolves, changes are made and the modified design is reassessed. This reassessment may modify existing safety requirements or identify new safety requirements to meet the safety objectives, which may necessitate further design changes. The safety assessment process is complete when the applicable SSA(s) and ASA results show that the applicable system-level and aircraft-level safety objectives have been satisfied and confirm applicable safety requirements have been met.

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

Sections 3.2 through 3.7 provide descriptions of the six principal processes within the safety assessment process. The details of the processes in this ARP describe one means of performing those processes; other means of completing the objectives of the processes may be possible.

3.1.2 Safety Analysis Methods

The safety assessment process includes safety analysis methods which may be applied throughout the typical development cycle to provide the analyst a means of qualitatively and/or quantitatively assessing the safety of a design. These methods include Fault Tree Analysis (FTA), Dependence Diagrams (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA), and Common Mode Analysis (CMA). The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may be incorporated into any of the higher-level assessments. Figure 3 shows where safety analysis methods can be used within the safety assessment process. The PRA/ZSA/CMA include consideration of physical and installation risks fundamental to the definition of both aircraft and system architectures. These analyses interact with the development process throughout the development lifecycle.

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. The PRA, ZSA, and CMA provide methods for evaluation of independence or the identification of specific dependencies due to a common cause. These methods may also aid the PASA and PSSA in generation of independence requirements (e.g., physical, installation requirements).

The PRA and ZSA support the overall development of the specific aircraft, system, and equipment architectures by evaluating the overall architecture sensitivity to aircraft-level hazards. PRAs are managed from an overall aircraft perspective to address particular physical hazards, within or external to the aircraft, which could affect the entire airframe (or several aircraft sections) and/or impact one or more aircraft systems and their installation. ZSAs are managed from a zonal perspective to address physical hazards related to physical installation.

The PRA and ZSA are described as safety methods in this document, but depending on company organization of these aircraft-wide safety activities evaluating more than just common cause considerations, they may also be considered as processes in their own right.

Section 4 summarizes the details of each safety analysis method addressed above.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

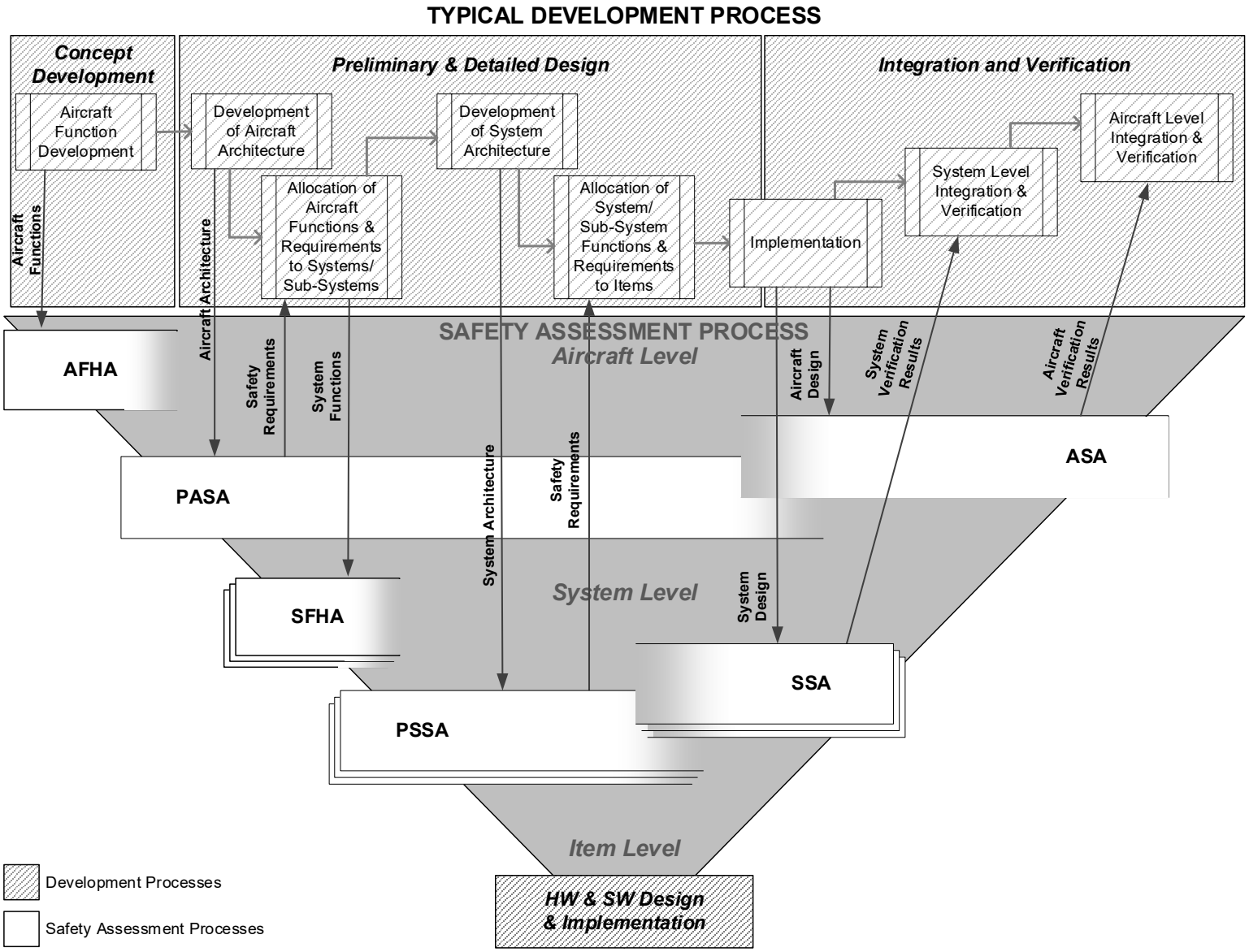


Figure 2 - Safety assessment process interaction with a typical development process

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

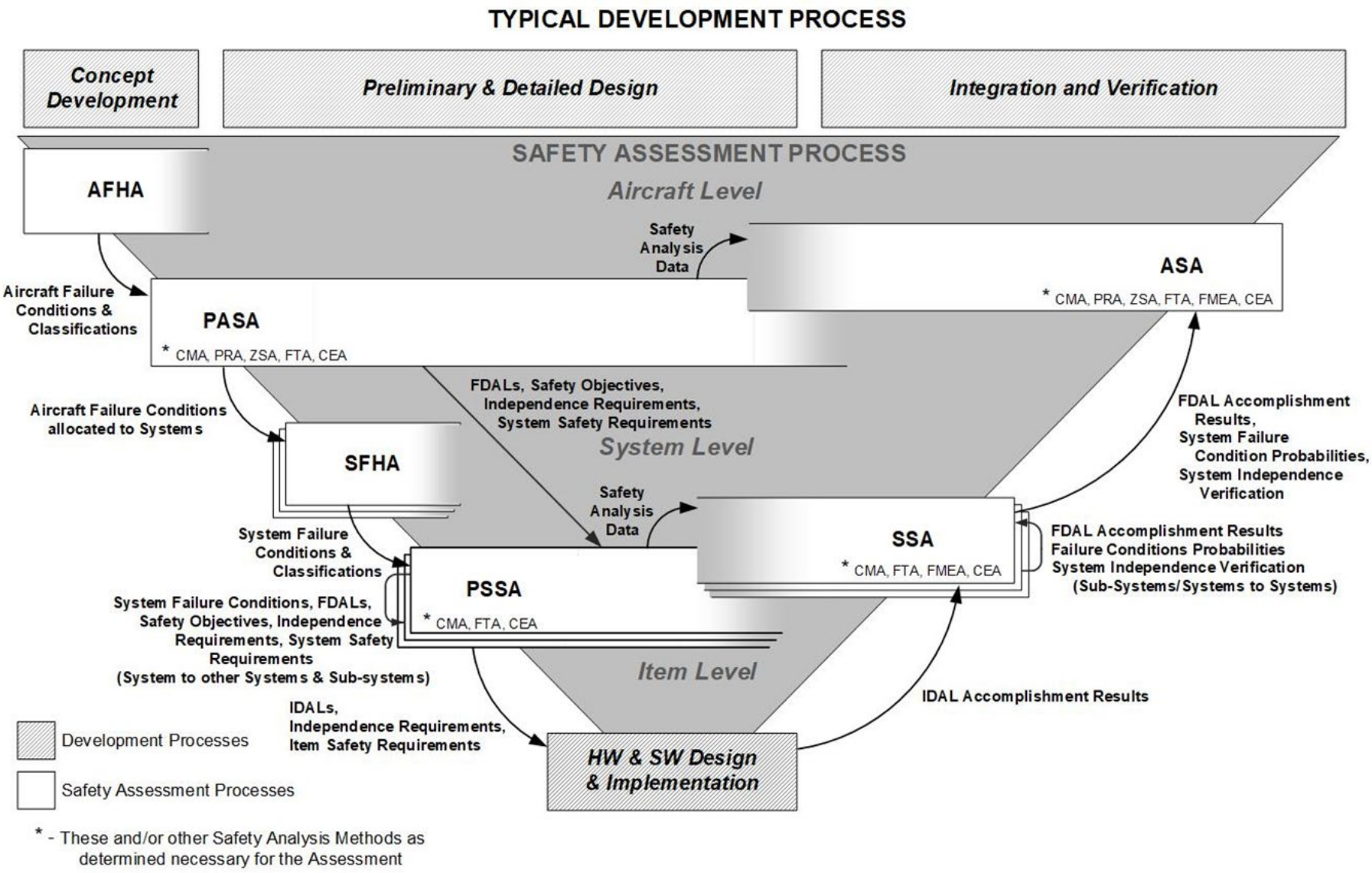


Figure 3 - General safety assessment process

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

3.2 Aircraft Functional Hazard Assessment (AFHA)

The AFHA is a systematic, comprehensive evaluation of the aircraft functions as defined at the beginning of aircraft development. An AFHA identifies and classifies the failure conditions associated with each aircraft-level function. The goal in conducting this AFHA is to clearly identify each failure condition along with the rationale for its severity classification. The classification of these failure conditions establishes the safety objectives that an aircraft should meet. The AFHA should also identify assumptions associated with aircraft and crew mitigations to limit the severity classification, e.g., operating limits, crew information presentation, operating procedures. The passing of failure conditions, their classifications, and associated assumptions from the AFHA to the PASA is the starting point for conducting the PASA.

For details in performing the AFHA, see Appendix A.

3.3 Preliminary Aircraft Safety Assessment (PASA)

The PASA is a systematic, comprehensive evaluation of a proposed aircraft architecture to determine how failures can lead to aircraft-level failure conditions identified by the AFHA and how the safety objectives can be met. The objective of the PASA is to use the safety objectives established from the failure conditions classifications to establish the safety requirements of the aircraft and to determine that the proposed architecture can reasonably be expected to meet the safety objectives. The PASA process is interactive and associated with design definition. Just as the design process is iterative, the PASA process is iterative.

The PASA addresses the failure conditions identified in the AFHA that may require an analysis at the aircraft level, in particular, failure conditions that cannot be allocated to a single system (i.e., AND-gates between different systems or functions). As addressed in 3.1, the PASA process may use various safety analysis methods. Common cause considerations are taken into account in the PASA process. The PASA methods of safety analysis may be qualitative and/or quantitative. See 3.8 on using depth of analysis to determine the type of analysis to apply in evaluating failure conditions. The PASA evaluates combined functional failure effects of the related systems and potential common cause failures between them, including consideration of their shared resources. The PASA also identifies safety requirements such as independence requirements and FDAL assignments for the associated aircraft functions. The development process allocates these safety requirements from the PASA to the individual PSSA processes. See 3.9 for details on development assurance level assignment. See Section 4 for descriptions of the various safety analyses that may be used in conducting the PASA. Once the aircraft-level safety requirements have been defined through PASA process and the implementing systems mature, the ASA process may be initiated as described in 3.7.

For details in performing the PASA, see Appendix B.

3.4 System Functional Hazard Assessment (SFHA)

The SFHA is a systematic, comprehensive evaluation of system functions conducted early in system development to identify and classify the failure conditions of each system-level function, including those fulfilling any aircraft-level functions allocated to the system. The goal in conducting the SFHA is to clearly identify each failure condition along with the rationale for its severity classification. The classification of these failure conditions establishes the safety objectives that the system should meet.

After aircraft functions have been allocated to systems by the design process, each system is examined using the SFHA process. If additional aircraft-level failure conditions affecting the system-level functions are identified, the SFHA is revised to identify and classify the system's failure conditions. Similarly, if system-level failure conditions affecting aircraft-level or other system-level functions are identified, these should be captured in the SFHA and passed to the AFHA. The SFHA should also identify assumptions associated with aircraft and crew mitigations to limit the severity classification, e.g., operating limits, crew information presentation, operating procedures. The passing of failure conditions, their classifications, and associated assumptions from the SFHA(s) to the PSSA(s) is used as the starting point for conducting the PSSA(s).

For details in performing the SFHA, see Appendix C.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

3.5 Preliminary System Safety Assessment (PSSA)

A PSSA process is a systematic, comprehensive evaluation of a proposed system architecture to determine how failures can lead to the system-level failure conditions identified by the SFHA. Safety objectives are established from failure conditions and classifications, and the PASA provides safety requirements based on the contribution of the system to aircraft failure conditions including allocated probability requirements and FDALs. The PSSA is used to establish the safety requirements of the system, including independence requirements, and to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the SFHA or PSSA processes and safety requirements allocated from the PASA and/or higher-level systems. As addressed in 3.1, the PSSA process may use various safety analysis methods to determine these requirements. See 3.8 on using depth of analysis to determine the type of analysis to apply in evaluating failure conditions. The PSSA process should consider the potential impact of Single Event Effects (SEE) on electronic airborne systems. The PSSA also identifies the necessary FDAL and Item Development Assurance Level (IDAL) assignments for the system function and items. See 3.9 for details on development assurance level assignment. See Section 4 for descriptions of the various safety analyses that may be used in conducting the PSSA.

The PSSA process identifies where protective strategies may be needed to meet the safety objectives. Such protective strategies may include redundancy, monitoring, partitioning, development assurance rigor, built-in-test, and safety-related maintenance tasks and intervals.

The PSSA process is an iterative assessment conducted at multiple stages of system development. It is an on-going process, starting in the early phases of design with the evaluation of the system architecture to determine system-level safety requirements. System-level safety requirements are then allocated to subsystems and finally subsystem requirements are allocated to equipment/items. This safety requirements allocation to subsystems will determine hardware reliability requirements and development assurance requirements for both hardware and software (refer to ARP4754B/ED-79B). These requirements and development assurance levels are captured in applicable specifications. The PSSA assignment of IDALs to items determines the appropriate hardware and software development assurance rigor. The PSSA also generates item requirements including but not limited to safety, reliability, independence, and separation. Common cause considerations are taken into account in the PSSA process. Care should be taken to account for potential latent failures and significant latent failures and their associated exposure times.

Once safety requirements have been defined through the PSSA process and the implementing subsystems/items mature, the SSA process may be initiated.

For details in performing the PSSA, see Appendix D.

3.6 System Safety Assessment (SSA)

An SSA is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the SFHA and relevant safety requirements are satisfied. The difference between a PSSA and an SSA is that a PSSA is a process to evaluate proposed architectures and identify safety requirements; whereas the SSA is verification that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the SFHA and PSSA, and safety requirements passed from the PASA.

The SSA integrates the results of the various analyses to verify the safety of the overall system and to cover all the specific safety requirements identified in the PSSA. The SSA uses the quantitative values obtained from the reliability predictions, SEE analysis, FMEA, or FMES. The SSA ensures that all significant failure modes are considered for inclusion in the FTA. The SSA process documentation includes results of the relevant analyses and their substantiations as needed. The SSA also includes applicable common cause consideration results.

The SSA process is generally represented through succeeding levels of verification through different levels of systems, subsystems, and items. Through these upward hierarchical verification levels, the implementation is assessed against the safety requirements identified in the PSSA process.

For details in performing the SSA, see Appendix E.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

3.7 Aircraft Safety Assessment (ASA)

The ASA is a systematic, comprehensive evaluation of the complete aircraft to show that safety objectives from the AFHA/PASA and safety requirements from the PASA are satisfied. The difference between a PASA and an ASA is that a PASA is a method to evaluate proposed architectures and identify safety requirements; whereas the ASA is verification that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the AFHA and PASA.

The ASA integrates the results of the various analyses to verify the safety of the overall aircraft and systems. This aircraft safety assessment is refined and updated throughout the development process to reflect the updated design.

The ASA uses the results obtained from the PASA and SSAs and ensures assessment of interdependencies between the aircraft functions and systems. The ASA ensures that system failure modes are considered for inclusion. The ASA also includes applicable common cause consideration results.

For details in performing the ASA, see Appendix F.

3.8 Determining Depth of Analysis for Failure Conditions

Failure conditions for the aircraft/system function should be evaluated to determine how the aircraft/system will satisfy safety objectives. The depth of analysis that should be employed in the assessment of the failure conditions is typically based on the failure condition classification, and in some cases, other aircraft/system characteristics. This evaluation generally follows a course to determine what type(s) of analysis/assessment should be employed in analyzing the failure condition, e.g., design or installation appraisal, verification analysis, or qualitative and/or quantitative assessment. While the determination of the course of analysis is straightforward for most categories, additional criteria are usually required to determine the course of analysis for "Major" failure conditions. The safety analyst should consult Depth of Analysis Flow Charts and associated text in advisory material for the current guidance to be used in determining depth of analysis of failure conditions, e.g., AC 25.1309-1A, AMC 25.1309, and AC29.2C.

3.9 Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) Assignment

Safety process activities within the PASA and PSSA processes include the assignment of FDALs and IDALs which define the level of rigor of development assurance activities. These levels of rigor are used to substantiate, to an adequate level of confidence, that development errors that could contribute to failure conditions have been identified and corrected.

Appendix P provides details in performing development assurance level assignment.

3.10 Considerations of Human Error in the Safety Assessment Process

The safety assessment process described in this document assumes that flight crews, cabin crews, maintenance crews, and other individuals participating in the operation of the aircraft follow documented procedures in foreseeable operating conditions (normal, malfunction or abnormal, and emergency). Intentional or unintentional deviation from these procedures is not considered in the safety assessment process described herein.

With the exception of some aspects of the CMA and the ZSA, the safety effects of potential flight crew and maintenance errors are evaluated using different analysis techniques. Refer to the appropriate certification advisory material on human factors for accomplishing human factor safety evaluations.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

4. SAFETY ANALYSIS METHODS

The safety analysis methods addressed in this section are used to support the safety assessment processes described in Section 3.

4.1 Fault Tree Analysis/Dependence Diagram/Markov Analysis/Model-Based Safety Analysis

FTA, DD, and MA are top-down analysis techniques. These analyses proceed down through successively more detailed (i.e., lower) levels of the design. The MBSA is an analysis technique used to model the system architecture and its functional design in order to characterize system behavior when subjected to failures in order to obtain specific safety analysis results. The reader is reminded that when FTA is presented herein, the DD, MA, and/or MBSA analysis techniques may be applicable/selected depending on the circumstances and the types of data desired.

After identifying the failure conditions in the AFHA or SFHA, the FTA can be applied as part of a safety assessment to determine what single failures or combinations of failures, if any, exist at the lower levels that might cause each failure condition. The FTA basic events may get their failure rates from the FMEAs or FMESs. The FTA might also use other failure rate sources, such as a reliability prediction or SEE analysis.

For details in performing the FTA, see Appendix G. For details in performing the DD, see Appendix H. For details in performing the MA, see Appendix I. For details in performing the MBSA, see Appendix N.

4.1.1 Applications of the FTA, DD, MA, and MBSA

The completed FTA facilitates technical and management assessments and reviews because it identifies only the failure events (single failure or failure combinations) which could individually or collectively lead to the occurrence of the undesired top event. In contrast, an FMEA identifies only single failures, including some that may be of no concern.

The FTA facilitates subdivision of system-level events into lower-level events for ease of analysis.

The FTA may be used to evaluate a proposed aircraft or system architecture to identify single failures or failure combinations leading to the top event. The FTA may be used to:

a. Quantify probability of occurrence for the top event.

b. Evaluate a proposed aircraft or system architecture to establish hardware failure probability budgets or hardware failure rate budgets.

c. Evaluate a proposed aircraft or system architecture to identify Functional Failure Sets (FFS) in order to assign FDALs and IDALs during the PASA or PSSA process.

d. Assess the safety impact of an architecture or design modification in support of the PASA or PSSA.

e. Identify the need for a design modification or identify unique situations that require special attention.

f. Show compliance with qualitative or quantitative safety objectives as part of the PSSA/SSA or PASA/ASA.

g. Establish the need for maintenance tasks and intervals necessary to meet the requirements of the safety assessment. See Section 5 for discussion of maintenance tasks and intervals.

h. Establish the need for a crew procedure(s) used to mitigate failure conditions.

When conducting FTAs for the PASA/ASA or PSSA/SSA, it is beneficial to align the failure detection means allocated to the maintenance tasks and related exposure times with those used by the maintenance program for the aircraft. However, some circumstances may require the fault tree to drive the development of a new task or interval within the maintenance program to support safety requirement compliance. 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).

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

An FTA uses Boolean logic gates to show the relationship of a failure condition to the failure modes that may cause it. The two most common logic gates are the AND-gate and 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 any one or more of the inputs produce an output representing the higher-level event. See Appendix G.

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. See Appendix H.

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-free and faulty equipment and the system redundancy and monitoring. A transition from one state to another occurs at a given transition rate, which reflects equipment failure and repair rates. A system changes state due to various events such as equipment 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. See Appendix I.

An MBSA employs an analytical model called a Failure Propagation Model (FPM). The analyst uses a software application to perform an analysis of the system FPM and generate outputs such as failure sequences, minimal cut sets, or other safety-focused results. These outputs are compared to objectives and requirements by safety analysts as part of the overall safety assessment process. MBSA can be applied as a failure propagation method in performing an FMEA or CEA. See Appendix N.

4.1.1.1 Analysis for Development or Design Errors

Systems, equipment, or their items (including software or hardware) may be qualitatively included in an FTA for the sake of evaluating the contribution of development errors to the top event (failure condition). A fault tree may be used to provide adequate analytic visibility of development safety issues for systems, especially when credit is taken for the following safety attributes:

a. Systems, equipment, or items which provide fail-safe protection against potential software development or design errors elsewhere in the aircraft or system, particularly where there may be complex functions implemented in software or hardware.

b. Systems, equipment, or items which provide protection against hardware failures.

Development or design errors (whether in the system, software, or hardware) are not the same as hardware failures. Unlike hardware failures, probabilities of such errors cannot be quantified. Therefore, numerical and categorical probabilities should not be indicated for potential errors in fault trees. Any analysis of these potential errors in an FTA should be expressed in terms of development assurance to protect against errors. The analysis should be evaluated on a purely qualitative basis. A relatively simple way of modeling the potential errors in a qualitative FTA can be done to determine the FFSs in order to assign FDALs or IDALs with architectural considerations in a PASA or PSSA, as described in Appendix P.

4.1.1.2 Average Probability

When conducting a quantitative FTA, the probabilities are estimated from the failure rates and exposure times of the basic 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 wear out or infant mortality is a consideration, then equipment reliability management methods such as “life limitations” or “enhanced burn-in” can be used to attain a constant failure rate. Failing that, other distribution functions (e.g., Weibull) would need to be applied. A Monte Carlo simulation could also be used. ARP5150A provides information regarding Weibull or Monte Carlo simulations, but these applications are beyond the scope of this document.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

The 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 time and “at risk” times is contained in Appendix G.

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) and Failure Modes and Effects Summary (FMES)

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

An FMEA is coordinated to manage the specific analysis scope. The level of analysis of the FMEA can be adapted to have enough detail to allow the PSSA probability budgets to be met. The analysis may be accomplished at different levels of detail (e.g., component, function). An FMEA may be used as source data for failure rates in probabilistic analyses such as the FTA. Furthermore, an FMEA may be used to supplement the FTA by providing a complementary list of failure effects from the bottom up.

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 is coordinated with the user to adequately address the need for inputs to higher-level FMEAs and/or SSA FTAs.

For details in performing an FMEA/FMES, see Appendix J.

4.3 Cascading Effects Analysis (CEA)

A CEA is a qualitative, bottom-up analysis which evaluates an initiating condition (e.g., a failure condition, failure mode, or combination of failure modes) and allows the analyst to determine the total effect on the aircraft for that initiating condition. The CEA iteratively identifies the direct and indirect effects that propagate from the initiating condition due to system dependencies. All systems directly or indirectly connected to the systems impacted by the initiating condition are considered in the CEA.

The CEA may be used to support any analysis that requires the determination of aircraft-level or multisystem effects for specific initiating conditions. For example, the CEA may be used to determine the system or aircraft effects of an FMEA failure mode, or the aircraft effects of a resource system (e.g., hydraulic, electrical) SFHA failure condition. The effects of each initiating condition are conveyed to the source analysis.

For details in performing the CEA, see Appendix O.

4.4 Zonal Safety Analysis (ZSA)

A ZSA is performed to evaluate the design and installation of systems and equipment to identify specific interactions or hazards, and potential maintenance hazards. The ZSA considers the physical installation of and interference between systems and equipment in order to identify potential hazards caused by mutual influences between equipment co-located on the aircraft as well as the influence of the zone operating environment on such installed equipment. The ZSA is generally performed by an airframe manufacturer but may also be performed by systems integrators or installers when applicable. ZSA concepts may also be useful in helping the PASA/PSSA processes generate physical installation requirements supporting identified Independence Principles and the SSA/ASA processes verify those requirements are met.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

The ZSA is intended to identify whether there are any zonal issues that could compromise intended independence (e.g., zone overheat affecting multiple equipment). Determining an installation solution in zones of limited volume can present challenges for which an alternate design solution or hazard mitigation should be considered.

For details in performing the ZSA, see Appendix K.

4.5 Particular Risk Analysis (PRA)

Particular risks are those physical events or influences which may violate independence, or compromise aircraft safety or aircraft survivability. These risks may be internal or external to the aircraft. Particular risks may influence several aircraft zones at the same time. Some of the particular risks may be subject to specific airworthiness requirements (e.g., engine uncontained rotor failures, tire burst).

The PRA is not a probabilistic analysis but a survivability analysis. Each particular risk is analyzed as a threat to the aircraft. The objective is not to determine how often these threats occur, but to determine the survivability of the aircraft in the presence of each threat. A probabilistic analysis may be used in support of the PRA, but the use of these analyses does not obviate the need for the survivability assessment performed in the PRA. PRA concepts may also be useful in helping the PASA/PSSA processes generate physical installation requirements supporting identified Independence Principles and the SSA/ASA processes verify those requirements are met. The results of some analyses conducted as part of the PRA, such as bird strike and tread separation analyses, may also contribute to the identification of structural design requirements.

For details in performing the PRA, see Appendix L.

4.6 Common Mode Analysis (CMA)

A CMA is a qualitative analytical method used to support evaluation of independence. In a CMA, engineering experience is systematically applied to review function, architecture, development or design, implementation, manufacturing, maintenance and operation in a logical way. Considerations are given to the independence of functions and their respective monitors. Identical systems or items could be susceptible to common development errors or failures that could cause simultaneous loss of function or malfunction of duplicate systems or items.

The CMA activity is used to facilitate the generation of requirements associated with independence and the assignment of development assurance levels associated with architecture considerations as part of PASA and PSSA. The CMA also supports independence verification occurring after implementation as part of SSA and ASA.

For details in performing the CMA, see Appendix M.

5. SAFETY-RELATED MAINTENANCE TASKS AND INTERVALS

The analytical methods in this ARP may assist manufacturers in the determination of maintenance tasks and associated intervals to ensure the aircraft can operate safely in the presence of failures. Consult the applicable regulations and guidance materials for the criteria to establish the required maintenance tasks.

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

Failures detected during periodic power-up or self-test routines may have short latent exposure time period. In other cases, however, the exposure time for some latent failures may be associated with equipment bench tests or specific aircraft maintenance tasks. In these cases, the latent period can be a considerable amount of time.

5.1 Certification Maintenance Requirements

Maintenance tasks and associated time intervals used to limit exposure times of Catastrophic and Hazardous failure conditions identified in the PSSA or SSA FTAs, are Candidate Certification Maintenance Requirements (CCMRs). Where detection is accomplished by an aircraft maintenance task, the time interval required to meet the safety objective should be transferred to the appropriate maintenance process for implementation of required maintenance procedures and time intervals.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Some CCMRs associated with safety requirements compliance may be designated Certification Maintenance Requirements (CMRs). A CMR is a mandatory periodic task which is required to maintain the safety of the aircraft. CMRs are designed to verify that a certain failure has or has not occurred, particularly significant latent failures. A CMR is established during the design certification of the aircraft as an operating limitation of the type certificate. CMRs are established in accordance with applicable regulatory guidance, e.g., AC 25-19A/AMC 25-19.

Once established, CMRs are required maintenance tasks and must be accomplished by the operator at the prescribed intervals 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 procedure, in fact, detects the latent failure of concern.

5.2 Maintenance Steering Group

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. The analysis defines a group of scheduled tasks to be accomplished at specified intervals to prevent deterioration of the inherent safety and reliability levels of the aircraft. The analysis also defines a group of non-scheduled tasks to restore the aircraft to an acceptable condition. CMRs on the other hand, are failure-finding tasks only, intended to limit the exposure to significant latent failures and wear out failures. The MSG-3 process examines failure paths by using the “next failure” criteria. (e.g., what is the next worst thing that can happen in the same system, given the first failure has occurred?). Once the MSG-3 process is complete, the minimum maintenance required is established in the MRB. Once the MRB issues their report of maintenance tasks, the aircraft operators use the report to develop their own maintenance program, working with their local authorities.

Consult AC 25-19A/AMC 25-19 for guidance on how CMR and MSG-3 tasks contribute to operators’ maintenance programs.

6. MASTER MINIMUM EQUIPMENT LIST (MMEL)

Modern aircraft are designed to have high function availability. The goal is that aircraft may be safely dispatched even if some of their components are inoperative. The list of equipment so designated is called the Master Minimum Equipment List (MMEL). Availability is usually accomplished through the use of redundancy. During the design development, a list is created through evaluation of such equipment. This list is used to determine if an aircraft can be dispatched with given equipment inoperative. For conditions where dispatch is allowed, there may be restrictions placed on the operation of the aircraft during the time allowed for dispatch in this configuration. Both qualitative and quantitative approaches have been shown acceptable to substantiate the limited time period for MMEL dispatch. The limited time period allows the aircraft to reach a major maintenance facility or to reach its next scheduled maintenance check. For example, FTA may provide rationale supporting an aircraft dispatch configuration for MMEL and be used to help determine allowable exposure time. The MMEL may also be considered in the PASA or PSSA to capture safety requirements (e.g., distinct annunciations or operational or maintenance constraints) that will be needed to ensure a successful assessment of the MMEL configuration. These applications of FTAs are associated with the risk of dispatch with equipment on the MMEL, not the average risk assessed for compliance with related regulations.

Consult CS-MMEL for guidance when the qualitative approach is supplemented by a quantitative approach.

7. TIME-LIMITED DISPATCH (TLD)

This section contains a discussion of a method currently being used to define and control dispatchability requirements for Full-Authority Digital Engine Control (FADEC) systems. The discussion is included here to provide background for this concept, Time-Limited Dispatch (TLD), which may be useful in approaching design solutions for other aircraft systems. The concept is one wherein a redundant system is allowed to operate for a predetermined length of time with faults present.

The TLD concept has been applied to dual-channel engine FADEC systems with regard to the failure condition of Loss Of Thrust Control (LOTC) of a single engine. Operating with faults present results in an increased probability of an LOTC event. TLD allows airlines to take advantage of the built-in safety margin of the FADEC system, permitting them to postpone maintenance actions for specific intervals, rather than possibly incurring delays and/or cancellations if they were forced to repair the faults prior to the next flight.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

TLD operation is conditional upon the resultant system operation and reliability being adequate to satisfy the safety requirements for operational approval. The recommended process for approval of TLD operations requires an analysis to show that the fleet average probability of an LOTC event is below a target level, such as 1.0E-05 events per operating hour. The certification authorities set the target level in terms of a fleet average LOTC rate. Faults that are classified as dispatchable are generally placed in either of two classes of dispatchable faults: a class that must be repaired in a short, defined time period and a class that is allowed to operate for a longer time before repair is required. Faults that are classified as non-dispatchable require immediate repair. Excluded from the set of dispatchable faults are those faults that must be repaired immediately (i.e., non-dispatchable faults) including those which unacceptably impact the LOTC rate. A list of which faults appear in each dispatch class and the allowable dispatch times for those faults are approved by the certification authorities. The engine type certificate data sheet will state whether the engine is approved with TLD. The limitations section of the engine maintenance manual should state the approved intervals for short-term and long-term dispatch.

Guidelines for TLD analysis for electronic engine control systems are described in ARP5107C which was revised by the SAE E-36 Committee and published in September, 2018. It provides methodologies and approaches which have been used for conducting and documenting the analyses associated with the application of TLD to the thrust control reliability of FADEC systems. It includes the background of the development of TLD, the structure of TLD that was developed and implemented on present generation commercial transports, and the use of Markov Analysis and analytic calculations to determine the periods of time during which an aircraft can be dispatched with known inoperative engine control system items, and to validate the application of TLD on FADEC-equipped aircraft. Although TLD can currently only be used for FADEC systems for LOTC, ARP5107C considers its techniques and processes applicable for other FADEC system failure effects and for systems other than FADEC (e.g., thrust reverser).

8. IN-SERVICE SAFETY ASSESSMENT

The granting of Type Certification (TC) for an aircraft is the transition point between the safety assessment before TC and the in-service safety assessment after TC. Documents describing practices for in-service safety assessments are ARP5150A and ARP5151A. Operators should consult applicable regulations from certification authorities.

To facilitate the beginning of the in-service safety assessment process, the designers may wish to develop a list of “safety-significant events” that the operators could include in their operator and service manuals to monitor or that a company field service engineer could monitor. The operators should be aware of these elements, and they may wish to pass any issues regarding these elements back to the manufacturer in accordance with ARP5150A Appendix M (Hazard Tracking) and Appendix N (Lessons Learned). The manufacturer should assess reports of issues with safety significant events in the field to determine if there is a trend or if the issue requires further investigation.

9. NOTES

9.1 Contribution Acknowledgement

The leadership of the S-18 and WG63 Committees would like to thank the committee members who have actively contributed, 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, and other S-18 and WG63 committee members, development of this document would not have been possible.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

9.2 Contributors

Derek Achenbach
Shakil Ahmed
Kathryn Baksa
Steven Beland
Ahmed Butt
David Cummins
Michael Curran
John Dalton
Aharon David
Laura Dominik
Mark Eley
Sylvain Engel
Charlie Falke
Daniella Fernandes
Daniel Fogarty
Jean Gauthier
Damien Glynn
Mallory Graydon
Humberto Guimaraes
Ricardo Hachiya
Joel Harrison
Adrian Hiliuta
Lee Howard
Martin Hunter
Salvatore Infantino
Christopher Lacey
Pascal Lambert
Linh Le
Trevor Lewis
Ronald Liffrig
Jim Marko
Bob Mattern
Craig McMillan
Fred Moon
Karl Morris
Chad Moses
Isaac Munene
Laurence Mutuel
Mike Noorman
Mark Olson
Robert Olson
Ji Paik
Steven Pallotto
Michael Peterson
Warren Prasuhn
Gradimir Radovanovic
Jomar Rocha
Bradley Schafer
Douglas Sheridan
Joel Smith
Rob Soffe
Alvaro Tamayo
John Thomas
Lirong Tian
Archana Verma
Inder Verma
Komal Verma
Robert Voros
Andrew Wallington
Andy Ward
Kimberly Wasson
Steve Wilson
Franck Ybert

9.3 Revision Indicator

A change bar (|) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY SAE COMMITTEE S-18, AIRCRAFT AND SYSTEM DEVELOPMENT AND SAFETY ASSESSMENT COMMITTEE, AND EUROCAE WORKING GROUP WG-63, COMPLEX AIRCRAFT SYSTEMS

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

APPENDIX A - AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA)

NOTE: The main body of this 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.

TABLE OF CONTENTS

A.1 INTRODUCTION 31
A.1.1 AFHA Process Overview 31

A.2 GATHER AFHA INPUTS 32
A.2.1 Review and Confirm Aircraft-Level Functions are Complete 32
A.2.2 Aircraft Functions 32
A.2.3 Aircraft Sub-Functions 33

A.3 IDENTIFY AIRCRAFT FAILURE CONDITIONS 34
A.3.1 Combined Failure Conditions 36

A.4 ASSESS AIRCRAFT FAILURE CONDITION EFFECTS 36

A.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY 40

A.6 AFHA ASSUMPTIONS 41

A.7 AFHA OUTPUTS 41

A.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS 43
A.8.1 Crew Awareness 44
A.8.2 Flight Phases and Associated Operational Conditions 44
A.8.3 Operational Events 45
A.8.4 Environmental Conditions 45
A.8.5 Environmental Events 46

A.9 AFHA SUBSTANTIATION 46
A.9.1 AFHA Completeness 47
A.9.2 Failure Condition Effect Correctness 47
A.9.3 Failure Condition Classification Correctness 48

Figure A1 AFHA activities 32

Table A1 Example of aircraft functions 33
Table A2 Example of aircraft function decomposition 33
Table A3 Aircraft-level failure condition identification matrix example 35
Table A4 Frequently used effect term examples 37
Table A5 Aircraft-level failure condition effects matrix example 39
Table A6 Failure condition severity classification examples 40
Table A7 AFHA format example 42
Table A8 AFHA format example data definitions 43

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

A.1 INTRODUCTION

The Aircraft Functional Hazard Assessment (AFHA) is a process that allows the identification and evaluation of potential hazards related to an aircraft regardless of the details of its design or implementation. It is performed early in the development process, re-evaluated anytime significant changes are made to aircraft functionality, and is used to establish the safety objectives for the functions of the aircraft to achieve a safe design.

When performing the AFHA, failure conditions are analyzed for their effect on the aircraft, crew and occupants to determine the associated severity classification. Flight phase, environmental and operational conditions should be considered in the assessment.

Top-level aircraft functions are typically decomposed to lower-level aircraft functions. This allows the analyst to determine if the functions and failure conditions under consideration are correct and complete for the chosen level of detail, and if the top-level function statement requires clarification. The level of detail resulting from this functional decomposition may vary between applications.

An AFHA does not consider the allocation of aircraft functions to systems. The AFHA may require change if the list of aircraft functions and failure conditions is found to be incomplete or incorrect, or if assumptions are found to be incorrect during the development process. The AFHA typically does not change as a result of system design. The effects of function allocation or design changes will likely be contained in a PASA or lower-level analysis.

A.1.1 AFHA Process Overview

The AFHA process is a top-down method for identifying failure conditions and assessing the severity of failure condition effects as shown in Figure A1.

The assessment process consists of the following activities:

a. Gather AFHA inputs.

b. Review and confirm the aircraft-level functions are complete.

c. Determine the failure conditions associated with the aircraft functions.

d. Determine the effects of each failure condition considering flight phases, operational and environmental conditions and events, and crew awareness.

e. Assess and classify the severity of each failure condition’s effects.

f. Capture and confirm AFHA assumptions.

For reuse of an existing and well vetted AFHA on a new or modified aircraft, aircraft functions and failure conditions should be re-examined to ensure the new application is similar in function, operation, and environment to the previous application.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

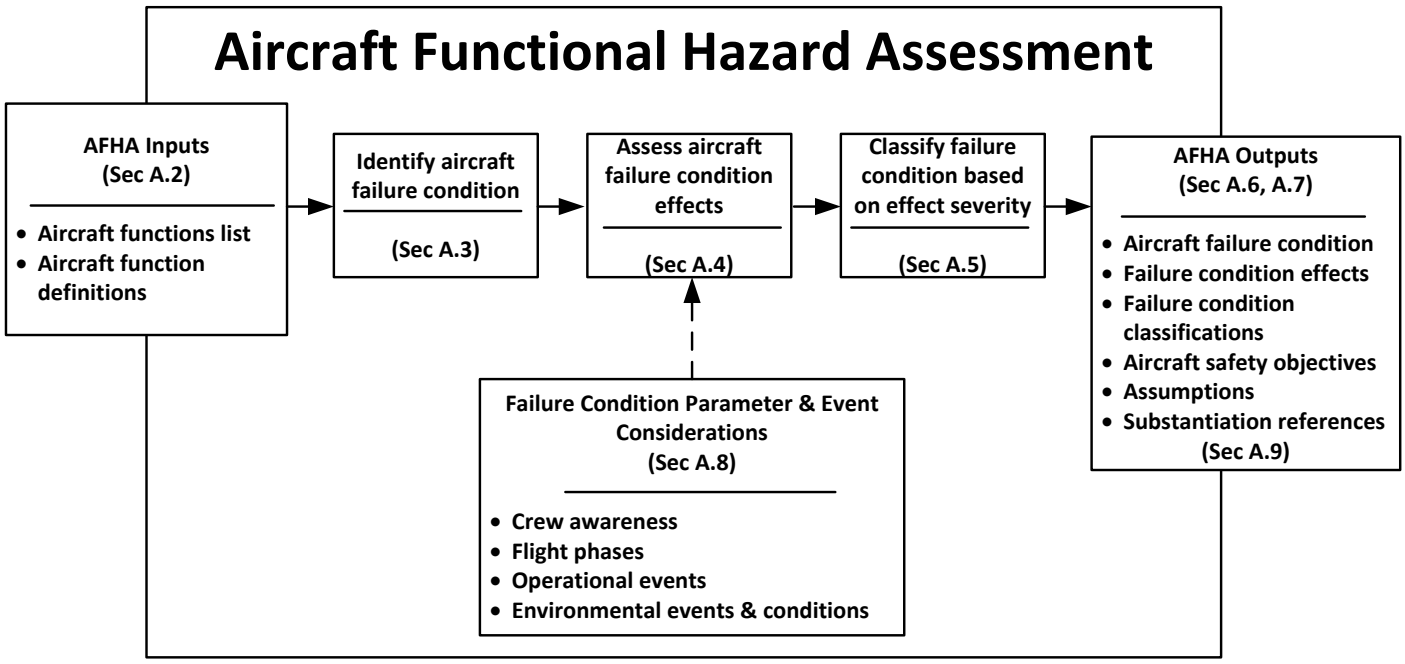


Figure A1 - AFHA activities

A.2 GATHER AFHA INPUTS

The inputs to the AFHA are the aircraft-level functions, derived from the aircraft design objectives and the fundamental necessities of flight due to the laws of physics, and the operational and environmental conditions the aircraft is designed to encounter.

A.2.1 Review and Confirm Aircraft-Level Functions are Complete

The AFHA does not define aircraft functions; however, it requires a clear, explicit, and complete list of aircraft functions as an input.

For the AFHA, the aircraft functions should be described in terms of what the function is to accomplish, rather than the means envisioned to implement the function. For example, at the aircraft level it is recognized that a means of propulsion is required for sustained flight. This function could be described as “to provide thrust,” as this describes the objective and not the means to accomplish it.

The completeness of the function list is essential to AFHA. A complete list of functions includes all those functions necessary for the operation of the aircraft. There should be consistency between the functions analyzed in the AFHA and the aircraft functional requirements.

A.2.2 Aircraft Functions

Aircraft functions are broadly stated and intended to be inclusive of all possible implementations, as no functional decomposition or design decisions have yet been considered. The list of aircraft functions used as an input to the AFHA should include all functions performed by the aircraft as a whole. Table A1 provides an example set of aircraft functions for a passenger aircraft.

The aircraft functions are generally common to all aircraft designed to perform similar missions and are defined by the development process.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Table A1 - Example of aircraft functions

ID #	Function
1.	Provide aerodynamic performance
2.	Control aircraft trajectory
3.	Control aircraft energy
4.	Provide survivable environment
5.	Provide crew situational awareness
6.	Maintain structural integrity
7.	Provide emergency services
8.	Provide passenger services

A.2.3 Aircraft Sub-Functions

The aircraft functions may contain a breakdown into sub-functions, resulting in a hierarchical structure with two or more levels. Failure conditions are derived from the lowest level of the function decomposition and generally do not depend on system allocation or architecture. Functional decomposition does not imply a particular allocation of functions to systems, but allows more specific failure conditions to be derived and assessed in the AFHA. Functional decomposition may require extracting more detail from the referenced aircraft requirements or making assumptions regarding aircraft functionality which are not yet defined in the requirements. Any such functional assumptions should be documented and subsequently confirmed.

While the level of detail and the number of hierarchical levels of functional decomposition are left to the developer and analyst's discretion, descending to a level of detail that is dependent on system-level design is not recommended. An example of function decomposition is shown in Table A2.

Table A2 - Example of aircraft function decomposition

ID #	Function
1	Provide aerodynamic performance
1.1	Provide lift
1.1.1	Provide lift (no further decomposition at the aircraft level)
2	Control aircraft trajectory
2.1	Provide pitch stability and control
2.1.1	Provide pitch control
2.1.2	Provide pitch stability
…	(additional sub-functions omitted)
3	Control aircraft energy
3.1	Maintain or increase aircraft energy
3.1.1	Provide thrust
3.1.2	Reduce drag
3.2	Reduce aircraft energy
3.2.1	Provide controlled aerodynamic drag
3.2.2	Provide high lift capability
3.2.3	Provide deceleration on ground
4	Provide survivable environment
4.1	Provide breathable atmosphere
4.1.1	Provide oxygenated atmosphere
4.1.2	Prevent atmosphere toxicity
4.2	Provide survivable temperature
4.2.1	Provide cabin temperature control
…	(additional functions and sub-functions omitted)

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

A.3 IDENTIFY AIRCRAFT FAILURE CONDITIONS

A failure condition is described by a statement that characterizes an abnormal state of a function. Failure conditions describe a failed state of the aircraft function including the amount and type of impairment. Knowledge of each function is necessary to properly define failure conditions which are correct in the context of the aircraft function, operation, and environment.

Failure conditions vary in detail with the level of function from which they are derived, from extremely broad descriptions for aircraft-level functions, such as “total loss of thrust” to very specific cases at the system-level function evaluation, such as “loss of altitude indication barometric correction.” Function decomposition to lower levels will lead to more detailed failure conditions which may be more appropriate for evaluation at the system level. Note that a failure condition is not the same as a failure mode, which describes how a particular device fails (e.g., open circuit resistor, valve jammed closed, fractured mechanical piece-part).

Failure conditions can be broadly categorized as the loss of a function or as a malfunction. Each function should be assessed and the potential for loss of the function and malfunction considered. In general, each aircraft function will have at least one loss of function and one malfunction of interest.

NOTE: The dictionary definition of malfunction includes loss of function. However, loss of function is separated here to conform to certification advisory material.

Loss of function may be total or partial. Total loss of function is a condition where the function cannot be performed by any means. Partial losses of function are conditions where the function can still be performed but only at reduced capability (e.g., reduced effectiveness or with increased difficulty). Examples of loss of function failure conditions may include:

a. Loss of oxygenated atmosphere for crew and passengers.

b. Loss of directional control of the aircraft on ground.

Malfunction is a condition where the operation of a function is different than intended excluding function loss. The aspect of the function which is incorrectly performed is described in the failure condition (e.g., erroneous, uncommanded action, misleading). Examples of malfunction failure conditions may include:

a. Uncommanded flight path pitch deviation.

b. Uncommanded release of oxygen masks for passengers.

c. Erroneous directional control of the aircraft on ground.

Failure conditions may have vastly different effects depending on whether the crew are notified and are able to perform timely mitigating actions. Where crew reaction is relevant and the effects of the failure condition are not intrinsically evident to the crew, separate failure conditions may be created considering whether the crew is aware or unaware of the condition. Examples of failure conditions considering crew awareness may include:

a. Loss of oxygenated atmosphere for crew and passengers with crew awareness.

b. Loss of oxygenated atmosphere for crew and passengers without crew awareness.

c. Loss of stall prevention functions with crew awareness.

d. Loss of stall prevention functions without crew awareness.

e. Loss of wing ice prevention with crew awareness.

f. Loss of wing ice prevention without crew awareness.

A failure condition identification matrix may be used to assist the analyst in considering all types of failure conditions for every function. This is one method of summarizing failure condition identification; other methods may be equally effective. Not all functions will have relevant failure conditions of all types.

AVA Documents Document Sharing Hub

Full document details: SAE ARP4761A

Table A3 illustrates a failure condition identification matrix for the aircraft level. Additional aircraft functions are added as additional rows. Additional types of failure conditions (such as distinct failure conditions with and without crew awareness) may be added as additional columns. These examples are not a full assessment and do not represent the only way to perform failure condition identification; they illustrate a useful method when performing an AFHA.

Failure conditions in the AFHA are broadly stated in order to provide a scope which encompasses all detailed failure scenarios that can lead to the top-level functional effect. Failure conditions should be derived from the list of aircraft-level functions.

If the functional decomposition is performed in such a way that the sub-functions identified are not related, failure conditions combining failures of multiple sub-functions may not be necessary. If the sub-functions are related, failure conditions combining failures of multiple related sub-functions should be identified. Functional dependency should be evaluated for all functions from which failure conditions are derived.

Table A3 - Aircraft-level failure condition identification matrix example

ID #	Aircraft Function	Total Loss	Partial Loss	Malfunction
3	Control aircraft energy			
3.1	Maintain or increase aircraft energy			
3.1.1	Provide thrust	3.1.1.T1 Insufficient thrust to maintain positive climb rate	3.1.1.P2 Insufficient thrust to meet required climb gradient	3.1.1.M1 Uncommanded high thrust
3.2	Reduce aircraft energy			
3.2.1	Provide controlled aerodynamic drag	3.2.1.T1 Total loss of controlled aerodynamic drag	3.2.1.P2 Reduced controlled aerodynamic drag	3.2.1.M1 Uncommanded aerodynamic drag device deployment
3.2.2	Provide high lift capability	3.2.2.T1 Total loss of high lift capability	3.2.2.P2 Reduced high lift capability	3.2.2.M1 Erroneous high lift device position without crew awareness 3.2.2.M2 Erroneous high lift device position with crew awareness
3.2.3	Provide deceleration on ground	3.2.3.T1 Total loss of deceleration on ground	3.2.3.P2 Reduced deceleration on ground capability	3.2.3.M1 Uncommanded deceleration on ground
4	Provide survivable environment			
4.1	Provide breathable atmosphere			
4.1.1	Provide oxygenated atmosphere	4.1.1.T1 Total loss of oxygenated air to crew and passengers	4.1.1.P2 Loss of oxygenated air to passengers only	None identified at the aircraft level
4.1.2	Prevent atmosphere toxicity	4.1.2.T1 Toxic atmosphere in flight deck or cabin	None identified at the aircraft level	None identified at the aircraft level
4.2	Provide survivable temperature and humidity			
4.2.1	Provide cabin temperature control	4.2.1.T1 Total loss of cabin temperature control	4.2.1.P2 Reduced cabin heating capability 4.2.1.P3 Reduced cabin cooling capability	4.2.1.M1 Cabin overheating 4.2.1.M2 Cabin excessive cooling

AVA Documents
Document Sharing Hub
Full document details: SAE ARP4761A

A.3.1 Combined Failure Conditions

If the function list developed for the assessment includes related functions, the AFHA should consider combined failures of the related functions. Functions are related when they are used together or alternatively to accomplish a higher-level function. Functions are not related when they do not contribute to or affect any higher-level functions in common (other than due to crew workload or incapacitation).

Examples of related functions that would require combined failure conditions may include:

a. Navigation and communication (external communication is used as a means to accomplish navigation tasks).

b. Pressurization and supplemental crew oxygen provision (both are means to maintain crew oxygenation).

c. Pressurization and flight control function—speed brakes (both are means to prevent extended exposure to high cabin altitude).

d. Ground directional control by friction, aerodynamic force, or asymmetric thrust (all are means of directional control on ground).

As an example, if a functional breakdown of the “provide situational awareness” function from Table A1 identifies “provide navigation capability” and “provide communication capability” as separate aircraft functions, the combined failure condition “total loss of navigation and communication” should be identified. Alternatively, if the functional breakdown for the “provide situational awareness” function identifies “determine own position,” “determine heading,” and “collision avoidance” as sub-functions, only the individual failure conditions would be necessary, as these sub-functions are not related (each of them is independently necessary to accomplish the top-level aircraft function). In this case, the various contributors to each failure condition (including the combined loss of navigation and communication systems) would be identified in the PASA (see Appendix B).

A.4 ASSESS AIRCRAFT FAILURE CONDITION EFFECTS

The AFHA next examines each failure condition and determines the effects on the aircraft, crew, and occupants should the failure condition occur in each flight phase. The assessment of the effects begins with a narrative description of the consequences of the failure condition followed by a statement summarizing the failure condition’s overall impact. Comparison of the effects with the description of the hazard classifications in the applicable certification advisory material will aid in the failure condition classification process.

Flight phases are distinct time periods within an average flight duration; see A.8.2 for further detail. Failure condition effects may vary depending upon the flight phase at the time of failure condition occurrence. The failure condition effects may also be affected by operating or environmental conditions. The failure condition effects assessment considers the most severe plausible effects during each flight phase or condition. Separate failure conditions may be needed to capture a range of effects.

The effects of a failure condition for any particular flight phase are all the expected effects during the flight when the failure condition occurs in that flight phase. This includes immediate effects and effects that would occur during subsequent flight phases due to the same failure condition. For example, the effects of a “loss of ground deceleration” failure condition during the cruise flight phase include the fact that ground deceleration will be unavailable for the subsequent landing.

The effects are described by a narrative and characterized with brief statements regarding the effect in aircraft, crew and occupant categories. Not all failure conditions may have effects in all categories or the effects of a failure condition in each category may not have the same severity.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

a. “Effect on Aircraft” refers to the ability of the aircraft to perform its functions and to the aircraft’s structural integrity. Aircraft effects are characterized by a statement evaluating the reduction in aircraft capability and safety margin caused by the failure condition.

b. “Effect on Flight Crew” refers to any direct physiological effect on flight deck crewmembers or to any increase in physical or mental activity required beyond the normal flight crew activity levels to counteract the effects of the failure and complete the flight safely. Typically, this includes the crew’s means of detecting the failure condition (if any) and their expected actions. Effects on crew are characterized by a statement evaluating the adverse physiological effects on the crew (if any) and the increase in crew workload caused by the failure condition (if any).

c. “Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)” refers to cabin crew or passenger discomfort, injury or fatalities. These effects may be the direct result of the failure condition, such as high G maneuvering or abnormal environmental conditions, or an indirect effect, such as loss of life due to loss of aircraft control resulting in an uncontrolled crash. Occupant effects are characterized by a statement evaluating the adverse physiological effects on the cabin crew or passengers caused by the failure condition.

Each of the failure condition’s effects is qualitatively expressed. Usage of standard assessment terms facilitates consistency between failure condition descriptions.

The qualitative effects assessments should consistently evaluate the same effects across all failure conditions. For example, the summary statement for effects resulting in a delayed rotation at takeoff should be consistent across different failure conditions, whether the delayed rotation is caused by a reduction in available thrust, by an inadequate control surface configuration, or by any other cause.

Table A4 provides an example of frequently used assessment terms to summarize failure condition effects. Table A4 is based on certification guidance material applicable to transport category aircraft. A set of standard effect assessment terms should be obtained from the appropriate current guidance material.

Table A4 - Frequently used effect term examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or crew fatalities	Multiple occupant fatalities
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort
No effect on aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology

A matrix or table may be used to capture the evaluation of each failure condition, applicable flight phases, failure effects descriptions, and relevant environmental or operational conditions. The specific evaluation format for describing the effects is not critical, provided it is thorough.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Table A5 illustrates a possible failure condition effects capture matrix for one aircraft-level failure condition. Similar tables would be constructed for each failure condition identified. The effects described in this example are illustrative; actual effects vary with each aircraft design.

In this method, one failure condition effects matrix is constructed for each failure condition. Additional depth can be added to the matrix by adding detail to the flight phases, such as separating “takeoff” into “takeoff below V1” and “takeoff above V1,” by adding specialized flight phases such as ETOPS cruise or CAT 2 approach, or by adding operational or environmental events to the failure condition. These are described further in Section A.8.

Initial assessment of the failure conditions should address the basic flight phases (taxi, takeoff, climb, cruise, descent, approach, and landing).

Assumptions may need to be established in order to predict some failure condition effects. Any such assumptions should be documented and subsequently confirmed.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Table A5 - Aircraft-level failure condition effects matrix example

Function: 3 Control Aircraft Energy / 3.2 Reduce Aircraft Energy / 3.2.2 Provide High Lift Capability			
Failure Condition: 3.2.2.M1 Erroneous High Lift Device Position Without Crew Awareness			
Flight Phase	**Effect on Aircraft**	**Effect on Flight Crew**	**Effect on Occupants**
Taxi Takeoff	The affected high lift device may be at a position such that the maximum angle of attack and lift achievable are less than the expected values for the commanded configuration. No warning or indication is presented to the crew. Complete loss of angle of attack safety margin and lift capability is possible.	The crew will be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. The crew will proceed with a normal takeoff; however, liftoff may not be possible at the expected rotation speed. No effective crew action to prevent a high-speed runway overrun.	Multiple occupant fatalities or severe injuries are possible.
Climb	The affected high lift device may fail to reach a fully stowed configuration. No warning or indication is presented to the crew. Complete loss of structural margins is possible if the device remains deployed at cruise speed.	The crew may be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. Identification of the condition due to reduced aircraft acceleration and increased noise is possible, but would require significant crew experience. Crew action to maintain control of the aircraft is not effective should structural failure of the high lift device occur.	Multiple occupant fatalities or severe injuries are possible.
Cruise	Erroneous high lift position will be detected by crew due to aircraft effects. See Erroneous high lift positioning failure condition.		
Descent	Erroneous high lift position will be detected by crew due to aircraft effects. See Erroneous high lift positioning failure condition.		
Approach	The affected high lift device may be at a position such that the maximum angle of attack and lift achievable are less than the expected values for the commanded configuration. No warning or indication is presented to the crew. Complete loss of angle of attack safety margin and lift capability is possible.	The crew will be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. The crew will proceed with a normal approach; however, lift capability may be insufficient at the expected reference speed. Stall recovery may not be possible at low altitude.	Multiple occupant fatalities or severe injuries are possible.
Landing	The affected high lift device fails to return to the stowed position for ground operation. No warning or indication is presented to the crew. No effect on functional capabilities for ground operation or safety margins.	The crew will be unaware of the condition until the external visual inspection preceding the subsequent flight. Crew will note the incorrect high lift device position during preflight walk around and note the equipment for maintenance action prior to dispatch.	No effect.

AVA Documents Document Sharing Hub

Full document details: SAE ARP4761A

A.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY

When the identification and summary of all failure condition effects is complete, the failure condition classification activity can begin. A classification is established for each flight phase by assessing the effects on aircraft, crew and occupants. The most severe of these effects drives the failure condition classification in each flight phase. An overall failure condition severity classification may be determined by selecting the worst-case classification from the applicable flight phases.

It is important to avoid assuming a severity classification during the identification of failure effects, as the assessment process can be incomplete if there is excessive focus on preconceived outcomes for common failure conditions.

The statements of effects from Section A.4 are used to determine the classification of each failure condition by comparison to the appropriate regulatory guidance. Table A6 provides an example of such a reference, based on certification guidance material for transport category aircraft. The classifications are: Catastrophic, Hazardous, Major, Minor, and No Safety Effect. Determination of the severity classification is direct if the qualitative assessment of the effects is consistently performed and the summaries clearly stated.

Table A6 - Failure condition severity classification examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew Excluding Flight Crew)	Classification
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or Crew fatalities	Multiple occupant fatalities	Catastrophic
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew	Hazardous
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries	Major
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort	Minor
No effect or aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology	No Safety Effect

For many functions, published certification guidance material can be used as a reference for the qualitative categorization of failure effects and severity classification. This guidance may include a brief statement describing the failure condition and applying a severity classification directly, or may describe certain types of effects which are considered unsafe conditions. This data can be used as reference points to classify similar failure conditions.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

A.6 AFHA ASSUMPTIONS

There are instances where details necessary to perform the AFHA are not yet available. In these cases, the safety analyst should make assumptions regarding operating or environmental conditions, airframe capabilities or other factors. Assumptions may be made for as-yet-unspecified development information. These are inputs to the AFHA process which are necessary, but were not yet available in the functional information provided to the AFHA process.

Any consideration made during the assessment that was not based on validated functional information should be documented as an assumption. Depending on the maturity of the aircraft definition at the time of the AFHA, the number of assumptions in an aircraft-level assessment may be significant or almost nonexistent.

Assumptions should be captured and formally communicated to the appropriate development information sources. The assumption may then be confirmed, or corrected based on new development information. In the latter case, a design change or a revision of the AFHA may be required.

Any assumptions made in the AFHA evaluation will be tracked as part of the development program activities.

A.7 AFHA OUTPUTS

The output of the AFHA process should include:

a. The list of aircraft-level functions and functional decomposition used as an input to the assessment including supporting discussions needed to aid the understanding of the function scope and purpose and the relationship between top-level functions and lower-level functions.

b. The detailed AFHA worksheet containing all the identified failure conditions, their effects during each flight phase, and their resulting severity classifications (which define the applicable safety objectives).

c. The list of assumptions used in identifying functions, performing the function decomposition, identifying failure conditions, determining failure condition effects or determining severity classifications.

d. The list of substantiation references used to determine failure conditions and effects are correct and complete.

Table A7 provides an example of a detailed AFHA results worksheet. Table A8 provides the definition description of the data field entries in the Table A7 AFHA example worksheet.

The AFHA is not expected to significantly change as the development process proceeds since the aircraft-level functions and decomposition do not depend on system architecture. Only assumptions found to be incorrect, changes to basic airframe definitions or high-level operating parameters have the potential to invoke a revision of the AFHA.

AFHA results are an input to the PASA. If the PASA identifies deficiencies in the analysis, or design deficiencies that cause aircraft functional information to be changed, this may result in an iteration of the AFHA.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Table A7 - AFHA format example

1	2	3	4	5	6
ID #	**Failure Condition**	**Flight Phase**	**Effects of Failure Condition on Aircraft, Crew, Occupants**	**Severity Classification**	**Assumptions, Comments, Rationale or Reference to Supporting Material**
Aircraft Function: (4) Provide Survivable Environment			Sub-Function: (4.1) Provide breathable atmosphere		
Sub-Function: (4.1.1) Provide oxygenated atmosphere					
4.1.1.T1	Unannunciated total loss of oxygenated air to crew or passengers	Climb Cruise Descent	Aircraft: No effect. Crew: Unaware or unable to counter the effects of the condition, the crew may be incapacitated by hypoxia or unable to restore sufficient levels of oxygen to the occupants in time to prevent permanent physiological harm. Occupants: Multiple occupant fatalities or severe injuries are possible due to the direct effects of hypoxia or due to crew incapacitation and subsequent loss of aircraft control.	Catastrophic	14CFR/CS 25.841(a)(2)(ii) “Pressurized Cabins” 14CFR /CS 25.1441(d) “Oxygen equipment and supply” 14CFR /CS 25.1443(c)(2) “Minimum mass flow of supplemented oxygen” AC 25-20 (6)(e)&(7) “Pressurized Ventilation and Oxygen System Assessment for Subsonic Flight Including High Altitude Operations” EASA Certification Review Item “Airworthiness Standards for Subsonic Transport Aeroplanes to be operated above 41,000 ft.”

AVA Documents Document Sharing Hub

Full document details: SAE ARP4761A

Table A8 - AFHA format example data definitions

Column	Table Entry	Entry Definition
--	Aircraft Function Sub Function	The hierarchy of the aircraft function and sub-functions being analyzed. The number of levels in the aircraft-level functional decomposition is at the analyst's discretion; however, the decomposition of aircraft-level functions should not presume a particular allocation of functions to systems. See Section A.2.
1	ID No.	Unique numbering system for organization, tracking, and traceability.
2	Failure Condition	Description of the failure or impairment of the function. See Section A.3.
3	Flight Phase	List the applicable aircraft operational phases for this failure condition. See Section A.4.
4	Effect of Failure Condition on Aircraft, Crew, Occupants	Description of the failure condition effects on the aircraft, crew and occupants. Sufficient detail should be provided to understand the failure scenario and conclude the severity classification based on the captured effects. Separate effects statements and classifications may be provided for each flight phase or a generalized effect and worst-case classification provided for the failure condition in all flight phases or for groups of flight phases. See Section A.4.
5	Severity Classification	Catastrophic, Hazardous, Major, Minor, or No Safety Effect as defined in applicable certification guidance material. See Section A.5.
6	Assumptions, Comments, Rationale, or Reference to Supporting Material	Data supporting the determination of effects and classification of the failure condition, including any applicable guideline material. See Sections A.6 and A.9.

A.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS

The effects of each failure condition are determined by constructing a scenario narrating its expected outcome. The failure effect scenario description includes immediate effects due to the failure condition and subsequent resulting effects due to the same failure condition. The failure effect scenario may also include events occurring concurrently with the failure condition under evaluation. This scenario includes the parameters at the moment the failure occurs. The events may intensify or mitigate the effects of the failure condition, or affect the crew's ability to recognize and correctly react to the failure condition situation.

In this context the term "parameter" is used for factors that are always present and vary in quantity or intensity (e.g., aircraft weight, aircraft speed) and for factors that may be present or absent but are commonly encountered (e.g., clouds obscuring vision, icing conditions). The term "event" is used for factors that occur at a distinct time and place and that are not regularly encountered (e.g., windshear).

Evaluating the influence of parameters and events on the failure conditions is part of the AFHA process. These factors should be carefully considered as they may be significant in some instances and irrelevant in others. For example, a wet runway is a significant factor when evaluating failure conditions associated with friction-based deceleration features, but is not significant when evaluating failure conditions related to environmental control of the cabin. Failure condition effects should consider that the failure condition can occur at any moment and under any condition encountered in the operating envelope of the aircraft. The failure condition effects should account for the failure effects over the range of the operating envelope and the analyst may separate the failure effects if they differ across the envelope.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

Evaluating failure effects for each flight phase as described in Section A.4 provides a structure that facilitates addressing the influence of the various operational and environmental factors where appropriate. Generally, each flight phase will provide an expected value or a range of values for most operating conditions (e.g., the flight phase “landing” limits aircraft weight and speed to values expected during that part of the flight).

The intended operating limits of the aircraft define the boundaries for many of these factors. For example, an aircraft intended to operate at altitudes above 25000 feet will consider the effects of high altitude exposure when evaluating the effects of related failure conditions during the climb, cruise, and descent flight phases. These factors should include consideration at their most severe limit within the approved flight envelope.

Sections A.8.1 through A.8.5 provide a method to address operational and environmental parameters and events; however, other methods may be equally effective.

A.8.1 Crew Awareness

Whenever the failure effect is significantly affected by crew action, separate failure conditions should be created and assessed, which consider the crew being either aware or unaware of the failure condition.

For failure conditions with crew awareness (i.e., which have an associated alert or are evident), the description of effects on the crew should capture how the crew becomes aware of the failure condition, how the crew is assumed to act in response to it, and the result of the expected crew action.

For failure conditions without crew awareness (i.e., which neither have an associated alert nor are evident), it should be assumed that the crew will continue to perform their duties normally, which may affect the severity of the failure condition effects. (i.e., crew will not take any action regarding the failure condition).

A.8.2 Flight Phases and Associated Operational Conditions

The flight profiles the aircraft is expected to perform should be determined. Certain aircraft perform only or mostly one type of flight profile (e.g., airliners perform transport flight profile), while others may perform several distinct types of flight profiles (e.g., some rotorcraft may perform transport, search and rescue, and other types of profiles). Based on the expected flight profiles, a list of flight phases should be determined. A flight phase is a distinct period within a flight, generally associated to the tasks being accomplished by the aircraft and its flight crew. As a minimum for a transport category flight profile, taxi, takeoff, climb, cruise, descent, approach, and landing should be considered.

The identified set of normal flight (and ground operation) phases should be applied through the entire assessment. A more detailed breakdown of the flight phases may be used where relevant distinctions in failure effects exist within the basic flight phases. Since failures can occur at any time, all normal flight phases should be considered for all failure conditions to ensure completeness.

Operational conditions, such as aircraft weight, speed, and altitude, may be directly related to the various phases of flight. For each flight phase, operational conditions should be considered throughout the approved flight envelope.

Specialized flight phases may also be considered. In general, a specialized flight phase should be considered when all of the following are true:

a. The specialized flight phase is deliberately initiated.

b. The specialized flight phase persists for a measurable duration.

c. The duration of the specialized flight phase can be determined as a fraction of a mission profile.

d. A particular aircraft can be expected to experience the specialized flight phase multiple times during its service life.

Specialized flight phases should be systematically considered when evaluating all functions, though when the effects of a failure condition are not affected by the specialized flight phase, it can be considered not applicable. Some examples of specialized flight phases include go-around, holding, and steep approach.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

A.8.3 Operational Events

Distinct occurrences and flight operations which are only performed as a response to specific occurrences or failures may be considered operational events. In general, an occurrence or flight operation should be assessed as an operational event when all of the following are true:

a. The occurrence or flight operation occurs at a distinct time.

b. The occurrences or flight operations have a known statistical probability, fleet wide, or industry wide rate of occurrence.

c. A particular aircraft is not expected to frequently experience the occurrence or flight operation during its service life, or may not experience it at all.

These operational events should be systematically considered when evaluating all functions, though they should only be applied to relevant failure conditions. Some examples of occurrences and flight operations that can be considered operational events include Rejected Takeoff (RTO) and in-flight diversion.

Operational events should be added to the relevant failure condition statements, creating new combined failure conditions. When considering the combination, it is important to ensure that the operational event is independent from the original failure condition. Examples of combined failure statements at the aircraft level are:

a. Loss of deceleration capability and RTO.

b. Erroneous fuel quantity indication and in-flight diversion.

Where operational events affect the severity of the failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and operational event) added to the AFHA. The combined failure condition should be assessed for all identified flight phases where the operational event can occur.

A.8.4 Environmental Conditions

Worst-case environmental conditions within the approved aircraft operating envelope should be considered to be present where relevant when evaluating the effects of failure conditions. These conditions are implicitly assumed and need not be specifically stated for every failure condition, though their influence should be described in the failure effects narrative when relevant. Examples of environmental conditions to be considered are:

a. Airfield temperature and altitude within the approved operating limits.

b. In-flight temperature and altitude within the approved operating limits.

c. Night time and clouds obscuring external vision, for aircraft approved for Instrument Flight Rules (IFR) operation.

d. Icing conditions, for aircraft approved for flight in known icing conditions.

e. Gusting and turbulence.

In some cases, the approved envelope for an environmental condition includes extremes that are infrequent. In these cases, it may be acceptable to define a range of normally encountered conditions, with conditions outside this range considered to be environmental extremes. Examples of potential environmental extremes include:

a. Cross winds at design limits.

b. High or low external temperature at design limits.

c. Gusts and turbulence at design limits.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

It may be acceptable to add the environmental extreme explicitly to the failure condition. Where environmental extremes affect the severity of the failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and environmental extreme) added to the AFHA. Examples of failure conditions incorporating environmental extremes are:

a. Loss of yaw control and cross wind at limit conditions.

b. Loss of load alleviation functions and wind gust at limit conditions.

The combined failure condition should be assessed for all identified flight phases.

A.8.5 Environmental Events

Certain abnormal environmental occurrences may be considered environmental events. Examples of environmental events include:

a. Wind shear or microburst.

b. Iced runway.

c. Icing conditions, for aircraft not approved for flight in known icing conditions.

When an environmental event affects the severity of a failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and environmental event) added to the AFHA. The combined failure condition should be assessed for all applicable flight phases.

A.9 AFHA SUBSTANTIATION

Substantiating data for the AFHA should be collected, showing that:

a. All the aircraft-level functions have been considered.

b. All failure conditions have been identified for each aircraft function.

c. The failure effects on the aircraft, crew and occupants are complete and correct for each failure condition occurring during each flight phase.

d. The correct failure classification has been selected based on the failure effects.

e. The assumptions used to develop the assessment are confirmed and evidence is provided. In cases where an assumption is incorrect, the correct information should be provided and the AFHA updated.

Substantiation of the completeness and correctness of the AFHA requires documentation of the rationale and assumptions for all failure effects and classifications.

For those failure conditions with effects that are not clearly predictable or demonstrably similar to previous applications, additional supporting information, such as simulation results, analytical studies, laboratory test results, flight test results, or field data may be necessary to substantiate the effects and classification. This information may be available in existing documentation or may have to be obtained from dedicated activities.

While comparison with previous experience may be sufficient rationale for typical failure effects and classifications, if a project integrates functions in new or novel ways, the assessment of effects may require more extensive examination.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

The failure condition identification matrix and failure condition effects matrix tools provide a guide for the assessment process. After initial assessments, the failure condition effects matrix may be expanded to include specialized flight phases, crew awareness, and environmental or operational conditions as previously described. These additional considerations may generate additional flight phases or new failure conditions combining failures with operational or environmental events. The rationale for the application of these factors to failure conditions should be recorded.

Documentation of supporting materials (e.g., analyses, studies, tests) used in determining the effects and classification of failure conditions should be preserved to substantiate the AFHA. When reusing AFHA content or substantiating by similarity, any applicable lessons learned acquired since the previous application should be incorporated.

A.9.1 AFHA Completeness

A multi-disciplinary engineering review is recommended to ensure that the AFHA has addressed all failure conditions and their effects. Reviewers should be able to find evidence within the AFHA documentation that:

a. All aircraft-level functions have been considered.

b. All failure conditions have been identified for each lower-level aircraft function in the aircraft function decomposition, including loss of the function and malfunction.

c. Where lower-level aircraft functions are related, all combined failure conditions which lead to the loss or malfunction of a higher-level aircraft function have been identified.

d. The effects of each failure condition have been determined for its occurrence during all flight phases, including any applicable specialized flight phases.

e. The influence of operating conditions, operational events, environmental conditions, and environmental events have been considered where appropriate.

f. All assumptions have been captured and confirmed.

AFHAs performed for previous aircraft of similar design and function may be reused, though effects and classifications should be confirmed to be applicable to the new design. Any gaps identified in previous analyses or other applicable lessons learned should be addressed.

A.9.2 Failure Condition Effect Correctness

There are multiple means to substantiate that the effects of each failure condition during each flight phase are correct. Different methods may be appropriate depending on the type of failure condition and the difficulty of assessing its consequences.

One or more of the following methods should be used to substantiate each failure condition’s effects:

a. Pilot and human factors evaluation: Failure conditions where crew reaction significantly influences the effects of the failure, should be evaluated by experienced pilots and human factors specialists. The means and timeliness of failure recognition, intuitive or procedural response and overall workload should be substantiated.

b. Engineering evaluation: Direct and indirect functional effects of the failure condition may be determined based on previous experience and knowledge of aircraft of similar design and operational characteristics, on data and rationale obtained through certification authority and industry literature, and on analytical or simulation results. Certification authorities and aircraft manufacturers may retain senior engineers recognized for their expertise and experience who may be consulted for this purpose.

c. Published historical data: Historic precedent or accident or incident narratives for similar occurrences can be used to determine the expected effects of the failure condition. Due to the fact that incidents or accidents are very specific occurrences, the analyst should ensure that the events in question are indeed representative of the failure condition.

AVA Documents
Document Sharing Hub
Full document details: SAE ARP4761A

d. Published guidance: Certification authority provided guidance material may specify a severity classification for the failure condition. When such a classification is given, the effect on aircraft, on flight crew, and on occupants excluding fight crew may be inferred. When guidance material is used as a reference to establish a severity classification, it is necessary to substantiate that the details of the particular application being considered are fully consistent with the scenario described in the guidance material. Aircraft function, operational, and environmental conditions should be shown not to increase the severity of the failure conditions.

e. Testing: Where necessary and practical, controlled testing may be performed to assist in the substantiation of failure effects. Equipment, system rig or aircraft prototype testing may confirm effects of failure conditions on the aircraft. Pilot in the loop testing on representative flight simulation platforms may be used to evaluate crew reaction, crew workload, or controllability aspects of a failure condition.

A.9.3 Failure Condition Classification Correctness

Confirmation of the correct severity classification consists of evaluating the known failure effects in relation to the qualitative severity scales associated with the applicable severity classifications and determining that the correct severity classification has been selected for each failure condition during each flight phase. This task can typically be accomplished by inspection of the AFHA worksheets. Failure conditions classified as Catastrophic generally do not require confirmation, as this classification is the most severe and carries the most stringent safety objectives.

Failure condition severities and requirements that are specified in aircraft certification guidance material have usually been specified due to accident or incident experience, or collaborative expert experience and opinion. If the guidance material specifies a worst-case failure condition severity, there is likely no need to further assess effects unless the applicant desires to show justification that the worst-case effects implied by the guidance material are not applicable to their particular aircraft.

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

APPENDIX B - PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA)

NOTE: The main body of this document contains information that places the procedures in this appendix in context. This appendix is to be used in conjunction with the main body of the document.

TABLE OF CONTENTS

B.1 PASA OVERVIEW 50

B.2 PASA INPUTS 51
B.2.1 Aircraft Functions and Failure Conditions from AFHA 51
B.2.2 Requirements 52
B.2.3 Initial Operational Considerations 52
B.2.4 Proposed Aircraft Architecture 52
B.2.5 Failure Conditions from System FHAs 52

B.3 INTERDEPENDENCE ANALYSIS 52

B.4 FAILURE CONDITION EVALUATION 54
B.4.1 Multifunction and Multisystem (MF&MS) Analysis 55
B.4.2 Assignment of FDALs 55
B.4.3 Supporting Analyses 56
B.4.4 PASA Safety Requirements and Assumptions 61

B.5 PASA COMPLETION 62

B.6 PASA OUTPUTS 63
B.6.1 Capturing PASA Outputs 63
B.6.2 Relationship Between PASA and ASA 64

Figure B1 PASA flow 51
Figure B2 Independence Principle flow through Common Cause Analyses 60

Table B1 Interdependence table example 53
Table B2 Combined Functional Failure Effects (CoFFE) table example 56
Table B3 Common Resource Analysis table example for failure condition “Loss of adequate deceleration means” 59

Documents
Document Sharing Hub
Full document details: SAE ARP4761A

B.1 PASA OVERVIEW

The Preliminary Aircraft Safety Assessment (PASA) process is a systematic examination of a proposed aircraft architecture. In the context of the AFHA failure condition safety objectives, the PASA also identifies aircraft-level safety requirements (e.g., FDAL, independence, probability, functional, or performance) to address AFHA failure conditions, whether they are allocated to one system or many systems.

The PASA identifies the interactions and dependencies between the aircraft systems, assesses how their failures can lead to the aircraft-level failure conditions identified by the AFHA, and determines whether the safety objectives can be met. The PASA process interacts with the development process by evaluating the proposed aircraft architecture and identifies the need for specific safety requirements. Just as the development process is iterative, the PASA process is iterative throughout the development cycle. Periodic updates to the PASA may be necessary as the aircraft architecture matures to ensure a complete set of data is available to support the aircraft certification.

The PASA is particularly important when evaluating complex integration of aircraft systems that pose additional failure combinations that might not otherwise be present when aircraft functions are implemented by stand-alone systems. From the aircraft-level perspective, typical interactions and interdependencies involve multiple systems that together implement an aircraft-level function; this includes reliance on common resources, e.g., hydraulic power, electrical power, air data, air-ground logic, common computing, and data networks.

The PASA process begins during the initial aircraft architecture development phase. The main objectives of the PASA are to assess the proposed aircraft architectures and develop safety requirements; with these requirements established, the aircraft and individual systems' development can proceed with reduced risk.

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

The PASA is conducted as shown in Figure B1. The PASA process includes the following activities which are described in more detail in the sections referenced:

a. Gather input data (Section B.2).

b. Perform an Interdependence Analysis (Section B.3).

c. Perform failure condition evaluation and propose safety requirements (Section B.4).

d. Determine whether safety considerations are achievable (Section B.5).

e. Document assessment results, including safety requirements (Section B.6).

Documents
Document Sharing Hub
Full document details: SAE ARP4761A