



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

GUIDELINES FOR DEVELOPMENT OF CIVIL AIRCRAFT AND SYSTEMS

EUROCAE ED-79A / SAE ARP 4754A

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-79A

December 2010

GUIDELINES FOR DEVELOPMENT OF CIVIL AIRCRAFT AND SYSTEMS

EUROCAE ED-79A / SAE ARP 4754A

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-79A

December 2010

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 63 and SAE Committee S-18, was approved by the Council of EUROCAE.
2. EUROCAE is an international non-profit making organisation in Europe. Membership is open to manufacturers and users of equipment for aeronautics, trade associations, national civil aviation administrations, and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. The findings of EUROCAE are resolved after discussion amongst Members of EUROCAE and in collaboration with RTCA Inc, Washington D.C., and/or the Society of Automotive Engineers (SAE), Warrendale PA, U.S.A., through their appropriate committees.
4. EUROCAE performance specifications and other documents are recommendations only. EUROCAE is not an official body of the European Governments. Its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
5. Copies of this document may be obtained from:

EUROCAE

102, rue Etienne Dolet
92240 MALAKOFF
France

Tel: 33 1 40 92 79 30

Fax: 33 1 46 55 62 65

Email: eurocae@eurocae.net

Website: www.eurocae.net

RATIONALE

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

TABLE OF CONTENTS

CHAPTER 1	SCOPE	1
	1.1 Purpose	2
	1.2 Document Background	3
CHAPTER 2	REFERENCES	5
	2.1 Applicable Documents	5
	2.1.1 SAE Publications	5
	2.1.2 FAA Publications	5
	2.1.3 EASA Publications	5
	2.1.4 RTCA Publications	6
	2.1.5 EUROCAE Publications	6
	2.2 Definitions	6
	2.3 Abbreviations and Acronyms	10
CHAPTER 3	DEVELOPMENT PLANNING	13
	3.1 Planning Process	13
	3.2 Transition Criteria	15
	3.2.1 Deviations from Plans	15
CHAPTER 4	AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS	16
	4.1 Conceptual Aircraft/System Development Process	17
	4.1.1 Development Assurance	19
	4.1.2 Introduction to Development Assurance Process	19
	4.1.3 Introduction to Hierarchical Safety Requirements Generated from Safety Analyses	20
	4.1.4 Identification of Aircraft-Level Functions, Function Requirements and Function Interfaces	22
	4.1.5 Allocation of Aircraft Functions to Systems	22
	4.1.6 Development of System Architecture	22
	4.1.7 Allocation of System Requirements to Items	22
	4.1.8 System Implementation	22
	4.2 Aircraft Function Development	22
	4.3 Allocation of Aircraft Functions to Systems	25
	4.4 Development of System Architecture:	25
	4.5 Allocation of System Requirements to Items	26
	4.6 System Implementation	26
	4.6.1 Information Flow - System Process To & From Item Process(es)	26
	4.6.2 Hardware and Software Design/Build	28
	4.6.3 Electronic Hardware/Software Integration	28

	4.6.4 Aircraft/System Integration.....	28
CHAPTER 5	INTEGRAL PROCESSES	29
5.1	Safety Assessment.....	29
5.1.1	Functional Hazard Assessments	31
5.1.2	Preliminary Aircraft / System Safety Assessment.....	31
5.1.3	Aircraft / System Safety Assessment.....	32
5.1.4	Common Cause Analysis.....	33
5.1.5	Safety Program Plan	34
5.1.6	Safety-Related Flight Operations or Maintenance Tasks	34
5.1.7	Relationship with In-Service Safety	34
5.2	Development Assurance Level Assignment	35
5.2.1	General Principles – Introduction to Development Assurance Level Assignment	35
5.2.2	FDAL and IDAL	36
5.2.3	Detailed FDAL and IDAL Assignment Guidelines	36
5.2.4	FDAL Assignment Taking Credit for External Events.....	48
5.3	Requirements Capture	49
5.3.1	Types of Requirements.....	50
5.3.2	Deriving Safety-related Requirements from the Safety Analyses	52
5.3.3	Capturing Maintenance Requirements for In-service Use.....	53
5.4	Requirements Validation	53
5.4.1	Process Objectives	54
5.4.2	Validation Process Model	54
5.4.3	Correctness Checks.....	58
5.4.4	Completeness Checks	58
5.4.5	Validation Rigor.....	61
5.4.6	Validation Methods	61
5.4.7	Validation Data.....	63
5.5	Implementation Verification	64
5.5.1	Verification Process Objectives	64
5.5.2	Verification Process Model	65
5.5.3	Verification Rigor.....	67
5.5.4	Verification Planning	67
5.5.5	Verification Methods	67
5.5.6	Verification Data.....	70
5.6	Configuration Management.....	71
5.6.1	Configuration Management Process Objectives	72
5.6.2	Configuration Management Process Activities:	73

5.7	Process Assurance	75
5.7.1	Process Objectives	75
5.7.2	Process Assurance Plan.....	76
5.7.3	Project Plan Reviews	76
5.7.4	Evidence of Process Assurance	76
5.8	Certification and Regulatory Authority Coordination	76
5.8.1	Certification Planning	77
5.8.2	Agreement on the Proposed Means of Compliance.....	77
5.8.3	Compliance Substantiation	77
5.8.4	Certification Data	78
CHAPTER 6	MODIFICATIONS TO AIRCRAFT OR SYSTEMS	81
6.1	Modification Process Overview	82
6.2	Modification Management Process	82
6.3	Modification Impact Analysis	83
6.4	Modification Categorization and Administration	84
6.5	Evidence for Acceptability of a Modification:.....	84
6.5.1	Use of Service History	84
6.6	Considerations for Modifications	85
6.6.1	Introducing a New Aircraft-Level Function.....	85
6.6.2	Replacing Item or System With Another on an Existing Aircraft	86
6.6.3	Adapting Existing Item or System to a Different Aircraft Type	87
6.6.4	Modification to Item or System Without Adding a Function: ...	88
6.6.5	STC Production Introduction.....	89
CHAPTER 7	NOTES	91
APPENDIX A	PROCESS OBJECTIVES DATA.....	92
APPENDIX B	SAFETY PROGRAM PLAN	101
APPENDIX C	FDAL/IDAL ASSIGNMENT PROCESS EXAMPLE.....	116
APPENDIX D	DELETED	121
MEMBERSHIP		122

CHAPTER 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 ARP 4761, "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.

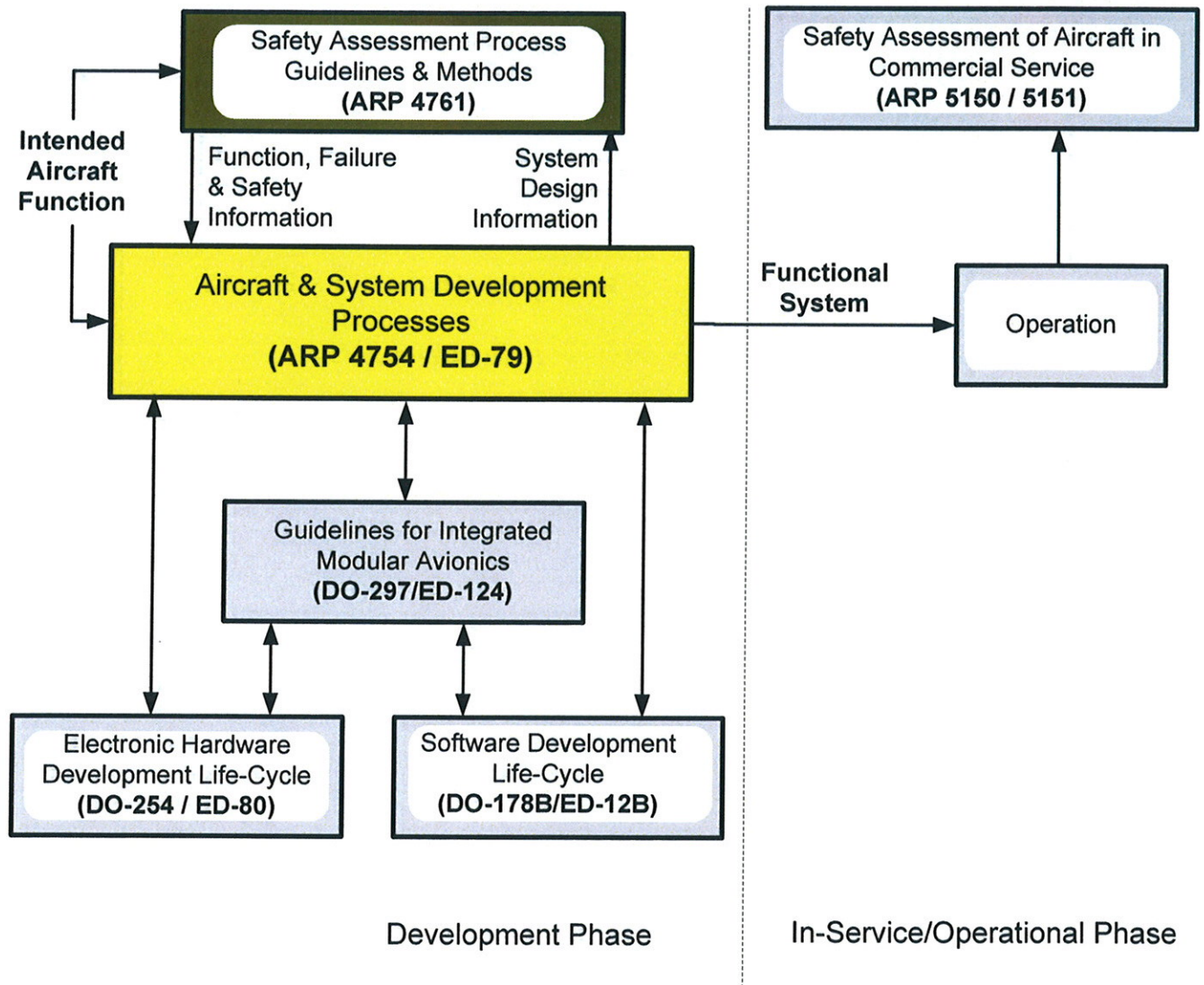


FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

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 EUROCAE / RTCA document ED-12 /DO-178, 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, ED-12A / DO-178A and ED-12B / DO-178B 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 ED-79 / ARP4754 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 ED-79 / ARP4754, come insights on the strengths and weaknesses of its guidelines. The underlying philosophy is succinctly represented in the original section 5.4 of ED-79 / 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 ED-79 / ARP 4754 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 ED-79 / ARP 4754 and ARP 4761, and their relationship with ED-12B / DO-178B and ED-80 / DO-254 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 ED-12B / DO-178B.

CHAPTER 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. (ED-12B / DO-178B)

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 ED-79 / ARP4754 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 ED-12B / DO-178B/, and design assurance level in ED-80 / DO-254 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. (ED-80 / DO-254)

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

CHAPTER 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.

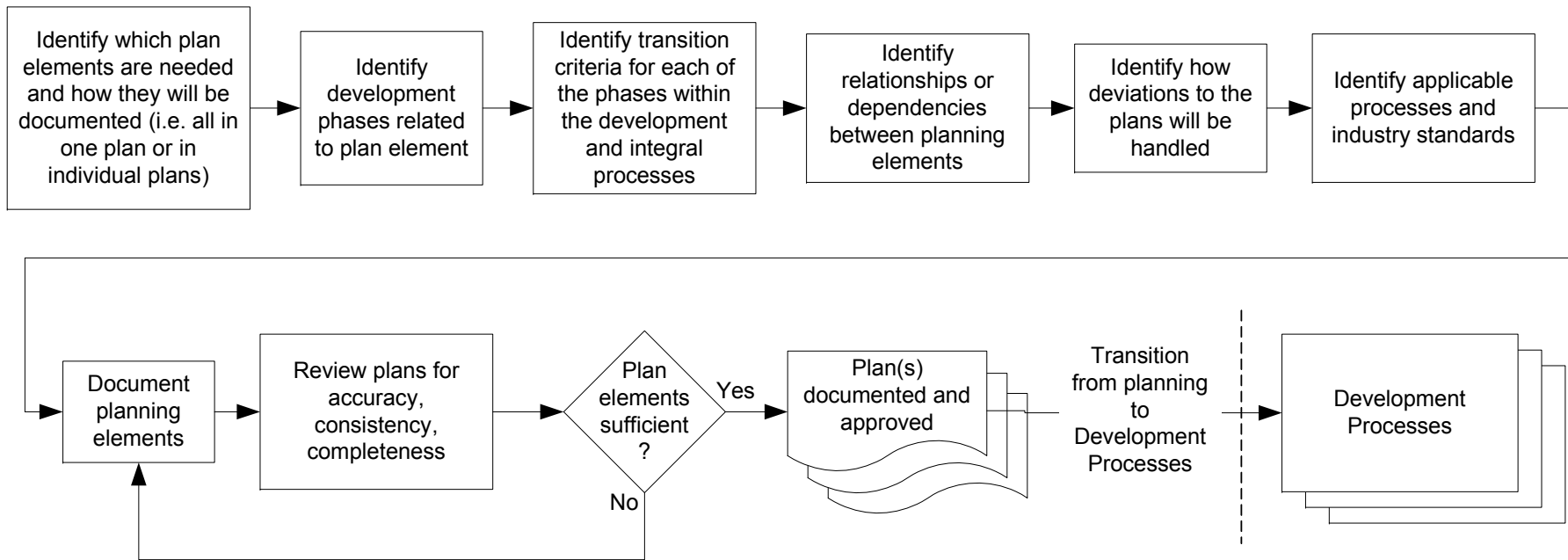


FIGURE 2 – PLANNING PROCESS

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.

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

CHAPTER 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.

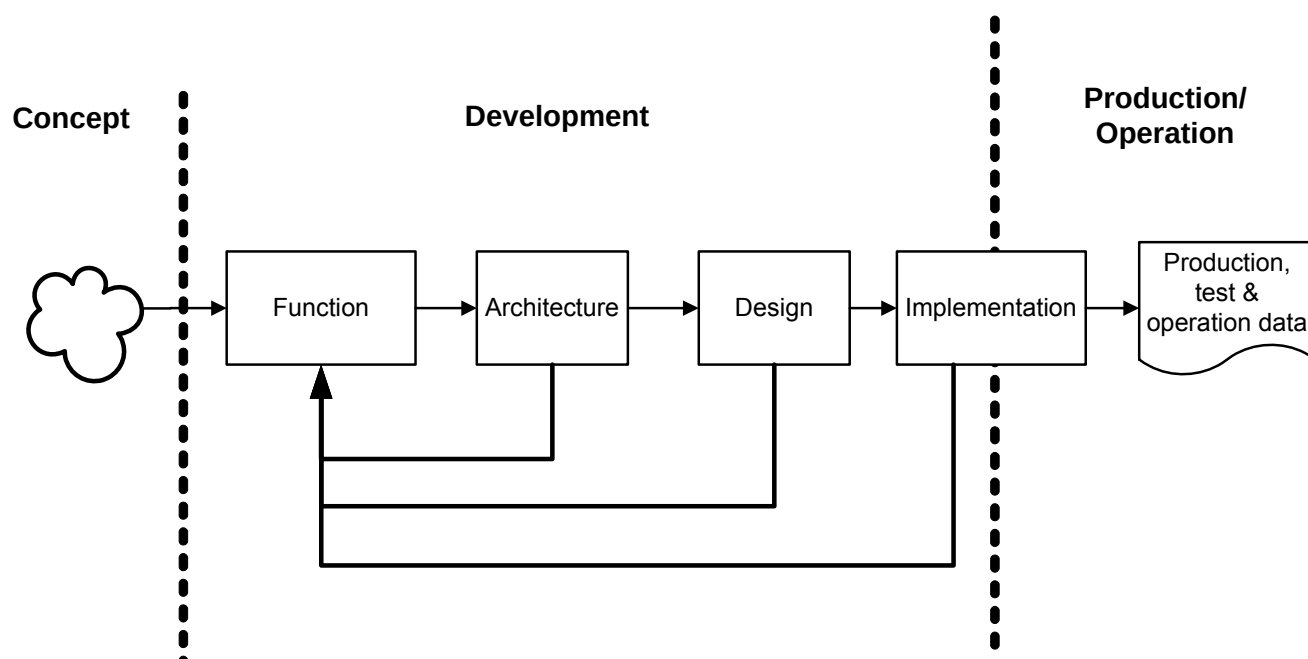


FIGURE 3 - DEVELOPMENT LIFE CYCLE

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.

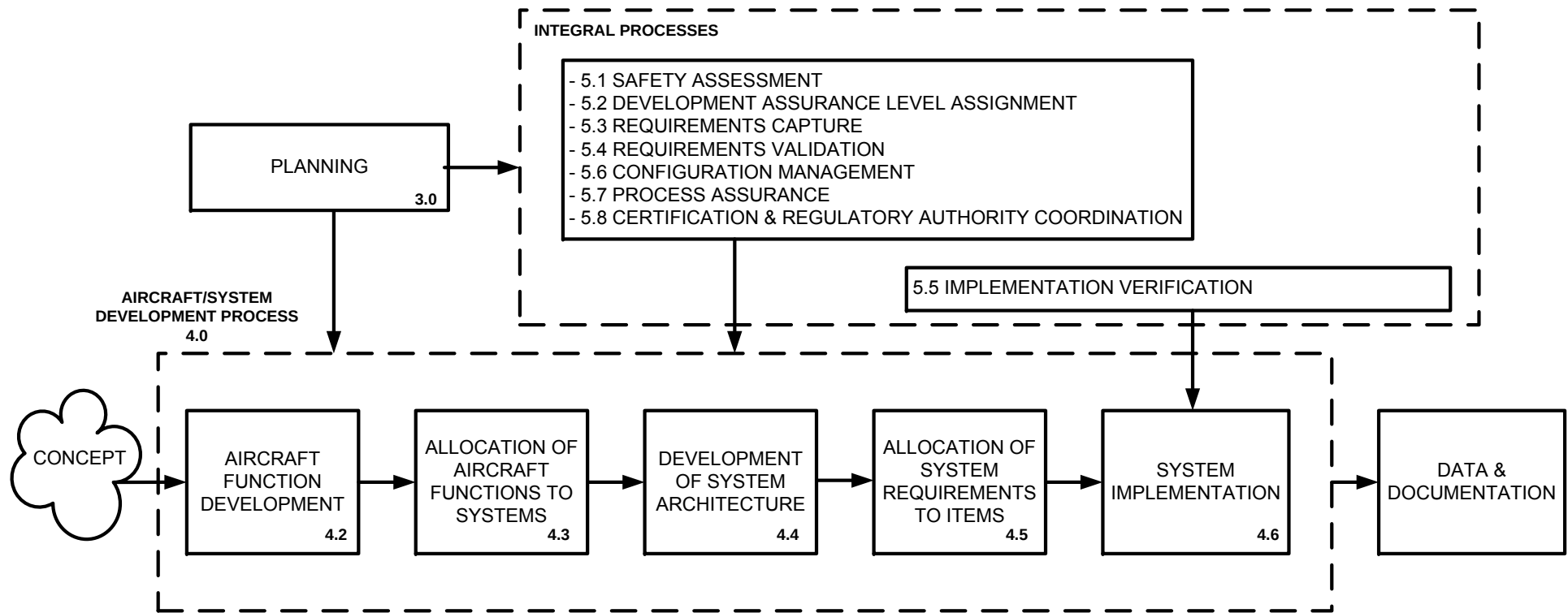


FIGURE 4 – AIRCRAFT OR SYSTEM DEVELOPMENT PROCESS MODEL

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 ED-12B / DO-178B and ED-80 / DO-254 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 ED-79A / ARP4754A regards the activities of ED-12B / DO-178B and ED-80 / DO-254 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 ED-12B / DO-178B and ED-80 / DO-254 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.

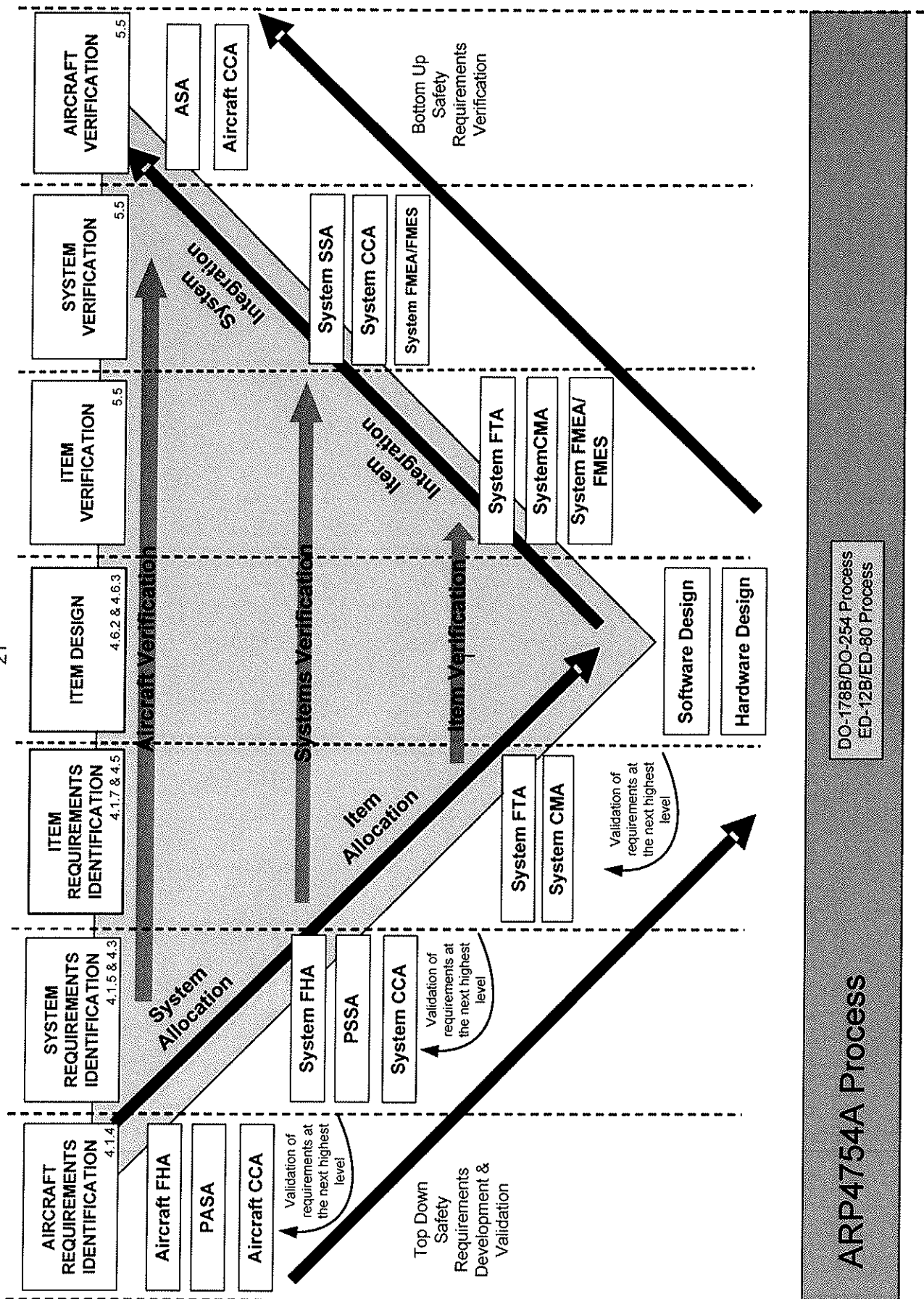


FIGURE 5 - INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

© EUROCAE, 2010

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 ED-12B / DO-178B software and ED-80 / DO-254 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

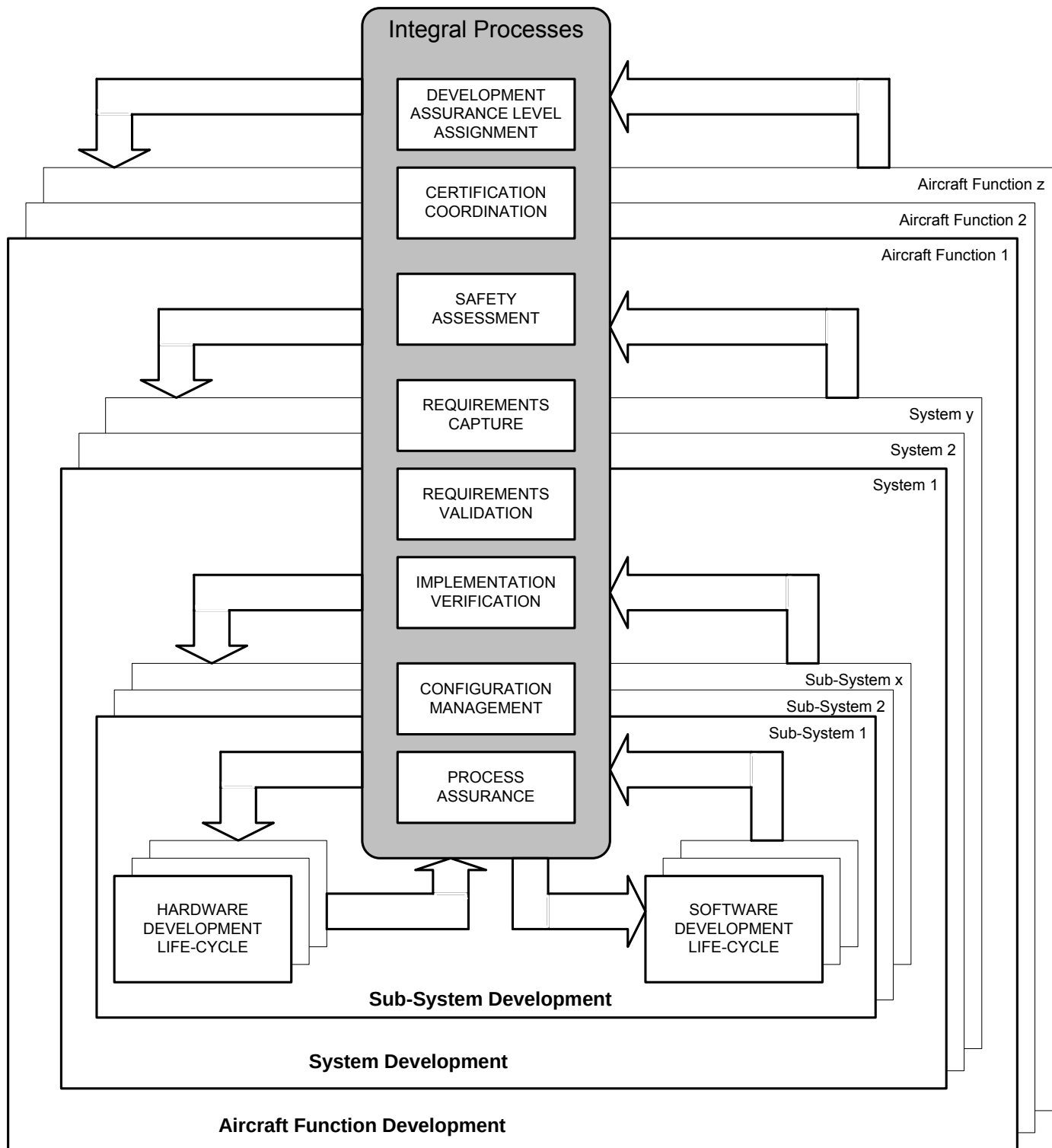


FIGURE 6 - AIRCRAFT FUNCTION IMPLEMENTATION PROCESS

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 ED-12B / DO-178B (for software), ED-80 / DO-254 (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.

CHAPTER 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.

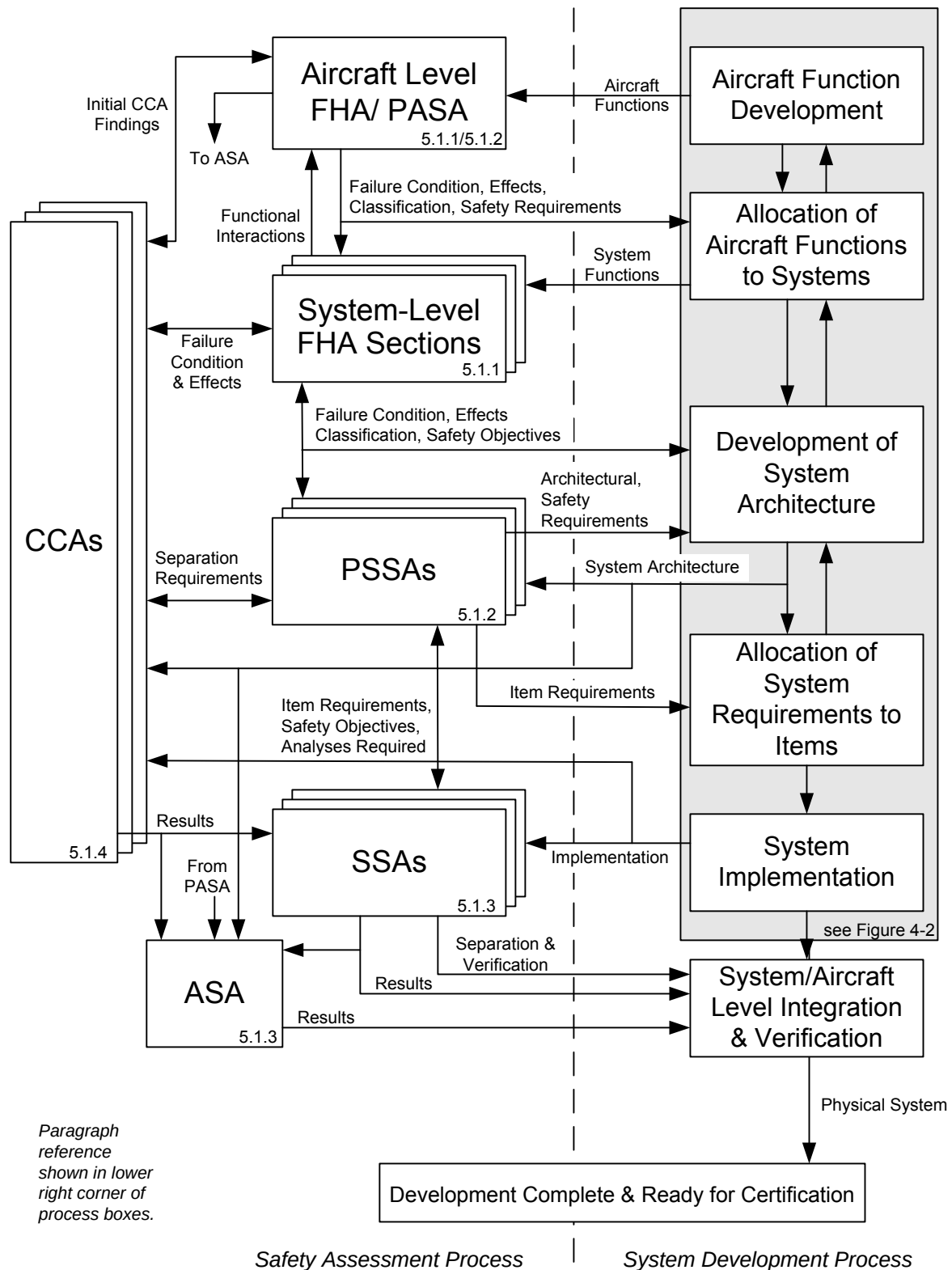


FIGURE 7 - SAFETY ASSESSMENT PROCESS MODEL

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 Analysis (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.