SAE Aerospace
An SAE International Group

AEROSPACE RECOMMENDED PRACTICE

SAE ARP4754 | REV. A

Issued 1996-11
Revised 2010-12

Superseding ARP4754

(R) Guidelines for Development of Civil Aircraft and Systems

RATIONALE

This document provides updated and expanded guidelines for the processes used to develop civil aircraft and systems.

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

SAE values your input. To provide feedback on this Technical Report, please visit
http://www.sae.org/technical/standards/ARP4754A

ACKNOWLEDGMENTS

The leadership of the S-18 and WG-63 Committees would like to thank the actively contributing committee members, and their sponsoring companies, for the time, effort, and expense expended during the years of development of this document. Without the experience, cooperation and dedication of these people, development of this document would not have been possible.

John Dalton, Chair S-18	**Boeing Commercial Airplane Group**
Eric M Peterson, Vice Chair S-18	**Electron International II, Inc.**
Bob Mattern, Secretary S-18	**Pratt & Whitney**
Fernanda Altoé	EMBRAER
Steve Beland	Boeing Commercial Airplane Group
Art Beutler	Honeywell International, Inc.
Alessandro Landi	Airbus
Arun Murthi	Aero & Space USA
Michael Burkett	Rolls Royce
Alfred DuPlessis	Omnicon Group
Ervin Dvorak	FAA
Rachid Elkhatib	Rockwell Collins, Inc.
Charlie Falke	CFSS LLC
Steve Fisher	Rolls Royce
Dan Fogarty	Boeing Commercial Airplane Group
ndré Forni	CTA-IFI
Jean Gauthier	Dassault Aviation
Scot Griffith	Honeywell International, Inc.
Nazan Gürbüz	STM
Don Heck	Boeing Commercial Airplane Group
Jean Pierre Heckmann	Airbus
Linh Le	FAA
Doug Kemp	Rolls Royce
Zdzislaw Klim	Bombardier Aerospace
Hals Larsen	FAA
Tom Lewis	Lockheed Martin
Liza Lyon	Messier-Dowty
Jim Marko	Transport Canada
Fred Moon	Bell Helicopter
Warren Prasuhn	Rockwell Collins, Inc.
John Riege	Woodward Govenor
Matt Sandnas	Goodrich
Tilak Sharma	Boeing Commercial Airplane Group
Doug Sheridan	Cessna Aircraft Co.
Alvaro Tamayo	Thales Avionics Canada
Cengiz Tendürüs	STM
Inder Verma	Electron International II, Inc.
Andy Wallington	GE Aviation
Nelson Wilmers	ANAC
Steve Wilson	Rockwell Collins, Inc.
Ed Wineman	Gulfstream

Charles Zamora, Chair WG-63	**Airbus**
Mark Nicholson, Secretary WG-63	**Univ. of York**
Philippe Bernard	Intertechnique
Alain Cabasson	Dassault Aviation
Ray Chase	GE Aviation
Jean-Daniel Chauvet	Thales
Jean-Luc Delamaide	EASA
Jonathan Hughes	CAA, U.K.
Yuriy Ivanov	NIIAO
Anne-Cecile Kerbrat	Aeroconseil
Paul O'Donovan	GE Aviation
Alan Perry	AEC
Marielle Roux	Rockwell Collins, FR
Jiri Rybecky	Airbus Deutschland
Andrew Ward	Rolls-Royce
Jörg Wolfrum	Diehl Aerospace

1. SCOPE

This document discusses the development of aircraft systems taking into account the overall aircraft operating environment and functions. This includes validation of requirements and verification of the design implementation for certification and product assurance. It provides practices for showing compliance with the regulations and serves to assist a company in developing and meeting its own internal standards by considering the guidelines herein.

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

This document addresses the development cycle for aircraft and systems that implement aircraft functions. It does not include specific coverage of detailed software or electronic hardware development, safety assessment processes, in-service safety activities, aircraft structural development nor does it address the development of the Master Minimum Equipment List (MMEL) or Configuration Deviation List (CDL). More detailed coverage of the software aspects of development are found in RTCA document DO-178B, “Software Considerations in Airborne Systems and Equipment Certification” and its EUROCAE counterpart, ED-12B. Coverage of electronic hardware aspects of development are found in RTCA document DO-254/EUROCAE ED-80, “Design Assurance Guidance for Airborne Electronic Hardware”. Design guidance and certification considerations for integrated modular avionics are found in appropriate RTCA/EUROCAE document DO-297/ED-124. Methodologies for safety assessment processes are outlined in SAE document ARP4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”. Details for in-service safety assessment are found in ARP5150, “Safety Assessment of Transport Airplanes In Commercial Service” and ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service.“ Post-certification activities (modification to a certificated product) are covered in section 6 of this document. The regulations and processes used to develop and approve the MMEL vary throughout the world. Guidance for the development of the MMEL should be sought from the local airworthiness authority.

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.

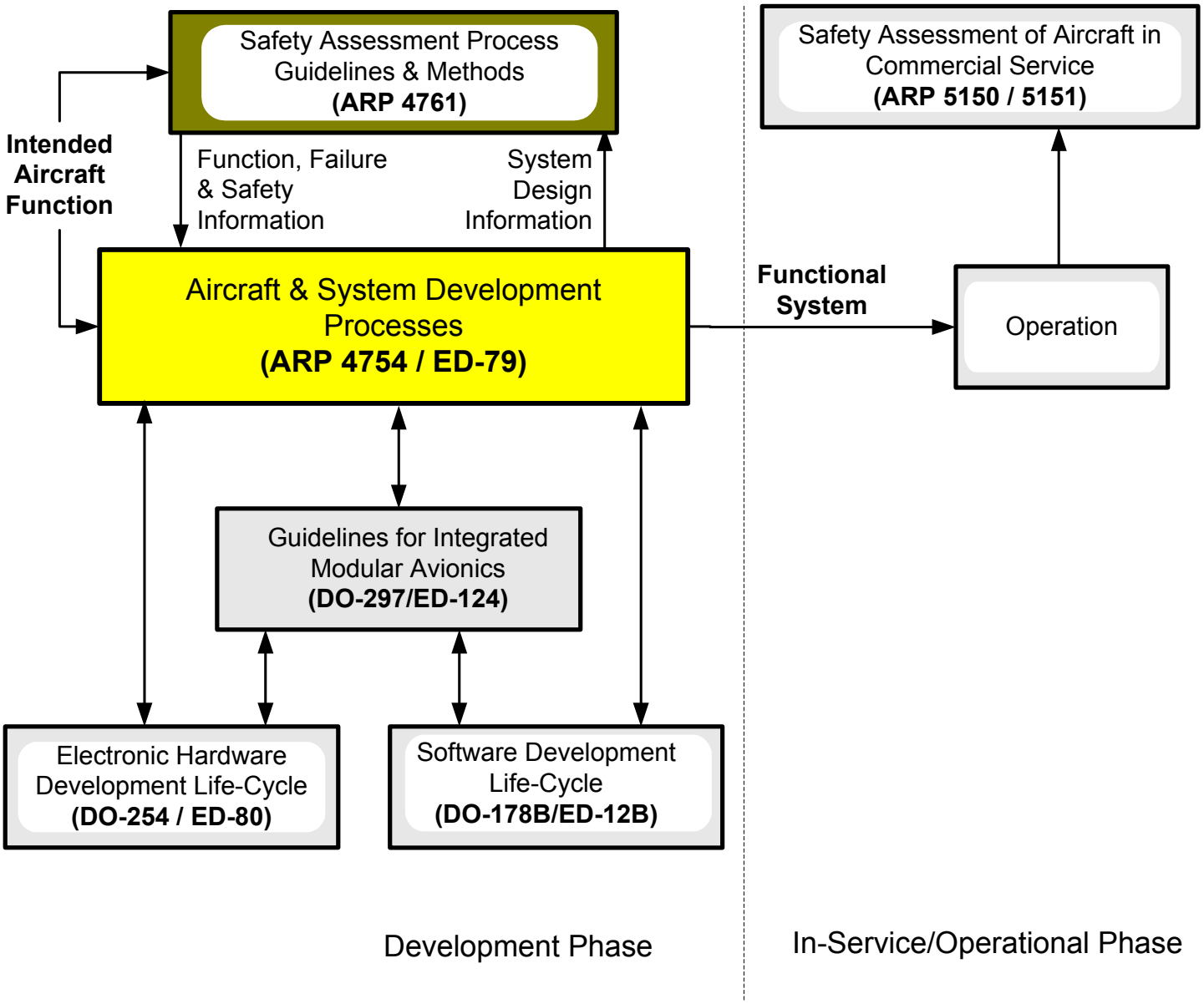

FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

1.1 Purpose

The guidelines herein are directed toward systems that support aircraft-level functions and have failure modes with the potential to affect the safety of the aircraft. Typically, these systems involve significant interactions with other systems in a larger integrated environment. Frequently, significant elements of these systems are developed by separate individuals, groups or organizations. These systems require added design discipline and development structure to ensure that safety and operational requirements can be fully realized and substantiated. A top down iterative approach from aircraft level downwards is key to initiating the processes outlined herein.

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 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 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 Task group (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 Federal Aviation Administration (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 design and support of large commercial aircraft, commuter aircraft, commercial and general aviation avionics, jet engines, and engine controls. Regulatory 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 14CFR/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, DO-178A/ED-12A and DO-178B/ED-12B being particularly significant.

The current trend in system design 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 14CFR/CS 23.1309 (see AC23.1309-1D, issued in 2009) and 25.1309 (see AMC 25.1309, published in 2003 and AC25.1309-Arsenal draft) the use of the ARP4754/ED-79 in aircraft certification has become increasingly widespread. Along with the increasing use, in particular Section 5.4 Assignment of Development Assurance Levels in the original ARP4754, come insights on the strengths and weaknesses of its guidelines. The underlying philosophy is succinctly represented in the original section 5.4 of ARP4754 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. Improvement to the development assurance level assignment process is one of the main features of this revision by providing a methodology to assign the correct development assurance levels.

When the original ARP 4754/ED-79 was published in 1996, the SIRT and WG-42 groups were dissolved. When the document came due for revision, a group with sufficient expertise at the aircraft level was required to address this work. The SAE S-18 Airplane Safety Committee was chosen because of their familiarity with the original document and the close association of the documents they develop and this ARP. Several S-18 committee members were on the SIRT group that developed the original ARP4754 document. At the same time, EUROCAE chartered a Working Group to update ED-79. WG-63 incorporated members from the original WG-42 working group, as well as representatives from a wide range of industrial and academic participants in the European Aerospace industry. Keeping to the Memorandum of Understanding for this document, WG-63 worked alongside S-18 to ensure that ED-79A is word-for-word equivalent to ARP4754A.

Revision A contains updates to the document that take into account the evolution of the industry over the intervening years. The relationship between ARP 4754/ED-79 and ARP 4761, and their relationship with DO-178B/ED-12B and DO-254/ED-80 are strengthened and discrepancies between the documents are identified and addressed. Revision A also expands the design assurance concept for application at the aircraft and system level and standardizes on the use of the term development assurance. As a consequence, for aircraft and systems Functional Development Assurance Level (FDAL) is introduced and the term design assurance level has been renamed Item Development Assurance Level (IDAL). Also included are enhancements created by feedback from the industry since the first publication. In addition, S-18 / WG-63 coordinated this revision effort with RTCA Special Committee 205 (SC-205) / EUROCAE WG-71 to ensure that the terminology and approach being used are consistent with those being developed for the update to DO-178B / ED-12B.

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 724-776-4970 (outside USA), www.sae.org.

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems

ARP5150 Safety Assessment of Transport Airplanes In Commercial Service

ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service

2.1.2 FAA Publications

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

14CFR Part 21 Certification Procedures for Products and Parts

14CFR Part 23 Airworthiness Standards: Normal, Utility, Acrobatic and Commuter Category Airplanes

14CFR Part 25 Airworthiness Standards: Transport Category Airplanes

14CFR Part 27 Airworthiness Standards: Normal Category Rotorcraft

14CFR Part 29 Airworthiness Standards: Transport Category Rotorcraft

14CFR Part 33 Airworthiness Standards: Aircraft Engines

14CFR Part 35 Airworthiness Standards: Propellers

AC 23.1309-1D System Safety Analysis And Assessment For Part 23 Airplanes

AC 25.19 Certification Maintenance Requirements

AC 25.1309-1A System Design and Analysis, Advisory Circular

2.1.3 EASA Publications

Available from European Aviation Safety Agency, Otto Platz 1, Postfach 101253, D-50452, Cologne, Germany, www.easa.eu.int.

IR-21 Certification Procedures for Aircraft, and Related Products & Parts

CS-23 Certification Specifications for Normal, Utility, Aerobatic, and Commuter 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 25.19 Certification Maintenance Requirements

AMC 25.1309 Equipment, Systems and Installations EASA Acceptable Means of Compliance

2.1.4 RTCA Publications

Available from Radio Technical Commission for Aeronautics Inc., 1828 L Street, NW, Suite 805, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-178 Software Considerations in Airborne Systems and Equipment Certification

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

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

DO-254 Design Assurance Guidance for Airborne Electronic Hardware.

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

2.1.5 EUROCAE Publications

Available from EUROCAE, 102 rue Etienne Dolet 92240, Malakoff, France.

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

ED-12B 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

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.

ACCEPTANCE: Acknowledgment by the certification authority that a submission of data, argument, or claim of equivalence satisfies applicable requirements.

AGREEMENT: Acknowledgment by the certification authority that a plan or proposal relating to, or supporting, an application for approval of a system or component, is an acceptable statement of intent with respect to applicable requirements.

AIRWORTHINESS: The condition of an aircraft, aircraft system, or component in which it operates in a safe manner to accomplish its intended function.

ANALYSIS: An evaluation based on decomposition into simple elements.

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

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

ASSESSMENT: An evaluation based upon engineering judgment.

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-178B / ED-12B)

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

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

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

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

CLASSIFICATION (FAILURE CONDITION): A discrete scale allowing categorization of the severity of the effects of a failure condition. The classification levels are defined in the appropriate CFR/CS advisory material (section 1309): Catastrophic, Hazardous/Severe-Major, Major, Minor, or No Safety Effect.

COMMON CAUSE ANALYSIS: Generic term encompassing zonal safety analysis, particular risk analysis, and common mode analysis.

Common Mode Analysis: An analysis performed to verify that failure events identified in the ASA/SSA are independent in the actual implementation.

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

COMPLEXITY: An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.

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

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

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.

CONFORMANCE: Established as correct with reference to a standard, specification or drawing.

DEMONSTRATION: A method of proof of performance by observation.

DERIVED REQUIREMENTS: Additional requirements resulting from design or implementation decisions during the development process which are not directly traceable to higher-level requirements.

DEVELOPMENT ASSURANCE: All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis. (AMC 25).

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

ERROR: An omitted or incorrect action by a crewmember 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 a component, part or element 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. (AMC 25.1309)

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

FAILURE MODE: The way in which the failure of a system or item occurs.

FAILURE RATE: The gradient of the failure distribution function divided by the reliability distribution function at time t.

$$\lambda(t) = F'(t)/(1-F(t))$$

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

FUNCTION: Intended behavior of a product based on a defined set of requirements regardless of implementation.

FUNCTION Development Assurance Level: The level of rigor of development assurance tasks performed to Functions. [Note: The FDAL is used to identify the ARP4754 /ED-79 objectives that need to be satisfied for the aircraft/system functions].

FUNCTIONAL FAILURE SET: A single Member or a specific group of Members that are considered to be independent from one another (not necessarily limited to one system) that lead(s) to a top level Failure Condition.

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

FUNCTIONAL INDEPENDENCE: An attribute where the Functions are different in order to minimize the likelihood of a common requirement error.

GUIDANCE: Recommended procedure for complying with regulations.

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

HARDWARE: An item that has physical being.

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

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

INDEPENDENCE: 1. A concept that minimizes the likelihood of common mode errors and cascade failures between aircraft/system functions or items, 2. Separation of responsibilities that assures the accomplishment of objective evaluation e.g. validation activities not performed solely by the developer of the requirement of a system or item.

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 or an item indicating that it can be relied upon to work correctly. It is sometimes expressed in terms of the probability of not meeting the work correctly criteria.

INTERCHANGEABILITY: The ability to substitute one part for another within a system and have the system perform to its specification.

ITEM: A hardware or software element having bounded and well-defined interfaces.

ITEM DEVELOPMENT ASSURANCE: All of those planned and systematic tasks used to substantiate, to an adequate level of confidence, that development errors have been identified and corrected such that the items satisfy a defined set of requirements.

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-178B/ED-12B, and design assurance level in DO-254/ED-80 objectives that need to be satisfied for an item].

ITEM DEVELOPMENT INDEPENDENCE – An attribute that minimizes the likelihood of a common mode error in the item development process.

MEAN TIME BETWEEN FAILURES (MTBF): Mathematical expectation of the time interval between two consecutive failures of a hardware item. NOTE: The definition of this statistic has meaning only for repairable items. For non-repairable items, the term Mean Time To Failure (MTTF) is used.

MEMBER: An aircraft/system function or item that may contain an error causing its loss or anomalous behavior. [This definition is limited to the Functional Failure Set application herein.]

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

MODELING TECHNIQUE: The approach used to model a given aspect of a system/function/item.

PARTICULAR RISKS: Particular risks are defined as those events or influences which are external to the aircraft or within the aircraft but external to the system(s) and item(s) being analyzed, but which may violate failure independence claims.

PARTITIONING: The mechanism used to separate portions of a system or an item with sufficient independence such that a specific development assurance level can be substantiated within the partitioned portion.

PRELIMINARY SYSTEM SAFETY ASSESSMENT: A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items.

PROCESS: A set of interrelated activities performed to produce a prescribed output or product. (DO-254/ED-80)

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

RELIABILITY: The probability that a system or 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.

REQUIREMENTS MODEL: A model representing completely or partially, the requirements at the abstraction level the model addresses.

RISK: The combination of the frequency (probability) of an occurrence and its associated level of severity.

SAFETY: The state in which risk is acceptable.

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

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

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

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

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

TEST: A quantitative procedure to prove performance using stated objective criteria with pass or fail results.

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

VALIDATION: The determination that the requirements for a product are correct and complete. [Are we building the right aircraft/ system/ function/ item?]

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met. [Did we build the aircraft/ system/ function/ item right?]

ZONAL SAFETY Analysis: The safety analysis standard with respect to installation, interference between systems, and potential maintenance errors that can affect system safety.

2.3 Abbreviations and Acronyms

AC	Advisory Circular (FAA)
AMC	Acceptable Means of Compliance (EASA)
AOA	Angle of Attack
ARAC	Aviation Rulemaking Advisory Committee (FAA)
ARP	Aerospace Recommended Practice (SAE)
ASA	Aircraft Safety Assessment
ASAT	Aircraft-Level Safety Assessment Team
ATC	Amended Type Certificate
CAT	Catastrophic
CFR	Code of Federal Regulations
CC	Change Control
CCA	Common Cause Analysis
CM	Configuration Management
CMA	Common Mode Analysis
CMP	Configuration Management Plan
CMR	Certification Maintenance Requirement
COTS	Commercial Off-The-Shelf
CS	Certification Specifications
DD	Dependence Diagram
EASA	European Aviation Safety Agency
ETOPS	Extended Twin Operations
ETSO	European Technical Standard Order
EUROCAE	European Organization 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 Modes and Effect Analysis
FMES	Failure Modes and Effect Summary
FTA	Fault Tree Analysis
HAZ	Hazardous
HDL	Hardware Description (Design) Language
HW or H/W	Hardware
ICA	Instructions for Continued Airworthiness
ICAO	International Civil Aviation Organization
IDAL	Item Development Assurance Level
IMA	Integrated Modular Architecture
IR	Implementation Rule
JAA	Joint Aviation Authorities
MA	Markov Analysis
MMEL	Master Minimum Equipment List
MSG-3	Maintenance Steering Group 3
MTBF	Mean Time Between Failures
OEM	Original Equipment Manufacturer
PASA	Preliminary Aircraft Safety Assessment
POA	Production Organization Approval
PR	Problem Report
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RTCA	RTCA, Inc.
SAE	SAE International
SC	System Control Category
SIRT	Systems Integration Requirements Task
SSA	System Safety Assessment
STC	Supplemental Type Certificate
SW or S/W	Software

TC	Type Certificate, Transport Canada
TSO	Technical Standard Order
V&V	Validation and Verification
VHDL	VHSIC Hardware Description (Design) Language
VHSIC	Very High Speed Integrated Circuit
WG-#	A numbered working group (EUROCAE).
ZSA	Zonal Safety Analysis

3. DEVELOPMENT PLANNING

The purpose of the development planning process is to define the means of producing an aircraft or system which will satisfy the aircraft/system requirements and provide the level of confidence which is consistent with airworthiness requirements. The objectives of the development planning process are:

- To define the activities of the development processes and integral processes of the development life cycle that will address the aircraft/system requirements, functional development assurance level(s) and item development assurance level(s).
- To define the development life cycle(s), including the inter-relationships between the processes, their sequencing, feedback mechanisms, and transition criteria.
- To select the life cycle environment, including the methods and tools to be used for the activities of each 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 comply with objectives of each integral process (section 5).

The outputs of the planning process can exist in various formats such as integrated schedules or formally released planning documents. The iterative nature of the design process should be considered during the planning process. Interrelationships between the planning elements and feedback loops should also be identified and managed, as appropriate.

3.1 Planning Process

Figure 2 is an example of the overall planning process and includes some generic objectives applicable to all planning elements. The basic process shown in Figure 2 suggests that all of the planning elements need to be thought about before documenting any of them. In reality, 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.

Throughout this document, the individual planning activities for each process are described in detail in their sections. Table 1 summarizes the elements that should be included in the planning phase. They should address the design and certification of the respective aircraft, system or item.

This process can be re-entered for aircraft or system changes, such as a new derivative model or modifications to an in-service aircraft.

3.2 Transition Criteria

A key component 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 stage of development to another should be tracked and managed, as appropriate.

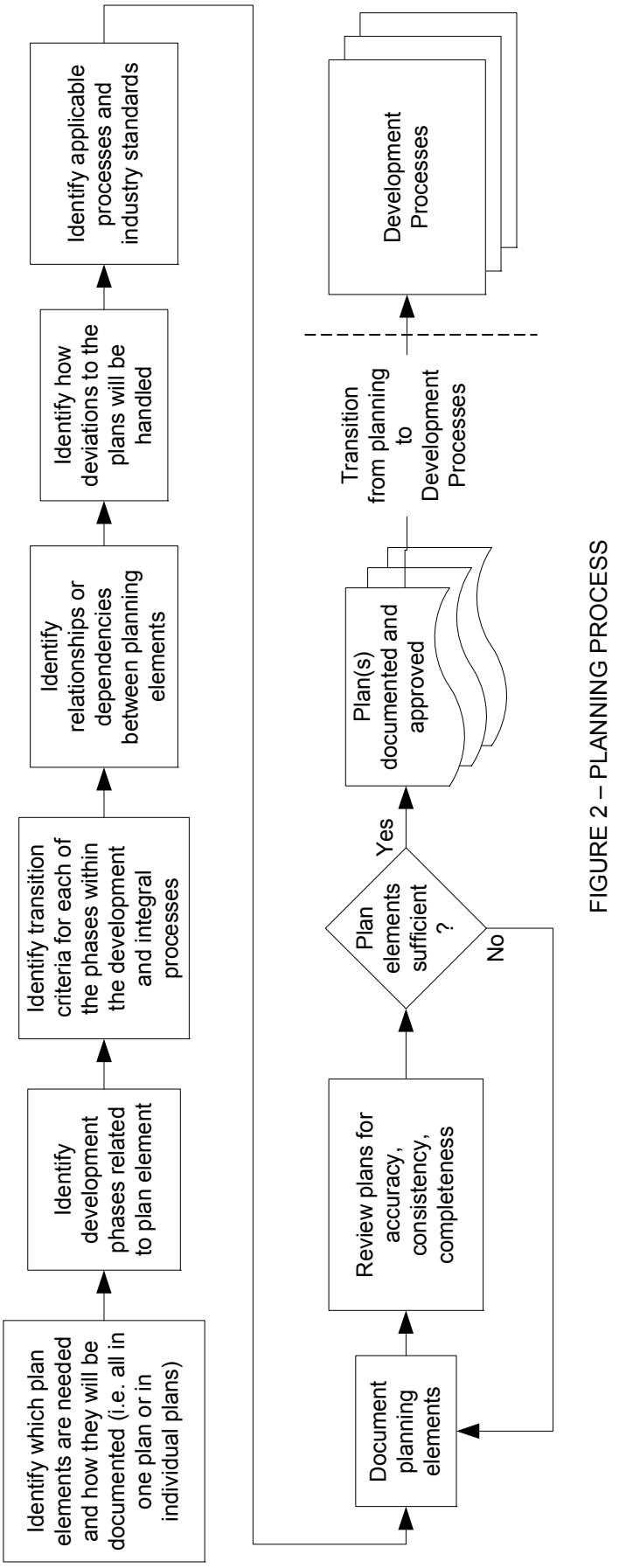

FIGURE 2 – PLANNING PROCESS

TABLE 1 – DEVELOPMENT PLANNING ELEMENTS

Planning Elements	Element Description	4754A Section
Development	Establish the process and methods to be used to provide the framework for the aircraft/system architecture development, integration and implementation.	This section and 4.0
Safety Program	Establish scope and content of the safety activities related to the development of the aircraft or system.	5.1.5
Requirements Management	Identify and describe how the requirements are captured and managed. Sometimes these elements are included in conjunction with the validation elements.	5.3
Validation	Describe how the requirements and assumptions will be shown to be complete and correct.	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
Certification	Describe the process and methods that will be used to achieve certification.	5.8

3.2.1 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 deviatations from the plans. Methods for reporting, gaining approval of, and documenting any deviations should be described in the planning elements.

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, and can be re-entered to address aircraft or system changes. Figure 3 is a simple illustration of a development life cycle. The guidelines contained in this document are primarily geared toward the “Development” phase.

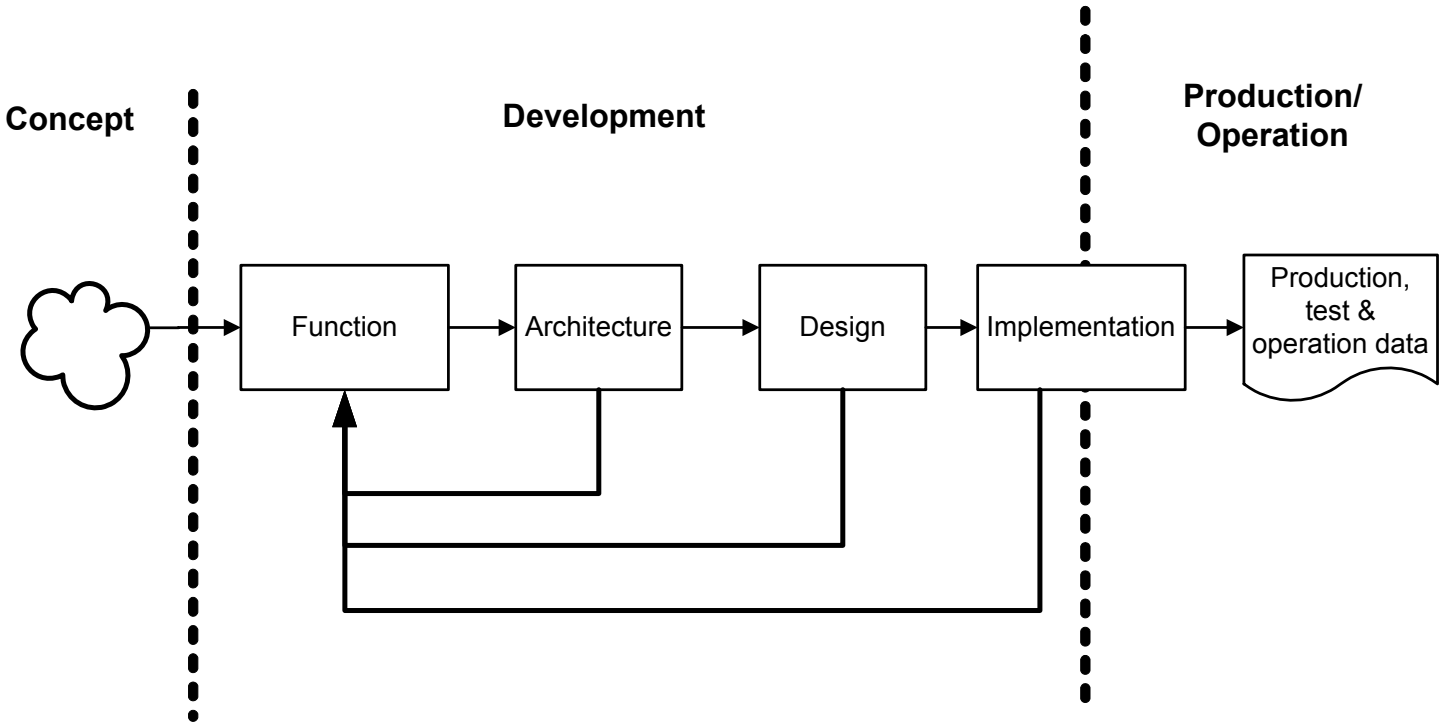

FIGURE 3 - DEVELOPMENT LIFE CYCLE

The Concept phase (i.e. research and preliminary development phase) determines the overall aircraft performance and configuration such as payload and range, aircraft size, number and locations of engines, airfoil, 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(ies),
- All regulatory compliance data is submitted and approved,
- The design has met all internal compliance data (as required),
- Limitations, maintenance and other operational information are provided to the aircraft operators.

4.1 Conceptual 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 4 provides a graphical representation of the system development process model 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 model for 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 company 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.

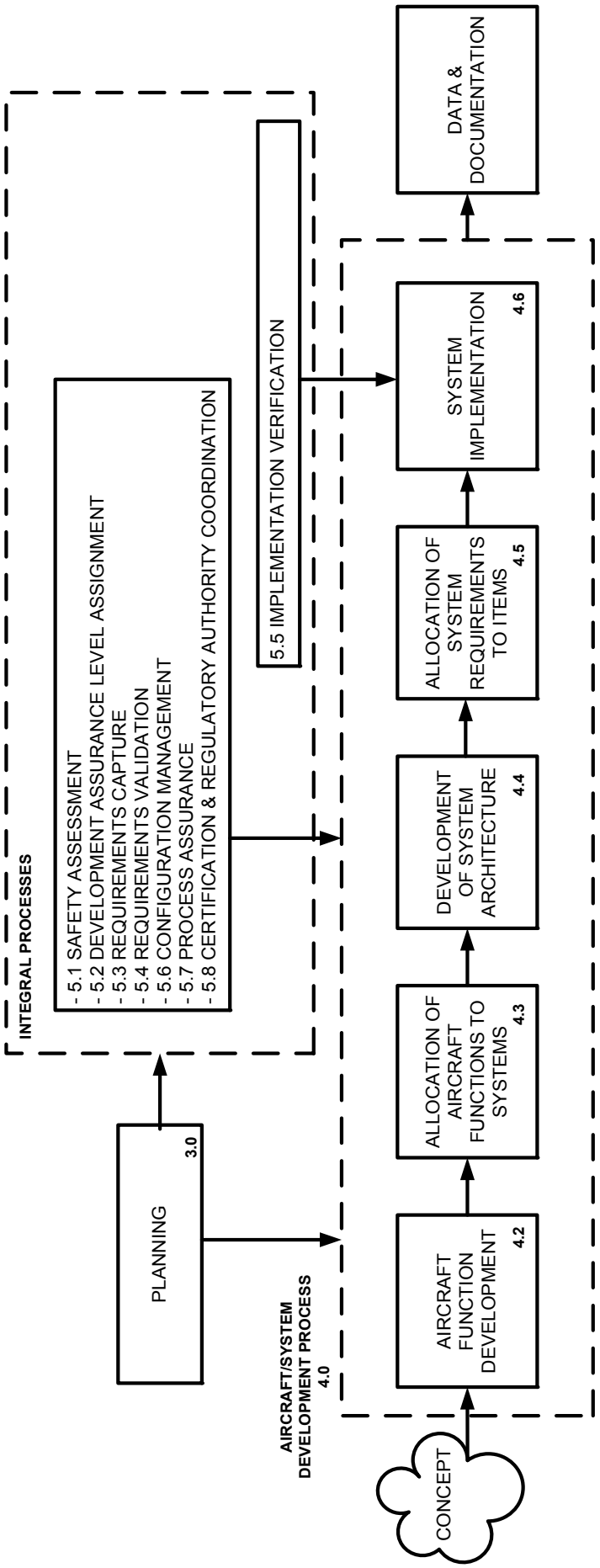

FIGURE 4 – AIRCRAFT OR SYSTEM DEVELOPMENT PROCESS MODEL

4.1.1 Development Assurance

Due to the highly complex and integrated nature of modern aircraft systems the regulatory authorities have highlighted concerns about the possibility of development errors causing or contributing to aircraft Failure Conditions. To address these concerns, a methodology to mitigate 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 14CFR/CS 25.1309; AMC25.1309 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-178B/ED-12B and DO-254/ED-80 has been recognized by industry and the various regulatory 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 the 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 (requirements determination and design errors) and undesirable, unintended effects. 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 demonstrates 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 function development assurance level (FDAL) 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 do not complement each other.

In this context, this ARP4754A/ED-79A regards the activities of DO-178B/ED-12B and DO-254/ED-80 as a 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 5.

Section 5.2 provides the guidelines for assigning the FDALs and IDALs starting from the aircraft level through to item level requirements. The objectives for accomplishment of each FDAL are outlined in Appendix A. The objectives for accomplishment of each IDAL are per DO-178B/ED-12B and DO-254/ED-80 for software and electronic hardware items, respectively.

In summary, 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.

4.1.3 Introduction to Hierarchical Safety Requirements Generated from Safety Analyses

Safety requirements exist at the aircraft, system, and item level. Types of safety requirements include independence, quantitative (probabilistic), qualitative, availability, integrity, monitoring, FDAL, operational and maintenance requirements.

Safety requirements are functionally decomposed from aircraft level function to item level in a hierarchical structure. At aircraft level the safety requirements are those requirements generated from the aircraft FHA based on aircraft functions e.g. directional control, deceleration on ground, etc. At system level, the safety requirements are all those system level requirements generated from the system FHA which are decompositions of the aircraft level safety requirements. At the next level down the requirements are all those aspects of the system which allow the safety objectives associated with the system FHA classifications to be satisfied. Figure 5 illustrates the various requirement levels. Safety requirements may also be generated from Common Cause Analyses.

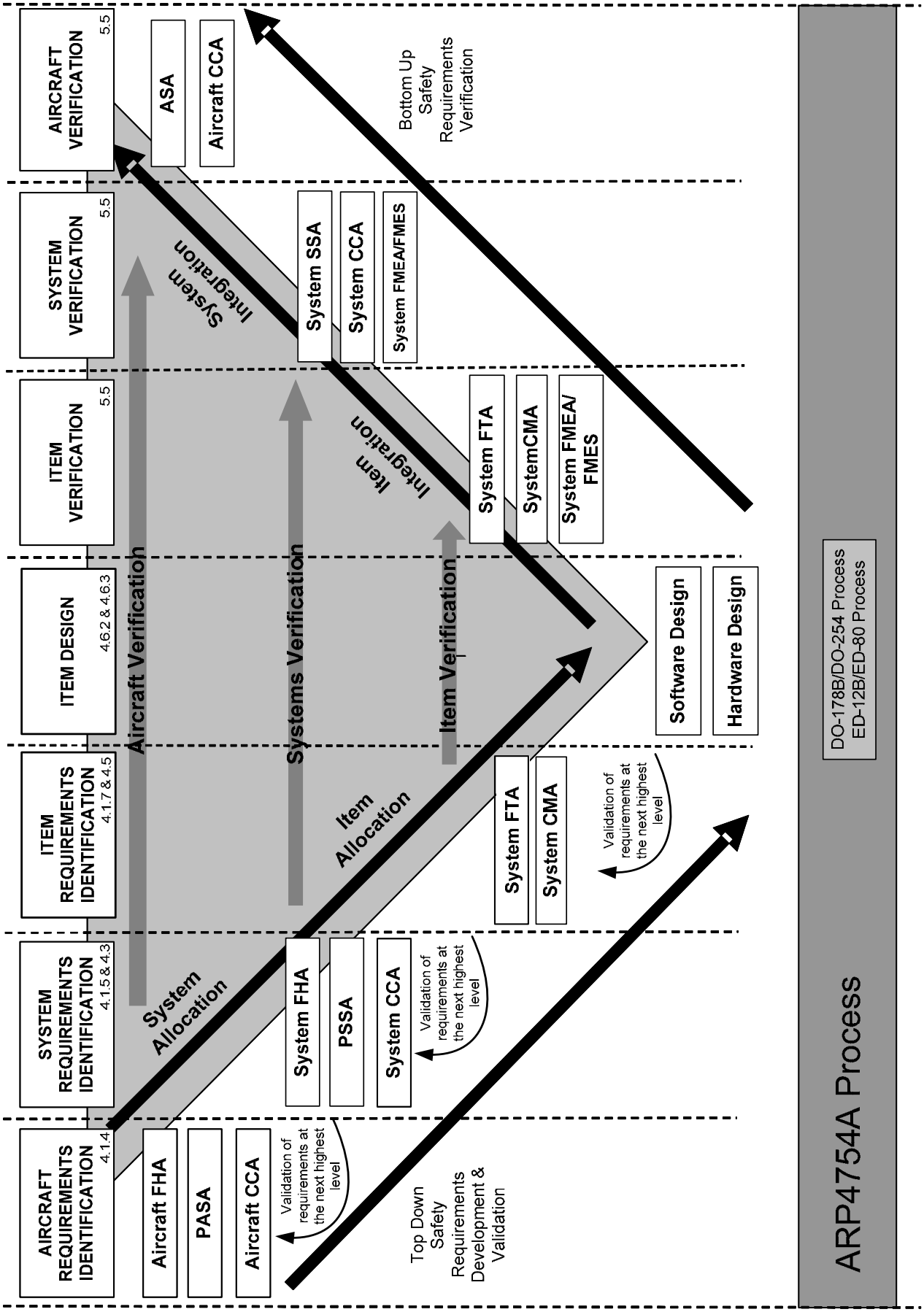

FIGURE 5 - INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

4.1.4 Identification of Aircraft-Level Functions, Function Requirements and Function Interfaces

This activity establishes basic aircraft level performance and operational requirements. From these basic requirements, aircraft level functions and their requirements can be established and the function interfaces with the external physical and operational environment identified. Aircraft-level functions are high-level activities and are not necessarily associated with a single, physical system implementation.

The output of this activity is a list of aircraft-level functions and the associated function requirements and interfaces for these functions.

4.1.5 Allocation of Aircraft Functions to Systems

This level of activity establishes the appropriate grouping of aircraft functions and the allocation of the requirements for these functions to systems. The output of this activity is a set of requirements for each aircraft system including their associated interfaces.

4.1.6 Development of System Architecture

The system architecture is accomplished as a part of this process activity. This system architecture establishes the structure and boundaries within which specific item designs are implemented to meet all of the established safety and technical performance requirements. The outputs of this activity include the system architecture to the item level and the allocation of system function and safety requirements to the appropriate items.

4.1.7 Allocation of System Requirements to Items

In practice, system architecture development and the allocation of requirements are tightly-coupled, iterative processes. With each iteration cycle, the identification and understanding of the requirements increases and the allocation of the system-level requirements to hardware or software items becomes clearer. Outputs of this allocation effort are requirements allocated to hardware and software, inclusive of safety objectives, development assurance levels and function/performance requirements.

4.1.8 System Implementation

The System Implementation stage of the process model interfaces the system process model described in this document and the DO-178B/ED-12B software and DO-254/ED-80 electronic hardware development process life-cycle guidance documents.

This stage also provides the tasks for ensuring the aircraft systems individually and collectively operate correctly.

The outputs of this phase include hardware-software integration procedures, system integration procedures, released hardware drawings, software source code together with related documentation, applicable development assurance data, breadboard or prototype hardware, if applicable; and lab/flight test articles.

4.2 Aircraft Function Development

While Figure 4 illustrates the generic system development process, Figure 6 shows an aircraft function implementation process. The model 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 actual system 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 6 are concurrent and may involve interactive dependencies that lead to alteration of previously established requirements.

As part of the function requirements allocation process, the associated Failure Condition classification information should be stated explicitly. This provides traceability in order to substantiate any advantage from further architectural partitioning. Derived requirements again emerge from this portion of the allocation process, and should be validated and their impact on safety determined.

Typical aircraft functions may include:

a. Flight Control

b. Ground Steering

c. Aircraft Aspects of ATC

d. Automatic Flight Control

e. Cargo Handling

f. Engine Control

g. Collision Avoidance

h. Ground Deceleration

i. Environmental Control

j. Passenger Comfort

k. Communication

l. Guidance

m. Navigation

n. Passenger Safety

When this document is applied to engine development, typical engine functions may include:

a. Modulate Thrust

b. Thrust Reverser Control

c. Passenger Safety

d. Aircraft Communication

e. Engine Health Monitoring

When this document is applied to propeller development, typical propeller functions may include:

a. Modulate Speed

b. Passenger Safety

c. Modulate Pitch of Blade

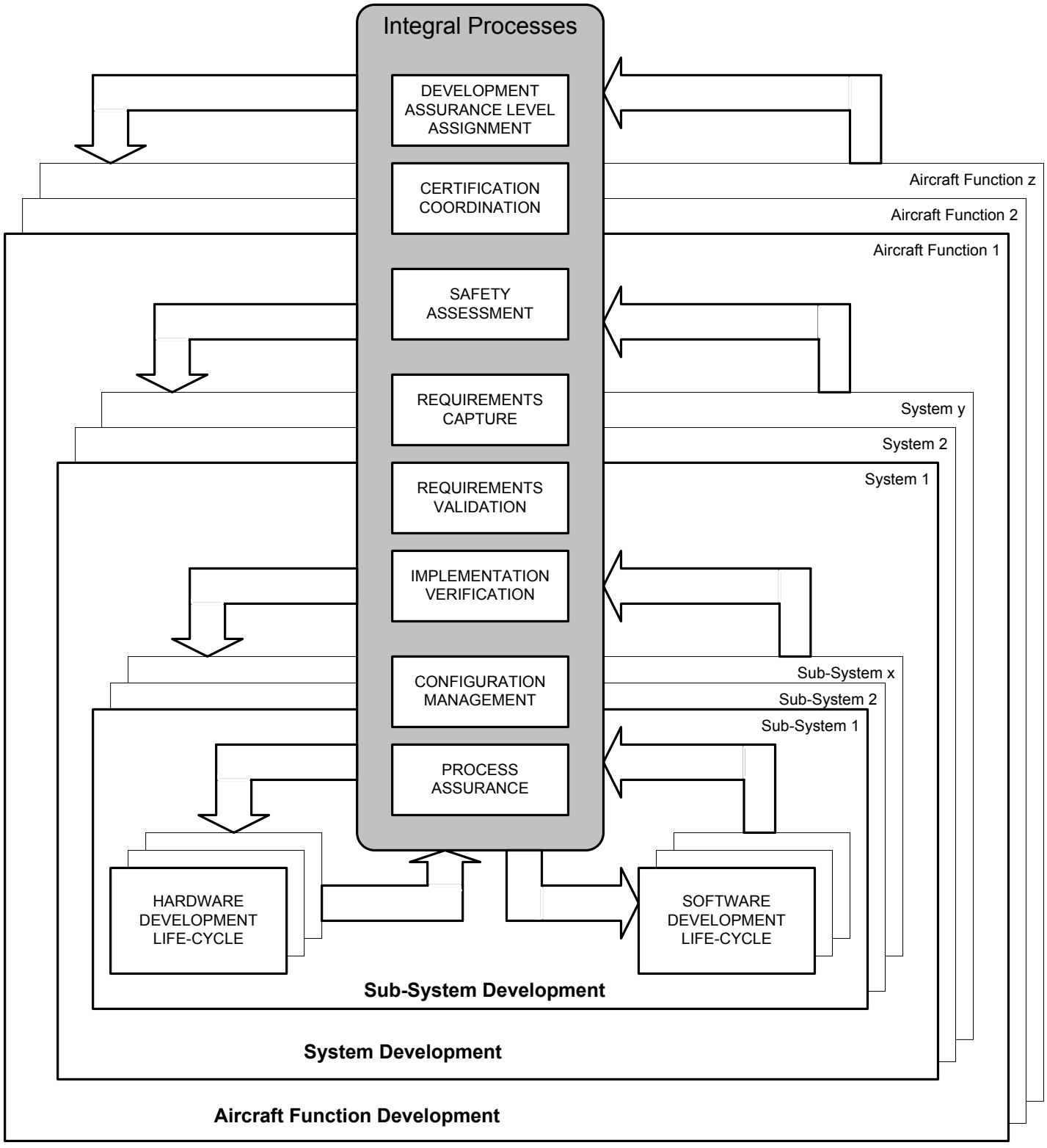

FIGURE 6 - AIRCRAFT FUNCTION IMPLEMENTATION PROCESS

4.3 Allocation of Aircraft Functions to Systems

The next level of activity consists of establishing the appropriate grouping of aircraft functions and the allocation of the related requirements (including requirements from the aircraft level FHA) to systems. The process for selecting the appropriate functional grouping 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 are subject to the same validation activity as are other requirements.

From the function allocations and the associated failure consequences, 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, allocations to systems and to people 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. The interfaces should be defined with all inputs having a source and all outputs having destination(s), either human or another system.

4.4 Development of System Architecture:

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, the Preliminary Aircraft Safety Assessment (PASA) / Preliminary System Safety Assessment (PSSA) and Common Cause Analysis (CCA) processes to establish feasibility in meeting the function and top level safety requirements assigned to the system. Guidelines for performing the PASA/PSSA and CCA are summarized in sections 5.1.2 and 5.1.4, respectively.

Derived requirements stemming from technology, architecture, system and item interfaces, or implementation choices become more clearly visible as work on the system architecture progresses. The potential impact of derived requirements on higher level requirements needs to be assessed.

The outputs of this activity are the definition of the system architecture to the item level and the allocation of top level system functional and associated lower level safety requirements. Requirements governing item interfaces, system constraints (physical, environmental, etc). and integration should be included.

4.5 Allocation of System Requirements to Items

In practice, system architecture development and the allocation of system requirements to item requirements are tightly-coupled, iterative processes. With each cycle, the identification and understanding of derived requirements increases and the rationale for the allocation of system-level requirements to hardware or software at the item level becomes clearer. The process is complete when all requirements can be accommodated within the final architecture. The decomposition and allocation of requirements to items should also ensure that the item can be shown to fully implement the allocated requirements.

Derived requirements arising from allocation may be system related or software-hardware related. Similarly the verification of implementation against allocated requirements may be performed at the system level or at the item level.

Outputs of this allocation effort are requirements allocated to hardware, with appropriate safety objectives and development assurance levels, and requirements allocated to software, including development assurance levels, for each item. Requirements governing hardware-software integration should be included, where necessary. The results of this activity are also used to update the preliminary system safety assessment.

4.6 System Implementation

System implementation has four primary points;

a. Information flow from the system process to the hardware & software processes and vice-versa,

b. Hardware/Software Design & Build,

c. Hardware/Software Integration and

d. System Integration.

These are further discussed in the next sub-paragraphs.

4.6.1 Information Flow - System Process To & From Item Process(es)

4.6.1.1 Information Flow From System Process To Hardware/Software Processes

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

The point where requirements are allocated to hardware and software items is also the point where the guidelines of this document transition to the guidance of DO-178B/ED-12B (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 hardware and/or software has been reached at the point when architecture, redundancy management and requirement decomposition are complete.

The following data is passed to the software and hardware processes as part of the requirements allocation:

a. Requirements allocated to hardware.

b. Requirements allocated to software.

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 and partitioning requirements and any item development independence requirement.

g. System verification activities to be performed at the software or hardware development level, as applicable.

h. Evidence of the acceptability by the system process of any data provided by the hardware and/or software 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 software process to determine if there is any impact on the SSA.

4.6.1.2 Information Flow From Hardware/Software 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 requirements (both hardware and software) to be evaluated against the system or item requirements and safety assessments,

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

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

d. Hardware failure rates, fault detection coverage, common cause analyses and latency intervals, for incorporation in the SSA,

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

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

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

h. Details of proposed hardware/software 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. Derived 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 Hardware and Software Design/Build

The hardware and software design/build processes should provide traceability to the requirements allocated to hardware and software. If hardware and software 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 electronic hardware-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 section 2.1.4 and 2.1.5 provide guidance for the development of electronic hardware and software.

4.6.3 Electronic Hardware/Software Integration

Depending on the nature of the system and the development process used, initial item electronic hardware and software integration may occur on breadboards, prototypes, computer emulation, lab or flight-worthy articles. The output is equipment under configuration control together with development assurance data and hardware and/or software life cycle data. Detailed procedures developed during the design-build process should be used to verify that all electronic hardware and software integration requirements are met.

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

4.6.4 Aircraft/System Integration

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 may dictate that some integration activities be performed on the aircraft. While the validity of on-the-aircraft integration is generally assumed to be high, more meaningful or cost-effective results often can be achieved in laboratory or simulation environments. Specific procedures for system integration vary widely across the industry.

During the integration process, identified deficiencies should 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 a verified integrated system, along with the data demonstrating that the system satisfies all functional and safety requirements.

Aircraft/System integration is the task of ensuring all the aircraft systems operate correctly individually and together as installed on the aircraft. This provides the means to show that intersystem requirements, taken as a group, have been satisfied. It also provides an opportunity to discover and eliminate undesired unintended functions.

5. INTEGRAL PROCESSES

The process elements described in this section are fundamental elements of the overall process. They have multiple interactions to the process tasks in section 4.1.

5.1 Safety Assessment

The safety assessment process is used by a company to show compliance with certification requirements (e.g. 14CFR/CS Parts 23 and 25, section 1309) and in meeting its own internal safety standards. The process includes specific assessments conducted and updated during system development and includes how it interacts with the other system development processes. The primary safety assessment processes are detailed in ARP 4761 and are summarized below.

a. Functional Hazard Assessment (FHA): Examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific failure conditions. The FHA is developed early in the development process and is updated as new functions or Failure Conditions are identified. Thus, the FHA is a living document throughout the design development cycle.

b. Preliminary Aircraft Safety Assessment / Preliminary System Safety Assessment (PASA/PSSA): Establish the aircraft or specific system or item safety requirements and provide a preliminary indication that the anticipated aircraft or system architectures can meet those safety requirements. The PASA and PSSA are updated throughout the system development process ultimately resulting in the Aircraft Safety Assessment and System Safety Assessments.

c. Aircraft Safety Assessment / System Safety Assessment (ASA/SSA): Collects, analyzes, and documents verification that the aircraft and systems, as implemented, meet the safety requirements established by the PASA and the PSSA.

d. Common Cause Analysis (CCA): Establishes and verifies physical and functional separation, isolation and independence requirements between systems and items and verifies that these requirements have been met.

Additionally, for appropriate management of the safety assessment process, a Safety Program Plan should be created. The Failure Conditions identified in the FHA may also be tracked through the development process to provide active status that the design implementation is satisfying the safety criteria.

Figure 7 shows the fundamental relationships between these four specific assessments 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.

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.

The safety assessment activities are summarized in the subsequent sections of this document.

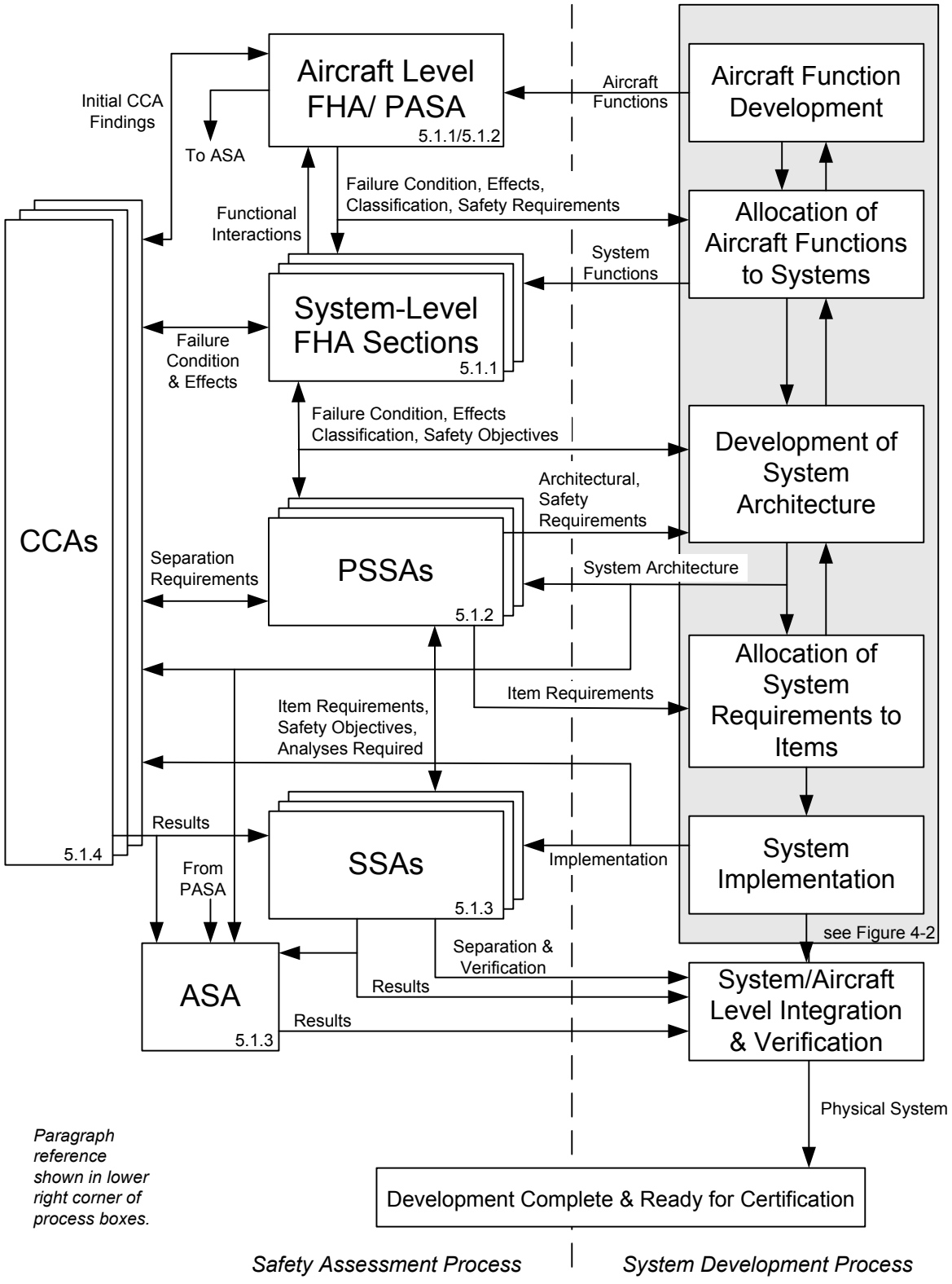

FIGURE 7 - SAFETY ASSESSMENT PROCESS MODEL

5.1.1 Functional Hazard Assessments

The functional hazard assessments (FHAs) should be carried out at both the aircraft and system levels. They should provide the following information relative to each function (aircraft or system level accordingly):

a. Identification of related Failure Condition(s).

b. Identification of the effects of the Failure Condition(s).

c. Classification of each Failure Condition based on the identified effects (i.e., Catastrophic, Hazardous/Severe-Major, Major, Minor, or No Safety Effect) and assignment of the necessary safety objectives, as defined in e.g. AC 25.1309-1A, AC23.1309-1D and AMC 25.1309 extended to include the No Safety Effect classification.

d. A statement outlining what was considered and what assumptions were made when evaluating each Failure Condition (e.g., adverse operational or environmental conditions and phase of flight).

The goal in conducting this step is to clearly identify the circumstances and severity of each Failure Condition along with the rationale for its classification.

Since it is possible that use of common architectures or complex components in separate systems could introduce additional aircraft-level Failure Conditions involving multiple functions, the FHA should identify and classify these new Failure Conditions. When aircraft-level functions are integrated by a system or combination of systems, the FHA should be re-evaluated to identify and classify Failure Conditions involving multiple functions. If the FHA is constructed in system-oriented sections, traceability of hazards and Failure Conditions between the aircraft-level and system-level is necessary.

Implementation choices made during development may introduce common causes for multiple aircraft-level Failure Conditions or interactions between systems resulting in failure. These common causes could cross system or function boundaries. A review of the implementations of systems should be performed to determine if there are such conditions and if they should be added to the aircraft-level FHA.

For details on performing an aircraft or a system level FHA, see ARP4761 Appendix A.

5.1.2 Preliminary Aircraft / System Safety Assessment

A Preliminary Aircraft / System Safety Assessment (PASA/PSSA) is a systematic examination of a proposed architecture(s) to determine how failures could cause the Failure Conditions identified by the FHA. The objectives of the PASA and PSSA are to complete the safety requirements of an aircraft, system or item and validate that the proposed architecture can reasonably be expected to meet the safety requirements. The PASA/PSSA may identify the need for alternative protective strategies (e.g., partitioning, built-in-test, monitoring, independence and safety maintenance task intervals, etc.). The PASA/PSSA outputs should be used as an input to the ASA/SSA and other documents, including, but not limited to, system requirements, software requirements, and hardware requirements.

The PASA/PSSA are iterative processes associated with the design definition. The PASA/PSSA is conducted at multiple stages of system development including aircraft, system, and item design definitions. At the lowest level, the PSSA determines the safety related design requirements of hardware and software.

For details on performing a preliminary aircraft or systems safety assessment (PASA/PSSA), see ARP4761 Appendix B.

5.1.3 Aircraft / System Safety Assessment

An Aircraft/System Safety Assessment (ASA/SSA) is a systematic, comprehensive evaluation of the implemented aircraft and system(s) to show that relevant safety requirements are satisfied. The difference between the PASA/PSSA and an ASA/SSA is that the PASA/PSSA are methods to evaluate proposed architectures and derive system/item safety requirements; whereas the ASA/SSA are methods to verify that the implemented design meets the safety requirements as defined in the PASA and PSSA.

The ASA/SSA integrates the results of the various analyses to verify the safety of the overall aircraft/systems and to cover all of the specific safety considerations identified in the PASA/PSSA. The ASA/SSA process data includes results of the relevant analyses and substantiation. This may include the following information:

a. List of previously agreed upon external event probabilities,

b. System description including functions and interfaces,

c. List of Failure Conditions (FHA, PASA, PSSA),

d. Failure Condition classification (FHA, PASA, PSSA),

e. Qualitative analyses for Failure Conditions (e.g. FTA, FMES, Markov Analysis, Dependence Diagrams),

f. Quantitative analyses for Failure Conditions (e.g. FTA, FMES, Markov Analysis, Dependence Diagrams),

g. The results obtained from Common Cause Analyses,

h. Safety related tasks and intervals (FTA, FMES, Markov Analysis, Dependence Diagrams),

i. Development Assurance Levels for aircraft functions and systems (FDAL) (PASA, PSSA),

j. Development Assurance Levels for electronic hardware and software items (IDAL)(PSSA),

k. Verification that safety requirements from the PASA, PSSA are incorporated into the design and/or testing process,

l. The results of the non-analytic verification processes (i.e. test, demonstration and inspection).

The Aircraft Safety Assessment should provide a summary of the aircraft safety activities from the beginning of the concept development to the completion of the detailed design development. It aims to show compliance with aircraft level requirements and objectives and give assurance that the appropriate methods and process have been applied. The Aircraft Safety Assessment verifies that:

- All the safety activities have been performed according to the Safety Plan,
- Safety requirements for the aircraft are satisfied and associated supporting material is available,
- Safety Validation/Verification process is completed and results accepted,
- All the activities undertaken form a logical argument supporting the conclusion that the aircraft is safe.

This assessment forms part of what is sometimes called a “safety case” or “safety synthesis”. A safety case or safety synthesis communicates a clear, comprehensible and defensible argument that the aircraft and systems are acceptably safe to operate in a particular context.

Note: When Fault Tree Analysis (FTA) is used herein, it should be understood that other analysis methods such as Dependence Diagrams (DD) or Markov Analsis (MA) may also be used if they are the appropriate analysis for the situation.

For details on performing an aircraft or systems level safety assessment (ASA/SSA), see ARP4761 Appendix C.

5.1.4 Common Cause Analysis

Independence between functions, systems or items may be required to satisfy the safety or regulatory requirements. Therefore, it is necessary to ensure that such independence exists, or that the lack of independence is acceptable. Common Cause Analysis (CCA) provides the tools to verify this independence, or to identify specific dependencies. Common cause events should be precluded for catastrophic failure conditions.

In particular, the CCA identifies individual failure modes or external events that can lead to a Catastrophic or Hazardous/Severe-Major Failure Condition. Common Cause Analysis is sub-divided into the following areas of study to aid in the assessment:

a. Particular Risks Analysis

b. Common Mode Analysis

c. Zonal Safety Analysis

These analyses may be performed at any stage of the design process. Obviously, the most cost-effective time is early in the design process because of the potential influence on system architecture and installation. However, confirmation may not always be feasible until implementation is complete.

A Particular Risk Analysis evaluates risks defined as those events or influences which are outside the system(s) and item(s) concerned, but which may violate failure independence claims. Some particular risks require analysis because of airworthiness regulations, while others arise from known external threats to the aircraft or systems. These particular risks may also influence several zones at the same time, whereas zonal safety analysis is restricted to each specific zone. Details for performing a Particular Risks Assessment are found in ARP4761, Appendix J.

A Common Mode Analysis is performed to verify that failure events identified in the ASA/SSA (FTA/DD or MA) are independent in the actual implementation. The effects of development, manufacturing, installation, maintenance and crew errors, and failures of system components that defeat the independence should be analyzed. Considerations should be given to the independence of functions and their respective monitors. Identical systems or items could be susceptible to common failures/faults that could cause failures in the multiple systems or items. The results of preliminary common mode analyses are key to the assignment of the development assurance levels. Details for performing a Common Mode Analysis are found in ARP4761, Appendix K.

A Zonal Safety Analysis should be performed on each zone of the aircraft. The objective of the analysis is to ensure that the installation meets the safety requirements with respect to basic installation, interference between systems, or maintenance errors. For details on performing a Zonal Safety Analysis are found in ARP4761, Appendix I.

5.1.5 Safety Program Plan

The Safety Program Plan should define the scope and the content of the safety activities that are applicable at the aircraft level. The concepts of a safety plan may also be applied at system level, if so desired. The following provides an overview on topics that might be covered through the Safety Program Plan:

- Identify the input requirements at the aircraft level for which safety design and analysis responsibility is being taken,
- Identify applicable safety standards,
- 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,
- Describe the safety activities and deliverables,
- Define the key project milestones for which reports are required,
- Include the principles of the management, validation of the safety requirements and the verification that the design meets those requirements,
- Identify the links with the other appropriate plans (e.g. certification plan, validation and verification plan, process assurance plan).

Appendix B herein provides example contents for the Safety Program Plan.

5.1.6 Safety-Related Flight Operations or Maintenance Tasks

The functions allocated to aircraft operations and maintenance personnel result in tasks and procedures that may have an associated safety requirement. Safety-effects of identified failure conditions may be resolved through assignment of specific tasks or identification of specific limitations to these personnel. Where safety-related tasks or limitations form part of the certification substantiation, they should be identified and recorded in the certification data (see 5.8.4). For certification maintenance requirements, see AC/AMC 25.19.

5.1.7 Relationship with In-Service Safety

A process for accomplishing in-service safety assessment is described in ARP5150 “Safety Assessment of Transport Airplanes in Commercial Service” and ARP5151 “Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service”. These documents contain an in-depth study of the processes used to establish and maintain surveillance of safety concerns on in-service airplanes and to resolve those issues and document the resolutions.

Taken as a whole, ARP4761 and ARP5150 (or ARP5151) 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 and the aircraft safety assessment. 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 Ongoing Safety Assessment Process includes three objectives:

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.

A Failure Condition can be caused by one or more Failures or Errors.

The mitigation of Failures is performed by setting safety qualitative and/or quantitative requirements, including the fail-safe design concept of AC/AMC 25.1309 which influence the system architectures. These aspects are described in section 5.1 of this document (Safety Assessment).

Errors are mitigated by implementation of a Development Assurance Process. The Development Assurance Process 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. The Development Assurance Level is the measure of 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 inter-related 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 level of Development Assurance necessary to mitigate the Failure Condition.

5.2.1 General Principles – Introduction to Development Assurance Level Assignment

The general principles for Development Assurance Level assignment taking into account Aircraft Level Failure Conditions severity classification are described in the following paragraphs.

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

- If a Catastrophic Failure Condition (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 Failure Condition could result from a combination of possible development errors between two or more independently developed 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 independently developed aircraft/system functions or items are assigned no lower than Development Assurance Level C. The Development Assurance process establishing that the two or more independently developed 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/Severe Major Failure Condition 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 Failure/Severe Major Condition could result from a combination of possible development errors between two or more independently developed 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 independently developed aircraft/system functions or items are assigned no lower than Development Assurance Level D. The Development Assurance process establishing that the two or more independently developed 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 Failure Condition could result from a possible development error in an aircraft/system function or item, then the associated development assurance process is assigned a level C.

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

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 requirement set. 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 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. The objectives to be met, dependent on the IDAL are given in the DO-254/ED-80 for electronic hardware and DO-178B/ED-12B 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 may not coincide with the boundaries between aircraft manufacturers and suppliers, or between suppliers and sub-tier suppliers or with physical packaging.

5.2.3 Detailed FDAL and IDAL Assignment Guidelines

The safety assessment techniques (e.g. Aircraft FHA, PASA, System FHA, PSSA, CMA) of ARP4761 can be used to identify Failure Conditions in a systematic manner early in system development. The relationships among functions, related Failure Condition Classifications, systems and item requirements, and the corresponding assignment of Development Assurance Levels is summarized in Figure 8. Proposed allocations of Aircraft Functions are evaluated for potential Failure Conditions using the aircraft FHA technique, to validate aircraft-level architectures and derive safety requirements for the various systems contributing to those aircraft level Functions. Particular Risk Analyses and Zonal Safety Analysis are not used to assign Development Assurance Level.

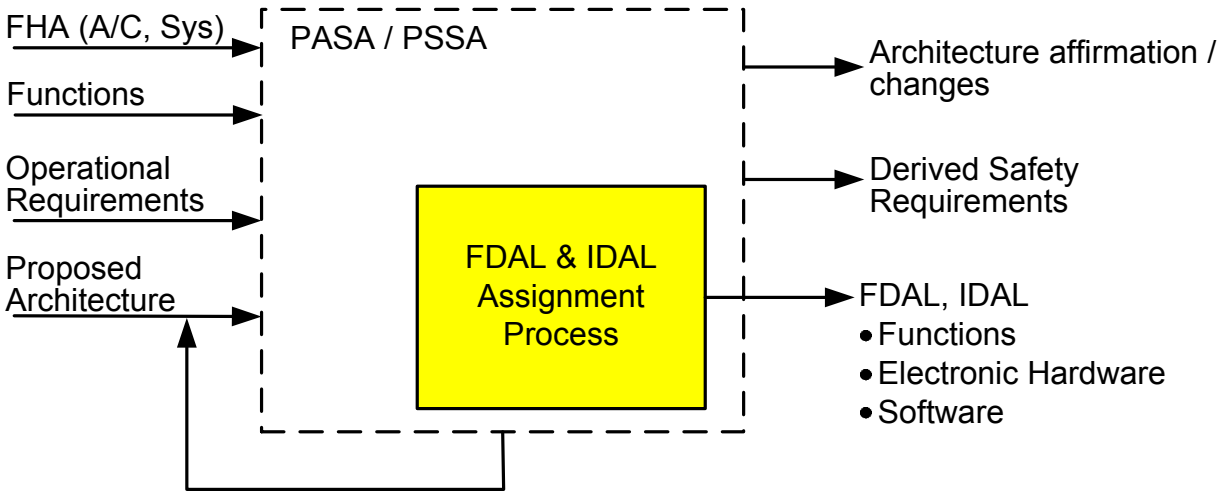

FIGURE 8 - FDAL/IDAL ASSIGNMENT PROCESS

Development Assurance Levels are assigned to aircraft/system functions and items so that the appropriate validation and verification processes are invoked to minimize 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 demonstrate compliance with the safety requirements. It should be understood that 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.

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 ARP.

TABLE 2 - TOP-LEVEL FUNCTION FDAL ASSIGNMENT

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

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 ensure 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 succeeding paragraphs.

The prerequisites for a good understanding of FDAL (and IDAL) assignment are the definitions of Functional Failure Set, Members and Independence.

A systematic approach to assigning Development Assurance Levels, when considering system architectures, is to use the concept of Functional Failure Sets (FFS). System Safety Assessment techniques are used to identify all the Functional Failure Sets (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 assessment techniques, such as Fault Tree Analysis (ref: ARP4761 Appendix D) or Dependence Diagrams (ref: ARP4761 Appendix E).

Conceptually, for FDAL (and subsequently IDAL) assignment purposes, a FFS is equivalent to a Fault Tree minimal cut set (as defined in ARP4761), whose members represent the result of potential development errors rather than failures. The FFS is used to identify combinations of members which may lead to each Failure Condition and assign the appropriate rigor to mitigate the potential 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 mode 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 mode Error is minimized between two or more members commensurate with the severity of the Failure Condition Classification.

For the purposes of assigning FDAL and IDAL, two types of independence attributes, Functional Independence and item Development Independence are considered.

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 requirement 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 mitigate 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 (GPS and Inertial Reference System),
- Provide AOA (vane and synthetic AOA 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.

Functional Independence is substantiated when the common sources of Error between multiple requirement sets have been minimized at a level of rigor commensurate with the Top-Level Failure Condition severity classification. If the presence of common Error sources in the requirements is indeterminate, then Functional Independence cannot be claimed. 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 mode 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 (VHDL coders, layout tools, etc.),
- Software development tool errors (compiler, linker, etc.),.

Examples of means to achieve Item Development Independence:

- Different technology such as use of hydraulic vs. electrical power,
- Different operating systems,
- Different computer/software languages,
- Different microprocessors,
- Different teams and processes,

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 flowed to those items from the system as needed. If the presence of common Error sources between the items is indeterminate or cannot be substantiated, then Item Development Independence cannot be claimed.

5.2.3.2.1.3 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 the development of items on which the Function(s) is(are) implemented, should not suffer from a common mode Error.

5.2.3.2.2 FDAL and IDAL Assignment Process

FDAL and IDAL assurance level 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. 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 and specific cases of Section 5.2.3.3 and 5.2.4.

Once an FDAL is assigned to the top-level aircraft function based on the top-level Failure Condition severity classification, the architecture of the system functions involved in the top-level Failure Condition are 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. System safety assessment techniques are used to identify the members within the Functional Failure Sets (FFSs) that lead to the top-level Failure Conditions. The identification of the FFS is the subject of PSSA and CMA where the independence attributes are considered. 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.

Table 3 provides the guideline for assigning FDAL to member(s) within a FFS relative to the severity classification of a given top-level Failure Condition. An example process of entering and navigating through Table 3 is presented in Appendix C. 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 option 1 or option 2 is at the discretion of the certification applicant based on what option is considered most appropriate to mitigate the identified Failure Conditions. Multiple entries into Table 3 are expected during the iterative design process; however, each entry should link to the top aircraft level Failure Condition (i.e. the same row in Table 3).

The IDAL assignment always follows the FDAL process. When the system architectures are refined down to the item level, the FDAL is assigned to a FFS member using Table 3. Care should be made to enter Table 3 at the same row that was entered at the top-level Failure Condition. The assignment becomes the IDAL of the related item. This IDAL will be used as an input for the application of DO-178B/ED-12B (software development assurance) or DO-254/ED-80 (electronic hardware design assurance).

For IDAL assignment the applicant may use option 1 or option 2 of the row related to the top-level Failure Condition classification (i.e. same row as FDAL assignment), 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 Section 5.2.3.3.

TABLE 3 - DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT TO MEMBERS OF A FUNCTIONAL FAILURE SET

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL (NOTES 2 & 4)		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1 (NOTE 3)	**OPTION 2**
Column 1	Column 2	Column 3	Column 4
Catastrophic	FDAL A (NOTE 1)	FDAL A for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Members).	FDAL B for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).
Major	FDAL C	FDAL C for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	FDAL D for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.
Minor	FDAL D	FDAL D for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	
No Safety Effect	FDAL E	FDAL E	

NOTE 1: When a FFS has a single Member and the mitigation strategy for systematic errors is to be FDAL A alone, 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 ensure that potential development error(s) having a catastrophic effect have been removed or mitigated.

NOTE 2: It is necessary to stay in the same row no matter the number of functional decompositions performed (e.g. for a Catastrophic Failure Condition any degree of decomposition from a top FDAL A FFS should include at least one FDAL A or two FDAL B Members).

NOTE 3: If there is a large disparity on the numerical availability of the Members in the Functional Failure Set, the higher level FDAL should generally be assigned to the higher availability Member.

NOTE 4: Some classes of 14CFR Part 23 /CS-23 aircraft have FDALs lower than shown in Table 3. See the current FAA AC23.1309 and equivalent EASA policy for specific guidance.

5.2.3.2.3 FDAL and IDAL Assignment cases

5.2.3.2.3.1 Case 1: Neither Functional nor Item Development Independence

If there is no Functional Independence and no Item Development Independence, column 2 of Table 3 is used to assign the FDAL and IDAL. The FDAL and IDAL are the same and are equal to the top-level function FDAL.

5.2.3.2.3.2 Case 2: Functional Independence and Item Development Independence

If both Functional and Item Development Independence are present, first assign the FDAL using Table 3 and then assign the IDAL using Table 3 (by substituting IDAL to FDAL). Option 1 or option 2 of the row related to the top-level Failure Condition classification (i.e. same row as FDAL assignment) can be used for the IDAL assignment. Review of the FFSs representing combinations of errors in both aircraft/system functions and items should be performed to ensure FDAL and IDAL assignments are compliant with the general principles of section 5.2.1. The purpose of reviewing these is to ensure that all possible combinations of errors in the Development of aircraft/system functions and items are adequately mitigated by FDAL and IDAL assignment in accordance with the general principles. The example shown in Figure 9 and Table 4 illustrates two invalid IDAL assignments given an FDAL assignment for F_1 and F_2 of B for a catastrophic failure condition, FC2. At the end of the assignment process if there is an IDAL required assignment higher than the corresponding FDAL the applicant should justify that the FDAL does not have to be reassigned at the IDAL level. (Figure 9 and Table 4 include all possible error combinations to illustrate the points of Case 2 and the general principles of section 5.2.1 and is not intended to illustrate presentation methodologies.)

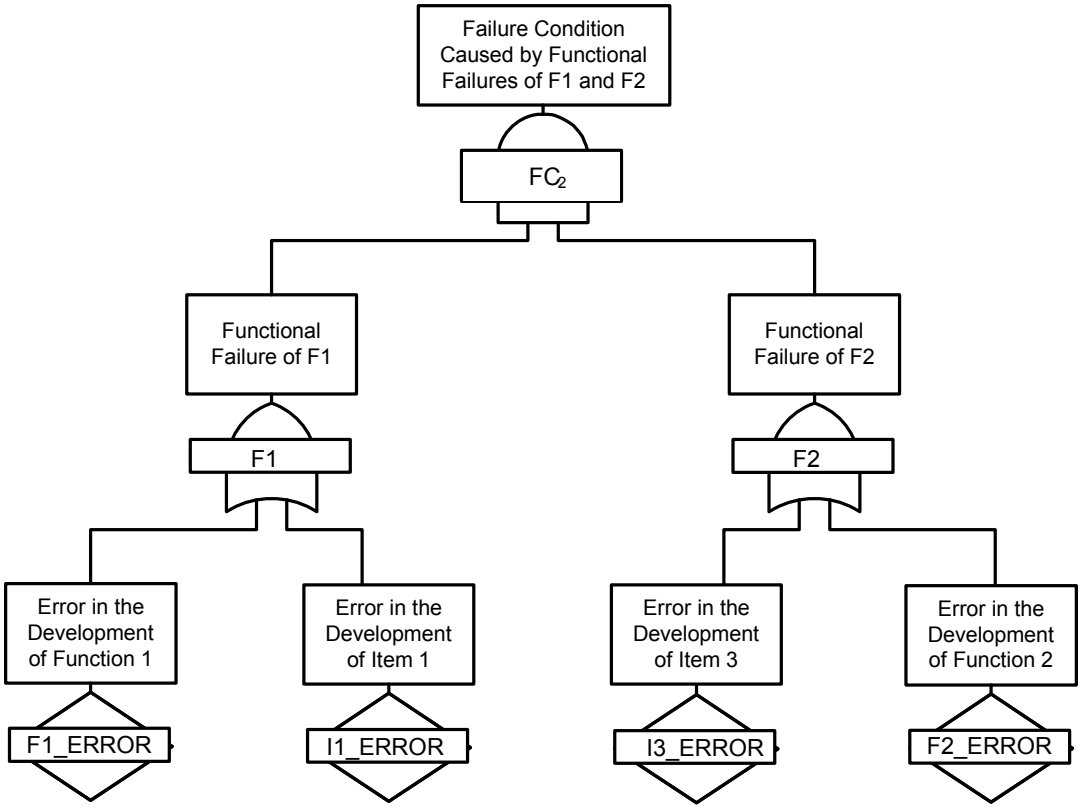

FIGURE 9 - FUNCTION INDEPENDENCE AND ITEM DEVELOPMENT INDEPENDENCE

The minimal equation or terms identifying the FFSs for the FC2 Failure condition is:

- F1 Error and F2 Error, or
- F1 Error and I3 Error, or
- I1 Error and F2 Error, or
- I1 Error and I3 Error.

TABLE 4 - EXAMPLE ASSURANCE ASSIGNMENT FOR DESIGN DEPENDENCY OF MULTIPLE FUNCTIONS SAME FC

FDAL Assignment		IDAL Assignment		Comment
F1	F2	I1	I3	
B	B	B	B	Acceptable
		A	C	Unacceptable: F1 level B & I3 level C not allowed; also I3 does not support F2 level B assignment
		C	A	Unacceptable: F2 level B & I1 level C not allowed; also I1 does not support F1 level B assignment
A	C	A	C	Acceptable
		C	A	Unacceptable: F2 level C & I1 level C not allowed; also I1 does not support F1 level A assignment
		B	B	Unacceptable: F2 level C & I1 level B not allowed; also I1 level B does not support F1 assignment
C	A	A	C	Unacceptable: F1 level C & I3 level C not allowed; also I3 does not support F2 level A assignment
		C	A	Acceptable
		B	B	Unacceptable: F1 level C & I3 Level B not allowed; also I3 level B does not support F2 assignment

Note: Some of the FFSs in Table 4 represent combinations of errors in both aircraft/system functions and items

5.2.3.2.3.3 Case 3: Functional Independence is claimed but not Item Development Independence

If independent Functions are implemented using non-independent items (or portions of the items that are not independent), and if an error in the development of the non independent items can lead to a common mode error between some or all of the Functions, then the IDAL of the “common” non independent items needs to be assigned the level of the highest FDAL. The fault tree in Figure 10 illustrates this condition with item I_2 affecting F_1 and F_2 which leads to the Catastrophic top-level Failure Condition with a FDAL A. In other words, if the common mode error can lead directly to a top-level Failure Condition, the IDAL of the common items is the FDAL of the top-level Function assigned based on the top-level Failure Condition Classification. In the Catastrophic case presented in Figure 10, a single member FFS is made up of item I_2 and thus an IDAL A is assigned.

The Functions implemented in the common design should be partitioned in order to confirm the Functional Independence claimed for FDAL assignment and to avoid an error in the development process of one Function affecting the other Functions through the common design. The Development Assurance Level of the partitioning Function should be assigned the FDAL commensurate with the most severe effect of an error in its development; this would be no lower than the highest FDAL of the implemented Functions. In the Catastrophic Failure Condition example case provided, the independence requirements defined for F_1 and F_2 would be an example of a subset of requirements of F_1 and F_2 having to be developed at FDAL A to ensure the functional independence claims of F_1 and F_2 are maintained.

If partitioning is not used or if its independence cannot be substantiated, the IDAL of the common design might force a reassignment of the FDAL of the Functions implemented in that design at the level of IDAL of the common design. This is typically the case when the implementation layer of a Function, or part of a Function, cannot be protected by the partitioning mechanism (e.g. Implementation of real time sequencing Functions in operating system layer or in micro-program layer). In that case the FDAL of the Functions that cannot be protected by the partition mechanism will either need to be reassigned at the IDAL of the common item or the upper-level Functions may be reallocated to the items to separate the independent and common portions of the design.

IDAL assignments that reflect the FDAL assignment of independent aircraft/system functions will need to substantiate that their development have minimized the sources of common development errors across the Functional Independence boundary. For example, if two functions (F_1 and F_2 in Figure 10) performing a FDAL A Function are performing Functions established as independent from one another and assigned a FDAL B (Option 2 in Table 3), the functional requirements are required to be developed to an FDAL B and it will be necessary to substantiate Functional Development Independence for these two functions. Further, the interactions between the pair of FDAL B Functions and interactions between their IDAL B items (Item I_1 & Item I_3 in Figure 10) need to be captured and validated at FDAL A under the aircraft Function even though these independent aircraft/system functions and items are individually level B.

If the items implementing the Functionally Independent FDAL B Functions have any common items that would prevent a claim for Item Development Independence, an IDAL A assignment would be necessary for at least the common portion as shown as Item I_2 in Figure 10. The item boundaries may be shaped iteratively along interfaces that can be used to substantiate the independence, but any common portion that remains would need to be assigned IDAL A. As in the case noted above of completely independent IDAL B items, the interactions between the pair of FDAL B Functions and interactions between their IDAL B items and their common IDAL A item need to be validated at FDAL A under the complete aircraft level Function even though some portions of this aircraft level Function are individually level B.

Review the FFSs representing combinations of errors in both aircraft/system functions and items to ensure FDAL and IDAL assignments are compliant with the general principles of section 5.2.1. The purpose of reviewing these is to ensure that all possible combinations of errors in the Development of aircraft/system functions and items are adequately mitigated by FDAL and IDAL assignment in accordance with the general principles. The example shown in Figure 10 and Table 5 illustrates two invalid IDAL assignments given an FDAL assignment for F_1 and F_2 of B. (Figure 10 and Table 5 include all possible error combinations to illustrate the points of Case 3 and the general principles of section 5.2.1 and is not intended to illustrate presentation methodologies.

Independent Functions using common resources based on the same designs (e.g. computers, networks, interfaces, and IMA) are likely to require careful consideration so these are discussed in ARP4761.

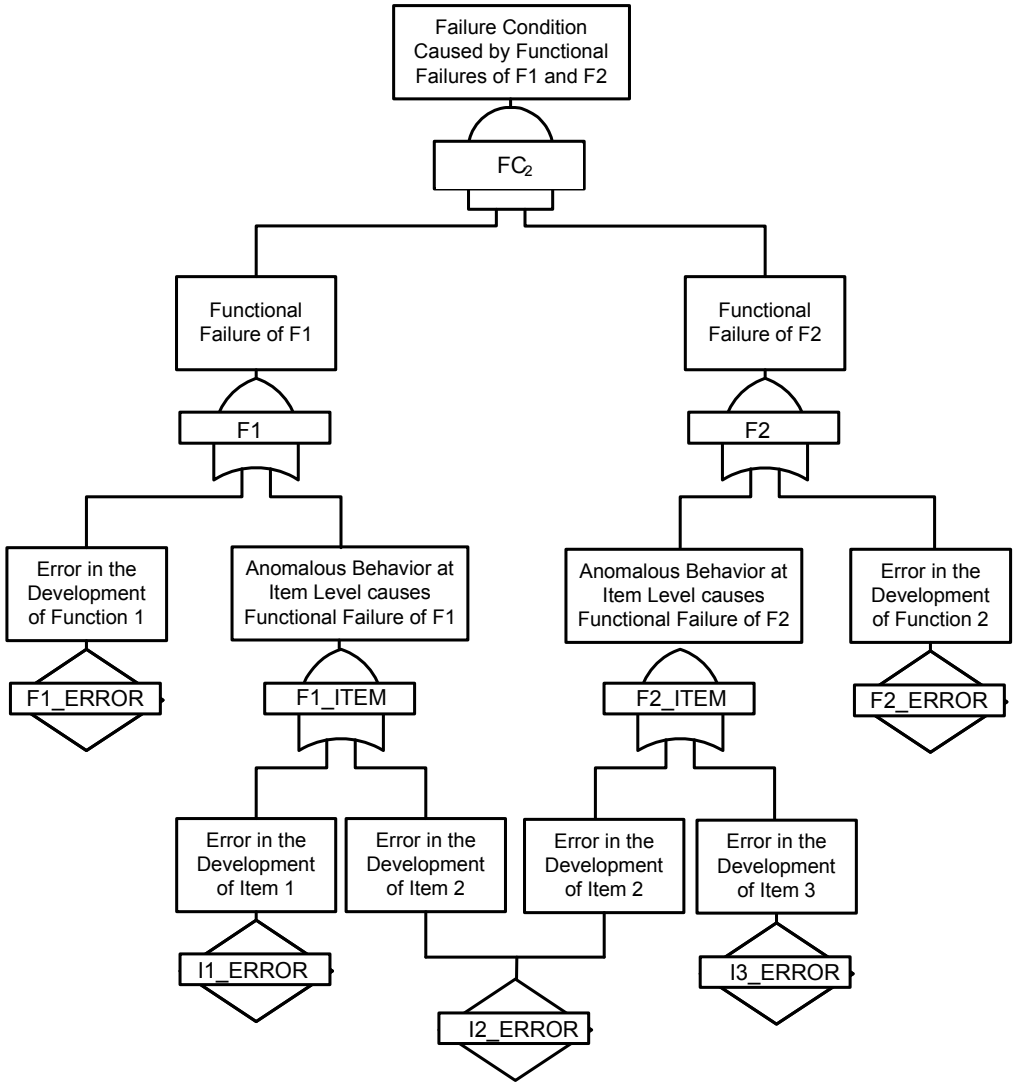

FIGURE 10 - DEVELOPMENT DEPENDENCY OF MULTIPLE FUNCTIONS IN THE SAME FC

The minimal equation or terms identifying the FFSs for the FC2 Failure condition is:

- F1 Error and F2 Error, or
- F1 Error and I3 Error, or
- I1 Error and F2 Error, or
- I1 Error and I3 Error, or
- I2 Error.

TABLE 5 - EXAMPLE ASSURANCE ASSIGNMENT FOR DESIGN DEPENDENCY OF MULTIPLE FUNCTIONS SAME FC

FDAL Assignment		IDAL Assignment			Comment
F1	F2	I1	I2	I3	
B	B	B	A	B	Acceptable
		B	B	B	Unacceptable: the common item I2 Level B does not support the top level failure condition.
		A	A	C	Unacceptable: See Case 2 (Table 4)
		C	A	A	Unacceptable: See Case 2 (Table 4)
A	C	A	A	C	Acceptable
		A	C	C	Unacceptable: the common item I2 level C does not support the top level failure condition.
		C	A	A	Unacceptable: See Case 2 (Table 4)
		B	A	B	Unacceptable: See Case 2 (Table 4)
C	A	A	A	C	Unacceptable: See Case 2 (Table 4)
		C	C	A	Unacceptable: the common item I2 level C does not support the top level failure condition.
		C	A	A	Acceptable
		B	A	B	Unacceptable: See Case 2 (Table 4)

Note: Additional cases could be evaluated but are not shown; the common item I2 has to be Level A to support the top level hazard.

5.2.3.2.3.4 Case 4: No functional independence but Item development independence

The top-level function is created in one system function which is decomposed into multiple items that are independent from one another. The system function FDAL is assigned the top function FDAL as per Table 2. The item IDALs are assigned using either option 1 or option 2 in the row corresponding to the Top-Level Failure Condition Classification in Table 3.

Note: Each independent item's failure alone should not lead to the top failure condition.

5.2.3.3 IDAL Assignment Additional Considerations

When applying the IDAL process to a given aircraft/system architecture, the architecture should be reviewed in the context of the following Cases:

- Components that can be fully assured by a combination of testing and analysis, relative to their requirements and identified Failure Conditions may be considered to provide a level of confidence equivalent to IDAL A, provided the design has been validated and verified. This can be useful when considering their role in relation to other Items or functions in a system to assign the FDALs and IDALs for the functions and items within that system. Examples include mechanical components, electro-mechanical devices, electro valves, or servo valves.

- Independent Functions together addressing a Catastrophic or Hazardous Failure Condition and using common resources based on the same COTS designs (e.g. computers, networks, interfaces) may require additional consideration (e.g configuration control, software testing on target processors). A traditional case of Functional and Item Development Independence is whereby independent functions are implemented in designs that are independent from one another.

5.2.4 FDAL Assignment Taking Credit for External Events

For systems that provide protection against an external event to the aircraft design, (e.g. cargo fire), the following guidelines may be applied in cases where no existing guidance material prescribing the associated FDAL exist. In addition to Failure Conditions related to erroneous operation or activation of the protection Function, there are at least two failure conditions to consider:

- Loss of protection combined with the external event: The FHA (per sec 5.1.1) needs to consider the classification. The FDAL of the protection Function protecting against the external event can be assigned based on Figure 11. If the loss of a protection Function combined with the external event is Catastrophic or Hazardous/Severe Major, the FDAL for the protection Function alone should be at least Level C.

- Loss of protection alone: The FHA (per sec 5.1.1) should consider the classification to reflect the reduction of safety margins (none, slight, significant or large) and impact on crew workload.

Table 3 does not apply when there is only a single function to protect against an external event. If the Function is implemented with multiple items then remain in the Table 3 row corresponding to Failure Condition of the loss of protection combined with the external event.

When the loss of protection alone has no effect on the aircraft or crew capability to safely complete the mission (often it is a latent failure), the level of reduction in safety margin can be evaluated considering the expected probability of the external event under protection: the more frequent the external event is, the higher the reduction in safety margin when the protection is lost. Figure 11 illustrates the relationship between these different attributes and provides guidelines on FDAL allocation when considering the loss of a protection Function (availability failure).

Some flight phases occur only occasionally, and these phases may arise in the FHA only when needed to differentiate flight conditions. The circumstances or frequency of any applicable conditional flight phase may be considered as a mitigating factor when determining the FDAL provided that the conditional flight phase is itself independent of the Function, or system whose FDAL is being assigned. Abnormal flight conditions like an impending stall (flying beyond stick shaker), overspeed, or an emergency descent may affect the FDAL assignment and would also be reflected in the associated Failure Conditions in the FHA. Operations and operational flight phases that are intentionally performed (e.g. autoland or ETOPS segments) would not be able to include this consideration in its FDAL justification. In this case, the applicant should substantiate to the Certification Authorities that the applicant’s proposed development assurance process meets an acceptable level of safety.

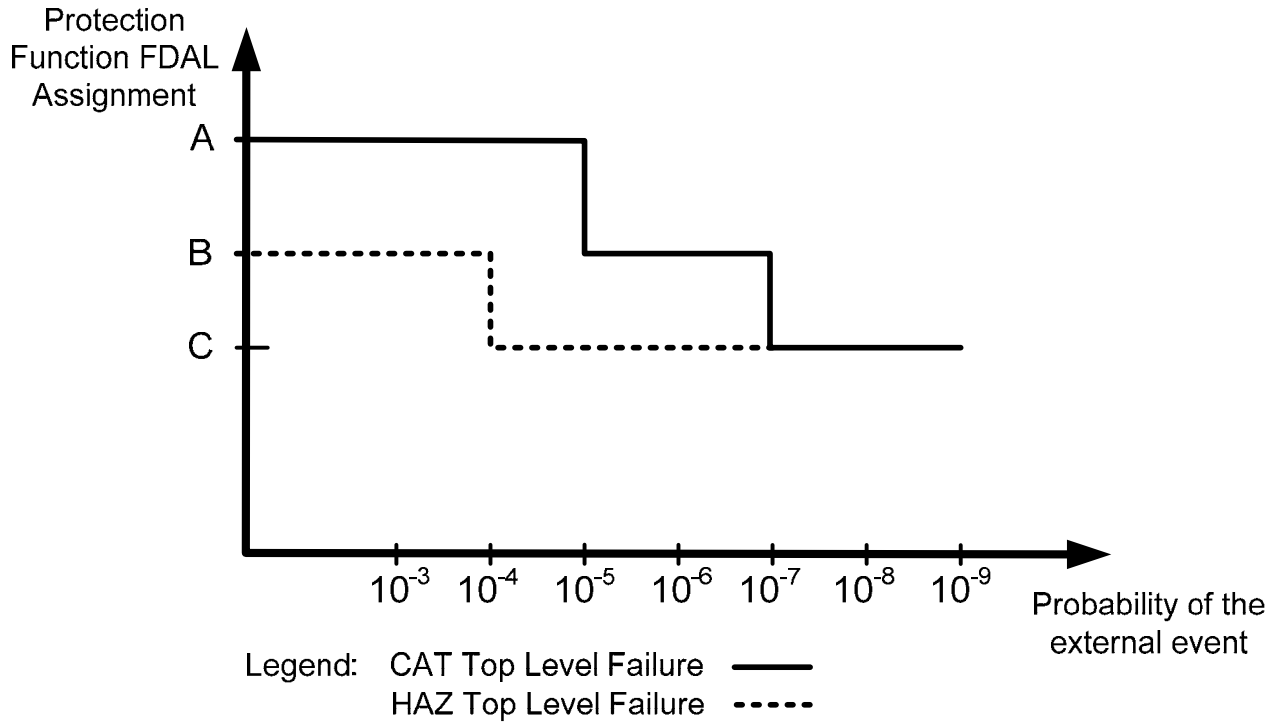

FIGURE 11 - PROTECTION FUNCTION FDAL ASSIGNMENT AS A FUNCTION OF PROBABILITY OF AN EXTERNAL EVENT

5.3 Requirements Capture

Requirements, together with related hazards, provide the common basis for the integral processes. Because the hazards may have different levels of importance, the allocation of requirements, through system architecture, has significant impact on the ease of substantiating certification.

The top level process in the aircraft development cycle includes the identification of aircraft functions and the requirements associated with these functions. The aircraft functions, including functional interfaces and corresponding safety requirements, form the basis for establishing the system architecture. Selection of the architecture establishes additional requirements necessary to implement that architecture. At each phase of the requirements identification and allocation process (i.e., system and item) both additional detail for existing requirements and new derived requirements are identified. Choices made and problems encountered during implementation are a primary source for derived requirements and may lead to identification of new system safety requirements. Detailed design activities will invariably introduce new requirements or modify existing requirements.

Requirements may be captured in different formats, textual or graphical being the most common. Irrespective of the format, requirement development plans and standards should be developed to establish consistency across the requirement set and ensure communication across the development team of requirement capture expectations. This is particularly important when using graphical or model requirement capture formats.

When graphical requirement capture is planned, the following topics should also be included:

- 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 graphical 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.

Models used to capture requirements and then directly used to produce embedded code (Software or HDL) come within the scope of DO-178B/ED-12B and DO-254/ED-80, from the time that certification credit is to be taken until the software or hardware is returned to the system processes for system verification.

5.3.1 Types of Requirements

The requirements associated with a given function define the way the function acts in its environment and include the definition of the user/machine interface. The types of requirements detailed below should be considered at various phases of the development activities (i.e., aircraft, system and item). There may be requirements that address strictly business or economic issues and do not impact safety or certification requirements.

5.3.1.1 Safety Requirements

The safety requirements for aircraft and system-level functions include minimum performance constraints for both availability and integrity of the function. These safety requirements should be determined by conducting a safety assessment consistent with the processes in section 5.1.

Safety requirements for aircraft and system functions are determined by identifying and classifying associated functional Failure Conditions. All functions have associated failure modes and associated aircraft effects, even if the classification is “No safety effect.” Safety related functional failure modes may have either contributory or direct effects upon aircraft safety.

Requirements that are defined to prevent failure conditions or to provide safety related functions should be uniquely identified and traceable through the levels of development. This will ensure visibility of the safety requirements at the software and electronic hardware design level.

5.3.1.2 Functional Requirements

Functional requirements are those necessary to obtain the desired performance 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.

5.3.1.2.1 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, operating practices, maintenance concepts, and desired features.

5.3.1.2.2 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.

5.3.1.2.3 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.

5.3.1.2.4 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.

5.3.1.2.5 Maintainability Requirements

Maintainability requirements include scheduled and unscheduled maintenance requirements and any links to specific safety-related functions. Factors such as the percent of failure detection or the percent of fault isolation may also be important. Provisions for external test equipment signals and connections should be defined in these requirements.

5.3.1.2.6 Interface Requirements

Interface requirements include the physical system 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.

5.3.1.3 Additional Certification Requirements

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

5.3.1.4 Derived Requirements

At each phase of the development activity, decisions are made as to how particular requirements or groups of requirements are to be met. The consequences of these design choices become requirements for the next phase of the development. Since these requirements result from the design process itself, they may not be uniquely related to a higher-level requirement and are referred to as derived requirements.

Derived requirements should be examined to determine which aircraft-level function (or functions) they support so that the appropriate Failure Condition classification can be assigned and the requirement validated. While derived requirements will not impact the higher-level requirements, some may have implications at higher levels. Derived requirements should be reviewed from a safety perspective (i.e. impact to safety analyses) at progressively higher system levels until it is determined that no further impact is propagated.

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 resulting from the fault or failure of 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 guidance of DO-178B/ED-12B 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.

5.3.1.5 Re-use of Existing Certificated Systems and Items

Systems and items which have been used on other aircraft are often reused in new or derivative aircraft. The maturity of these systems 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 or item, the requirements to which the system or item was certificated should be validated according to the new application, and modified as necessary. Any derived requirements, assumptions, 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 things like different cable loading or bus termination conventions.

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

5.3.2 Deriving Safety-related Requirements from the Safety Analyses

The types of safety-related requirements for each function, whether at the aircraft, system or item level, 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 derived using the results of the safety assessments. These safety requirements are usually 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, however, and these need to be selected in a manner that covers needed combinations without having to consider an exponentially increasing number of irrelevant combinations:

Combinations should be considered when there are common resources used for multiple functions. The relevant combinations are identified and the analyses repeated to derive requirements for the identified functional combinations. With increasingly shared resources used in aircraft architectures, this case occurs often.

Combinations should also be considered when there are sibling functions whose parent function has a more severe effect category than any one child. A typical case would occur when multiple systems working together or in complementary ways satisfy an aircraft function.

5.3.3 Capturing Maintenance Requirements for In-service Use

Once the requirements used for developing the aircraft are captured, it is prudent to ensure that the level of safety established for certification is maintained during the life of the aircraft through development of appropriate maintenance requirements. These 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 to maintain the safety protection features should be captured as ICA. Depending on their criticality, some ICAs may need a higher level of visibility and protection against inadvertent deletion or modification; in such case include them 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. Certification authorities may have a need for a constraint on undesired operating behaviors). While the format of the validation effort is left to the developer, a structured process should be defined in the validation plan (see 5.4.7.1).

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

- Identify the requirement interfaces (i.e. with the aircraft, with other systems, with items, with people, with processes),

- 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 insure along with the user of the data that it is fit for purpose,
- Extra rigor should be applied when crossing organizational or corporate boundaries. (see section 5.3.1.1 and 5.3.1.2 for guidelines)
- An independent reviewer should challenge the assumptions and interpretations of captured requirements with the requirement originator, ideally as they are being captured, in order to ensure that these requirements have the same meaning for the requirement originators and recipients.
- Non-complex items may be considered as meeting IDAL A rigor when they are fully assured by a combination of testing and analysis, however requirements for these items should be validated with the rigor corresponding to the FDAL of the function.

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 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 the safety assessment process. 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 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 functions in the system or for unintended functions to be induced in interfacing systems.

5.4.2 Validation Process Model

Requirements and assumptions should be validated at each hierarchical level of requirements definition. This includes validation of requirements at the aircraft function, system and item levels as well as validation of the FHA.

The relationship of validation to system development is shown in Figure 5. An expanded validation process model is shown in Figure 12. 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.

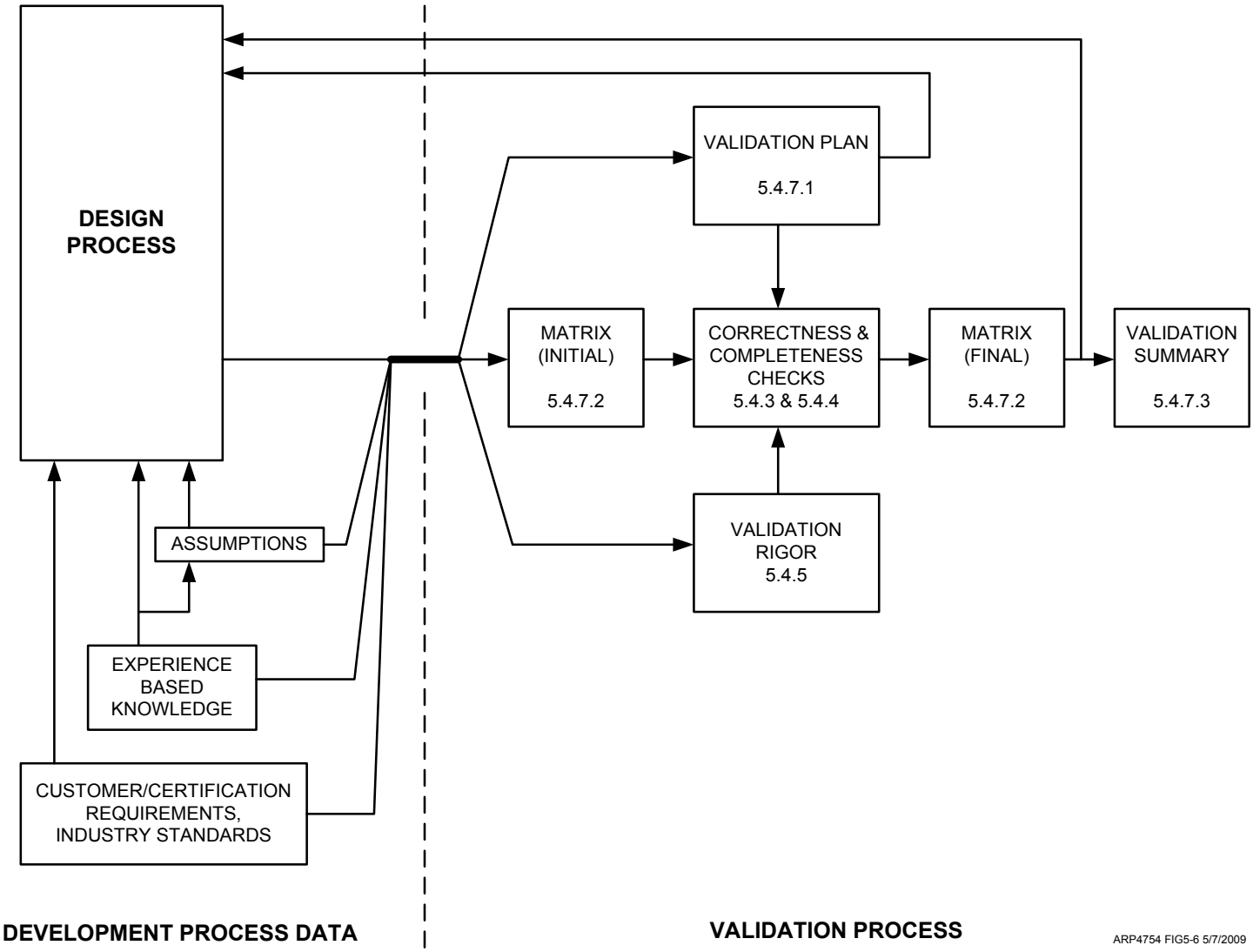

FIGURE 12 - VALIDATION PROCESS MODEL

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.

a. 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 5.4.7.1 and 5.4.6).

b. Determination of Validation Rigor:

Once the development assurance levels have been assigned and validated by the safety assessment processes, the necessary rigor of validation is then applied to the requirement (see 5.4.5).

c. Correctness and Completeness Checks:

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

Completeness is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment. (Additional information on these checks is provided in 5.4.3 and 5.4.4).

d. Management and Validation 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, 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 validation of assumptions focuses on ensuring that assumptions are:

- Explicitly stated,
- Appropriately disseminated,
- Justified by supporting data.

The processes used to validate assumptions may include: reviews, analyses, and tests. Where the consequences of an erroneous assumption appear to have significant potential to reduce safety, one possible validation strategy consists of showing how the system design, in fact, limits or bounds the achievable consequences of an assumption error.

The remainder of this section provides guidance 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 regulatory authorities may represent the interests of the air traffic control system not only in regulation but also agreeing on an assumption about the level of traffic density.

- Design assumptions associated with Crew interface, system interface and reliability should be considered. Accepting 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 member 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, 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 fault data by all related interfacing systems, fault 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 parts derating, consideration of potential failure latency and exposure periods, the completeness of the failure modes analysis, the adequacy of test data to establish or demonstrate MTBF predictions and the applicability of in-service proven parts.

- Serviceability assumptions usually assume that provisions for service and repair do not degrade safety. This assumption may be validated 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, mount integrity, grounding and shielding) should be considered. Validating 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 design process should be defined in the validation plan.

e. Validation Matrix:

The validation process includes preparation of a validation matrix (see 5.4.7.2) 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.

f. Validation Summary:

Data describing the process, as well as the results. (see 5.4.7.3).

5.4.3 Correctness Checks

During the validation process both the correctness of Failure Condition classification and 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. This list should be tailored and expanded for the specific application.

a. Is the requirement correctly stated? (e.g.)

   (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 section 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 requirements set to be complete?

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

d. Does the requirement set correctly reflect the safety analyses?

   (1) Are all derived 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 reliability, availability, and fault tolerance requirements included?

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 types 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 5.4.7.1).

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 insure 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. Are all owners of interfacing systems or processes represented in the systems requirements set?

   (1) All Higher level functions allocated to this system fully covered.

   (2) Safety requirements represented

   (3) Regulatory standards and guidance represented

   (4) Industry and company design standards represented

   (5) Flight operations and maintenance scenarios represented

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 throttles 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 functional requirements set 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 assumptions adequately defined and addressed?

5.4.4.2 User, Operator and Maintainer Involvement

One of the difficulties in achieving a complete set of requirements is 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).

a. Operation and Maintenance Scenarios

An effective means of identifying missing requirements early in the design 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 users 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 possible operating environments and operating modes but should cover anomalous operating conditions as well. Possible misbehaviors would be considered for each step in a scenario. How this misbehavior 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 4.1.2) 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 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.

b. 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. The tools used to create prototypes should minimize development time.

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 Rigor

The level of validation rigor is determined by the function development assurance level(s) for the aircraft or system (FDAL) and item development assurance level(s) for the item (IDAL). Requirement validation methods are identified in 5.4.6 and their acceptable use is described in 5.4.6.1.

The application of independence in the validation process is also dependent upon the development assurance level. This independence needs to be applied between requirements capture (5.3) and the validation activities in section 5.4. The validation plan (see 5.4.7.1) should include a description of the validation activities to which independence is applied.

The most common means of achieving 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 f) and reviews by customers, users, maintainers and certification authorities and item developers (see 5.4.4.2).

Although all validation methods may not directly lend themselves to 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 independence where indicated by the development assurance level (see Appendix A).

5.4.6 Validation Methods

Several methods may be needed to support validation. These methods include: traceability, analysis, modeling, test, similarity, and engineering review. Validation should consider both intended and unintended functions. Intended function requirements validation involves evaluation against objective pass/fail criteria. Vigilance during all analysis and testing can be used to identify unintended system/item operations or side-effects. While the absence of unintended functions can not be validated directly, ad hoc testing and targeted analyses can be used to reduce the probability of their presence.

a. Traceability (Bi-directional flow of requirements):

Traceability is an essential component of validation of the aircraft, systems and item requirements. The requirement should either be traceable to a parent requirement, or by identification of the specific design decision or data from which the requirement was derived.

Traceability by itself may be sufficient to demonstrate that a lower level requirement satisfies a higher level requirement with regards to completeness. 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 not be traceable to a parent requirement (i.e. derived requirements); these requirements should have rationale to document their validity.

Untraced requirements should be reviewed to determine whether they are:

- derived as part of the development process (see Section 5.3.1.4) or ,
- developed from a missing parent requirement that may be added or,
- assumptions that need to be managed (see Section 5.4.2 (d)).

b. Analysis:

A wide range of analysis methods and techniques may be used to determine requirements acceptability. Several specific safety-related analysis methods are described in ARP4761. Early discussion with regulatory authorities on the acceptability of the FHA and PSSAs will assist in the validation of the safety-related requirements.

c. Modeling:

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

d. Test:

Special tests, simulations, or demonstrations may be used to validate requirements. These activities may occur at anytime during development based on availability of mock-ups, prototypes, simulations or actual hardware and software. 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.

e. Similarity (Experience)

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:

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

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

f. 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.

5.4.6.1 Recommended Methods

Table 6 identifies validation methods and data as a function of the allocated development assurance level A-E. For example, to validate requirements to level A or B, analysis, tests of intended function, and directly applicable similarity may be used to establish correctness and completeness. Validation of some requirements may use one method for correctness checks and another method for completeness checks.

TABLE 6 - REQUIREMENTS VALIDATION METHODS AND DATA

Methods and Data (see 5.4.6.a-f and 5.4.7)	Development Assurance Level - A and B	Development Assurance Level - C	Development Assurance Level - D	Development Assurance Level - E
PASA/PSSA	R	R	A	N
Validation Plan	R	R	A	N
Validation Matrix	R	R	A	N
Validation Summary	R	R	A	N
Requirements Traceability (Non-Derived Requirements)	R	R	A	N
Requirements Rationale (Derived Requirements)	R	R	A	N
Analysis, Modeling, or Test	R	One recommended	A	N
Similarity (Service Experience)	A		A	N
Engineering Review	R		A	N

Note: R - Recommended for certification, A - As negotiated for certification, N - Not required for certification

For each requirement, a combination of the recommended and allowable methods necessary to establish the required confidence in the validation of that requirement, should be identified and then applied.

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 plan should include 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. How the status of validation will be maintained, or managed, when changes are made to requirements.

f. Roles and responsibilities associated with the validation.

g. A schedule of key validation activities.

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

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

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. It is recommended that a preliminary tracking process be described in the certification plan, and that it should be updated as required. The final data should be included in the validation summary. The specific format is up to the applicant, but it should at least 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, as described in 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 paragraphs that follow.

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 (Have we built the aircraft right?).

c. Ensures that the safety analysis remains valid for the system as implemented.

5.5.2 Verification Process Model

Figure 13 shows an overview of a generic process model 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 paragraph 5.5.3).

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

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

Level of verification is determined by the FDAL and IDAL (see paragraph 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.

More than one verification method may be necessary to substantiate compliance with the requirements. For example, an analysis may be required in conjunction with a physical test to assure that worst case issues have been covered.

During the process of verifying intended functions, any anomalies recognized (such as an unintended function or incorrect performance) should be reported so that they can be reviewed and dispositioned. 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 6 “Aircraft Function Implementation Process” in section 4.2).

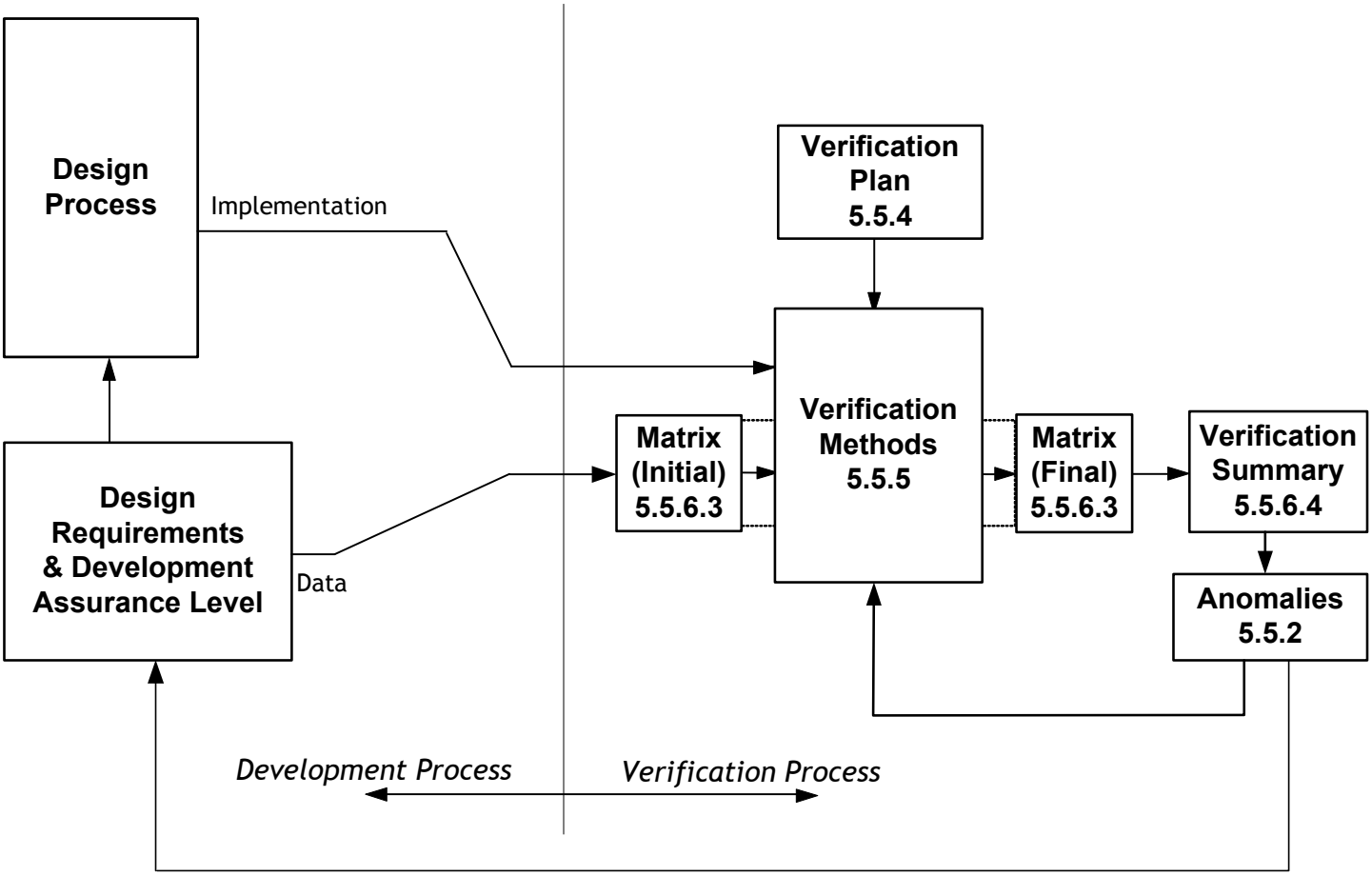

FIGURE 13 - VERIFICATION PROCESS MODEL

5.5.3 Verification Rigor

The level of verification rigor is determined by the function development assurance level(s) for the aircraft or system (FDAL) and the item development assurance level(s) for the item (IDAL). Additional verification rigor commensurate with the development assurance level, ie. independence, needs to be applied between the aircraft or system design implementation in section 4.6 and the verification activities in section 5.5. The most common means of achieving independence in verification is independent development of the verification methods described in section 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 is applied. Appendix A highlights the specific verification objectives appropriate to the development assurance level.

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 show compliance with each requirement based on 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. Identification of system verification credit taken from hardware or software verification activities,

f. Identification of key verification activities and sequence of any dependent activities,

g. Identification of verification data.

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 or Review,

b. Analysis,

c. Test or Demonstration,

d. Service Experience.

Each of these methods is discussed in the paragraphs that follow.

5.5.5.1 Inspection or Review

Inspection or 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 of compliance 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 paragraphs.

5.5.5.3 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.

5.5.5.3.1 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.

5.5.5.4 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 cases 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 perform unintended functions (i.e., not consciously part of the design) that impact safety. Ad hoc testing, and special vigilance during normal testing, may be used to identify unintended system or item operation or side-effects. It should be noted that complete absence of unintended function can never be established by test.

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 or group of tests, the following should be specified:

a. Required input variability should be considered in setting the test criteria.

b. Actions required and action order if time dependent.

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

d. The requirements covered by the test(s).

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 or failure of the testing process including its relationship to the verification program.

5.5.5.4.1 Test Facilities

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

a. The hardware and software under test are present in the facility and 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 failures to meet high level requirements are annunciated and logged.

Provision of the above 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 perform unexpected results.

5.5.5.5 Similarity / Service Experience

Verification credit may be derived from design and installation 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 demonstrate that no significant failures remain unresolved in these installations. See section 6.5 for more detail.

5.5.5.6 Recommended Verification Methods

Table 7 lists a variety of recommended and allowable verification methods and data as a function of the development assurance level. The necessary scope and coverage associated with these methods and data also depends on the development assurance level and, if known, may be further influenced by the specific related fault condition.

For example, an implementation being verified to level A or level B may involve inspection or review and analysis, and should involve some form of test. The extent to which each method needs to be applied or data developed will be the result of agreement with the certification authorities, based on the specific system to be certificated.

TABLE 7 - VERIFICATION METHODS AND DATA

Methods and Data (see paragraphs 5.5.5 and 5.5.6)	**Development Assurance Level**			
	A and B	**C**	**D**	**E**
Verification Matrix	R	R	A	N
Verification Plan	R	R	A	N
Verification Procedures	R	R	A	N
Verification Summary	R	R	A	N
ASA/SSA (note 3)	R	R	A	N
Inspection, Review, Analysis, or Test (note 1)	R (Test and one or more of others)	R (One or more)	A	N (note 2)
Test, unintended function	R	A	A	N
Service Experience	A	A	A	A

Note: R - Recommended for certification, A - As negotiated for certification, N - Not required for certification

NOTE 1: These methods provide similar degrees of verification. The selection of which methods will be most useful may depend on the specific system architecture or the specific function(s) implemented. DO-178B/ED-12B and DO-254/ED-80 define applicable tests for software and electronic hardware depending on the IDAL.

NOTE 2: As necessary to show installation and environmental compatibility.

NOTE 3: The ASA/SSA report (paragraph 5.1) is included in this table since it is directly related to the third objective of the verification process (paragraph 5.5.1).

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 in accordance with Table 7 and to support certification data requirements. 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-178B/ED-12B 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. A typical verification plan might include:

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 item (hardware or software) verification activities.

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 together with the results achieved provides the evidence necessary to establish the appropriateness of the verification effort.

5.5.6.3 Verification Matrix

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. While the specific format may be determined by the applicant, it should contain, at least:

a. Requirement,

b. Associated Function,

c. Verification Method(s) Applied,

d. Verification Procedure and results reference(s),

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 development assurance level allocated.

c. The verification matrix as described in paragraph 5.5.6.3.

d. A description of any open problem reports and an assessment of the related impact on safety.

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

f. Verification coverage summary.

5.6 Configuration Management

This section discusses the objectives and activities of the system configuration management process. It is applicable to the system, item(s) that make up the system, certain facilities and tools, and the required certification data. Figure 14 presents an overall Configuration Management Process Model.

The existence of an independent entity or organization to perform the configuration management activities should not be implied 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 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. Establishment of a configuration management plan.

b. Establishment of configuration, which includes:

(1) System and item requirements,

(2) Applicable certification data (Table 9),

(3) Facilities, tools, and any other data, where configuration is essential to establishing development assurance for requirements substantiation compliance,

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

c. 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:

Changes are recorded, approved and implemented,

Identified problems and their resolution are recorded.

d. Assurance that physical 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 time in the system development process where requirements compliance substantiation is first desired. The traceability of the final proposed configuration to that configuration baseline is a necessary element of demonstrating development assurance.

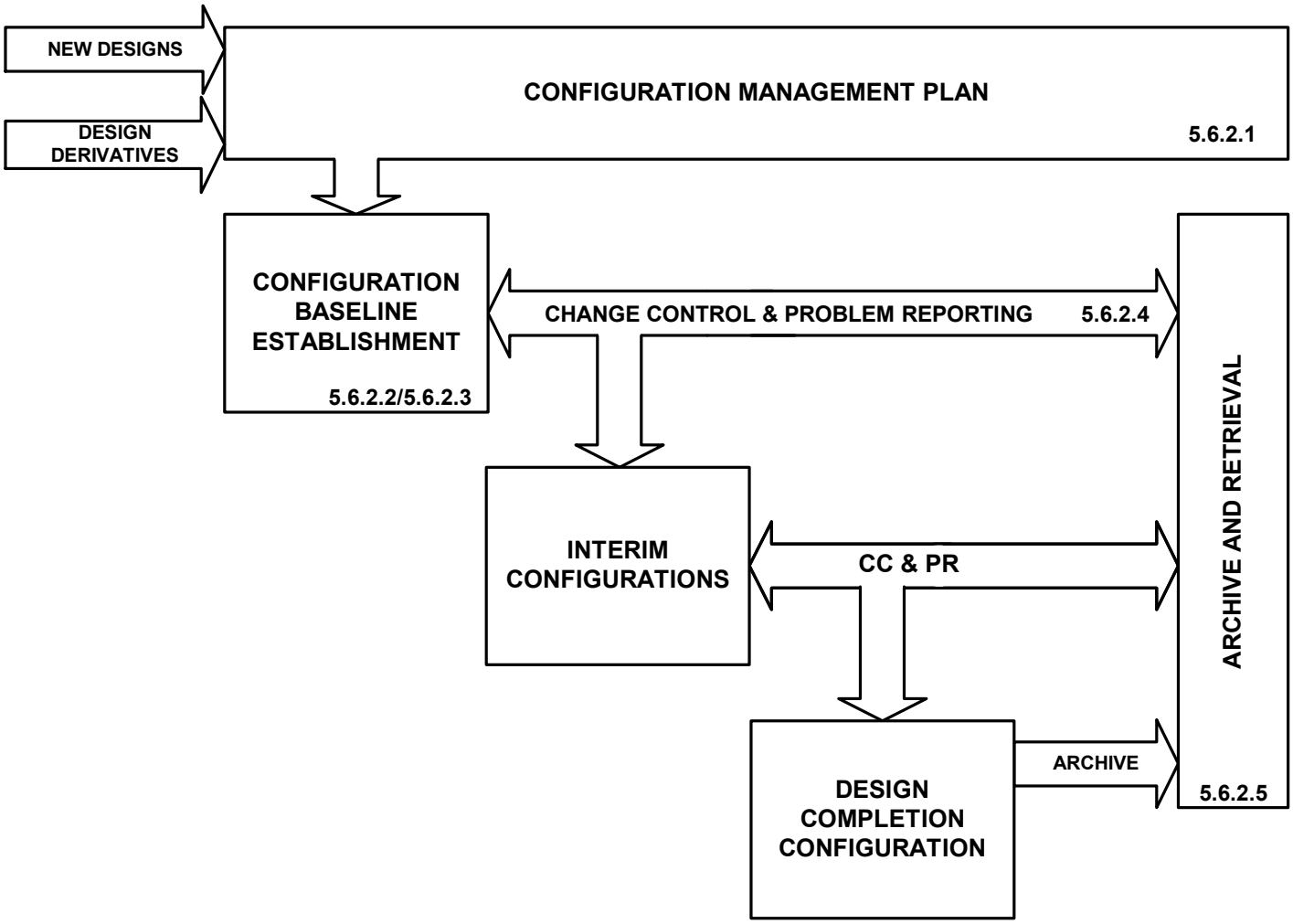

FIGURE 14 - CONFIGURATION MANAGEMENT PROCESS MODEL

5.6.2 Configuration Management Process Activities:

The configuration management process shown in Figure 14 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 (CMP) establishes the methods to be used to achieve the objectives of the configuration management process throughout the system development life cycle. The CMP should be created and agreed to by the aviation authority, when necessary. 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 section 5.6.2.2 through 5.6.2.5 should also be included.

5.6.2.2 Configuration Identification

The objective of the configuration identification activity is to unambiguously and uniquely label each Configuration Item so that a basis is established for 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

The objective of the configuration baseline establishment activity is to create and maintain control of and traceability of Configuration Items. Guidelines include:

a. A baseline should be established for Configuration Items used for requirements compliance substantiation.

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 derivative baseline from an established baseline.

d. A derivative baseline should be traceable to the previous baseline.

The design completion configuration in Figure 14 is typically that configuration used for entry into service or certification.

5.6.2.4 Change Control and Problem Reporting

The objective of change control (CC) and problem reporting (PR) is to record changes or issues identified during review, testing or service and their resolutions. The following guidelines highlight the aspects of change control and problem reporting that are significant in demonstrating development assurance:

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 preserve the integrity of a system / item by providing protection against unauthorized change.

5.6.2.5 Archive and Retrieval

The objective of the archive and retrieval activity is to ensure that the Configuration Items can be retrieved. Data retention procedures should be established to satisfy airworthiness 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 integrity of the stored data 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.

5.6.2.6 Data 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). These categories differ by virtue of the configuration management controls placed on the data. Table 8 allocates the configuration control process activities to the two data control categories. An "X" in a Table 8 SC1 or SC2 column indicates that the configuration management objectives apply to the system life cycle data for that category. SC2 activities form a sub-set of SC1 activities.

Appendix A identifies the usage of the control category mapping for system development life cycle data by system development assurance level. The configuration management objectives identified by SC1 and SC2 should be applied as identified in Appendix A for each data type.

TABLE 8 - CM ACTIVITIES TO CONTROL CATEGORY MAPPING

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	5.6.2.4a	X	
Change Control – Integrity assurance	5.6.2.4d	X	X
Change Control – Tracking	5.6.2.4b,c	X	
Configuration Index Establishment	5.8.4.2	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.

c. To establish evidence that the activities and processes adhered to the 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. Particular emphasis should be placed on the certification-related activities. The following issues should be considered when producing the Process Assurance Plan:

a. The scope and content of the other project plans (development, certification, validation, verification, and configuration management) 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, operational, and maintenance procedures are defined.

d. Sufficient project review opportunities are defined to best achieve the timely detection of development errors.

e. Sufficient coordination with the certification authorities is planned.

5.7.3 Project Plan Reviews

The following issues should be considered when assessing the project 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.

5.7.4 Evidence of Process Assurance

Evidence of conformance with the project plans can include:

a. Dated and approved project plans.

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

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

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

5.8 Certification and Regulatory Authority Coordination

The objective of the certification process is to substantiate that the aircraft and its systems comply with applicable requirements. In most situations the aircraft certification is accomplished through compliance with a series of certification plans (including references to plans for equipment qualification). Planning and coordination are vital to:

- establish effective communications between the applicant and the certification authority,

- reach agreement on the intended means of showing that the aircraft, its systems and items meet specific regulatory requirements, and industry standards.

5.8.1 Certification Planning

Certification planning separates the regulatory aspects of the overall development process into manageable tasks that can be accomplished in a logical and sequential manner. The certification plan describes the certification project, identifies the certification basis (applicable regulations and any special conditions which may apply), outlines the means by which the applicant expects to demonstrate compliance and provides a schedule for the project.

Depending on the complexity and extent of the certification project, there may be a single certification plan for the project or a top-level plan for the aircraft and a set of related plans for each of the aircraft systems. The certification plan(s) for the project is prepared by the applicant and agreed to by the certification authority. The certification plan for an aircraft or installation of a system includes the definition of the processes and requirements to be used for development assurance, and identifies the proposed means of compliance with the regulations. Since many of the development assurance activities occur well before an implementation is available, early coordination with the certification authorities is recommended. An early certification plan may be missing significant detail, necessitating subsequent updates. Even so, early coordination and approval of the plan is strongly encouraged. Early certification planning can minimize the effects of misinterpretations of internal requirements, industry standards, regulations and advisory materials.

5.8.2 Agreement on the Proposed Means of Compliance

The applicant proposes a means of compliance that defines how the development of the aircraft, system or item will satisfy the applicable certification basis. The applicant should:

a. Submit plans to the certification authority for review before relevant development activities occur. If additional substantiating data concerning the plans or means of compliance is requested, it should be submitted in time to allow meaningful review.

b. Resolve issues identified by the certification authority concerning the means by which the aircraft system will be shown to comply with airworthiness requirements.

c. Obtain agreement with the certification authority on the plans.

5.8.3 Compliance Substantiation

The certification data is the evidence that the aircraft, system or item satisfies airworthiness requirements. This includes both the data that are submitted to the certification authority and the data required to be retained. The certification authority determines the adequacy of the data for showing regulatory compliance. The applicant should develop a certification summary to describe how it was determined that the system, as installed on the aircraft, or the aircraft itself (as appropriate) complies with the agreed certification plan.

The certification summary / compliance report should provide an outline of the results of the activities established in the certification plan. Any deviation from the agreed plan should be described together with rationale to substantiate the deviation. In addition to addressing the content of the certification plan, the certification summary should include:

a. A statement of compliance to the airworthiness requirements.

b. An outline of any open problem reports that impact functionality or safety.

5.8.4 Certification Data

Possible aircraft and system certification data, as appropriate, is listed in Table 9. Table 9 includes a cross-reference to sections of this document where related information, including information about the development assurance level, can be found.

TABLE 9 - CERTIFICATION DATA CROSS REFERENCE

Certification Data	Cross Reference Description Paragraph
Certification Plan	5.8.4.1
Development Plan	5.8.4.3
Design Description	5.8.4.4
Validation Plan	5.4.7.1
Verification Plan	5.5.6.1
Configuration Management Plan	5.6.2.1
Process Assurance Plan	5.7.2
Configuration Index	5.8.4.2
Functional Hazard Assessment	5.1.1
Preliminary Aircraft / System Safety Assessment	5.1.2
Aircraft / System Safety Assessment	5.1.3
Common Cause Analysis	5.1.4
Validation Data	5.4.7
Verification Data	5.5.5
Evidence of Configuration Management	5.6.2
Evidence of Process Assurance	5.7.4
Certification Summary / Compliance Report	5.8.3

All certification data in the above table should be generated as required. The certification data to be submitted to the certification authority includes the certification plan, certification summary, and configuration index.

The certification data described in this document does not imply a requirement for specific arrangement or grouping of data or delivery format (such as paper, computer files, or remote terminal displays). Whatever form is selected by the applicant should provide for efficient retrieval and review by the certification authority as required by regulations and laws in effect governing in-service aircraft. Appendix A highlights certification data recommendations by Development Assurance Level.

5.8.4.1 Certification Plan

The certification plan for an aircraft, or installing a system or component on an aircraft should address both the system and the aircraft environment within which the system will be used. The amount of detail contained in the plan should vary depending on the classification of the associated aircraft hazard(s). Each plan should include:

a. A functional and operational description of the system and the aircraft on which the system will be installed. Hardware and software should be addressed in this description. This description should establish the functional, physical, and information relationship between the system and other aircraft systems and functions.

b. A statement of the relationship of this certification plan to any other relevant certification plan(s).

c. A summary of the functional hazard assessment (aircraft hazards, Failure Conditions, and classification).

d. A summary of the preliminary aircraft/system safety assessment (aircraft/system safety objectives and preliminary system development assurance levels).

e. A description of any novel or unique design features that are planned to be used in meeting the safety objectives.

f. A description of the new technologies or new technology applications to be implemented.

g. The system certification basis including any special conditions.

h. The proposed methods of showing compliance with the certification basis, including an outline of the anticipated development assurance processes (safety assessment, validation, verification, configuration management, and process assurance).

i. A list of the data to be submitted and the data to be retained under configuration control.

j. The approximate sequence and schedule for certification events.

k. Identification of the personnel or specific organization responsible for certification coordination.

5.8.4.2 Configuration Index

The system configuration index identifies all of the configuration items that, together, comprise the system. In addition the configuration index identifies procedures and limitations that are integral to system safety. Any system design features or capabilities provided in excess of those required to establish system safety under the applicable regulations should be identified.

A typical system configuration index will include the following information:

a. Configuration identification of each system item,

b. Associated item configuration identification (hardware/software),

c. Interconnection of items,

d. Required interfaces with other systems,

e. Safety-related operational or maintenance procedures and limitations.

When applicable, information describing permissible interchangeability or intermixability of alternate items within the system should be included.

5.8.4.3 Development Plan

The development plan should identify the top-level processes planned for use, the key events that mark the planned development cycle, and the organizational structure and key individual responsibilities supporting the development. 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. This development plan should provide sufficient detail to achieve a mutual understanding of the key elements and their relationships.

5.8.4.4 Design Description

A design description may also need to be provided to facilitate a common understanding of:

- the intended aircraft-level functionality provided or supported by the system(s),

- the anticipated system operating environment(s),

- and the specific intended capabilities of the system(s) as installed on the aircraft.

The description should also identify primary fault or failure containment means. New or novel design elements should be identified; along with specific architectural features and design elements that perform a specific role in establishing or maintaining aircraft system safety.

6. MODIFICATIONS TO AIRCRAFT OR SYSTEMS

The objective of this section is to describe how the material in this document could be applied when modifying an item, system or aircraft. 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. Thus, a modification needs to be controlled in such a way that the effects of a modification are known, fully validated and verified. A modification to an item, system or aircraft may be undertaken for a number of reasons, ranging from adding new functionality to responding to a required corrective action. The modification process should form part of an overall safety management program.

Differences exist between the U.S. and European approaches to assuring modifications to aircraft and systems. Differences are highlighted in this section where deemed necessary.

The certification basis defines the applicable requirements, regulations, special conditions, and other appropriate regulatory material. An aircraft receives its Type Certificate (TC), when an applicant has demonstrated to a certification authority that the aircraft has been designed in accordance with the requirements and regulations that were applicable to aircraft as identified within the type certification basis. The holder of the type certificate may make changes to the type design. Depending on the type certificate holder's individual aviation authority rules, this may be conducted as a TC Modification, or as an Amended Type Certificate (ATC) modification. When introducing an item, system or aircraft modification, the potential effects in the certification basis should be assessed and classified as either "minor" or "major", as defined in the relevant paragraph of 14 CFR/ IR Part 21. Approval of the modification classification should be obtained from the relevant airworthiness authority.

If the applicant for a "major" modification is not the type certificate holder, this will usually require a Supplemental Type Certificate (STC) application to be made. The TC modification / ATC / STC is issued when the applicant has demonstrated to a certification authority that the design change will ensure that the modified aircraft will continue to be in compliance with the requirements / regulations that are applicable to that aircraft.

There is also a regulatory process for authorization of equipment. This process is known as a (European) Technical Standard Order (TSO / ETSO). It allows equipment to be integrated into several aircraft types. A TSO /ETSO approval signifies a minimum performance standard for the equipment. Integration of the equipment into an aircraft system is undertaken through the appropriate TC, ATC or STC processes. If approval is sought for a change to a TSO/ETSO item it should be assessed and classified as either "minor" or "major", as indicated above. The TSO / ETSO holder can approve Minor changes (as an appropriately approved production organization, e.g. IR Part 21 Subpart G POA, with agreed "alternative" design procedures) without need for any further involvement of the authorities. However, all "major" modifications should be submitted to the relevant airworthiness authority for approval.

6.1 Modification Process Overview

The applicant proposes a method or means of compliance that defines how it will be demonstrated that the modified item, system or aircraft satisfies the certification basis. Since it is possible that the certification basis may change from the original type certification, it will be necessary to assess the proposed means of showing compliance to ensure compatibility with the agreed certification basis. Note that these methods or means of compliance for modifying aircraft do not deviate from the established item or system development process as represented in the previous sections of this document. The objectives of a modification process are to:

a. Develop a modification management process and co-ordinate it with all stakeholders,

b. Perform modifications using the approved process,

c. Conduct and document an initial modification impact analysis,

d. Determine a classification for the modification (i.e. "minor / major"),

e. ntegrate the modification into the item, system and aircraft as required,

f. Conduct and document a modification accomplishment summary / compliance substantiation,

g. Maintain configuration control of data related to the modification, see Section 5.6.

6.2 Modification Management Process

The modification management process provides a structured means to control and co-ordinate activities between stakeholders. For example, the applicant, system integrator and item developer would each need a defined modification management process that is coordinated with the modification process of other stakeholders. The process documentation should include:

a. Description (why, what, how and schedule) of the proposed modifications to items, systems or the aircraft,

b. Results of an initial modification impact analysis,

c. The proposed modification implementation strategy,

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

e. Results of verification activities on the implemented modification,

f. Results of the final modification accomplishment summary activities,

g. Updates to the aircraft configuration management data on any modified item or system, see section 5.6.

6.3 Modification Impact Analysis

When a modification is proposed to an item, system or aircraft an initial impact analysis should be performed and should include an evaluation of the impact of the modification on the original safety assessments. For instance, if an aircraft level modification is proposed, the validity of 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
  - Safety margins are reduced,
  - Architectural Assumptions,
  - Validity of the environmental qualification test results is affected,
  - V&V methods or procedures are modified.
- Operational or procedural characteristics are changed. For example:
  - Aircraft operational or airworthiness characteristics,
  - Flight crew procedures,
  - Increased pilot workload,
  - Situational awareness, warnings, cautions or advisories,
  - Displayed information to make flight decisions.

The primary result of the initial impact analysis should be the Failure Condition classification(s) and the system(s) impacted by the proposed modification. Additionally the impact analysis identifies the change classification (i.e. “major/minor” change).

The modification impact analysis should be confirmed or updated once verification activities have been completed. Results of these analyses should be reflected in:

a. The appropriate certification documentation,

b. The verification activities needed to assure that no adverse effects are introduced during the modification process,

c. The modification summary in which the impact of the implemented modifications is confirmed.

A rationale for the level of re-analysis undertaken should be provided based on factors such as the operational history and the required level of assurance of the item, system or aircraft being modified. It may be necessary to repeat a significant part of the safety assessment process as a result of a modification. In particular, if the item or system being modified was included within a Common Cause Analysis to demonstrate full independence from other items or systems, in order to substantiate a lower development assurance level assignment prior to initial certification, that CCA will require re-investigation to ensure that its conclusion remains valid.

Modification, including modification impact analysis and the design activities working towards 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 confirmatory impact analysis can be produced.

6.4 Modification Categorization and Administration

Aviation Authority requirements and regulations categorize aircraft modifications into either “minor or major” changes. These changes need to be managed via the processes identified above. However, for any modification it will be shown that:

a. The modified item, system or aircraft meets the applicable certification requirements, regulations and specifications and environmental requirements,

b. Any airworthiness provisions not complied with are compensated for by factors that provide an equivalent level of safety and,

c. No feature or characteristic makes the item, system or aircraft unsafe for the uses for which certification is requested.

6.5 Evidence for Acceptability of a Modification:

If credit is sought for development assurance activities performed on a previously qualified item or certificated system “baseline”, the proposed item or system and its certification data should be traceable to that baseline. In some cases, such evidence may not be adequate. The following paragraphs provide guidelines for:

a. Supplementing the existing certification data to support certification of modifications to existing items or systems or new installations of previously qualified items or systems,

b. Using service history obtained from an installation on one aircraft type to support the qualification of that item or system certification on a different aircraft type or a similar item or system on the same aircraft type.

To supplement existing certification data, the applicant may:

a. Evaluate the data available from the previous certification to determine which certification 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 certification objectives for the new application,

c. Use service history in accordance with the guidelines below to satisfy the certification requirements,

d. Specify the strategy for accomplishing compliance with this document in the Certification Plan.

6.5.1 Use of Service History

Service history may be used to support certification of a new / modified item or system if an analysis shows the history to be applicable and changes to the referenced item or system configuration have been appropriately controlled and documented. This method allows validation of a requirement by comparison to the requirements of similar in-service items or systems. 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:

- The applicant should propose, in the Certification Plan, how service history will be used (e.g., the amount of service experience available and a description of how the service data will be analyzed).
- The applicant should conduct an analysis to determine the extent to which the service history is applicable. Such an analysis should show that:

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

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

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

6.6 Considerations for Modifications

Modifications to existing aircraft, system or item may take various forms, including addition, deletion, or change to the functionality of an item or system. Example modifications are:

- Introducing a new aircraft-level function.
- Replacing one item or system with another on an existing aircraft.
- Adapting an existing item or system to a different aircraft type.
- Modification to Item or System without adding a function.

Since most systems implement multiple functions, it is likely that a specific modification for such a system would involve more than one of these forms. Example modifications are discussed below with regards to the process introduced in Sections 6.1 and 6.2.

6.6.1 Introducing a New Aircraft-Level Function

Considerations for addressing the introduction of a new aircraft-level function include:

- The applicant should develop the new aircraft function in accordance with the guidelines provided in this document. In the modification impact analysis emphasis should be given to the following:
  - The Functional Hazard Assessment should address the Failure Conditions and associated hazards for the new function and identify the safety objectives for the items or systems to be modified.

- The FHA should also identify the manner in which other items, systems and functions are affected by the introduction of the new aircraft function. This may be achieved by conducting analysis on functional interactions and interdependencies, and by determining the degree to which the aircraft function is integrated with other aircraft functions.

This analysis then forms the basis of the classification of the proposed modification. The modification implementation strategy should incorporate actions to substantiate the interactions with other items, systems and functions.

- If credit is sought for development assurance activities performed on a previously certificated “baseline” aircraft or system, the proposed system or item and its certification data should be traceable to that baseline.
- If certification data is not available to the applicant for unmodified areas of the aircraft on which the aircraft function is reliant, the modification impact analysis should identify the assumptions that were made about those areas to support the results of the safety assessment process. The modification implementation strategy should incorporate actions to substantiate the assumptions.
- The applicant has the option to repeat all the elements of the safety assessment process relating to the un-modified function(s) if necessary.

When a new function is introduced into an aircraft it is considered to be a configuration change to the aircraft.

6.6.2 Replacing Item or System With Another on an Existing Aircraft

Installing a replacement item or system in a previously certificated aircraft type may change the implementation of an aircraft function or functions without adding a new aircraft-level function. The replacement item or system may be installed for a number of reasons including: replacement of obsolescent equipment, improvement of reliability or integrity, equipment has enhanced or additional functionality or in compliance with a regulatory mandate. Considerations for addressing the installation of replacement item or system in previously certificated aircraft type include:

- The applicant should develop the replacement item or system in accordance with the guidelines provided in this document. In the modification impact analysis, emphasis should be given to the following:
  - The Functional Hazard Assessment (FHA) should address the Failure Conditions and associated hazards for the replacement item or system and identify the safety objectives for the items or systems to be modified.
  - The FHA should also identify the manner in which other items, systems and functions are affected by the introduction of the replacement. This may be achieved by conducting analysis on functional interactions and interdependencies, and by determining the degree to which the aircraft function(s) performed by the replacement is integrated with other aircraft functions.

This analysis then forms the basis of the classification of the proposed modification. The implementation strategy should incorporate actions to substantiate the interactions with other functions and systems.

- The modification impact analysis should consider:
  – Installation design of the replacement item or system;
  – Areas on which the replacement item or system is reliant;
  – Availability of certification data for the item or system being replaced;
  – Certification basis for the aircraft.

It may be necessary as part of the modification implementation strategy to develop safety assessment data to ensure that the safety objectives for the replacement item or system are correct and complete and to ensure that the aircraft-level safety objectives have been satisfied.

- If credit is sought for development assurance activities performed on a previously certificated “baseline” aircraft, the proposed item or system and its certification data should be traceable to that baseline.

- If the item or system being modified was included within the baseline certificated aircraft's Common Cause Analysis (CCA) to demonstrate functional and item independence from other items or systems, in order to substantiate a development assurance level reduction, that CCA will require re-investigation to ensure that its conclusion remain valid.
- If certification data is not available for unmodified areas of the aircraft on which the item or system is reliant, the modification impact analysis should identify the assumptions that were made about those areas to support the results of the safety assessment process. The modification implementation strategy should incorporate actions to substantiate the assumptions. However, if this includes areas that were subjected to the CCA, this approach will require specific analysis and review with the certificating authority to ensure that the baseline CCA conclusions remain valid.

6.6.3 Adapting Existing Item or System to a Different Aircraft Type

Items or systems previously approved for operation in one aircraft type should be re-examined for use in a different aircraft. Should the applicant choose to seek credit from the previous certification, the certification authority will require evidence that the design, installation, and application are similar. If the evidence were not available, the relevant parts of Sections 4 and 5 would be applied as necessary to provide evidence that the item or system to be installed satisfies the certification requirements/regulations. Considerations for addressing installation in a different aircraft include the following:

- The applicant should undertake a modification impact analysis considering:
  - Similarity of installation and operation on both the existing and proposed aircraft,
  - Similarity of functions on which the transferred item or system is reliant,
  - Impact of the transferred item or system on other items or systems in the proposed aircraft,
  - Similarity of existing aircraft installation Certification basis and proposed aircraft installation Certification basis,
  - Adequacy of the certification data available from the previous installation.

This analysis then forms the basis of the classification of the proposed modification. If the safety objectives are the same for the proposed installation as they were in the previous installation and provided that an appropriate level of aircraft similarity is established, no additional effort will be required.

The modification impact analysis should identify the functions associated with the original application affected by the functions associated with the new installation. The assessment should address unmodified functionality on which the new installation relies. This may be achieved by conducting analyses of the interaction and interdependencies between the new item or system and other aircraft items or systems. The modification implementation strategy should incorporate actions to substantiate the interactions with other items, systems and functions.

- If credit is sought for development assurance activities performed on a previously certificated "baseline" aircraft, the proposed item or system and its certification data should be traceable to that baseline.
- If the item or system being modified by the introduction of an adapted item or system was included within the baseline certificated aircraft's Common Cause Analysis (CCA), to demonstrate functional and item development independence from other items or systems in order to substantiate the assignment of a development assurance level lower than the top-level Failure Condition classification, that CCA will require re-investigation to ensure that its conclusion remains valid.
- If certification data is not available for unmodified functions of the aircraft on which the adapted item or system is reliant, the modification impact analysis should identify the assumptions that were made about those functions to support the results of the safety assessment process. The modification implementation strategy should incorporate actions to substantiate these assumptions. However, if this includes areas that were subjected to the CCA, this approach will require specific analysis and review with the certificating authority to ensure that the baseline CCA conclusions remain valid.

- The modification implementation strategy will need to allow the applicant to supplement the existing certification data under the following conditions in order to satisfy the certification requirements/regulations:

  a. The certification data from the previous installation is not available to substantiate that the new installation satisfies the safety objectives of the proposed installation.

  b. The certification data from the previous installation is inadequate to define and substantiate the affected area.

Any requirements impacted by the new installation should be validated and the new installation verified in accordance with the guidelines provided in sections 5.4 and 5.5.

6.6.4 Modification to Item or System Without Adding a Function:

A modification to a previously approved item or system may change the implementation of an aircraft function without adding a new aircraft-level function. A modification may result from a change in requirements or desired performance, correction of an implementation error, an enhancement to equipment reliability or replacement of obsolescent equipment. Considerations for addressing an item or system modification on a previously certificated aircraft include:

- The modification impact analysis which should consider the impact of the modification on:

  - Areas on which the item or system is reliant.

  - Certification basis for the aircraft.

  - Existing requirements / regulations (including the impact on unchanged requirements).

  - System architecture.

  - Area affected by the modification. This may be achieved by conducting an analysis of the interaction of the altered item or system with other aircraft items or systems. The modification implementation strategy should incorporate actions to substantiate the identified interactions.

This analysis then forms the basis of the classification of the proposed modification.

- If credit is sought for development assurance activities performed on a previously certificated “baseline” aircraft or system, the proposed item or system modification and its certification data should be traceable to that baseline.

- If the item or system being modified was included within the baseline certificated aircraft’s Common Cause Analysis, to demonstrate functional or item development independence from other items or systems in order to substantiate the assignment of a development assurance level lower than the top-level Failure Condition classification, that CCA will require re-investigation to ensure that its conclusion remains valid.

- If certification data is not available for unmodified areas of the aircraft on which the item or system modification is reliant, the modification impact analysis should identify the assumptions that were made about those areas to support the results of the safety assessment. The modification implementation strategy should incorporate actions to substantiate the assumptions. However, if this includes areas that were subjected to the CCA, this approach will require specific analysis and review with the certificating authority to ensure that the baseline CCA conclusions remain valid.

- The modification implementation strategy should allow the applicant to supplement the existing certification data under the following conditions:

  a. The certification data from the previous installation is not available to substantiate that the altered item or system satisfies the safety objectives of the proposed installation.

  b. The certification data from the previous development is inadequate to define and substantiate area(s) affected by the item or system alteration.

- The requirements impacted by the modification should be validated and the altered implementation verified in accordance with the guidelines provided in Sections 5.4 and 5.5.

6.6.5 STC Production Introduction

Items or systems previously qualified, certificated, and approved for operation in one aircraft, by an STC modification (see sections above) are occasionally introduced into the production process of an aircraft to provide the item or system as a part of a revised aircraft baseline. Such a process may be referred to as an in-line Type Certificate holder modification or might be incorporated into the production process as a STC. While the introduction of the modification using the TC process will need to follow the criteria defined above; where the STC approach is used, additional considerations to those already given are necessary. Topics to be considered for a STC production introduction are:

- Alignment of Projects. The STC holder, the TC holder/aircraft manufacturer and the certification authority should work closely on a coordinated basis to ensure that expectations between the various stakeholders are met.

- Alignment of Data expectations. There will need to be a coordinated effort to ensure that the data provided by the STC satisfies the certification requirements/regulations applicable to the aircraft and modification certification basis and that of the TC holder/aircraft manufacturer.

- Coordination of data transfer. Once the activity for a production introduction begins there needs to be a process that manages the data transfer between the TC holder, the STC holder, and with the certification authority. In cases where there are issues with certification data, reporting systems need to be implemented that track and resolve the data issue. Typically, this is done through coordination memos.

- Clarification of assumptions for engineering data / design reuse for unchanged remnants:

  - Evaluate the data available from the previous certification effort to determine which objectives are satisfied for the new application and which objectives require additional consideration.

  - Use reverse engineering to develop certification data necessary to satisfy the objectives of this document.

  - Use service history where applicable to satisfy the objectives of this document.

  - Specify the strategy for accomplishing compliance with this document in the Certification Plan.

- Comprehensive coordination of STC implementation to ensure confidence that the certification requirements' remain valid, including compatibility of multiple STCs.

Refer to FAA/EASA 14CFR/IR Part 21 for administrative and technical STC process requirements.

7. NOTES

7.1 The leadership of the S-18 and WG-63 Committees would like to thank the actively contributing committee members, and their sponsoring companies, for the time, effort, and expense expended during the years of development of this document. Without the experience, cooperation and dedication of these people, development of this document would not have been possible.

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

PREPARED BY SYSTEMS INTEGRATION SUBCOMMITTEE
(FAA SYSTEMS INTEGRATION REQUIREMENTS TG (SIRT)
OF COMMITTEE AS-1, AVIONICS/ARMAMENT INTEGRATION

APPENDIX A – PROCESS OBJECTIVES DATA

This appendix outlines the aircraft/system life cycle process objectives and data outputs described in this document. Table A-1 provides the details by function development assurance level, which should be assigned according to the guidelines in section 5.2. Activities of section 5.2 are not included in Table A-1, since the section 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 A-1 includes guidelines for:

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

   R*- Recommended for certification with process independence,

   R - Recommended for certification,

   A - As negotiated for certification,

   N - Not required for certification.

b. The reference to the system life cycle data objectives and content.

c. The system control category (SC) objectives assigned to the data by development assurance level (see section 5.6.2.6)

Table A-1 identifies data content rather than data format. Life cycle data may be combined in a manner consistent with the users development processes.

TABLE A-1 - PROCESS OBJECTIVES, OUTPUTS & SYSTEM CONTROL CATEGORY

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
1.0 Planning Process														
1.1	System development and integral processes activities are defined	5.8.1 5.8.4.1	R	R	R	R	R	Certification Plan	①	①	①	①	①	
		3.1 5.1.5 Appx B	R	R	R	R	N	Safety Program Plan	②	②	②	②		
		3.1 5.8.4.3	R	R	R	R	N	Development Plan	②	②	②	②		
		5.4.2a 5.4.7.1	R	R	R	A	N	Validation Plan	②	②	②	②		
		5.5.3 5.5.5.1	R	R	R	A	N	Verification Plan	②	②	②	②		
		5.6.2.1	R	R	R	R	A	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	R	R	R	A	N	Plans in objective no. 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.
* Independence is achieved when the activity is performed by a person(s) other than the developer of the system/item.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
2.0 Aircraft and System Development Process and Requirements Capture														
2.1	Aircraft-level functions, functional requirement, functional interfaces and assumptions are defined	4.1.4 4.2 5.3	R	R	R	R	N	List of Aircraft-level functions Aircraft-level Requirements	①	①	①	②		Note: Requirements capture process objectives presented in section 5.3 are included in this development process
2.2	Aircraft functions are allocated to systems	4.1.5 4.3	R	R	R	R	N	System Requirements	①	①	①	②		
2.3	System requirements, including assumptions and system interfaces are defined.	5.3	R	R	R	R	N	System Requirements	①	①	①	②		
2.4	System derived requirements (including derived safety-related requirements) are defined and rationale explained.	4.4 5.3.1.4 5.3.2	R	R	R	A	N	System Requirements	①	①	①	②		
2.5	System architecture is defined.	4.1.6 4.4 5.8.4.4	R	R	R	A	N	System Design Description	①	①	②	②		
2.6	System requirements are allocated to the items.	4.1.7 4.5 4.6 5.3	R	R	R	R	N	Item Requirements	①	①	①	②		
2.7	Appropriate item, system and aircraft integrations are performed.	4.6.3 4.6.4	R	R	R	A	N	Verification Summary	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.
* Independence is achieved when the activity is performed by a person(s) other than the developer of the system/item.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
3.0 Safety Assessment Process														
3.1	The aircraft/system functional hazard assessment is performed.	5.1.1 5.2.3 5.2.4	R*	R*	R	R	R	Aircraft FHA System FHA	①	①	①	①	①	
3.2	The preliminary aircraft safety assessment is performed.	5.1.2 5.2.3 5.2.4	R*	R*	R	A	N	PASA	①	①	①	①		
3.3	The preliminary system safety assessment is performed.	5.1.2 5.1.6 5.2.3 5.2.4	R*	R*	R	A	N	PSSA	①	①	①	②		
3.4	The common cause analyses are performed.	5.1.4	R	R	A	N	N	Particular Risk Assessment	①	①	①			
			R*	R*	A	N	N	Common Mode Analysis	①	①	①			
			R	R	A	N	N	Zonal Safety Analysis	①	①	①			
3.5	The aircraft safety assessment is performed.	5.1.3 5.1.6	R*	R*	R	A	N	ASA	①	①	①	①		
3.6	The system safety assessment is performed.	5.1.3 5.1.6	R*	R*	R	A	N	SSA	①	①	①	②		
3.7	Independence requirements in functions, systems and items are captured	5.3.2 5.2.3 5.1.2	R*	R*	R	R	N	System, HW, SW Requirements PASA PSSA	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.
* Independence for the safety artifacts is achieved when the safety activity is performed by a person(s) other than the developer of the system/item.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
4.0 Requirements Validation Process														
4.1	Aircraft, system, item requirements are complete and correct.	5.4 5.4.2 c 5.4.3 5.4.4	R*	R*	R	A	N	Validation Results	②	②	②	②		Includes coordination of interfaces between systems and between items.
4.2	Assumptions are justified and validated	5.4.2.d	R*	R	R	A	N	Validation Results	②	②	②	②		
4.3	Derived requirements are justified and validated.	5.3.1.4 5.3.2 5.4.2	R*	R*	R	A	N	Validation Results	②	②	②	②		
4.4	Requirements are traceable.	5.4.3 5.4.4	R	R	R	A	N	Validation Results	②	②	②	②		
4.6	Validation compliance substantiation is provided.	5.4.2.e 5.4.2.f 5.4.8 5.4.7.4	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.
* Independence for the requirement artifacts is achieved when the validation activity is performed by a person(s) other than the developer of the requirement.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
5.0 Implementation Verification Process														
5.1	Test or demonstration procedures are correct.	5.5.4.3	R*	R	R	A	N	Verification Procedures	①	①	②	②		
5.2	Verification demonstrates intended function and confidence of no unintended function impacts to safety.	5.5.1 5.5.5.3	R*	R	R	A	N	Verification Procedures	①	①	②	②		
		5.5.5.2	R*	R	R	A	N	Verification Results	②	②	②	②		
5.3	Product implementation complies with aircraft, and system requirements.	5.5.1 5.5.2	R*	R	R	A	N	Verification Procedures	①	①	②	②		
			R*	R	R	A	N	Verification Results	②	②	②	②		Specific item verification activities are performed under DO-178B/ED-12B and DO-254/ED-80.
5.4	Safety requirements are verified.	5.5.1 5.5.5.3	R*	R*	R	A	N	Verification Procedures and Results (ASA, SSA)	②	②	②	②		See Appendix A, Section 3.0, Safety Assessment Objectives for specific safety objectives and control categories.
5.5	Verification compliance substantiation is included.	5.5.6.3	R	R	R	A	N	Verification Matrix	②	②	②	②		
		5.5.6.4	R	R	R	A	N	Verification Summary	②	②	②	②		
5.6	Assessment of deficiencies and their related impact on safety is identified.	5.5.6.4	R	R	R	A	N	Verification Summary	②	②	②	②		
			R	R	R	A	N	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.
* Independence is achieved when the verification activity is performed by a person(s) other than the developer.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
6.0 Configuration Management Process														
6.1	Configuration items are identified.	5.6.2.2	R	R	R	A	N	CM Records	②	②	②	②		
6.2	Configuration baseline and derivatives are established.	5.6.2.3	R	R	R	A	N	Configuration Baseline Records	①	①	②	②		
6.3	Problem reporting, change control, change review, and configuration status accounting are established.	5.6.2.4	R	R	R	R	N	Problem reports CM Records	②	②	②	②		
6.4	Archive and retrieval are established.	5.6.2.5	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	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
7.0 Process Assurance Process														
7.1	Assurance is obtained that necessary plans are developed and maintained for all aspects of system certification.	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 those plans.	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.
* Independence is achieved when the process assurance activity is performed by a person(s) other than the developer.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
8.0 Certification and Regulatory Authority Coordination Process														
8.1	Compliance substantiation is provided.	5.8.3	R	R	R	A	N	Certification Summary	①	①	①	②		
		5.8.4.2	R	R	R	A	N	Configuration Index	①	①	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

The first task that should be accomplished on any new program is the creation of a safety program plan. 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 a 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 the 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 design 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 a safety program plan example. Details for accomplishing the tasks described herein may be found in ARP4761.

Example Safety Program Plan

Table of Contents

1.0 Scope and Purpose

The purpose of this safety program plan is to define the scope of the safety work and 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 items according to the milestones (reviews) of the development plan.

The program has the overall responsibility for the design safety of the product. The tasks 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. The aircraft level safety analysis tasks are accomplished by an airplane level team led by a group with airplane 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 compliance is verified using a bottom-up approach. Component requirements verification is gathered into system and eventually aircraft verification as the program proceeds through the build and deliver phase of the program.

This document covers all phases of the development of *(insert program name here)*. The plan covers the development of the maintenance planning documents under the Maintenance Steering Group process (MSG-3) and the development of the Master Minimum Equipment List (MMEL). The in-service “Operate and Monitor” phase of the program will be governed by standards such as ARP 5150 after initial delivery and are not covered here.

2.0 Organizational Structure of the Program

The organizational structure of the program should be outlined here.

2.1 Safety Group Sub-Teams:

Sub-teams, each with a well-defined focus, will be formed. The sub-teams allow for better division of safety tasks. Example sub-teams are: Particular Risks Assessment (PRA) Team and Aircraft-Level Safety Assessment Team (ASAT).

3.0 Safety Responsibilities:
The overall ownership (usually consisting of the Chief Program Engineer and his staff) 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.

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:

- Establish and communicate the safety requirements at all tiers of definition
- Identify aircraft/system functions required for continued safe flight and landing
- Develop an Aircraft-Level Functional Hazard Assessment (FHA) [if at the OEM level]
- Develop System FHA manual and ensure System FHAs are performed consistently in accordance with this guidelines [if at the OEM level]

- Conduct thorough, integrated survivability assessments [if at the OEM level]
- Identify safety lessons learned from previous programs and provide visibility to program management
- Identify aircraft level safety issues and provide visibility to program management responsible for assuring implementation of committed safety changes [if at the OEM level]
- Monitor the completion of the preliminary system safety assessments, to ensure that safety requirements are 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, including the documentation that their compliance meets the safety requirements.
- Coordinate with the Test Organization to ensure proper testing of failure modes developed in the Fault Trees and FMEAs.
- Work with the Chief Pilot to ensure that there are no design issues that could lead to a flight crew caused incident or accident.
- Work with the maintenance organization to ensure that there are no design issues that could lead to a maintenance-caused incident or accident.
- Play an active role in the Candidate Certification Maintenance Requirement (CMR) meetings.
- Play 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.
- Play an active role in the Flight Operations development of the Master Minimum Equipment List (MMEL).
- Coordinate Aircraft level Safety certification activities [if at the OEM level]

Aircraft Safety Group deliverables may include:

- Safety Program Plan
- Aircraft Level FHA
- Aircraft level PASA/ASA
- Aircraft-level safety requirements and objectives
- System-level safety requirements
- Validation/verification progress reports, as required for the safety program
- Special Aircraft-Level Safety Assessments, as required by the program
- Safety Program Schedules
- Safety case deliverable.

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 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 Design and Design-support organizations.

Organization	Roles and Responsibilities
Aircraft Safety Group	Prepares draft Safety Program Plan document. Circulates plan for review, obtains comments, updates the document, and obtains approval signatures. Communicates the plan to others. Insures implementation of the plan.
Other Design Organizations	Reviews and concurs with the plan.
Chief Project Engineer	Reviews and approves plan.

3.3 Safety-Related Requirements

A safety assessment team, led by safety, consists of safety focals from all the aircraft/systems and facilitates the development of aircraft/system level safety requirements. Each safety-related system-level or aircraft-level design requirement will have a compliance owner having the primary responsibility for its accomplishment. A major role for the design organization will be to ensure that relevant safety-related requirements are identified and properly acted upon. These requirements will include applicable Federal Aviation Regulations (FARs) and Certification Specifications (CSs) and any applicable supplementary regulatory-agency requirements. The requirements will also include the applicable company requirements.

The primary sources of design safety requirements for the program are defined in the following paragraphs.

Organization	Roles and Responsibilities
Aircraft Safety Group	Documentation and upkeep of safety requirements
Design Organizations	Reviews, concurs with and implements safety requirements where they are an affected owner

3.3.1 Safety-Related Requirements from Regulatory Agencies:

The Designers and the appropriate Design-Support organizations will identify all the airworthiness requirements from regulatory agencies and the amendment levels that will apply to the program. All differences with respect to the regulatory requirements applicable to the baseline will be specifically identified. Regulatory requirements include the regulatory airworthiness standards and all other relevant safety-related requirements documented in issue papers, special conditions, and certification requirement items. The Certification organization will maintain a current record of the regulatory requirements applicable to the aircraft as the program evolves. The information will be made available to the program organizations.

3.3.2 Safety-Related Requirements in the Requirements Database

The Safety organization and the applicable Design and Design-Support organizations will have the responsibility for supplying the information that will be added to the Requirements Database. The Systems Engineering organization will have the responsibility for managing the database and publishing this material. The Design organizations are responsible for reviewing the safety-related requirements, resolving any issues that arise, and approving the safety portion of the database.

3.3.3 Requirements from Functional Hazard Assessment Results:

The Chief Project Engineer will ensure that the safety objectives including the derived probabilistic requirements that result from the Functional Hazard Assessment are properly allocated to systems.

3.3.4 Maintenance Steering Group (MSG-3) Analysis:

The Aircraft Safety Group will participate in the MSG-3 analysis process in order to ensure that the design safety requirements are not compromised during the development of the maintenance plan.

3.3.5 The Master Minimum Equipment List (MMEL) 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.

3.3.6 Flight Testing

The Safety organization will participate in the planning and execution of 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 aircraft-level safety requirements. These activities will be in accordance with the Flight Test Program Plan. The Safety organization will maintain oversight on test readiness reviews, including the First Flight Readiness Review. Safety issues arising from flight testing will be dispositioned using the processes in this plan.

3.4 Special Aircraft-Level Safety Assessments [for airframe manufacturers]:

A Special Aircraft-Level Safety Assessment is any aircraft-level safety assessment required for certification other than an aircraft-level threat-survivability assessment, the aircraft level FHA, FTA or an aircraft-level separation assessment. Two special aircraft level safety assessments that have been identified as candidates on some programs in the past are Return to Land Assessment, and Blade Out Analysis. Others maybe identified as the program proceeds toward completion.

3.4.1 Return to Land Assessment:

An FAA issue paper identifies the requirement for a Return to Land Assessment. The aircraft must be able to return to any field from which it departed in any dispatchable configuration, and it must be able to return to any field from which it departed following any failure or failure combination not shown to be extremely improbable.

Organization	Roles and Responsibilities
Aircraft Safety Group	Facilitates the Return to Land assessment
Aerodynamics	Perform assessment

3.4.2 Blade Out/Engine Vibration Assessment:

An assessment of engine vibration following a single blade loss and its possible effects on the aircraft will be developed to ensure the aircraft remains capable of continued safe flight and landing. Particular focus will be on whether the flight crew can perform their functions and maintain adequate control of the aircraft during high vibration scenarios.

Note: This assessment may be included in the PRA in some companies.

Organization	Roles and Responsibilities
Aircraft Safety Group	Facilitates the Blade Out assessment
Affected Design Organizations	Perform assessment
Program Engineering	Review and approve assessment

3.5 Certification Plan for Aircraft-Level Safety [for airframe manufacturers]:

The Certification Plan for Aircraft-Level Safety contains information showing compliance with 14 CFR/CS Part 25.1309 regarding the interactions of 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 the 14 CFR/CS Part 25.1309 requirements for the hazards identified in the aircraft FHA.

Organization	Roles and Responsibilities
Aircraft Safety Group	Prepare Certification Plan for Aircraft-Level Safety
Program Engineering	Review and approve Certification Plan

3.5.1 Aircraft-Level Safety Assessment Document:

The Aircraft-Level Safety Assessment document summarizes the program's safety-related activities and provides single point documentation for the tasks identified in the Safety Plan. Part of this activity is sometimes called safety synthesis All or part of this document may be provided to the regulatory agencies in the form of an Aircraft Safety Certification Summary to demonstrate compliance with the Certification Plan for Aircraft-Level Safety identified above.

The Aircraft Safety Group will prepare the Aircraft-Level Safety Assessment document.

Organization	Roles and Responsibilities
Aircraft Safety Group	Prepare Aircraft Level Safety Assessment Document
Design	Provide data, review and approve Aircraft Level Safety Assessment

3.6 Aircraft Safety Program Schedule:

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.

3.7 Preliminary Design Reviews

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

Organization	Roles and Responsibilities
Aircraft Safety Group	Participate in the Preliminary Design Review to ensure all safety requirements, hazards and safety lessons learned are presented and resolved.
Design	Conduct the Preliminary Design Review

3.8 Critical Design Reviews:

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

Organization	Roles and Responsibilities
Aircraft Safety Group	Participate in the Critical Design Review to ensure all safety requirements, hazards and safety lessons learned are presented and resolved
Design	Conduct the Critical Design Review

3.9 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.

Engineering Operations will lead the meeting and walk-through process for the Engineering Safety Review. Items identified will be tracked to closure to ensure that all issues are corrected prior to first flight. The Aircraft Safety Group will support the process as required.

Organization	Roles and Responsibilities
Engineering Operations	Plan and coordinate Engineering Safety Review
Manufacturing	Make aircraft available and prepare it for Engineering Safety Review
Aircraft Safety Group	Participates in the Engineering Safety Review to determine that the aircraft was built as designed.

4.0 Common Cause Assessments:

4.1 System Separation:

Note: (This example cites a case where a unique separation document is developed. Some companies include this work in their basic safety analyses.)

A Separation Work Group, led by the Aircraft Safety Group, will develop the system physical and functional separation requirements. The purpose of this activity is to ensure aircraft flight capability is maintained by assuring adequate separation of functions, including the threats defined in the PRA document (see 4.2.1). Design will review and approve the separation requirements. Cross functional teams responsible for specific areas of the aircraft (herein referred to as Volume Teams) will assure the implementation of the system separation requirements.

The Separation Work Group deliverables may include (varies by company):

- Establish and validate separation requirements to incorporate into the requirements database.
- Participate in analyzing the system designs and installations to verify compliance with the requirements.
- Interface with Design to accomplish these tasks.

4.1.1 System Separation Requirements Incorporation into the Requirements Database:

The Aircraft Safety Group and the appropriate Design organizations will be responsible for defining the functional and physical separation requirements so they can be included into the aircraft requirements database.

Organization	Roles and Responsibilities
Aircraft Safety Group	Lead the Separation Requirements development Activity
Design	Review, approve and implement the Separation Requirements.

4.1.2 System Separation Requirements Compliance Verification:

Once the separation requirements are established and documented, a verification process needs to be identified to ensure that the separation requirements are implemented into the design and manufacturing of the aircraft. The Volume Teams (made up of members from systems, design, safety organizations) lead this effort. The Design Organization will determine the most effective method of completing this task. Methods may include Zonal reviews, Fly-throughs and As-Built reviews.

Organization	Roles and Responsibilities
Volume Teams	Lead the Separation Requirements Verification Activity to assure Separation Requirements are met.
Design Organizations	Review and approve the Separation Verification

4.2 Aircraft Survivability:

Use the hazard classification chart listed in AC/AMC 25.1309 to define the severity levels of the hazards.

4.2.1 Particular Risk Review Team (PRRT):

The PRRT task is to assess the aircraft design for external threats that may compromise continued safe flight and landing (ARP4761 Particular Risk Assessment). These threats are limited to those external to the system in question (e.g. hydraulic system vulnerability to engine burst) or to the aircraft (e.g. birdstrike).

The PRRT deliverables are:

- Identify credible flight safety threats that are appropriate for survivability analysis.
- Provide the requirements so they can be listed in the requirements database.
- Assess the aircraft survivability with respect to each identified threat, taking into account physical and functional system separation requirements and system hardening.
- Validate and document the aircraft/system safety requirements for survivability.
- Verify that the aircraft design incorporates design solutions for each identified threat

The team will review all survivability requirements from other aircraft models. They will also research any new threats generated by the new technology used on the aircraft. Any threat-survivability requirements identified will be included in the requirements database.

The consequences of the threats resulting in a hazard class I or II will be documented.

Organization	Roles and Responsibilities
Aircraft Safety Group	Leads the PRRT process
Design Focals	Participate in the PRRT
Program Engineering	Review and approve the PRRT document and implement changes required.

4.3 Zonal Safety Analysis (ZSA)

A ZSA will be performed in each zone of the aircraft after the components are situated in the as-built configuration. The analysis consists of consideration of installation aspects of individual systems and components and the mutual influence between several systems/components installed in close proximity on the aircraft. Zone Chiefs will be assigned for each zone of the aircraft. They will lead the ZSA for their zone, utilizing participants from the effected design groups and from functional support groups. The conclusions of the ZSAs will provide inputs to the relevant SSAs. Findings of exceptions in the ZSA should result in a design change or a documented justification for a deviation.

Organization	Roles and Responsibilities
Zone Chiefs	Lead the ZSA for their areas.
Aircraft Safety Group	Participates in the Zonal Safety Analysis
Program Engineering	Review and approve the Zonal Safety Analysis and implement changes required.

4.4 Common Mode Analysis (CMA):

A Common Mode Analysis (CMA) is performed to verify that ANDed events in the FTA are truly independent. The effects of design implementation, manufacturing, maintenance errors and failures of system components that defeat redundant design principles should be analyzed. Generally speaking, the CMA contributes to the verification that independent principles have been applied when necessary. Considerations should be given to the independence of functions and their respective monitors. Components with identical hardware and/or software could be susceptible to generic (common cause) faults which could cause failures in multiple systems. The CMA process is based on analyzing designs and implementation for elements that may defeat the redundancy or independence of functions within the design. Wherever required redundancy or independence is compromised, justification for the acceptability of the compromise is required.

Organization	Roles and Responsibilities
Aircraft Safety Group	Leads the CMA.
Design Focals	Participate in the CMA.
Program Engineering	Review and approve the Common Mode Analysis and implement changes required.

5.0 Safety Assessments and Analyses:

The safety assessment and analysis process includes requirements generation, validation and verification which supports the aircraft development activities. These processes provide a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards have been properly addressed. The safety assessment processes have both qualitative and quantitative components.

5.1 Common Naming Convention:

One of the tools required to perform multi-function analyses 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 team. This method ensures that multiple occurring events in the aircraft architecture are correctly represented in the tree and identified in cut sets.

Organization	Roles and Responsibilities
Aircraft Safety Group/Reliability	Develop and implement FMEA and FTA Ground Rules and Assumptions.
Design	Use the ground rules and assumptions document in the development of the FTAs and FMEAs.

5.2 Aircraft Level FHA and PASA

A team led by the Aircraft Safety Group is responsible for developing the Aircraft Level FHA and for ensuring that all system level FHAs are consistent with other system FHAs and with the aircraft FHA. This team will also be responsible for preparing a Preliminary Aircraft level Safety Assessment (PASA) based on the aircraft FHA, with refinement over the course of the development program. This team will assess the effects of individual and combined system failures on aircraft level functions. From this activity, safety requirements (for example functional separation requirements to ensure that combinations of system failures do not compromise continued safe flight and landing) can be generated and submitted into the requirement database with appropriate compliance owner and affected owners. The team will have the responsibility to track the functional hazard status to closure. The Aircraft level FHA is complete when all functional hazards have been identified and addressed.

Organization	Roles and Responsibilities
Aircraft Safety Group	Develop and document Aircraft Level FHA
Design	Provide input and review of Aircraft Level FHA

5.2.1 Continued Safe Flight and Landing Functions List:

The Aircraft Safety Group will provide the program with the list of functions that are required for Continued Safe Flight and Landing. This list is used to help determine the architectural layout of the aircraft.

Organization	Roles and Responsibilities
Aircraft Safety Group	Develop Continued Safety Flight and Landing functions list
Design	Review and concur with the list and use to determine architecture and capabilities

5.3 System Level FHA:

System Level Functional Hazard Assessments (FHA) are conducted at the beginning of the aircraft development cycle. They should identify and classify the Failure Conditions associated with the aircraft functions, including the rationale for the classification. The Aircraft Safety Group will coordinate reviews of system level FHAs to ensure that all hazards have been identified and that the FHAs are consistent between design groups. The results of these reviews will produce the safety objectives including the budgeted probabilistic safety requirements for each system/function . The System level FHAs provide the basis for analyzing combinations of system failures and assessing Aircraft level effects.

Organization	Roles and Responsibilities
Aircraft Safety Group	Ensure the System Level FHAs are performed in accordance with FHA Manual
Design	Prepare the System Level FHAs

5.3.1 FHA Manual:

Safety should prepare a Functional Hazard Assessment Manual to aid the designers in accomplishing the task. This will help to ensure consistency in the FHA results

5.3.2 FHA Compliance Verifications and Closure

FHA Requirements Compliance Verification is the process of determining and documenting whether each FHA derived safety criterion is complied with. The FHA closure status will be presented to program management on a regular interval to give visibility of the remaining safety tasks. Results will be summarized in the Aircraft-level Safety Assessment document.

Organization	Roles and Responsibilities
Aircraft Safety Group	Plan and coordinate FHA requirements verification and closure.
Program Engineering	Review and approve the FHA requirements verification and closure.

5.4 Preliminary System Safety Assessment:

The Preliminary System Safety Assessment (PSSA) is a systematic examination of the proposed system architecture(s) to determine how failures can cause the functional hazards identified by the FHA. The objective of the PSSA is to establish the safety requirements of the system and to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the FHA. The PSSA is also an interactive process associated with the design definition. The PSSA is conducted at multiple stages of the system development including system, component, and hardware/software design definitions.

Organization	Roles and Responsibilities
Aircraft Safety Group	Ensure development of system FHA and provide input to the PSSA process.
Design	Perform PSSA and implement changes required.

5.5 System Safety Assessment

The System Safety Assessment (SSA) is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the development documents, principally from the FHA and derived safety requirements from the PSSA, are met. The SSA is usually based on the PSSA FTA or other approved methods and uses the quantitative values obtained from the Failure Modes and Effects Summary (FMES). The SSA also verifies that qualitative aspects e.g. development assurance levels have been accomplished. The SSA should verify that all significant effects identified in the FMES are considered for inclusion as primary events in the FTA. The FMES is a summary of failures identified by the FMEA(s) which are grouped together on the basis of their failure effects. The SSA should also include applicable common cause analysis results.

Organization	**Roles and Responsibilities**
Design	Create the SSA.
Aircraft Safety Group	Participates in the SSA.
Program Engineering	Review and approve the SSA.

5.6 System FTAs and FMEAs

The system FTAs and FMEAs are performed with Safety Engineering maintaining oversight to ensure that FMEA and FTA processes are consistently applied across systems. Safety Engineering and the ASA team will also track FTA and FMEA progress to ensure that FHA Failure Conditions are adequately addressed. This will include all Catastrophic and Hazardous Failure Conditions as well as significant Major conditions for which this level of analysis is deemed appropriate. Finally, Design will collect the system FTAs and FMEAs and use them as required to develop multi-function analyses to be included in the Aircraft-Level Safety Assessment Document.

Organization	**Roles and Responsibilities**
Design	Create the FTAs and FMEAs.
Aircraft Safety Group	Participates in the FTAs and FMEAs.
Program Engineering	Review and approve the FTAs and FMEAs.

APPENDIX C – FDAL/IDAL ASSIGNMENT PROCESS EXAMPLE

The process for assigning Development Assurance Levels to Functions (FDAL) and to items (IDAL) with architectural considerations (see section 5.2.3.2) is shown in the Figures C-1 and C-2. This process should be applied each time the aircraft/system architecture is modified, during the PASA/PSSA when all causes of the Failure Conditions need to be identified and reassessed, and each time the Functional Hazard Assessment is revised. When considering re-use of previously developed aircraft/system functions and items, their associated FFS should satisfy the general principles defined in Section 5.2.1 and may not require full application of each step of the process described in the Figure C-1 and C-2.

The process in the following flowchart is top down, starting from a Failure Condition Classification identified in the Aircraft Level FHA and its associated Top-Level FDAL; then assigning Function FDALs to identified FFSs and its Members; culminating with assignment of the IDAL to items (software/electronic hardware). Ultimately, the intent is to go through the process flow described below to satisfy all the Failure Conditions identified in the FHA. The process flow is represented as a single pass flow; however, it should be understood that there is interaction between the aircraft/system functional levels and the item development levels thus may require multiple iterations across the FDAL/IDAL boundary.

Step by Step Process Description

a) Select a FC from the FHA

The list of Failure Conditions (FCs) identified in the Aircraft or System Level Functional Hazard Assessment (see Section 5.1.1) is the input to the FDAL and IDAL assignment process. The Preliminary Aircraft Safety Assessment/Preliminary System Safety Assessments use the Failure Condition data for the purposes of FDAL Assignment.

b) Assign top FDAL per Table 2

A top FDAL is assigned based on the Failure Condition Classification. This is performed for each Failure Condition in the aircraft and system FHAs in accordance with Table 2 of Section 5.2.3. For systems that provide protection against an external event, this may also consider external events per Section 5.2.4.

c) Identify the Functional Level FFSs

At this stage of the development process, the functional failure set analysis should be performed to identify FFSs and their associated functional Members. There may be single member FFS(s) or multiple member FFSs. Conceptually, an FFS is equivalent to a Fault Tree minimal cut set (as defined in ARP4761), whose members represent the result of potential development errors rather than failures.

d) Select a Functional Failure Set (FFS)

Select a single FFS from the identified FFSs.

The FDAL assignment process is applied to all identified FFSs, for each Failure Condition in the FA and is applied to all identified FFs.

e) Does the FFS have Multiple Members?

At this stage a multiple Member FFS has functionally independent Members.

f) Are Functional Independence Claims Valid?

For a FFS with multiple Members, Functional Independence can be claimed when the common sources of Error between multiple requirement sets have been minimized at a level of rigor commensurate with the top FDAL. If the presence of common Error sources in the requirements is indeterminate, then Functional Independence claims are invalid (see Section 5.2.3.2.1.1).

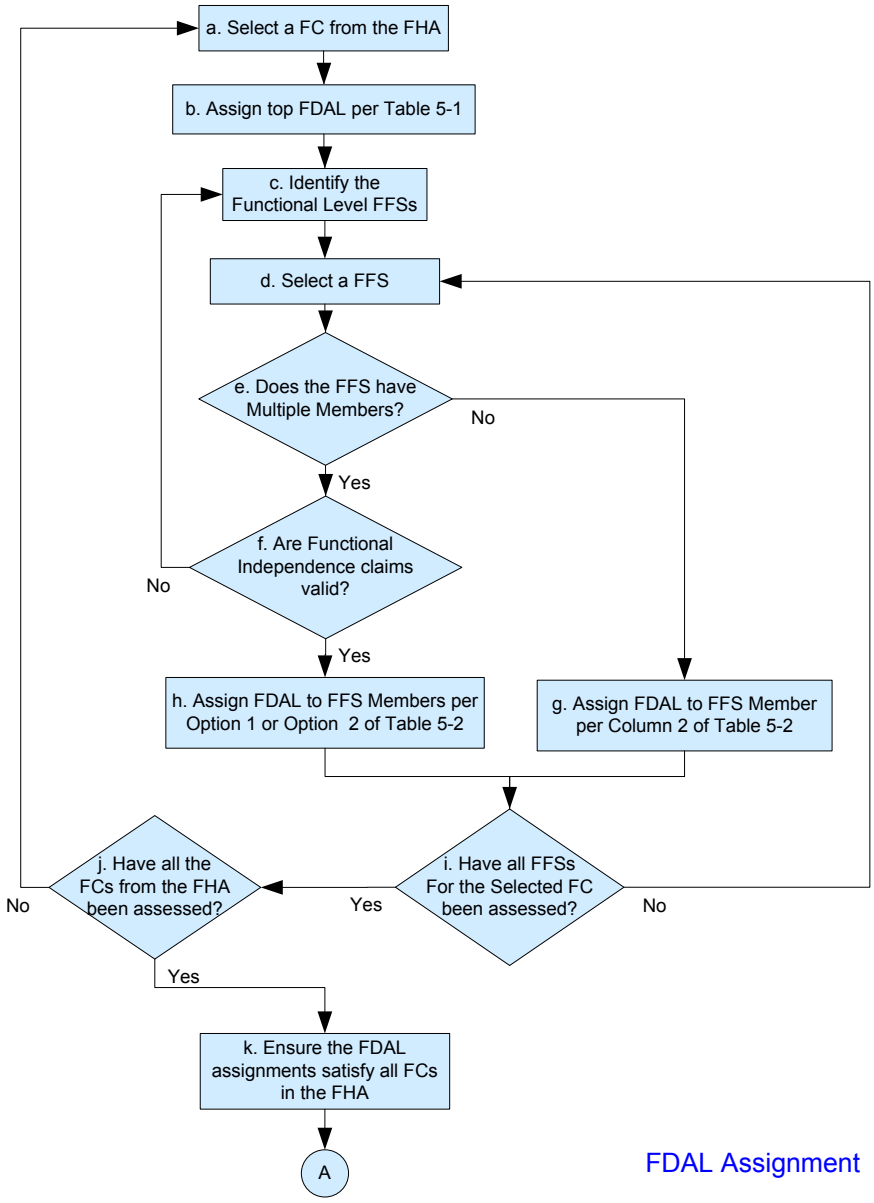

Figure C- 1 Example FDAL/IDAL Assignment with Architecture Considerations Process Flow Chart (1 of 2)

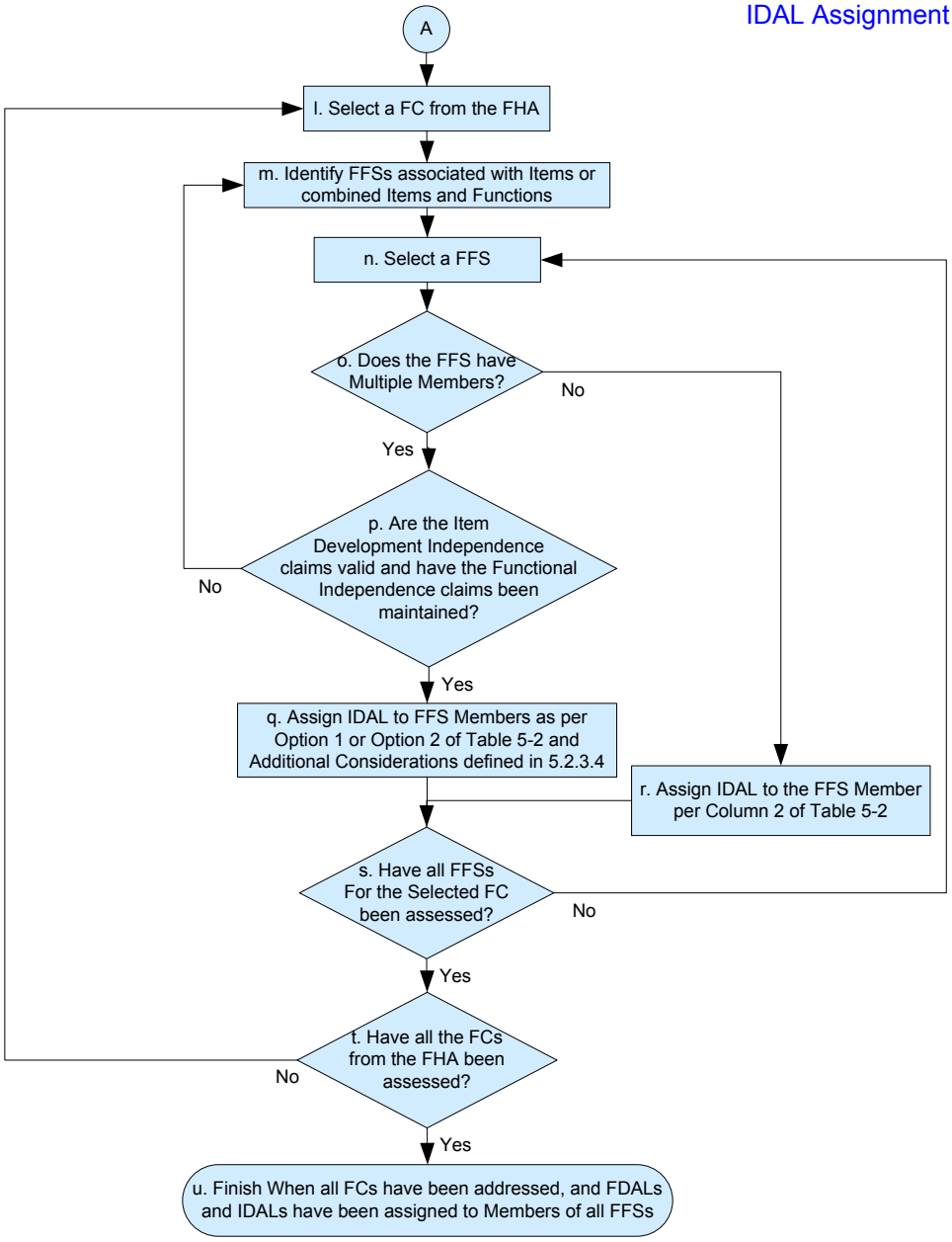

Figure C-2 Example FDAL/IDAL Assignment with Architecture Considerations Process Flow Chart (2 of 2)

g) Assign FDAL to FFS Member per Column 2 of Table 3

If the FFS has a single Member, (i.e. an error in the development of that Member can directly result in the Failure Condition being assessed) then the FDAL should be assigned to that Member as per Column 2 of Table 3 of Section 5.2.3.2.2.

h) Assign FDAL to FFS Members per Option 1 or Option 2 of Table 3

The choice of whether to apply Option 1 or Option 2 is at the discretion of the applicant but should consider what functional implementation is most appropriate to mitigate the FCs. Considerations may also be warranted for external events per Section 5.2.4.

i) Have all FFSs for the Selected Failure Condition been assessed?

Once FDALs have been assigned to the Members in the selected FFS, the FDAL assignment process should be applied to each of the identified FFSs for the selected Failure Condition.

j) Have all the Failure Conditions from the FHA been assessed?

Once FDALs have been assigned to all Members of all FFSs associated with the selected Failure Condition, the FDAL assignment process should be applied to each of the Failure Conditions identified in the FHA.

k) Ensure the FDAL assignments satisfy all FCs in the FHA

Compile a list of all functions and select the FDAL assignment(s) that satisfy all applicable FFSs and Failure Conditions.

It is recognized that FFSs may share common Members and FCs may relate to common functions; therefore, the FDAL assignment to Members of all the FFSs for all FCs identified from the FHA should be reviewed to ensure that the Top FDAL for each FC in the FHA is satisfied.

Futhermore, it is recognized that one may need to reassign the appropriate FDAL and/or reallocate functions to ensure the FDAL assignments satisfy the general principles defined in Section 5.2.1.

l) Select a FC from the FHA

The System Safety Assessment needs to apply the IDAL assignment process to each Failure Condition in the FHA. Once the FHA has been established for the Aircraft or System, the first Failure Condition (FC) from the FHA – and then each subsequent FC thereafter - should be selected for the purposes of IDAL Assignment.

m) Identify FFSs Associated with Items or Combined Items and Functions

Each functional level FFS will have one or more associated item level FFS(s). Furthermore, FFSs may exist that combine aircraft/system functions and items. The item level FFS(s) and any FFSs with combined items and Functions should be identified using the techniques shown in Figure 9 of Section 5.2.3.2.3.2 and Figure 10 of Section 5.2.3.2.3.3.

n) Select a FFS

Select a single FFS from the identified FFSs.

o) Does the FFS have Multiple Members?

At this stage a multiple Member FFS may have Independent Members. When the Members include both aircraft/system functions and items, all Members of the FFS must demonstrate both Functional Independence and Item Development Independence.

p) Are the Item Development Independence Claims Valid and Have the Functional Independence Claims Been Maintained?

Item Development Independence is substantiated when the common sources of Error between multiple items have been minimized by applying a level of rigor commensurate with the top FDAL, based on the state of the art and in-service experience. If the presence of common Error sources in the items is indeterminate, then Item Development Independence cannot be claimed (see Section 5.2.3.2).

In addition, functional Independence claims should remain valid as in step f.

q) Assign IDAL to the FFS Member per Column 2 as per Option 1 or Option 2 of Table 3 and Additional Considerations defined in Section 5.2.2.3

The choice of whether to apply Option 1 or Option 2 is at the discretion of the applicant but should consider what Item Development implementation is most appropriate to mitigate the FCs.

r) Assign IDAL to the FFS Member per Column 2 of Table 3

If the FFS has a single Member, (i.e. an error in the development of that Member can directly result in the Failure Condition being assessed) then the IDAL should be assigned to that Member as per Column 2 of Table 3 of Section 5.2.3.2.2.

s) Have all the FFSs for the Selected FC been assessed?

Once IDALs have been assigned to the Members in the selected FFS the IDAL assignment process should be applied to each of the other identified FFS for the selected FC.

t) Have all the FCs from the FHA been assessed?

Once IDALs have been assigned to all Members of all FFSs associated with the selected FC the IDAL assignment process should be applied to each of the other FCs identified in the FHA.

u) Finish when all FCs have been addressed and FDALs and IDALs have been assigned to Members of all FFSs

The FDAL and IDAL assignment process is complete when all Failure Conditions identified in the FHA have been addressed, and FDALs and IDALs for all Members have been identified to satisfy the general principles defined in Section 5.2.1.

It is recognized that FFSs may share common Members and FCs may relate to common functions and/or items; therefore, the FDAL and IDAL assignment to Members of all the FFSs for all FCs identified from the FHA should be reviewed to ensure that the Top FDAL for each FC in the FHA is satisfied, and FDALs and IDALs for all Members have been identified to satisfy the general principles defined in Section 5.2.1.

At the end of the assignment process, an IDAL required assignment higher than the corresponding FDAL may be indication that the Functional Independence at the FDAL assignment has been invalidated. Therefore, the applicant may have to justify the architecture supporting the top level FC.

APPENDIX D - DELETED

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