SAE INTERNATIONAL

AEROSPACE RECOMMENDED PRACTICE

ARP4754™ REV. B

Issued 1996-11
Revised 2023-12

Superseding ARP4754A

(R) Guidelines for Development of Civil Aircraft and Systems

RATIONALE

This SAE Aerospace Recommended Practice (ARP) provides processes used to develop civil aircraft and systems. It has been revised to incorporate known errata and specific industry comments necessary to maintain the recommendations consistent with industry state-of-the-art.

TABLE OF CONTENTS

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/ARP4754B/

1. SCOPE

This SAE Aerospace Recommended Practice (ARP) provides recommendations for the development of aircraft and systems, taking into account aircraft functions and operating environment. It provides practices for ensuring the safety of the overall aircraft design, showing compliance with regulations, and assisting a company in developing and meeting its own internal standards. These practices include validation of requirements and verification of the design implementation for safety, certification, and product assurance.

The guidelines in this document were developed in the context of U.S. Title 14 Code of Federal Regulations (14 CFR) Part 25 and European Union Aviation Safety Agency (EASA) Certification Specification (CS) CS-25. They may be applicable in the context of other regulations, such as 14 CFR Parts 23, 27, 29, 33, and 35, and CS-23, CS-27, CS-29, CS-E, and CS-P.

This document addresses the development cycle for aircraft and systems that implement aircraft and system functions. It does not include detailed information on the following subjects and references:

- Software development; refer to RTCA DO-178C/EUROCAE ED-12C.
- Electronic hardware development; refer to RTCA DO-254/EUROCAE ED-80.
- Integrated modular avionics development; refer to RTCA DO-297/EUROCAE ED-124.
- Airworthiness security process; refer to RTCA DO-326A/EUROCAE ED-202A.
- Safety assessment processes; refer to ARP4761A/EUROCAE ED-135.
- A process for accomplishing in-service safety assessment is described in ARP5150A and ARP5151A or in other documents such as the guidance material of EASA Part 21 (GM21) when required by applicable regulation. In this document, wherever references to ARP5150A/ARP5151A are made, the reader should understand this also implies EASA Part 21 (GM21).
- Master Minimum Equipment List (MMEL) or Configuration Deviation List (CDL) development; refer to applicable regulatory guidance from the applicable Certification Authority.
- Aircraft structure and aerodynamics development.

Figure 1 outlines the relationships between the various development documents, which provide guidelines for safety assessment, electronic hardware and software life cycle processes, and the system development process described herein.

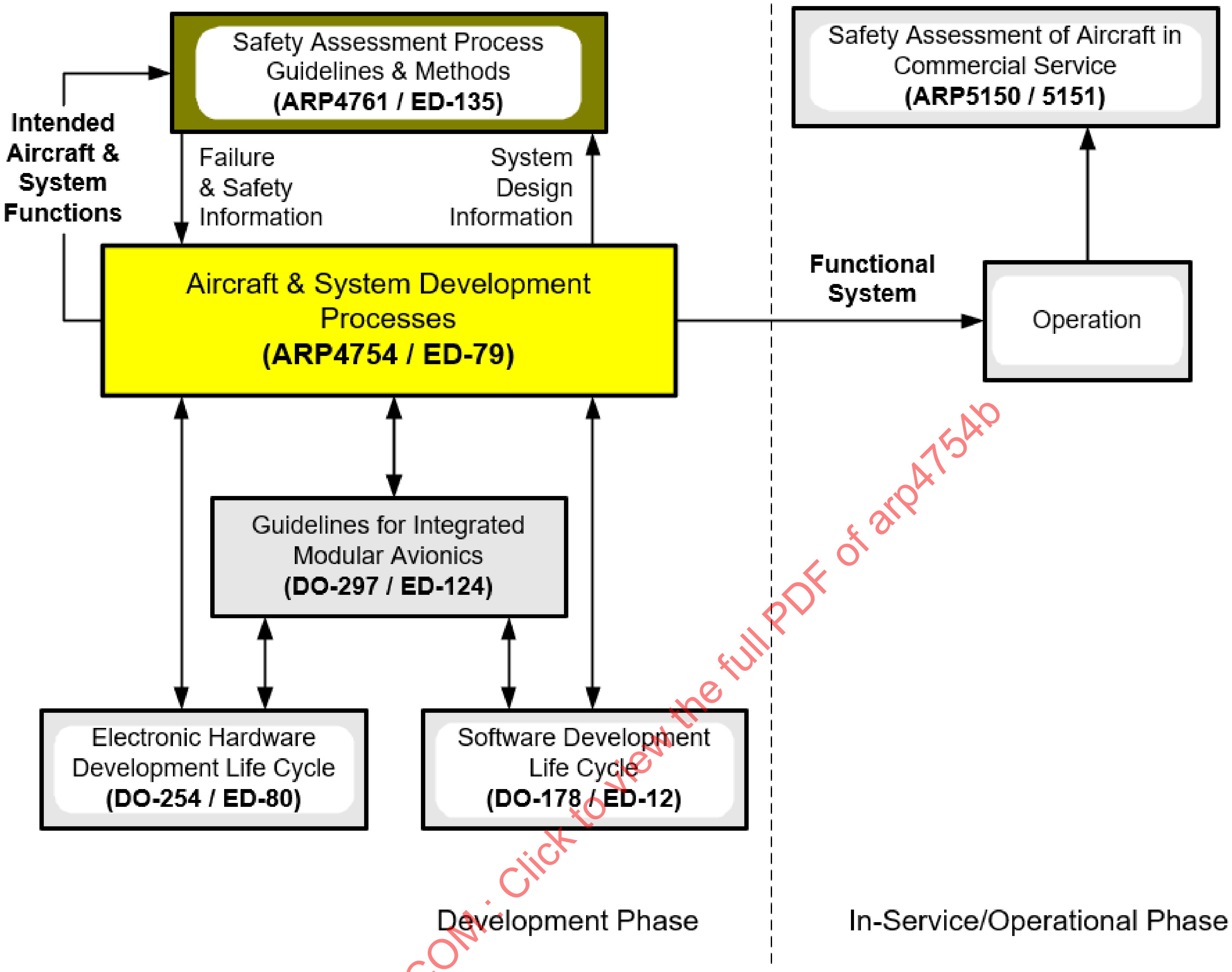


Figure 1 - Guideline documents covering development and in-service/operational phases

1.1 Purpose

The guidelines herein are industry best practices for the development of aircraft and of systems. Modern aircraft typically comprise a large integrated environment consisting of multiple systems with significant dependencies and interactions. Frequently portions of these systems are developed by separate individuals, groups, or organizations. These systems require design discipline and systematic development to ensure that safety and operational requirements can be fully realized and substantiated. Adherence to these guidelines is recommended for development of all aircraft systems, especially those that may contribute to failure conditions with the potential to affect safety.

The contents are recommended practices and should not be construed to be regulatory requirements. For this reason, the use of words such as “shall” and “must” is avoided except if used in the context of an example. It is recognized that alternative methods to the processes described or referenced in this document may be available to an organization desiring to obtain certification.

This document provides neither guidelines concerning the structure of an individual organization nor how the responsibilities for certification activities are divided. No such guidance should be inferred from the descriptions provided.

1.2 Development Assurance

A process is needed which establishes levels of confidence that development errors that can cause or contribute to identified failure conditions have been minimized with an appropriate level of rigor. This henceforth is referred to as the development assurance process. To establish levels of confidence for the aircraft systems as a whole, the process outlined herein presents guidelines for developing aircraft- and system-level requirements, including requirements allocated to items. The process includes validating requirements, and verifying that requirements are met, together with the necessary configuration management and process assurance activities. As development assurance level assignments are dependent on classification of failure conditions, the safety analysis process is used in conjunction with the development assurance process defined herein to identify failure conditions and severity classifications which are used to establish the level of rigor required for development.

Development assurance is a process-based approach which establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.

1.3 Document Background

During development of Revision B to RTCA/EUROCAE document DO-178/ED-12, it became apparent that system-level information would be required as input to the software development process. Since many system-level decisions are fundamental to the safety and functional aspects of aircraft systems, regulatory involvement in the processes and results relating to such decisions is both necessary and appropriate.

This document was originally developed in response to a request from the Federal Aviation Administration (FAA) to SAE. The FAA requested that SAE define the appropriate nature and scope of system-level information for demonstrating regulatory compliance for highly integrated or complex avionic systems. The Systems Integration Requirements Taskgroup (SIRT) was formed to develop an ARP that would address this need.

The initial members of SIRT recognized that harmonization of international understanding in this undertaking was highly desirable and encouraged participation by both FAA and Joint Aviation Authorities (JAA) representatives. A companion working group was formed under EUROCAE, WG-42, to coordinate European input to the SIRT group. The task group included people with direct experience in development and support of large commercial aircraft, commuter aircraft, commercial and general aviation avionics, jet engines, and engine controls. Certification Authority personnel with a variety of backgrounds and interests participated in the work of the task group. Both formal and informal links with RTCA special committees (SC-167 and SC-180) and SAE committee (S-18) were established and maintained. Communication with the harmonization working group addressing 14 CFR/CS 25.1309 was maintained throughout development of this document.

Throughout development of this document, discussion returned repeatedly to the issue of guideline specificity. Strong arguments were presented in favor of providing a list of very specific certification steps, i.e., a checklist. Equally strong arguments were made that the guidelines should focus on fundamental issues, allowing the applicant and the Certification Authority to tailor details to the specific system. It was recognized that in either case certification of all but the most idealized systems would require significant engineering judgment by both parties. The quality of those judgments is served best by a common understanding of, and attention to, fundamental principles. The decision to follow this course was supported by several other factors; the variety of potential systems applications, the rapid development of systems engineering, and industry experience with the evolving guidance contained in DO-178/ED-12 and their revisions being particularly significant.

The current trend in system development is an increasing level of integration between aircraft functions and the systems that implement them. While there can be considerable value gained when integrating systems with other systems, the increased complexity yields increased possibilities for errors, particularly with functions that are performed jointly across multiple systems. Following the Aviation Rulemaking Advisory Committee (ARAC) recommendations to respond to this increased integration which referenced ARP4754/ED-79 in advisory materials for compliance to 14 CFR/CS 23.1309 (refer to AC23.1309-1D, issued in 2009) and 25.1309 (refer to AMC 25.1309, published in 2003 and AC 25.1309 Draft ARSENAL revised) the use of the ARP4754/ED-79 in aircraft certification has become increasingly widespread. Along with the increasing use, in particular 5.4 of the original document, assignment of development assurance levels in the original ARP4754/ED-79, come insights on the strengths and weaknesses of its guidelines. The underlying philosophy is succinctly represented in the original 5.4 of ARP4754/ED-79 as follows:

> *"If the PSSA shows that the system architecture provides containment for the effects of design errors, so that the aircraft-level effects of such errors are sufficiently benign, the development assurance activities can be conducted at a reduced level of process rigor for the system items wholly within the architectural containment boundary."*

Experience has shown that the processes and definitions used to determine containment have yielded different interpretation and application of the philosophy. Revision A improved the development assurance level assignment process by providing a methodology to assign the correct development assurance levels (see 5.2).

Revision A contained updates to the document that took into account the evolution of the industry over the intervening years. EUROCAE WG-42 had been closed on completion of their task, the initial publication of ARP4754/ED-79. In order to support S-18 activities in maintaining the document, a new companion working group was formed under EUROCAE, WG-63, to coordinate European input. The relationship between ARP4754/ED-79 and ARP4761, and their relationship with DO-178B/ED-12B and DO-254/ED-80 were strengthened and discrepancies between the documents were identified and addressed. Revision A also explained the top-down development assurance concept for application at the aircraft and system level and standardized the use of the term development assurance. As a consequence, for aircraft and systems, Function Development Assurance Level (FDAL) was introduced and the term Item Development Assurance Level (IDAL) is used to describe that the level of rigor of development assurance tasks performed on item(s), e.g., IDAL is the appropriate "Software Level" in DO-178B/ED-12B and "Design Assurance Level" in DO-254/ED-80 objectives that need to be satisfied for an item. It also included enhancements created by feedback from the industry since the first publication. In addition, S-18/WG-63 coordinated the Revision A effort with RTCA Special Committee 205 (SC-205)/EUROCAE WG-71 to ensure that the terminology and approach being used were consistent with those being developed for the update to DO-178C/ED-12C.

Subsequent to the publication of Revision A, the FAA recognized ARP4754A as an acceptable method for establishing a development assurance process in AC 20-174.

1.4 Revision B Overview

Revision B is primarily focused on the necessary updates to align its contents with ARP4761A/ED-135. There were extensive discussions within S-18/WG-63 on the need to limit scope of this revision versus expanding its contents to include emerging system development techniques in use by the industry. Given the timeframe of ARP4761A/ED-135 publication, and the necessity to maintain consistency between both ARP4754B/ED-79B and ARP4761A/ED-135, the first option, limiting the scope, was chosen and suggested changes that would further expand ARP4754/ED-79 contents were deferred for a new Revision C. As a result, while the general principles of FDAL/IDAL assignment were retained in ARP4754B/ED-79B, the details of FDAL/IDAL assignment activities were transferred to ARP4761A/ED-135. The same approach was adopted for all safety assessment process contents in ARP4754B/ED-79B. Validation and verification sections have been changed to allow for a less prescriptive use of the many validation and verification methods, and concepts such as "unintended behavior" and "derived requirements" have been further clarified based on experience in applying ARP4754A/ED-79A in recent developments. The section addressing modifications has been completely changed to better account for different change categories used by the industry, including reuse. The definitions section, the objectives appendix, and certification coordination contents have been revisited and updated accordingly. A detailed example of an aircraft system development process has been added in Appendix E. Keeping to the Memorandum of Understanding for this document, WG-63 worked alongside S-18 to ensure that ED-79B is word-for-word equivalent to ARP4754B.

2. REFERENCES

2.1 Applicable Documents

The following publications are referenced in this guideline document. The applicable issue of referenced publications is the revision noted in this section. Where later versions of these documents are available, applicants should check their applicability. Note that the revision level of references may not be noted elsewhere in the document unless pertinent.

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.

ARP4761A	Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment
ARP5150A	Safety Assessment of Transport Airplanes in Commercial Service
ARP5151A	Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service

2.1.2 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.

Part 21	Certification Procedures for Aircraft and Related Products and Parts
CS-23	Certification Specifications for Normal-Category Aeroplanes
CS-25	Certification Specifications for Large Aeroplanes
CS-27	Certification Specifications for Small Rotorcraft
CS-29	Certification Specifications for Large Rotorcraft
CS-E	Certification Specifications for Engines
CS-P	Certification Specifications for Propellers
AMC 20-189	The Management of Open Problem Reports
AMC 25-19	Certification Maintenance Requirements
AMC 25.1309	Equipment, Systems and Installations EASA Acceptable Means of Compliance

2.1.3 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-80	Design Assurance Guidance for Airborne Electronic Hardware.
ED-124	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations
ED-135	Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment
ED-202A	Airworthiness Security Process Specification
ED-218	Model-Based Development and Verification Supplement to ED-12C and ED-109A

2.1.4 FAA Publications

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

14 CFR Part 21	Certification Procedures for Products and Parts
14 CFR Part 23	Airworthiness Standards: Normal Category Airplanes
14 CFR Part 25	Airworthiness Standards: Transport Category Airplanes
14 CFR Part 27	Airworthiness Standards: Normal Category Rotorcraft
14 CFR Part 29	Airworthiness Standards: Transport Category Rotorcraft
14 CFR Part 33	Airworthiness Standards: Aircraft Engines
14 CFR Part 35	Airworthiness Standards: Propellers
AC 20-174	Development of Civil Aircraft and Systems
AC 20-189	Best Practices for Management of Open Problem Reports (OPRs)
AC 25.1309-1A	System Design and Analysis, Advisory Circular
AC 25-19A	Certification Maintenance Requirements
FAA CPG	FAA and Industry Guide to Product Certification, Third Edition
TAEsdaT2-5241996	Transport Airplane and Engine Issue Area - Systems Design and Analysis Harmonization Working Group (includes AC/AMJ 25.1309 Draft ARSENAL revised System Design and Analysis)

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
DO-326A	Airworthiness Security Process Specification
DO-331	Model-Based Development and Verification Supplement to DO-178C and DO-278A

2.2 Definitions

This section provides definitions for terms used in this document. Citations are provided to other industry sources when usage in this document is consistent with the definition in the referenced source material. The shared definitions in ARP4761A/ED-135 and ARP5150A and those in this document have been coordinated to be identical.

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

ASSUMPTIONS: 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 (RTCA DO-178C/ED-12C).

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.

COMPLIANCE: Successful adherence to applicable regulations.

CONFIGURATION BASELINE: A known aircraft/system/item configuration against which a change process can be undertaken.

CONFIGURATION ITEM: Aircraft, system, item and related data that is under configuration control.

DEMONSTRATION: A method of proof of performance by observation.

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

DEVELOPMENT ASSURANCE: All 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 safety objectives (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).

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.

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 (FCC): 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-failure distribution function F(t)

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

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.

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.

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

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.)

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.

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 that 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 distance to provide physical independence between hardware elements.

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.

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.

UNINTENDED BEHAVIOR: Unexpected operation of integrated aircraft systems in ways contrary to intended functionality.

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.

2.3 Abbreviations and Acronyms

AC	Advisory Circular (FAA)
AFHA	Aircraft Functional Hazard Assessment
AMC	Acceptable Means of Compliance (EASA)
ARAC	Aviation Rulemaking Advisory Committee (FAA)
ARP	Aerospace Recommended Practice (SAE)
ASA	Aircraft Safety Assessment
ATC	Amended Type Certificate
CCMR	Candidate Certification Maintenance Requirement
CDL	Configuration Deviation List
CEA	Cascading Effects Analysis
CFR	Code of Federal Regulations
CM	Configuration Management
CMA	Common Mode Analysis
CMCC	Certification Maintenance Coordination Committee
CMR	Certification Maintenance Requirement
CS	Certification Specifications
EASA	European Union Aviation Safety Agency
ETSO	European Technical Standard Order
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FC	Failure Condition
FDAL	Function Development Assurance Level
FFS	Functional Failure Set
FHA	Functional Hazard Assessment
FMEA	Failure Mode and Effect Analysis

FMES	Failure Mode and Effect Summary
FTA	Fault Tree Analysis
HW	Hardware
ICA	Instructions for Continued Airworthiness
IDAL	Item Development Assurance Level
IMA	Integrated Modular Avionics
MA	Markov Analysis
MBSA	Model-Based Safety Analysis
MMEL	Master Minimum Equipment List
MSG-3	Maintenance Steering Group 3
OPR	Open Problem Report
PASA	Preliminary Aircraft Safety Assessment
PRA	Particular Risk Analysis
PRRT	Particular Risk Review Team
PSSA	Preliminary System Safety Assessment
RTCA	RTCA, Inc.
SC1	System Control Category 1
SC2	System Control Category 2
SFHA	System Functional Hazard Assessment
SIRT	Systems Integration Requirements Taskgroup
SSA	System Safety Assessment
STC	Supplemental Type Certificate
SW	Software
TC	Type Certificate
TSO	Technical Standard Order
USA	United States of America
WG	EUROCAE Working Group
ZSA	Zonal Safety Analysis

3. DEVELOPMENT ASSURANCE PLANNING

The purpose of the development assurance planning process is to define the means of developing an aircraft or system that will satisfy the aircraft/system requirements and provide the level of confidence which is consistent with the applicable certification basis. Modifications to existing aircraft and/or systems are considered during the development assurance planning process as described in Section 6. The objectives of the development assurance planning process are:

- To define the activities of the development assurance processes of the development life cycle that will address the aircraft/system requirements, Function Development Assurance Level(s) (FDALs), and Item Development Assurance Level(s) (IDALs)

- To define the development life cycle(s), including the inter-relationships between the processes, their sequencing, feedback mechanisms, and transition criteria

- To select the development environment for the development life cycle, including the methods and tools to be used for the activities of each development life cycle process

- To define the development standards consistent with the aircraft/system safety objectives for the aircraft/system to be produced

- To develop plans that satisfy the objectives of each integral process

The outputs of the development assurance planning process are documented in one or more planning documents, which can exist in various formats. The iterative nature of the design process should be considered during the development assurance planning process. Interrelationships between the planning elements and feedback loops should also be identified and managed, as appropriate.

3.1 Development Assurance Planning Process

Figure 2 is an example of the overall development assurance planning process and includes some generic objectives applicable to all planning elements. The development of these planning elements may not happen at the same time. Therefore, it is important to make sure the planning elements are consistent with each other and collectively make up a complete plan for the entire development life cycle. The reviewers should keep this in mind when reviewing individual planning elements.

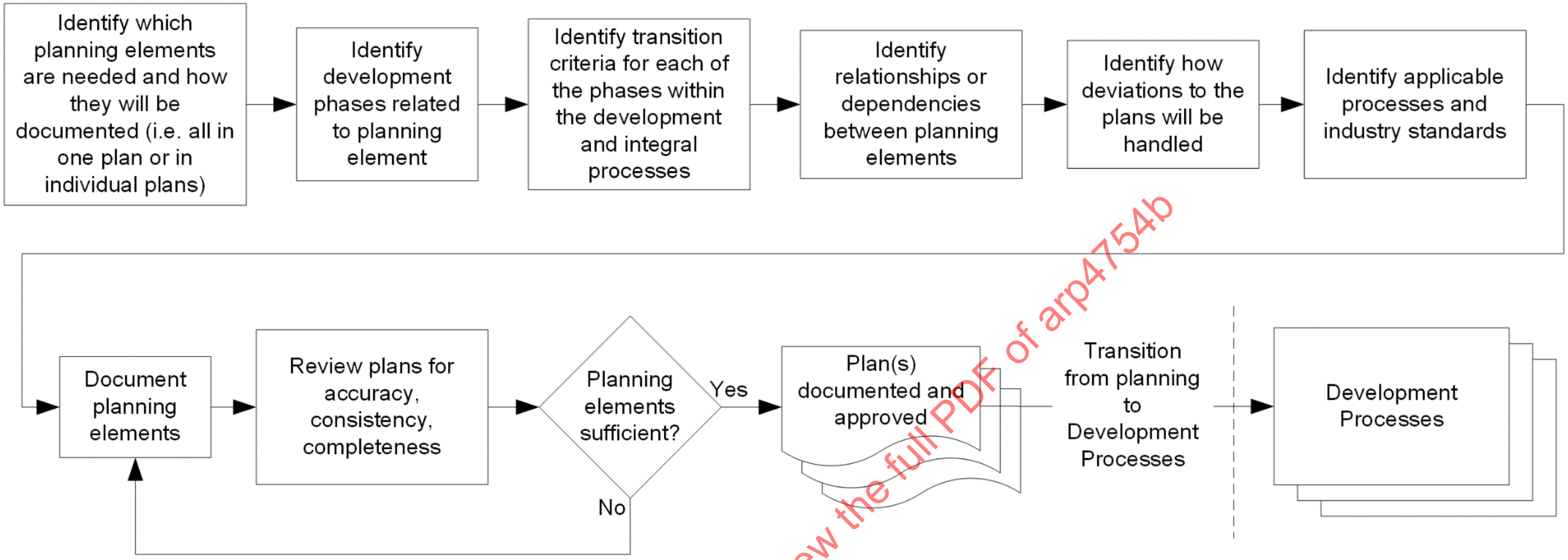

Identify which planning elements are needed and how they will be documented (i.e. all in one plan or in individual plans)
Identify development phases related to planning element
Identify transition criteria for each of the phases within the development and integral processes
Identify relationships or dependencies between planning elements
Identify how deviations to the plans will be handled
Identify applicable processes and industry standards
Document planning elements
Review plans for accuracy, consistency, completeness
Planning elements sufficient?
Yes
No
Plan(s) documented and approved
Transition from planning to Development Processes
Development Processes

Figure 2 - Development Assurance planning process

Table 1 summarizes the planning elements that should be included in the planning phase.

The development assurance planning process can be re-entered for aircraft or system changes, such as a new aircraft derivative or modifications to an in-service aircraft.

Table 1 - Planning elements

Planning Elements	Planning Element Description	Process Section
Development	Establish the process and methods to be used to provide the framework for the aircraft/system development, integration, and implementation.	Section 4
Safety Program	Establish scope and content of the safety activities related to the development of the aircraft or system.	5.1
Requirements Capture	Identify and describe how the requirements are captured and managed. Sometimes the requirements capture planning elements are included in conjunction with the requirements validation planning elements.	5.3
Requirements Validation	Describe how the requirements will be shown to be complete and correct, and how the assumptions will be managed.	5.4
Implementation Verification	Define the processes and criteria to be applied when showing how the implementation satisfies its requirements.	5.5
Configuration Management	Describe the key development-related configuration items and how they will be managed.	5.6
Process Assurance	Describe the means to assure the practices and procedures to be applied during system development are followed.	5.7

3.2 Development Assurance Plan

The results of the development assurance planning process should be documented in a development assurance plan or collection of plans. Each of the planning elements described in Table 1 should be addressed within the development assurance plan(s).

The development assurance plan(s) directly contribute to the Certification Authority coordination activities described in 3.3. It may be beneficial to structure the development assurance plan or collections of plans such that effective coordination with the Certification Authorities is facilitated. If a collection of plans is used, it may be beneficial to include a top-level summary that provides an overview of the plan for each of the development assurance planning elements.

The development assurance plan(s) should identify:

a. The scope of the development activity, including considerations for modification or reuse of previously certificated systems, equipment, and items (see Section 6)

b. The processes and methods associated with each of the planning elements in Table 1

c. The key events that mark the planned development cycle

d. The organizational structure, roles, and responsibilities supporting the development

e. The means to identify and address unintended behaviors

The processes and events should be described in sufficient detail to establish their relative significance to the aircraft/system development, their relative timing and interdependencies, and the nature of the results expected at event or process completion. For complex systems, it is advisable to provide descriptions of the specific development processes that are planned to manage this complexity at the aircraft/system level.

3.2.1 Design Description

A design description may be provided to facilitate a common understanding of the applicability of the planning elements captured in the development assurance plan(s). This description, which may be referenced by the development assurance plan(s), may include the intended or anticipated:

- Aircraft-level functionality provided or supported by the system(s)
- System operating environment(s)
- Capabilities of the system(s) as installed on the aircraft
- Primary fault or failure containment means
- New or novel design features
- Architectural and design features that perform a specific role in establishing or maintaining aircraft system safety

3.2.2 Transition Criteria

A key element of planning is the establishment of life cycle process checkpoints and reviews, which are aligned with program phases and gates. The plans should clearly define maturity expectations to provide visibility on the progress and integration state for the major elements of design, implementation, and certification. This can be accomplished by clearly identifying the technical and process entrance and exit criteria. Issues left open when transitioning from one phase of development to another should be tracked and managed, as appropriate.

3.2.3 Deviations from Plans

During development there may be times when it is necessary to deviate from the documented plans. Therefore, during the planning phase it is important to identify a process to address deviations from the plans. Methods for reporting, gaining approval of, and documenting any deviations should be described in the planning elements.

3.3 Certification Authority Coordination

A significant consideration in development assurance planning is Certification Authority coordination. The goal of this coordination is to identify how development assurance processes will contribute to a certification effort, and what development assurance data may be used for that purpose. Planning and coordination are vital to:

- Establish effective communications between the applicant and the Certification Authority
- Reach agreement with the Certification Authorities on the intended means of showing that the aircraft, its systems, equipment, and items meet specific regulatory requirements and industry standards

This section provides a number of topics that applicants could raise or consider during the interactions between development assurance and certification. For specific information on product certification and planning, consult appropriate regulatory guidance.

Early coordination with the Certification Authorities is recommended for development assurance planning. This coordination is crucial when establishing the detail of the development assurance planning process, which varies depending on the functions and their associated hazards. Early coordination can reduce uncertainty in the certification process and can minimize the effects of misinterpretations of company processes, industry standards, regulations, and advisory materials.

Certification Authority coordination begins during the planning phase, but continues through development and product certification.

The following list contains development assurance topics for Certification Authority coordination:

a. A description which establishes the functional relationships, physical layout, and data exchange interfaces within the aircraft and/or system(s) under development

b. Regulatory gaps for new aircraft types (e.g., unmanned aircraft systems), or for applications of new technologies (e.g., artificial intelligence)

c. Development assurance planning elements for the specific application, including aircraft-level and/or system-level planning elements that support the scope of the development:

    1. The scope of the development assurance process including rationale for any aspects that are tailored and/or in some cases eliminated; this may include process substitutions or alternate methods not covered by this document

    2. A high-level description of the relevant integral processes (e.g., safety assessment, validation, verification, configuration management, and process assurance); requirements management processes should include details specifically related to safety requirements

    3. A description of the interactions between certification and system requirements, design, and key safety assessment activities (see 5.1)

    4. If applicable, address the plan to re-use processes, methods, or data from a previously approved product

    5. A plan to develop a process for detecting errors in the implementation; this can include planning for a practical set of tests, direct inspection, or other verification methods to fully characterize system behaviors in normal operation and in failed states

    6. Roles and responsibilities of various groups involved in the development from aircraft level to item level; consider the roles of suppliers relative to aircraft developers in the processes, e.g., aircraft safety group involvement in derived requirement and safety requirement reviews

d. The Aircraft and/or System Functional Hazard Assessment(s) including failure conditions, effects, classifications, and substantiation data

e. As the project progresses, the Preliminary Aircraft and/or System Safety Assessment(s), including aircraft/system safety objectives, design decisions affecting compliance, and preliminary development assurance levels

f. A list of the data to be submitted to the Certification Authorities, and the data to be retained under configuration control

Certification Authority coordination continues throughout the development life cycle. In order to show that the aircraft, its systems, equipment, and items meet specific regulatory requirements and industry standards, a summary of the development assurance process outputs may be provided (see 4.7).

4. AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS

This section provides an overview of a generic approach for developing aircraft and aircraft systems from conceptual definition to certification. This section establishes common terminology and expectations associated with development processes and their inter-relationships in order to understand the intent and applicability of the substantiating material.

The development life cycle has a beginning and an end. A new development cycle can be initiated to perform aircraft or system modifications, or to create a new derivative aircraft. The guidelines contained in this document are primarily geared toward the “Development” phase as shown in Figure 3.

The concept phase (i.e., research and preliminary development phase) determines the overall aircraft/system performance and configuration such as payload and range, aircraft size, number and locations of engines, airfoil, and applications of new technologies in design and manufacturing.

The development phase follows the concept phase, readying the implementation for production/operation. The development phase is complete when:

- Build/test information is provided to a production facility or facilities
- All regulatory compliance data is completed, and the Certification Authority concurs with the showing made by the applicant
- The design has met all applicable internal requirements
- Limitations, maintenance, and other operational information are provided to the aircraft operators

4.1 Generic Aircraft/System Development Process

The generic aircraft/system development process outlined in this section establishes a framework for discussing the process. This section does not imply a preferred method or process; nor does it imply a specific organizational structure. Figure 3 provides a graphical representation of the aircraft/system development process with the numerical entries in each activity box representing the section numbers of this document in which the activity is further explained.

A top-down sequence for developing a specific system implementation from knowledge of an intended aircraft function provides a convenient conceptual representation of the system development process. A typical system development progresses in an iterative and concurrent fashion using both top-down and bottom-up strategies. In this document, emphasis is focused on the top-down aspect since it provides the necessary links between aircraft safety and system development. It is recognized that organizations may structure their functional/product breakdown with additional layers. The processes described in this document would then be applied, with appropriate adaptations, to these layers from the aircraft to item levels.

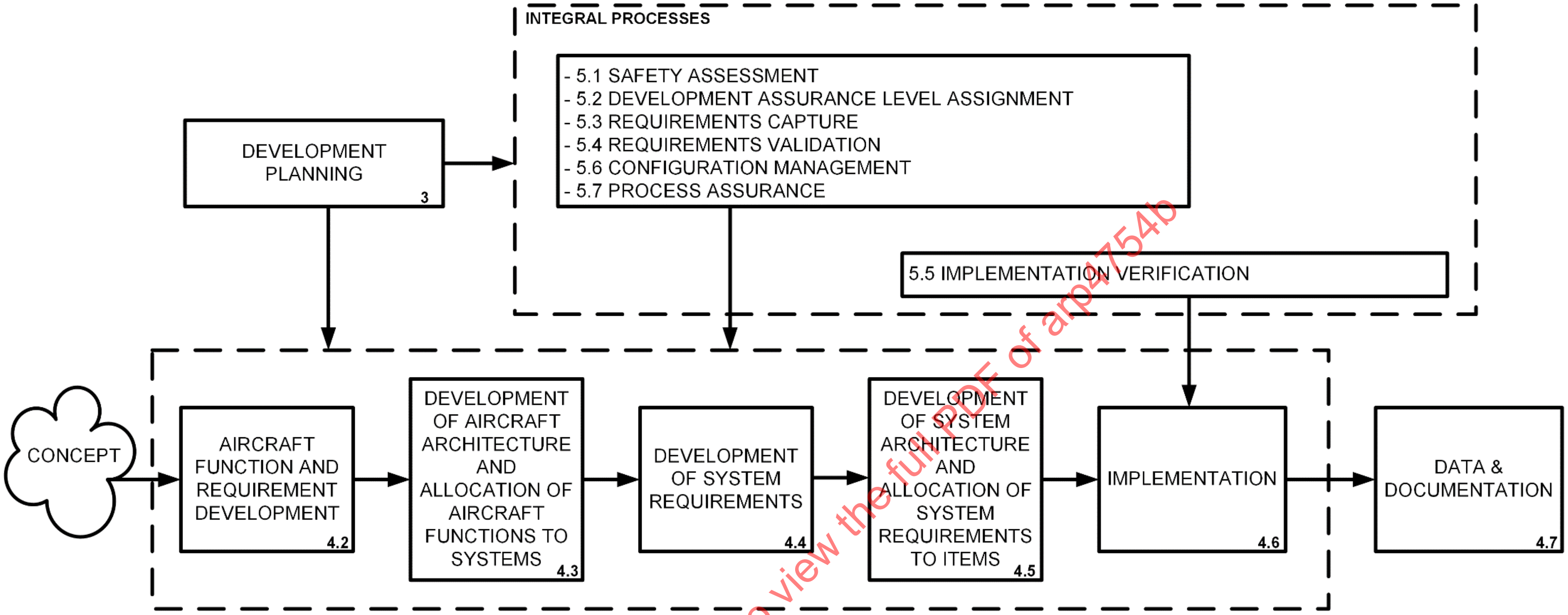

INTEGRAL PROCESSES
- 5.1 SAFETY ASSESSMENT
- 5.2 DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT
- 5.3 REQUIREMENTS CAPTURE
- 5.4 REQUIREMENTS VALIDATION
- 5.6 CONFIGURATION MANAGEMENT
- 5.7 PROCESS ASSURANCE
5.5 IMPLEMENTATION VERIFICATION
DEVELOPMENT PLANNING 3
CONCEPT
AIRCRAFT FUNCTION AND REQUIREMENT DEVELOPMENT 4.2
DEVELOPMENT OF AIRCRAFT ARCHITECTURE AND ALLOCATION OF AIRCRAFT FUNCTIONS TO SYSTEMS 4.3
DEVELOPMENT OF SYSTEM REQUIREMENTS 4.4
DEVELOPMENT OF SYSTEM ARCHITECTURE AND ALLOCATION OF SYSTEM REQUIREMENTS TO ITEMS 4.5
IMPLEMENTATION 4.6
DATA & DOCUMENTATION 4.7

Figure 3 - Aircraft/system development process

4.1.1 Development Assurance

Due to the highly complex and integrated nature of modern aircraft systems, the Certification Authorities have highlighted concerns about the possibility of development errors causing or contributing to aircraft failure conditions. To address these concerns, a methodology to minimize the likelihood of development errors is required. The following text reflects the concerns expressed in current certification requirements/regulations:

a. A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of highly integrated systems that perform complex and interrelated functions, particularly through the use of electronic technology and software-based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems. Thus, other assurance techniques, such as development assurance utilizing a combination of process assurance, validation and verification coverage criteria, or structured analysis or assessment techniques applied at the aircraft level, if necessary, or at least across integrated or interacting systems, have been applied to these more complex systems. Their systematic use increases confidence that errors in requirements or design and integration or interaction effects have been adequately identified and corrected.

b. Considering the above developments, as well as revisions made to 14 CFR/CS 25.1309, AMC 25.1309 was revised to include new approaches, both qualitative and quantitative, which may be used to assist in determining safety requirements and establishing compliance with these requirements, and to reflect revisions in the rule, considering the whole aircraft and its systems. It also provides guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analysis. The analytical tools used in determining numerical values are intended to be used in addition to (but not replace) qualitative methods based on engineering and operational judgment.

Therefore, a process is needed which establishes levels of confidence that development errors that can cause or contribute to identified failure conditions have been minimized with an appropriate level of rigor. This henceforth is referred to as the development assurance process.

4.1.2 Introduction to Development Assurance Process

The guidance material presented in DO-178C/ED-12C and DO-254/ED-80 has been recognized by industry and the various Certification Authorities to establish levels of confidence that a specific item of software and electronic hardware respectively performs to its intended design requirements. To establish levels of confidence for the aircraft systems as a whole, the process outlined herein presents guidelines for developing aircraft-level, system-level, and item-level requirements. The process includes validating requirements, and verifying that requirements are met, together with the necessary configuration management and process assurance activities. As development assurance level assignments are dependent on classification of failure conditions, the safety analysis process is used in conjunction with the development assurance process defined herein to identify failure conditions and severity classifications which are used to derive the level of rigor required for development.

Complex systems and integrated aircraft-level functions present greater risk of development error and undesirable, unintended behavior. At the same time, it is generally not practical (and may not even be possible) to develop a finite test suite for highly integrated and complex systems which conclusively confirms that there are no residual development errors. Since these errors are generally not deterministic and suitable numerical methods for characterizing them are not available, other qualitative means should be used to establish that the system can satisfy safety objectives. Furthermore, there is no direct correlation between Functional Development Assurance Level and numerical probabilities. The safety objectives associated with Failure Condition Classifications can be satisfied by both the designated function development assurance rigor and by numerical analysis methods (as needed). These two separate methods, in general, are not related and complement each other.

In this context, this Aerospace Recommended Practice regards the activities of DO-178C/ED-12C and DO-254/ED-80 as means to implement the development assurance rigor for the software and electronic hardware items. These software- and electronic hardware-related processes are no longer considered to be adequate to mitigate aircraft/system errors without a development assurance process from aircraft level down to item level, as shown in Figure 4.

In summary, development assurance is a process-based approach which establishes confidence that aircraft/system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.

4.1.3 Introduction to Hierarchical Safety Requirements Generated from Safety Assessment

Safety objectives are the qualitative and/or quantitative attributes necessary to achieve the required level of safety for an identified failure condition, depending on its classification. Safety requirements are those which are necessary to achieve either a safety objective or satisfy a constraint established by the safety process. Safety requirements may exist at the aircraft, system, and item levels. Through the application of the Aircraft Functional Hazard Assessment (AFHA) process, failure conditions and associated classifications for the aircraft functions are identified. The classification of these failure conditions establishes the safety objectives for the aircraft functions. Through the application of the Preliminary Aircraft Safety Assessment (PASA) process, the proposed aircraft architecture is evaluated against its safety objectives. Safety requirements are generated through the PASA activities. The safety requirements generated through the PASA activities are passed to the development process to be allocated to systems.

Through the application of the System Functional Hazard Assessment (SFHA) process, failure conditions and associated classifications for the system functions are identified. The classification of these failure conditions establishes the safety objectives for the system functions. Through the application of the Preliminary System Safety Assessment (PSSA) process, proposed system architectures are evaluated against their safety objectives, and allocated requirements from the PASA process. Safety requirements are generated through the PSSA activities. The safety requirements generated through the PSSA activities are passed to the development process to be allocated to items.

Figure 4 illustrates the interactions between the safety assessment process and the development process at the various hierarchical levels of development.

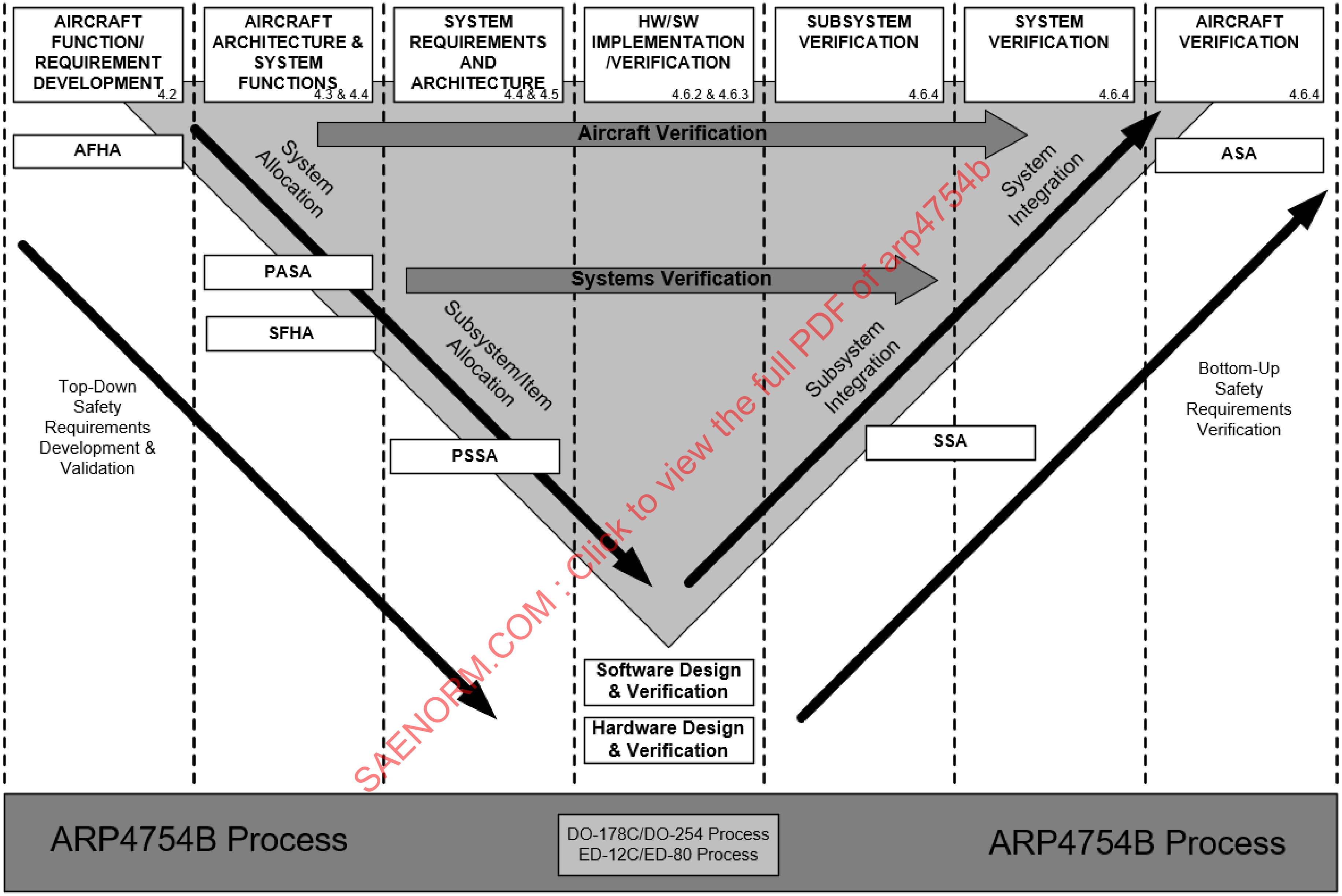

AIRCRAFT FUNCTION/ REQUIREMENT DEVELOPMENT
4.2
AIRCRAFT ARCHITECTURE & SYSTEM FUNCTIONS
4.3 & 4.4
SYSTEM REQUIREMENTS AND ARCHITECTURE
4.4 & 4.5
HW/SW IMPLEMENTATION /VERIFICATION
4.6.2 & 4.6.3
SUBSYSTEM VERIFICATION
4.6.4
SYSTEM VERIFICATION
4.6.4
AIRCRAFT VERIFICATION
4.6.4
AFHA
Aircraft Verification
ASA
System Allocation
System Integration
PASA
Systems Verification
SFHA
Subsystem/Item Allocation
Subsystem Integration
Top-Down Safety Requirements Development & Validation
PSSA
SSA
Bottom-Up Safety Requirements Verification
Software Design & Verification
Hardware Design & Verification
ARP4754B Process
DO-178C/DO-254 Process
ED-12C/ED-80 Process
ARP4754B Process

Figure 4 - Interaction between Safety Assessment and development processes

4.2 Aircraft Function and Requirement Development

While Figure 3 illustrates the generic aircraft/system development process, Figure 5 shows an aircraft function implementation process. The aircraft function implementation process includes multiple system development processes. Each system development process can consist of multiple item development processes. There are certain integral processes that take place repetitively during each of the development activities.

Most development processes involve many iterative cycles, making the experience appear more cyclic than sequential. The entry point for aircraft function implementation may occur at any point in the cycle. For a new aircraft-level function, the process begins with the top-level definition of functions. For adding functions to an aircraft, the entry point may occur in the context of changes to a particular item. However, regardless of the entry point, an assessment of the impact of the new or modified function on other aircraft-level functions and their supporting requirements is necessary. In practice many of the development activities shown in Figure 5 are concurrent and may involve interactive dependencies that lead to alteration of previously established requirements.

Outputs of this activity are a list of aircraft functions and requirements.

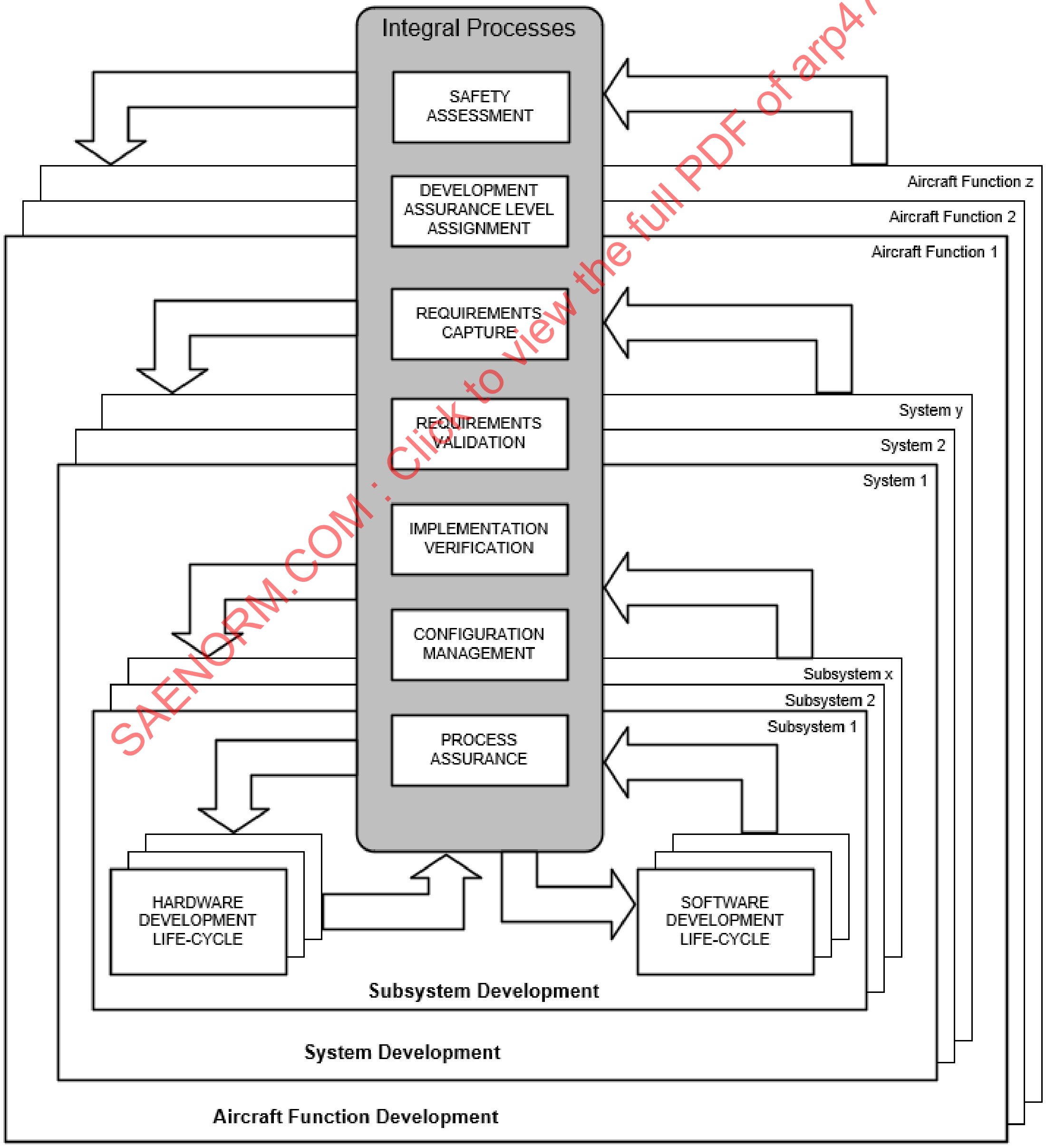


Figure 5 - Aircraft function implementation process

4.3 Development of Aircraft Architecture and Allocation of Aircraft Functions to Systems

The next level of activity consists of establishing the aircraft architecture, determining the appropriate grouping of aircraft functions, and the allocation of the functions to systems. During the process of developing the aircraft architecture, candidate architectures are iteratively evaluated using functional and performance analyses and the PASA process to establish feasibility in meeting the top-level safety objectives for the aircraft.

The process for selecting the appropriate grouping of aircraft functions out of the range of possible groupings is often complicated. No specific recommendations for accomplishing the grouping activity are provided in this document. However, careful attention to the basis for the selection decisions, including related assumptions, is fundamental to the success of subsequent processes. The functional groupings interact with the aircraft architecture and are the basis for system architecture development. While it is not necessary to know in detail how a system will be implemented to accomplish the necessary functional groupings, implementation constraints, failure effects, and life cycle support may all play a significant role in selecting the most appropriate groupings. The allocation should also define inputs, processes performed, and outputs, and consider operational and support aspects. Assumptions that are made in the course of this process become a vital part of the overall system requirements package and should be documented.

The output of this activity is an aircraft architecture with aircraft functions allocated to systems.

4.4 Development of System Functions and Requirements

Once aircraft functions are allocated to systems, system functions are determined relative to their role in the aircraft architecture. The system functions should be described in terms of what the system is to accomplish, rather than the means envisioned to implement the system function. System functions may be the intended behaviors of the system, such as intended actions of the system, the prevention of undesirable system function actions, and the provision of outputs that are in turn used by other systems. For instance, the supply of electrical power by the aircraft is a system-level function. The power supply within equipment is not a system-level function.

From the function allocations and the associated Failure Condition Classifications, further specific system requirements necessary to achieve the safety objectives are determined. Derived requirements and additional assumptions will emerge during this phase as the consequences of the various combinations of functions and allocations to systems are considered. These, in turn, may alter the aircraft-level function requirements.

The output of this activity is a set of requirements for each aircraft system together with associated interfaces, including safety requirements and development assurance levels from the PASA process. The interfaces are defined with each input having a source and each output having a destination.

4.5 Development of System Architecture and Allocation of System Requirements to Items

In practice, system architecture development and the allocation of system requirements to items are tightly coupled and iterative processes. Requirements arising from allocation may be system-related or item-related. With each cycle, the identification and understanding of derived requirements increases and the rationale for the allocation of system-level requirements to items becomes clearer. The process is complete when all requirements can be accommodated within the final architecture. The development of the system architecture and the allocation of requirements to items ensures that the items perform all intended system functions.

The system architecture establishes the structure and boundaries within which specific item designs are implemented to meet the established requirements. More than one candidate system architecture may be considered for implementation. These candidate system architectures may be evaluated using such factors as technology readiness, implementation schedules, producibility, contractual obligations, economics, prior experience, and industry precedence. The candidate architectures are then iteratively evaluated using functional and performance analyses. In particular, the PASA and PSSA processes establish feasibility with respect to top-level safety objectives assigned to each system. PASA/PSSA activities are summarized in 5.1.2 and 5.1.4, respectively.

Requirements stemming from technology, architecture, system, equipment, and item interfaces, system constraints (physical, environmental, etc.), integration, and implementation choices become more clearly visible as work on the system architecture progresses.

The output of this allocation effort is a system architecture with requirements allocated to items, including safety requirements and development assurance levels from the PASA/PSSA processes.

4.6 Implementation

Implementation has four primary points:

a. Information flow between the system process, which includes development assurance and safety assessment processes, to and from the item-level processes

b. Item design/build

c. Item integration and verification

d. Aircraft/system integration and verification

These are further discussed in the next sub-sections.

4.6.1 Information Flow—System Process to and from Item Processes

4.6.1.1 Information Flow from System Process to Item Processes

System requirements are decomposed and allocated to items as determined by the system architecture. The decomposition and allocation of requirements to items follows the system process. The interface between the system process and the item processes is dealt with in the following sections.

The point where requirements are allocated to items is also the point where the guidelines of this document transition to the guidance of DO-178C/ED-12C (for software), DO-254/ED-80 (for electronic hardware), and other existing industry guidelines. This document provides guidelines for architecture, development assurance level, and functional decomposition including redundancy management. This means that the requirement allocation to items has been reached at the point when architecture, redundancy management, and requirement decomposition are complete.

The following data is passed to the item processes as part of the requirements allocation:

a. Requirements allocated to hardware item(s)

b. Requirements allocated to software item(s)

c. Development assurance level(s) for item(s) and a description of associated failure condition(s), if applicable

d. Allocated failure rates and exposure interval(s) for hardware failures

e. System description

f. Design constraints, including function isolation, separation, data/models of other external interfacing elements, partitioning requirements, and any item development independence requirements

g. System verification activities to be performed at the item development level, as applicable

h. Evidence of the acceptability by the system process of any data provided by the item processes to the system process on which any activity or assessment has been conducted by the system process; an example of such an activity is the system process evaluation of derived requirements provided by the item processes to determine if there is any higher-level functional or safety impact (see 5.3.3)

4.6.1.2 Information Flow from Item Processes to System Process

The information listed below should be included in the data passed to the system process in support of system-level development activities and integral processes:

a. Derived item requirements which may have a higher-level functional or safety impact (see 5.3.3)

b. Description of the implemented item architecture sufficient to show the achieved independence and failure containment capabilities (e.g., hardware segregation, software partitioning)

c. Evidence of system/item verification activities performed at the item development level, if any

d. Hardware failure rates, failure detection coverage, common cause considerations, and latency intervals, for incorporation in the System Safety Assessment (SSA)

e. Problem or change documentation that may impact system or item requirements, to be evaluated against the system or item requirements or the safety assessments

f. Any limitations of use, configuration identification/status constraints, or performance/timing/accuracy characteristic

g. Data to facilitate integration of the items into the system (e.g., installation drawings, schematics, parts lists)

h. Details of proposed item verification activities to be performed during system-level verification

Additionally, evidence should be made available that the process activities consistent with the assigned Item Development Assurance Level(s) have been performed, including any assurance achieved through tools.

4.6.1.3 Information Flow Between Hardware Design Life Cycle and Software Life Cycle Processes

The information below should be passed between the hardware and software life cycle processes. This information should flow via the systems process. This data includes:

a. Requirements needed for hardware/software integration, such as definition of protocols, timing constraints, and addressing schemes for the interface between hardware and software

b. Instances where hardware and software verification activities require coordination

c. Identified incompatibilities between the hardware and the software, which may be part of a reporting and corrective action process

4.6.2 Item Design/Build

The item (e.g., electronic hardware or software) design/build processes should provide traceability to the requirements allocated to items. If item implementation proceeds in parallel with the requirements allocation and architecture definition phases, then sufficient discipline is needed to ensure that derived requirements are captured and that all function requirements are achieved in the implementation.

The outputs of this phase include item (e.g., electronic hardware or software) integration procedures, released hardware drawings, software source code together with related life cycle data, applicable development assurance data, breadboard or prototype hardware, if applicable, and lab/flight test articles. The RTCA/EUROCAE documents referenced in 2.1 provide guidance for the development of electronic hardware and software.

4.6.3 Item Integration and Verification

Depending on the nature of the system and the development process used, initial item integration may occur on breadboards, prototypes, computer emulation, or lab/flight test articles. The output is items under configuration control together with development assurance data and item life cycle data. Detailed procedures should be used to verify that item integration is complete and all item requirements are met.

It may be beneficial to enhance the item integration process through development of interface documents. This would ensure that the integrated items provide compatible functionality (e.g., correctly initialized electronic hardware, memory maps).

4.6.4 Aircraft/System Integration and Verification

Aircraft/system integration and verification are the tasks of ensuring all the aircraft systems operate correctly, both individually and together, as installed on the aircraft.

Normally, systems integration begins with item-by-item integration and progresses to complete system integration. The difficulty of fully anticipating or modeling the aircraft environment at any particular stage in development dictates that integration activities may need to be performed at various phases of implementation (i.e., intra-system, inter-system, aircraft-level). While the confidence of on-the-aircraft integration can be high, more meaningful or cost-effective results often can be achieved in laboratory or simulation environments. Specific procedures for systems integration will vary depending on the capabilities of test facilities, the functional interactions being represented, and the interdependencies between functions/systems being assessed.

In addition to verifying intended functionality, this activity provides an opportunity to identify and address “unintended behaviors.” Previous versions of this document referred to ”unintended functions.” By its definition, a function is an intended behavior, meaning that it was defined to operate in a specific manner. Therefore, “unintended behavior” is used throughout this document.

A strategy/method should be developed to investigate for unintended behaviors, citing the level of testing to be performed (i.e., intra-system, inter-system, aircraft-level) and the types of testing to be performed (e.g., scenario-based testing, targeted testing, opportunistic testing by suitably qualified and experienced personnel, etc.).

Integration affords the opportunity to identify and address unintended behaviors. Such behaviors can arise from issues such as requirements gaps or unanticipated interaction between functional elements. Particular attention during integration should be directed at dedicated testing of features implemented in the design which addresses potential unsafe operating conditions. Examples of mitigating features are monitors, fault isolation means, partitioning and their related or relevant system interfaces. Such tests may be developed from consideration of the following elements (examples only—not a checklist of cases):

a. Testing and/or simulation of failed states developed to challenge architectural protective features (including outside of the operational envelope, as necessary)

b. Operation of individual pilot inputs/combinations of pilot inputs over a wide range of input values and rates

c. Signals out of range, invalid inputs, etc.

d. Normal and abnormal power up sequences

e. Power transients, failures, and abnormal levels

f. Failure conditions including sequential failures

g. External signal abnormal ranges and/or failure conditions

h. Databus disturbances, internal and external

i. Monitor-focused specific tests to expose nuisance susceptibility

During the integration and verification processes, identified deficiencies will be referred back to the appropriate development or integral activity (requirements capture, allocation or validation; implementation; verification, etc.) for resolution, and the process iterated. When all iterations are concluded, the output of this activity is an integrated and verified system, along with the data confirming that the system satisfies all requirements. A summary of verification results obtained will be documented accordingly, including the results of the activities performed to investigate for unintended behaviors.

Although the complete absence of unintended behaviors can never be established, the monitoring for unintended behaviors during requirements-based testing, in conjunction with the guidelines outlined in this section, provides the means to show that a set of system requirements, taken as a group, have been satisfied.

4.7 Summary of Development Assurance Process Outputs

The activities established in the development assurance plan(s) and the results should be summarized. Any deviation from the agreed development assurance plan(s) should be described together with rationale to substantiate the deviation. The summary should include:

a. An outline of the results of the development assurance activities.

b. Confirmation that the activities defined in the development assurance plan(s) have been completed, including details of the configuration for each activity performed, and a description and rationale for any deviations from the development assurance plan(s).

c. Reference to supporting development assurance data as identified in Appendix A, including, but not limited to:

   1. Safety assessment data; see 5.1 and refer to ARP4761A/ED-135

   2. Validation data; see 5.4.7

   3. Verification data; see 5.5.6 which includes the data from activities performed to investigate for unintended behaviors described in 4.6.4

   4. Configuration management data; see 5.6.3

   5. Process assurance data; see 5.7.4

d. Open Problem Reports (OPRs), including:

   1. Identification of each OPR (configuration management number)

   2. Short description of each OPR, including system/safety effect and the mitigation for each OPR that impacts functionality or safety

   3. Classification of each OPR

   4. Mitigation for certification acceptability (justification, why closure of the OPR can be deferred)

   5. Functional limitations and operational restrictions, if any

   6. OPR interrelationships (if needed)

NOTE: Regulatory guidance on OPRs may be applicable (e.g., AMC 20-189/AC 20-189 for the management of OPRs).

5. INTEGRAL PROCESSES

The process elements described in this section are fundamental elements of the overall development process. They have multiple interactions to the process activities in Section 4.

5.1 Safety Assessment

The safety assessment process is used to show compliance with certification requirements and internal safety standards. The process includes specific assessments that are conducted and updated during aircraft/system development. These assessments interact with development processes throughout the development life cycle. The safety assessment process consists of the six principal assessment processes summarized in 5.1.1 through 5.1.6. These principal assessment processes consist 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.

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. The principal methods are Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA), and Common Mode Analysis (CMA); other methods may include Fault Tree Analysis (FTA), Dependency Diagram (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), Failure Mode and Effects Analysis/Summary (FMEA/FMES), and Cascading Effects Analysis (CEA) as required. The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may stand alone or be incorporated into any of the higher-level assessments.

Independence between functions, systems, equipment, or items may be required to satisfy the safety requirements. Therefore, it is necessary to ensure that such independence exists, or that the lack of independence is acceptable. The PRA, ZSA, and CMA provide the methods for evaluation of independence or the identification of specific dependencies due to common cause. These methods may also aid the PASA and PSSA in generation of independence requirements (e.g., physical, installation requirements).

The safety assessment process is detailed in ARP4761A/ED-135.

Figure 6 shows the fundamental relationships between the safety assessment processes and the system development processes. In reality, there are many feedback loops within and among these relationships, though they have been omitted from the figure for clarity. Note: Only those aspects of the methods associated with Common Cause Considerations are shown in the figure; for example, the PRA also covers aspects outside common cause considerations.

The level of detail needed for the various safety assessment activities is dependent on the aircraft-level Failure Condition Classification, the degree of integration, and the complexity of the system implementation. The safety assessment process should be planned and managed so as to provide the necessary assurance that all relevant failure conditions have been identified, and that all significant combinations of failures that could cause those failure conditions have been considered. The safety assessment process is of fundamental importance in establishing appropriate safety objectives for the aircraft and systems and determining that the implementation satisfies these objectives.

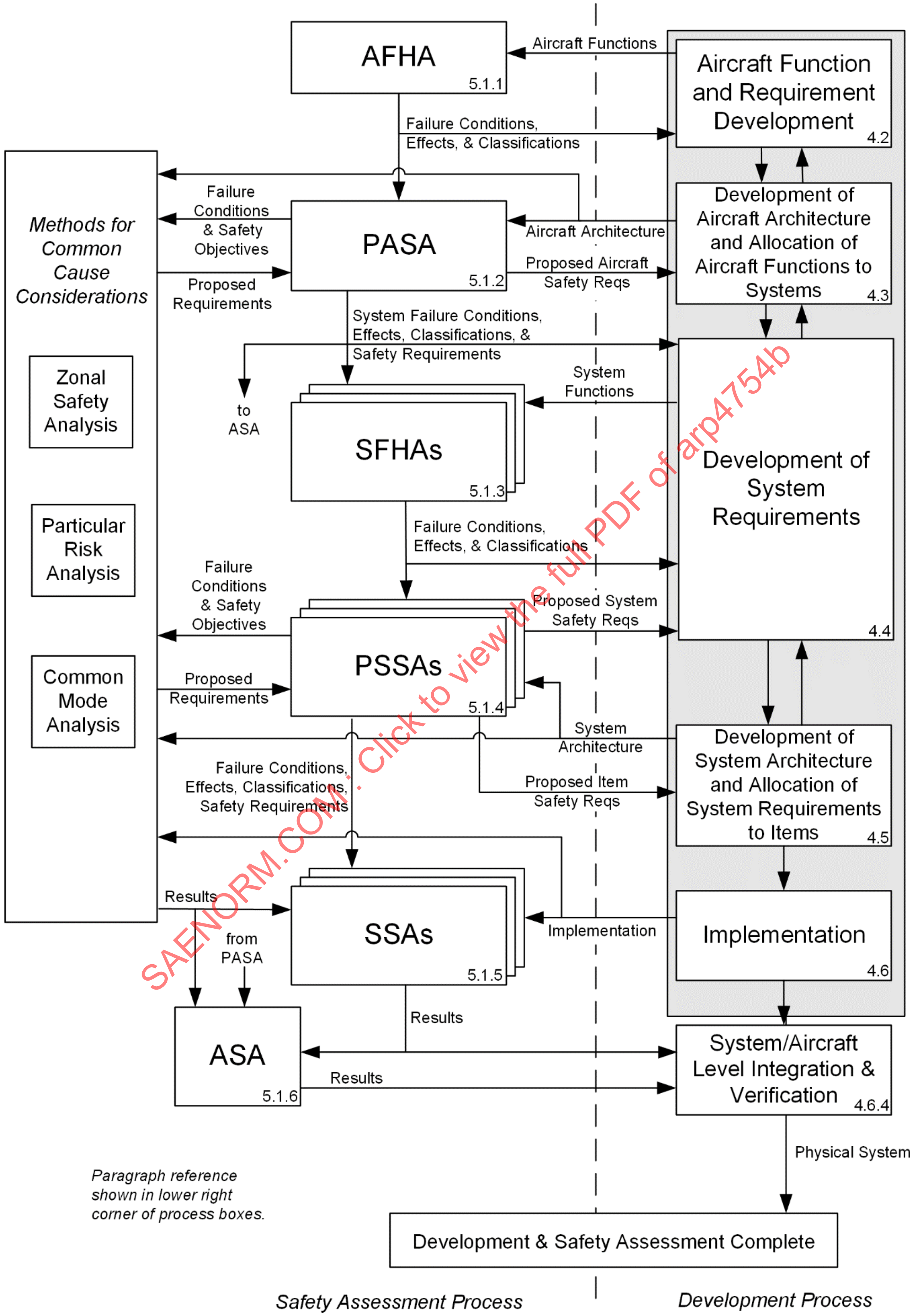

AFHA
5.1.1
Aircraft Functions
Aircraft Function and Requirement Development
4.2
Failure Conditions, Effects, & Classifications
Methods for Common Cause Considerations
Failure Conditions & Safety Objectives
PASA
5.1.2
Aircraft Architecture
Development of Aircraft Architecture and Allocation of Aircraft Functions to Systems
4.3
Proposed Aircraft Safety Reqs
Proposed Requirements
System Failure Conditions, Effects, Classifications, & Safety Requirements
to ASA
System Functions
Zonal Safety Analysis
SFHAs
5.1.3
Development of System Requirements
4.4
Particular Risk Analysis
Failure Conditions, Effects, & Classifications
Failure Conditions & Safety Objectives
Proposed System Safety Reqs
PSSAs
5.1.4
Common Mode Analysis
Proposed Requirements
System Architecture
Development of System Architecture and Allocation of System Requirements to Items
4.5
Failure Conditions, Effects, Classifications, Safety Requirements
Proposed Item Safety Reqs
Results
SSAs
5.1.5
Implementation
Implementation
4.6
from PASA
Results
ASA
5.1.6
Results
System/Aircraft Level Integration & Verification
4.6.4
Physical System
Paragraph reference shown in lower right corner of process boxes.
Development & Safety Assessment Complete
Safety Assessment Process
Development Process

Figure 6 - Safety Assessment process model

5.1.1 Aircraft Functional Hazard Assessment

The AFHA is a process that allows the identification and evaluation of potential hazards related to an aircraft's functions regardless of the details of its design. The objectives of the AFHA process are to identify the failure conditions associated with the aircraft functions.

The objectives of the AFHA process are accomplished by systematically analyzing the aircraft-level functions to identify the failure conditions, determine their effects on the aircraft, crew, and occupants, and then to establish the associated severity classification. The classification of these Failure Conditions establishes the safety objectives for the aircraft. Assumptions made during the AFHA process should be captured and confirmed to be correct.

Failure conditions and associated safety objectives may be monitored through the development process to track that the design implementation is satisfying the safety objectives.

Appendix A of ARP4761A/ED-135 provides guidelines on how to perform an AFHA.

5.1.2 Preliminary Aircraft Safety Assessment

The PASA is a systematic, comprehensive evaluation of a proposed aircraft architecture to determine how failures, errors, or external events can lead to aircraft-level failure conditions identified by the AFHA and how the aircraft-level safety objectives can be met. The objectives of the PASA process are to evaluate the proposed architecture against the safety objectives, and to propose aircraft-level safety requirements and assumptions.

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 aircraft-level safety objectives can be met. The PASA process interacts with the development process by evaluating the aircraft architecture against aircraft-level safety objectives and identifies the need for specific aircraft-level and system-level safety requirements. Just as the development process is iterative, the PASA process is iterative throughout the development cycle. The PASA process may use various qualitative and/or quantitative safety analysis methods. Common cause considerations are taken into account in the PASA process. 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 the independence requirements and Function Development Assurance Level (FDAL) assignments for the associated aircraft functions. Once the aircraft-level safety requirements have been identified through the PASA process and the implementing systems' designs mature, the ASA process may be initiated.

Appendix B of ARP4761A/ED-135 provides guidelines on how to perform a PASA.

5.1.3 System Functional Hazard Assessment

The SFHA is a systematic process that allows the identification and evaluation of potential hazards related to a system's functions regardless of the details of its implementation. It is performed at the beginning of the system development process and re-evaluated any time changes are made to the system functions. The objectives of the SFHA process are to identify and classify the failure conditions associated with the system functions.

The objectives of the SFHA process are accomplished by systematically analyzing the system-level functions to identify the failure conditions, determine their effects on the aircraft, crew, and occupants, and then to establish the associated severity classification. Crew awareness, flight phase, and environmental and operational conditions are also considered in the assessment. The classification of these failure conditions establishes the safety objectives for the system. Assumptions made during the SFHA process should be captured and confirmed to be correct.

Failure conditions and associated safety objectives may be monitored through the development process to track that the design implementation is satisfying the safety objectives.

Appendix C of ARP4761A/ED-135 provides guidelines on how to perform an SFHA.

5.1.4 Preliminary System Safety Assessment

The PSSA process is a systematic evaluation of a proposed system architecture to determine how failures, errors, or external events can lead to system-level failure conditions identified by the SFHA and how the system-level safety objectives can be met. The objectives of the PSSA process are to evaluate the proposed system architecture against the safety objectives and allocated requirements from PASA, and to propose system-level safety requirements and assumptions.

Through the PSSA process, safety requirements for system, subsystem, and items are identified to guide the architecture development as necessary to meet the safety objectives and requirements. The PSSA process may use various safety analysis methods to determine these requirements. The PSSA also identifies the necessary FDAL and Item Development Assurance Level (IDAL) assignments for the system functions and items.

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/intervals.

The PSSA process is interactive and associated with the design definition. Just as the development process is iterative, the PSSA process is iterative. The PSSA process starts in the early phases of design with the evaluation of the system architecture to identify and propose system-level safety requirements. System-level safety requirements are then allocated to subsystems and finally subsystem requirements are allocated to equipment/items. 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 their associated exposure times. Once the system-level safety requirements have been identified through the PSSA process and the implementing subsystems/equipment/items' designs mature, the SSA process may be initiated.

Appendix D of ARP4761A/ED-135 provides guidelines on how to perform a PSSA.

5.1.5 System Safety Assessment

The SSA is a systematic, comprehensive evaluation of the implemented system. The objective of the SSA process is to confirm that the safety objectives and relevant safety requirements are satisfied. The difference between the PSSA and the SSA is that the PSSA is a process to evaluate proposed architectures and identify safety requirements, whereas the SSA is a process to verify 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 relevant safety requirements identified in the PSSA. The SSA process documentation includes results of the related 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, hardware reliability requirements and architectural requirements are verified against the safety requirements identified in the PSSA process.

The SSA establishes maximum exposure times for latent failures to be considered for aspects of the aircraft operation and maintenance.

Appendix E of ARP4761A/ED-135 provides guidelines on how to perform an SSA.

5.1.6 Aircraft Safety Assessment

The ASA is a systematic, comprehensive evaluation of the complete aircraft. The objective of the ASA process is to confirm that the safety objectives and relevant safety requirements are satisfied. The difference between a PASA and an ASA is that a PASA is a process 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 ASA 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 includes 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 and checks for consistency of those results with PASA and SSA results.

Appendix F of ARP4761A/ED-135 provides guidelines on how to perform an ASA.

5.1.7 Safety Program Plan

For appropriate management of the safety assessment process, a safety program plan should be created. The safety program plan(s) should define the scope and the content of the safety activities that are applicable at the aircraft and system levels. The following provides an overview of topics that should be covered, unless otherwise justified, through the safety program plan to support development assurance:

a. Identify the input data for the safety assessment process

b. Identify applicable safety standards

c. Identify the project safety organization and define responsibilities within this organization and its relationship with partners and/or suppliers with respect to the safety process

d. Describe the applicable safety assessment activities and their outputs, including the associated deliverables

e. Define the key project milestones for which safety process outputs are required

f. Include the principles of the management and validation of the safety objectives, assumptions, and safety requirements, and the verification that the design meets those requirements

g. Identify the links with the other appropriate plans (e.g., validation plan, verification plan, process assurance plan)

The safety program plan may address additional safety topics beyond those that support development assurance, including company policies, company procedures, and specific safety details necessary to support certification. Appendix B provides an example for organizing the contents of an aircraft-level safety program plan.

5.1.8 Safety-Related Flight Operations or Maintenance Tasks

The safety assessment may rely on or take into consideration flight crew, aircraft operations, or maintenance personnel actions. The tasks and procedures assumed to be performed may be necessary to ensure safety requirements are met. Where human performed tasks or limitations are relied on to ensure safety or to form part of the certification substantiation, they should be identified and recorded in the certification data. Regulatory guidance on specific types of tasks and limitations may be applicable (e.g., AC 25-19A/AMC 25-19 for Certification Maintenance Requirements on transport category airplanes).

5.1.9 Relationship with In-Service Safety

A process for accomplishing in-service safety assessment is described in ARP5150A and ARP5151A or in other documents, such as the guidance material of EASA Part 21 (GM21) when required by applicable regulation. These documents contain an in-depth study of the processes used to establish and maintain surveillance of safety concerns on in-service aircraft (i.e., continued airworthiness) and to resolve those issues and document the resolutions.

Taken as a whole, ARP4761A/ED-135 and ARP5150A (or ARP5151A or other applicable guidance material) encompass the safety assessment process for the entire life cycle of the civil aircraft and its systems and items from conceptual design to obsolescence.

Safety is not self-sustaining. When an aircraft is delivered it has an initial level of safety as identified by the SSA(s) and ASA. As aircraft are operated, the level of safety is maintained through a continuing process of monitoring service experience, identifying safety-related issues and opportunities, and then addressing these issues through appropriate product or procedure changes.

The in-service safety assessment process includes the following:

a. Maintain the airworthiness (certification) of the aircraft

b. Maintain the safety of the aircraft

c. Improve the safety of the aircraft

The in-service safety assessment process is expected to be continuous, iterative, and closed-loop. When an event is identified, assessed, and action implemented, the monitoring continues to validate the effectiveness of the action.

5.2 Development Assurance Level Assignment

The prerequisites needed for a good understanding of this section are the definitions of function, failure condition, failure, error, and independence.

Development errors are addressed by instituting a development assurance process. The development assurance process establishes confidence that aircraft and system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety. The development assurance level expresses the rigor applied to the development process to limit, to a level acceptable for safety, the likelihood of errors occurring during the development process of aircraft/system functions and items that have an adverse safety effect if they are exposed in service.

The development assurance level of an aircraft/system function or item applies not only to the development process of this aircraft/system function or item, but also to the development of the interfaces with all the other aircraft/system functions or items interrelated to the extent that they may affect the function or item being examined.

The development assurance level is assigned depending on the severity classification of failure conditions considering the possible independence between development processes that can limit the consequences of development errors. The more severe the Failure Condition Classification, the greater the development assurance level necessary to limit the likelihood of development errors to an acceptable level of confidence.

Specific considerations for how to conduct development assurance level assignment are described in ARP4761A/ED-135.

5.2.1 General Principles—Introduction to Development Assurance Level Assignment

The general principles for development assurance level assignment taking into account top-level failure conditions severity classification are described in the following paragraphs:

When a Catastrophic Failure Condition (FC) is involved, the assignment principles are:

- If a Catastrophic FC could result from a possible development error in an aircraft/system function or item, then the associated development assurance process is assigned level A.

- If a Catastrophic FC could result from a combination of possible development errors between two or more independent aircraft/system functions or items, then either one development assurance process is assigned level A, or two development assurance processes are assigned at least level B. The other independent aircraft/system functions or items are assigned no lower than development assurance level C. The development assurance process establishing that the two or more independent aircraft/system functions or items are in fact independent should remain level A.

When a Hazardous FC is involved, the assignment principles are:

- If a Hazardous FC could result from a possible development error in an aircraft/system function or item, then the associated development assurance process is assigned at least level B.

- If a Hazardous FC could result from a combination of possible development errors between two or more independent aircraft/system functions or items, then either one development assurance process is assigned at least level B, or two development assurance processes are assigned at least level C. The other independent aircraft/system functions or items are assigned no lower than development assurance level D. The development assurance process establishing that the two or more independent aircraft/system functions or items are in fact independent should remain level B.

When a Major FC is involved, the assignment principles are:

- If a Major FC could result from a possible development error in an aircraft/system function or item, then the associated development assurance process is assigned at least level C.

- If a Major FC could result from a combination of possible development errors between two or more independent aircraft/system functions or items, then one development assurance process is assigned at least level C, or two development assurance processes are assigned at least level D. The development assurance process establishing that the two or more independent aircraft/system functions or items are in fact independent should remain level C.

When a Minor FC is involved, the assignment principles are:

- If a Minor FC could result from a possible development error in an aircraft/system function or item, then the associated development assurance process is assigned at least level D.

- If a Minor FC could result from a combination of possible development errors between two or more independent aircraft/system functions or items, then one development assurance process is assigned at least level D.

When a No Safety Effect FC is involved, the assignment principle is:

- If a No Safety Effect FC could result from one or a combination of possible development error(s) in an aircraft/system function or item, then the associated development assurance process(es) may be assigned level E.

5.2.2 FDAL and IDAL

To address the general principles during the development phase, two phases can be identified with two different types of development processes: function development phase and item development phase.

Function development phase: During this phase, requirements for functions are developed and allocated to items. The requirement development process includes validation (assurance of completeness and correctness) of the set of requirements. The level of rigor of the development process for function requirement development is given by the development assurance level of the function hereafter called FDAL. The objectives to be met for functions and requirements are provided within this document; Appendix A gives the applicability of these objectives for each FDAL.

Item development phase: During this phase items are developed. The level of rigor of the development process for items is given by the electronic hardware or software assurance level called hereafter IDAL. In the context of IDAL assignment, an item does not contain architectural features to be used for credit in mitigating potential development errors within itself. Architectural features to be used for credit in mitigating potential development errors should include design independence between two or more items when assigning their IDAL. The objectives to be met, dependent on the IDAL, are given in DO-254/ED-80 for electronic hardware and DO-178C/ED-12C for software. The objectives to be met for the integration of electronic hardware and software are provided by this document. Note that the boundaries between systems and items might not coincide with the boundaries between aircraft manufacturers and suppliers, or between suppliers and sub-tier suppliers or with physical packaging.

The design of simpler hardware items (e.g., mechanical hardware, electro-mechanical devices, electro valves, or servo valves), including the identification of all their failure modes, can be fully assured by a combination of testing and analysis. Such simpler hardware items do not have an IDAL, although the system function using them will have an FDAL. Validation and verification activities for these items should be consistent with established and accepted development processes and techniques for these types of hardware items.

5.2.3 Detailed FDAL and IDAL Assignment Guidelines

The AFHA and SFHA processes are used to identify failure conditions in a systematic manner early in system development. The functions, their failure conditions and classifications, and the proposed architectures to implement those functions are assessed to assign development assurance levels in the PASA and PSSA processes, as shown in Figure 7. Development assurance levels are assigned to aircraft/system functions and items so that the appropriate validation and verification processes are invoked to minimize the potential for errors in their development processes. The assigned development assurance level does not imply particular random hardware failure probabilities, i.e., the probability analysis of the failure condition is also required when necessary to confirm that the safety requirements are satisfied. The level of rigor in the development assurance of an aircraft/system function or item is established by assignment of a development assurance level, be it a FDAL to a function or IDAL to an item.

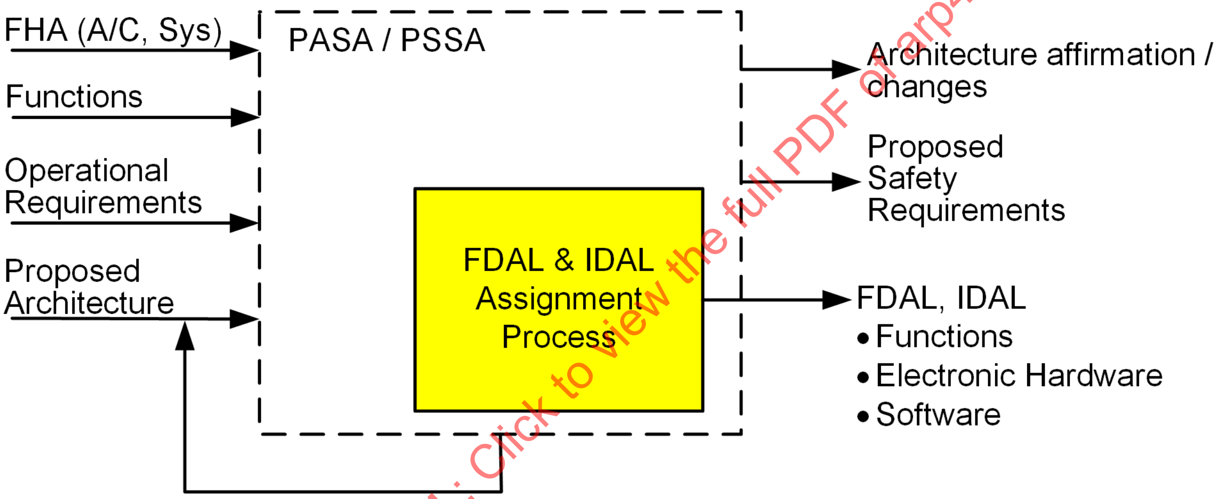


Figure 7 - FDAL/IDAL assignment process

Interactions of system functions making up an aircraft function need to be assessed at the FDAL of the aircraft function. Interactions of items making up a system function need to be assessed at the higher of the FDALs of the aircraft and system functions.

The development assurance level assignment process begins with FDAL assignment to the functions involved in the aircraft's and/or systems' FHA failure conditions (called herein top-level failure conditions).

An FDAL is assigned to the top-level function, based on its most severe top-level Failure Condition Classification. This is performed for each function in the aircraft and system FHAs in accordance with Table 2. This assignment establishes the rigor for the applicable development assurance processes described in this document.

Table 2 - Top-level function FDAL assignment

Top-Level Failure Condition Severity Classification	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No Safety Effect	E

For detailed FDAL and IDAL assignment considerations, such as the role of simple hardware items or external events, refer to ARP4761A/ED-135.

5.2.3.1 FDAL Assignment without System Architecture Consideration

Table 2 can be used to directly assign the development assurance levels for everything under that function (i.e., FDAL for all the functions supporting the top-level Function, and IDAL for all items in the architecture at the same level as the top-level function FDAL). When the mitigation strategy for systematic errors is a single FDAL A development process for a Catastrophic failure condition, then the applicant may be required to substantiate that the development process for that member has sufficient independent validation/verification activities, techniques, and completion criteria to provide confidence that potential development error(s) having a Catastrophic effect have been removed or mitigated. In this case, the development assurance process needs to provide confidence that development error(s) will be detected and resolved within the process rather than relying on independence within the architecture.

5.2.3.2 FDAL Assignment with System Architecture Consideration

Once an FDAL is assigned to a top-level function based on the top-level failure conditions' severity classification, the architecture of the system functions involved in that top-level function is examined to determine the development assurance levels of those system functions. This section describes a process for determining the FDALs for the supporting system functions.

During allocation of a top-level function into two or more independent sub-functions (i.e., one sub-function by itself cannot cause the top-level hazard), it is possible to assign an FDAL of at least one of the sub-functions lower than the top-level function's FDAL. However, there may also be functional allocations where the FDAL assignment of at least one of the sub-functions may be as high as the level of the top hazard. Several different FDAL assignment cases are discussed in ARP4761A/ED-135.

The prerequisites of FDAL (and IDAL) assignment are the details of the Functional Failure Set (FFS), its members, and their independence.

A systematic approach to assigning development assurance levels, when considering system architectures, is to use the concept of FFSs. System Safety Assessment processes are used to identify all the FFSs that lead to each top-level failure condition and the members of each FFS. The FFSs for a given failure condition may be identified by using qualitative safety analyses, such as FTA (refer to ARP4761A/ED-135, Appendix G) or DD (refer to ARP4761A/ED-135, Appendix H).

Conceptually, for FDAL (and subsequently IDAL) assignment purposes, an FFS is analogous to a fault tree minimal cut set (as defined in ARP4761A/ED-135). More specifically, an FFS is a set of one or more members whose potential development errors combine to result in a top-level failure condition; in contrast, a fault tree minimal cut set is a set of one or more failures that combine to result in a top-level failure condition. The FFS is used to assign the appropriate rigor to mitigate the potential development errors. A failure condition may have a single FFS or multiple FFSs, and each FFS may contain either a single or multiple members.

5.2.3.2.1 Independence Attributes

Independence between aircraft/system functions or items can protect against potential common development errors and is a fundamental attribute to consider when assigning development assurance levels.

The intent of independence attributes is to have sufficient confidence that the likelihood of a common development error is minimized between two or more members commensurate with the severity of the Failure Condition Classification.

Four types of independence attributes are defined: functional independence, item development independence, physical independence, and process independence. For the purposes of assigning FDAL and IDAL, functional independence and item development independence are considered.

Physical independence and process independence are not used in FDAL and IDAL assignment. Physical independence provides mitigation against undesirable effects caused by failures and events but is not intended to mitigate development errors. After the development assurance level is assigned, process independence may be used to minimize the likelihood of development errors.

5.2.3.2.1.1 Functional Independence

Functional independence is an attribute where the functions are different in order to minimize the likelihood of a common development error. For example, allocation of two different sets of functional requirements could minimize the likelihood of the same error being present in both. Analysis should show that the requirements have been subjected to a sufficiently thorough examination, at a level commensurate with the severity of the failure condition being examined, and no adverse commonality was identified.

Functional independence minimizes the likelihood of common sources of error associated with:

- Common requirements errors
- Common requirement interpretation errors

Examples of functional independence where different requirements are employed to implement/achieve an aircraft or system-level function and may minimize the likelihood of errors leading to the relevant top-level failure conditions include:

- Decelerate on the ground (wheel brakes, engine thrust reversers and ground spoilers)
- Control direction on ground (nose wheel steering, differential braking, and the rudder at high speed)
- Control aircraft in the air (flight control surfaces and vectored thrust)
- Provide relative aircraft position (communication and navigation)
- Navigate (Global Positioning System and Inertial Reference System)
- Provide Angle of Attack (vane and synthetic Angle of Attack computed from airspeed and inertial data)
- Provide fuel quantity (engine fuel flow rate and tank fuel probes)

The requirements necessary to enforce/maintain functional independence should be managed throughout the development cycle and may lead to constraints on item development and system architecture.

Functional independence is substantiated when the common sources of error between multiple sets of requirements have been minimized at a level of rigor commensurate with the top-level failure condition severity classification. This should be substantiated at all levels of abstraction or requirement decomposition.

5.2.3.2.1.2 Item Development Independence

Item development independence is an attribute where the items are different in order to minimize the likelihood of a common development error between the individually developed items.

Examples of errors that may be mitigated by item development independence:

- Software design error (including software requirements, software architecture, etc.)
- Software development error (including software development process, software configuration control, etc.)
- Hardware design error (including hardware requirements, hardware architecture, etc.)
- Hardware development error (including hardware development process, hardware configuration control, etc.)
- Electronic hardware tool errors (Hardware Description Language coders, layout tools, etc.)
- Software development tool errors (compiler, linker, etc.)

Examples of means to achieve item development independence:

- Different operating systems
- Different computer/software languages
- Different microprocessors
- Different teams and processes to drive different designs

Item development independence is substantiated when the common sources of error between multiple items have been minimized. Substantiation is accomplished by applying a level of rigor commensurate with the severity of the top-level Failure Condition Classification with considerations such as the state-of-the-art and in-service experience. Requirements for independence between items should be allocated to those items from the system as needed. If the presence of common error sources between the items cannot be minimized, then item development independence cannot be claimed.

5.2.3.2.1.3 Physical Independence

Physical Independence is used to minimize 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. Variations in material properties and manufacturing tolerances can prevent two like items from failing at the exact same time. Physical separation can protect against some, but not all event-driven threats. For example, it may protect against ballistic FOD, but not a common mode icing condition.

5.2.3.2.1.4 Process Independence

Process Independence 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. After the development assurance level is assigned, process independence may be used to minimize the likelihood of development errors.

5.2.3.2.1.5 Summary of Functional and Item Development Independence

Functional independence ensures that the function requirements should not suffer from a common error, whereas item development independence ensures that item designs on which the function(s) is/are implemented should not suffer from a common development error.

5.2.3.2.2 FDAL and IDAL Assignment Process Overview

FDAL and IDAL assignment is a top-down process starting with the failure condition severity classification from the FHA and assigning the top-level FDAL in the PASA/PSSA. After decomposing the top-level function into sub-functions, the sub-functions' FDALs are assigned. Each sub-function is then decomposed and/or allocated further into items and then items' IDALs are assigned. The FDAL and IDAL assignment process should be applied when developing new functions and new items. Nevertheless, experience identifies that development often makes use of aircraft/system functions and items that have been developed and certificated for previous applications (see 5.3.1.11). When considering re-use of previously developed aircraft/system functions and items, their FDAL and IDAL should be shown to address the general principles defined in 5.2.1. Specific considerations are described in the FDAL and IDAL assignment process found in ARP4761A/ED-135.

Once an FDAL is assigned to the top-level aircraft function based on the top-level failure condition severity classification, the architecture implementing the system functions involved in the top-level failure condition is examined to delineate the development assurance levels of those system functions.

If it can be shown that the aircraft or system architecture provides containment for the effects of development errors by two or more independent members, development assurance levels may be assigned with consideration of the containment provided by the architecture. Safety assessment processes are used to identify the members within the FFSs that lead to the top-level failure conditions. The identification of the FFS is the subject of PASA/PSSA and the independence attributes of the FFS are considered in CMA. A top-level failure condition may have more than one FFS.

The level of rigor for substantiating the independence among the members of the FFS is the same FDAL assigned to the top-level failure condition per Table 2. The members within a given FFS may be assigned their own FDALs which may be lower than the top-level failure condition severity classification, provided the functional independence attribute is satisfied. Interactions of systems making up an aircraft function need to be assessed at the FDAL of the aircraft function, including substantiation of the asserted functional independence.

The general principles (see 5.2.1) provide the guideline for assigning FDAL to member(s) within an FFS relative to the severity classification of a given top-level failure condition. An example process of entering and navigating through the General Principles is presented in ARP4761A/ED-135. The process is repeated for all top-level failure conditions for each function, and then the most stringent FDAL is assigned to that function in consideration of its role in all its failure conditions. The choice of assignment per these general principles is at the discretion of the certification applicant based on what option is considered most appropriate to address the identified failure conditions.

The IDAL assignment always follows the FDAL process. When the system architectures are refined down to the item level, the FDAL is assigned to an FFS member using the general principles. Care should be made to enter into the IDAL assignment process consistent with the FDAL assignment approach relative to the top-level failure condition. ARP4761A/ED-135 provides process description to maintain this consistency. The assignment becomes the IDAL of the related item. This IDAL will be used as an input for the application of DO-178C/ED-12C (software development assurance) or DO-254/ED-80 (electronic hardware design assurance).

For IDAL assignment, the options available in the general principles related to the top-level Failure Condition Classification may be used, provided the FFS has item development independence. However, whichever option is chosen, the final FDAL and IDAL combination should be in accordance with the general principles of 5.2.1 and the general cases presented in ARP4761A/ED-135.

5.3 Requirements Capture

The aircraft development process includes the identification of aircraft/system functions and establishing the requirements associated with these functions. These functions, including functional interfaces and corresponding requirements to meet safety objectives, form the basis for establishing the architecture. Choices made and problems encountered during implementation are a primary source for derived requirements and may lead to identification of new system requirements to meet safety objectives.

Plans and standards addressing requirement capture should be developed to establish consistency across the set of requirements, particularly when using model requirement capture formats, and ensure communication across the development team of requirement capture expectations.

When a modeling approach is planned to be used to represent requirements, the planning activity should:

- Identify the use of models/modeling.

- Identify the intended tools and their usage during the development.

- Define modeling standards and libraries in order to establish a common understanding of the use of the models based on the modeling language to be used. Model contents should be in a readable form. Means should be provided to unambiguously identify symbols or names relative to the actual signals and interfaces represented. The model should be developed in a layered manner. For example, subsets of model elements which may be used more than once may be handled and represented either as a unit or as the full contents.

System models may or may not support the software/hardware development processes. If these models are further developed such that they can be used to capture item requirements and then directly used to produce embedded code (software/Hardware Description Language), this process should also apply DO-178C/ED-12C and DO-254/ED-80 from when the system requirements are allocated to items until the software or hardware is returned to the system processes for system verification. Refer to DO-331/ED-218 for more software model-based development guidelines.

5.3.1 Classes of Requirements

Different classes of requirements should be considered at various phases of the development activities (i.e., aircraft, system and item). Requirement classes may not be mutually exclusive (i.e., a requirement may be associated with multiple requirement classes). The sub-sections that follow outline common classes of requirements; additional classes may exist.

5.3.1.1 Safety Requirements

Safety requirements are those which are necessary to achieve either a safety objective or satisfy a constraint established by the safety process. Safety requirements may exist at the aircraft, system, and item levels. Types of safety requirements may include independence, probability, availability, integrity, monitoring, operational, and maintenance requirements.

Safety requirements are identified by the safety assessment processes as described in 5.1.

Safety requirements should be uniquely identified to ensure visibility through the levels of development.

5.3.1.2 Functional Requirements

Functional requirements are those necessary to obtain the intended behavior of the system under the conditions specified. They are a combination of customer desires, operational constraints, regulatory restrictions, and implementation realities. These requirements define all significant aspects of the system under consideration. Regardless of the original source, all functions should be evaluated for their safety-related attributes.

5.3.1.3 Customer Requirements

Customer requirements will vary with the type of aircraft, the specific function, or the type of system under consideration. Requirements may include those associated with the operator's intended payload, route system, Air Traffic Management, operating practices, maintenance concepts, and desired features.

5.3.1.4 Operational Requirements

Operational requirements define the interfaces between the flight crew and each functional system, the maintenance crew and each aircraft system, and various other aircraft support people and related functions or equipment. Actions, decisions, information requirements, and timing constitute the bulk of the operational requirements. Both normal and non-normal circumstances need to be considered when defining operational requirements.

5.3.1.5 Performance Requirements

Performance requirements define those attributes of the function or system that make it useful to the aircraft and its operation. In addition to defining the type of performance expected, performance requirements include function specifics such as: accuracy, fidelity, range, resolution, speed, and response times.

5.3.1.6 Physical and Installation Requirements

Physical and installation requirements relate the physical attributes of the system to the aircraft environment. They may include size, mounting provisions, power, cooling, environmental restrictions, visibility, access, adjustment, handling, and storage. Production constraints may also play a role in establishing these requirements.

5.3.1.7 Maintainability Requirements

Maintainability requirements include scheduled and unscheduled maintenance requirements and any links to specific safety-related functions. Factors such as the percentage of failures that are detectable and the percentage of failures that can be isolated may also be important. Provisions for external test equipment signals and connections should be defined in these requirements.

5.3.1.8 Interface Requirements

Interface requirements include the physical system, equipment, and item interconnections along with the relevant characteristics of the specific information communicated. The interfaces should be defined with all inputs having a source and all output destinations defined. The interface descriptions should fully describe the behavior of the signals.

5.3.1.9 Certification Requirements

Additional functions, functional attributes, or implementations may be required by certification regulations or may be necessary to show compliance with certification regulations. Requirements of this class should be defined and agreed upon with the appropriate Certification Authorities.

5.3.1.10 Derived Requirements

At each phase of the development activity, design decisions are made as to how particular requirements or groups of requirements are to be met. The consequences of these design decisions become requirements for the next phase of the development. Since these requirements result from the design process itself, they may introduce behaviors or characteristics beyond those specified in higher-level requirements and are referred to as derived requirements.

Derived requirements should be examined to determine which functions they support so that the appropriate Failure Condition Classification can be assigned, and the requirement validated. See 5.3.3 for the evaluation of derived requirements.

For example, derived requirements may result from the decision to select a separate power supply for equipment performing a specific function. The requirements for the power supply, including the safety requirements, are derived requirements. The Failure Condition Classification(s) associated with the function supported by the power supply determines the necessary development assurance level.

Derived requirements may also result from architecture choices. For example, selecting a triplex architecture for achieving a high integrity functional objective would have different consequences and different derived requirements from selection of a dual monitored architecture for achievement of the same objective.

Derived requirements may result from a design decision to isolate function implementations having more severe Failure Condition Classifications from the failure effects of systems having less severe Failure Condition Classifications.

Derived requirements also include those defining the electronic hardware-software interface. Some of these requirements may be significant at the system level. The remainder, dealing with detailed aspects of the electronic hardware-software interface, may be handled under the guidelines of DO-178C/ED-12C and DO-254/ED-80.

Derived requirements should be captured and treated in a manner consistent with other requirements applicable at that development phase. Derived requirements should include rationale and/or references to applicable design standards.

5.3.1.11 Re-Use of Systems, Equipment, or Items from Previously Certificated Products

Systems, equipment, and items that have been used on other aircraft are often reused in new or derivative aircraft. The maturity of these systems, equipment, and items has benefit, but it should not be assumed that they meet the requirements of the new installation. Even if no design changes are to be made to the system, equipment, or item, the requirements to which the system, equipment, or item was certificated should be validated according to the new application and modified as necessary. Assumptions from the previously certificated aircraft should be managed for the new or derivative aircraft (see 5.4.2.4). Derived requirements, compatibility of the interfaces, and the operational environment should be validated as well. Care should be taken in interface definitions that may be broad and may have been met in an earlier application but may not be met in the re-use instance due to considerations such as cable loading or bus termination conventions.

Verification activities should then be carried out against these requirements, including integration with the aircraft as required.

See Section 6 for more information.

5.3.2 Capturing Safety Requirements from the Safety Analyses

The types of safety requirements for each function, whether at the aircraft, system, equipment, or item levels, are typically the independence requirements, probabilistic availability and integrity requirements, no single failure criteria, monitor performance requirements, safety or protective features, development assurance levels, and operational and maintenance limitations. The probabilistic requirements are typically handled through a budgeting process.

For a given function, safety requirements are established using the results of the PASA and PSSA. These safety requirements include a straightforward assignment from failure categories based on the consequences of that function's failure. There are circumstances when some combinations need to be considered. These need to be selected in a manner that covers needed combinations without having to consider an exponentially increasing number of irrelevant combinations.

The safety analysis process may also identify assumptions that need to be managed to closure. These assumptions may be about a capability within a system, features in another system, or a future activity (e.g., flight crew or maintenance procedures) that have not yet been defined. Assumptions relating to capabilities within a system can be managed at system level; all other assumptions are managed at aircraft level. Confirmation as to whether the assumption is correct or not should be fed back to the originating safety process. The management of assumptions typically results in, or points to existing, requirements that when successfully verified, provide the evidence that the assumption was confirmed.

5.3.3 Identifying and Evaluating Derived Requirements

Derived requirements should be identified and their functional and safety impact should be evaluated for acceptability at progressively higher levels until it is determined that no further impact is propagated. The methods for identifying and evaluating derived requirements should be documented as part of the development assurance planning process. These methods should align with the objectives of the safety assessment process.

5.3.4 Capturing Maintenance Requirements for In-Service Use

While the requirements used for developing the aircraft and/or systems are being captured, maintenance requirements are also captured to ensure the continued airworthiness of the aircraft throughout its life. These activities, which support the requirements, can then be included in the Instructions for Continued Airworthiness (ICA). The periodic maintenance, inspection, or overhaul that are required to maintain the integrity of the system or structure or to maintain the safety protection features should be captured as maintenance requirements in the ICA. Depending on their criticality, some ICAs may need a higher level of visibility and protection against inadvertent deletion or modification; in such cases, they should be included in the Airworthiness limitations section of the maintenance manual, as appropriate.

5.4 Requirements Validation

Validation of requirements is the process of ensuring that the specified requirements are sufficiently correct and complete so that the product will meet the needs of customers, users, suppliers, maintainers and Certification Authorities, as well as aircraft, system and item developers (e.g., flight crews, as users, may have a need for a certain system behavior for thrust control and a level of performance for that behavior). While the format of the validation effort is left to the developer, a structured process should be defined in the validation plan (see 5.4.7).

Given the importance of effectively capturing requirements that will satisfy these needs, the following guidelines may be helpful:

- Identify the interfaces (i.e., with the aircraft, with other systems, with other equipment, with items, with people, with processes, across organizational or corporate boundaries).

- Identify the individuals that have a primary interest in an interface or a need for an interface.

- Interfaces should be formalized through agreements (e.g., statement of work, plan, manual, requirements document, interface document, legal contract).

- The agreement should define the ground-rules so an interface can be realized. (Who owns which side of the interface; what is the means of identifying problems and correcting them; what is the format or constraints associated with the interface?)

- The agreement should define the interface behaviors that are to be provided when an input is received.

- The agreement should define the background and context of interfaces, to the extent necessary to assess if it is appropriate.

- The provider of data should have visibility to how the interface is going to be used to help ensure, along with the user of the data, that it is fit for purpose.

- An independent reviewer (see 5.4.5) should challenge the assumptions and interpretations of captured requirements with the requirement owner, ideally as they are being captured, in order to ensure that these requirements have the same meaning for the requirement owners and recipients.

Ideally, requirements should be validated before the design implementation commences. However, in practice, particularly for complex and integrated systems, the validation of requirements may not be possible to complete until the system implementation is available and can be tested in its operational context. In consequence, validation is normally a staged process continuing through the development cycle. At each stage, the validation activity provides increasing confidence in the correctness and completeness of the requirements.

The validation process at each level of the requirements hierarchy should involve all relevant technical disciplines, including System Safety. Experience indicates that careful attention to requirements development and validation can identify subtle errors or omissions early in the development cycle and reduce exposure to subsequent redesign or inadequate system performance.

Testing may simultaneously serve the purposes of verification as well as validation when the system implementation is used as part of the requirements validation process. One purpose of this activity is to check that the requirements are met by the implemented system, while a separate purpose is checking that the requirements are appropriate to the context in which the system is operating. Such dual purposes should be reflected by coordination of the verification and validation plans.

5.4.1 Validation Process Objectives

Ensuring correctness and completeness of requirements are the objectives of the requirements validation process (i.e., are we building the right aircraft?).

Examination of requirements to ensure they are both necessary and sufficient is a key aspect of validation. A further objective of the validation process is to limit the potential for unintended behavior in the system or for unintended behavior to be induced in interfacing systems.

5.4.2 Validation Process

Requirements should be validated at each hierarchical level of requirements definition. This includes validation of requirements allocated to aircraft, system, and item levels, and the management of assumptions.

The relationship of validation to system development is shown in Figure 4. An expanded validation process diagram is shown in Figure 8. Inputs to the validation process may include a description of the system (including the operating environment), the system requirements, a definition of system architecture, and the development assurance level.

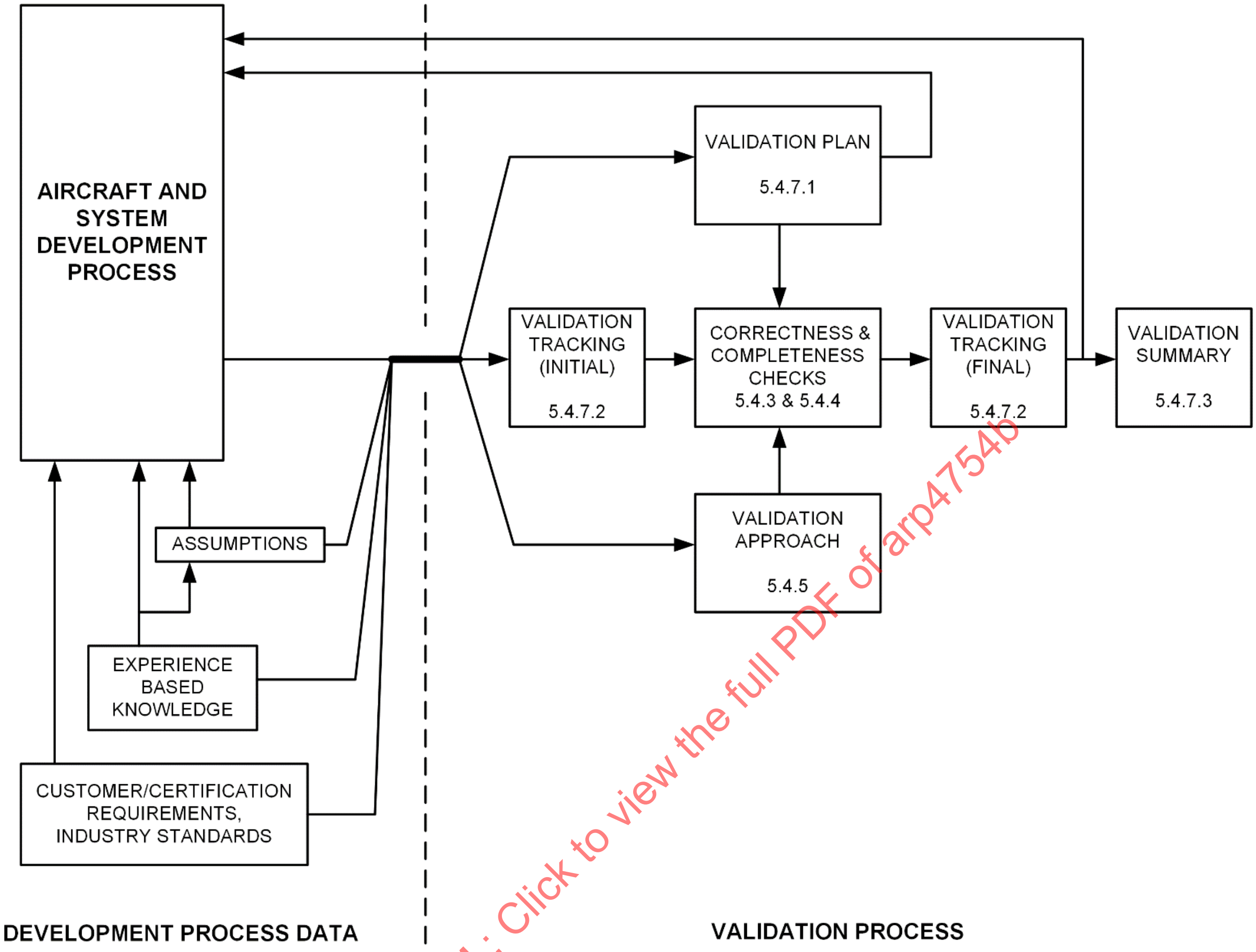

AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS
VALIDATION PLAN 5.4.7.1
VALIDATION TRACKING (INITIAL) 5.4.7.2
CORRECTNESS & COMPLETENESS CHECKS 5.4.3 & 5.4.4
VALIDATION TRACKING (FINAL) 5.4.7.2
VALIDATION SUMMARY 5.4.7.3
ASSUMPTIONS
VALIDATION APPROACH 5.4.5
EXPERIENCE BASED KNOWLEDGE
CUSTOMER/CERTIFICATION REQUIREMENTS, INDUSTRY STANDARDS
DEVELOPMENT PROCESS DATA
VALIDATION PROCESS

Figure 8 - Validation process

An overview of the requirements validation process is outlined below. These processes may be used for validation at the various hierarchical levels. These processes may be used to support certification.

5.4.2.1 Validation Plan

The validation plan should define the specific methods to be used for validation of requirements, data that will be collected, data storage requirements, and validation schedule. Additional information on validation planning is provided in 5.4.5, 5.4.6, and 5.4.7.

5.4.2.2 Determination of Validation Approach

Once the development assurance levels of the functions have been assigned by the safety assessment processes, the necessary approach to validation is then applied to the set of requirements for the specific function (see 5.4.5).

5.4.2.3 Correctness and Completeness

Correctness is the degree to which an individual requirement is unambiguous, verifiable, unique, consistent with other requirements, and necessary for the set of requirements.

Completeness is the degree to which a set of correct requirements satisfies the interests of customers, users, maintainers, and Certification Authorities, as well as aircraft, system, and item developers under all modes of operation and life cycle phases for the defined operating environment.

Additional information on correctness and completeness checks is provided in 5.4.3 and 5.4.4.

5.4.2.4 Management of Assumptions

In the majority of system development programs, a number of assumptions (or judgments) are made that are not directly provable at the time the information is needed. The existence of such assumptions is not, by itself, a certification concern, provided that the consequences of an incorrect assumption are assessed and documented. However, the possibilities for miscommunication about the basis and scope of such assumptions are numerous and the related consequences can jeopardize satisfactory implementation of safety requirements. Thus, assumptions (either explicit or implicit) should be identified, and their reasonableness and rationale established based on the specific system and its development assurance level.

Assumptions may be used early in the development process as a substitute for more explicit knowledge that will be available later. Aircraft and system development is iterative and concurrent and is not only top-down but may have bottom-up influences. Also, all interfacing systems and items within the system may not be at the same development phase to support the system design process. Requirements may have to be based on assumptions rather than on traceable requirements for work to progress on a particular system. In these cases, requirements validation consists of showing that the explicit knowledge or acceptable rationale was indeed obtained and that any inconsistencies between the explicit knowledge and the related assumption were resolved.

Any requirements based on assumed parent requirements should be identified and should be traced back. Requirements based on assumed higher-level requirements should be resolved by the time of certification.

The process of managing assumptions includes ensuring that assumptions are:

- Explicitly stated
- Appropriately disseminated
- Confirmed by supporting data

Where the consequences of an erroneous assumption appear to have significant potential to reduce safety, one possible requirements validation strategy consists of showing how the system design limits or bounds the achievable consequences of an assumption error.

The remainder of this section provides guidelines for identifying and judging the reasonableness of assumptions. To facilitate this purpose, assumptions are categorized below.

- Operational/environmental assumptions associated with air traffic, maintenance, cargo, personnel, flight dynamics, ATC systems, performance, operational procedures, and passengers (e.g., exposure times, traffic densities, maintenance intervals, performance limitations) should be considered. Frequently it is difficult or not possible to agree on the requirements with the primary owners of these systems. This may require the aircraft designer to make assumptions about the operational context. Other individuals, or documents and/or standards, may act on behalf of these system owners when agreeing on the operational context. For example, the Certification Authorities may represent the interests of the air traffic control system not only in regulation but also confirming an assumption about the level of traffic density.

- Design assumptions associated with crew interface, system interface, and reliability should be considered. Confirming assumptions in this area may be accomplished by review against existing industry experience and practice.

    - The crew interface assumptions may include the interaction of the crew with the equipment and the operational environment under normal and emergency conditions, crew performance characteristics (e.g., response times, display interpretation, physical limitations), and crew interaction. Some examples of assumptions about the crew interface are crew response times to various types of messages, event recognition times (e.g., recognition of hardovers), decision making strategies, and the discrimination accuracy on the basis of physical shape, visual form, color, or dynamic performance.

- System interface assumptions may address issues associated with the meaning or logical interpretation of the data exchanged (e.g., format, integrity, latency, resolution) or they may focus on the physical characteristics of the data signal (e.g., voltage levels, impedance, signal to noise ratio). Some examples of assumptions about the system interface include the probability of misreads of data bus information, correct processing of failure data by all related interfacing systems, failure containment, and characteristics of incorrect inputs.

- Reliability topics for which assumptions are often made may include: the adequacy of failure rate modeling over the life cycle, dispatch inoperative considerations, the adequacy of scheduled maintenance tasks and their frequency, the adequacy of piece-part derating, consideration of potential failure latency and exposure periods, the completeness of the failure modes analysis, the adequacy of test data to establish or support reliability predictions, and the applicability of in-service reliability data.

- Serviceability assumptions usually assume that provisions for service and repair do not degrade safety. This assumption may be confirmed by review of service and maintenance procedures and associated equipment.

- Installation assumptions (e.g., separation, isolation, cable binding, wire sizing, environment, power hook-up, circuit breaker sizing, ventilation, drainage, sources of contamination, mounting characteristics, grounding, and shielding) should be considered. Confirming assumptions in this area may be accomplished by review against industry standards and practice, selective testing, and/or inspections of mockup, prototype, or production drawings/hardware.

The means of managing assumptions during the development process should be defined in the validation plan.

5.4.2.5 Validation Matrix

The validation process includes preparation of a validation matrix (see 5.4.7) that references requirements and validation results, including, as appropriate, those for hardware/software performance, derived requirements, environmental and operational considerations, requirements based on assumptions, and supporting data. The source of each requirement should be identifiable. This matrix should be updated regularly during the development and included in the validation summary.

5.4.2.6 Validation Summary

The validation summary includes data describing the process, as well as the results (see 5.4.7).

5.4.3 Correctness Checks

During the validation process the correctness of the stated requirements content should be reviewed and justified. Correctness checks should be carried out at each level of the requirements hierarchy. The following questions may help assess correctness of requirements. The answers to these questions may be determined through application of the validation methods described in 5.4.6. This list should be tailored and expanded for the specific application.

a. Is the requirement correctly stated? For example:

1. Does the requirement have a unique interpretation (unambiguous)?
2. Is it identifiable as a requirement?
3. Is the requirement redundant?
4. Does the requirement conflict with others?
5. Does the requirement contain errors of fact?
6. Is it physically possible to meet the requirement?
7. Is the statement of the requirement expressed, where possible, in terms of what, when, and “how well,” rather than “how to”?

8. Is there enough information available to allow a future change to be made completely and consistently with visibility to the impact on those with an interest in or interface with the system?

9. Does the requirement include specific tolerances?

10. Is the requirement verifiable as described in 5.5?

11. If it is a derived requirement, is it supported by a rationale?

12. Is the source(s) of the requirement identified and correct?

13. Does the requirement contain multiple characteristics that may be better listed as separate requirements?

b. Is the requirement necessary for the set of requirements to be complete?

c. Is the set of requirements better suited to be combined into a single requirement?

d. Does the set of requirements correctly reflect the safety analyses? For example:

1. Are all requirements from safety assessments included?

2. Are all system failure conditions identified and classified correctly?

3. Is the impact of unsafe design or design errors considered?

4. Are integrity, reliability, availability, and failure tolerance requirements included?

e. Are the selected validation method(s) sufficient to assure requirement correctness (see 5.4.6)?

f. Are all assumptions against the requirement captured?

5.4.4 Completeness Checks

The completeness of a set of requirements by its nature may be difficult to prove. As a basis for performing a completeness check of requirements, it is possible to use the list of possible classes of requirements (see 5.3.1). Individuals with a generally stated need for the system may have unstated or unanticipated specific needs and expectations. Completeness is viewed as a probable outcome of following a validation process that may include a combination of templates and checklists, as well as the involvement of actual customers, users, maintainers, Certification Authorities, and developers.

The specific validation process for assessing completeness should be defined in the validation plan (see 5.4.7).

5.4.4.1 Templates and Checklists

A template in the form of a standard specification format, based on lessons learned, may reveal omissions and help prevent incomplete requirements.

Checklists may be used by authors and reviewers for completeness checks. The checklist should cover all areas that have a primary interest in the system and their applicable interfaces to ensure that their needs and expectations will be satisfied.

The following material provides assistance in developing checklist questions for assessing the completeness at each hierarchical level of requirements. This list should be tailored for the specific application.

a. Is it apparent from the traceability and supporting rationale that the requirement(s) will satisfy the parent requirement?

b. Does the requirements set fully cover the following?

1. All higher-level functions allocated to this system

2. Safety assessments

3. Regulatory standards and guidance

4. Industry and company design standards

5. Flight operations and maintenance scenarios

c. Are all interfaces to other systems, people, and processes identified?

d. Are the constraints (e.g., protocol, mounting configuration, and timing) associated with each interface defined in sufficient detail for the interface to be realized?

e. Are the system, people, or process behaviors that result from an interface agreed to and captured as requirements on both sides of the interface? For example, an engine system may provide data to a flight display system. How that data is used in the flight display system and how the crew may respond to that data should be agreed to as an interface requirement with the engine control system owner. Another example is the flight crews' input to the throttle: the throttle's input to the engine, which results in engine thrust behavior. The expected thrust behavior should be agreed to and captured as requirements with the flight crew or those that represent flight crews in general.

f. For a required behavior, should there be an associated prohibited behavior defined and, if yes, is the prohibited behavior defined?

g. Is the set of functional requirements fully allocated and traced to the system architecture?

h. Does the functional allocation clearly allocate between electronic hardware and software in the system architecture?

i. Are all assumptions captured and controlled by a managed process?

5.4.4.2 User, Operator, and Maintainer Involvement

One of the difficulties in achieving a complete set of requirements is that users don't always know what behaviors they do or don't want from a system. This is particularly true with new or novel features. There are a number of means of eliciting requirements from users. The early capture of operation and maintenance scenarios, as well as prototyping, are example means of eliciting requirements. These are not proposed as the best means but are suggested as ways that have been beneficial in identifying missing requirements (see 5.3).

5.4.4.2.1 Operation and Maintenance Scenarios

An effective means of identifying missing requirements early in the development process is writing down scenarios of how a system should function to accomplish a desired goal in response to inputs from users of that system. One example of how scenarios may be used is to define the procedures for the operating and maintenance manuals early in the development process. This provides visibility of how the system is proposed to work in different operational scenarios to users that interact with the system. Such visibility may aid in the identification of missing desired behaviors or protection features that should be captured in the scenarios and subsequently in the requirements. In such a scenario, the user may be another system but typically the users are people.

A number of scenarios may have to be explored for a given function to describe the behavior under different conditions and operating modes. Each scenario examines a sequence of steps from the user's initiating action, through each action step taken by an identified system or person on the way to the end goal.

The scenarios should not only cover the intended operating environments and operating modes but should cover anomalous operating conditions as well. Possible unintended behaviors would be considered for each step in a scenario. How this unintended behavior is to be managed or protected against would be defined and may itself be another scenario. Scenarios may also be used to agree on the functional allocation (see 4.3) as each interacting system's behavior is described in each step.

The pilot starting an engine would be an example of a scenario. The main scenario would be to describe the actions that a pilot would take to initiate a start, the subsequent actions taken by each of the cooperating systems, all the way to an engine achieving idle. Additional scenarios may include starter assisted air starts and windmill starts. Scenarios associated with anomalous operating conditions may begin with a pilot incorrectly initiating a start and how the cooperating systems are to respond, as well as a possible anomaly of the engine stalling during a start. The stalled start may be covered by a scenario that defines the steps that a system or person are to take to secure the engine start.

There are a number of methods for developing and documenting scenarios (e.g., state diagram, timeline diagrams). The particular approach is left to the developer.

5.4.4.2.2 Prototyping or Modeling

Prototypes are models of the desired system that may be hardware- and/or software-based and may or may not be development versions of the system. Prototypes permit users of a system to interact with a proposed model of the system to uncover missing requirements, behaviors of the system that should be prohibited, and potential problems with user interaction.

How well the prototype represents the actual system may drive the likelihood of identifying missing requirements and unintended behaviors. The fidelity of the prototype representation should be considered for its intended use.

The model should be developed in a structured manner. For example, subsets of model elements which may be used more than once may be handled and represented either as a unit or as the full contents.

Model use for requirements validation typically uses a model of the environment of a system being developed, which is interfaced to a prototype of a design solution for those requirements. An environment model that is representative of the environment of the system being developed provides a high degree of functional coverage in exercising either a simulated or real system.

5.4.5 Validation Approach

Requirement correctness and completeness should be assured for aircraft and system functions assigned development assurance level A, level B, or level C. In addition, validation process independence is recommended for level A and level B. The objectives for level D would be as negotiated and documented in the validation plan. Appendix A provides a summary of the process objectives for requirement validation based on FDAL.

Validation methods are identified and recommendations for their application are described in 5.4.6. The validation plan should describe the planned validation methods and the criteria for their application. Specific validation method(s) for each requirement should be applied based on the function(s) being validated and the criteria defined in the plan.

Where validation process independence is recommended, this independence should be applied between the requirements capture activities in 5.3 and the validation activities in 5.4. The validation plan (see 5.4.7) should include a description of the validation activities to which process independence is applied.

The most common means of achieving process independence in requirements validation is an independent review of requirement data and supporting rationale to determine if there is sufficient evidence to argue the correctness of a requirement and the completeness of a set of requirements. These include engineering reviews (see 5.4.6) and reviews by customers, users, maintainers, and item developers (see 5.4.4).

Although some validation methods may not directly lend themselves to process independence (e.g., analysis, scenarios, similarity, and requirements tracing), the outcomes of these validation method activities and their appropriateness are reviewable and should be done with process independence where indicated by the development assurance level (see Appendix A).

5.4.6 Validation Methods

Several methods have been established to support validation. These methods include traceability, analysis, modeling, test, similarity, and engineering review. Validation should consider both intended functions and unintended behaviors. Intended function requirements validation involves evaluation against established criteria. While it is acknowledged that validation is key in identifying and addressing unintended behaviors, strategies to investigate for unintended behaviors as part of integration and verification are outlined in 4.6.4.

Requirement traceability and/or requirement rationale for derived requirements should be established for each requirement. Each requirement and the set of requirements should also be subject to engineering review. Although traceability and engineering review may be sufficient to assure requirement completeness and correctness, some requirements may need additional validation methods to achieve this objective. For FDAL A and B requirements, an additional validation method should be applied when traceability and/or requirement rationale for derived requirements, combined with engineering review, are not sufficient to assure correctness and completeness. The list below provides some examples of types of requirements where an additional validation method may be necessary (examples only—not a checklist of cases).

- Complex state machine
- Safety monitor definition (e.g., threshold, confirmation time, persistency)
- Performance and tolerance definition
- Dynamic behaviors (e.g., oscillation frequency, latency, time delay)
- Numerical values (e.g., accuracy values, detection thresholds, response time, transitory time, min/max boundaries) that are based on assumptions requiring an implementation to be confirmed

The validation plan should describe the extent to which the validation methods will be applied based on the specific function(s) being validated.

5.4.6.1 Traceability and/or Rationale (Bi-Directional Relationship of Requirements)

Traceability is an essential element of validation of the aircraft, system, and item requirements. The requirement should trace to a parent requirement, and/or identify the specific design decision or data from which the requirement was developed. Requirement traceability from both top-down and bottom-up perspectives helps determine that all parent requirements have been captured by lower-level requirements and that all lower-level requirements can be traced to valid parent requirements.

Traceability by itself may be sufficient to confirm that a lower-level requirement satisfies a higher-level requirement. However, where additional value has been added through design decisions or detail, additional rationale should be captured. This rationale should document how the lower-level requirement(s) satisfy the parent requirement. Some lower-level requirements may introduce behaviors or characteristics beyond those specified in higher-level requirements. These derived requirements should have rationale to document their validity and their functional and safety impact should be evaluated at relevant higher levels (see 5.3.3).

Untraced requirements should be reviewed to determine whether they are:

- Derived as part of the development process (see 5.3.1)
- Developed from a missing parent requirement that may be added
- Associated with assumptions that need to be managed (see 5.4.2)
- Unnecessary and should be deleted

5.4.6.2 Analysis

A wide range of analysis methods and techniques may be used to determine requirements acceptability. Several methods specific to safety analysis are described in ARP4761A/ED-135. Early discussion with Certification Authorities on the acceptability of the FHA and PASA/PSSAs will assist in the validation of the safety requirements.

5.4.6.3 Modeling

Models of systems/items may be used to validate the requirements.

5.4.6.4 Test

Special tests, simulations, or demonstrations may be used to validate requirements. These activities may occur at any time during development based on when mock-ups, prototypes, simulations, or actual hardware and software may be available. Care should be exercised to ensure any simulation is sufficiently representative of the actual system, its interfaces, and the installation environment.

Item verification tests may also be used to support validation of the requirements derived to design the item.

5.4.6.5 Similarity

This method allows validation of a requirement by comparison to the requirements of similar certificated systems. The similarity argument gains strength as the period of experience with the system increases. Arguments of similarity should not be used until there is adequate confidence that the period of experience is satisfactory. Similarity may be claimed if either:

- The two systems/items have the same function and Failure Condition Classification, and operate in the same environment with similar usage, or

- The two systems/items perform similar functions in equivalent environments.

5.4.6.6 Engineering Review

Application of personal experience through reviews, inspections, and demonstrations can support determination of completeness (see 5.4.4) and correctness (see 5.4.3). The properly justified rationale or logic should be documented. A collaborative review of requirements is an effective means of validating derived requirements in cases where the system is similar to previous systems within the experience of the reviewers, prior to the opportunity to test the implementation during verification. The reviews should be documented including the review participants and their roles. The value of the review will depend on the care taken with the review and the experience level of the reviewers.

5.4.7 Validation Data

5.4.7.1 Validation Plan

A requirements validation plan should be in place throughout the development process. This plan should outline how the requirements will be shown to be complete and correct and how the assumptions will be managed. The validation plan should include, unless otherwise justified, descriptions of:

a. The methods to be used

b. The data to be gathered or generated

c. What should be recorded (such as summaries, reviews, or investigations)

d. The means for timely access to requirements validation information

e. The validation criteria (completeness and correctness checks)

f. The tracking process for validation status, including when changes are made to requirements

g. Roles and responsibilities associated with the validation

h. A schedule of key validation activities

i. The means of managing assumptions at the different design levels and phases of development

j. The means to be used to provide independence of the requirements definition from the validation activities

k. The process to be followed if any issues are identified during validation activities

l. The data to be included in the validation summary

Aspects of the validation process that may also serve as part of verification should be coordinated with the verification plan.

5.4.7.2 Validation Tracking

A validation matrix or other adequate approach is desirable to track the status of the requirements validation process. The level of detail should depend upon the development assurance level of the function addressed by the requirement and should be described in the validation plan. The final data should be included in the validation summary. The specific format is up to the applicant, but it may contain:

a. Requirement

b. Source of the requirement

c. Associated function(s)

d. Development assurance level

e. Validation method(s) applied

f. Validation supporting evidence reference(s)

g. Validation conclusion (valid/not valid)

5.4.7.3 Validation Summary

The validation summary should provide assurance that the requirements were properly validated. The summary should include:

a. A reference to the validation plan and a description of any significant deviations from the plan

b. The validation matrix (see 5.4.7.2)

c. Identification of supporting data or data sources (see 5.4.7.2)

5.5 Implementation Verification

The purpose of verification is to ascertain that each level of the implementation meets its specified requirements.

The verification process ensures that the system implementation satisfies the validated requirements. Verification consists of inspections, reviews, analyses, tests, and service experience applied in accordance with a verification plan. These activities are described in the following sub-sections.

5.5.1 Verification Process Objectives

The verification process:

a. Confirms that the intended functions have been correctly implemented.

b. Confirms that the requirements have been satisfied (e.g., have we built the aircraft right?).

c. Ensures that the conclusions drawn from the safety analysis are correct for the system as implemented.

5.5.2 Verification Process

Figure 9 shows an overview of a generic process diagram for verification at each level of system implementation.

The verification process is composed of three distinct elements described as follows:

a. Planning: Includes planning for the resources required, the sequence of activities, the data to be produced, collation of required information, selection of specific activities and assessment criteria, and generation of verification-specific hardware or software (see 5.5.4)

b. Methods: Includes the activity in which the verification methods are employed (see 5.5.5)

c. Data: Includes evidence of the results developed in the process (see 5.5.6)

The verification approach is determined by the FDAL(s) for the aircraft or system function(s) (see 5.5.3).

The inputs to the verification process include the set of documented requirements for the implemented aircraft, system or item and a complete description of the system or item to be verified.

During the process of verifying intended functions, any anomalies recognized (such as an unintended behavior or incorrect performance) should be reported so that they can be reviewed and dispositioned (see 4.6.4). Checking the verification process, design implementation process or requirement definition process may be warranted to identify the source of the anomaly.

It should be mentioned that verification is a process which, due to the iterative nature of the development process, may appear repeatedly during the design process (see Figure 5).

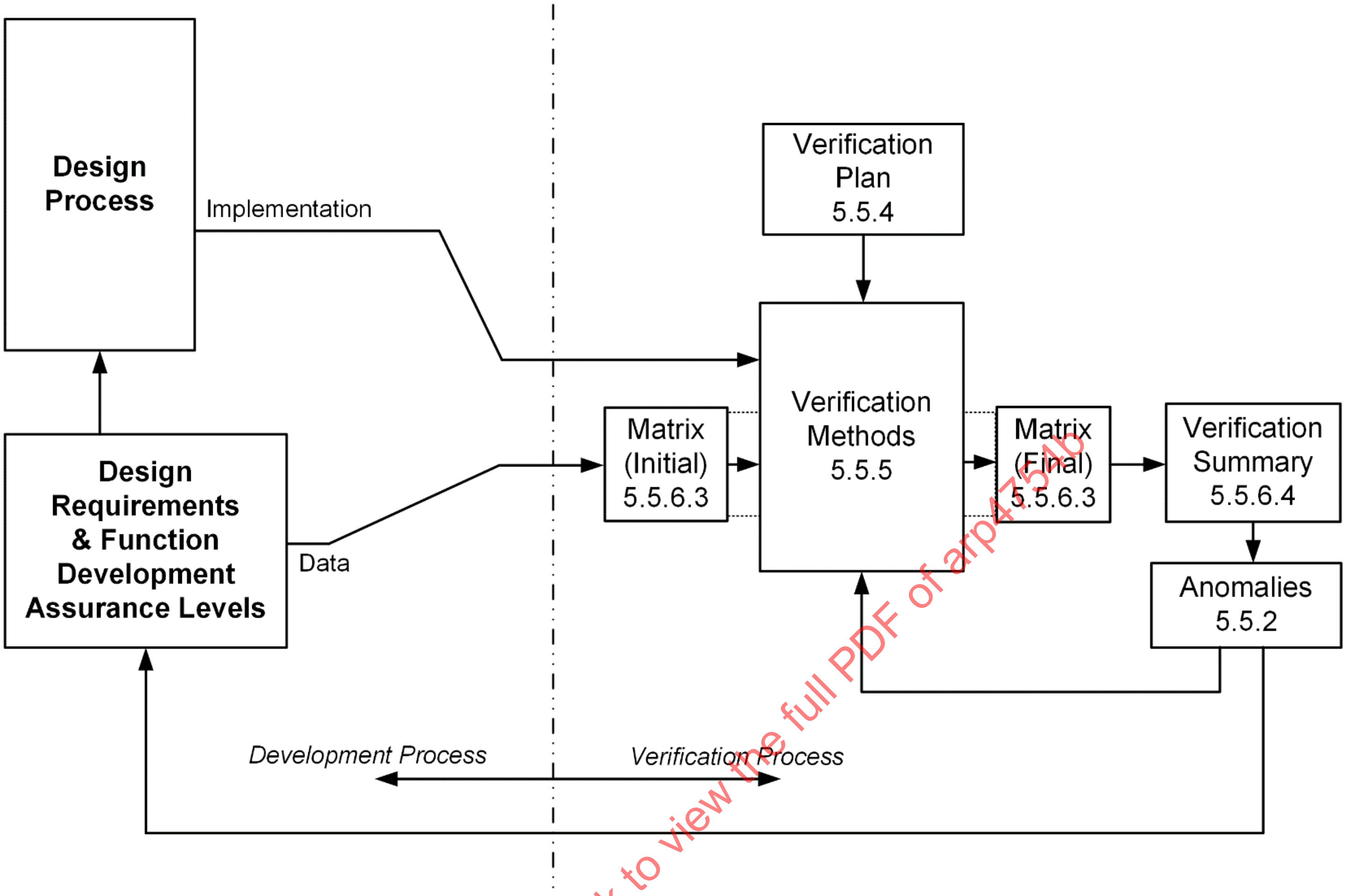


Figure 9 - Verification process

5.5.3 Verification Approach

The implementation should be verified to confirm that the requirements for aircraft and system functions assigned development assurance level A, level B, or level C are satisfied. In addition, verification process independence is recommended for all level A requirements, and for level B safety requirements. The objectives for level D would be as negotiated and documented in the verification plan. Appendix A provides a summary of the process objectives for verification based on FDAL.

Verification methods are identified and recommendations for their application are described in 5.5.5. The verification methods and procedures should ensure the implementation of each requirement is fully verified. The verification plan should describe the extent to which the verification methods will be applied based on the specific function(s) being verified.

Where the application of independence in the verification process is recommended within this section, this independence should be applied between the implementation and the verification activities described in 4.6 and 5.5, respectively. The most common means of achieving independence in verification is independent development of the verification methods and procedures described in 5.5.5 (e.g., individuals or groups not involved in the aircraft or system design generate the verification methods). The verification plan (see 5.5.4) should include a description of the verification activities to which independence will be applied.

5.5.4 Verification Planning

The purpose of this phase is to define the processes and criteria to be applied when showing how the implementation satisfies its requirements. The following activities should be performed during the planning phase:

a. Identification of the roles and responsibilities associated with conducting the verification activities and a description of independence between design and verification activities

b. Identification of the system or item configuration, including the definition of any special test equipment, facilities, and any special hardware or software features to be verified

c. Definition of the specific verification methods to be employed to confirm that the implementation satisfies each requirement, taking into account the development assurance level

d. Definition of the criteria to be used to assess the evidence resulting from each verification method applied (i.e., success criteria)

e. Definition of the means for ensuring that the verification methods and procedures can fully verify the implementation of the requirements

f. Identification of system verification credit taken from other levels including hardware or software verification activities

g. Identification of key verification activities and sequence of any dependent activities

h. Identification of verification data

i. Description of the verification environment(s) that will be used

5.5.5 Verification Methods

The purpose of these activities is to verify that the implementation satisfies its requirements, including the intended operating environment. Four basic methods may be employed in the verification of the aircraft and any system or item:

a. Inspection/review

b. Analysis

c. Testing or demonstration

d. Similarity/service experience

Each of these methods is discussed in the following sub-sections.

Appropriate verification method(s) should be selected to ensure the implementation of each requirement is fully verified. The preferred verification method for requirements is by test, wherever practical. Other method(s) may be used to augment the test, or instead of test, where necessary or applicable.

5.5.5.1 Inspection/Review

Inspection/review consists of visual examinations of process documents, drawings, hardware, or software to verify that requirements have been satisfied. Generally, a checklist or similar aid is used. Inspection that the system or item meets established physical implementation and workmanship is a typical type of inspection/review.

5.5.5.2 Analysis

An analysis provides evidence that the implementation satisfies the requirements by performing a detailed examination (e.g., functionality, performance, safety) of a system or item. Evaluations of how the system or item is expected to perform in normal and non-normal conditions should be included. Analysis methods include, but are not limited to, those described in the following sub-sections.

5.5.5.2.1 Modeling

Modeling of complex systems typically consists of a combination of computation and test; however, modeling deterministic systems behavior may also be entirely computational. Modeling may be used for system parameter evaluation, to provide early system information, or other purposes.

5.5.5.2.2 Coverage Analysis

Coverage analysis is performed to determine the degree to which the requirements are addressed throughout the development and verification activities. This is typically implemented using some form of traceability.

5.5.5.3 Testing or Demonstration

Testing provides repeatable evidence of correctness by exercising a system or item to verify that the requirements are satisfied. Test readiness reviews establish the applicability of the test procedures to system or item requirements. Testing has the following two objectives:

a. To demonstrate that the system or item implementation performs its intended functions. Testing an intended function involves evaluation against objective pass/fail criteria established by the requirements.

b. To provide confidence that the implemented system does not exhibit unintended behavior (i.e., behavior not consciously part of the design) that impacts safety. This is accomplished by looking for system behavior beyond the expected behavior specified by the requirements set being tested. It should be noted that complete absence of unintended behavior may not always be attainable due to high degrees of complexity, but devices that employ simple logic gates and/or logic may have failure combinations that are fully identifiable and analyzable/testable.

Tests are performed on all or part of the physical system or item or an appropriate validated model using procedures documented in sufficient detail so that a second party could reproduce the test results. Problems uncovered during testing should be reported, corrective action tracked, and the modified system(s) and/or item(s) retested.

For each test procedure or group of test procedures, the following should be specified:

a. The purpose or rationale for the test(s)

b. The requirements covered by the test(s)

c. Required input variability, considered in setting the test criteria

d. Actions required and, if actions are time/sequence dependent, define the action order

e. Expected results and the tolerances associated with those results

Test result data should contain the following:

a. The version of the test specification used

b. The version of the system or item being tested

c. The version or reference standard for tools and equipment used, together with applicable calibration data

d. The results of each test including a PASS or FAIL declaration

e. The discrepancy between expected and actual results

f. A statement of success of or deficiency in the testing process including its relationship to the verification program

5.5.5.3.1 Test Facilities

Functionality may be provided in a system test facility which will improve the probability of detecting incorrect or unintended behavior:

a. The hardware and software under test are present in the facility and are representative software and hardware.

b. A model of the environment may be used to set inputs to the system under test in a way that is representative of actual service, using representations of user control inputs.

c. A model of the environment may receive the outputs of the system under test and calculate and present the system behavior in terms of the high-level requirements.

d. The behavior of the system under test is made plainly visible in terms of high-level parameters.

e. The high-level manual inputs are made repeatable to facilitate regression testing.

f. Significant events, such as failure or warning messages, and deficiencies against the high-level requirements are annunciated and logged.

Provision of this functionality allows developmental testing for risk reduction using the models to generate the test results and interpret the results with a very high productivity, and a manageable means to detect and record any unexpected results.

5.5.5.4 Similarity/Service Experience

Verification credit may be derived from design and installation similarity appraisals and evidence of satisfactory service experience on other aircraft using the same or other systems that are similar in their relevant attributes. This method should use documented experience along with engineering and operational judgment to establish that no significant failures remain unresolved in these installations. See 6.4.1 for additional information regarding the use of service history.

5.5.6 Verification Data

The purpose of verification data is to provide evidence that the verification process was conducted. This evidence may be required for compliance substantiation as agreed with Certification Authorities (see 3.3). A reasonable approach is to maintain a verification matrix during development and to produce a verification summary report.

Requirements for software verification are included in DO-178C/ED-12C and for electronic hardware verification in DO-254/ED-80. A summary of software and hardware verification should be included in the verification data of the system in which it is embedded.

5.5.6.1 Verification Plan

The verification plan establishes the strategies to show how the aircraft and system implementation satisfy their requirements. The verification plan should include, unless otherwise justified, descriptions of:

a. Roles and responsibilities associated with conducting the verification activities

b. A description of the degree of independence of the design and verification activities

c. Application of verification method(s)

d. Verification data to be produced

e. Sequence of dependent activities

f. A schedule of key verification activities

g. Identification of system verification credit taken from other levels, including item (hardware or software) verification activities

h. Description of the verification environments that will be used

Some aspects of the verification process may also support validation of specific requirements and should be coordinated with the validation plan.

5.5.6.2 Verification Procedures and Results

Data describing the verification procedures and the results achieved provides the evidence necessary to establish the appropriateness of the verification effort.

5.5.6.3 Verification Tracking

A verification matrix or an equivalent tracking document should be produced to track the status of the verification process. The level of detail of this matrix should depend on the development assurance level of the system or item being verified. The specific format is up to the applicant, but it may contain:

a. Requirement

b. Associated function

c. Verification method(s) applied

d. Verification procedure and results reference(s) (including verification results from other levels as applicable)

e. Verification conclusion (i.e., pass or fail, verification coverage summary)

5.5.6.4 Verification Summary

The verification summary provides visibility for the evidence used to show that the aircraft, system, or item implementation satisfies its requirements. The summary should include:

a. A reference to the verification plan and a description of any significant deviations from the plan

b. The FDAL(s) assigned to the function(s)

c. The verification matrix as described in 5.5.6.3

d. Identification of supporting data or data sources (see 5.6 for supporting data criteria)

e. Verification coverage summary

5.6 Configuration Management (CM)

This section discusses the objectives and activities of the system configuration management process. It is applicable to the configuration items described in 5.6.1. Figure 10 presents an overall configuration management process.

The existence of an independent entity or organization to perform the configuration management activities should not be inferred by the title or content of this section.

Data and records need to meet the following criteria if they are to be used to support certification:

a. The data and records should be retrievable for later reference.

b. The source of the data generated, such as by analysis or test, and the methods used, should be sufficiently controlled so as to allow regeneration of the same or similar data.

This provides archived evidence for future enhancements, problem resolution, and review by Certification Authorities.

5.6.1 Configuration Management Process Objectives

The objectives of the configuration management process are to provide:

a. Identification of configuration items, which include:

    1. Plans

    2. Life cycle data and records generated by the execution of plans (e.g., requirements, validation, verification, implementation data)

    3. Applicable certification data as agreed with Certification Authorities (see 3.3)

    4. Facilities, tools, and any other data, where configuration is essential to accomplishing development assurance activities

    5. Any other data that uniquely identifies the system and/or item versions during development, production, and operation

b. Technical and administrative control by:

    1. Identifying modification status and change control of a system configuration in relation to a configuration baseline

    2. Providing controls to ensure that:

        i. Changes are recorded, approved, and implemented

        ii. Identified problems, current status, and, if applicable, their resolution are recorded

c. Assurance that archiving, recovery, and control are maintained for relevant system data

Configuration management is both a system development and a certification activity. A configuration baseline should be established at the times in the system development process where requirements validation or implementation verification activities are initiated. A history of changes between configuration baselines is a necessary element of the development assurance process.

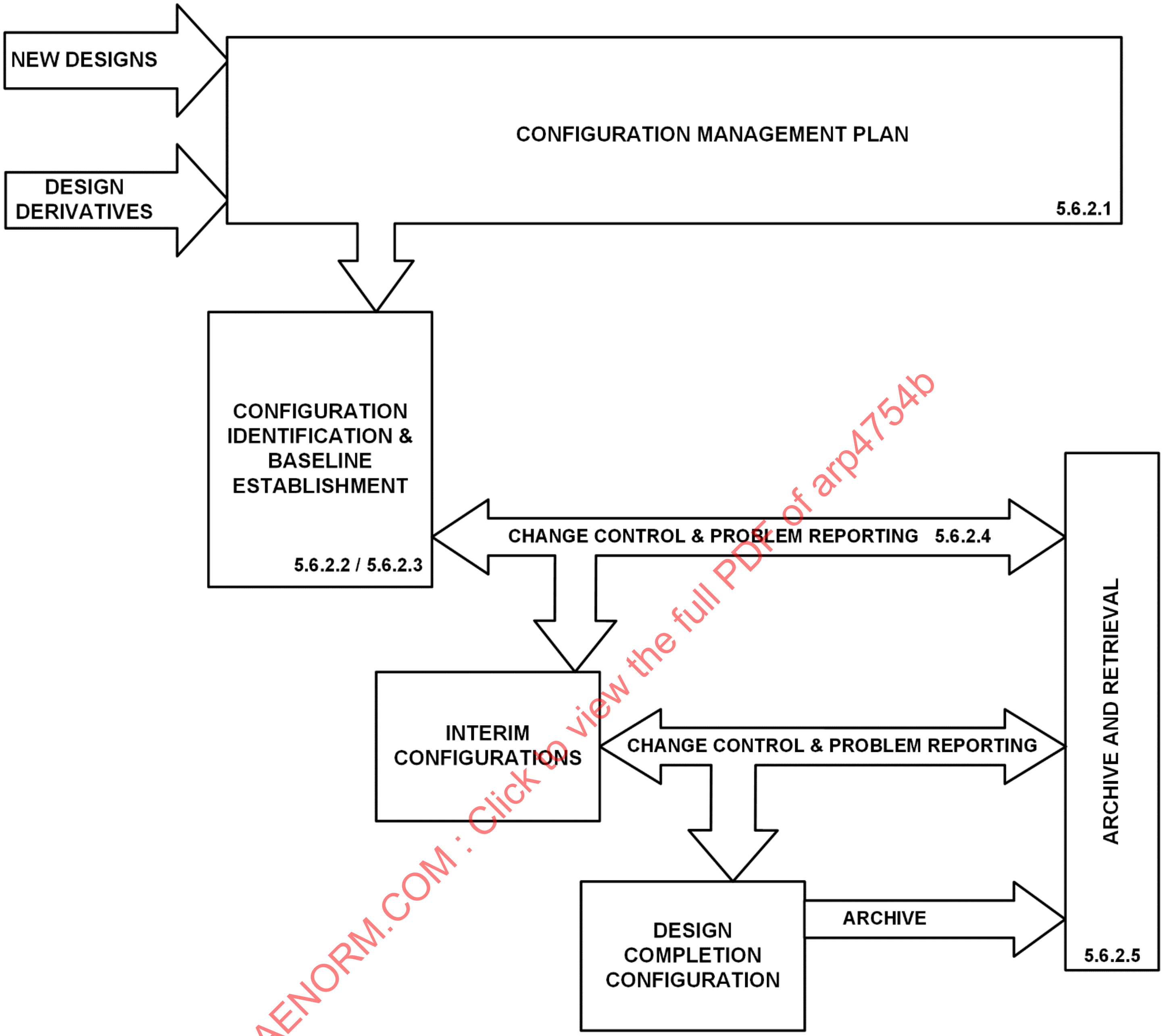

NEW DESIGNS
DESIGN DERIVATIVES
CONFIGURATION MANAGEMENT PLAN
5.6.2.1
CONFIGURATION IDENTIFICATION & BASELINE ESTABLISHMENT
5.6.2.2 / 5.6.2.3
CHANGE CONTROL & PROBLEM REPORTING 5.6.2.4
INTERIM CONFIGURATIONS
CHANGE CONTROL & PROBLEM REPORTING
DESIGN COMPLETION CONFIGURATION
ARCHIVE
ARCHIVE AND RETRIEVAL
5.6.2.5

Figure 10 - Configuration Management process model

5.6.2 Configuration Management Process Activities

The configuration management process shown in Figure 10 includes:

a. Configuration management plan

b. Configuration identification

c. Baseline establishment

d. Change control and problem reporting

e. Archiving and retrieval activities

Continuity of these activities significantly enhances their effectiveness and the credibility of the overall configuration management process. For certification purposes, evidence of a continuous configuration management process may include, but is not limited to, historical records or successive reports from these activities.

5.6.2.1 Configuration Management Plan

The configuration management plan establishes the methods to be used for the configuration management process throughout the system development life cycle. The plan should include a description of the configuration management environment, including procedures, tools, methods, standards, organizational responsibilities, and interfaces. A description of the activities presented in 5.6.2.2 through 5.6.2.5 should also be included, unless otherwise justified.

5.6.2.2 Configuration Identification

Configuration identification unambiguously and uniquely labels each configuration item to establish control and reference.

The set of Configuration Items should be recorded as part of the archiving and retrieval activity.

5.6.2.3 Configuration Baseline Establishment

Configuration baseline establishment activity creates and maintains control of and traceability of Configuration Items. Guidelines include:

a. A baseline should be established for configuration items used for requirements validation or implementation verification.

b. Once a baseline is established it should be archived, protected, and subject to change control procedures.

c. Change control activity should be followed when developing a new baseline from an established baseline.

d. Each new baseline should be traceable to the previous baseline.

The design completion configuration in Figure 10 is typically that configuration used for entry into service or certification. The configuration baseline should be captured as part of a configuration index (see 5.6.3).

5.6.2.4 Change Control and Problem Reporting

The change control and problem reporting processes record changes or issues identified during review, testing, or service and records their resolutions. The following guidelines highlight the aspects of change control and problem reporting that are significant in the development assurance process:

a. Means should be established to document changes and the resolution of problems.

b. Change control should ensure that any change to a system/item is appropriately identified by a change to its configuration identification.

c. Change control should ensure that changes to a system/item require applicable changes to the documentation associated with the system/item.

d. Change control should protect against unauthorized change of a system/item.

e. Problem reports to remain open at the time of certification should be reviewed to determine whether they have an impact on safety or operational limitations.

5.6.2.5 Archive and Retrieval

Archive and retrieval activity ensures that the configuration items can be retrieved. Data retention procedures should be established to satisfy certification requirements. The following guidelines are provided:

a. Data associated with the system or item should be retrievable from a controlled source (for example, the organization or company that developed the system).

b. Procedures should be established to ensure the stored data is not corrupted for as long as may be required. These procedures should include:

   1. Ensuring that no unauthorized changes can be made.

   2. Selecting storage media that minimize regeneration errors or deterioration.

   3. Exercising and/or refreshing archived data at a frequency compatible with the storage life of the medium.

   4. Storing duplicate copies in physically separate archives that minimize the risk of loss in the event of a disaster.

5.6.3 Configuration Management Data

The data defined in this section is the typical output of the configuration management processes.

5.6.3.1 Configuration Index

The configuration index is used to identify all of the configuration items that together document the system as implemented. This includes both system and item artifacts, as well as identification of procedures and limitations that are integral to system safety.

A system configuration index should include, unless otherwise justified, the following information:

a. Plans

b. Life cycle data and records generated by the execution of plans (e.g., requirements, validation, verification, implementation data)

c. Associated item configuration identification (hardware/software)

d. Required interfaces with other systems (e.g., Interface Control Document)

e. Safety-related operational or maintenance procedures and limitations

f. Permissible interchangeability or intermixability of alternate equipment/items within the system, when applicable

5.6.4 System Control Categories

The development life cycle data of a configuration item can be assigned one of two categories: System Control category 1 (SC1) or System Control category 2 (SC2). Appendix A identifies System Control categories for each type of development life cycle data based on FDAL.

Table 3 identifies the configuration management process activities applicable to the two System Control categories. An “X” in a Table 3 SC1 or SC2 column indicates the configuration management process activities that apply to the System Control category. All configuration management process activities defined in 5.6.2 apply to SC1 development life cycle data. Only a subset of configuration management process activities applies to SC2 development life cycle data.

Table 3 - CM process activities applicable to System Control categories

CM Process Activity	Section Reference	SC1	SC2
Configuration Identification	5.6.2.2	X	X
Configuration Baseline(s) Establishment	5.6.2.3	X	
Problem Reporting	5.6.2.4 (a)(e)	X	
Change Control—Tracking	5.6.2.4 (b)(c)	X	
Change Control—Protection	5.6.2.4 (d)	X	X
Archive and Retrieval	5.6.2.5	X	X

5.7 Process Assurance

This section describes the activities that ensure that the development assurance activities are maintained and followed. The process assurance activities described are not intended to imply or impose specific organizational structures or responsibilities. However, process assurance should have a level of independence from the development process.

5.7.1 Process Objectives

The objectives of the process assurance activities are:

a. To ensure the necessary plans are developed and then maintained for all aspects of aircraft, system, and item development.

b. To ensure development activities and processes are conducted in accordance with those plans.

5.7.2 Process Assurance Plan

The Process Assurance Plan describes the means to assure that the practices and procedures to be applied during system development are followed. The following issues should be considered when producing the Process Assurance Plan:

a. The scope and content of the development assurance plans are consistent with the development assurance level of the aircraft function, system, or item.

b. Project communications, coordination and sequencing, and progress monitoring mechanisms are defined.

c. Change control and operational and maintenance procedures are defined.

d. Project reviews provide sufficient opportunities to detect any development errors in a timely manner.

e. Sufficient coordination with the Certification Authorities is planned.

f. Deviations from the plans are identified and managed (reported, approved, and documented).

g. Reports are generated to record Process Assurance activities and confirm adherence with plans.

h. Independence of process assurance activities from development.

5.7.3 Process Assurance Reviews

5.7.3.1 Development Assurance Plan Reviews

The following issues should be considered when assessing the plans:

a. Applicable procedures and practices are documented.

b. Defined communication practices ensure the timely exchange of information between the applicable processes and affected personnel.

c. Procedures for plan updates due to process, schedule, or technical changes are defined.

d. Plan updates are appropriately tracked and controlled.

5.7.3.2 Activity, Data, and Report Reviews

Process assurance reviews are an assessment of the development assurance activities, their related data, and reports.

The following issues should be considered when assessing the data and reports:

a. Approved plan activities are executed.

b. Data is correct and complete in accordance with approved plan.

c. Plan deviations are managed.

d. Data and report updates are appropriately tracked and controlled.

5.7.4 Process Assurance Data

Evidence of adherence with the plans may include:

a. Dated and approved plans

b. Reports, metrics, and summaries of reviews, as required by the plans

c. Actual data developed from design, verification, validation, configuration management, and safety activities

d. Confirmation (e.g., completed checklists and meeting minutes) of timely process assurance reviews

6. MODIFICATIONS TO AIRCRAFT OR SYSTEMS

The objective of this section is to describe how the guidelines in this document could be applied when making a modification to an aircraft, system, equipment, or item or when reusing a system, equipment, or item.

One of the goals of the development and safety assessment processes is to maintain, or improve on, the existing safety level provided by the original certification basis. The term “modification/reuse” in this section is taken to mean either:

- The introduction of a system, equipment, or item in an existing application,
- The change to a system, equipment, or item in an existing application, or
- The introduction of an existing system, equipment, or item in a new aircraft application; new application may include an updated certification basis, new use of existing equipment, or new operational context or environment.

Thus, a modification/reuse needs to be controlled in such a way that all the effects of a modification/reuse are known, fully understood, validated, and verified. A modification/reuse to an aircraft, system, equipment, or item may be undertaken for a number of reasons, ranging from adding new functionality to responding to a required corrective action (including piece-part or system obsolescence). The modification/reuse process should be a consideration in the development assurance plan and safety program plan. The modification processes described in this section are applicable to any kind of modifications (design changes to Type Certificate (TC)/Amended Type Certificate (ATC), Supplemental Type Certificate (STC), Amended Supplemental Type Certificate (ASTC), or Technical Standard Order (TSO)/European Technical Standard Order (ETSO)) and covers re-use cases. All modifications/reuses should be assessed for aircraft-level and systems-level effects and captured in a modification impact analysis. When developing a new aircraft, system, equipment, or item, it is common to evaluate previous designs and, wherever practical, re-use part or all of those previous designs. The entirety of these re-used functions can include: those parts that have been modified, those parts that are unchanged from their previous application that are intended to be used in the new application, and those parts that are unchanged from their previous application but not intended to be used in this application; each needs to be assessed for aircraft-level and system-level effects.

6.1 Modification/Reuse Process Overview

The applicant proposes a method or means of compliance that defines how it will be shown that the reused or modified aircraft, system, equipment, or item satisfies the certification basis, which may have changed from the original type certification. It is necessary to ensure that the proposed means of showing compliance is compatible with the agreed certification basis. This section provides the scope of application of the established system or item development processes in Sections 4 and 5 of this document. The modification process may include:

a. Develop and coordinate a modification management process. This includes crafting a strategy and approach to the certification process (i.e., certification planning), including determining a certification basis for the project. (When changing an existing or introducing a new aircraft, system, equipment, or item modification, the potential effects in the certification basis should be assessed and classified as either “Minor” or “Major,” as defined in 14 CFR/IR Part 21/EASA Part 21. Approval of the modification classification should be obtained from the relevant Certification Authority.)

b. Conduct and document a modification impact analysis; this should include an analysis for the reused system, equipment, or item to ensure that the safety implications are addressed for all functions within the system, equipment, or item (whether or not they are used) (see 6.3).

c. Perform the approved modification process.

d. Integrate the reused system, equipment, or item, or the modification into the aircraft, system, equipment, and item as required.

e. Provide a summary of the modification management process outputs established by the modification impact analysis; see 4.7 for a summary of the process outputs.

f. Maintain configuration control of data (see 5.6).

6.2 Modification Management Process

The modification management process provides a structured means to control and co-ordinate the design. The process documentation should include:

a. Description of the proposed modification or reused system, equipment, or item

b. Results of an initial modification impact analysis

c. The proposed implementation strategy (such as activities as defined in Table 5)

d. Implementation and integration of the modification using the agreed implementation strategy

e. Results of verification activities on the implemented modification

f. The final modification accomplishment summary activities

g. Updates to the aircraft configuration management data on any modified system, equipment, or item

6.3 Modification Impact Analysis

When a modification is proposed to an aircraft, system, equipment, or item, an impact analysis should be performed and should include an evaluation of the impact of the modification on the original development assurance activities and safety assessments. For instance, if an aircraft-level modification is proposed, the assumptions made for the architectural forms used, the development assurance level allocations and its installation should be reviewed. The following are examples of areas that could adversely affect aircraft safety or operation:

- Safety-related information is changed. For example:
  - Failure Condition classification(s) changed or added
  - Development assurance level
  - Design assumptions
  - Validation and/or verification methods or procedures are changed
- Operational or procedural characteristics are changed. For example:
  - Validity of the environmental qualification test results is affected
  - Aircraft operational or airworthiness characteristics
  - Flight crew procedures
  - Increased pilot workload
  - Situational awareness, warnings, cautions, or advisories
  - Displayed information to make flight decisions

Figure 11 provides a high-level overview of the modification impact analysis.

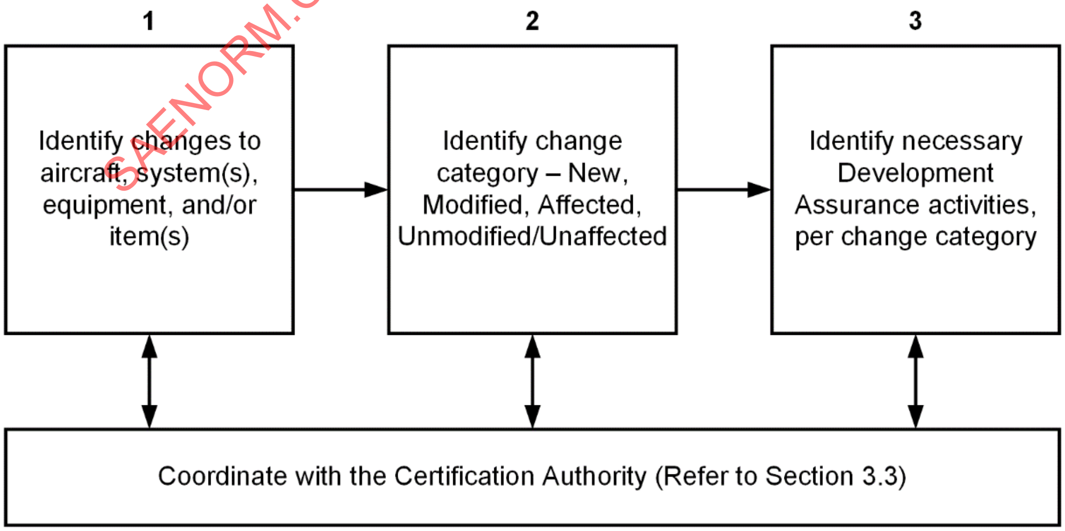

1
Identify changes to aircraft, system(s), equipment, and/or item(s)
2
Identify change category – New, Modified, Affected, Unmodified/Unaffected
3
Identify necessary Development Assurance activities, per change category
Coordinate with the Certification Authority (Refer to Section 3.3)

Figure 11 - Modification impact analysis

The design activities effort aimed at developing an acceptable implementation of a modification is an iterative process. The initial impact analysis may have to be revisited a number of times before the final version of the impact analysis can be produced.

Step #1: The first step is to identify the changes intended by the project. Changes can include any combination of the changes to the aircraft, system(s), equipment, or item(s). Identify the certification basis and the applicable policies and guidance materials to initiate the plan for development assurance, taking into account the applicable Function Development Assurance Level(s) (FDAL(s)) and Item Development Assurance Level(s) (IDAL(s)). Coordinate with the Certification Authority to ensure an acceptable certification path (see 3.3).

Step #2: The second step is the determination of the change category as part of the modification/reuse impact analysis. The change category is used to determine how the integral processes are to be applied to each function under evaluation. Table 4 provides an example of change category assignment.

NOTE: A function or implementation change may have a different change category applied for each portion of the aircraft or system. For example, the changed function or implementation could be classified as modified, while the interfacing functions or implementations could be classified as affected. Alternatively, one change category may be applied for the complete aircraft or system.

Table 4 - Example Change Category assignment

Change Description		Change Category (see Table 5)
Function	**Implementation**	
Function is completely unmodified and unaffected.	The implementation may have changed, for example, to: - Resolve obsolescence of non-complex hardware items. - Correct a deficiency that may have been identified pre- or post-certification, that results in the implementation performing the original intended function (e.g., implement a problem report or resolve a nuisance trip). It does not include the replacement of complex hardware items or the substitution of equipment with a different design that achieves the same function.	Unmodified and Unaffected
No change to function, however it is affected by related new or modified functions causing inputs to be changed when functional outputs are unchanged.	Interfacing system or installation environment has changed.	Affected
A modification of an aircraft or system function such that the functional output under normal and/or abnormal operating conditions (e.g., performance or operation) is changed.	Replacement of complex hardware items and the substitution of item with a different design that achieves the same function.	Modified
A new function is introduced to the aircraft.	Reuse of equipment from a different aircraft model. Reallocation of a function to different system/equipment.	New

NOTE: The change category should be determined, regardless of the type of modification, including re-use. The change category should also consider the impact of the change on the function (e.g., calculate airspeed) and the functional interfaces (e.g., static pressure, total air temperature).

Step #3: The last step is to determine the extent of development assurance process to be applied starting with the safety assessment guidelines defined in 5.1, including the determination of the associated Failure Condition Classifications.

Table 5 identifies the development assurance activities for the integral processes that may be used for the change categories of Modified, Affected or Unmodified/Unaffected given in Table 4. For the change category of New, the process as defined in Section 4 should be applied. The activities to be undertaken should be agreed with the relevant Certification Authorities, taking into account how the aircraft or system was previously certificated. If necessary, these activities may be documented in a Development Assurance Plan.

The assurance activities include:

- Requirements management
- Safety assessment process
- Requirements validation
- Implementation verification
- Configuration management
- Process assurance

For Certification Authority coordination, see 3.3.

Table 5 - Development Assurance activities per Change Category

Development Assurance Activity	**Change Category**		
	Modified	**Affected**	**Unmodified/Unaffected**
Requirements Management	The function's entire set of requirements, including interface requirements, is to be documented. Make a distinction between the modified and unmodified/unaffected portions of the function.	The function's entire set of requirements, including interface requirements, is to be documented. Make a distinction between the portions in this function that are affected by a new/modified function relative to the unchanged portion of the function.	No changes are required other than documentation corrections, provided a previous specification describes the function so that it can be confirmed that it is unmodified and unaffected.
Safety Assessment Process	Safety analyses updated as necessary to reflect as-built design following the guidelines of ARP4761A/ED-135.	Reassess safety analyses and update as necessary to reflect as-built design following the guidelines of ARP4761A/ED-135.	Reassess FDAL/IDAL assignments to ensure they are appropriate for the implementations. Ensure any legacy FDAL/IDAL allocations support any FDAL allocated to the unmodified and unaffected function in the changed implementation. Reassess safety assessments to ensure that each safety analysis reflects the system and aircraft implementation and remains valid.
Requirements Validation	Reassess the entire set of requirements for the function to determine it is complete and correct with the modified requirements, taking into account applicable service history. Ensure the parent requirements fulfilled by the modified function are still satisfied (all of the siblings of the modified requirement are still appropriate).	Reassess the portion of the set of requirements which are affected to confirm it is complete and correct when considering the new/modified function or implementation.	Reassess to confirm the unmodified and unaffected function is not affected by new/modified functions added to the system. Reassess to confirm the function is unmodified and unaffected by the new implementation.
Implementation Verification	Identify the degree of verification needed: - For unchanged requirements, assess existing verification data and identify any need for verification activities. - For new/modified requirements, plan and perform implementation verification activities. Assess the need for regression testing.	Reassess existing verification data for the function for impacts due to the new/modified functional input or implementation: - Identify the degree of regression verification needed by assessing existing verification data. - Plan and perform any necessary verification activities.	Identify the degree of verification needed: - Identify the degree of regression verification needed by assessing existing verification data. - Plan and perform any necessary verification activities.
Configuration Management	Identify the modification definition and confirm it is appropriately documented. Review changes to the function preceding this modification. Assess any Open Problem Reports (OPRs) to identify if they cause the function to be changed or the documentation or process to be corrected. Capture the set of OPRs to be addressed as part of the change and justify those not addressed.		
Process Assurance	Confirm modification activities' adherence to the modification plan. Document evidence.		

Plans should be developed, as needed, to capture the required processes.

6.4 Reuse of Evidence from Previous Certification Process

If credit is sought for development assurance activities performed on a system, equipment, or item from a previously certificated "baseline," the proposed system, equipment, or item and its certification data should be traceable to that baseline and confirmed to be appropriate to the new application. In some cases, such evidence may not be adequate and would need to be supplemented.

To supplement existing certification data, the applicant may:

a. Evaluate the data available from the previous certification to determine which development assurance objectives are satisfied for the new application and which objectives require additional consideration; this activity forms part of the modification impact analysis.

b. Use reverse engineering, where all assumptions can be verified, to develop certification data necessary to satisfy the development assurance objectives for the new application.

c. Use service history in accordance with the guidelines in 6.4.1 to satisfy the development assurance objectives.

d. Specify the strategy for development assurance activities.

6.4.1 Use of Service History

Service history may be used to support certification of a new/modified system, equipment, or item if an analysis shows the history to be applicable. An assessment of both the changes to the referenced item in its original system configuration and the use of all functions within the referenced item in the new/modified system configuration should have been successfully completed. This method may be used to verify a requirement by comparison to the requirements of similar in-service systems, equipment, or items. The similarity argument gains strength as the applicable period of service experience increases. Arguments of similarity should not be used until any significant problems experienced in service have been understood and resolved.

Considerations for the use of service history include:

a. The applicant should propose how service history will be used and what credit is being sought for certification (e.g., the amount of service experience available and a description of how the service data will be analyzed).

b. The applicant should conduct an analysis to determine the extent to which the service history is applicable. Such an analysis should show that:

    1. Problem reporting procedures during the period of applicable service history were sufficient to provide an appropriate cross-section of in-service problems.

    2. Changes to the referenced system, equipment, or item during the service history period did not materially alter the safety or performance of the system, equipment, or item.

    3. Actual usage of the referenced system, equipment, or item during the service history period was consistent with the intended usage for the new or modified system, equipment, or item; if the operational environments of the existing and proposed applications differ, additional validation and verification activities related to the differences should be conducted.

c. The applicant should analyze any reported safety-related problems, together with their causes and corrective actions, and establish whether or not they are relevant to the proposed system, equipment, or item, modification, or application.

7. NOTES

7.1 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.

7.2 Contributors

Derek Achenbach

Shakil Ahmed

Kathryn Baksa

Steven Beland

Art Beutler

Ahmed Butt

David Cummins

Michael Curran

John Dalton

Aharon David

Laura Dominik

Mark Eley

Sylvain Engel

Charlie Falke

Meade Ferrigan

Stephen Fisher

Daniel Fogarty

Jean Gauthier

Damien Glynn

Mallory Graydon

Humberto Guimaraes

Ricardo Hachiya

Heather Hayes

J.P. Heckmann

Adrian Hiliuta

Lee Howard

Martin Hunter

Salvatore Infantino

Christopher Lacey

Pascal Lambert

Linh Le

Trevor Lewis

Ronald Liffrig

Jim Marko

Bob Mattern

Tone McGregor

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

7.3 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 revision 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 S-18 AIRCRAFT AND SYSTEM DEVELOPMENT AND SAFETY ASSESSMENT COMMITTEE
AND EUROCAE WORKING GROUP WG-63, COMPLEX AIRCRAFT SYSTEMS

APPENDIX A - PROCESS OBJECTIVES DATA

NOTE: The main body of ARP4754B/ED-79B describes the context for the information provided in this appendix. This appendix should be used in conjunction with the main body of this document.

This appendix outlines the aircraft/system life cycle process objectives and data outputs described in this document. Table A1 provides the details by Function Development Assurance Level (FDAL), which should be assigned according to the guidelines in 5.2. Activities of 5.2 are not included in Table A1, since the 5.2 activities are used to identify applicability and rigor for the other activities. The scope and detail of the life cycle data varies depending on the assigned development assurance levels.

Table A1 includes:

a. The process objectives applicable for each development assurance level (5.2):

1. R* - Recommended for certification with process independence.

2. R - Recommended for certification.

3. A - As negotiated for certification.

4. N - Not required for certification.

b. Reference to the section where the system life cycle objective is described; references are only to the third level section heading to provide context.

c. Reference to the life cycle data outputs that support the objective.

d. The System Control (SC) category objectives assigned to the data by development assurance level (see 5.6.4).

Table A1 identifies data content rather than data format. Life cycle data may be combined in a manner consistent with the user's development processes.

Table A1 - Process objectives, outputs, and System Control category

Objective			Objective Applicability and Independence by FDAL (see 5.2)						System Control Category for Outputs by FDAL (see 5.6.4)					
Objective Number	Objective Description	Section	A	B	C	D	E	Output	A	B	C	D	E	Comments
1.0 Development Assurance Planning														
1.1	System development and integral processes activities are defined.	3.3	R	R	R	R	R	Certification Authority coordination						
		3.2	R	R	R	R	N	Development Assurance Plan	②	②	②	②		
		5.1.7	R	R	R	R	N	Safety Program Plan	②	②	②	②		
		5.4.7	R	R	R	A	N	Validation Plan	②	②	②	②		
		5.5.6	R	R	R	A	N	Verification Plan	②	②	②	②		
		5.6.2	R	R	R	R	N	Configuration Management Plan	②	②	②	②		
		5.7.2	R	R	R	R	N	Process Assurance Plan	②	②	②	②		
1.2	Transition criteria and inter-relationship among processes are defined.	3.2.2	R	R	R	A	N	Plans in objective no. 1.1	②	②	②	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective			Objective Applicability and Independence by FDAL (see 5.2)						System Control Category for Outputs by FDAL (see 5.6.4)					
Objective Number	**Objective Description**	**Section**	**A**	**B**	**C**	**D**	**E**	**Output**	**A**	**B**	**C**	**D**	**E**	**Comments**
2.0 Aircraft and System Development Process and Requirements Capture														
2.1	Aircraft-level functions, functional requirements, functional interfaces, and assumptions are defined.	4.2 5.3	R	R	R	R	N	List of aircraft-level functions	①	①	①	①	①	Requirements capture process presented in 5.3 is included in this development process.
								Aircraft-level requirements	①	①	①	②		
2.2	Aircraft functions are allocated to systems based on the aircraft architecture.	4.3	R	R	R	R	N	Aircraft architecture data Aircraft function allocations	①	①	①	②		
2.3	System requirements, system interfaces, and assumptions are defined.	4.4 5.3	R	R	R	R	N	System requirements	①	①	①	②		
2.4	Traceability and/or rationale is captured for system requirements.	5.4.6	R	R	R	A	N	System requirements	①	①	①	②		
2.5	System requirements are allocated to the items based on the system architecture.	4.5 4.6	R	R	R	R	N	System architecture data System requirement allocations	①	①	①	②		
2.6	Appropriate aircraft, system, and item integrations are performed.	4.6	R	R	R	A	N	Verification Summary	②	②	②	②		Integration affords the opportunity to identify and address unintended behaviors; see 4.6.4.
2.7	Summarize development assurance process outputs.	4.7	R	R	R	A	N	Summary of development assurance process outputs	①	①	①	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective			Objective Applicability and Independence by FDAL (see 5.2)						System Control Category for Outputs by FDAL (see 5.6.4)					
Objective Number	Objective Description	Section	A	B	C	D	E	Output	A	B	C	D	E	Comments
3.0 Safety Assessment Process														
3.1	Failure conditions associated with the aircraft/system functions are identified, and their severity classifications are established.	5.1.1 5.1.3	R*					AFHA/SFHA outputs; refer to ARP4761A/ ED-135	①					The AFHA/SFHA processes establish the Failure Condition Classifications used to assign FDAL; modulation based on FDAL does not apply.
3.2	Safety objectives for the identified failure conditions are established.	5.1.1 5.1.3	R*					Safety process outputs; refer to ARP4761A/ ED-135	①					The AFHA/SFHA or PASA/PSSA processes establish the safety objectives used to assign FDAL; modulation based on FDAL does not apply.
3.3	The proposed aircraft/system architecture is evaluated against its safety objectives and relevant safety requirements.	5.1.2 5.1.4	R*	R*	R	A	N	PASA/PSSA outputs; refer to ARP4761A/ ED-135	①	①	①	②		Physical hazards inherent in implementation of aircraft/system functions should be assessed regardless of the development assurance levels assigned to these functions.
3.4	Aircraft-/system-level Safety Requirements, FDAL and IDAL assignments, and assumptions are captured.	5.3.2	R*	R*	R	A	N	Aircraft-/system-level safety requirements, FDAL and IDAL assignments, and assumptions	①	①	①	②		
3.5	The aircraft/system implementation satisfies its safety objectives and relevant safety requirements.	5.1.5 5.1.6 5.1.8	R*	R*	R	A	N	ASA/SSA outputs; refer to ARP4761A/ED-135	①	①	①	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective			Objective Applicability and Independence by FDAL (see 5.2)						System Control Category for Outputs by FDAL (see 5.6.4)					
Objective Number	**Objective Description**	**Section**	**A**	**B**	**C**	**D**	**E**	**Output**	**A**	**B**	**C**	**D**	**E**	**Comments**
4.0 Requirements Validation Process														
4.1	Aircraft/system requirements are complete and correct.	5.4	R*	R*	R	A	N	Validation results	②	②	②	②		Includes coordination of interfaces between systems and between items. System requirements include those allocated to items. Validation affords the opportunity to identify and address unintended behaviors; see 5.4.
4.2	Assumptions are managed.	5.4.2	R*	R*	R	A	N	Validation results	②	②	②	②		
4.3	The functional and safety impacts of derived requirements are acceptable at relevant higher levels.	5.3.3 5.4.6	R*	R*	R	A	N	Validation results	②	②	②	②		
4.4	Validation substantiation is provided.	5.4.2 5.4.7	R	R	R	A	N	Validation Summary (including Validation Matrix)	②	②	②	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective			Objective Applicability and Independence by FDAL (see 5.2)						System Control Category for Outputs by FDAL (see 5.6.4)					
Objective Number	**Objective Description**	**Section**	**A**	**B**	**C**	**D**	**E**	**Output**	**A**	**B**	**C**	**D**	**E**	**Comments**
5.0 Implementation Verification Process														
5.1	Verification methods and procedures are sufficient.	5.5	R*	R	R	A	N	Verification procedures	①	①	②	②		Sufficient verification methods and procedures ensure that the implementation of each requirement can be fully verified.
								Evidence of verification procedure sufficiency	②	②	②	②		
5.2	Verification confirms that the implementation satisfies the aircraft and system requirements.	5.5	R*	R	R	A	N	Verification procedures	①	①	②	②		Verification affords the opportunity to identify and address unintended behaviors; see 5.5.5.3.
								Verification results	②	②	②	②		
5.3	Verification confirms that the implementation satisfies the safety requirements.	5.5	R*	R*	R	A	N	Verification procedures	①	①	②	②		Safety requirement verification may also be included within the ASA/SSA outputs; see Table A1, Objective 3.5.
								Verification results	②	②	②	②		
5.4	Verification substantiation is included.	5.5.6	R	R	R	A	N	Verification Matrix	②	②	②	②		
								Verification Summary	②	②	②	②		
5.5	Assessment of deficiencies and their related impact on safety is identified.	5.5.6	R	R	R	A	N	Verification Summary	②	②	②	②		
								Problem Reports	②	②	②	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective		Section	Objective Applicability and Independence by FDAL (see 5.2)					Output	System Control Category for Outputs by FDAL (see 5.6.4)					Comments
Objective Number	Objective Description		A	B	C	D	E		A	B	C	D	E	
6.0 Configuration Management Process														
6.1	Configuration items are identified.	5.6.2	R	R	R	A	N	CM records	②	②	②	②		
6.2	Configuration baselines are established.	5.6.2 5.6.3	R	R	R	A	N	Configuration Index	①	①	②	②		
6.3	Problem reporting, change control, change review, and configuration status accounting are established.	5.6.2	R	R	R	R	N	Problem Reports CM records	②	②	②	②		
6.4	Archive and retrieval are established.	5.6.2	R	R	R	R	N	CM records	②	②	②	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

Objective		Section	Objective Applicability and Independence by FDAL (see 5.2)					Output	System Control Category for Outputs by FDAL (see 5.6.4)					Comments
Objective Number	Objective Description		A	B	C	D	E		A	B	C	D	E	
7.0 Process Assurance Process														
7.1	Assurance that aircraft/system plans for development assurance are established and maintained.	5.7.3	R*	R*	R*	R	N	Evidence of process assurance	②	②	②	②		
7.2	Development activities and processes are conducted in accordance with the aircraft/system plans for development assurance.	5.7.3 5.7.4	R*	R*	R*	R	N	Evidence of process assurance	②	②	②	②		

R* - Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.

APPENDIX B - SAFETY PROGRAM PLAN

A Safety Program Plan should be established during the development assurance planning process. This plan outlines what should be accomplished to assess the design safety of the product. It also outlines what individuals/organizations should be responsible for accomplishing these tasks and how the assessment will be reviewed and recorded. It is organized on a chronological timeline and arranged according to how a given company assigns responsibilities for the tasks involved. This appendix contains an example which could be used as a template to create an aircraft-level safety plan for a given program.

Each program is unique, and the plan should be tailored to fit the parameters of the program. Also, each company has its own organizational structure and may assign functions to groups or individuals that are different than those shown in the example. This is appropriate; however, several elements of the plan should be represented in all plans. The plan will have to be tailored to the size and scope of the specific program. The example is provided as a template to aid in the creation of the plan and to help assure that all aspects are incorporated. It is not intended to be a prescriptive template but is a guide to organizing a plan.

What follows should cover all aspects of a large-scale development. Smaller programs may show a different structure but should cover the same assessment elements appropriate to the scope of the given product development. For example, a developer of a lower-level system would not include airframe-level reviews.

The objective of the plan is to provide a clear picture at the beginning of a program of the tasks to be accomplished and the individuals/organizations responsible for accomplishing them.

This appendix provides an aircraft-level safety program plan example. An overview of the process, including inputs and outputs, is presented in Figure 6; details for accomplishing the tasks described herein may be found in ARP4761A/ED-135.

Editor’s Notes: Editor’s notes are enclosed in parenthesis and provided in italics. Where necessary, the reader will be directed to the appropriate section of ARP4754B/ED-79B or ARP4761A/ED-135 for further information on the method or process involved. Editor’s notes may also provide clarification to the reader; e.g., when the scope of the example is limited for brevity.

EXAMPLE SAFETY PROGRAM PLAN

TABLE OF CONTENTS

B.1 SCOPE AND PURPOSE

The purpose of this aircraft Safety Program Plan is to define the scope of the safety work, the deliverables planned for the program, and to assign responsibilities. It also indicates the principles of the safety assessment tasks, management, and the schedule for deliverable elements according to the milestones (reviews) of the Development Assurance Plan.

(Editor's Note: Safety plans, although not a certification plan, usually include additional reference and activities related to several certification requirements that include additional details on activities related to the continuous airworthiness and in-service safety, such as Certification Maintenance Requirements (CMRs) and Master Minimum Equipment List (MMEL). This example will present only minor details related to these topics to focus on more details on the safety process associated with ARP4761A/ED-135, not going through ARP5150A/ARP5151A, and to avoid being outdated by newer Certification Authority interpretations and requirements.)

The program has the overall responsibility for the design safety of the product. The activities are organized to accomplish the goal to ensure that the aircraft/system design will not cause or contribute to an aircraft accident. The plan describes the safety processes in general. For each specific process task, the roles and responsibilities have been identified for the responsible parties.

The responsibility for the safety assessment tasks is split among the organizations and groups. The aircraft-level safety analysis tasks are accomplished by an aircraft-level team led by a group with aircraft-level analysis responsibility (e.g., the aircraft safety group).

The safety assessment process should be consistent with industry safety assessment standards. During the conceptual development phase of the program, the process develops and validates requirements using a top-down approach.

During the detailed design and test phase of the program, design implementation is measured against the requirements and is verified using a bottom-up approach. Item requirements verification is gathered into system and eventually aircraft verification as the program proceeds through the build and deliver phase of the program.

B.1.1 Applicable Safety Standards

(Editor's Note: All applicable safety standards of the program should be outlined here.)

B.2 ORGANIZATIONAL STRUCTURE OF THE PROGRAM

(Editor's Note: The organizational structure of the program should be outlined here as shown in Figure B1. Throughout the document is described one potential allocation of roles and responsibilities amongst the Safety and Design Engineering groups. Though this is a viable organization practice, other allocations of responsibilities may be equally appropriate depending on the program, organization, and expertise.)

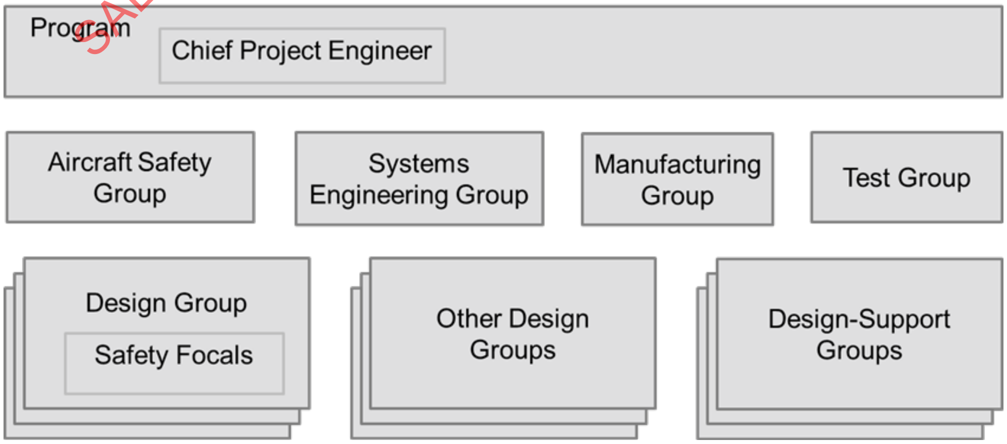


Figure B1 - Example program organizational structure

(Editor's Note: Throughout the document, examples of "Other Design Groups" include Structure and Engine.)

B.2.1 Safety Group Sub-Teams and Working Groups

Sub-teams and working groups, each with a well-defined focus, may be formed, composed by safety specialist from the aircraft safety groups and safety focals from systems design groups and applicable design specialist. The sub-teams allow for better division of safety tasks. An example sub-team is the Particular Risk Review Team (PRRT).

(Editor's Note: The use of sub-teams and working groups will vary based on organizations' practices. The examples are a possible way of accomplishing the activities and processes defined herein.)

B.3 SAFETY RESPONSIBILITIES

The overall ownership of the safety program is chartered with the authority necessary to ensure the program meets all of its requirements. A primary responsibility of this group is to plan, coordinate, and manage safety-related activities and provide a management overview, with the objective that the design will neither cause nor contribute to an aircraft accident. These activities will bring to the program a consistent approach to aircraft/system design safety.

B.3.1 Aircraft Safety Group

An aircraft safety group is chartered with the responsibility to perform and/or monitor the program safety tasks.

The aircraft safety group responsibilities are to:

- Establish and communicate the safety requirements at all tiers of definition
- Ensure that the methods for identifying and evaluating derived requirements at aircraft and system level align with the objectives of the aircraft safety assessment process
- Develop an Aircraft Functional Hazard Assessment (AFHA)
- Perform the Preliminary Aircraft Safety Assessment (PASA), documenting and baselining the results, ensuring that safety requirements are established, validated, and documented, as well as other key assumptions and analysis are documented and communicated to the appropriate groups
- Provide visibility to program management of the program safety activities status
- Develop System Functional Hazard Assessment (SFHA) manual and ensure SFHAs are performed consistently in accordance with this manual
- Perform Particular Risk Analyses (PRA)
- Participate in the Zonal Safety Analysis (ZSA), monitoring the completion and documentation of the activities, and assuring that identified issues were addressed
- Identify safety lessons learned from previous programs and provide visibility to program management and to the development process for consideration
- Identify aircraft-level safety issues and provide visibility to program management responsible for assuring implementation of committed safety changes
- Monitor the completion of the Preliminary System Safety Assessments (PSSA) to ensure that PSSAs' results are baselined and documented, which includes safety requirements established, validated, and documented
- Coordinate to promote consistency of analysis methods and approaches used in verification of safety requirements (e.g., mission lengths and other exposure times)
- Monitor the completion of Aircraft and System Safety Assessments (ASA and SSAs), including the documentation capturing that the safety objectives from the FHAs and the safety requirements from PASA and PSSAs are satisfied

- Coordinate with the test group and flight crew human factors evaluation group to ensure proper testing of the required assumptions and analysis used during safety assessment process

- Work with the chief test pilots and line pilots as applicable to ensure that there are no issues with the design or flight crew assumptions that could lead to a flight crew caused incident or accident

- Work with the maintenance group to ensure that there are no design issues that could lead to a maintenance-caused incident or accident

- Perform an active role in the Candidate Certification Maintenance Requirement (CCMR) meetings

- Perform an active role in the maintenance planning meetings to accomplish the Maintenance Steering Group 3 (MSG-3) planning for scheduled maintenance to ensure that safety issues are resolved and properly dispositioned

- Perform an active role in the flight operations development of the MMEL

- Coordinate aircraft-level safety certification activities

(Editor's Note: As discussed in the scope section, this example will intentionally present only minor details related to CMR, MSG-3, and MMEL aspects. However, it is understood that those aspects are relevant and additional considerations might be included in a safety program plan.)

Aircraft safety group deliverables may include:

- Safety Program Plan

- AFHA

- PASA

- Aircraft-level safety requirements and objectives

- System-level safety requirements

- Validation/verification progress reports, as required for the safety program

- Safety program schedules

- ASA

B.3.2 Safety Program Plan

The aircraft safety group will prepare the safety program plan and maintain it, updating it as necessary. The plan will be reviewed and approved by the Chief Project Engineer and other appropriate leaders of the parties involved in the development program.

The safety program is integrated throughout the development program and addresses those activities that are related to aircraft safety. Satisfactory execution of the safety program will depend on effective participation by all development and development support groups.

Table B1

Roles	Responsibilities
Aircraft Safety group	Prepares safety program plan document. Circulates plan for review, obtains comments, updates the document. Independent review and technical approval of the Safety Program Plan. Obtains formal consent approval signatures from other relevant groups and chief project engineer. Communicates the plan to each involved group. Ensures implementation of the plan.
All design groups	Review and concur with the plan.
Chief Project Engineer	Reviews and authorizes the release of plan.

B.3.3 Safety Requirements

The safety groups, led by Aircraft Safety group, including safety focals from all the aircraft/systems, facilitates the development of aircraft-/system-level safety requirements by performing the safety assessment process. The process includes safety requirement(s) generation and verification that the implementation satisfies its requirements. The safety assessment process is iterative and hierarchically validates these safety requirements for completeness and correctness at each tier, i.e., from aircraft to systems to items to verification of the implementation. Each system-level or aircraft-level safety requirement will have a verification owner having the primary responsibility for its accomplishment. A major role for the design groups will be to ensure that relevant safety requirements are properly acted upon. Applicable regulatory requirements, regulatory guidance, and company requirements will be used to identify safety requirements through the safety assessment process.

Table B2

Roles	Responsibilities
Aircraft Safety group	Documentation and upkeep of aircraft safety requirements.
Systems design groups	Documentation and upkeep of system-level safety plan. Review, concur with, and implement safety requirements where they are an affected owner.

B.3.3.1 Requirements in the Requirements Database

The Aircraft Safety group and the applicable systems design and design support groups will have the responsibility for supplying the information that will be added to the requirements database. The systems engineering group will have the responsibility for managing the database and publishing this material. The system design groups are responsible for reviewing the safety requirements, resolving any issues that arise, and approving the safety portion of the database. The chief project engineer will ensure that the safety objectives and requirements are properly allocated to systems.

B.3.4 Certification Plan for Aircraft-Level Safety

The certification plan for aircraft-level safety contains information showing compliance with 14 CFR/CS Part 25.1309 and other relevant regulatory requirements that take account of the interactions with aircraft systems. This aspect is not usually addressed in the individual system certification plans. In this plan, the aircraft safety group describes the analytical approaches used to show that the program meets those requirements.

Table B3

Roles	Responsibilities
Aircraft Safety group	Prepares certification plan for aircraft-level safety. Independent Review and technical approval of certification plan.
Chief Project Engineer	Reviews and authorizes the release of certification plan.
Certification Authority or delegate	Reviews and approves the certification plan.

B.3.4.1 Aircraft Safety Assessment Document

The ASA document summarizes the program's safety-related activities and provides single point documentation for the tasks identified in the safety plan. It is an output of the ASA process described in B.4.6. All or part of this document may be provided to the Certification Authorities in the form of an aircraft safety certification summary to show compliance with the certification plan for aircraft-level safety.

B.3.5 Aircraft Safety Program Schedule and Milestones

The overall schedule for execution of the safety program plan has been incorporated into the program master schedule. The Safety Program Plan will be effective during the remainder of the preliminary design phase and will continue through aircraft development to first delivery.

B.3.5.1 Preliminary Design Reviews

Preliminary Design Reviews will be performed to ensure that product requirements are complete and correct, and that the design approach is consistent with the requirements. The Aircraft Safety group and safety specialists from design groups will participate in these reviews to ensure that all safety requirements are considered and can be met.

Table B4

Roles	Responsibilities
Aircraft Safety group	Participates in the Preliminary Design Review to ensure all safety requirements, hazards, and safety lessons learned are presented and resolved.
Systems design groups	Conduct the Preliminary Design Review. Ensure that the related safety requirements, hazards, and safety lessons learned are addressed.

B.3.5.2 Critical Design Reviews

Critical Design Reviews will be performed to ensure that product requirements are complete and correct, and the design implementations are consistent with the requirements. The Aircraft Safety group and safety specialists from design groups will take an active part in these reviews to ensure that all safety requirements are being considered and met.

Table B5

Roles	Responsibilities
Aircraft Safety group	Participates in the Critical Design Review to ensure all safety requirements, hazards, and safety lessons learned are presented and resolved.
System design groups	Conduct the Critical Design Review. Ensure that the related safety requirements and the system design definitions are complete and correct.

B.3.5.3 Engineering Safety Review

An Engineering Safety Review will be held prior to first flight to verify that the aircraft and its systems were built in the correct configuration and without flaws or errors that might affect safety of flight. Usually, a number of discrepancies are found which are corrected prior to first flight. This review is a complete inspection of the aircraft. Manufacturing opens access panels and otherwise prepares the aircraft to be inspected as thoroughly as possible. Following this inspection, a determination is made whether the aircraft is ready for first flight.

The program will prepare plans for the Engineering Safety Review well in advance of the scheduled first flight date on the master-phasing schedule. The Aircraft Safety group will review these plans and provided comments. The final plans will be coordinated with all affected groups on the program by the Program.

Chief Project Engineer will lead the meeting and walk-through process for the engineering safety review. Discrepancies identified will be tracked to closure to ensure that all issues are corrected prior to first flight. The Aircraft Safety group and safety specialist from system design groups will support the process as required.

Table B6

Roles	Responsibilities
Chief Project Engineer	Plans and coordinate Engineering Safety Review.
Manufacturing	Makes aircraft available and prepares it for Engineering Safety Review.
Aircraft Safety group	Participates in the Engineering Safety Review to determine that the aircraft was built as designed.

B.3.6 Safety-Related Maintenance Tasks and Intervals

The Aircraft Safety group and safety specialists from design groups will assure that safety-related maintenance tasks and intervals are consistent with the safety analyses, the assumptions, and the safety requirements. The Aircraft Safety group and the design groups (including the safety focal) will participate in both the MSG-3 analysis process as well as CMR process in order to ensure that the design safety requirements are not compromised during the development of the maintenance plan. The safety specialist will provide, based on the safety assessment process, the CCMRs for the Certification Maintenance Coordination Committee (CMCC) meetings.

B.3.7 The Master Minimum Equipment List Process

The Aircraft Safety group will participate in the MMEL development in order to ensure that the design requirements are properly applied to the list of minimum equipment available for dispatch and that the restrictions applied are appropriate and complete.

(Editor's Note: It is not the intent of this example to provide guidelines on the MMEL process, therefore no guidance or detailed information on the activities performed will be presented. Some guidelines and guidance are provided for instance in ARP4761A/ED-135 main body and CS-MMEL.)

B.3.8 Testing

The Aircraft Safety group and safety specialists from design groups will participate in the planning and execution of ground and flight testing to ensure that the design safety issues are addressed. This will include determining what tests are required and the method of testing that will most adequately satisfy the safety requirements and/or confirm the required assumptions and analysis used during safety assessment process. These activities will be in accordance with the aircraft test program plan. The safety groups will maintain oversight on Test Readiness Reviews, including the First Flight Readiness Review. Safety issues arising from testing will be dispositioned using the processes in this plan. Additional tests performed by supplier and/or partners at lower levels will be monitored by the safety groups whenever necessary to ensure that the design safety issues are addressed.

B.4 SAFETY ASSESSMENT PROCESS AND ANALYSIS METHODS

The safety assessment process evaluates aircraft functions and the design of systems performing these functions. The safety assessment process identifies and classifies failure conditions associated with those functions and systems, and applies development assurance rigor commensurate with the classification of those failure conditions. This gives confidence that the likelihood of errors and failures that may lead to failure conditions has been minimized. The safety assessment process is iterative and hierarchically validates safety requirements for completeness and correctness at each tier, i.e., from aircraft to systems to items to verification of the implementation. The process includes safety objective(s) and safety requirement(s) generation and verification that the implementation satisfies its requirements. The safety assessment process is both qualitative and quantitative in nature, with its activities supporting the aircraft development process. Guidelines on the safety assessment processes and analysis methods are detailed in ARP4761A/ED-135.

The Failure Conditions Classification and the safety objectives defined in AC 25.1309 Draft ARSENAL revised and AMC 25.1309 will be used to define the severity of the effects of a failure condition and its related safety objective.

B.4.1 Aircraft Functional Hazard Assessment

The Aircraft Safety group is responsible for developing the AFHA and for ensuring that all system-level FHAs are consistent with other system FHAs and with the AFHA. The AFHA is a high-level, qualitative assessment 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 classification of these failure conditions establishes the safety objectives that an aircraft should meet.

The AFHA is complete when all failure conditions have been clearly identified along with the rationale for their severity classifications. This includes substantiating data showing that all aircraft functions have been considered; all failure conditions have been identified for each aircraft function and flight phase with their resulting severity classifications; the effects are correct and complete; and the assumptions used have been confirmed and evidence is provided.

Table B7

Roles	Responsibilities
Aircraft Safety group	Develops and documents AFHA. Reviews and confirms that the aircraft functions are complete. Provides AFHA key assumptions to the development to be confirmed.
Design groups	Provide input and review of AFHA and its assumptions.

B.4.2 Preliminary Aircraft Safety Assessment

The Aircraft Safety group will also be responsible for performing a PASA based on the AFHA and a proposed aircraft architecture, with refinement over the course of the development program. This team will assess how failures can lead to aircraft-level failure conditions identified by the AFHA and how the AFHA safety objectives can be met. From this activity, it is possible to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the AFHA. In addition, aircraft safety requirements (including independence requirements and Function Development Assurance Level (FDAL) assignments for the associated aircraft functions) can be generated and submitted into the requirement database with appropriate verification owner and affected owners. The PASA process may use various safety analysis methods with more details presented in the next sections. Common cause considerations taken into account in the PASA, including additional details on how requirements are identified and verified, are detailed in the next sections. The team will have the responsibility to track the functional hazard status to closure.

The PASA is complete when all the resulting safety requirements are provided to the development process to guide adjustment of the architecture, requirements, or operations, which will be re-evaluated through this preliminary assessment process until they are found to be achievable. 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.

Once the aircraft-level safety requirements have been defined through PASA process and the implementing systems mature, the project transitions to performing an ASA.

Table B8

Roles	Responsibilities
Aircraft Safety group	Performs, documents, and updates PASA. Proposes corrections and inputs for AFHA, SFHA, and PSSA. Provides proposed safety requirements and key assumptions to the design groups.
Design groups	Review and concur with the inputs for the SFHA and PSSA, as well as with the proposed safety requirements.

B.4.2.1 Common Naming Convention

One of the tools used to perform multi-function analyses when using Fault Tree Analysis (FTA) is a common naming convention for labeling all basic events used in a fault tree. This is required so that multiple occurring events are properly identified. A common naming convention will be used to assign a name to a basic event that will be used across the design groups. This method ensures that multiple occurring events in the aircraft architecture are correctly represented in the tree and identified in cut sets.

Table B9

Roles	Responsibilities
Aircraft Safety group	Develops and implements Failure Mode and Effect Analysis (FMEA) and FTA ground rules and assumptions.
Design groups	Use the ground rules and assumptions document in the development of the FTAs and FMEAs.

B.4.3 System Functional Hazard Assessments

SFHAs are conducted at the beginning of the system development cycle. They should identify and classify the failure conditions associated with the system's functions, including the rationale, assumptions, and any additional supporting information to substantiate classification. The classification of these failure conditions establishes the safety objectives that the system should meet. 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 condition. The Aircraft Safety group will coordinate reviews of SFHAs to ensure that all hazards have been identified and that the FHAs are consistent between design groups and with the AFHA and PASA. These reviews will allow update or completion of the AFHA and the PASA, with potential to identify new or correct safety requirements for each system/function. Although the SFHAs are not needed to start the PASA, these failure conditions are used to support a more complete analysis of the aircraft-level failure conditions to check the system failure effects conditions before the PASA is finished.

Table B10

Roles	Responsibilities
Aircraft Safety group	Ensures the SFHAs are performed in accordance with FHA Manual. Ensures consistency between SFHA and PASA.
Design groups	Perform the SFHAs. Ensure that SFHA rationale, assumptions or any additional supporting information are captured.

B.4.3.1 Functional Hazard Assessment Manual

The Aircraft Safety group should prepare an FHA manual to aid the designers and safety focals in accomplishing the task. This will help to ensure consistency in the FHA results. The manual will include common information such as flight phases, environmental and operational conditions, and naming conventions for labeling the failure conditions.

B.4.4 Preliminary System Safety Assessment

The PSSA is a systematic examination of a proposed system architecture and equipment/item designs to determine how failures can lead to the system-level failure conditions identified by the SFHA. The objective of the PSSA is 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 and safety requirements passed down by the PASA and/or higher-level systems. Once the PSSA process confirms it, the outputs are captured as a baseline. The PSSA process results provide sufficient analysis information to validate safety requirements identified from the PSSA process and may be used for some validation records. The outputs include the safety requirements, analysis information to support their validation, evaluation results for safety requirements and objectives, updated failure condition list, assumptions required to make the PSSA valid, and the necessary FDAL and Item Development Assurance Level (IDAL) assignments for the system function and items. The PSSA is also an interactive process associated with the design definition. The PSSA is conducted at multiple stages of the system development, including system, equipment, and item design definitions.

Table B11

Roles	Responsibilities
Aircraft Safety group	Provides input to the PSSA process. Uses feedbacks from the PSSA in the appropriate processes.
System design groups *	Perform PSSA. Capture key assumptions and safety requirements to design of system, equipment, and/or items. Review and concur with the assumptions and safety requirements used to design the system, equipment, and/or items. Implement changes required.

* The safety activity is performed by a person(s) other than the developer of the system/equipment/item.

B.4.5 System Safety Assessment

The SSA is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the SFHA and relevant safety requirements from the PSSA are satisfied. 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 process may use various safety analysis methods with more details presented in the next sections. A main portion of the SSA usually consists of FTA applied on the actual system implementation to determine what single failures or combinations of failures, if any, can exist at the lower levels that might produce each failure condition. The SSA uses the quantitative values obtained from the reliability predictions, FMEA, or Failure Mode and Effects Summary (FMES). The SSA ensures that all significant failure modes are considered for inclusion in the FTA. During the safety assessment process, the FMES effects should be reviewed to ensure that no new effects by the Line Replaceable Unit (LRU) on multiple systems that were not identified in the FHA and requirements allocation have been found. The SSA also includes common cause considerations, including details on how requirements are defined and verified.

The SSA process is performed in succeeding levels of verification through different levels of systems and subsystems. Hardware reliability requirements and architectural requirements that are allocated throughout the development process are evaluated against the safety requirements identified in the PSSA process. The SSA is complete when it has verified that the implemented system meets the identified safety objectives and requirements (e.g., qualitative, quantitative, FDAL/IDAL assignment, independence) and/or any deviations to the identified safety objectives and requirements, which have been agreed by the higher-level SSA/ASA process.

The resulting SSA documentation shows the delta between the original safety requirements and the new safety requirements, as well as capturing any necessary justification for the requirement and/or architecture changes. If the issue is associated with a requirement received from the PASA/PSSA, the result is fed back to the appropriate processes to determine if a change to the requirement can be made.

(Editor's Note: It is an organizational choice defining how each PASA/ASA and PSSA/SSA process interact.)

Table B12

Roles	Responsibilities
System design groups *	Perform and document the SSA. Review PSSA if necessary. Implement changes required.
Aircraft Safety group	Participates in the SSA. Maintains oversight to ensure that methodologies are consistently applied across systems. Updates ASA/PASA if necessary.

* The safety activity is performed by a person(s) other than the developer of the system/equipment/item.

B.4.6 Aircraft Safety Assessment

The ASA is a systematic, comprehensive evaluation of the complete aircraft to show that safety objectives from the AFHA and safety requirements from the PASA are satisfied. The Aircraft Safety group will integrate the results of the various analyses performed by the safety specialists from the design groups, verifying evidences confirming the applicable aircraft safety requirements are valid and stable, as well as that the analyses (e.g., SSA) used to satisfy aircraft-level safety requirements are completed and reflect the certification configuration. Aircraft-level and multi-function analyses will be conducted to show the aircraft-level safety requirements are satisfied. Finally, the Aircraft Safety group will collect those evidences and analyses and use them as required to be included in the ASA.

Once the aircraft-level safety requirements have been defined through PASA process and the maturity of implementing systems develops, the process converts to assessing the satisfaction of these aircraft-level safety requirements through the system-level PSSAs and SSAs. The ASA ensures that all significant system failure modes are considered for inclusion. The ASA also includes applicable common cause consideration results. The results of these assessments are documented in the ASA, which may be updated incrementally as the aircraft architecture matures. Once the ASA process starts, PASA data may need to be maintained in the PASA records and/or in the aircraft development life cycle data (e.g., requirements and their rationales).

(Editor's Note: It is an organizational choice defining how each PASA/ASA and PSSA/SSA process interact.)

Table B13

Roles	Responsibilities
Design groups	Provide required data for ASA activities. Implement changes required.
Aircraft Safety group	Performs and documents ASA. Independent review and technical approval of ASA. Reviews PASA data if necessary.
Chief Project Engineer	Reviews and authorizes the release of the ASA.
Certification Authority or delegate	Reviews and approves the ASA.

B.4.7 Function Development Assurance Level and Item Development Assurance Level Assignment

The assignment of FDALs and IDALs activity is part of PASA or PSSA processes. These levels of rigor of development assurance tasks are used to substantiate, to an adequate level of confidence, that development errors have been identified and corrected such that the aircraft/systems/items satisfy a defined set of requirements. The activities are associated with the process of establishing the characteristics of how potential errors contribute to failure conditions so that FDALs and IDALs may be assigned in accordance with development process principles. The output of this activity is a list of the functions, their respective FDALs, a list of the items involved with the functions, their respective IDALs, and the documentation of the related Functional Failure Sets. The Aircraft Safety group will oversee the activity to ensure it is consistently applied across systems and processes.

B.4.8 Safety Analysis Methods

The safety assessment process includes safety analysis methods, which are applied throughout the development cycle to provide the analyst a means of qualitatively and/or quantitatively assessing the safety of a design. The Aircraft Safety group will maintain oversight to ensure that these methodologies are consistently applied across systems, especially when required to develop multi-function analyses to be included in the ASA. The following provides a brief description of the methods used:

- A Fault Tree Analysis (FTA) is a failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, an FTA is a “top-down” system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated. The analyst begins with an undesired top-level hazard event and systematically determines all credible single failures and failure combinations of the system functional blocks at the next lower level which could cause this event. The analysis proceeds down through successively more detailed (i.e., lower) levels of the design until a primary event is uncovered or until the fault tree shows support of the undesired event under evaluation.

- Dependence Diagrams (DD) may be used as an alternate method of representing the failure model data. Each DD represents a failure condition (unwanted top event). It is constructed utilizing rectangular boxes, which represent fault events leading to the top event. These boxes are arranged in series or parallel formation. Series chains are OR situations, while parallel chains represent AND situations.

- Markov Analysis (MA) is an alternative method to model failure. It is based on a statistical technique used in forecasting the future behavior of a variable or system whose current state or behavior does not depend on its state or behavior at any time in the past.

- A Failure Mode and Effects Analysis/Summary (FMEA/FMES) is a systematic method for identifying failure modes of a system, function, or hardware item and determining the effects on the next higher level. An FMEA may be developed at any indenture level (e.g., piece-part, function, black box). An FMEA may be used in conjunction with probabilistic techniques such as the FTA to produce a quantitative analysis. The FMES is a summary of failures identified by the FMEA(s) which are grouped together on the basis of their failure effects.

- Model-Based Safety Analysis (MBSA) is a methodology and process where, using a modeling language, the architecture and functional behavior are captured in models which are augmented with failure mode models. The analyst applies a software application to perform an analysis of the system failure propagation model, generating outputs such as failure sequences, minimal cut sets, or other results. This methodology establishes a common communication mechanism between a development team and a safety team.

- A Cascading Effects Analysis (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.

- Common Mode Analysis (CMA) is a qualitative analytical method used to support evaluation of independence by applying, in a logical way, engineering experience systematically to review function, architecture, development, implementation, manufacturing, maintenance, and operation.

- Particular Risk Analysis (PRA) and Zonal Safety Analyses (ZSA) support the overall development of the specific aircraft, system, and equipment architectures by evaluating the overall architecture sensitivity to hazards that might impact multiple systems. PRAs are managed from a global aircraft perspective to address particular physical hazards, within or external to the aircraft, which could affect the airframe globally (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.

(Editor’s Note: The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may stand alone or be incorporated into any of the higher-level assessments. The PRA and ZSA are described as safety methods in this document but, depending on company organization of these aircraft-wide safety activities, they may also be considered as processes in their own right.)

B.5 COMMON CAUSE CONSIDERATIONS

B.5.1 Common Mode Analysis

The CMA activity is used by the safety specialists, at any indenture level (aircraft, system, or item), to evaluate and substantiate independence relative to common cause failures, common cause errors, or both, identifying independence shortcomings (e.g., in architectures or requirements) and thereby documenting and initiating changes to be made. These changes would then be re-evaluated iteratively until the safety process substantiates, with sufficient confidence, that the independence principles can be achieved. As part of the PASA and PSSA, 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. The CMA also supports independence verification occurring after implementation as part of SSA and ASA. The Aircraft Safety group will tailor a CMA questionnaire to be used on the activity, and update whenever necessary, including any new concern that may have arisen during the development. The group will also ensure the transition from the questionnaire to a "final" checklist to be used during the verification activities in the ASA/SSA processes. The team will also oversee the activity to ensure it is consistently applied across systems and processes.

Table B14

Roles	Responsibilities
Aircraft Safety group	Prepares/tailors and updates the CMA questionnaire/checklist to be used during PASA/PSSA and SSA/ASA process. Uses the CMA questionnaire on PASA process to define Independence requirements and assign FDAL. Uses the CMA checklist on ASA process to verify the independence requirements and FDAL assignment. Documents the PASA/ASA CMA findings.
Safety focal from system design groups	Uses the CMA questionnaire on PSSA process to define independence requirements and assign FDAL/IDAL. Uses the CMA checklist on SSA process to verify the independence requirements and FDAL/IDAL assignment. Documents the PSSA/SSA CMA findings.
System design groups	Review and approve the Common Mode Analysis, the independence requirements, and implement changes required.

B.5.2 Particular Risk Analysis

Particular risks are those physical events or influences which may violate independence, or compromise aircraft safety or aircraft survivability. The PRA is not a probabilistic 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 establish the survivability of the aircraft in the presence of each threat, considering all its potential effects, and ensure hazards relevant to the particular risk have been minimized/prevented to the extent practical, in accordance with specific regulatory requirements. A PRRT, led by the Aircraft Safety group, will be set to perform PRA for each particular risk.

The PRRT will aid the safety specialists performing the PASA, ASA, PSSA, and SSA. The PRRT will identify requirements (e.g., physical segregation/separation, survivability, functional interactions) based on proposed installation and/or layout to adequately addresses the independence principles identified in the PASA and PSSA. The results of some analyses conducted as part of the PRA, such as bird strike and tread separation analyses, will contribute to the identification of structural design requirements. Design team will review and approve those requirements so that they can be included into the aircraft requirements database with an appropriate verification owner with the primary responsibility for its accomplishment. Cross-functional teams responsible for specific areas of the aircraft (herein referred to as volume teams) will assure the implementation of those requirements.

PRRT will also perform a verification process, part of the ASA/SSA, using the PRA methodology to ensure that those requirements are implemented into the design and manufacturing of the aircraft. The PRRT will also confirm that, in the event of a defined threat, the aircraft implementation is such that consequences are minimized at an acceptable level in terms of survivability.

The review of the consequences for each particular risk will be documented and any prerequisites upon which it may rely captured in the appropriate requirement database. If consequences are acceptable, justification for certification will be provided. For the unacceptable consequences, the design teams will be informed to perform the changes.

The PRRT deliverables are:

- Identify and characterize the particular risks to be analyzed
- Identify and allocate the related requirements so they can be included in the requirements database
- Assess the aircraft survivability with respect to each identified threat
- Verify that the aircraft design incorporates solutions or adequate mitigations for each identified threat

The team will review all survivability requirements from the company's previous aircraft. They will also research any new threats generated by the new technology used on the aircraft.

Table B15

Roles	Responsibilities
PRRT	Conducts the PRA. Aids the safety specialists performing the PASA, ASA, PSSA, and SSA. Documents the PRA. Identifies proposed requirements and required changes for any unacceptable consequences.
Aircraft Safety group	Leads the PRRT.
Design groups	Participate in the PRRT. Review and approve the PRRT documentation and requirements, and implement changes if required.

B.5.3 Zonal Safety Analysis

A ZSA is performed to evaluate the design and installation of systems and equipment to identify specific interactions or hazards and potential maintenance hazards. A ZSA will be performed in each zone of the aircraft throughout the development process or, when necessary, on the partial re-design of the existing zone. The ZSA will be performed by inspection on each zone and by examining cross-zonal interactions. Early zonal analysis will employ mock-up representation of the basic aircraft design. Later phases of the zonal analysis will be performed on the built aircraft. The analysis consists of consideration of installation aspects of individual systems and equipment and the mutual influence between several systems/equipment installed in close proximity on the aircraft. Zone chiefs will be assigned for each zone of the aircraft. They will lead volume teams (made up of members from systems, design, and safety groups) responsible for the ZSA for their zone, utilizing participants from the affected design groups and from functional support groups, including the Aircraft Safety group and safety focals from design groups. Each team will identify the applicable physical independence requirements (assisted by the zonal questionnaire) related to the independence principles from PASA and PSSA; prepare a ZSA checklist for their zone; and organize a list of inherent hazards (supported by the applicable system design group safety focal). This list is based on, for each system or equipment in the zone, the identification of physical hazards inherent to the system/equipment potentially having external effects.

The Aircraft Safety group will assure the harmonization of the collected information. For the inspections, the volume team, supported by the design groups, will determine the most effective method of completing this task. Methods may include zonal reviews, fly throughs, and as-built reviews. The conclusions of the ZSAs, including records of who, how, and when the assessment was performed, will be documented. Findings of exceptions in the ZSA will also be recorded and result in a design change or a documented justification for a deviation.

Table B16

Roles	Responsibilities
Volume teams	Lead and conduct the ZSA for their areas. Prepare the ZSA material to be evaluated during the ZSA (e.g., checklist/questionnaire). Document the ZSA. Identify required changes for any unsafe installations.
Aircraft Safety group	Participates in the ZSA. Assures the information/criteria harmonization (e.g., questionnaires, inherent hazards) between volume teams. Provides the aircraft-level safety data/requirements. Reviews aircraft-level safety documentation with the results.
Safety focals from design groups	Provide the system-level safety data/requirements. Review system-level safety documentation with the results.
System design groups	Implement design changes required (at any level).

APPENDIX C - DELETED

Previous guidelines in this appendix have been superseded by the material found in ARP4761A/ED-135 Appendix P.

APPENDIX D - DELETED

Previous guidelines in this appendix have been superseded by the material found in 5.2 herein.

APPENDIX E - DEVELOPMENT ASSURANCE CONTIGUOUS EXAMPLE

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

E.1 INTRODUCTION

This appendix provides a detailed example of the aircraft and systems development for a function of a hypothetical S18 airplane. Because the aircraft selected for this example is an airplane, “S18 airplane” is the terminology used.

This appendix describes, in detail, a contiguous example of the design development process for the S18 airplane Wheel Brake System (WBS), with interactive exchanges including handoffs to and from the safety analysis contiguous example in ARP4761A/ED-135 Appendix Q. The goal is to show the interactive relationship between ARP4754B/ED-79B and ARP4761A/ED-135. In order to present a clear picture, some of the airplane-level tasks are provided to better understand potential interactions that may drive requirements down to the WBS level. The function “Decelerate on Ground” is broken down into a single system and its items. This function is chosen because it has sufficient complexity to allow use of all the methodologies, yet is simple enough to present a clear picture of the process flow.

The methodologies applied here are an example of one way to utilize the principles defined in the main body. Other formats may be used to accomplish the documentation, as long as the principles outlined in the main body are followed.

It should be stressed here that the content of this appendix is an illustrative and informative example, and is not meant to be comprehensive in its discussion of the development activity that a program to develop a WBS would entail, or fully represent the outputs that could be created, either in scope or content. This example is not intended to establish any additional recommended practices beyond those described in the main body of the document.

This example contains references to documentation that a company may use to assure itself of the safety of its products, but does not include the documentation that the Original Equipment Manufacturer (OEM) would be required to submit at the airplane level for airplane certification. Some of these documents are submitted to the Certification Authorities for the purpose of certification (e.g., the WBS Functional Hazard Assessment (FHA)). Other documents are internal to the company and not required to be submitted for certification. No implication is made that these documents should be submitted to a Certification Authority, although all documents should be available for submission if requested by the Certification Authority. Safety and certification are not synonymous terms. The example shows the systems engineering process as applied to the development of an airplane, including some processes that are beyond certification requirements. This development process in itself does not constitute a comprehensive process for guaranteeing certification but provides a significant input to the overall certification process success.

In a real development program, the development process is usually far more complex. For example, in a real development program, development of the airplane, airplane systems and items often occurs concurrently, rather than serially as depicted in example flow.

In a real development program, the safety process occurs concurrently with the development processes, constantly receiving inputs from and providing feedback to development processes.

Figure E1 depicts the interaction of activities within this example and in ARP4761A/ED-135 Appendix Q. The blue-shaded rectangles represent the development activities. The yellow-shaded octagons represent the safety activities described in ARP4761A/ED-135 Appendix Q. This figure provides a guide to the structure of the examples and should allow the reader to quickly find specific areas within the example using the cross references. Where iterations are indicated, the directionality of these interactions is not shown; the nature of the interactions in these cases is described in the main body of this document and/or in this example.

In addition to the activities shown in Figure E1, there are two additional integral processes of aircraft and systems development described in this example: configuration management (Section E.6) and process assurance (Section E.7).

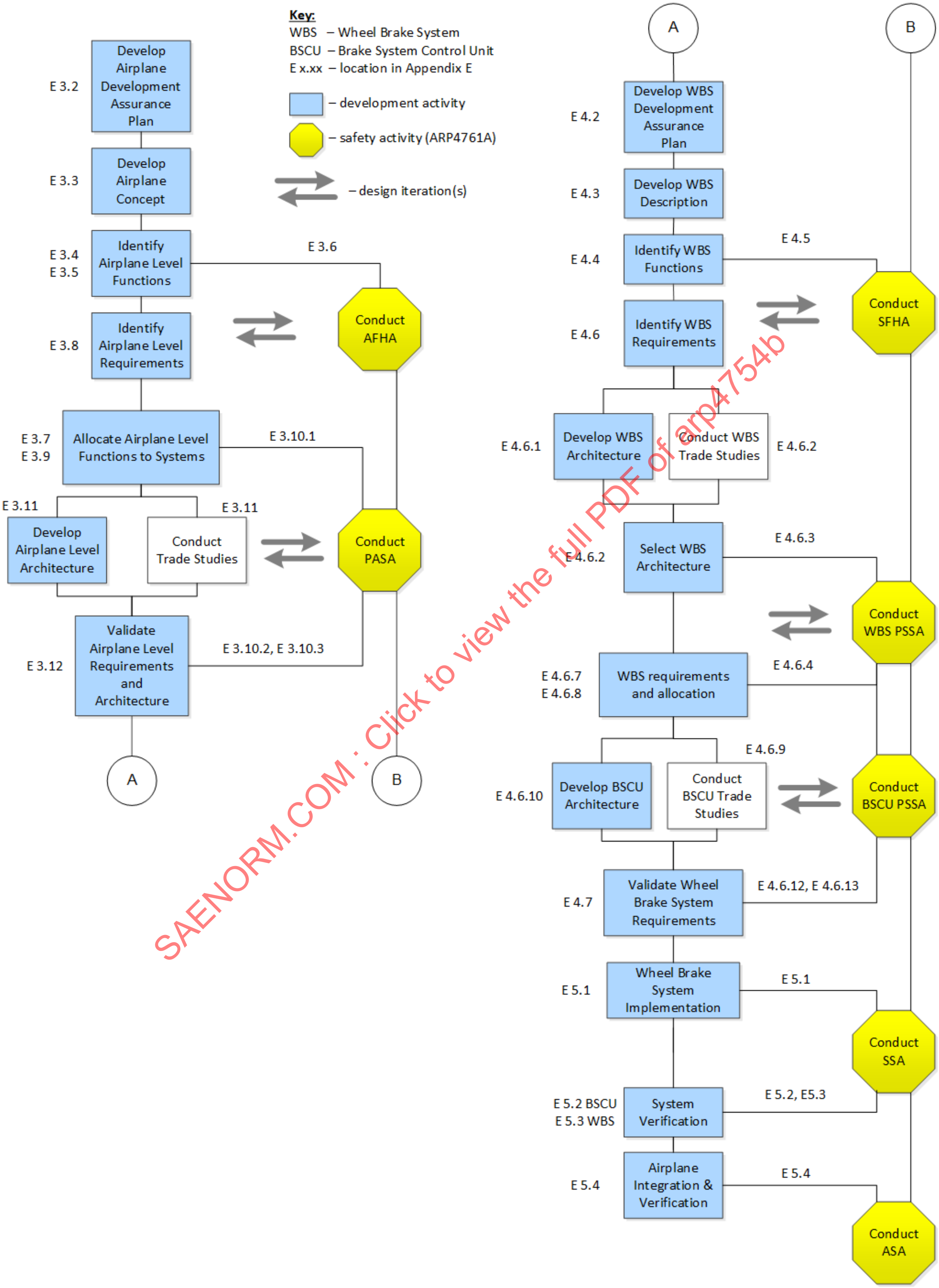

Key:
WBS – Wheel Brake System
BSCU – Brake System Control Unit
E x.xx – location in Appendix E
– development activity
– safety activity (ARP4761A)
– design iteration(s)
E 3.2
Develop Airplane Development Assurance Plan
E 3.3
Develop Airplane Concept
E 3.4
E 3.5
Identify Airplane Level Functions
E 3.6
Conduct AFHA
E 3.8
Identify Airplane Level Requirements
E 3.7
E 3.9
Allocate Airplane Level Functions to Systems
E 3.10.1
E 3.11
E 3.11
Develop Airplane Level Architecture
Conduct Trade Studies
Conduct PASA
E 3.12
Validate Airplane Level Requirements and Architecture
E 3.10.2, E 3.10.3
A
B
A
B
E 4.2
Develop WBS Development Assurance Plan
E 4.3
Develop WBS Description
E 4.4
Identify WBS Functions
E 4.5
Conduct SFHA
E 4.6
Identify WBS Requirements
E 4.6.1
Develop WBS Architecture
Conduct WBS Trade Studies
E 4.6.2
E 4.6.2
Select WBS Architecture
E 4.6.3
Conduct WBS PSSA
E 4.6.7
E 4.6.8
WBS requirements and allocation
E 4.6.4
E 4.6.9
E 4.6.10
Develop BSCU Architecture
Conduct BSCU Trade Studies
Conduct BSCU PSSA
E 4.7
Validate Wheel Brake System Requirements
E 4.6.12, E 4.6.13
E 5.1
Wheel Brake System Implementation
E 5.1
Conduct SSA
E 5.2 BSCU
E 5.3 WBS
System Verification
E 5.2, E5.3
E 5.4
Airplane Integration & Verification
E 5.4
Conduct ASA

Figure E1 - ARP4754B Appendix E and ARP4761A Appendix Q example flow

E.2 DOCUMENT GUIDANCE

This section is intended for guidance to be used throughout the example. This section includes definitions, explanation of sections, and thoughts from the authors.

Editor's Notes: Editor's Notes are enclosed in parentheses and provided in italics. Where necessary, the reader is directed to the appropriate section of ARP4754B/ED-79B or ARP4761A/ED-135 for further information on the method or process involved. Editor's Notes may also provide clarification to the reader, e.g., when the scope of the example is limited for brevity.

The phrase "main body": When the reader sees the phrase "main body," it implies the main body of ARP4754B/ED-79B and the section called out in reference to the example given.

Blue table borders: The use of blue borders indicates information that was received from ARP4761A/ED-135 Appendix Q. The system development process and safety assessment process are concurrent processes with data interfaces. This system development process example contains a number of data inputs (documents, tables, etc.) that are produced by following the safety assessment process in ARP4761A/ED-135 and documented in ARP4761A/ED-135 Appendix Q. Inputs from the safety assessment process are enclosed in boxes to distinguish the data inputs from explanatory text. An example of such a data input is:

Title	
Object Identifier	Object Content

E.3 AIRPLANE DEVELOPMENT PROCESS

E.3.1 Airplane Introduction

The airplane development process included the development of the airplane-level functions, requirements, and architecture for the S18 airplane. The purpose was to develop a list of airplane requirements of all classes as shown in main body 5.3.1, determine a proposed airplane design that can reasonably satisfy the requirements, and develop the lower-level requirements to be considered in the design of the airplane systems, lower-level systems, and items.

E.3.2 Airplane Planning Documents

The airplane Development Assurance Plan defined the development assurance process activities including integral processes of the airplane development life cycle. Also included were the life cycle environment, including the methods and tools to be used for the activities of each life cycle process, and the development standards. The plan was communicated to all S18 program stakeholders.

(Editor's Note: Early coordination with the Certification Authorities for development assurance planning as described in main body 3.3 has not been included in this example. This example does not include any planning documents.)

An example Development Assurance Plan table of contents is included in Table E1. This table is an example of how all planning elements from the main body can be included in a single plan. In some cases, similar content is combined into a single plan section, such as key individual responsibilities, with references to multiple main body sections which call for responsibilities to be defined.

The left-hand side of the table provides a notional plan's section numbers and headers. The right-hand side of the table represents where the reader can find relevant information in the main body. The section numbers have no correlation to the example in this appendix.

Table E1 - Example Development Assurance Plan table of contents

Plan Table of Contents		ARP4754B Reference Section
1	Introduction	
1.1	Scope	
1.2	Applicability	
1.5	Definitions and Acronyms	
2	Applicable Documents	
3	Development Assurance Plan	Section 3
3.1	Development Assurance	1.2
3.1.1	Scope of Development Activity	Section 4, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
3.1.2	Plan Tailoring Rationale	3.3(a.1)
3.1.3	Design Description	3.2.1
3.1.4	Organizational Structure with Roles and Responsibilities, Including Independence	3.2(d), 3.3(c.6), 5.1.7(c), 5.4.7.1(g), 5.5.4(a), 5.6.2.1, 5.7
3.1.5	Complexity Management (Aircraft- or System-Level)	3.2, 4.1.1(a), 4.1.2
3.1.6	Deviations from Plan	3.2.3, 4.7, 5.4.7.3, 5.5.6.4, 5.7.2, 5.7.3.2
3.1.7	Top-Level Processes and Methods	3.1, 3.2, 4.1, 5.1, 5.4.1, 5.4.2, 5.4.6, 5.5.1, 5.5.2, 5.5.5, 5.6.2
3.1.7.1	Architecture Development	4.3, 4.5, 4.6.1.1, 4.6.1.2(b)
3.1.7.2	Integration	4.6.3
3.1.7.3	Implementation	4.2, 4.6, 5.5.3
3.1.7.4	Relationships between Integral Processes	Section 3, 4.1
3.1.7.5	Interactions between Requirement, Design, Safety Activities	4.1.3
3.1.8	Plan to Re-Use Processes, Methods, or Data	3.3(c.4), 5.2.3.3.2, 5.3.1.11
3.1.9	Rationale and Plan to Address “Fully Analyzable and Fully Testable” Systems	3.3(c.5), 4.6.4, 5.5.4, 5.5.5
3.1.10	Key Development Cycle Milestones and Events	3, 3.2(c), 5.1.7
3.1.11	Transition Criteria	3.2.2
3.1.12	Development Assurance Process Outputs	3.3, 4.2, 4.5, 4.6.2, 4.7, 5.1.7, 5.4.7, 5.5.6
3.2	Safety Process	
3.2.1	Scope and Content of Safety Activities (Aircraft- or System-Level)	5.1
3.2.2	Input Requirements for Safety Design and Analysis	5.1, 5.1.7(a)
3.2.3	Applicable Safety Standards	5.1.7(b)
3.2.4	Safety Organization Relationship with Partners or Suppliers	3.3(c.6), 5.1.7(c)
3.2.5	Safety Assessment Activities and Outputs	5.1.7(d)
3.2.6	Validation and Verification of Safety Requirements	5.1.7(f)
3.2.7	Safety Process Interaction with Development Assurance Planning Elements	5.1.7(g)
3.3	Requirements Management	3.3 (c.2)
3.3.1	Requirements Capture	3.1, 5.3
3.3.2	Requirements Management	3.3(c.2)
3.3.3	Management of Safety Requirements	3.3(c.2), 4.1.3, 5.1.2, 5.1.4, 5.1.7(f), 5.3.1.1, 5.3.2
3.3.4	Derived Requirement Evaluation for Safety Impact	5.3.1.10, 5.3.3
3.4	Requirement Validation Process	5.4.1, 5.4.2, 5.4.2.5, 5.4.5
3.4.1	Validation Methods	5.4.5, 5.4.6
3.4.2	Correctness and Completeness Checks	5.4.2.3, 5.4.3, 5.4.4
3.4.3	Management of Assumptions	5.4.2.4
3.4.4	Validation Matrix	5.4.2.5, 5.4.7.2
3.4.5	Validation Summary	5.4.2.5, 5.4.7.2
3.4.6	Validation of Requirement Changes	5.4.7.1(f)
3.5	Implementation Verification	5.5, 5.5.2, 5.5.3, 5.5.4, 5.5.5, 5.5.6
3.5.1	System or Item Configuration to be Verified	5.5.4(b)
3.5.2	Verification Methods	5.5.4(c), 5.5.5, 5.5.6.1(c)

Plan Table of Contents		ARP4754B Reference Section
3.5.3	Verification Success Criteria	5.5.4(d)
3.5.4	Verification Credit from Hardware or Software Activities	5.5.4(e), 5.5.4(f), 5.5.6.1(g)
3.5.5	Verification Activities	5.5.4(g)
3.5.6	Verification Procedures	5.5.3, 5.5.5.3, 5.5.6.3(d)
3.5.7	Verification Data	5.5.6, 5.5.6.1, 5.5.6.2, 5.5.6.3, 5.5.6.4
3.5.8	Sequence of Dependent Verification Activities	5.5.4(g), 5.5.6.1(e)
3.5.9	Verification Test Environment	5.5.4(i), 5.5.5.3.1, 5.5.6.1(h)
3.6	Configuration Management Process	5.6
3.6.1	Configuration Management Methods	5.6.2.1
3.6.2	Configuration Management Environment: Procedures, Tools, Methods, Standards	5.6.2.1
3.6.3	Configuration Identification	5.6.2.2, 5.6.3.1
3.6.4	Configuration Baseline Establishment	5.6.2.3
3.6.5	Change Control and Problem Reporting	5.6.2.4
3.6.6	Archival and Retrieval	5.4.7.1(d), 5.6.2.5
3.6.7	Configuration Data	5.6.3, 5.6.4
3.7	Process Assurance Process	5.7.2
3.7.1	Project Plan Reviews	5.3.7.1
3.7.2	Activity, Data, and Report Reviews	5.7.3.2
3.7.3	Process Assurance Data	5.7.4

E.3.3 Airplane Concept

The S18 airplane was developed by finalizing different high-level airplane operational profiles. The airplane operational profiles were developed from the marketing and business decisions made during these initial marketing efforts, such as independent market surveys, customer requests, and initial design and trade studies. The airplane concept development was the finalization of the different high-level airplane operational profiles, some of which include:

a. High-level airplane requirements (e.g., payload, range)

b. Tradeoff between an airplane that flies faster versus an airplane that consumes less fuel

c. Tradeoff between an airplane that predominately supports hub-and-spoke versus point-to-point operations

The S18 airplane program operating characteristics were established based on customer interface during the initial market research. The airplane concept of operations led to the airplane mission specification, which then led to preliminary airplane sizing and preliminary airplane design. This information was used to create an operational profile for the airplane and was flowed from the airplane level to all systems for use in safety assessments, including the single event effects analysis.

The operational profile for the S18 airplane includes:

a. Two engine passenger airplane for 300 to 350 passengers

b. Maximum range of 5000 nautical miles at 0.86 Mach

c. Altitude ceiling of 41000 feet

d. An average flight duration of 5 hours

e. An airplane life of 100000 flight hours

f. A power on time of 100 operating hours

A concept drawing developed for the S18 airplane is shown in Figure E2.

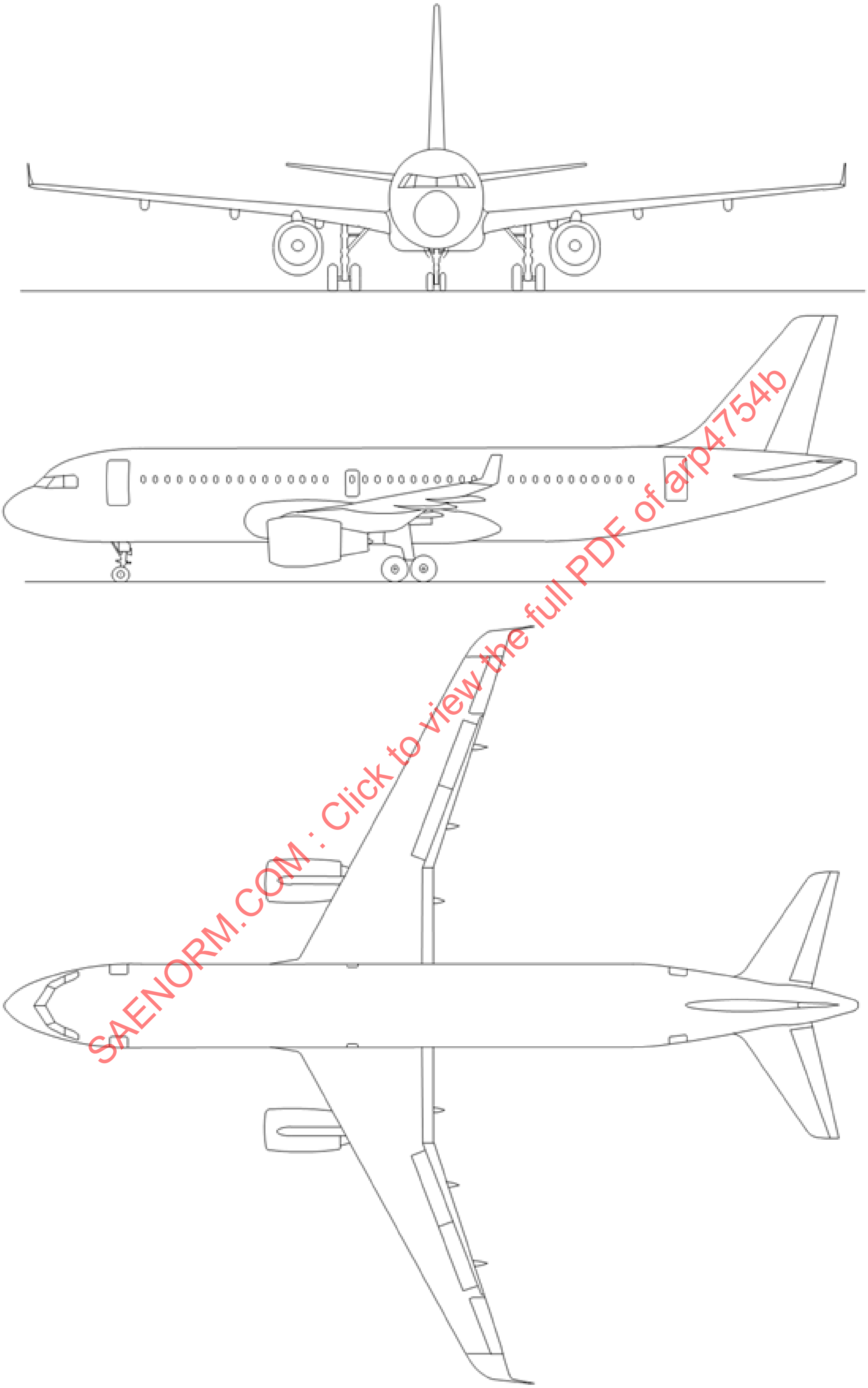


Figure E2 - Airplane concept drawing

Once the airplane concept was firmed up, the development of its functions, architecture, functions allocation, and requirements was initiated, with the process conducted in an almost concurrent, iterative sequence.

E.3.4 Airplane Functions

The airplane functions for the S18 airplane program were initially developed based on prior airplane program history, marketing specifications, and certification requirements for the intended operation of the airplane.

The S18 airplane was designed to perform the following functions:

a. Provide Aerodynamic Performance

b. Control Airplane Trajectory

c. Control Airplane Energy

  1. Maintain or Increase Airplane Energy

  2. Reduce Airplane Energy

    i. Provide Controlled Aerodynamic Drag

    ii. **Decelerate on Ground**

  3. Provide High Lift Capability

d. Provide Survivable Environment

e. Provide Crew Situational Awareness

f. Maintain Structural Integrity

g. Provide Emergency Services

h. Provide Passenger/Cargo Services

(Editor's Note: "Decelerate on Ground" function is in bold text because it is the focus of the example.)

(Editor's Note: The airplane function list shows that there is typically a large context and hierarchy of functions provided to other processes. This example provides enough functional definition to support the system development and safety assessment process examples, but is not a complete functional definition for the S18 airplane.)

E.3.5 Airplane Functional Decomposition

The S18 airplane-level functions as shown in E.3.4 were further defined.

(Editor's Note: To the maximum extent possible, the functions do not imply a specific design/implementation. For example, there are several different design solutions which could be used to decelerate on the ground. The determination of the allocation of functions to systems was completed as part of a trade study not included in this example.)

The S18 airplane-level function "Decelerate on Ground" was decomposed to the system level as shown in Figure E3.

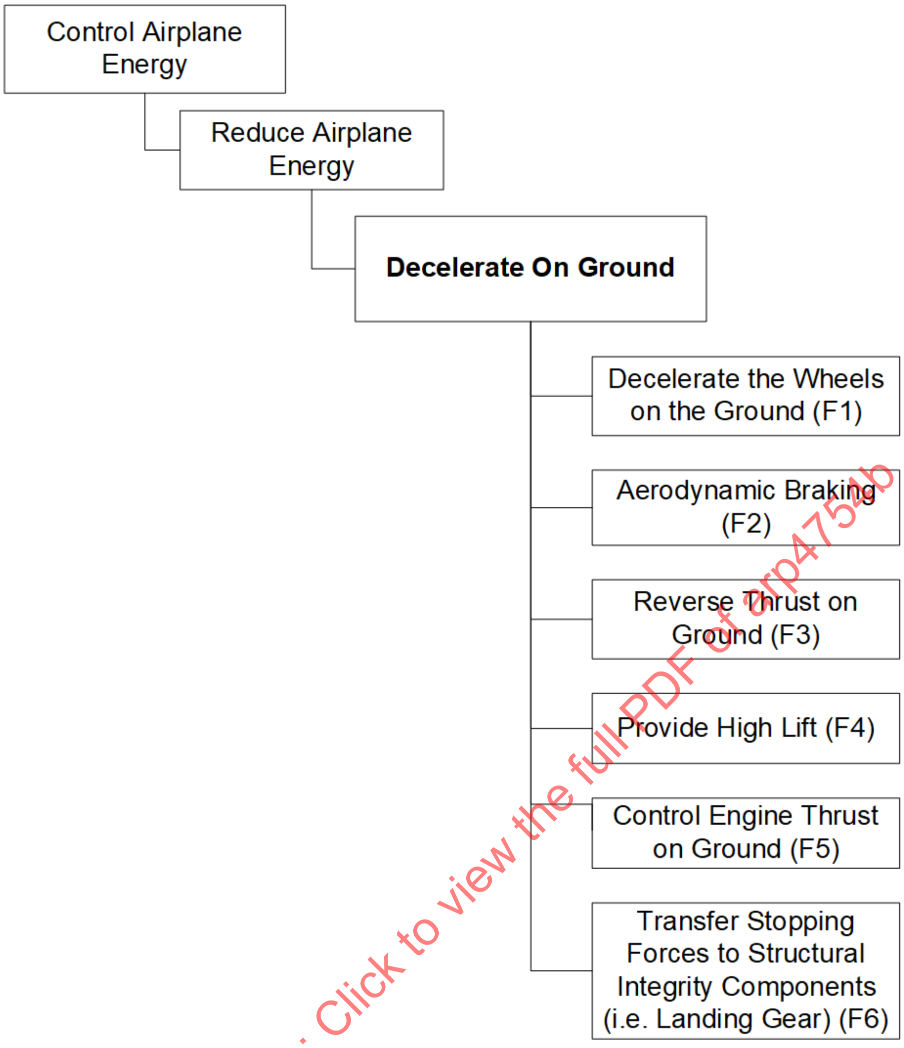

Control Airplane Energy
Reduce Airplane Energy
Decelerate On Ground
Decelerate the Wheels on the Ground (F1)
Aerodynamic Braking (F2)
Reverse Thrust on Ground (F3)
Provide High Lift (F4)
Control Engine Thrust on Ground (F5)
Transfer Stopping Forces to Structural Integrity Components (i.e. Landing Gear) (F6)

Figure E3 - Decomposition of Decelerate on Ground function

When used, Fx notation represents the identification of a function that is considered to implement the aircraft function “Decelerate on Ground.”

E.3.6 Aircraft Functional Hazard Assessment (AFHA) Interactions

Using the airplane operational profile from E.3.3 and functional failures for each of the airplane functions identified in E.3.4, the AFHA determined airplane-level hazards as part of the safety assessment process.

The AFHA provided hazards associated with the function “Decelerate on Ground.” The failure condition severity classification assigned in the AFHA (e.g., Major, Hazardous, Catastrophic), along with conditions assigned that moderate the hazard (e.g., runway departure speeds), was a factor in determining the airplane architecture required for the “Decelerate on Ground” function.

The AFHA hazards for the “Decelerate on Ground” function are found in ARP4761A/ED-135 Appendix Q.

(Editor’s Note: The AFHA activity was conducted in accordance with the guidance of ARP4761A/ED-135 Appendix A. Although this example focuses on the “Decelerate on Ground” function, other airplane functions might have been allocated to the WBS, such as “Control Direction on Ground.”)

E.3.6.1 AFHA Assumptions

Assumptions made while accomplishing the effect evaluation of each failure condition have been captured and numerically identified for reference. Table E2 presents the assumptions analysis made during the development of this functional hazard assessment. These assumptions were confirmed through the development process and the confirmation communicated back to the AFHA process.

Table E2 - AFHA assumptions

Assumption Identifier	Description
ASMP 3.2.2-1	Overrunning the runway length above “XYZ” knots is considered a high speed overrun.
ASMP 3.2.2-2	The directional aspect of asymmetric failures of deceleration systems are functionally addressed by failure conditions of the “Control direction on ground” airplane function (see function 2.3 AFHA).
ASMP 3.2.2-3	The flight crew will divert to a suitable airfield if aware of a condition that renders the airplane incapable of landing at the originally intended destination.
ASMP 3.2.2-4	Crew awareness is not a factor for the identified malfunction, as these are immediately evident due to aircraft behavior and do not have their effects intensified or mitigated by crew awareness features.
ASMP 3.2.2-5	The flight crew will not initiate a Rejected Takeoff (RTO) in response to an annunciated failure of deceleration features during takeoff due to alert suppression.
ASMP 3.2.2-6	Taxi is performed at groundspeeds below 30 knots.
ASMP 3.2.2-7	Landings with failure condition in combination with environmental factors have been assessed.
ASMP 3.2.2-8	Failures of deceleration capability will be detected and annunciated by on-board systems.

E.3.7 Initial Airplane Architecture Development and Function Allocation

After airplane function decomposition in Figure E3, the airplane architecture development was initiated with supporting systems identified, and airplane sub-functions were allocated concurrently to the airplane’s supporting systems.

E.3.7.1 Initial Airplane Architecture

Airplane architectures were developed for each airplane function, given airplane requirements and AFHA categorizations that were developed. The airplane architecture development determined resulting airplane systems included on the airplane, and was an iterative process with the airplane function allocation process and the Preliminary Aircraft Safety Assessment (PASA) process.

Review of the S18 airplane architecture showed that the “Decelerate on Ground” function was intended to be accomplished using two independent systems:

a. Wheel brakes. The S18 airplane has two main landing gear struts with four wheels each for a total of eight wheels. Each wheel is equipped with a brake.

b. Thrust reversers. The S18 airplane is equipped with a thrust reverser on each engine. The thrust reversers are intended to aid deceleration, especially in conditions where friction-based deceleration is ineffective (wet or iced runways).

The following airplane features might have affected the “Decelerate on Ground” function:

a. Engines. The S18 airplane has two under-wing mounted turbofan engines in order to produce forward thrust. The engine thrust is reduced during deceleration on ground, to maximize deceleration and allow deployment of the thrust reversers.

b. Flaps. The S18 airplane’s wings are each equipped with two flap panels. The flaps are extended to increase the wing’s lift and drag coefficients. The flaps are extended to allow lower takeoff and landing speeds, which facilitates deceleration on ground.

c. Spoilers. The S18 airplane’s wings are each equipped with two spoiler panels. The spoilers are intended to be deployed on landing, to reduce lift and increase the effectiveness of the wheel brakes.

The initial airplane-level architecture of the WBS, as shown in Figure E4, was provided to the PASA process.

(Editor's Note: Interfaces to the hydraulics systems and the Electric Brake Unit (EBU) are shown, but detailed development and safety analysis are outside of the scope of this example.)

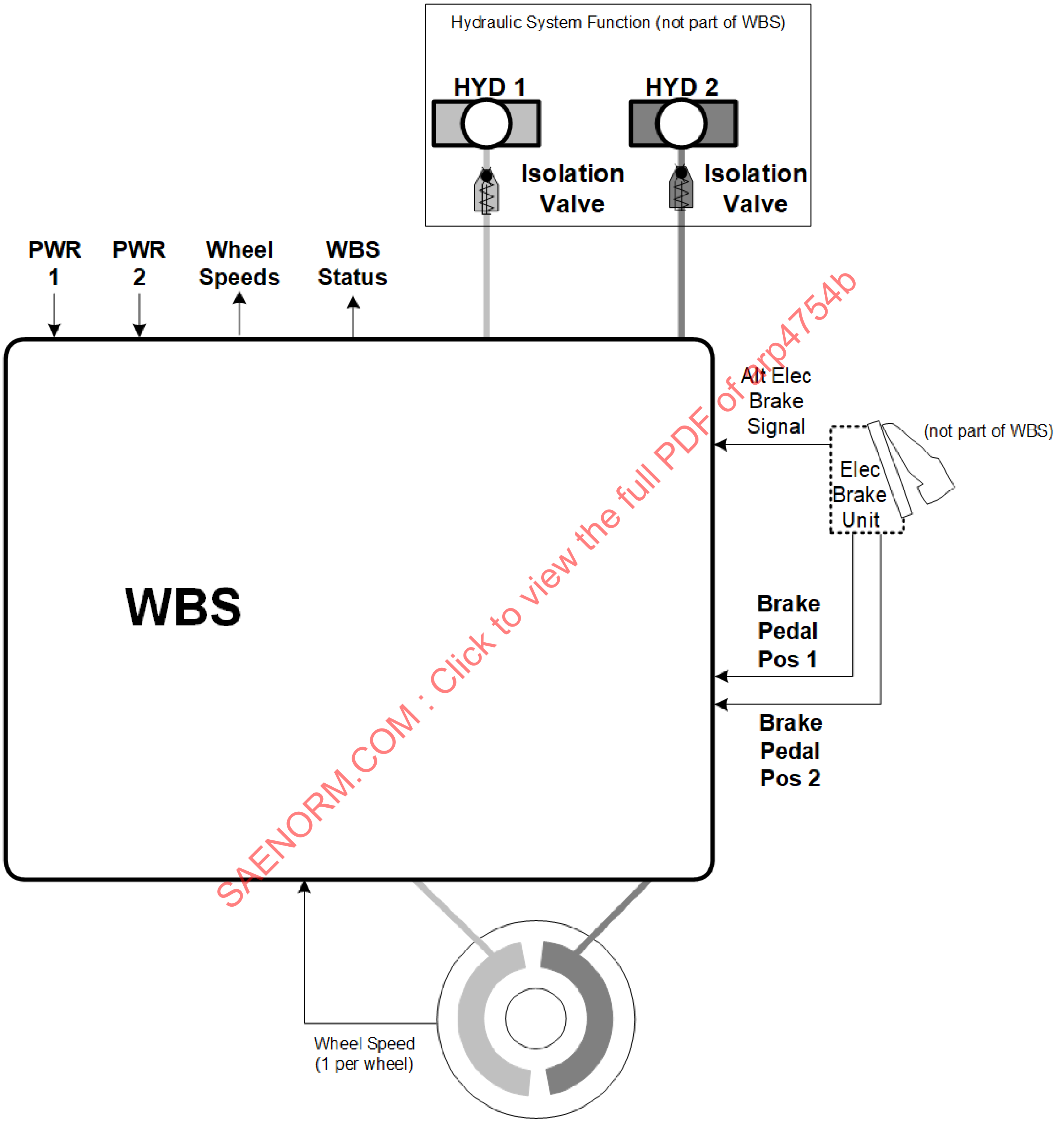


Figure E4 - Initial airplane-level Wheel Brake System architecture schematic

E.3.7.2 Airplane Function Allocation

The S18 airplane-level functions as shown in E.3.4 were defined during the airplane architecture development process. The next process step was to allocate functions to the supporting systems.

The S18 airplane-level function allocation for “Decelerate on Ground” is shown in Table E3. The initial WBS requirements, presented later in E.4.5, were outputs of the allocation activity, along with the functional requirements for the other systems' functions shown in Table E3. Table E3 content assumes some systems were present on the S18 airplane, as shown in the top row (Wheel Brake System, thrust reverser, etc.). These systems were identified from the development of the initial high-level architectures. This allocation was an important input into the PASA. The purpose of the function allocation was to identify the system(s) which implement the respective function(s).

(Editor's Note: Function allocation was a recursive, iterative process. After airplane functions were allocated to systems by the design process, each system which integrates multiple airplane functions was re-examined using the System Functional Hazard Assessment (SFHA) process.)

Table E3 - Airplane function allocation (excerpt)

Function	S18 Airplane	Wheel Brake System	Thrust Reverser	Spoilers	Flaps	Engine Controls	Structural Integrity (Landing Gear, Fuselage, etc.)
Decelerate on Ground	X	X	X	X	X	X	X
Decelerate the Wheels on the Ground		X					
Reverse Thrust on Ground			X			X	
Provide Aerodynamic Braking				X			
Provide High Lift					X		
Control Engine Thrust on Ground						X	
Transfer Stopping Forces to Structural Integrity Components				X			X

E.3.8 Airplane Requirements Development

The initial development of airplane requirements included market/technology research and certification requirements. These requirements established preliminary requirement sets. Usage of “know how” from previous programs expanded this preliminary requirement set to a degree sufficient for initial architecture trade studies.

(Editor's note: For the sake of brevity, not all airplane requirements are discussed.)

E.3.8.1 Sizing Requirements Derived from Airplane Runway Operating Requirements

The S18 airplane and its systems were “sized” for the intended mission as defined by market requirements. The intended mission included requirements to operate from specific runway types and lengths. In addition, regulations 14 CFR/CS 25.125(c) and 14 CFR/CS 25.735 specified requirements applicable to this function. Factors that translated the function “Decelerate on Ground” into quantified requirements for the WBS included the following:

- Airplane landing weight
- Airplane takeoff weight
- Takeoff and approach speeds
- Flight characteristics of the airplane
- Specified airplane operating environmental conditions

- Assumed failure conditions, including those specified by certification requirement 14 CFR/CS 25.735

The sizing requirements for the WBS was developed as a function of required energy absorption, and deceleration requirements.

E.3.8.2 Airplane Requirements Specification

Table E4 is an excerpt from the initial airplane requirements specification that showed a subset of the requirements which were used to trace to WBS requirements. Additional airplane requirements might have been obtained from other sources, such as regulatory material. It should be noted that those requirements required to comply with 14 CFR/CS 25.735 and sub-sections were further decomposed once allocated to the WBS.

Table E4 - Initial S18 Airplane Requirements Specification (excerpt)

Requirement Number	Requirement	Source	Additional Information
S18-ACFT-R-1000	The S18 airplane shall have a means to decelerate on ground.	Airplane concept	Must comply with 14 CFR/CS 25.735.
S18-ACFT-R-1100	The S18 airplane shall have a means to decelerate the wheels on ground.	Airplane concept	Must comply with 14 CFR/CS 25.735.
S18-ACFT-R-1110	The S18 airplane shall have pilot-controlled wheel braking capability.	Airplane concept	Conventional pedal based controls scheme was confirmed by airframe design team in coordination meeting ABC123. Must comply with 14 CFR/CS 25.735.
S18-ACFT-R-1120	The S18 airplane shall have an autobraking capability during landing and RTO.	Business case trade study	Business case trade study established the need for technological improvements in CAT IIIb auto-landing capability. (Report MRS18-XXX) Must comply with 14 CFR/CS 25.735(c)(2).
S18-ACFT-R-1130	The S18 airplane shall have anti-skid braking.	Business case trade study	Business case trade study established the need for all weather operation and stability of the airplane during runway runs. (Report MRS18-XXX). Must comply with 14 CFR/CS 25.735 (e).
S18-ACFT-R-1140	The S18 airplane shall provide interface for Wheel Brake System status and annunciations.	Business case trade study	Business case trade study TS18-XXXX determined the need to provide WBS information to the crew.
S18-ACFT-R-0181	The S18 airplane shall decelerate the wheels on gear retraction.	Business case trade study	Business case trade study TS18-XXXX determined the need to prevent high speed wheel rotation after the gear are stowed.
S18-ACFT-R-0182	The S18 airplane shall be capable of decelerating the wheels differentially.	Business case trade study	Business case trade study TS18-XXXX determined that nose gear alone are not sufficient to steer the aircraft under all environmental and operational conditions.
S18-ACFT-R-0183	The S18 airplane shall have a parking brake to prevent airplane motion on the ground.	Airplane concept	The regulation defines the need for parking brake control and defines performance requirements. Must comply with 14 CFR/CS 25.735(d).
S18-ACFT-R-0184	The S18 airplane shall have hydraulically driven braking.	Business case trade study	Business case trade study TS18-XXXX determined that the hydraulic drive of WBS is more economically feasible than electrical systems given the reuse of hydraulic systems from previous S18 airplane. Once the mechanism has been determined that will power the wheel brake, then that power system must be compliant with 14 CFR/CS 25.735 (b).

Requirement Number	Requirement	Source	Additional Information
S18-ACFT-R-0185	The S18 airplane shall have an autobrake override that can be initiated by the flight crew.	14 CFR/CS 25.735(c)(2)	N/A
S18-ACFT-R-0186	The S18 airplane shall meet safety requirements while operating in an average atmospheric radiation environment per the IEC 62396 standard with an altitude of 40000 feet and a latitude of 45 degrees.	S18 airplane internal documentation	IEC 62396, referenced in AIR6219/ER-008, is the industry standard for analyzing single event effects. For the operational mission selected, the industry average for the radiation environment is appropriate.

E.3.9 Preliminary System-Level Architecture Development for "Decelerate on Ground" Function

Once the airplane-level function decomposition and allocation to systems (shown in Figure E3 and Table E3) and architecture matured in development, development of system-level architecture was pursued further to fulfill airplane-level requirements. At the same time, common resource systems required for the airplane systems to perform their functions were identified and defined. System-level architecture and system-level common resources that supported the "Decelerate on Ground" function are described in E.3.9.1 and E.3.9.2, respectively.

E.3.9.1 Architecture for "Decelerate On Ground" Function

a. Wheel Brake System (WBS): The WBS actuates all eight brakes on the main gear wheels. An EBU provides brake pedal position inputs to the WBS. The WBS is hydraulically actuated and powered by hydraulic system 1 (HYD 1) and hydraulic system 2 (HYD 2). The WBS is electrically controlled. The WBS uses redundant electrical buses such that no single electrical bus loss results in loss of the WBS. The WBS uses the ground detection information as an input. The WBS implements the function "Decelerate the Wheels on the Ground (F1)."

b. Ground Spoiler System: The ground spoiler system actuates all four spoilers on the wings. The symmetric spoilers on the left and right wings are controlled in pairs. The two pairs of spoilers may be commanded symmetrically in response to pilot manual commands. There is no automatic spoiler command in the S18 airplane. There is no other method of controlling or actuating the spoilers. The ground spoiler system is hydraulically actuated and powered by HYD 1 and hydraulic system 3 (HYD 3). The ground spoiler system is electrically controlled by an Electronic Flight Control Unit (EFCU). The ground spoiler system uses redundant electrical buses such that no single electrical bus loss results in loss of any EFCU channel. The ground spoiler system uses the ground detection information and wheel speed data as inputs. The ground spoiler system implements the function "Aerodynamic Braking (F2)."

c. Thrust Reverser System: The thrust reverser system controls and actuates the thrust reversing mechanisms on each engine. Each reversing mechanism is controlled independently in response to pilot manual commands. There is no automatic thrust reverser command in the S18 airplane. The thrust reverser system is hydraulically actuated and powered by HYD 1 and HYD 2. The thrust reverser system is electrically controlled by an Electronic Engine Control Unit (EECU). The thrust reverser system uses redundant electrical buses such that no single electrical bus loss results in loss of any EECU channel. The thrust reverser system uses the ground detection information as an input. The thrust reverser system implements the function "Reverse Thrust on Ground (F3)."

d. Flap System: The flap system actuates the multiple flap surfaces on the wings. All flap surfaces are controlled simultaneously in response to pilot manual commands. There is no automatic flap command in the S18 airplane. There is no other method of controlling or actuating the flaps. The flap system is hydraulically actuated and powered by HYD 1 and HYD 3. The flap system is electrically controlled by the EFCU. The EFCU uses redundant electrical buses such that no single electrical bus loss results in loss of any EFCU channel. The flap system implements the function "Provide High Lift (F4)."

e. Propulsion System: The propulsion system controls forward thrust on each engine in response to pilot manual commands. There is no automatic propulsion command in this S18 airplane. The propulsion system is electrically controlled through 2 EECUs. The left-hand engine EECU controls the left-hand engine and the right-hand engine EECU controls the right-hand engine. The propulsion system relies on ground detection information from other airplane systems as an input. The propulsion system implements the function "Control Engine Thrust on Ground (F5)."

E.3.9.2 Common Resources for "Decelerate On Ground" Function

a. R1 Hydraulic System: The hydraulic system provides power to multiple airplane systems. There are three hydraulic systems on the S18 airplane. HYD 1 is driven by engine 1 (left hand). HYD 2 is driven by engine 2 (right hand). An additional hydraulic system, HYD 3, provides minimal flight control capability in case of the loss of all engines in flight; refer to 14 CFR/CS 25.671(d).

b. R2 Electrical System: The electrical system provides power to multiple airplane systems. There are three major electrical buses distributing power to airplane systems. Each major electrical bus can be powered by one or more engine driven generators. The system architecture was conceived to provide power to multiple systems such that no single electrical system failure causes loss of any essential loads.

c. R3 Ground Detection Information System: The ground detection information system provides information to multiple airplane systems. The in-air or on-ground status of the airplane is determined by detecting compression of the left and right main landing gear shock absorbers and its information is consolidated using both signals. Whenever the signals mismatch, an additional input from wheel speed is used to accommodate this failure. The air/ground system is electrically powered.

E.3.10 Preliminary Aircraft Safety Assessment Interactions

In parallel with the airplane development process, the PASAs were performed with the design configuration identified early in the airplane development. This was an iterative process between development and safety assessment, with the objective to define an airplane architecture that met the safety requirements.

E.3.10.1 Provide Airplane Information to PASA Process

The development process provided airplane functions, airplane requirements, airplane architecture, and airplane function allocation to the PASA process. The airplane functions, architecture, function allocation, and requirements are shown in E.3.4, E.3.7.1, E.3.7.2, and E.3.8, respectively.

E.3.10.2 Assignment of Function Development Assurance Level

The AFHA was conducted as part of the safety assessment process described in ARP4761A/ED-135 Appendix Q. The outputs of the AFHA process, which provided inputs to the PASA process, were the failure conditions, effects, classification, and safety objectives. Based on those safety objectives, the PASA process assigned the Function Development Assurance Levels (FDALs) as shown in Table E5. The Development Assurance Plan included the means to develop functions as FDAL A and C. Further development assurance level details were expected from the Preliminary System Safety Assessment (PSSA).

When used, Fx notation represents the identification of a function, while [FFx] is a general function failure of Fx, and [FFx.y] is a detailed functional failure of function Fx. While used in the aircraft-level safety assessments, this notation is not otherwise carried forward into system development activities or data.

Table E5 - FDAL assignment (PASA outputs)

Function Development Assurance Level	
PASA-SR-01	[F1] Decelerate wheels function shall be developed FDAL A
PASA-SR-02	[F2] Ground spoiler function shall be developed FDAL C (as minimum)
PASA-SR-03	[F3] Thrust reverser function shall be developed FDAL C (as minimum)
PASA-SR-04	[F4] Flap function shall be developed FDAL C (as minimum)

(Editor's Note: All PASA FDAL assignments are shown in Table E5 for consistency with ARP4761A/ED-135 Appendix Q. However, only the Decelerate Wheels FDAL assignment, PASA-SR-01, is discussed later in this appendix. The other FDAL assignments shown in Table E5 apply to systems outside the focus of this example. PASA-SR-01 is addressed through the generalization of representing a single FDAL A function validated and allocated to the systems level for further decomposition. This is captured with an FDAL attribute for each requirement at the lower levels. Table A1 provides the applicability of the objectives for each FDAL and process. Safety requirements were developed by the PSSA and required validation and verification commensurate to their failure condition.)

The Development Assurance Plan addressed the generation of evidence and data that supported the development of functions with different FDALs. Development activities were performed, and associated evidence and data was generated as defined in this plan. The Development Assurance Plan outlined the means used to perform, review, and approve development activities for varying FDAL levels. The Development Assurance Plan defined the appropriate process required for the FDAL for a particular function or item (see main body 3.2).

(Editor's Note: FDALs do not imply particular random failure probabilities. Probabilities are allocated separately from the FDAL assignment process.)

E.3.10.3 Proposed Safety Requirements from PASA and Safety Methods

The proposed safety requirements in Table E6 were inputs received from ARP4761A/ED-135 Appendix Q, Preliminary Aircraft Safety Assessment.

Table E6 - Proposed safety requirements (PASA output)

SR#	Proposed Safety Requirements
PASA-SR-05	[FF1.1] Complete loss of wheel brake shall be less than 1.0E-07 for a landing.
PASA-SR-06	[FF2.2] Symmetrical partial loss of ground spoiler shall be less than 1.0E-03 for a landing.
PASA-SR-07	[FF3.2] Loss of one thrust reverser shall be less than 1.0E-03 for a landing.
PASA-SR-08	[FF4.2] Symmetrical partial loss of flaps shall be less than 1.0E-03 for a landing.
PASA-SR-09	No single failure or event shall result in the complete loss of wheel brake and the symmetrical partial loss of ground spoiler
PASA-SR-10	No single failure or event shall result in the complete loss of wheel brake and the loss of one thrust reverser.
PASA-SR-11	No single failure or event shall result in the complete loss of wheel brake and the symmetrical partial loss of flap.
PASA-SR-12	Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.
PASA-SR-13	The Alternate/Emergency Brake System hydraulic equipment and piping shall be installed aft of the engine 1 UERF trajectory envelope.
PASA-SR-14	Two redundant control lanes shall be provided between the Electric Brake Unit and each of the two Alternate/Emergency Meter Valves.
PASA-SR-15	Two redundant control lanes defined in the proposed requirement [PASA-SR-14] shall use vertically separated routes in the portion of the fuselage crossing the UERF area so that no engine 1 UERF debris can affect both lanes together.
PASA-SR-16	At least one of the two redundant control lanes between the Electric Brake Unit and each of the two Alternate/Emergency Meter Valves shall allow control of the corresponding valve until complete stop of the airplane in case of loss of power from both engine driven generators.
PASA-SR-17	The control lane between the EBU and each of the two Alternate/Emergency Meter Valves allowing control of the corresponding valve until complete stop of the airplane in case of loss of power from both engine driven generators shall be routed in the cabin ceiling area in the portion of the fuselage crossing the UERF area.
PASA-SR-18	Flailing shaft of the flap hydraulic motor moving parts shall not impact on brake pressure valve.

(Editor's Note: PASA proposed safety requirements are shown in Table E6 for consistency with ARP4761A/ED-135 Appendix Q. However, only requirements PASA-SR-05, PASA-SR-10, PASA-SR-12, PASA-SR-13, and PASA-SR-14 are discussed later in this appendix. The other proposed safety requirements shown in Table E6 apply to systems outside the focus of this example. UERF acronym stands for Uncontained Engine Rotor Failure. The acronym is left in Table E6 because that is how it is received from safety as shown by the blue box.)

While most proposed safety requirements were expected to be generated by the PASA, safety analysis methods generated proposed safety requirements and provided them to the development process. The proposed safety requirement as shown in Table E7 was received from the ARP4761A/ED-135 Appendix Q, Particular Risk Analysis (PRA).

Table E7 - Proposed safety requirements (PRA output)

Reference	Proposed Requirement	Rationale	Allocated to
PRA-UERF-FUEL-01-01	The fuel tank design shall include outer wing tanks which alone retain sufficient fuel reserves to ensure completion of the flight or a safe diversion, and are located outside the UERF trajectory envelope.	In case of large external fuel leak as a result of damage to fuel tanks caused by a UERF, the airplane's flying range may be affected to the point that the aircraft will not be able to reach its destination airport or any diversion runway, with potentially Catastrophic consequences.	Structure Design

(Editor's Note: This proposed safety requirement from the PRA is shown in this example to illustrate this source of safety requirements. However, the proposed safety requirement shown in Table E7 is outside the focus of this example.)

E.3.11 Follow-On Airplane-Level Architecture Development

The PASA process provided the following architecture feedback:

The hydraulic common power source analysis described in ARP4761A/ED-135 Appendix Q pointed out that because thrust reversers and wheel brakes use only HYD 1 and HYD 2 power sources, the airplane does not satisfy the safety objective for loss of deceleration capability if the probability of loss of both HYD 1 and HYD 2 was not extremely improbable (>1.0E-09).

Furthermore, the PRA showed that the current airplane design was not sufficient to satisfy an independence principle because a single UERF event could cause loss of wheel brakes and thrust reversers caused by the simultaneous loss of both HYD 1 and HYD 2 power sources.

Therefore, PASA recommended an additional means of ensuring sufficient power for airplane deceleration other than using HYD 1 and HYD 2 powers only, according to PASA-SR-12. The development process captured this requirement in S18-ACFT-R-1550 and considered all possible solutions. Based on a Hydraulic-Electric Brake Study, the design team chose to incorporate a hydraulic accumulator (i.e., emergency accumulator) capable of providing sufficient energy to assure safe airplane deceleration by braking the wheels during all airplane operational modes including the HYD 1 and HYD 2 loss case (S18-ACFT-R-1551).

Furthermore, the PRA showed that the current airplane design was not sufficient to satisfy an independence principle because a single UERF event could cause loss of wheel brakes caused by the simultaneous loss of both NORMAL Mode and the single alternate brake signal between the EBU and the WBS.

Therefore, the PASA proposed a dual redundant command path from the EBU to the Alternate/Emergency Meter Valves, according to PASA-SR-14.

Figure E5 reflects the design changes resulting from architecture feedback.

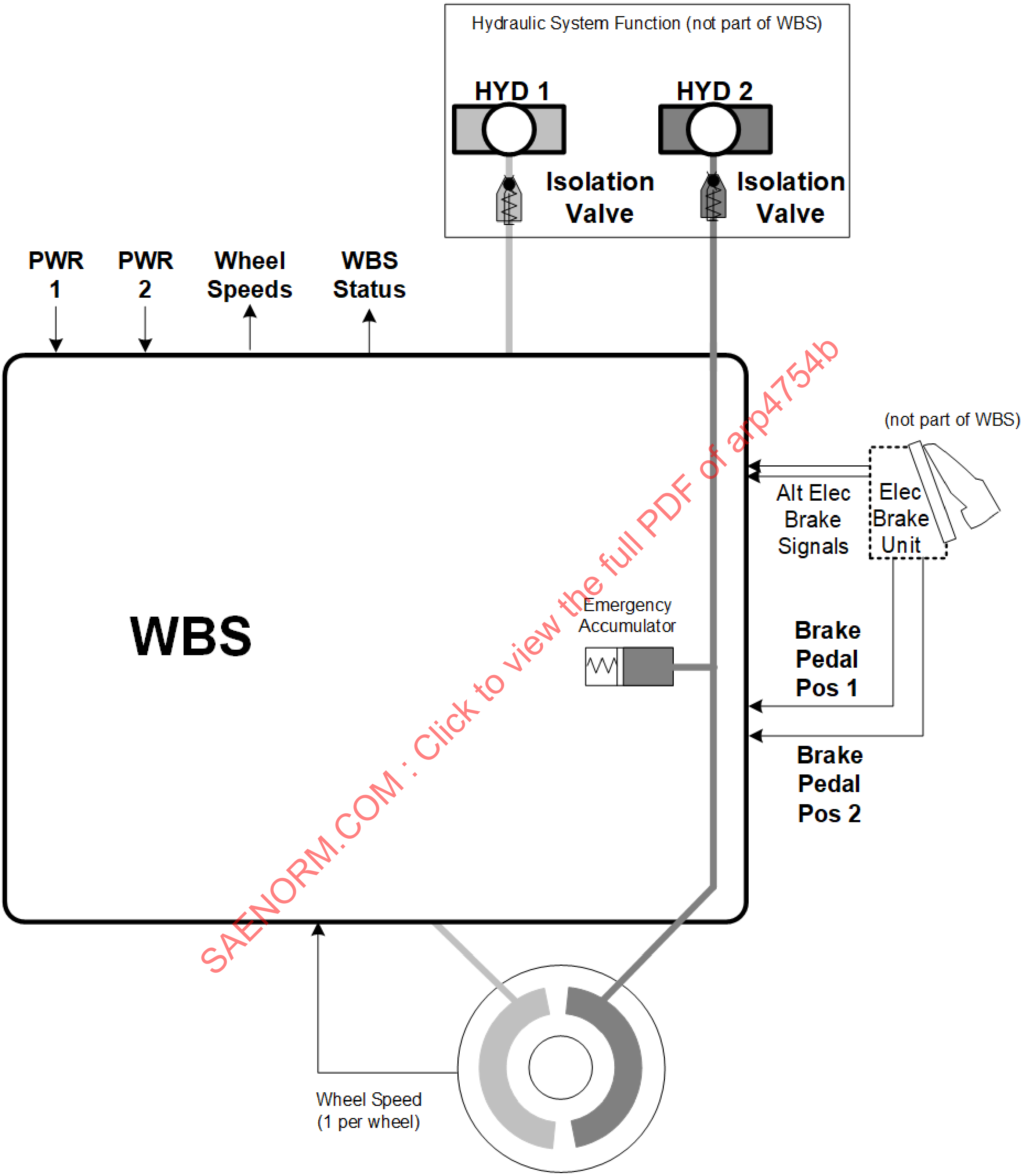


Figure E5 - Airplane-level Wheel Brake System architecture schematic

E.3.12 Airplane Requirements Validation and Assumption Management

The requirements validation and assumption management processes of main body 5.4 were continuous throughout the development life cycle.

E.3.12.1 Airplane Requirements Validation

At the airplane level, the main goal was to ensure that the set of requirements was complete and that each requirement was correct. A critical aspect was to ensure airplane-level requirements were both necessary and sufficient to meet the needs of operators, maintainers, and Certification Authorities, as well as airplane and system developers. A validation matrix, shown in Table E8, was used to illustrate the outcome of the validation process. In this case, the three validation methods determined to be applicable were engineering review, analysis, and traceability. The review included evaluation of questions as described in main body 5.4.

(Editor's Note: For the sake of brevity, only a sample of requirements are shown in the validation matrix, Table E8, and the actual evidence articles; e.g., the simulation methods, results, and the correctness and completeness checklist are not shown. In this example, the FDALs associated with functions/requirements are captured as separate requirements and/or documented as attributes as shown in the associated function column in Table E8.)

Following the guidance of main body 5.4.7.2, Table E8 was created to track the status of validating each requirement and the set of requirements as a whole including additional requirements resulting from architecting decisions and PASA activity. The categorization as a safety requirement resulted from the PASA activity. (See main body 4.1.3, 5.3.1.1, and 5.3.2 for discussion about identifying safety requirements through safety assessments.) The FDALs shown in Table E8 came from the PASA as shown in Table E5.

Table E8 - Airplane Requirements Validation Matrix (sample)

Requirement ID and Requirement	Safety Req	Source of Requirement	Associated Function (if Applicable) and the FDAL		Validation Method	Validation Evidence	Validation Conclusion
S18-ACFT-R-1000 The S18 airplane shall have a means to decelerate on ground.	No	Airplane concept	Decelerate on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1100 The S18 airplane shall have a means to decelerate the wheels on ground.	No	Airplane concept	Decelerate the Wheels on Ground	A	Engineering review Traceability	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1110 The S18 airplane shall have pilot-controlled wheel braking capability.	No	Airplane concept	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1120 The S18 airplane shall have an autobraking capability during landing and RTO.	No	Business case trade study	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1130 The S18 airplane shall have anti-skid braking.	No	Business case trade study	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1140 The S18 airplane shall provide interface for WBS status and annunciations.	No	Business case trade study	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0181 The S18 airplane shall decelerate the wheels on gear retraction.	No	Business case trade study	Decelerate the Wheels on Gear Retraction	A	Engineering review	Correct & Completeness Checklist 1234	Valid

Requirement ID and Requirement	Safety Req	Source of Requirement	Associated Function (if Applicable) and the FDAL		Validation Method	Validation Evidence	Validation Conclusion
S18-ACFT-R-0182 The S18 airplane shall be capable of decelerating the wheels differentially.	No	Business case trade study	Decelerate the Wheels Differentially for Directional Control	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0183 The S18 airplane shall have a parking brake to prevent airplane motion when parked.	No	Airplane concept	Control Airplane Energy	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0184 The S18 airplane shall have hydraulically driven braking.	No	Business case trade study	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0185 The S18 airplane shall have an autobrake override that can be initiated by the flight crew.	No	14 CFR/CS 25.735(c)(2)	Decelerate the Wheels on Ground	A	Engineering review Traceability	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0186 The S18 airplane shall meet safety requirements while operating in an average atmospheric radiation environment per the IEC 62396 standard with an altitude of 40000 feet and a latitude of 45 degrees.	No	S18 airplane internal documentation	Protect against Single Event Effects (SEE)	A	Engineering review	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-0933 The Wheel Brake System decelerate the wheels on the ground function shall be developed as FDAL A.	Yes	PASA-SR-01	Decelerate the Wheels on Ground	A	Analysis	PASA	Valid
S18-ACFT-R-1322 No single failure or event shall result in the complete loss of wheel brake and the loss of one thrust reverser.	Yes	PASA-SR-10	Decelerate on Ground	A	Engineering review Traceability Analysis	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1385 Complete loss of wheel braking shall be less than 1.0E-07 for a landing.	Yes	PASA-SR-05	Decelerate the Wheels on Ground	A	Engineering review Traceability Analysis	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1550 Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.	Yes	PASA-SR-12	Decelerate on Ground	A	Engineering review Traceability Analysis	Validation Checklist 1234	Valid
S18-ACFT-R-1551 Wheel Brake System shall include an emergency accumulator to supply hydraulic power to the wheel brakes.	No	Hydraulic-electric brake study	Decelerate the Wheels on Ground	A	Engineering review	Correct & Completeness Checklist 1234	Valid

Requirement ID and Requirement	Safety Req	Source of Requirement	Associated Function (if Applicable) and the FDAL		Validation Method	Validation Evidence	Validation Conclusion
S18-ACFT-R-1552 The Alternate/Emergency Brake System hydraulic equipment and piping shall be installed aft of the engine 1 UERF trajectory envelope.	Yes	PASA-SR-13	Decelerate on Ground	A	Engineering review Traceability Analysis	Correct & Completeness Checklist 1234	Valid
S18-ACFT-R-1600 Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.	Yes	PASA-SR-14	Decelerate on Ground	A	Engineering review Traceability Analysis	Correct & Completeness Checklist 1234	Valid

(Editor's Note: S18-ACFT-R-0186 is included here to provide visibility of an aircraft-level overarching requirement that is later allocated to aircraft systems and items. This is the introduction of the function "Protect against Single Event Effects (SEE).")

E.3.12.2 Airplane Assumption Management

For confirmation tracking purposes, assumptions have been summarized in Table E9. For tracking purposes, the assumptions received from the AFHA, as shown in Table E2, have had identifier prefix "AFHA" added. PASA and PRA assumptions were identified as received from the PASA and PRA.

Table E9 - Airplane-level safety assumptions

Assumption Identifier	Description	Confirmation
AFHA ASMP 3.2.2-1	Overrunning the runway length above "XYZ" knots is considered a high speed overrun.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-2	The directional aspect of asymmetric failures of deceleration systems are functionally addressed by failure conditions of the "Control direction on ground" airplane function. (See function 2.3 AFHA.)	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-3	The flight crew will divert to a suitable airfield if aware of a condition that renders the airplane incapable of landing at the originally intended destination.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-4	Crew awareness is not a factor for the identified malfunction, as these are immediately evident due to aircraft behavior and do not have their effects intensified or mitigated by crew awareness features.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-5	The flight crew will not initiate an RTO in response to an annunciated failure of deceleration features during takeoff due to alert suppression.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-6	Taxi is performed at groundspeeds below 30 knots.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-7	Landings with failure condition in combination with environmental factors have been assessed.	Coord Memo S18a-CM00Y1
AFHA ASMP 3.2.2-8	Failures of deceleration capability will be detected and annunciated by on-board systems.	Coord Memo S18a-CM00Y1
PASA-ASMP-01	It is assumed that the high speed overrun is above 30 knots and low speed overrun is below (or equal) 30 knots. This assumption has been derived from the AFHA assumption ASMP 3.2.2-1 and ASMP 3.2.2-6 for the establishment of the criteria and terms of "high speed overrun" and "low speed overrun."	Coord Memo S18a-CM00Y2
PASA-ASMP-02	The degraded state of systems considered in the CoFFE analysis has been defined such as half functional capability.	Coord Memo S18a-CM00Y2
PASA-ASMP-03	Wheel Brake System uses ground detection information together with the wheel speed information. These functions are developed independently so that even if Erroneous Ground Detection Information (AGS.MF) is provided on ground, i.e., with false in-flight status, wheel braking function is available if there is correct wheel speed information.	Coord Memo S18a-CM00Y2
PRA-UERF-ASSUMPTION-01	The BSCU is installed in the avionics compartment located in the nose fuselage section of the airplane, forward of the UERF area.	PRA
PRA-UERF-ASSUMPTION-02	The electrical lines transmitting the brake control signals from the Electric Brake Unit to the BSCU are routed "to the shortest" from one end to the other in the nose fuselage section of the airplane, thus are kept forward of the UERF area.	PRA

Assumption Identifier	Description	Confirmation
PRA-UERF-ASSUMPTION-03	The hydraulic reservoirs and the high pressure manifolds of the hydraulic subsystems 1 and 2 are located in the fuselage, aft of the UERF area.	PRA
PRA-UERF-ASSUMPTION-04	The hydraulic power distribution lines from the engine driven pumps to the respective hydraulic reservoirs and high pressure manifolds exit the engine pylons aft of the wing rear spars, then run along, aft of, the wing rear spars to the fuselage, and are kept aft of the UERF area inside the fuselage.	PRA
PRA-UERF-ASSUMPTION-05	The hydraulic distribution lines routed to the forward part of the fuselage to supply hydraulic equipment located forward of the UERF area are fitted with appropriate isolation means located aft of the UERF area.	PRA
PRA-UERF-ASSUMPTION-06	The power supply lines from the electrical power center(s) to the EBU are routed “to the shortest” from one end to the other in the nose fuselage section of the airplane.	PRA
PRA-UERF-ASSUMPTION-07	In case of cabin depressurization the airplane altitude will be limited by procedure to 10000 feet.	PRA

The assumptions as shown in E.3.6.1 were confirmed through the development process and the confirmation was communicated back to the AFHA in Coord Memo S18a-CM00Y1 and to the PASA process in Coord Memo S18a-CM00Y2. The PRA assumptions were reviewed as part of the final design review for confirmation by the PRA.

E.4 WHEEL BRAKE SYSTEM DEVELOPMENT PROCESS

E.4.1 Wheel Brake System Introduction

This section describes, in detail, the system architecture development for the WBS. The WBS is developed to implement the “Decelerate the Wheels on the Ground” sub-function of the “Decelerate on Ground” airplane-level function (see E.3.8).

The purpose of this section is to illustrate that development of a system architecture involves taking system functions, requirements, results of the safety assessment analyses, interfacing systems, and other activities into account.

E.4.2 Wheel Brake System Planning

At the systems level, the WBS Development Assurance Plan was the top-level planning document which is similar to the airplane Development Assurance Plan (see E.3.2).

E.4.3 Wheel Brake System Description

The S18 WBS is comprised of the brake pedal control system, brake hydraulic system, anti-skid and autobrake systems, brakes/wheels/tires, brake temperature monitor system, brake cooling fans, tire pressure indication system, and tire and brake monitoring system.

(Editor’s Note: For brevity, the example will only show certain aspects of the systems architecture in detail.)

The airplane has two main landing gear attached to the wings and a nose gear. The WBS is installed on the two main landing gear. The nose gear wheels are unbraked. The eight main gear wheels have multi-disc carbon brakes.

Brakes on the main gear wheels are used to provide safe retardation of the airplane during taxiing and landing phases and in the event of a Rejected Takeoff (RTO). The wheel brakes also prevent unintended airplane motion when parked, and may be used to provide differential braking for airplane directional control. A secondary function of the WBS is to stop main gear wheel rotation upon gear retraction.

Braking on ground is commanded manually via brake pedals, or automatically (autobrake) without the need for pedal application. The autobrake functionality allows the pilot to pre-arm the decelerate function prior to takeoff or landing and is only available in the NORMAL Mode.

Brake application is controlled by left and right meter valves located in the wheel wells. The meter valves are operated via electrical signals, through the EBU, from toe pedals integral to the rudder pedal assembly. Differential control of the left and right brakes is available to both the captain and first officer. The parking brake handle is used to set the parking brake. To set the parking brake, the brake pedals are fully depressed. The parking brake handle can be pulled up and will latch when the pedals are released. The WBS maintains brake clamping force without further flight crew action once the parking brake has been set. The brake pedals are depressed to unlatch the parking brake handle.

The brake pedal position is also electrically fed to a brake computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical airplane and system states, to provide correct brake functions and improve system fault tolerance, and generate warnings, indications, and maintenance information to other systems. This computer is accordingly named the Brake System Control Unit (BSCU).

The WBS includes a Normal Brake System and Alternate/Emergency Brake System which operate in NORMAL, ALTERNATE, or EMERGENCY Modes.

a. NORMAL Mode is operated with BSCU and HYD 1 hydraulic system. NORMAL Mode includes either autobrake or manual braking. Autobrake is only available in the NORMAL Mode.

b. ALTERNATE Mode is on standby and is selected automatically when the Normal Brake System fails. It is operated with HYD 2 hydraulic system.

c. EMERGENCY Mode is selected when the Normal Brake System has failed and HYD 2 hydraulic system is lost. It is operated with an emergency hydraulic accumulator.

Switch-over of the mode can be automatic under defined failure conditions or manually selected. Mode transitions are depicted in Figure E6.

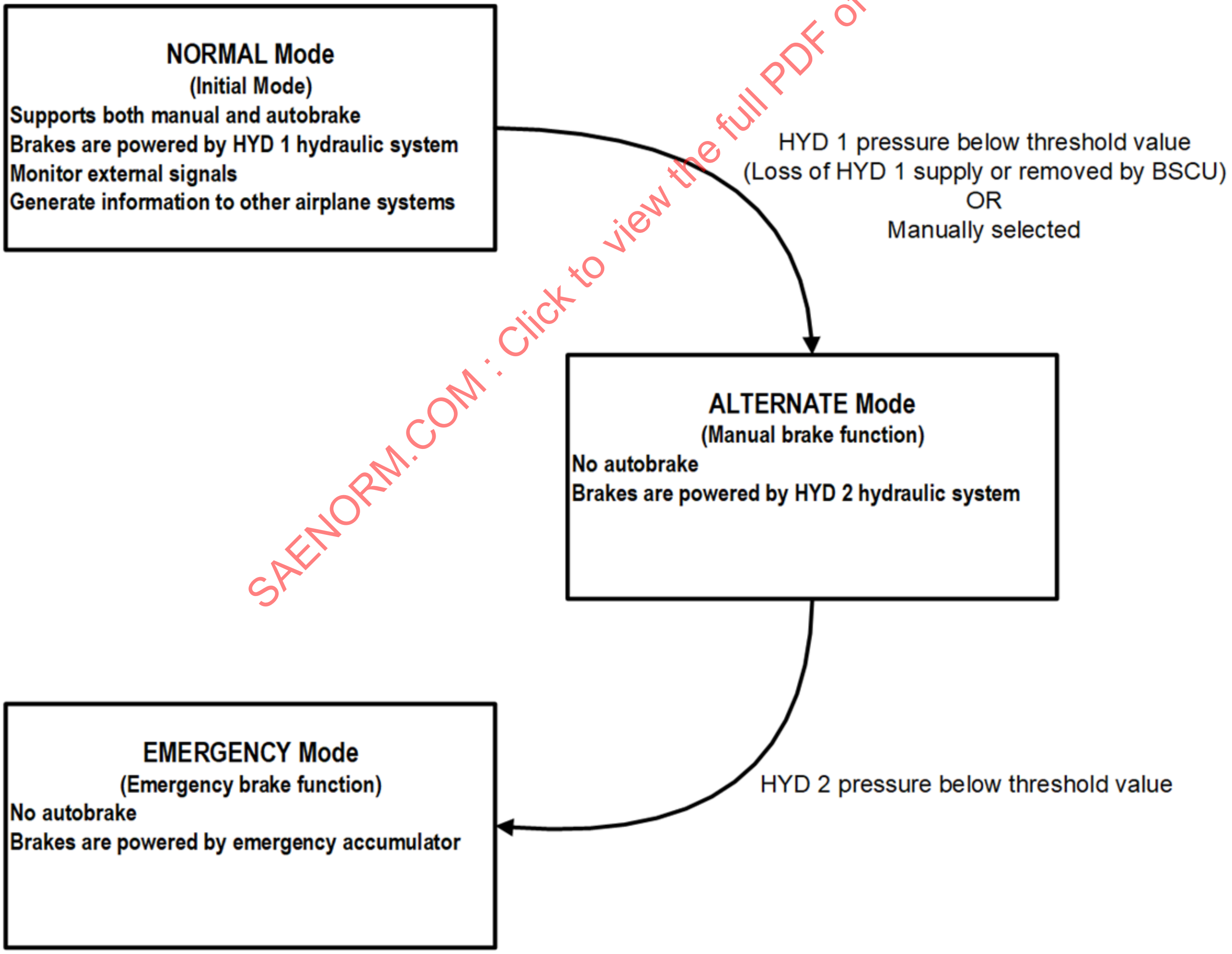

NORMAL Mode
(Initial Mode)
Supports both manual and autobrake
Brakes are powered by HYD 1 hydraulic system
Monitor external signals
Generate information to other airplane systems
HYD 1 pressure below threshold value
(Loss of HYD 1 supply or removed by BSCU)
OR
Manually selected
ALTERNATE Mode
(Manual brake function)
No autobrake
Brakes are powered by HYD 2 hydraulic system
HYD 2 pressure below threshold value
EMERGENCY Mode
(Emergency brake function)
No autobrake
Brakes are powered by emergency accumulator

Figure E6 - WBS mode transitions

E.4.4 Wheel Brake System Functions

The WBS is assigned to perform the following functions:

a. Decelerate the wheels on the ground.

    1. Decelerate the wheels on command (manual or automatic).

    2. Automatically command wheel deceleration on landing and Rejected Takeoff (RTO).

    3. Prevent tire skidding during wheel deceleration.

    4. Provide WBS annunciation.

b. Decelerate the wheels on gear retraction.

c. Decelerate the wheels differentially for directional control.

d. Prevent airplane motion when parked.

e. Provide wheel speed data to the airplane.

The wheel brake function is also supported by and/or provides support to a number of functions from different airplane systems. The interfacing functions associated with the WBS identified for this example are:

a. Provide electrical power.

b. Provide hydraulic power.

c. Display system annunciation.

Figure E7 depicts how the airplane-level interfacing functions, “Provide Electrical Power” and “Provide Hydraulic Power,” support the WBS functions. Likewise, the WBS function “provide WBS annunciation” supports the interfacing function “Display System Annunciation” which provides crew operational awareness to the WBS status.

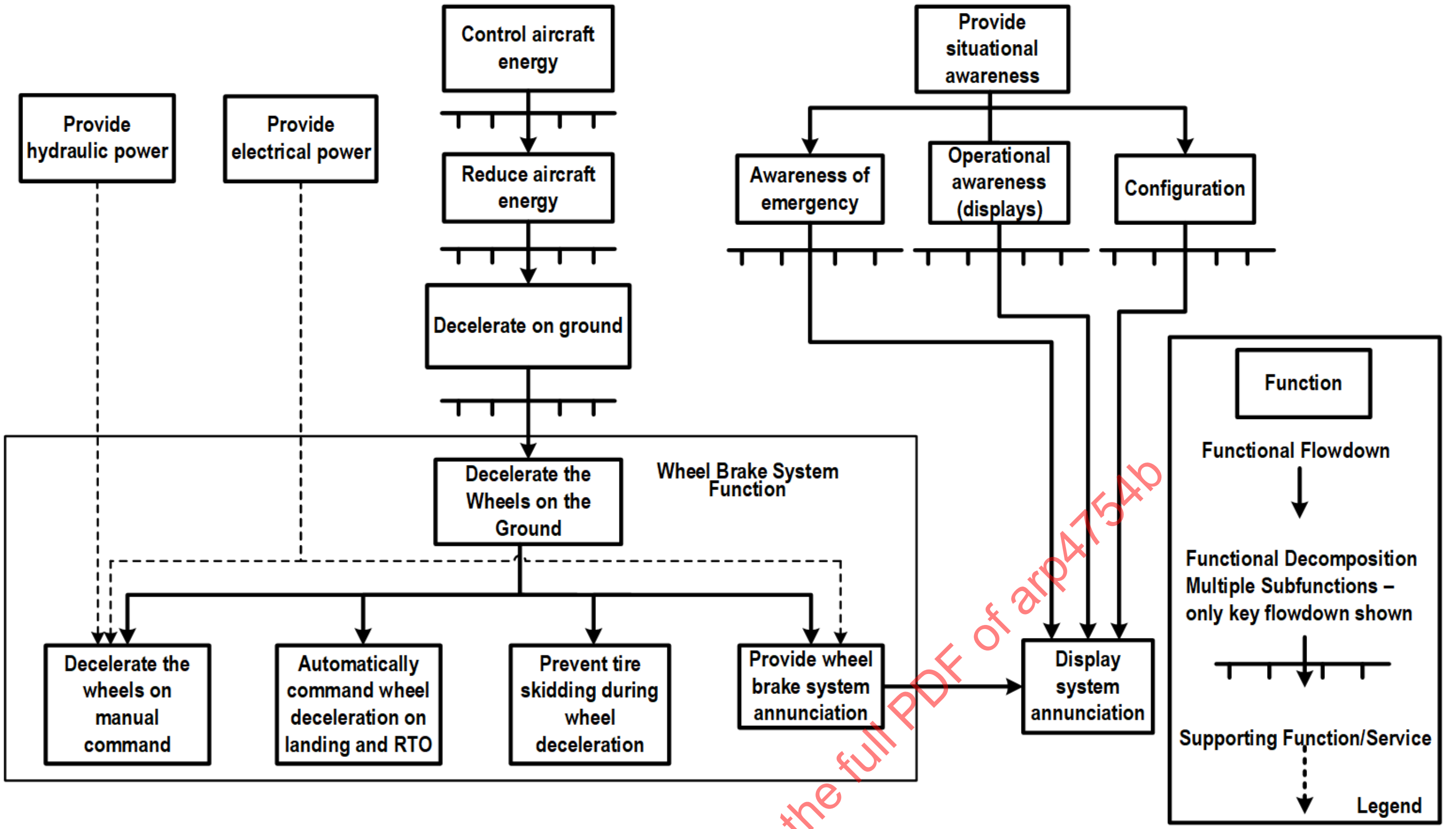

Control aircraft energy
Provide situational awareness
Provide hydraulic power
Provide electrical power
Reduce aircraft energy
Awareness of emergency
Operational awareness (displays)
Configuration
Decelerate on ground
Function
Functional Flowdown
Decelerate the Wheels on the Ground
Wheel Brake System Function
Functional Decomposition Multiple Subfunctions – only key flowdown shown
Decelerate the wheels on manual command
Automatically command wheel deceleration on landing and RTO
Prevent tire skidding during wheel deceleration
Provide wheel brake system annunciation
Display system annunciation
Supporting Function/Service
Legend

Figure E7 - Decomposition of Wheel Brake System functions

E.4.5 System Functional Hazard Assessment

The SFHA was prepared through the safety assessment process. Using the WBS description from E.4.3 and functional failures for each of the WBS functions in E.4.4, the SFHA determined failure conditions.

The SFHA provided failure conditions associated with the function “Decelerate the Wheels on the Ground.” The severity classifications assigned in the SFHA (e.g., Catastrophic, Hazardous, Major), along with conditions assigned that further defined the failure condition (e.g., loss of less than 50% wheel deceleration) were a factor in determining the WBS architecture required for the “Decelerate the Wheels on the Ground” function and other associated functions.

The SFHA failure conditions for the “Decelerate the Wheels on the Ground” function are found in ARP4761A/ED-135 Appendix Q.

E.4.5.1 SFHA Assumptions

Assumptions made while accomplishing the effect evaluation of each failure condition have been captured and numerically identified for reference. Table E10 presents the assumptions analysis made during the development of this functional hazard assessment. These assumptions were confirmed through the development process and the confirmation communicated back to the SFHA process.

Table E10 - SFHA assumptions

Assumption Identifier	Description
SASP 1.1-1	Loss of 80% or more of deceleration capability is considered a total loss of the deceleration means.
SASP 1.1-2	Failure Conditions are assessed on wet runway conditions.
SASP 1.1-3	RTO is considered an operational condition caused either by an external event or by a system failure (annunciated or perceived by the flight crew) during takeoff run.
SASP 1.1-4	The flight crew will not initiate an RTO due to an annunciated failure of the deceleration function after V1.
SASP 1.1-5	Taxi is performed at groundspeeds below 30 knots.
SASP 1.1-6	Overrunning the runway length at or above “XYZ” knots is considered a high speed overrun.
SASP 1.1-7	Overrunning the runway length below “XYZ” knots is considered a low speed overrun.
SASP 1.1-8	Failures of deceleration capability will be detected and annunciated by on-board systems.

E.4.6 Wheel Brake System Requirements

Initial WBS requirements were captured by the allocation of the WBS-related airplane functional requirements, the derived requirements associated with these functions, and the associated functional interfaces to the WBS. The certification requirements were assigned to the WBS either by decomposing airplane-level certification requirements or directly from the regulations.

Table E11 illustrates the functional and certification requirements allocated to WBS in order to define initial system architecture for use in the safety analysis defined in ARP4761A/ED-135 Appendix Q. The table also contains design decisions from past experience and additional functions derived from the certification requirements in order to set an initial WBS architecture. The source column provides additional context for the traced from content. The validation for these requirements is described in E.4.7.

At this stage of requirements development, not all certification requirements were agreed upon with the Certification Authority. The certification requirements were finalized after the WBS architecture was agreed to by the OEM and applicable subcontractor.

The WBS requirement set was provided at this point in sufficient detail so that the SFHA process could commence. The requirements allocation and derivation process continued parallel to the safety analysis.

Table E11 - Initial Wheel Brake System requirements WBS-0001-103 - Version 1.0 (excerpt)

Requirement Number	Requirement	Associated Function (if Applicable) and the FDAL		Traced From	Source
S18-WBS-R-0020	The Wheel Brake System shall have a means to decelerate the wheels on the ground.	Decelerate the wheels on ground	A	S18-ACFT-R-1100	S18 Airplane Requirements Specification
S18-WBS-R-0021	The Wheel Brake System shall be capable of decelerating the S18 airplane to a complete stop/to taxi speed in 2000 feet when wheel brakes, high lift speed brakes and reverse thrust are available, including when at maximum landing weight.	Decelerate the wheels on ground	A	Derived	S18 airplane trade study
S18-WBS-R-0041	The Wheel Brake System shall provide directional control on ground by a differential braking function.	Decelerate the wheels differentially for directional control	A	S18-ACFT-R-0182	S18 Airplane Requirements Specification
S18-WBS-R-0042	The Wheel Brake System shall provide a parking brake to prevent airplane motion on the ground.	Prevent airplane motion when parked	A	S18-ACFT-R-0183	S18 Airplane Requirements Specification
S18-WBS-R-0043	The Wheel Brake System shall provide autobraking capability during landing and RTO.	Decelerate the wheels on ground	A	S18-ACFT-R-1120	S18 Airplane Requirements Specification
S18-WBS-R-0044	The Wheel Brake System shall provide anti-skid braking.	Decelerate the wheels on ground	A	S18-ACFT-R-1130	S18 Airplane Requirements Specification
S18-WBS-R-0045	The Wheel Brake System shall provide hydraulic brake control.	Decelerate the wheels on ground	A	S18-ACFT-R-0184	S18 Airplane Requirements Specification

Requirement Number	Requirement	Associated Function (if Applicable) and the FDAL		Traced From	Source
S18-WBS-R-0046	The Wheel Brake System shall override the autobrake when commanded by the flight crew.	Decelerate the wheels on ground	A	S18-ACFT-R-0185	S18 Airplane Requirements Specification
S18-WBS-R-0047	The Wheel Brake System shall meet safety requirements while operating in an average atmospheric radiation environment per the IEC 62396 standard with an altitude of 40000 feet and a latitude of 45 degrees.	Protect against Single Event Effects (SEE)	A	S18-ACFT-R-0186	S18 Airplane Requirements Specification
S18-WBS-R-0049	Wheel Brake System shall be controlled and monitored by a computer system called the Brake System Control Unit.	Decelerate the wheels on ground	A	Derived	Design decision made to decrease the pilot workload and fulfill the brake functions like autobrake, annunciation, anti-skid
S18-WBS-R-0050	Each wheel shall have its own hydraulic circuit.	Decelerate the wheels on ground	A	Derived	Design architecture decision
S18-WBS-R-0052	Each hydraulic Wheel Brake System circuit shall have meter valves, anti-skid valves and hydraulic fuses.	Decelerate the wheels on ground	A	Derived	Design architecture decision
S18-WBS-R-0055	Anti-skid system shall be capable to prevent skidding of the tires by reducing the pressure applied to the brakes.	Decelerate the wheels on ground	A	Derived	Design architecture decision
S18-WBS-R-0062	Wheel Brake System shall include an emergency accumulator to supply hydraulic power to the wheel brakes.	Decelerate the wheels on ground	A	S18-ACFT-R-1551	S18 Airplane Requirements Specification
S18-WBS-R-0065	The emergency accumulator shall be capable of providing 2000 psi.	Decelerate the wheels on ground	A	Derived	Design architecture decision
S18-WBS-R-0066	The Alternate/Emergency Brake System hydraulic equipment and piping shall be installed aft of the engine 1 UERF trajectory envelope.	Decelerate the wheels on ground	A	S18-ACFT-R-1552	S18 Airplane Requirements Specification
S18-WBS-R-0120	No single failure or event shall cause the complete loss of hydraulic power for both the WBS Normal and Alternate/Emergency Brake Systems.	Decelerate the wheels on ground	A	S18-ACFT-R-1550	S18 Airplane Requirements Specification
S18-WBS-R-0100	The Wheel Brake System decelerate the wheels on the ground function shall be developed as FDAL A.	Decelerate the wheels on ground	A	S18-ACFT-R-0933	S18 Airplane Requirements Specification
S18-WBS-R-0150	Complete loss of decelerate the wheels on the ground function shall be less probable than 1.0E-07 for a landing.	Decelerate the wheels on ground	A	S18-ACFT-R-1385	S18 Airplane Requirements Specification
S18-WBS-R-0200	Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.	Decelerate on ground	A	S18-ACFT-R-1600	S18 Airplane Requirements Specification

(Editor's Note: Due to the complexity of the requirement capturing process, not all requirements are shown here but some requirements related to the "Decelerate the wheels on the ground" function are shown to explain the process.)

(Editor's Note: The generic wording of requirement S18-WBS-R-0047 does not imply nor assume that the WBS is commanding braking during flight at high altitude. The expressed need is that the WBS should withstand the specified environment without impacting compliance to its safety requirements, considering that atmospheric radiation encountered during flight may affect WBS equipment with lasting effects on braking functions up to and including the ground phase.)

With the initial requirements set, the architecture studies and the safety assessment process (commencing with the SFHA) began. The requirements development process was a coupled process where the system designers deriving the requirements worked closely with the safety engineer. The results of the requirements development and safety assessment processes were uploaded to the requirement database. Through the architecture development and the SFHA studies the interface requirements were clarified between the WBS and other airplane supporting functions. Section E.4.6.6 describes how these interface requirements were derived from these studies.

E.4.6.1 Initial Wheel Brake System Architecture Concept

(Editor's Note: Normally an architecture or design document includes the description of the system and its interfacing systems. While there is no recommended method to capture and document the system architectures, for the purposes of this example, the output of this process consists of architecture diagrams.)

The system functional requirements as shown in Table E11 were used in conjunction with the high-level interface logic diagram, Figure E8, to help the team develop the initial architecture concept.

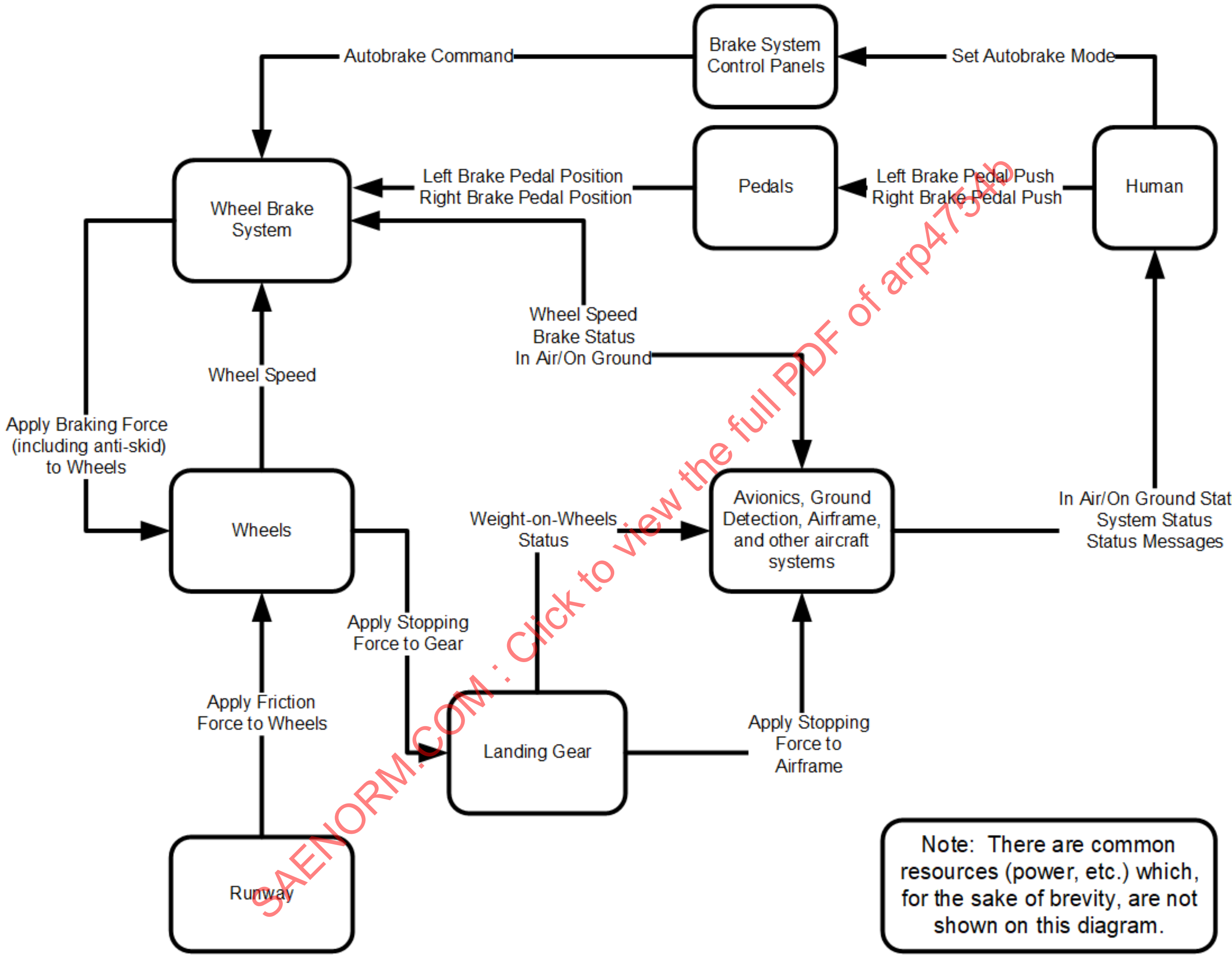

Brake System Control Panels
Autobrake Command
Set Autobrake Mode
Wheel Brake System
Left Brake Pedal Position
Right Brake Pedal Position
Pedals
Left Brake Pedal Push
Right Brake Pedal Push
Human
Wheel Speed
Brake Status
In Air/On Ground
Wheel Speed
Apply Braking Force (including anti-skid) to Wheels
Wheels
Weight-on-Wheels Status
Avionics, Ground Detection, Airframe, and other aircraft systems
In Air/On Ground Status
System Status
Status Messages
Apply Stopping Force to Gear
Apply Friction Force to Wheels
Landing Gear
Apply Stopping Force to Airframe
Runway
Note: There are common resources (power, etc.) which, for the sake of brevity, are not shown on this diagram.

Figure E8 - High-level interface diagram

As part of a design decision made to decrease the pilot workload and fulfill the brake functions like autobrake, annunciation, and anti-skid, the following new requirement was introduced as S18-WBS-R-0049 in Table E11:

The WBS shall be controlled and monitored by a computer system called the Brake System Control Unit (BSCU).

In addition to a BSCU, the WBS consists of:

a. Shutoff Valve: The Shutoff Valve (SOV) responds to commands from the BSCU to apply hydraulic pressure to the brake discs. The SOV is used to switch from the Normal Brake System to the Alternate/Emergency Brake System, when the BSCU becomes unable to control the Normal Brake System via the Normal Meter Valve (NMV).

b. Selector Valve: The Selector Valve connects the HYD 2 supply to the Alternate/Emergency Brake System and removes the HYD 1 supply to the Normal Brake System when the HYD 1 pressure falls below a threshold value, either from loss of HYD 1 supply itself or from its removal by the BSCU due to the presence of faults.

c. Normal Meter Valves: The function of the NMVs is to control pressure in the Normal Brake System to the demanded level and to provide regulation for the anti-skid function while the WBS is in the NORMAL Mode. The NMVs are controlled by the BSCU, which receives electrical brake pedal position inputs from the EBU.

d. Emergency Accumulator: The Emergency Accumulator provides an emergency reserve of hydraulic pressure for the Alternate/Emergency Brake System. A fully charged emergency accumulator provides enough pressure to apply pressure for the required number of presses of the brake pedals while the WBS is in the EMERGENCY Mode. The emergency accumulator also supplies hydraulic pressure for the parking brake function.

e. Alternate/Emergency Meter Valves: The function of the Alternate/Emergency Meter Valve is to control pressure in the Alternate/Emergency Brake System to the level demanded by the brake pedals while the WBS is in the ALTERNATE or EMERGENCY Modes. The Alternate/Emergency Meter Valves receive alternate electrical brake signals from the EBU and have no interface with the BSCU.

f. Shutoff/Anti-Skid Valves: The Shutoff/Anti-Skid Valves (S/ASVs) follow BSCU commands to control hydraulic pressure to the brake pads in the Alternate/Emergency Brake System. These valves perform two functions: (1) they are the shutoff valves for Alternate/Emergency Brake System when the WBS is in the NORMAL Mode, and (2) they are used to restrict the hydraulic line pressure to the brakes in order to prevent locking of the wheels when the WBS is in the ALTERNATE or EMERGENCY Modes.

Other components associated with wheel braking are:

a. Electric Brake Unit: The EBU provides the mechanical interface to the flight crew and electrical interface to the WBS. The EBU provides brake pedal positions to the BSCU. The BSCU uses these inputs to calculate commands to the SOV and NMVs in the NORMAL Mode, and the Shutoff/Anti-Skid Valves in the ALTERNATE and EMERGENCY Modes. The EBU also provides dual-redundant alternate electrical brake signals to control the Alternate/Emergency Meter Valves in the ALTERNATE and EMERGENCY Modes.

b. Wheel Brakes: The wheel brakes will provide friction force to the wheel. The brakes will also house temperature sensors which will provide brake temperature to the BSCU.

c. Parking Brake: The parking brake handle is used to set the parking brake system. The parking brake has been intentionally not detailed in Figure E9 to simplify the schematic.

d. Wheel Speed Sensor: A wheel speed sensor is used to sense wheel speed on each wheel.

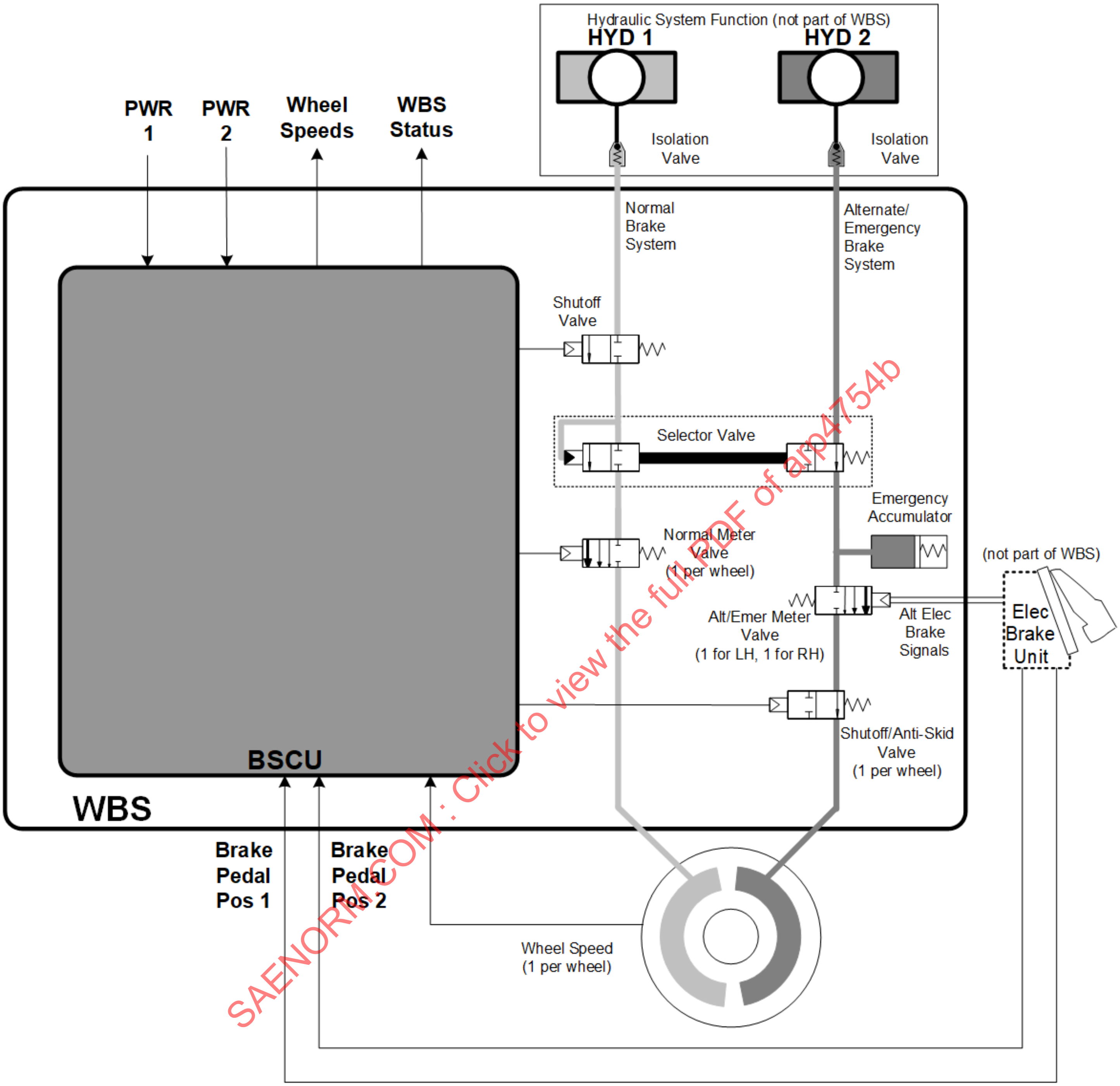


Figure E9 - High-level Wheel Brake System architecture

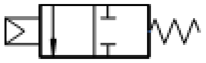
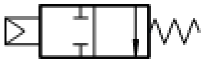
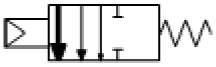
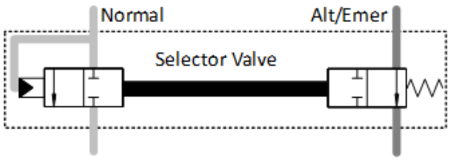
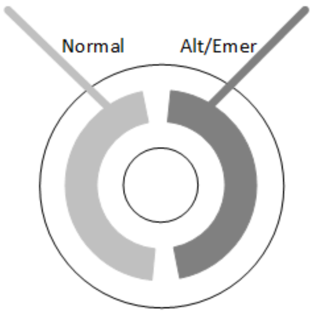
Legend	
Electro-Hydraulic Component	**Description**
	Normally closed valve; open when signal drives input.
	Normally open valve; closed when signal drives input.
	Normally closed valve; open when signal drives input. Opens with increasing flow rate with increasing signal.
	Selector Valve normally closed for Normal, open for Alt/Emer; opens for Normal, closes for Alt/Emer when pressure is applied from Normal. In the example, the spring-loaded Selector Valve automatically opens Alt/Emer if normal pressure falls below a threshold or is shut off via the Shutoff Valve.
	Wheel brakes, either input (Normal or Alt/Emer) provides hydraulic pressure to apply 100% of braking.

Figure E9 - High-level Wheel Brake System architecture (continued)

Since the proposed high-level architecture has been established, it was re-evaluated against the system-level functional, operational, and other classes of requirements that have been identified thus far. This architecture was passed to the system safety team to initiate the PSSA process for initial evaluation from a safety perspective.

E.4.6.1.1 Wheel Brake System Architectural Decisions Based on Safety Requirements

The WBS safety assessment process began as soon as the systems design team had an initial architecture concept (WBS ARCH 1). The team analyzed the initial architecture concept against the requirements input from the airplane level and the safety objectives from the AFHA.

The proposed safety requirement from PASA "[FF1.1] Complete loss of wheel brake shall be less than 1.0E-07 for a landing" was based on PASA results that the loss of brake commands needs to have a probability lower than 1.0E-07. Safety analysis of the initial architecture relative to this safety requirement identified a need for architectural mitigation. The system design was modified to include two redundant BSCU commands in order to meet the loss of function requirement.

As a result of the analysis, the following requirement was added to the requirements database along with justification information: "S18-WBS-R-0509: The WBS shall have dual BSCU command functions."

E.4.6.1.2 Modified Wheel Brake System Description

Braking on ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The autobrake functionality allows the pilot to pre-arm the deceleration rate prior to takeoff or landing. Autobrake is only available in NORMAL Mode.

Based on the requirement (S18-ACFT-R-1385) that loss of all wheel braking was less probable than 1.0E-07 for a landing, a design decision was made that each wheel has a brake assembly operated by two independent sets of hydraulic pistons. One set is operated from the HYD 1 hydraulic supply and is used in the NORMAL Mode. The Alternate/Emergency Brake System is on standby and is selected automatically when the Normal Brake System fails. It is operated independently using the HYD 2 hydraulic power supply and is backed by an emergency accumulator which is also used to drive the parking brake. The emergency accumulator supplies the Alternate/Emergency Brake System in the EMERGENCY Mode, when the HYD 2 supply is lost and the NORMAL Mode is not available. Switch-over is automatic under various failure conditions, or can be manually selected. Reduction of HYD 1 pressure below a threshold value, either from loss of HYD 1 supply itself or from its removal by the BSCU due to the presence of faults, causes an automatic selector valve to connect the HYD 2 supply to the Alternate/Emergency Brake System. An anti-skid function is available in both the normal and alternate/emergency brake systems, and operates at all speeds greater than 2 m/s.

In the Normal Brake System, all eight wheels are individually braked from their own servo valves, which are also used to apply anti-skid. In the Alternate/Emergency Brake System, a dual meter valve provides a low pressure hydraulic braking input via four servo valves which provide the anti-skid function to four pairs of wheels. Operation of the Alternate/Emergency Brake System is precluded when the Normal Brake System is in use to maintain independence between the two systems.

In the NORMAL Mode, the brake pedal position is electrically fed to the BSCU. This in turn produces corresponding control signals to the brakes. In addition, the BSCU monitors various signals which denote certain critical airplane and system states, to provide proper brake system functionality and improve fault tolerance, and generates warnings, indications and maintenance information to other systems.

E.4.6.2 Wheel Brake System Architecture Trade Studies

(Editor's Note: The main body does not include guidelines to perform trade studies during the development of an airplane. However, since trade studies can often help to find and optimize solutions to design problems, the S18 WBS team has decided to perform one to help refine the system architecture. There are many methods and procedures for performing trade studies and the main body does not prescribe or recommend any particular method or procedure. Therefore, this example does not show the details of the trade study. Instead this example shows only the results and how the results were utilized to finalize the architecture with which the development will continue. It should be noted that the parameters in the trade study results are examples of possible parameters. The inputs to and the outputs of a real trade study depend upon the system at hand, environment in which the development is taking place, the business, and numerous other factors.)

A trade study ensued to evaluate options for achieving dual BSCU command functions. Considerations for the trade study included:

a. Where to install two Line Replaceable Units (LRUs)

b. Cost of two LRUs versus cost of one LRU with two systems

c. Potential common causes of two LRUs versus one with two systems

d. How will the two systems coordinate with each other

The safety and development teams examined architecture options in a trade study, summarized in Figure E10, that helped determine the optimized architecture. Once the architecture was selected, system development continued the requirements development process, allocating system-level requirements to system components. This architecture continued to be analyzed and had the potential to change until the requirements were validated. To ensure a successful development life cycle, it was important that architecture at this point was firm enough to ensure that future changes have little or preferably no impact on other systems. Therefore the validation of interface requirements was thorough and completed fairly early in the requirements validation process.

After two candidate architectures (WBS ARCH 2 and WBS ARCH 3) that met safety objectives were downselected, the third WBS architecture (WBS ARCH 3) from the trade study was selected and specified to the BSCU supplier. The associated BSCU architecture, referenced as "iteration 1" in Figure E11, was carried forward in this example. This BSCU architecture consists of one BSCU, which houses two independent command channels.

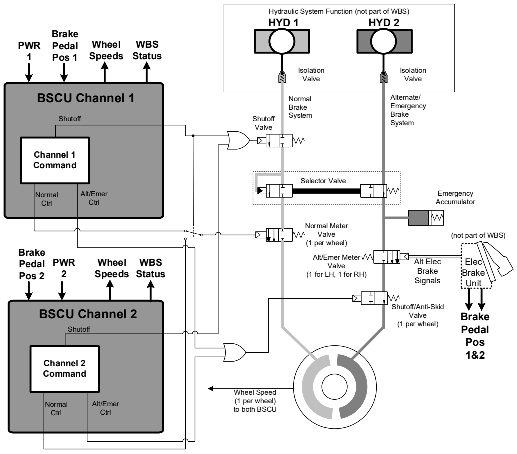
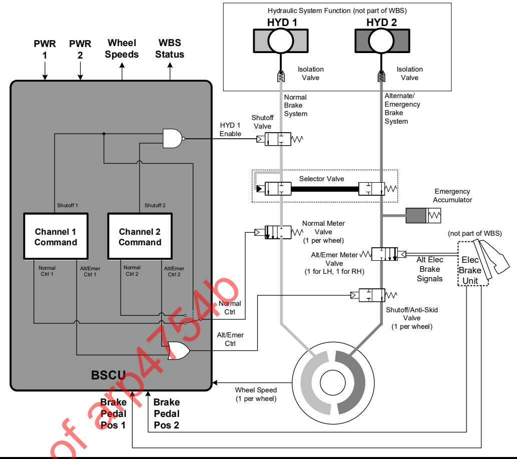
System Architecture	**WBS ARCH2 (2 BSCU)**	**WBS ARCH3 (1 Dual BSCU)**
Uses the following facts: 1) All costs are based on system supplier rates 2) Arch 2 is based on reuse of previous S-18 wheel braking system design	 Hydraulic System Function (not part of WBS) HYD 1 HYD 2 PWR 1 Brake Pedal Pos 1 Wheel Speeds WBS Status Isolation Valve Isolation Valve BSCU Channel 1 Shutoff Channel 1 Command Normal Ctrl Alt/Emer Ctrl Normal Brake System Alternate/ Emergency Brake System Shutoff Valve Selector Valve Emergency Accumulator Normal Meter Valve (1 per wheel) (not part of WBS) Alt/Emer Meter Valve (1 for LH, 1 for RH) Alt Elec Brake Signals Elec Brake Unit Brake Pedal Pos 2 PWR 2 Wheel Speeds WBS Status BSCU Channel 2 Shutoff Channel 2 Command Normal Ctrl Alt/Emer Ctrl Shutoff/Anti-Skid Valve (1 per wheel) Brake Pedal Pos 1&2 Wheel Speed (1 per wheel) to both BSCU	 Hydraulic System Function (not part of WBS) HYD 1 HYD 2 PWR 1 PWR 2 Wheel Speeds WBS Status Isolation Valve Isolation Valve Normal Brake System Alternate/ Emergency Brake System HYD 1 Enable Shutoff Valve Selector Valve Emergency Accumulator Shutoff 1 Shutoff 2 Channel 1 Command Channel 2 Command Normal Ctrl 1 Alt/Emer Ctrl 1 Normal Ctrl 2 Alt/Emer Ctrl 2 Normal Meter Valve (1 per wheel) (not part of WBS) Alt/Emer Meter Valve (1 for LH, 1 for RH) Alt Elec Brake Signals Elec Brake Unit Normal Ctrl Alt/Emer Ctrl Shutoff/Anti-Skid Valve (1 per wheel) BSCU Wheel Speed (1 per wheel) Brake Pedal Pos 1 Brake Pedal Pos 2
Cost	**WBS ARCH2 (2 BSCU)**	**WBS ARCH3 (1 Dual BSCU)**
OEM Cost		
Non-Recurring Cost	$X	$Y
Recurring Cost		
Price per Aircraft	$X1	$Y1
Manufaturing per Aircraft (ROM)	$X2	$Y2
Total Recurring	$X3	$Y3
System Characteristics	**WBS ARCH2 (2 BSCU)**	**WBS ARCH3 (1 Dual BSCU)**
Number of Line Replaceable Units	X	Y
System Weight in kg	X	Y
in lbs	X	Y
Power Consumption in W		
Installation Hours (Hrs)	X	Y
Difficulty of installation	X	Y
(1 Difficult - 10 Easy)	3 - Note due to location of second BSCU and interconnect switches	6
Technical		
FAR 25.735 Compliant	Yes	Yes
Meets Safety Objectives	Yes	Yes
Certification Risk	Low	Low
Reliability / Maintainability	**WBS ARCH2 (2 BSCU)**	**WBS ARCH3 (1 Dual BSCU)**
MTBF		
System in flight hours	X	Y

Figure E10 - Wheel Brake System architecture trade study summary

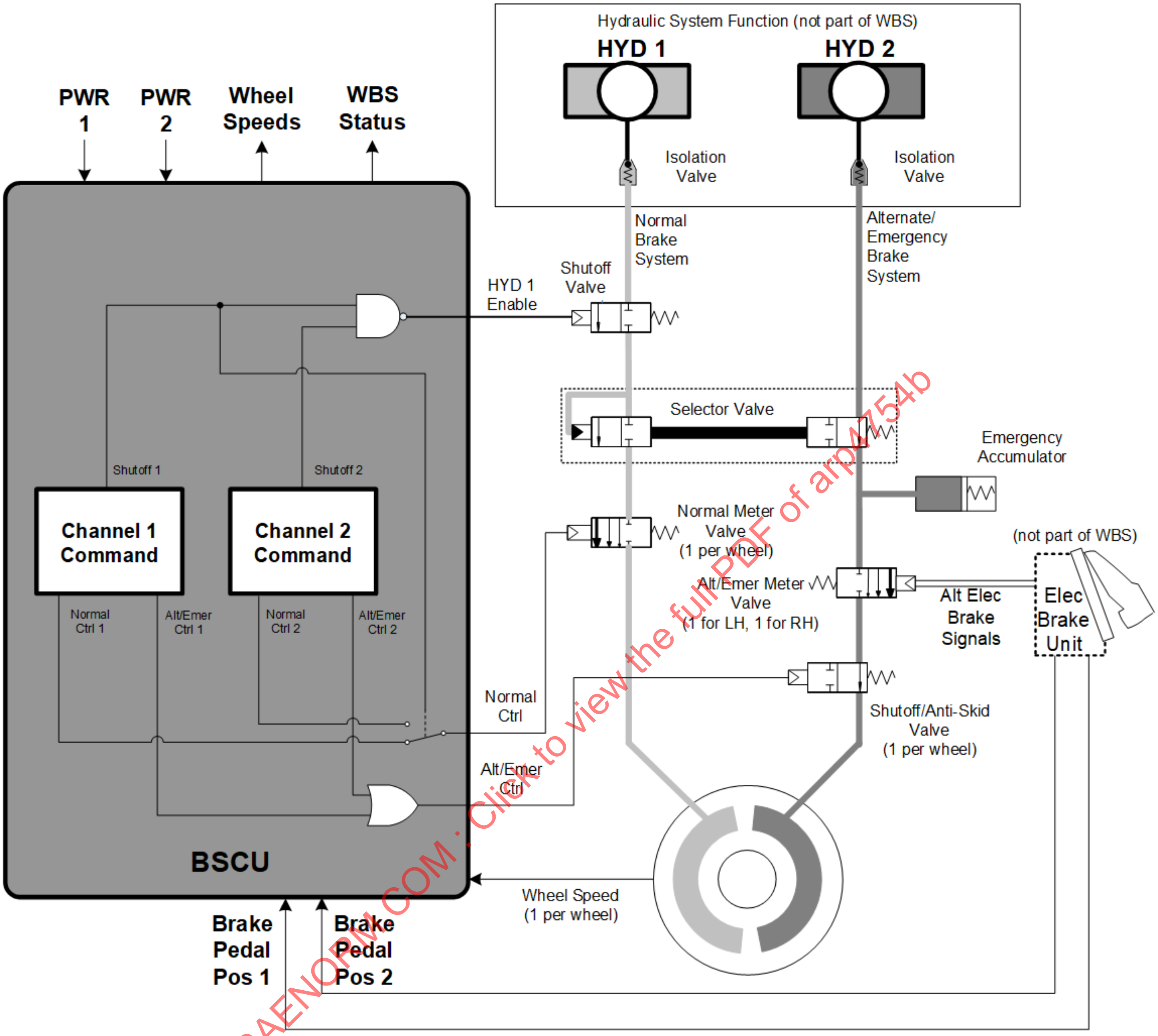


Figure E11 - WBS architecture 3 with BSCU architecture iteration 1

E.4.6.3 Provide Outputs to Wheel Brake System PSSA Process

The development process provided WBS functions, WBS requirements, WBS architecture, and WBS function allocation to the WBS PSSA process. The WBS functions, requirements, architecture, and function allocation are shown in E.4.4, E.4.6, E.4.6.2, and E.4.4, respectively.

E.4.6.4 Wheel Brake System PSSA Assumptions and Proposed Safety Requirements

As described in main body 5.2, the WBS functions were assigned FDALs applied to the various development processes associated with each function. The required FDALs for the WBS functions were derived from failure conditions and classifications provided by the WBS SFHA. Assignment of FDAL to functions within the WBS was done as part of the ARP4761A/ED-135 PSSA process.

The WBS PSSA process determined that the WBS functions responsible for “Decelerate the Wheels on the Ground” required FDAL A.

Lower-level proposed safety requirements were identified through the analyses carried out during the WBS PSSA process. The requirements, shown in Tables E12 and E13, were identified and passed down for assessment at the BSCU level. The reassessment at the BSCU level confirmed the proposed design satisfied the lower-level safety requirements identified.

Table E12 - Proposed independence requirements (WBS PSSA outputs)

Ref No.	Proposed Independence Requirement
1	Airplane electrical power 1 independent from airplane electrical power 2
2	NORMAL Mode braking function independent from ALTERNATE Mode braking function, for total loss failure condition.
3	The NMVs and their control are independent from the SOV and its control such that no single failure results in uncommanded braking.

Proposed independence requirements 2 and 3 were applicable to the WBS. Therefore, safety requirements S18-WBS-R-0120 and S18-WBS-R-0326 were created in coordination with the safety team (see Table E19). Proposed independence requirement 1 was outside the scope of the WBS and airplane requirements flowdown was not traceable to this proposed requirement. This was an assumption communicated to the airplane development process. In addition, this independence requirement was decomposed into WBS requirement S18-WBS-R-0130 to maintain independence with respect to electrical power.

Table E13 - Proposed safety requirements (WBS PSSA outputs)

Ref No.	Proposed Safety Requirement
1	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.
2	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.
3	The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight.
4	The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight.
5	The SOV and NMV commands shall be provided by the BSCU upon loss of either airplane electrical power input.
6	When “HYD 1 Enable” output is enabled, then “Alt/Emer Ctrl” output shall be disabled.
7	When “HYD 1 Enable” output is disabled, then “Alt/Emer Ctrl” output shall be enabled.
8	No single failure shall cause erroneous NMV command and inhibit the SOV function.
9	The wheel brake command function of the BSCU shall be developed to FDAL A.

The WBS PSSA process also identified assumptions shown in Table E14 used in the safety assessment that were managed by the system development process.

Table E14 - Safety assessment assumptions (WBS PSSA outputs)

Ref No.	Safety Assessment Assumption
1	The probability of “Loss of Normal Braking System Hydraulic Equipment” will be less than 3.3E-05 per flight.
2	The probability of “Loss of Alternate Braking System Hydraulic Equipment” will be less than 3.3E-05 per flight
3	The probability of 7 or more wheel speed sensors erroneous or inoperative will be less than 1.0E-07 per flight.
4	The probability of loss of an airplane electrical power bus will be less than 1.0E-04 per flight.
5	The probability of loss of a Left brake pedal position input will be less than 1.0E-04 per flight.
6	Airplane electrical power bus 1 is independent from airplane electrical power bus 2.
7	HYD 1 hydraulic system is independent from HYD 2 hydraulic system.

Assumptions 1 and 2 were applicable to the WBS, therefore safety requirements S18-WBS-R-6111 and S18-WBS-R-6112 were created to capture assumptions 1 and 2. Assumptions 3 through 7 were outside the scope of the WBS; these assumptions were communicated to the airplane development process.