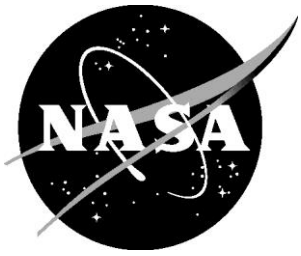
NASA/CR–2015-218982



Application of SAE ARP4754A to Flight Critical Systems

Eric M. Peterson
Electron International II, Inc., Phoenix, Arizona

November 2015

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

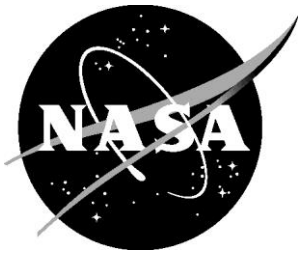
- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/CR–2015-218982



Application of SAE ARP4754A to Flight Critical Systems

Eric M. Peterson
Electron International II, Inc.; Phoenix, Arizona

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NNL13AA04B/NNL14AB74T

November 2015

Acknowledgments

This contract work was awarded by NASA under Contract No. FCSR-NNL13AA06B, Task Order No. NNL14AB74T. The NASA technical monitor for this task is Mr. Wilfredo Torres-Pomales.

EII Technical Team
Inder Verma
Bruce Vacey Jr.
Yu-Hsien Tu
Yiping Tao
Tom Garner

SAAB Sensis Team
Paul Davis
Stacy Candeias

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Table of Contents

Table of Figures

Table of Tables

Acronyms and Abbreviations

AC	Advisory Circular
AC/SYS LCP	Aircraft & Systems LCP (ARP4754A)
ACO	Aircraft Certification Office
AGPWS	Airborne Ground Proximity Warning System
AKA	Also Known As
AP	Autopilot
APP	Application
ARP	Aerospace Recommended Practice
ATA	Air Transport Association
ASA	Airplane Safety Assessment
CB	Circuit Breaker
CCB	Change Control Board
CDR	Critical Design Review
CFR	Code of Federal Regulations
CHGD	Changed
CM	Configuration Management
CN No.	Change Notice Number
CNTLLR	Controller
COMM	Communication
DAL	Development Assurance Level
DO	Generic term used in reference to RTCA “DO” identified documents
EE	Electronic Equipment
ESS	Essential
EWIS	Electrical Wiring Interface System
FADEC	Full Authority Digital Engine Controller
FC	Failure Condition
FDAL	Functional Development Assurance Level
FFS	Functional Failure Set
FHA	Functional Hazard Assessment
FMS	Flight Management System
GPS	Global Positioning System
HW	Hardware
HW LCP	Hardware Life Cycle Process
IDAL	Item Development Assurance Level
IMA	Integrated Modular Avionics
I/O	Input / Output
ITAR	International Traffic in Arms Regulations
LCP	Life Cycle Process
LRU	Line Replaceable Unit
MCDU	Multipurpose Control Display Unit
MoC	Means of Compliance
OEM	Original Equipment Manufacturer
PA	Process Assurance
PASA	Preliminary Aircraft Safety Assessment
PFD	Primary Flight Display
PHAC	Plan for Hardware Aspects of Certification
PROCS	Procedures
PSAC	Plan for Software Aspects of Certification
PSCP	Project Specific Certification Plan

PSSA	Preliminary System Safety Assessment
QA	Quality Assurance
R	Recommended
REQTS	Requirements
RI	Recommended with Independence
RWC	Reuse with Change
SAE	Society of Automotive Engineers
SCC	System Control (category)
SSA	System Safety Assessment
SSAT	System-wide Safety Assurance Technologies
SW	Software
SW LCP	Software Life Cycle Process
Sys	System
TBA	To Be Assigned
TSO	Technical Standard Order
V & V	Validation and Verification
VALDN	Validation
WX	Weather

1 Executive Summary

The effort described herein supports NASA's Aviation Safety Program's System-wide Safety Assurance Technologies (SSAT) Project, which is conducting research directed at improving the safety of current and future aircraft operating in the National Airspace System. Under SSAT a technical challenge has been raised that targets the assurance of flight critical systems – a technical challenge to address, among other things, the sound assurance of safety-critical distributed systems properties and the complex interactions between systems and subsystems.

There is an ongoing trend in the aviation industry of increasing adoption of ever more sophisticated computer-based technology to realize aircraft systems performing a wide variety of functions with different safety criticality levels. State-of-the-art aircraft avionics are network-centric systems of systems that are highly complex, software-intensive, and functionally integrated. The use of legacy components and multiple vendors to supply different functions that must share resources on a common distributed platform adds further complexity to these systems. The intricate patterns of interaction resulting from large-scale functional integration and distributed processing can expose a system to many non-intuitive failure mechanisms with a potential for severe safety-relevant effects. The level of rigor in the development process is determined by considerations of complexity and safety criticality. The predictability and robustness of the integrated system in the face of uncertainty in interactions and health status of components is of major importance in the "certifiability" of the system.

The SAE International (formerly the Society of Automotive Engineers [SAE]) Aerospace Recommended Practice (ARP) 4754, Revision A (hereafter ARP4754A) describes a recommended process-based development assurance framework for systems that implement and support aircraft-level functions.

The purpose of ARP4754A is to provide guidelines for the generation of evidence to substantiate with adequate confidence (i.e., assurance level) that errors in requirements, design, and implementation of the system have been identified and corrected and that the system satisfies the applicable certification regulations. ARP4754A states what objectives need to be accomplished based on system development assurance level (DAL) assignments, but it does not provide a justification for the guidelines and its application requires significant engineering judgment.

2 Scope, Motivation and Objectives of this Report

This report documents applications of ARP4754A to the development of modern computer-based (i.e., digital electronics, software and network-based) aircraft systems. This study is to offer insight and provide educational value relative to the guidelines in ARP4754A and provide an assessment of the current state-of-the-practice within industry and regulatory bodies relative to development assurance for complex and safety-critical computer-based aircraft systems.

The primary objectives of this study are to:

- Develop case studies on the application of ARP4754A to the development and assurance of computer-based aircraft systems with architecture level complexity representative of state-of-the-art technology,
- Generate guidelines on the application of ARP4754A to the development and assurance of computer-based aircraft systems and to,
- Identify issues of concern in the current guidance, policy, and practice (i.e., processes, methods, tools or techniques) of development and assurance for computer-based aircraft systems.

As the above objectives were being accomplished, additional topics were also addressed. The following areas of study are detailed in Appendices C and D:

- Justification for ARP4754A guidelines,
- How to transition from safety analysis to system architecture,
- Relationship between risk mitigation and ARP4754A,
- Development Assignment levels in AC23.1309.1E vs ARP4754A (AC 20-174), Differences – Why? Are the levels assigned equivalent?,
- Insight as to why Options 1 / 2 of ARP4754A Table 3 are equivalent,
- Engineering judgment,
    - ARP4754A requires significant engineering judgment – which parts,
    - How engineering judgment is leveraged / used in ARP4754A,
    - How to make up for “missing” engineering judgment for new comers in order to apply the recommended practice.

3 Case Study Scenario Development Summary

Three case studies on the development and assurance of computer-based aircraft systems (i.e., avionics) at the architecture level following the guidelines in ARP4754A were developed. The case studies captured the following characteristics:

- Are representative of current state-of-the-art systems in terms of complexity and safety criticality,
- Include examples of the application of the DAL assignment guidelines with system architecture consideration,
- Are performed at a level of detail that ensures educational value and allows insight into the sorts of development and assurance problems requiring engineering judgment,
- Enable the identification of issues of concern in the current guidance, policy, and practice of system development and assurance.

Appendix A captures the three scenarios developed in support of this study effort. Each scenario synopsizes the development activities to accomplish ARP4754A objectives and responds to the objectives identified above.

4 ARP4754A Application Guidelines Summary

Upon completion of the case studies outlined in section 3, development and assurance guidelines on the application of ARP-4754A based on lessons learned and insight gained in the course of performing the case studies were developed. These ARP4754A application guidelines provide insight into the rationale for development assurance level (DAL) assignments with system architecture consideration as well as consider the system complexity and safety criticality.

A review of the notes and activities associated with the case study developments identified a few general guidelines. Additional material derived from a questionnaire and roundtable discussions were collected from industry to enhance the lessons learned material. This additional solicited experience information is summarized in Appendix B.

The study results indicate that ARP4754A provides a systematic path for aircraft function design and development. It provides for early removal of errors resulting in less iteration to get a function design correct. The ARP establishes compatibility with the other industry standards and processes (DO-178, DO-254 and DO-297). Users advocate tailoring the activities outline in the ARP according to their individual scope of work and criticality of function being developed.

FDAL/IDAL Assignment Guidelines

For almost all development project scenarios, the functional development assurance level (FDAL) can and will be assigned using the functional hazard assessment classification with the assurance level assigned per ARP4754A Table 2 or ARP4754A Table 3 using the single member functional failure set (FFS) column. Most project developments, especially at the aircraft function level, provide minimum opportunity to use the functional independence attribute.

Similarly, the Item development assurance level (IDAL) will be assigned commensurate with the FDAL (and therefore the hazard) supported or implemented by the Item.

No special tools need to be used to assign the FDAL and IDAL. A common mode analysis (CMA) evaluates for satisfaction of the independence characteristics.

Engineering Judgment Guidelines

In general, the key engineering use areas in ARP4754A include planning, requirements capture and requirements validation. The requirement management objectives rely the most on engineering judgment. The generation of acceptable, clear, concise requirement text relies on experience and engineering judgment. Validation of requirements is primarily accomplished through the application of knowledgeable experience.

Aircraft Level: Optimum planning to support the ARP4754A objectives relies on substantial engineering judgment in order to organize the project into an efficient, executable development process which creates the necessary evidence. In conjunction with the planning efforts, establishing the initial certification position with regards to how the project will satisfy the development assurance objectives also relies heavily on engineering judgment.

System Level: Engineering judgment is a key element in the re-use of systems and/or items. The judgment experience is used in understanding the baseline system and item functionality so as to plan and implement the desired re-use evolution. The ability to determine the system functionality which is not changing and that which is changing as part of a new application optimizes the project efforts to satisfy ARP4754A development objectives and simplify the certification efforts.

Re-Use Guidelines

ARP4754A facilitates re-use but the advantages lie primarily at system and Item levels. Validation and verification objective activities can be minimized to those necessary for only new or changed requirements.

For aircraft manufacturers, evaluation and application of ARP4754A should be considered early in the development process. By actively contracting development of the airplane level avionic requirements from the system supplier re-applying the certificated system will help mitigate some of the aircraft level objective evidence that must be created on the new airplane for the “old” system.

5 ARP4754A Application Guidance, Policy or Practice Issues Summary

The study sought also to identify issues regarding current guidance, policy and practice of ARP4754A development and assurance of computer-based aircraft systems. The case study application insights and the author's previous lessons learned experiences in applying ARP4754A were used to identify and summarize these issues.

Issues with the current guidance, policies and practices were also solicited from Industry through a questionnaire and discussion roundtable as detailed in Appendix B. The following issues summarize the major concerns regarding the on-going invocation of ARP4754A.

ARP4754A Application Criteria

The primary issue identified by the industry responses was the certification authorities' inconsistent understanding and application of ARP4754A as part of the overall certification process, both within a single authority as well as between the various regulatory authorities worldwide. The certification authorities represented a divergence of opinion across projects on the depth and extent of ARP development process application as well as the acceptable evidence for showing objective satisfaction.

Industry participants were inconsistent on what would help mitigate these inconsistencies. Some respondents wanted a detailed checklist applied, similar to the DO-178 Job Aid, to create a level playing field. Other wanted acceptance of their existing processes as they are shown to satisfy the ARP objectives.

The level of certification authority involvement in the ARP development process, the inconsistency and alignment of ARP application and the ARP interpretation that "recommended" really means "required" were all highlighted as project obstacles. Finally, the late resolution of acceptable ARP4754A "compliance" evidence impacted timely project development.

FDAL/IDAL Assignment

All respondents of the questionnaire indicated a difficulty in applying the assurance level assignment process. A review of the examples provided in the questionnaire responses indicates that there remain problems differentiating between failure and error mitigation techniques. Confusion and misunderstandings were encountered during assignment interpretation. (It should be noted that only 25% of the respondents indicated that they had received training on the ARP). There were a number of examples of issues associated with assigning assurance level when the functional failure set included non-complex Items.

No special tools were used to aid in the assurance assignment level process. Error trees, fault trees and common mode analysis were used by some to visualize the development process architecture.

A number of respondents would like to see a "how to", step by step detailed explanation for FDAL and IDAL assignment.

ARP Application General

ARP4754A application requires a steep learning curve for those non-legacy ARP4754 literate industry members. General industry interpretation is that the ARP increases documentation efforts.

Validation of requirements is a problematic effort. First, there is the interpretation of the validation method table in the ARP, which seems to imply to some industry readers that a minimum of two methods are recommended in the absence of clear ARP text descriptions. Secondly, most design engineers have experience defining and verifying but not justifying their requirement set. This activity is viewed as being new and unfulfilling work. And finally, validation puts additional demands on the scarce experienced personnel resources.

A number of respondents would like to see more “how to” information in order to address the steep learning curve. “How To”:

- Satisfy the derived requirement review and analysis objective,
- Accomplish process assurance,
- Establish aircraft/system requirement standards to satisfy capture and validation objectives.

One ARP application observation of note was that it’s not just about what is being done but who does it as well. Expertise (skills and experience) matters.

6 Results and Recommendations

The industry questionnaire responses indicate that ARP4754A is viewed favorably by the engineering groups for development. The ARP establishes a structured process with known communications which was viewed positively. Company managements tended to view the ARP as only adding costs since they were not focused on reducing future project costs.

Industry was unanimous in wanting consistency in interpretation of the ARP across the certification authority environment.

ARP4754A and the Item development process standards (RTCA DO documents) form a consistent strategy to mitigate error sources in support of regulation compliance. The individual processes act in concert to provide a comprehensive safety development solution.

Recommendations

Certification authorities should study and implement an effective way of evaluating, within the certification framework, satisfaction of ARP4754A objectives. The goal of this activity should be to mitigate the existing large disparity in ARP interpretations during project application.

Industry should initiate an effort to synergize the objectives and configuration control criteria across the industry process documents. ARP4754A, DO-178, DO-254 and DO-297 differences lead applicants to apply the most severe common denominator across a project and thus are not optimizing the development objectives to support a common safety perspective.

More examples and “how to” information are also recommended to accelerate the learning curve of new ARP4754A applicants. It is worth noting that the current ongoing revision to ARP4761 will address some of industry identified issues. The details of how to assign FDAL/IDAL as well as identifying independence attributes and principles are being addressed.

The study scenarios herein also aid in addressing some industry comments in the application of ARP in during reuse scenarios (ARP4754A section 6). The equivalence of ARP4754A Table 3 options discussed herein may also help in the understanding of the FDAL/IDAL assignment process.

Appendix A Case-Study Data

Three different but related airplane development scenarios were developed and evaluated as part of the ARP4754A Task Study effort. These architecture level studies are synoptic in nature so as to focus on following the guidelines in ARP4754A while developing computer-based avionic airplane systems. The three case studies presented in this appendix accomplish the goals of the task including:

- Are representative of current state-of-the-art systems in terms of complexity and safety criticality,
- Include examples of the application of the DAL assignment guidelines with system architecture consideration,
- Are performed at a level of detail to provide educational value and allow insight into the sorts of development and assurance problems requiring engineering judgment,
- Have enabled the identification of issues of concern in the current guidance, policy, and practice of system development and assurance.

The three architecture scenarios developed represent examples of three different development cases presented in ARP4754A Section 6, “Modifications to Aircraft or Systems”. Each of the scenarios artifacts are uniquely identified with postulated configuration control strategies just as they would be on a “real” development program. The contents of each of the scenario developed ARP4754A artifact is presented in an abbreviated, outline format to highlight only the content needed to address the ARP objectives.

The scenarios include:

- Baseline Architecture,
- Study Architecture 1,
- Study Architecture 2.

Each of the scenarios is briefly described in the following paragraphs.

It should be noted that the intent of the case studies is to provide insight into satisfying ARP4754A development objectives for the scenarios postulated. The artifacts or process activities may not identify or address all representative certification aspects of the particular scenario.

BASELINE ARCHITECTURE

The baseline architecture captures the activities associated with development of a new airplane type to be certificated under 14CFR Part 25. The airplane itself is of conventional construction and conventionally controlled (non-electronic flight controls). The avionics suite to be included in the design is a re-application of an Integrated Modular Avionics (IMA) based avionic system previously certificated on a different airplane manufacturer's type airplane.

The functions included in the IMA avionics include:

- Autopilot (autoflight) (ATA22)[1],
- Communications (ATA23),
- Displays (ATA31),
- Navigation/Flight Management (ATA34),
- Maintenance (ATA45).

Note 1 - Air Transport Association function nomenclature has been used to enhance readability.

Artifact examples of the following airplane level ARP4754A objectives are developed:

- Airplane Certification Plan,
- Avionics Certification Plan,
- Avionics Development Plan,
- Avionic System Preliminary Aircraft Safety Assessment (PASA).

Artifact examples of the following system level ARP4754A objectives are developed:

- Avionic System Development Plan.

STUDY ARCHITECTURE 1

This architecture scenario captures the development of an update to an existing IMA avionic system implementation on the same legacy airplane as originally certificated. A revision to an existing IMA avionic function as well as the introduction of a new function to the IMA is explored. No airplane function changes are contemplated. The IMA system architecture, with the same initial function set, as that postulated in the baseline architecture scenario is used.

In this scenario, revision artifacts are developed for updates to one of the existing implemented functions (Flight Management (ATA34)) and for the addition of new functionality to the maintenance function (ATA45). The new function addition affects multiple elements within the implementation which are also explored.

Artifact examples of the following airplane level ARP4754A objectives are developed:

- Project Specific Certification Plan (PSCP).

Artifact examples of the following system level ARP4754A objectives are developed:

- Avionic System Development Plan.

STUDY ARCHITECTURE 2

This architecture scenario captures the development of an airplane and an existing IMA avionic system implementation update on a legacy airplane for the introduction of airborne ground proximity warning equipment (AGPWS) certificated to Technical Standard Order 92c (TSO-92c). The IMA system architecture, with the same function set, as that postulated in the baseline architecture scenario is used. Both airplane and avionic system changes are contemplated and developed.

In this scenario, revision artifacts are developed for updates to multiple existing functions due to the addition of the AGPWS TSO equipment.

Artifact examples of the following airplane level ARP4754A objectives are developed:

- Airplane Project Specific Certification Plan.

Artifact examples of the following system level ARP4754A objectives are developed:

- Avionic System Development Plan.

Appendix A.1 Baseline Architecture (aka SAAB-EII 100)

Introduction

An example of planning the development of flight deck functionality for a new airplane that uses an existing “certificated” avionic system from another airplane. For the purposes of this scenario development, the airplane is identified as the SAAB-EII 100 to provide a common reference framework for the development activities.

Example documentation developed:

Airplane Level

Airplane Certification Plan (CP010)
Avionics Certification Plan (CP100)
Avionics Development Plan (ADP100)
PASA CMA/Development Assurance assignment excerpt (SE100PASA)

Systems Level

Avionic System Development Plan (ASDP100)

Item Level

None – not a feature of study

NASA Study Baseline Architecture Example Study Excerpt	# SAAB-EII 100 ## Airplane Certification Plan			
ARP4754A 5.8.4.1	SIZE A	FSCM NO	DWG NO CP010	REV A
	SCALE 1 : 1		SHEET 1 OF 2	

REVISIONS				
CN No.	REV	DESCRIPTION	DATE	APPROVED
-	-	Initial release	2 Feb 2015	J Allen
46	A	Updated Figure 1 with revised document numbers.	18 Feb 2015	J Allen

Editor Note: Configuration control of the certification plan document is per system control category 1, under full problem report/change management process control.

A.1 CP010 1 System Description:

- New airplane type development, aka SAAB-EII 100.
- Certificated under 14CFR Part 25 as Transport Category airplane.
- Conventional aluminum construction.
- Two underwing mounted XYZ high thrust turbofan engines
- Conventional mechanical flight control system (ATA 27) certificated using conventional techniques defined in advisory material.
- Advanced avionics flight deck featuring LCD “glass” displays & IMA mechanization.

A.1 CP010 2 Certification Planning:

- This plan provides an overview of the certification activities for the SAAB-EII 100 to show compliance with the certification regulations.
- Certification will be accomplished by a series of aircraft function/system certification plans as shown in Figure 1. The following airplane function plans will be generated:

    - Avionics Certification Plan (CP100),
        - Includes FMS, Displays, Crew Alerting, Radios & Autopilot
    - Flight Control Certification Plan (CP200),
    - Electrical Power Certification Plan (CP300),
    - Hydraulics Certification Plan (CP400),
    - Environmental Control Certification Plan (CP500),
    - Water, Waste Certification Plan (CP600),
    - Thrust Management Certification Plan (CP700),
    - etc.

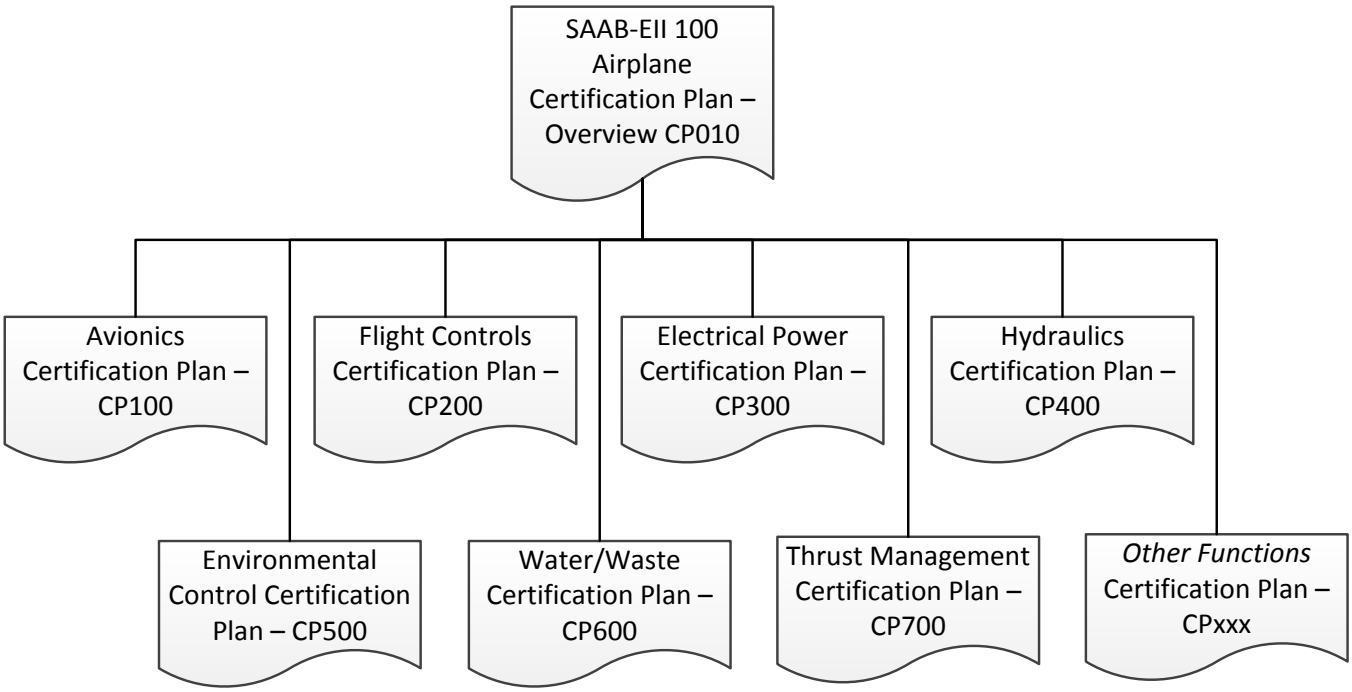


Figure 1 SAAB-EII-100 Certification Plan Hierarchy

A.1 CP010 3 FHA Summary:

- A summary of the planned airplane level functions is shown in Figure 2.
- Catastrophic and hazardous functional failure conditions will be identified for the SAAB-EII 100.
- See individual function/system plans for a summary of failure condition associated with each specific function area.

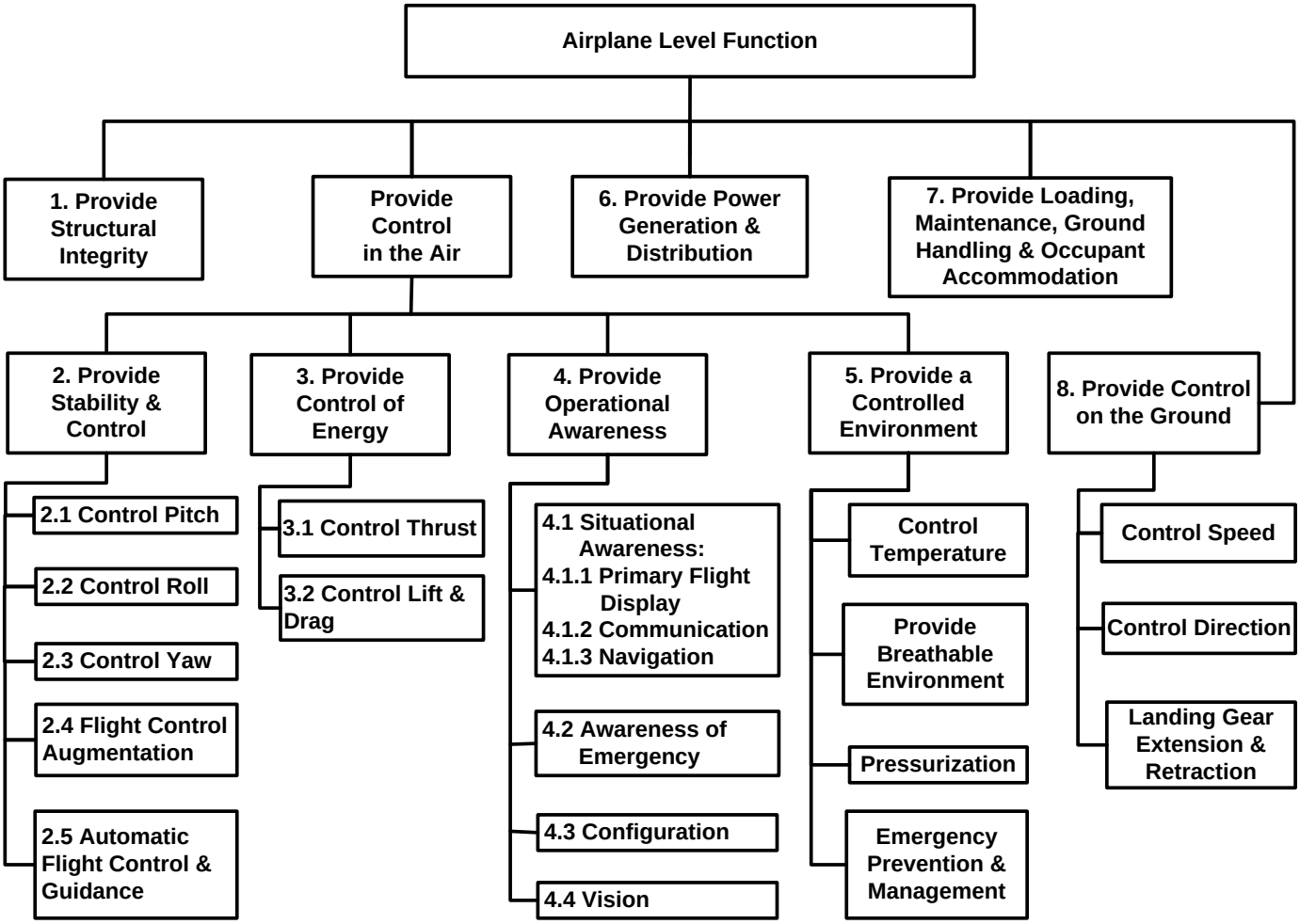


Figure 2 Airplane Function Diagram

A.1 CP010 4 Safety Objectives and Assurance Levels:

- The safety assessment process will follow the activities outlined in ARP4754A using the methods and tools described in ARP4761.
- Safety objectives will be identified from safety assessments and prior experience.
- Development assurance levels will be assigned as recommended in ARP4754A as advised in AC20-174 guidance material.
- See individual function/system certification plans (as noted in section 2) for the safety objectives and assigned functional development assurance levels (FDALs) associated with each function/system specific area.
- Safety Activities Management for the SAAB-EII 100 is outlined in the SAAB-EII 100 Safety Program Plan.

Editor Note: The Safety Program Plan was not developed as part of the scenario example artifacts.

A.1 CP010 5 Novel or Unique Design Features:

- Avionic system will be implemented using state-of-the-art IMA platform technology.
- See Avionics Certification Plan (CP100) for more details.

A.1 CP010 6 Certification Basis:

- SAAB-EII 100 airplane will be certificated to 14CFR Part 25:
  - Current amendments,
  - Current advisory material.

A.1 CP010 7 Compliance Methods:

- Compliance to the regulations will be shown by analysis, inspection and test.
- See individual function/system certification plans for regulations and compliance associated with each specific area.
- Summary for 14CFR 25.1309, Systems, equipment and installations:
  - Airplane function and system development process per AC20-174 using ARP4754A at assigned FDAL,
  - Airborne electronic hardware development per AC20-152 using DO-254 at assigned IDALs,
  - Airborne software development per AC20-115C using DO-178C at assigned IDALs,
  - Safety assessments (FHA, PSSA, SSA) per ARP4761.
- IMA development per AC-148 and AC-170.
- Airplane mechanical systems per AC25-21 and AC25-22.

--------End of CP010 Airplane Certification Plan Excerpt-------

NASA Study Baseline Architecture Example Study Excerpt	SAAB-EII 100 Avionics Certification Plan			
ARP4754A 5.8.4.1	SIZE A	FSCM NO	DWG NO CP100	REV -
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
CN No.	REV	DESCRIPTION	DATE	APPROVED
-	-	Initial release		

Editor Note: Configuration control of the certification plan document is per system control category 1, under full problem report/change management process control.

A.1 CP100 1 System Description:

The avionic system integrates the following airplane level functions into a single system implementation:

- Provide Stability & Control
  - Automatic Flight Control & Guidance,
- Provide Operational Awareness
  - Situational Awareness: Primary Flight Display, Communication, Navigation,
  - Awareness of Emergency
  - Configuration
- Provide Loading, Maintenance, Ground Handling & Occupant Accommodation
  - Maintenance.

The Company “A” Advanced Flight Deck integrates the following functions into a single avionic system implementation:

- Integrated Modular Avionics (IMA – ATA 42) (see Figure 3) from Company “A”
  - Company “A” IMA implementation certificated on other aircraft.
  - IMA includes the following functions:
    - Autopilot/Autoflight (ATA 22),
    - Communications (ATA23),
    - Displays (ATA31),
    - Navigation/Flight Management (ATA34), and
    - Maintenance (ATA 45).

A.1 CP100 2 Certification Support Planning:

- Certification will be accomplished by a series of airplane function certification plans.
- The Avionics Certification Plan (this document) defines the regulations and compliance methodology for the included avionic functions. This Avionics Certification Plan interacts with the following aircraft level function/system plans:
  - Flight Control Certification Plan (CP200),
  - Thrust Management Certification Plan (CP700),
  - Electrical Power Certification Plan (CP300),
  - etc.

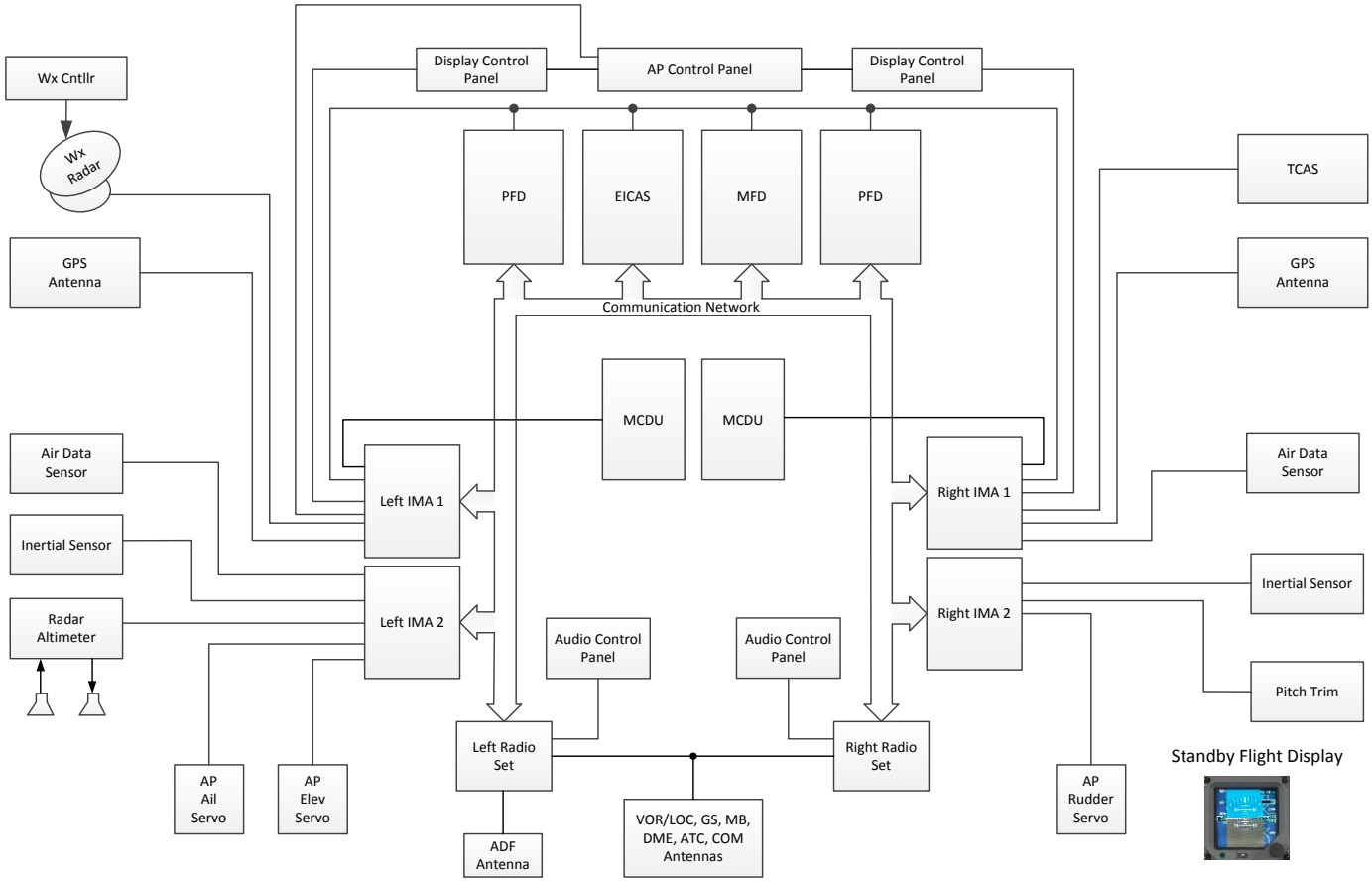


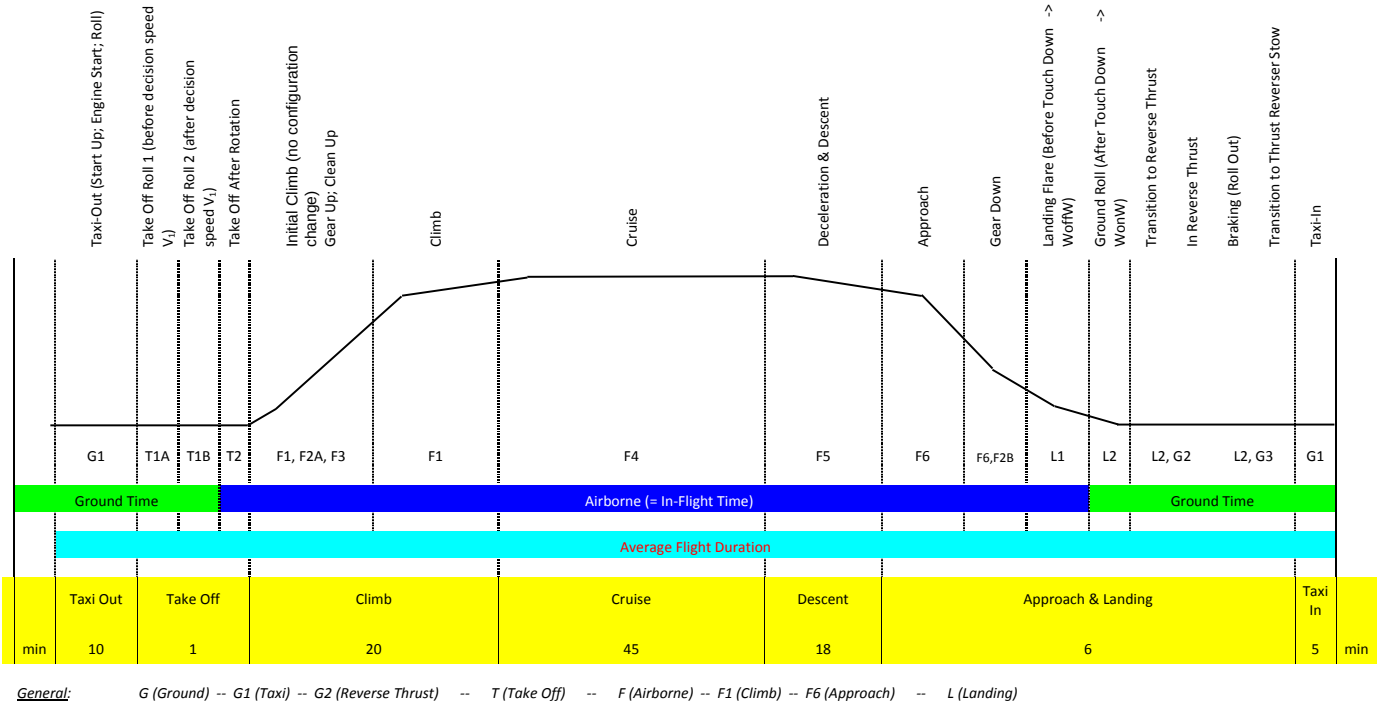
Figure 3 SAAB-EII 100 Avionics Architecture

A.1 CP100 3 FHA Summary:

- The associated average flight profile for the SAAB-EII 100 Airplane is presented in Figure 4 with flight phase description identified in Table 1.
- The functional failure conditions developed for the Avionic System are summarized in Table 2 (see SE100AVFHA for the full FHA analysis).

Editor's Note: SE100AVFHA was not developed as part of the scenario example artifacts.

Editor's Note: Normally, only the catastrophic and hazardous failure conditions would be included and summarized in the certification plan. Major and minor failure conditions have been included as part of this scenario development since they will be used later in the example.



General: *G (Ground) -- G1 (Taxi) -- G2 (Reverse Thrust) -- T (Take Off) -- F (Airborne) -- F1 (Climb) -- F6 (Approach) -- L (Landing)*

Figure 4 Average Flight Profile

Table 1 SAAB-EII 100 Flight Phase Descriptions

G - Ground		
G1	Taxi (General)	Pushback, ground taxi, takeoff runway align
G2	Reverse Thrust (General)	Weight on Wheels, high speed, reverse thrust & braking
G3	Braking (Roll Out)	Weight on Wheels, low speed, reverse thrust stow & braking
T - Take Off		
T1	Take Off (General)	Airplane aligned for Take Off, acceleration on ground through decision speed, rotation speed and rotate
T1A	Take Off Roll before V_1	Airplane on ground prior to decision speed V_1
T1B	Take Off Roll after V_1, before V_R	Airplane on ground after V_1 but before rotation speed V_R
T2	Take Off after Rotation	Nose gear off the ground (@ rotation speed V_R). T2 is the Phase between lift-off and the initiation of gear retraction. This time should be not less than 3 seconds and may be longer than 3 seconds if, on a particular airplane type, a longer delay is found to be appropriate (§25.111 (b)).
F - Flight		
F1	Climb (General)	Airborne flight after rotation, climb, capture altitude for cruise flight
F2A	Landing Gear Up	Gear retraction
F2B	Landing Gear Down	Gear extension
F3	Clean Up	Flap retraction, Climb configuration
F4	Cruise	Level flight at selected altitude(s)
F5	Descent	Deceleration, Descent to approach until flare transition
F6	Approach (General)	Landing configuration, gear down
GA – Go Around		
GA1	Go Around	Airborne flight transition from approach to clean up.
L - Landing		
L1	Landing Flare	Airplane transition approach - flare, Weight off Wheels
L2	Ground Roll	Airplane after Touch Down, Weight on Wheels, Thrust Reverse, active braking to taxi speed

Table 2, Avionic FHA Summary summarizes the following functional hazard assessment information:

Column 1: Description of the airplane level functional area

Column 2: Unique failure condition (hazard) tracking identification number

Column 3: Failure condition (hazard) description

Column 4: Flight phase(s) of interest for the postulated failure condition identified in column 3.

Column 5: Failure condition effects on airplane, occupants and crew qualitative description.

Column 6: Failure condition classification based on the descriptions entered in column 5.

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
Situational Awareness: Primary Flight Display (4.1.1)	31.01	Loss of all attitude display information in cockpit (including standby)	Flight	Crew is unable to determine correct airplane attitude using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.02	Display of misleading pitch or roll attitude to both pilots simultaneously (including standby)	Flight	Crew is unable to determine correct airplane attitude using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.03	Display of misleading pitch or roll attitude to one pilot.	Flight	Excessive crew workload. Crew must use cross-side display and standby attitude instrument to recognize condition.	Hazardous
	31.04	Loss of primary attitude display to both pilots	Flight	Significant increase in crew workload. Crew must rely on standby instrument for attitude reference information	Major
	31.05	Loss of all airspeed display information including standby airspeed	Flight	Crew is unable to determine correct airplane airspeed using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.06	Loss of primary airspeed display information to both pilots	Flight	Significant increase in crew workload. Crew must rely on standby instrument for airspeed reference information.	Major

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
	31.07	Erroneous standby airspeed display combined with airspeed miscompare on primary displays	Flight	Crew is unable to determine correct airplane airspeed using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.08	Erroneous airspeed displayed to both pilots simultaneously.	All	Excessive crew workload. Crew must use cross-check with standby airspeed instrument to recognize condition.	Hazardous
	31.09	Erroneous airspeed display information to one pilot	Flight	Significant increase in crew workload. Crew must use cross-side display and standby airspeed instrument to recognize condition.	Major
	31.10	Erroneous airspeed displayed on standby instrument	All	Significant increase in crew workload. Crew must use cross check with primary displays to recognize condition.	Major
	31.11	Loss of all altitude display information including standby altitude	Flight	Crew is unable to determine correct airplane altitude using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.12	Erroneous standby altitude display combined with altitude miscompare on primary displays	Flight	Crew is unable to determine correct airplane altitude using flight deck instruments resulting in loss of airplane.	Catastrophic
	31.13	Loss of primary altitude data to both pilots	Flight	Significant increase in crew workload. Crew must rely on standby instrument for altitude reference information.	Major
	31.14	Erroneous altitude display information to one pilot	Flight	Significant increase in crew workload. Crew must use cross-side display and standby altitude instrument to recognize condition.	Major
	31.15	Erroneous altitude displayed on standby instrument	All	Significant increase in crew workload. Crew must use cross check with primary displays to recognize condition.	Major
	31.16	Loss of all heading display information including standby heading	Flight	Crew is unable to determine correct airplane heading using flight deck instruments resulting in loss of airplane.	Catastrophic

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
	31.17	Loss of stabilized heading display information to both pilots	Flight	Significant increase in crew workload. Crew must rely on compass for heading reference information.	Major
	31.18	Erroneous heading display information to both pilots simultaneously	Flight	Significant increase in crew workload. Crew must recognize condition and rely on compass for heading reference information.	Major
	31.19	Loss of primary engine parameters display for both engines	Flight	Crew is unable to optimally control engine operation and must rely upon FADEC operation or displayed secondary engine parameters and independent airplane monitoring. Excessive crew workload.	Hazardous
	31.20	Loss of primary engine parameter display from a single engine	Flight	Significant increase in crew workload. Crew must rely on FADEC operation and throttle lever position.	Major
	31.21	Erroneous primary engine parameter displays for both engines	Take off	Excessive crew workload. Crew must control engines based on throttle lever position and rely on nominal FADEC control operation.	Hazardous
	31.22	Erroneous primary engine parameter displays from a single engine	Flight	Significant increase in crew workload. Crew must control engine based on throttle lever position and rely on nominal FADEC control operation.	Major
Situational Awareness: Communications (4.1.2)	23.01	Loss of all navigation and communication information (non-restorable)	Flight	Flight crew unable to navigate and communicate resulting in resulting in loss of airplane.	Catastrophic
	23.02	Loss of all communications	Flight	Loss of all voice and data communications from the airplane. Significant increase in crew workload. Crew must rely upon alternative navigation communication resources.	Major
	23.03	Erroneous datalink communication information	Taxi, Flight	Significant increase in crew workload. Crew verifies received datalink information via voice communications.	Major

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
Situational Awareness: Navigation (4.1.3)	34.01	Loss of navigation information display	Flight	Significant increase in crew workload. Crew must rely upon communication with air traffic control and backup heading display information to establish position.	Major
	34.02	Loss of navigation guidance information (flight management)	Flight	Significant increase in crew workload. Crew must manage flight plan through manual operation of navigation resources.	Major
	34.03	Erroneous display of navigational or positional information to both pilots simultaneously.	Take off, Approach	Excessive crew workload. Crew must identify positional error using other navigation sources or communications cross-checks.	Hazardous
	34.04	Erroneous display of radio altitude data to both pilots simultaneously.	Approach, Go Around	Crew makes hard landing due to misjudged or missing flare maneuver. Crew may recognize discrepancy with barometric altitude and/or glideslope presentation. Excessive crew workload.	Hazardous
	34.05	Erroneous Lateral Navigation	Flight	Significant increase in crew workload. Crew must identify positional error using other navigation sources or communications cross-checks.	Major
	34.06	Loss of Lateral Navigation – High altitude flight	Flight	Significant increase in crew workload. Crew must manage flight plan through manual operation of navigation resources.	Major
	34.07	Loss of Lateral Navigation – Low altitude flight	Approach, Landing, Go Around	Excessive crew workload. Crew must identify positional error using other navigation sources or communications cross-checks.	Hazardous
	34.08	Loss of or erroneous Vertical Navigation	Flight	Significant increase in crew workload. Crew must manage flight plan through manual operation of navigation resources.	Major

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
Situational Awareness: Emergency Awareness (4.2)	31.23	Loss of aural annunciation of caution or warning for identified conditions	Taxi, Flight	Crew must rely upon visual annunciations or other flight deck effects of caution and warning conditions.	Major
	31.24	Loss of visual display of caution or warning identified conditions	Taxi, Flight	Crew must rely upon aural annunciations or other flight deck effects of caution and warning conditions.	Major
	31.25	Erroneous display of caution or warning conditions	Taxi, Flight	Crew must rely upon cross-check of other flight deck information to identify erroneous/nuisance warning.	Major
	31.26	Loss of landing gear aural warning	Landing, Flight	Crew must rely upon redundant landing gear hand position and landing gear position indicators.	Major
Situational Awareness: Configuration (4.3)	31.27	Loss of take-off configuration warning combined with erroneous aircraft configuration	Take Off	Airplane is not in correct configuration for take-off resulting in loss of airplane.	Catastrophic
	31.28	Erroneous display of aircraft configuration	Take Off	Airplane is not in correct configuration for take-off resulting in loss of airplane.	Catastrophic
	31.29	Loss of take-off configuration warning	Take Off	Crew not notified if aircraft is not appropriately configured for takeoff. Configuration warning is auxiliary feature to supplement normal crew procedure.	Major

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
Provide Stability & Control: Automatic Stability & Control (2.5)	22.01	Erroneous engagement of autopilot at low altitude	Take off, Landing, Go Around	May reduce crew capability for controlling the airplane during specific maneuvers. Interference with crew control near the ground may jeopardize continued safe flight and landing.	Hazardous
	22.02	Erroneous autopilot disengagement at low altitude without annunciation	Approach, Landing, Go Around	Airplane deviates from planned vertical and/or lateral flight path and airspeed resulting in unsafe flight near to the ground until recognized by the crew. Airplane may land hard and/or short of runway due to incomplete or no flare. Landing gear or fuselage damage resulting in loss of airplane.	Catastrophic
	22.03	Erroneous autopilot command which exceeds authority limits	Flight	Airplane structural damage may result due to unrestricted pitch, roll or yaw commands. May result in rapid flight path responses, unsafe airplane flight paths and loss of altitude. Possible ground contact if occurs at low altitude resulting in loss of airplane.	Catastrophic
	22.04	Erroneous autopilot command with failure of override or disengagement capability	Flight	Unsafe airplane flight path due to inability of crew to regain control resulting in loss of airplane.	Catastrophic
	22.05	Loss of automatic stability & control capability (loss of autopilot)	Flight	Crew continues flight under manual control.	Major
	22.06	Loss of normal control surface capability due to erroneous operation of autopilot	Flight	Crew must recognize erroneous control behavior and coordinate autopilot disconnect with necessary autopilot function override forces to maintain desired flight path.	Major

Table 2 SAAB-EII 100 Avionics FHA Summary

1	2	3	4	5	6
Function	**FC #**	**Failure Condition (Hazard Description)**	**Flight Phase**	**Effect of Failure Condition on Aircraft/Crew**	**Classification**
Provide Stability & Control: Crew Control Guidance (2.5)	22.07	Loss of flight director commands, guidance cues.	Approach, Landing, Go Around	Crew may need to abort an instrument approach.	Major
	22.08	Erroneous flight director commands, displays and annunciations	Approach, Landing, Go Around	Crew follows erroneous commands until discrepancy detected through cross-checks with other flight deck visual cues.	Major
Maintenance (7)	45.01	Incorrect data loaded into avionics platform without detection	All	Possible incorrect functional operation of multiple avionic functions leading to incorrect crew airplane operation resulting in loss of airplane.	Catastrophic
Provide Control of Energy: Control Thrust (3.1)	33.01	Erroneous automatic thrust control performance prediction/thrust targets	Take-off	Potential inadequate takeoff thrust control settings. Crew manually adjusts engine performance during takeoff roll.	Major
	33.02	Erroneous takeoff data provided to FADECs	Take off	Potential inadequate takeoff thrust control settings. Crew must cross check displayed engine data against settings provided to FADEC.	Hazardous
	33.03	Loss of ability to automatically control thrust	Flight	Crew must manage energy through manual means.	Minor
	33.04	Erroneous automatic thrust control commands	Flight	Crew recognizes throttle reduction through aural and flight path deviation and takes over control of engines manually.	Major
	33.05	Erroneous automatic thrust control (retard)	Take off	Crew recognizes throttle reduction through aural and flight path deviation and takes over control of engines manually.	Major

A.1 CP100 4 Safety Objectives and Assurance Levels:

- Safety objectives will be established using ARP4761 safety activities.
- Development assurance per ARP4754A, commensurate with assigned functional development assurance levels, will ensure structured development mitigation of errors.
- Airplane safety activities managed in accordance with the airplane safety program plan.

A.1 CP100 5 Novel or Unique Design Features:

- Avionic system will be implemented using state-of-the-art IMA platform technology.

A.1 CP100 6 Certification Basis:

- The avionics functions for the SAAB-EII 100 airplane will be certificated to 14CFR Part 25;
  - Current amendments,
  - Current advisory material.

- Table 3 Applicable Regulations & Certification Plan Cross Reference identifies the regulations applicable to the avionics system functions including non-system specific regulations.
- A letter (e.g. “(a)”) included with the Applicable Certification Plan document number identifies a specific regulation sub-paragraph for which compliance is planned for demonstration in that certification plan.

Table 3 Applicable Regulations & Certification Plan Cross Reference

Regulation	Applicable Cert Plan Avionics	Others
SUBPART A - General		
General		
25.1 Applicability	CP100	
SUBPART B - FLIGHT		CP200
SUBPART C - STRUCTURE		CPxxx
SUBPART D – DESIGN & CONSTRUCTION		CP200, CPxxx
Design & Construction – General		
25.611 Accessibility provisions	CP100	
25.631 Bird strike damage	CP100	
Design & Construction – Control Systems		
25.672 Stability augmentation & automatic & power-operated systems	(a) CP100	CP200
25.677 Trim systems	(b) CP100	CP200
25.703 Takeoff warning system	CP100	CP200
SUBPART E – POWERPLANT		CPxxx
SUBPART F – EQUIPMENT		
General		
25.1301 Function and installation	CP100	CPxxx
25.1303 Flight and navigation instruments	CP100	
25.1305 Powerplant instruments	CP100	
25.1307 Miscellaneous equipment	CP100	
25.1309 Equipment, systems and Installation	CP100	(e) CP300
25.1310 Power Source Capacity and Distribution	(a) CP100	CP300
25.1316 System Lightning Protection	CP100	CP200, CPxxx
25.1317 High-intensity Radiated Fields (HIRF) Protection	CP100	CP200, CPxxx
25.1321 Arrangement and visibility	CP100	
25.1322 Flight crew alerting	CP100	CP200, CPxxx
25.1323 Airspeed indicating system	CP100	
25.1325 Static pressure systems	CP100	
25.1326 Pitot heat indication systems	CP100	
25.1327 Magnetic direction indicator	CP100	
25.1329 Flight guidance system	CP100	
25.1331 Instruments using a power supply	CP100	CP300
25.1333 Instrument systems	CP100	
25.1337 Powerplant instruments	CP100	
Electrical Systems and Equipment		CP300
Lights		CPxxx
25.1381 Instrument Lights	CP100	
Miscellaneous Equipment		
25.1431 Electronic equipment	CP100	CPxxx
SUBPART G – OPERATING LIMITATIONS and INFORMATION		
Operating Limitations		
25.1629 Instructions for Continued Airworthiness	CP100	CPxxx
Marking and Placards		
25.1541 General	CP100	

Table 3 Applicable Regulations & Certification Plan Cross Reference

Regulation	Applicable Cert Plan	
	Avionics	Others
25.1543 Instrument markings – general	CP100	
25.1545 Airspeed limitation information	CP100	
25.1549 Powerplant and auxiliary power unit instruments	CP100	
25.1551 Oil quantity indication	CP100	
25.1553 Fuel quantity indication	CP100	
25.1555 Control markings	CP100	
25.1563 Airspeed placard	CP100	
SUBPART H – ELECTRICAL WIRING INTERCONNECTION SYSTEMS (EWIS)		
25.1705 Systems and functions: EWIS	CP100	
25.1707 System separation: EWIS	CP100	
25.1709 System safety: EWIS	CP100	
25.1729 Instructions for Continued Airworthiness: EWIS	CP100	

Editor Note: In this example excerpt only the means of compliance for 25.1301 & 25.1309 (yellow highlight in Table 3*) have been developed. See* Table 4*.*

Compliance Methods

- Compliance to the regulations will be shown by analysis, inspection and test as identified in Table 4. The following means of compliance (MoC) summaries are used:
  - Inspection (may be on or off airplane, review),
  - Test (laboratory, ground, flight or equipment qualification),
  - Analysis (safety, simulation, numerical calculation).

- Table 4 Content Description:
  - Column 1 – Regulation number and sub-paragraph identification (as applicable).
  - Column 2 – Regulation text.
  - Column 3 – Compliance approach description, discussion of industry standards, advisory material used to support compliance.
  - Column 4 – Sequentially numbered list of the means of compliance. The sequential numbers match with compliance artifacts identified in Column 5.
  - Column 5 – Sequentially numbered list of compliance artifacts (e.g. documents, reports, analyses, inspections) which contain evidence of rule compliance.

- Development process at the airplane and system levels for the avionic system functionality will satisfy the objectives in ARP4754A.

- See the ***SAAB-EII 100 Avionics Development Plan*** for the details of the planned airplane level function and system development life cycle process.

- Note that Company “A” will be using similarity to satisfy ARP4754A development objectives at the system level for the evolution of their existing IMA avionic system to the SAAB-EII 100 airplane application.

Table 4 Avionics Function Means of Compliance (MoC) Matrix				
1	**2**	**3**	**4**	**5**
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
25.1301	Function and installation			
	Each item of installed equipment must –			
(a)	(1) Be of a kind and design appropriate to its intended function	The Avionics system operation will be described in a System Description Document and demonstrated to be appropriate for its intended function through inspection, analysis and test. AC20-115C – Airborne Software Assurance AC-152 – DO-254, Design Assurance Guidance for Airborne Electronic Hardware AC20-145 Guidance for Integrated Modular Avionics (IMA) that Implement TSO-C153 Authorized Hardware Elements AC20-148 – Reusable Software components AC20-170 Change 1 – Integrated Modular Avionics Development, Verification, Integration and Approval using DO-297 & TSO C153 AC20-174 - Development of Civil Aircraft and Systems ARP4754A – Guidelines for Development of Civil Aircraft and Systems	1 2 Inspection 3 Test 4 Inspection 5 Inspection, Analysis 6 Inspection 7 Inspection, Analysis 8 Inspection	1 SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 Avionics IMA Qualification Test Reports 4 Avionics IMA PHACs 5 Avionics IMA CEH deliverables 6 Avionics IMA PSACs 7 Avionics IMA software deliverables 8 Avionics equipment assembly drawings

Table 4 Avionics Function Means of Compliance (MoC) Matrix

1	2	3	4	5
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
		DO-178C – Software considerations in Airborne Systems & Equipment Certification DO-254 – Design Assurance Guidance for Airborne Electronic Hardware DO-297 – Integrate Modular Avionics (IMA) Development Guidance and Certification Considerations		
	(2) Be labeled as to its identification, function, or operating limitations, or any applicable combination of these factors	All equipment will be labeled for identification and function. Any identified operating limitations will be included as placards or as part of the airplane flight manual.	1 2 Inspection 3 Inspection 4 Inspection	1 SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 Avionics equipment assembly drawings 4 Airplane Flight Manual
	(3) Be installed according to limitations specified for that equipment; and	Equipment will be installed as specified on SAAB-EII 100 airplane and Avionics Company “A” installation drawings.	1 Inspection	1 Avionics equipment assembly drawings
	(4) Function properly when installed	Equipment will be tested on ground and airborne for correct function operation.	1 Test 2 Test	1 Flight Test Certification Report 2 Ground Test Certification Report
(b)	EWIS must meet the requirements of subpart H of this part	See Subpart H for complete EWIS compliance approach and MoC statements.		

Table 4 Avionics Function Means of Compliance (MoC) Matrix

1	2	3	4	5
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
25.1309	Equipment, systems and installations			
(a)	The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.	The Avionics system operation will be described in an Airplane Flight Manual, System Description Document and demonstrated to be appropriate for its intended function through inspection, analysis and test. AC20-115B – Airborne Software Assurance AC-152 – DO-254, Design Assurance Guidance for Airborne Electronic Hardware AC20-145 Guidance for Integrated Modular Avionics (IMA) that Implement TSO-C153 Authorized Hardware Elements. AC20-148 – Reusable Software components AC20-170C1 – Integrated Modular Avionics Development, Verification, Integration and Approval using DO-297 & TSO C153.	1 2 Inspection 3 Test 4 Inspection 5 Inspection, Analysis 6 Inspection 7 Inspection, Analysis 8 Inspection	1 SAAB-EII 100 Airplane Flight Manual SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 Avionics IMA Qualification Test Reports 4 Avionics IMA PHACs 5 Avionics IMA CEH deliverables 6 Avionics IMA PSACs 7 Avionics IMA software deliverables 8 Avionics equipment assembly drawings
(b)	The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that – (1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and	The Avionics Safety Analysis will show through analysis that the occurrence of any failure conditions which would prevent safe flight and landing are extremely improbable and that other failure conditions which reduce the capability of the airplane or crew to cope with adverse operating conditions are improbable.	1 2 Inspection 3 Analysis	1 SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 SAAB-EII 100 Airplane Safety Analysis (ASA) - Avionics

Table 4 Avionics Function Means of Compliance (MoC) Matrix

1	2	3	4	5
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
	(2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.	AC20-174 Development of Civil Aircraft and Systems ARP4754A – Guidelines for Development of Civil Aircraft and Systems AC/AMJ25.1309 System Design and Analysis, RTCA Draft Arsenal revised 2002		
(c)	Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards	Warnings will be provided to the crew for unsafe operating conditions and to enable corrective actions. The warning system will be designed to minimize crew errors to mitigate creating additional hazards. Warnings for specific airplane and system failure conditions will be evaluated through simulation as well as ground and airborne test.	1 2 Inspection 3 Test 4 Test 5 Test	1 SAAB-EII 100 Airplane Flight Manual SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 Avionics Certification Lab Test Report 4 Flight Test Certification Report 5 Ground Test Certification Report

Table 4 Avionics Function Means of Compliance (MoC) Matrix

1	2	3	4	5
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
(d)	Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider— (1) Possible modes of failure, including malfunctions and damage from external sources. (2) The probability of multiple failures and undetected failures. (3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and (4) The crew warning cues, corrective action required, and the capability of detecting faults.	The Avionics Safety Analysis will evaluate through analysis system failures and combinations of failures in support of the regulatory objectives identified in paragraph (b). This analysis will be supplanted by ground, flight and simulator testing for specific failures and/or failure combinations. AC20-174 Development of Civil Aircraft and Systems AC/AMJ25.1309 System Design and Analysis, RTCA Draft Arsenal revised 2002	1 2 Inspection 3 Analysis 4 Test 5 Test 6 Test	1 2 Avionics Certification Summary 3 SAAB-EII 100 Airplane Safety Analysis (ASA) - Avionics 4 Avionics Certification Lab Test Report 5 Flight Test Certification Report 6 Ground Test Certification Report

Table 4 Avionics Function Means of Compliance (MoC) Matrix

1	2	3	4	5
Regulation	**Regulation Text**	**Compliance Approach**	**MoC**	**Compliance Artifacts**
(e)	In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft.	The Avionics system electrical power sources will be designed, qualified and installed to comply with these objectives. The electrical power system will be described in the Airplane Flight Manual and the Avionics System Description Document. Electrical generation and distribution compliance to this paragraph is provided in the Electrical Power Certification Plan, CP300. AC20-174 Development of Civil Aircraft and Systems AC/AMJ25.1309 System Design and Analysis, RTCA Draft Arsenal revised 2002	1 2 Inspection 3 Analysis 4 Test	1 SAAB-EII 100 Airplane Flight Manual SAAB-EII 100 Avionics System Description 2 Avionics Certification Summary 3 SAAB-EII 100 Airplane Safety Analysis (ASA) - Avionics 4 Avionics IMA Qualification Test Reports
(f)	EWIS must be assessed in accordance with the requirements of §25.1709.	The Avionics System Safety Analysis will include the associated airplane wiring system as one of the functional elements being assessed for showing compliance to this requirement.	1 Inspection 2 Analysis	1 Avionics Certification Summary 2 SAAB-EII 100 Airplane Safety Analysis (ASA) - Avionics

------End of CP100 Airplane Avionics Certification Plan Excerpt-------

NASA Study Baseline Architecture Example Study Excerpt	# SAAB-EII 100 # Avionics Development Plan			
ARP4754A 5.8.4.3	SIZE A	FSCM NO	DWG NO ADP100	REV A
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
	REV	DESCRIPTION	DATE	APPROVED
	-			
	A	Revised figure 6 to separate maintenance level testing requirements into two independent sets. See Figure 7.	18 Feb 2015	

Editor Note: Configuration control of avionics development plan document is per system control category 2, using version change management process control.

A.1 ADP100 1 Introduction:

- This Plan describes the airplane level development process for avionics functions to be installed on the SAAB-EII 100 airplane.
- Plan addresses engineering life cycle including function design, requirements generation, analysis, requirements validation, function verification.
- Plan includes the identification and assignment of the appropriate Functional Development Assurance Level (FDAL) rigor to be performed at the airplane level as well as the flow down system tiers.

A.1 ADP100 2 Avionics Development Overview:

- The avionics development process will ensure support of the certification process outlined in CP100.
- The avionics development process is structured to ensure satisfaction of ARP4754A objectives commensurate with the rigor of the assigned development assurance level (FDAL).
- The avionics development process is based on re-use of an integrated modular avionic implementation certificated on another airplane.
- The SAAB-EII 100 avionics development process will generate the necessary project artifacts for the airplane functionality to support the existing Company “A” Advanced Flight Deck functions as well as generating the documentation needed to define unique SAAB-EII 100 airplane characteristics (e.g. interfaces, functional properties, installations).
- Figure 5 presents a high level summary of the Avionics development activities. It should be noted that the non-linear aspects of the development activities (feedback paths) are not shown.

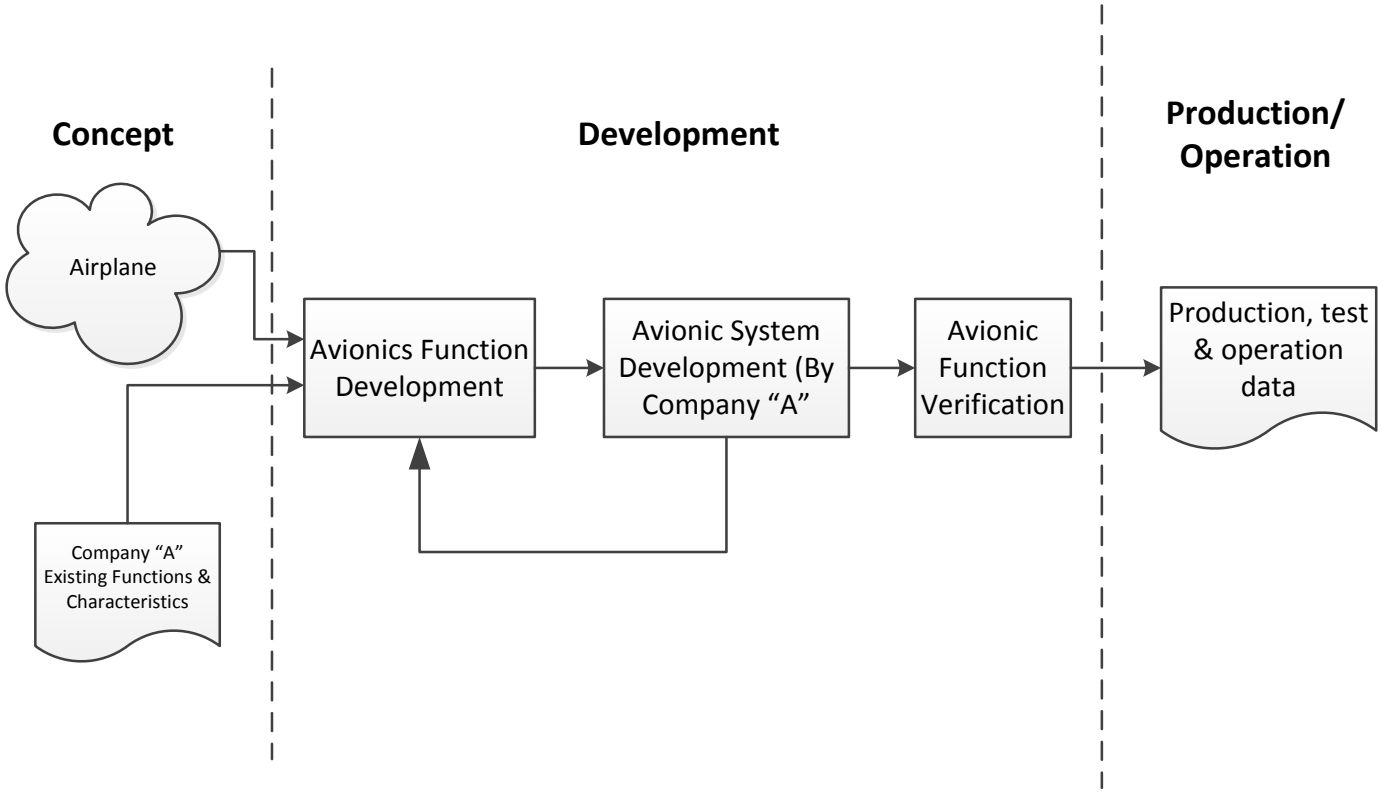


Figure 5 Avionic System Development Requirement Activities

A.1 ADP100 3 System Description:

Avionics Flight deck will include Company “A” Advanced Flight Deck which integrates multiple avionic functions into a single system implementation:

- Integrated Modular Avionics (IMA – ATA 42) from Company “A”
  - Company A IMA implementation certificated on other aircraft.
  - IMA includes the following system functions:
    - Autopilot/autoflight (ATA 22),
    - Communications (ATA23),
    - Displays (ATA31),
    - Navigation/Flight Management (ATA34), and
    - Maintenance (ATA 45).

A.1 ADP100 4 Avionics Function Requirements Development:

- Airplane Avionic function requirements will be captured and validated for the following functions:
  - Autopilot/autoflight (ATA 22),
  - Communications (ATA23),
  - Displays (ATA31),
  - Navigation/Flight Management (ATA34), and
  - Maintenance (ATA 45).

- Airplane Avionic Function Development initial life cycle is shown in Figure 6.
- Airplane Avionics Development ARP4754A objective activities accomplished to the level of rigor assigned for each function.
- See Table 5 FDALs assigned based on results identified in Avionics PASA (Document SE100PASA), section FDAL Assignment.
- Airplane Avionic Function Development life cycle post PASA recommended updates shown in Figure 7.

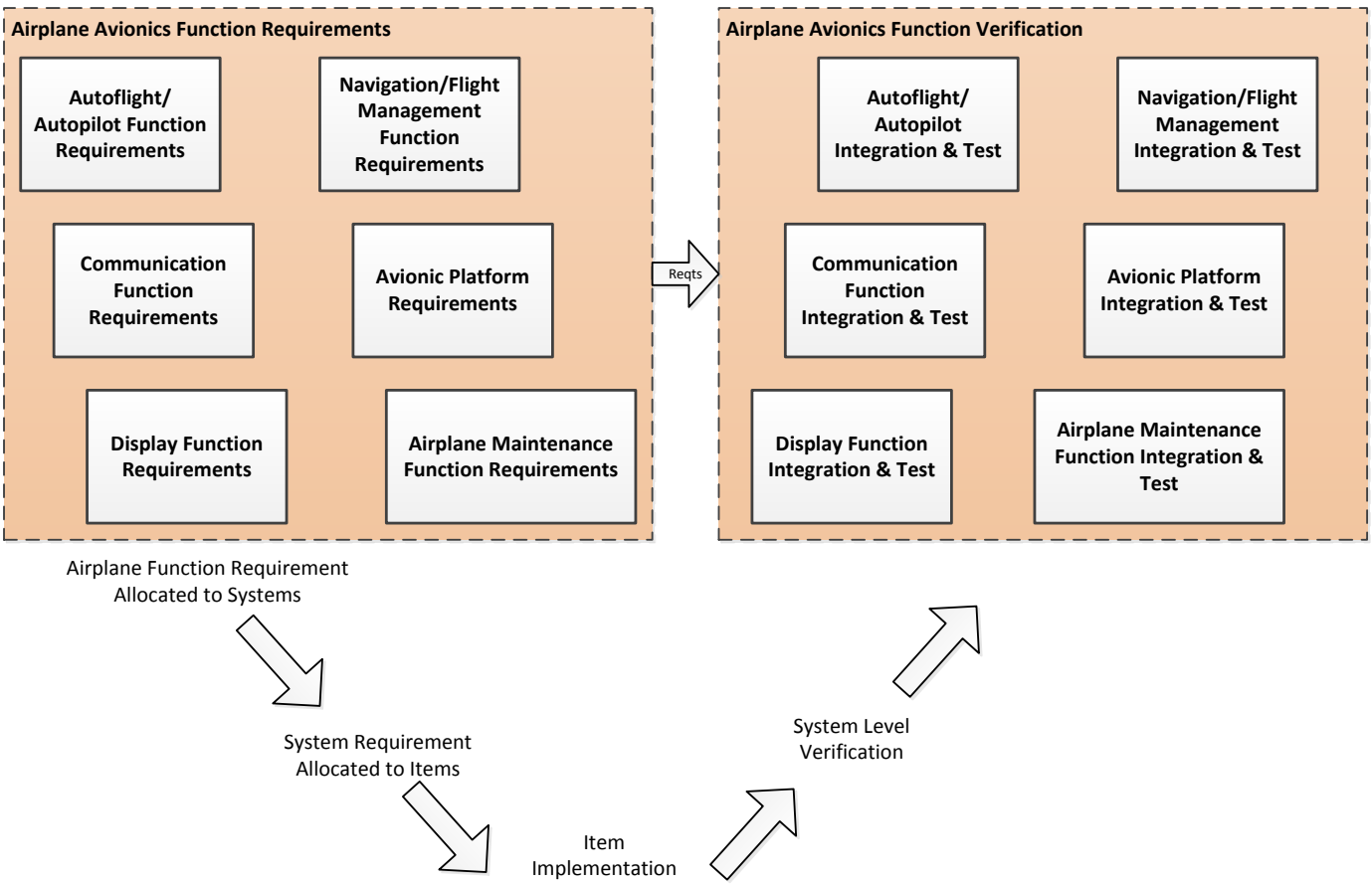


Figure 6 Airplane Avionic Function Development Life Cycle - Initial

Table 5 SAAB-EII 100 Avionic Function FDAL Assignments

Avionic Function	FDAL
Autopilot/Autoflight (ATA22)	A
Communications (ATA23)	A
Displays (ATA31)	A
Navigation/Flight Management (ATA34)	B
Maintenance (ATA45)	
Maintenance A Testing & Data/Program Loading	A
System(s) Maintenance Testing	D
Platform	A

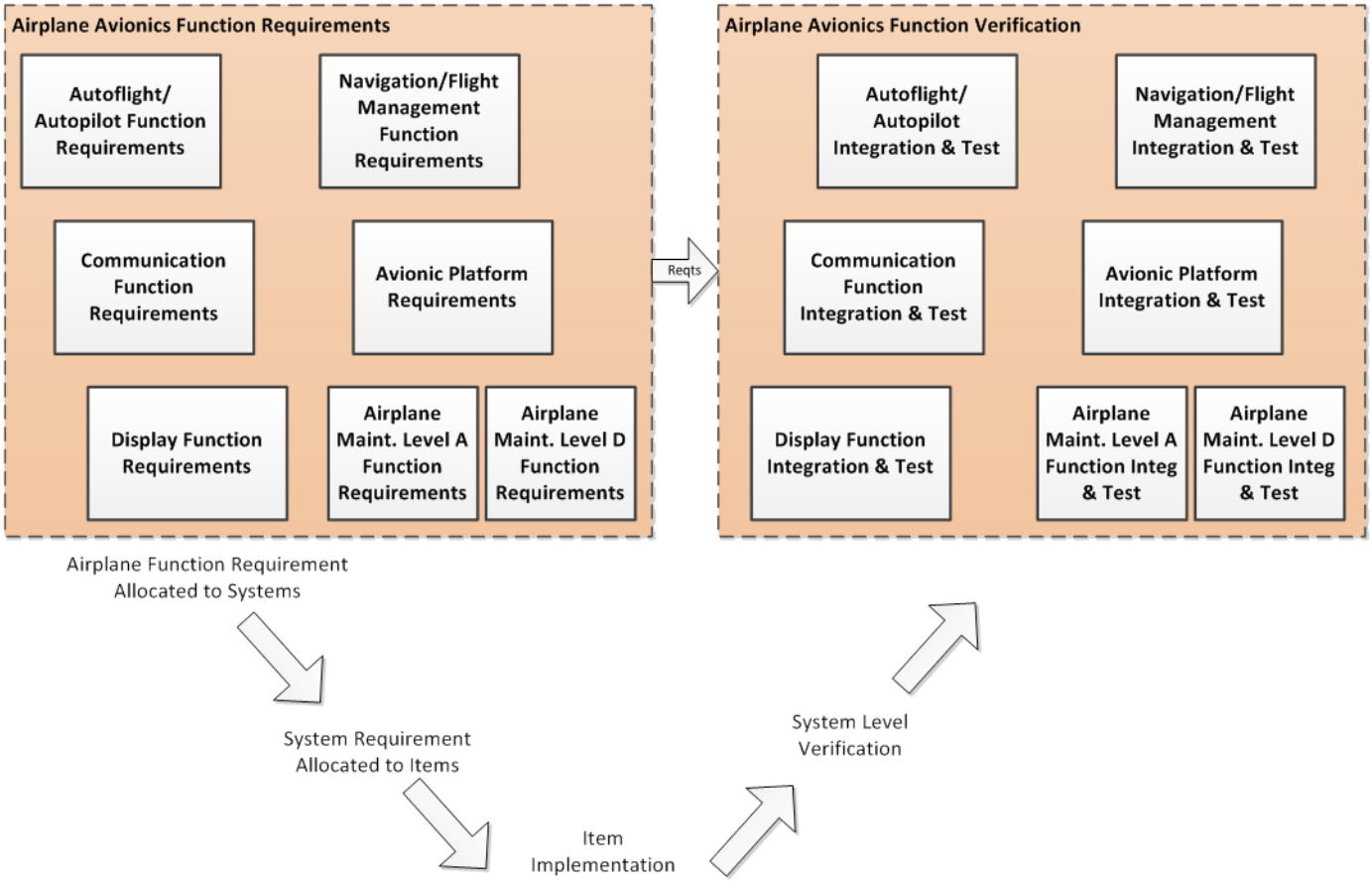


Figure 7 Airplane Avionic Function Development –Life Cycle - Post PASA

A.1 ADP100 4.1 Requirements Capture & Validation:

- Requirements for each of the avionic functions will be captured and managed independently but may be combined into a single document structure for transmittal to the avionic system supplier.
  - Maintenance function development further split into Level A maintenance and Level D maintenance to facilitate different criticalities and optimize project development activities.
- Requirements captured using database style requirements documentation tool.
- Requirements validated using process and techniques outlined in ARP4754A.
  - Requirements validated using combination of methods:
  - Methods of validation include:
    - Traceability,
    - Analysis,
    - Test,
    - Modeling or,
    - Inspection (engineering review).

A.1 ADP100 4.2 Avionic Function Verification:

- Verify avionic system implementation satisfies captured airplane level requirements.
- Airplane Level Requirements verified using process accomplishing objectives of ARP4754A.
    - Function requirements verified using a combination of methods.
    - Methods of verification include:
        - Inspection (engineering review),
        - Analysis and,
        - Test (demonstration).
- Avionic safety assessments accomplished by integrating Company “A” avionic safety assessment data into Airplane Safety Group generated SAAB-EII 100 Airplane Safety Assessment.
- Preferred method of avionic function verification will be test.
- Requirements based functional verification procedures will be developed and executed against the final installed avionics functions, on ground and in-flight.

A.1 ADP100 5 ARP4754A Objectives Mapping:

- Table 6 presents a high level mapping of ARP4754A objectives to program artifacts which provide evidence for satisfaction of the ARP objectives.

Table 6 Avionics System ARP4754A (Appendix A) Summary of Objectives Mapping

ARP4754A			**SAAB-EII 100**
Objective Ref No	**Objective Description**	**Output**	**Reference Data**
1.0 Planning			
1.1 / 1.2	System development and integral processes activities are defined and include transition criteria and interrelationships.	Certification Plan	SAAB-EII 100 Certification Plan,CP010 Avionics Certification Plan, ACP100
		Safety Program Plan	*Avionics Safety Program Plan, Doc # TBA*
		Development Plan	Avionics Development Plan, ADP100 (this document)
		Validation Plan	
		Verification Plan	
		Configuration Management Plan	*Doc # TBA*
		Process Assurance Plan	*Doc # TBA*
2.0 Aircraft and System Development Process and Requirements Capture			
2.1	Aircraft-level functions, functional requirement, functional interfaces and assumptions are defined	List of Aircraft-level functions Aircraft-level Requirements	*SAAB-EII 100 Avionics Function Requirements, Doc # TBA*
2.2	Aircraft functions are allocated to systems	System Requirements	Company “A” objective
2.3	System requirements, including assumptions and system interfaces are defined.	System Requirements	
2.4	System derived requirements (including derived safety-related requirements) are defined and rationale explained.	System Requirements	
2.5	System architecture is defined.	System Design Description	
2.6	System requirements are allocated to the items.	Item Requirements	
2.7	Appropriate item, system and aircraft integrations are performed.	Verification Summary	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA*
3.0 Safety Assessment Process			
3.1	The aircraft/system functional hazard assessment is performed.	Aircraft FHA System FHA	SAAB-EII 100 Airplane (Avionics) FHA, SE100AvFHA Avionic System FHA is Company “A” objective.
3.2	The preliminary aircraft safety assessment is performed.	PASA	SAAB-EII 100 Preliminary Aircraft Safety Assessment (PASA), SE100PASA
3.3	The preliminary system safety assessment is performed.	PSSA	Company “A” objective

ARP4754A			SAAB-EII 100
Objective Ref No	**Objective Description**	**Output**	**Reference Data**
3.4	The common cause analyses are performed.	Particular Risk Assessment	*Docs TBA*
		Common Mode Analysis	SAAB-EII 100 Preliminary Aircraft Safety Assessment (PASA), SE100PASA
		Zonal Safety Analysis	*Docs TBA*
3.5	The aircraft safety assessment is performed.	ASA	*SAAB-EII 100 Airplane Safety Assessment (ASA), SE100ASA*
3.6	The system safety assessment is performed.	SSA	Company "A" objective
3.7	Independence requirements in functions, systems and items are captured	System, HW, SW Requirements PASA PSSA	SAAB-EII 100 Preliminary Aircraft Safety Assessment (PASA), SE100PASA provides airplane level PSSA is Company "A" objective
4.0 Requirements Validation Process			
4.1	Aircraft, system, item requirements are complete and correct.	Validation Results	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA* *System level – See Company "A" artifacts*
4.2	Assumptions are justified and validated	Validation Results	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA*
4.3	Derived requirements are justified and validated.	Validation Results	
4.4	Requirements are traceable.	Validation Results	
4.6	Validation compliance substantiation is provided.	Validation Summary (including Validation Matrix)	
5.0 Implementation Verification Process			
5.1	Test or demonstration procedures are correct.	Verification Procedures	*Avionics Function Verification Procedures, Doc # TBA*
5.2	Verification demonstrates intended function and confidence of no unintended function impacts to safety.	Verification Procedures	
		Verification Results	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA* *Flight Test Certification Report* *Ground Test Certification Report*

ARP4754A			SAAB-EII 100
Objective Ref No	**Objective Description**	**Output**	**Reference Data**
5.3	Product implementation complies with aircraft, and system requirements.	Verification Procedures	*Avionics Function Verification Procedures, Doc # TBA*
		Verification Results	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA* *Flight Test Certification Report* *Ground Test Certification Report*
5.4	Safety requirements are verified.	Verification Procedures and Results ASA, SSA	*Avionics Function Verification Procedures, Doc # TBA* *Airplane level – Avionics Function Validation & Verification Report, Doc # TBA*
5.5	Verification compliance substantiation is included.	Verification Matrix	*Airplane level – Avionics Function Validation & Verification Report, Doc # TBA* *Flight Test Certification Report, Doc # TBA* *Ground Test Certification Report, Doc # TBA*
		Verification Summary	
5.6	Assessment of deficiencies and their related impact on safety is identified.	Verification Summary	
		Problem Reports	
6.0 Configuration Management Process			
6.1	Configuration items are identified.	CM Records	*Title and Doc # TBA*
6.2	Configuration baseline and derivatives are established.	Configuration Baseline Records	
6.3	Problem reporting, change control, change review, and configuration status accounting are established.	Problem reports CM Records	
6.4	Archive and retrieval are established.	CM Records	
7.0 Process Assurance Process			
7.1	Assurance is obtained that necessary plans are developed and maintained for all aspects of system certification.	Evidence of Process Assurance	*Title and Doc # TBA*
7.2	Development activities and processes are conducted in accordance with those plans.	Evidence of Process Assurance	

-------- End of ADP100 Avionics Development Plan Excerpt-------

Title	SAAB-EII 100 PASA	Doc No.	SE100PASA	Date	4/24/2015

NASA Study Baseline Architecture Example document excerpt.	# SAAB-EII 100 ## Avionic System Preliminary Aircraft Safety Assessment (PASA)			
ARP4754A 5.1.2	SIZE A	FSCM NO	DWG NO SE100PASA	REV -
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
CN No.	REV	DESCRIPTION	DATE	APPROVED
	-	Initial release	12 Feb 2015	

Editor Note: Configuration control of safety document is per system control category 1, under full problem report/change management process control. Background color used to highlight this as safety assessment document.

Editor Note: Extract contains only the PASA information pertinent to FDAL assignment.

Avionic System PASA Section FDAL Assignment

- Avionics Functionality – Table PASA-1 Columns 1 and 2 summarize failure conditions and classifications from *SE100AVFHA*.
- Table PASA-2 Column 3 identifies assigned FDAL based only on single failure condition classifications.
- Table PASA-1 Column 4 highlights where the PASA-CMA has identified that independence characteristics exist such that the FDAL assignment may take credit for architectural error mitigation. The assignment is based on the Failure Condition Classification and the existence of functional independence. Functional independence is established if the development exhibits different functions with different requirements.
- Table PASA-1 Column 5 identifies assigned FDAL based on an evaluation of the independence characteristics associated with the development process need to support each Avionic Function. The assigned FDAL is based on most severe failure condition being supported. In this case, multiple catastrophic FCs will be implemented resulting in the common hardware and software functionality requiring FDAL A assurance.

Table 7 PASA-1 Avionic Functions FDAL Assignment

1	2	3	4	5
Avionic Function FC ID Numbers	**FC Classification**	**FC FDAL**	**Functional Independent Attribute (Y/N)**	**Assigned FDAL**
Autopilot/Autoflight (ATA22)			**N**	**A**
22.02, 22.03, 22.04	Catastrophic	A		
22.01	Hazardous	B		
22.05, 22.06, 22.07, 22.08	Major	C		
Communications (ATA23)			**N**	**A**
23.01	Catastrophic	A		
23.02, 23.03	Major	C		
Displays (ATA31)			**N**	**A**
31.01, 31.02, 31.05, 31.07, 31.11, 31.12, 31.16, 31.27, 31.28	Catastrophic	A		
31.03, 31.08,31.19, 31.21	Hazardous	B		
31.04, 31.06, 31.09, 31.10, 31.13, 31.14, 31.15, 31.17, 31.18, 31.20, 31.22, 31.23, 31.24, 31.25, 31.26, 31.29	Major	C		
Navigation/Flight Management (ATA34)			**N**	**B**
34.03,31.04, 31.07	Hazardous	B		
34.01, 34.02, 31.05, 31.06, 34.08	Major	C		
Maintenance (ATA45)			**N[1]**	**A & D[1]**
45.01	Catastrophic	A		
45.xx	Minor	D		
Platform			**N**	**A[2]**
Multiple FC IDs				

Note 1: Development process for Maintenance functionality will need to be partitioned during the development life cycle so that maintenance functions supporting multi-assurance levels may be accomplished **OR** all maintenance functionality must be developed to FDAL A.

Editor's Note: The independence requirements summarized in the PASA Section CMA to follow were developed through evaluation of the planned avionic architectural implementation using fault tree analysis, dependency diagrams or other requirement identification techniques. The use of "independence" conforms to the definition identified in ARP4754A (1) – "concept which minimizes the likelihood of common mode errors and cascade failures".

Avionic System PASA Section CMA

Independence Requirement Summary:

1. Display of Primary Attitude information shall be independent of standby attitude information
2. Display of Primary Airspeed information shall be independent of standby airspeed information.
3. Display of Primary Altitude information shall be independent of standby airspeed information.
4. Display of Primary Heading information shall be independent of standby airspeed information.
5. Left engine parameter displays shall be independent of right engine parameter displays.
6. Navigation capability shall be independent of communication capability.
7. Captain displayed navigation/position information shall be independent of First Officer displayed navigation/position information.
8. Take off configuration monitoring shall be independent of aircraft configuration.
9. Autopilot engagement monitoring/warning shall be independent of autopilot.
10. Autopilot command monitoring/limiting shall be independent of autopilot command generation.
11. Maintenance data load monitoring/annunciation shall be independent of maintenance data load.

Individual independence requirement evaluations are presented in Tables CMA-1 through CM-7.

Table 8 PASA-2 Avionic System FDAL Assignment Summary

Avionic Function	Independence Attribute	FDAL
Autopilot/Autoflight (ATA22)	N	A
Communications (ATA23)	N	A
Displays (ATA31)	N	A
Navigation/Flight Management (ATA34)	N	B
Maintenance (ATA45)	N[1]	A[1]
1 .Maintenance A Testing & Data/Program Loading (45.01)	Y	A
2. Misc. Airplane Function Maintenance Testing (45.xx)	Y	D
Platform	N	A

Note 1: Maintenance (ATA45) Independence Attribute:

The Maintenance Function Independence attribute is not demonstrated in current planned development activity. If PASA recommendations are accepted; to capture Maintenance functionality in two independently managed requirement sets, then independence criteria will be satisfied and ARP4754A option 1 or 2 may be used to assign the FDAL for Maintenance A Testing (1) and Misc. Airplane Function Maintenance Testing (2).

Table 9 PASA CMA-1

1. Display of Primary Attitude information shall be independent of standby attitude information. **2.** Display of Primary Airspeed information shall be independent of standby airspeed information. **3.** Display of Primary Altitude information shall be independent of standby altitude information. **4.** Display of Primary Heading information shall be independent of standby heading information.		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	Redundant primary and standby displays will each be electrically powered from circuit breaker protected independent power sources.
	Data Source (input) Failure	Redundant sensors are used to provide information to primary displays. Standby instrument contains independent sensors for local display.
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	Primary and standby displays of attitude, airspeed, altitude and heading will be implemented using different technologies by different manufacturers.
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	Primary and standby displays of attitude, airspeed, altitude and heading will be implemented using different software languages by different manufacturers using different toolsets.
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for display of flight deck information (attitude, airspeed, altitude, heading) causes failure condition of interest due to error in common requirement.	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Displays ATA31) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for these independence requirements. FDAL will be assigned based on most severe failure condition – Level A.

Table 10 PASA CMA-2

5. Left engine parameter displays shall be independent of right engine parameter displays		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	Redundant primary and standby displays will each be electrically powered from circuit breaker protected independent power sources.
	Data Source (input) Failure	The left and right engine data sources and interface paths will be independent.
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	Primary engine display hardware will be developed to assurance level commensurate with functional hazard.
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	Primary engine display software will be developed to assurance level commensurate with functional hazard.
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for display of left and right engine parameter information causes failure condition of interest due to error in common requirement(s).	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Displays ATA31) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL will be assigned based on most severe failure condition – Level A.

Table 11 PASA CMA-3

6. Navigation capability shall be independent of communication capability		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	Redundant communication and navigation function items will each be electrically powered from circuit breaker protected independent power sources.
	Data Source (input) Failure	
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	Navigation and communication hardware will be developed to assurance level commensurate with functional hazard.
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	Navigation and communication software will be developed to assurance level commensurate with functional hazard.
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for communication function causes failure condition of interest due to error in common requirement(s).	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Communications ATA23) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL will be assigned based on most severe failure condition – Level A.

Table 12 PASA CMA-4

7. Captain displayed navigation/position information shall be independent of First Officer displayed navigation/position information		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	Captain and First officer navigational/positional displays and sensor information paths will each be electrically powered from circuit breaker protected independent power sources.
	Data Source (input) Failure	Redundant and independent sensor inputs will be selected and validate for use in displayed navigation information.
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	Captain and First Officer navigational/positional displays developed assurance level commensurate with functional hazard.
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	Captain and First Officer navigational/positional displays developed assurance level commensurate with functional hazard.
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for communication function causes failure condition of interest due to error in common requirement(s).	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Communications ATA23) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL will be assigned based on most severe failure condition – Level A.

Table 13 PASA CMA-5

8. Take off configuration monitoring shall be independent of aircraft configuration		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	*Editor – Not pertinent to ARP4754A example.*
	Data Source (input) Failure	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	*Editor – Not pertinent to ARP4754A example.*
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for configuration monitoring function causes failure condition of interest due to error in common requirement(s).	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Communications ATA23) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL will be assigned based on most severe failure condition – Level A.

Table 14 PASA CMA-6

9. Autopilot engagement monitoring/warning shall be independent of autopilot. 10. Autopilot command monitoring/limiting shall be independent of autopilot command generation.		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	*Editor – Not pertinent to ARP4754A example.*
	Data Source (input) Failure	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	*Editor – Not pertinent to ARP4754A example.*
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for configuration monitoring function causes failure condition of interest due to error in common requirement(s).	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Communications ATA23) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL will be assigned based on most severe failure condition – Level A.

Table 15 PASA CMA-7

11. Maintenance data load monitoring/annunciation shall be independent of maintenance data load.		
CONCEPT & DESIGN: DESIGN ARCHITECTURE		
Common Mode Sources	**Common Modes Failure /Errors**	**Analysis / Discussion**
External Sources	Electrical Power Distribution failure	*Editor – Not pertinent to ARP4754A example.*
	Data Source (input) Failure	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: TECHNOLOGY, MATERIAL, EQUIPMENT TYPE		
Redundant, Similar Hardware	Hardware development errors Common components fail (type, usage, etc.) Verification tools	*Editor – Not pertinent to ARP4754A example.*
Redundant, Similar Software	Common software development errors Common software development tools Verification tools	*Editor – Not pertinent to ARP4754A example.*
CONCEPT & DESIGN: SPECIFICATIONS		
Same specification	Specification for maintenance monitoring function causes failure condition of interest due to error in common requirement(s) with data load function.	Avionics Development Plan indicates that avionic function requirements will be captured and managed as independent elements. Error mitigation is acceptably established between functions. However, functionality within a specific functional area (e.g. Maintenance ATA45) may have common requirements, common development processing and potential for common requirement misinterpretation. A functional development independence attribute is not demonstrated for this independence requirement. FDAL shall be assigned based on most severe failure condition – Level A. It is recommended that the Avionic Maintenance function requirement specification be subdivided into the elements of Maintenance which must support catastrophic (Level A) failure conditions and those that must support normal airplane maintenance functions. Using this life cycle process, there would be no common errors in Maintenance Level D functionality which may cause or contribute to a Level A FC.

------- End of SE100PASA Preliminary Aircraft Safety Assessment excerpt --------

Title	Avionic System Development Plan	Doc No.	SDP100	Date	4/24/2015

NASA Study Baseline Architecture Example document excerpt.	Company A Avionic System Development Plan			
ARP4754A 5.8.4.3	SIZE A	FSCM NO	DWG NO ASDP100	REV -
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
	REV	DESCRIPTION	DATE	APPROVED
	-	Initial release		

Editor Note: Configuration control of avionics system development plan document is per system control category 2, using version change management process control.

A.1 SDP100 1 Introduction:

- Plan describes the system development process for Avionics functions to be installed on the SAAB-EII 100 airplane.
- Plan addresses engineering life cycle including function design, requirements generation, analysis, requirements validation, function verification for re-used functionality and modified functionality.
- Plan includes the identification and assignment of the appropriate Item Development Assurance Level (IDAL) rigor to be performed for airborne electronic hardware and software development.
- Plan fulfills the intent of ARP4754A objectives planning for:
  - Development (section 4),
  - Requirements Management (section 5.3),
  - Validation (section 5.4),
  - Verification (section 5.5).

A.1 SDP100 2 Avionics System Description:

The Company “A” Avionics Flight Deck integrates multiple avionic functions into a single Integrated Modular Avionic (IMA) system implementation:

- The Integrated Modular Avionics (IMA – ATA 42) includes the following functions:
  - IMA implementation certificated on “OTHER” aircraft
  - Baseline IMA includes the following system functions:
    - Autopilot/autoflight (ATA 22),
    - Communications (ATA23),
    - Displays (ATA31),
    - Navigation/Flight Management (ATA34), and
    - Maintenance (ATA 45).

A.1 SDP100 3 Avionics System Development Overview:

- The avionics system development process will ensure support of the certification process outlined in the SAAB-EII 100 Avionics Certification Plan (CP100).
- The avionics system development process is structured to ensure satisfaction of ARP4754A objectives commensurate with the assigned development assurance level (FDAL).
- This plan responds to the following ARP4754A planning objectives:
  - Requirements Management,
  - Requirements Validation,
  - Requirement Verification,
  - Configuration Management,
  - Process Assurance.
- The avionics system development process is based on re-using an integrated avionic implementation certificated on another airplane.
- The SAAB-EII 100 avionics system development process will use a combination of similarity/service experience to previous program ARP4754A objective data and the generation of new objective evidence for the unique airplane functionality to satisfy the SAAB-EII 100 ARP4754A development life cycle.
- Figure 8 presents a high level summary of the Avionics System development activities.

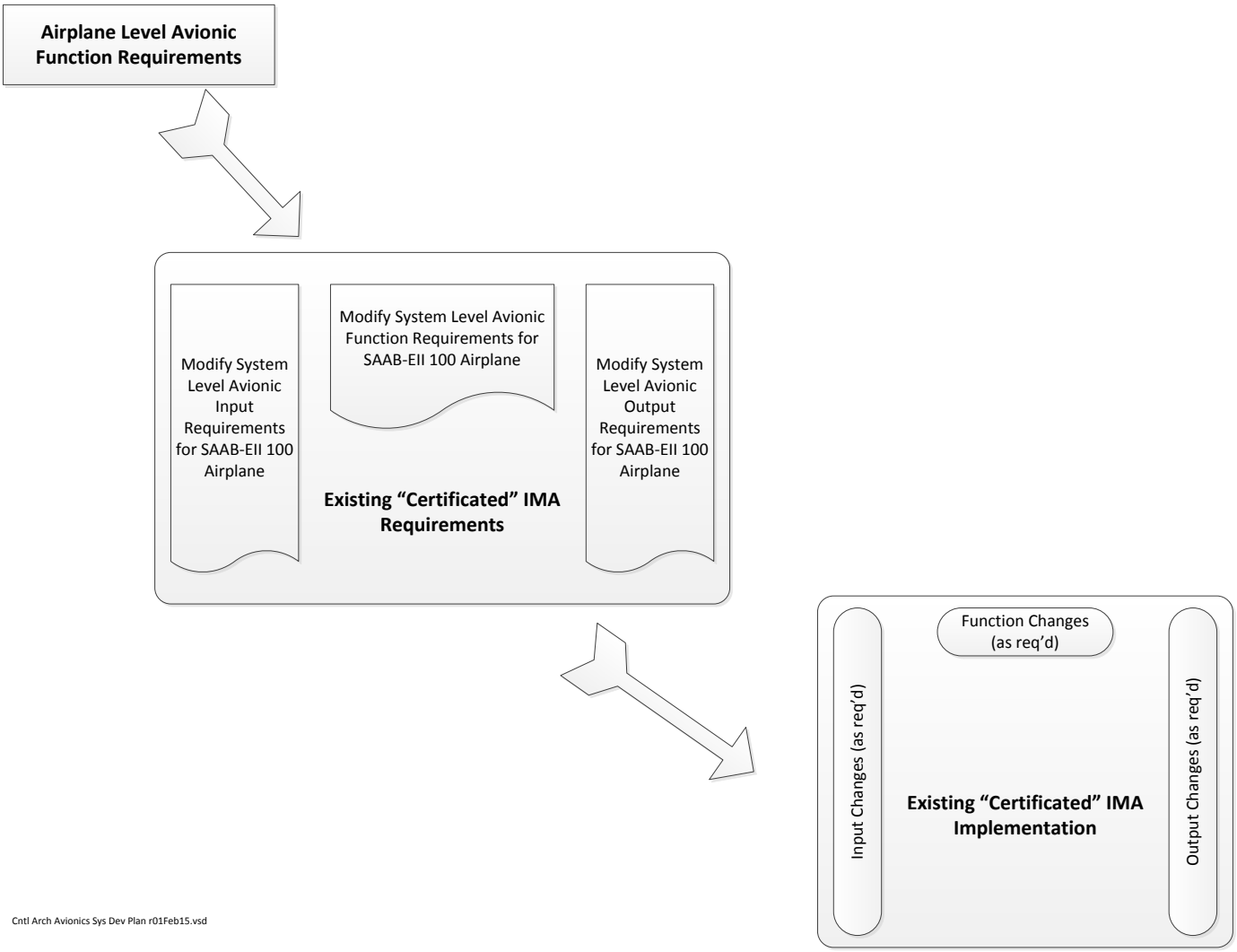


Figure 8 Generalized Avionics System Development Life Cycle

A.1 SDP100 3.1 Reuse Analysis Plan:

- Table 16 presents the top level SAAB-EII Avionics Development plan and strategy for reuse of baseline avionic system functionality.
- Table 17 presents the planned program strategy nomenclature descriptions.

Table 16 SAAB-EII 100 Avionics Reuse Strategy

1	2	3	4	5	6
System Functional Area	**System Func or Item**	**Existing FDAL /IDAL**	**New FDAL /IDAL**	**Rigors Differ**	**Program Strategy**
Autopilot/Autoflight (ATA 22)	Sys	A	A	No	Adapt
SW - AFCS App	Item	A	A	No	RWC
HW - AP Control Panel	Item	B	B	No	Reuse
HW - Pitch servo	Item	B	B	No	Reuse
HW - Roll Servo	Item	B	B	No	Reuse
HW - Yaw Servo	Item	B	B	No	Reuse
HW - Pitch Trim Servo	Item	B	B	No	Reuse
Communications (ATA 23)	Sys	A	A	No	Reapply
SW - Radio Tune App - Comm	Item				Reuse
HW - Radio Set - Comm	Item				Reuse
HW - Radio Set - Datalink	Item				Reuse
HW - Antennas - Comm	Item				Reuse
HW - Audio Control Panel	Item				Reuse
HW - TCAS	Item				Reuse
Displays (ATA 31)	Sys	A	A	No	Adapt
SW - PFD Graphics Common App	Item	A	A	No	Reuse
SW - PFD Graphics Instrument "T" App	Item	B	B	No	Reuse
SW - Warn Function App	Item				RWC
SW - Warn Function Common App	Item				Reuse
SW - WX Graphics App	Item				Reuse
HW - Display Control Panel	Item	B	B	No	Reuse
HW - Standby Instrument	Item				Reuse
HW - Display Unit - PFD	Item	A	A	No	Reuse
HW - Display Unit - EICAS	Item	A	A	No	Reuse
HW - Display Unit - MFD	Item	B	B	No	RWC
Navigation/Flight Management (ATA34)	Sys	B	B	No	Adapt
SW - Flight Management App	Item				Reuse
SW - Take off Performance App	Item				RWC
SW - MCDU Host App	Item				Reuse
SW - GPS Nav App	Item				Reuse
SW - Radio Tune App - Nav	Item				Reuse
HW - Inertial Sensor	Item				Reuse
HW - Radio Set - Nav	Item				Reuse
HW - Antennas - Nav	Item				Reuse
HW - GPS Antenna	Item				Reuse
HW - MCDU	Item				Reuse
Maintenance (ATA45)	Sys	A	A	No	Adapt
SW - CMC App	Item	D	D		RWC
SW - Dataload App	Item	A	A		Reuse
IMA Platform	Sys	A	A	No	Adapt
SW - Operating System App	Item	A	A		Reuse
SW - Middleware Apps	Item	A	A		Reuse
SW - HW Abstraction Layer App	Item	A	A		RWC
SW - Comm Network Core App	Item	A	A		RWC
SW - Comm Network Messaging App	Item	A	A		RWC
HW - Power Supply	Item	A	A		Reuse
HW - Cabinets	Item	A	A		Reuse
HW - Multipurpose computers	Item	A	A		Reuse
HW - Comm Network	Item	A	A		Reuse
HW - Airplane Interfaces	Item	C	C		New
Sensors	Sys	D	D	No	Reapply
HW - Weather Radar	Item				Reuse
HW - Weather Radar Controller	Item				Reuse

Determining the Item Change Type	
Program Strategy (Column 6)	**Description**
Reuse	Reusing an item (SW Application or HW element) from another aircraft program without modification to the item itself.
Reuse with Change (RWC)	Reusing an item from another airplane program with modifications to the item.
New	Develop a new item; i.e. this is the first instance of this function implementation.

Determining the System Change Type	
Program Strategy (Column 6)	**Description**
Reapply	Select Reapply if the entire system is being reused from another airplane program (i.e., all of the items in the system are identified as Reapply). The activities are related to adding traceability from existing system requirements to new airplane program Function requirements and integration of the system.
Adapt	Select Adapt if one or more of the items is identified as Reuse with Change with other items are identified as Reuse.

Table 17 Reuse Strategy Nomenclature

A.1 SDP100 4 Avionic System Safety:

- The system safety process includes requirements development as well as implementation verification activities that support the avionic system development.
- This process provides a methodology to evaluate airplane function failure conditions and the avionic system design performing these functions to establish that the identified hazards have been properly addressed.
- The avionics systems development process will include the following safety activities:

    - Avionic System Functional Hazard Analysis,
    - Preliminary Avionic System Safety Assessment,
        - Safety requirement development
        - FDAL / IDAL assignment (assignment substantiation)
    - Avionic System Safety Assessment,
    - Avionic System Common Cause Analysis,
    - Avionic System Level FMEA,
    - Equipment Level Safety Assessment(s)(as needed).

A.1 SDP100 5 Avionic System Requirements Development, Validation & Verification:

- Requirements development, validation and avionic system requirement verification plans are discussed in this section.
- Figure 9 presents the high level avionics system development process flow.
- Any changes in FDAL or IDAL assignments between the established baseline artifact level of rigor and the SAAB-EII 100 program assigned level will be evaluated on a case-by-case basis for a negotiated development approach.
    - Note- FDAL assignments A-B-C have minimal differences with respect to ARP4754A process objectives.

A.1 SDP100 5.1 Requirements Development & Management:

- The Avionic System "X.Y" requirements set will form the baseline for the SAAB-EII 100 Avionic System.
- The baseline requirements were developed to the level of rigor identified in Column 3 of Table 16 and include the following information:
    - Unique requirement identifier,
    - Requirement text,
    - Rationale (reason for having the requirement if requirement was derived),
    - Parent trace linkage capability,
    - Safety related attribute.

- As part of the SAAB-EII 100 development process, the baseline Company "A" avionic system requirement set will be evolved to include traceability information between the SAAB-EII 100 requirement specifications and the baseline avionic requirement set. See Figure 10 for artifact evolution plan.
- Requirements that need to be modified to satisfy SAAB-EII OEM requirements will be managed through the configuration management process to ensure traceability to the baseline.
- Changed requirements will be revalidated using the requirement validation process.
- New requirements will be introduced to the baseline requirement set using the CM process and validated using the validation process.
- All SAAB-EII 100 baseline requirement set validation attributes will be set initially to invalid status.
- An illustration of the requirement levels and tracing between these levels is shown in Figure 11.

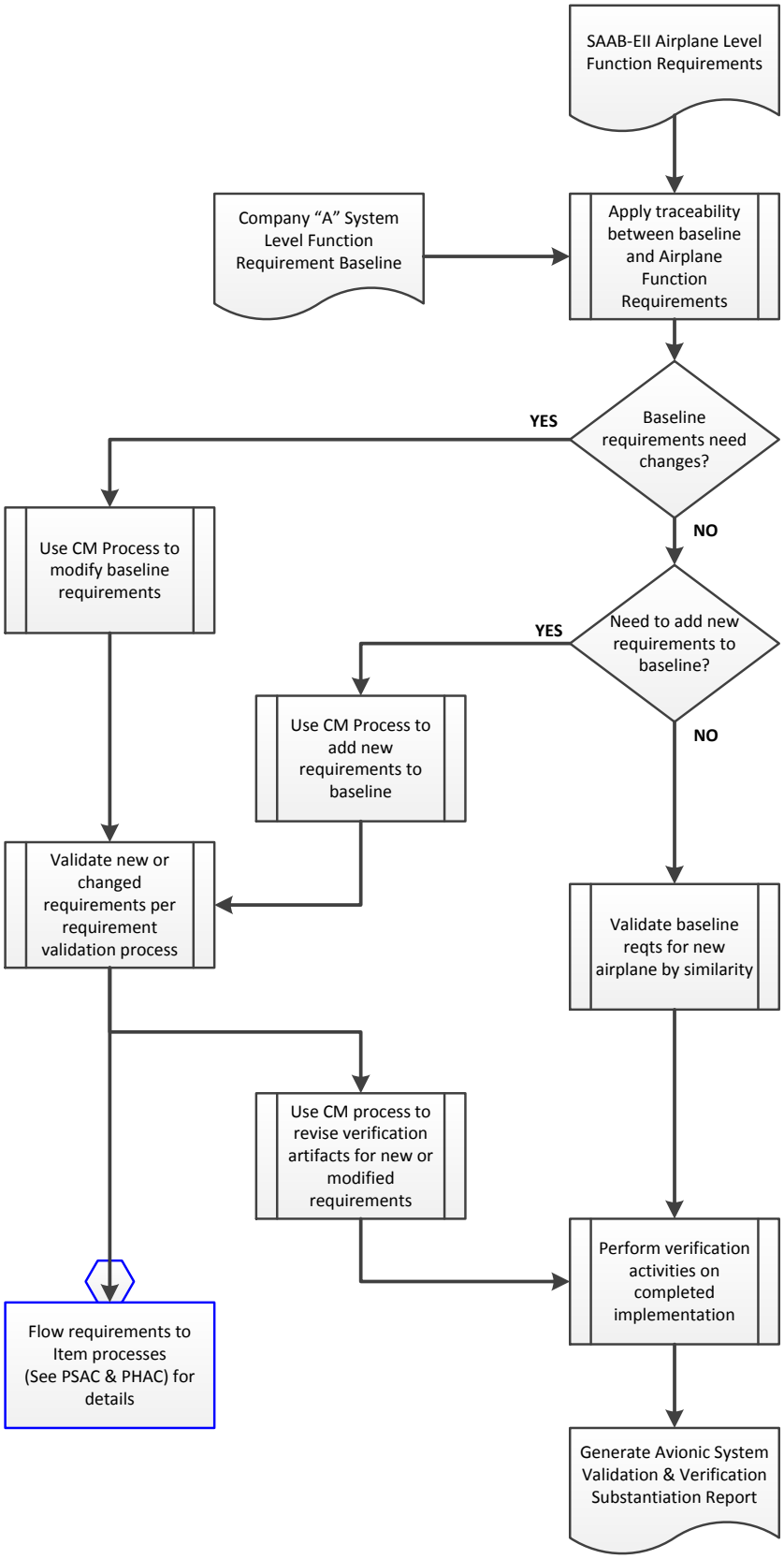


Figure 9 System Requirements Activity Plan

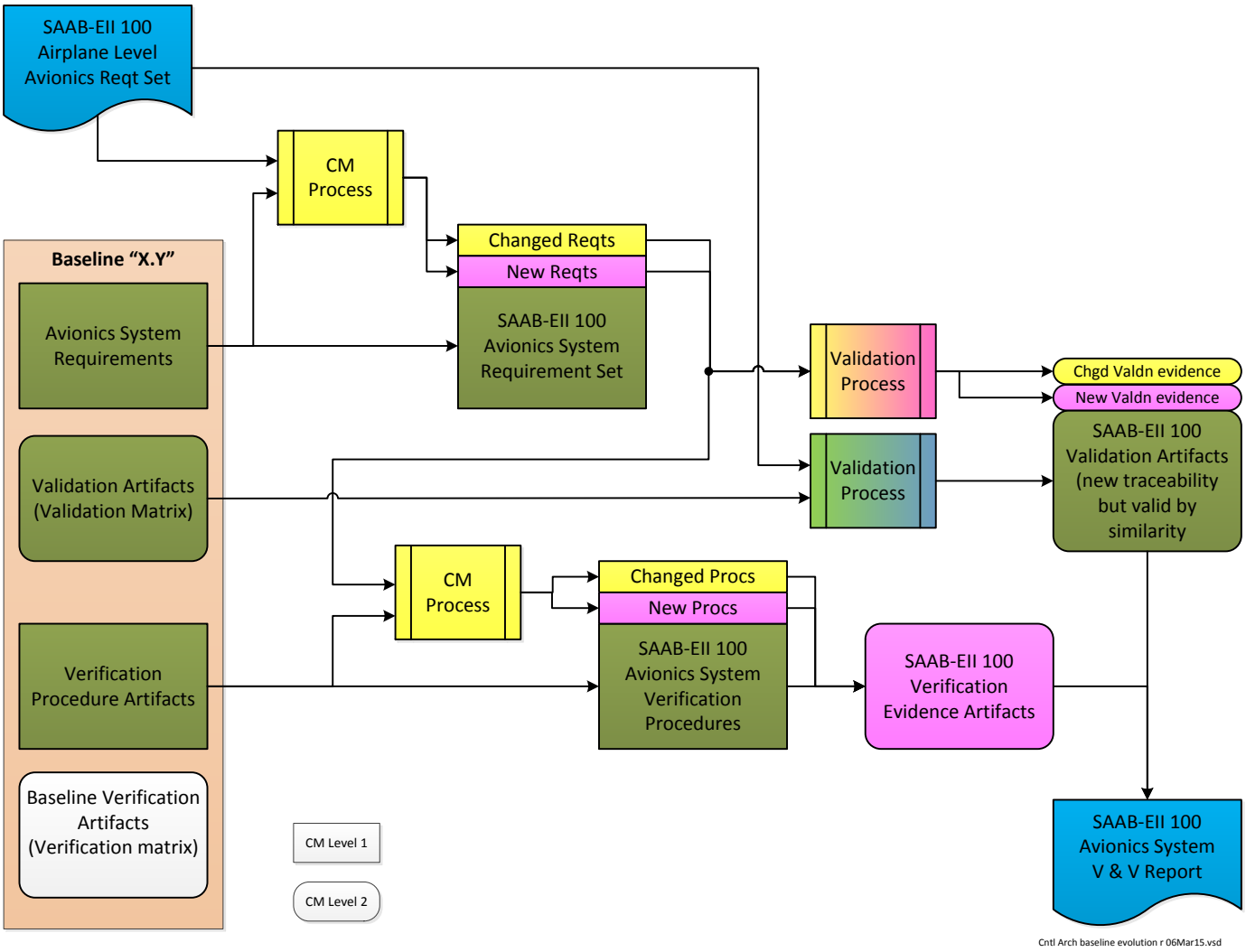


Figure 10 Baseline X.Y Evolution on SAAB-EII 100

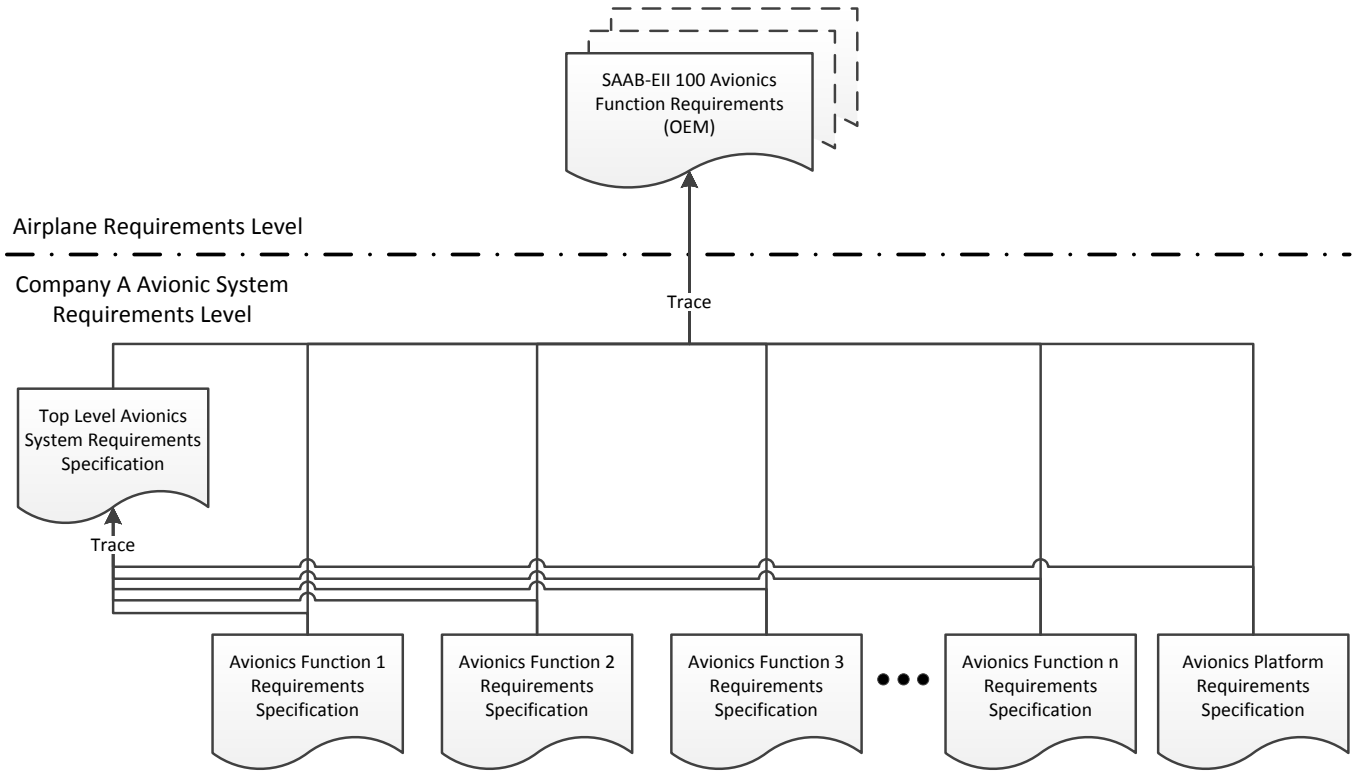


Figure 11 Baseline Requirements and Tracing

A.1 SDP100 5.2 Requirements Validation:

- The validation of requirements and specific assumptions ensures that the specified requirements are sufficiently correct and complete so that the developed product will provide the intended functionality.
  - Validation is a structured process for ensuring the correctness and completeness of the set of captured requirements.
  - The validation process also includes capture and evaluation of assumptions made during the requirement capture process to ensure:
    - Assumptions have been explicitly stated,
    - Assumptions are appropriately disseminated and,
    - Assumptions are justified by supporting data.
- Validation activities will be tracked using a matrix containing the requirements and their validation status.
- Validation activities accomplished and the completed validation matrix will be included in the Avionics System Validation and Verification Summary Report.
- Deviations from the validation process will be captured and reported in the Summary Report.

A.1 SDP100 5.2.1 Requirements Validation Methods & Process:

- Requirements will be validated using structured process accomplishing objectives of ARP4754A.
- Requirements will be validated using combination of methods:
- Methods of validation include:
  - Traceability,
  - Analysis (Modeling),
  - Test,
  - Similarity or,
  - Inspection (engineering review).
- It is anticipated that the bulk of the avionic systems requirements will be validated through similarity to the certificated baseline.
- Traceability will be established between the baseline requirement set and the SAAB-EII 100 avionic function requirement set, where appropriate.
- Baseline requirement set derived requirements and assumptions will be revalidated as part of the SAAB-EII 100 validation process.
- Artifacts will be generated as demonstration of the validation process for all requirements.
- For simplicity of process, validation of requirement sets supporting FDALs A through C will be accomplished with independence.
- Requirements supporting FDAL assignments A thru C will be summarized in a validation matrix.
- This matrix tracks the validation status of each requirement or assumption and captures the validation methods used to establish the validation result and artifact references capturing the evidence.
- An example validation matrix shown in Table 18.

Table 18 Example Completed Validation Matrix

				Validation Method						
Unique ID	**Text (Requirement or Assumption)**	**Safety**	**Requirement Source**	**Inspect**	**Analysis**	**Similarity**	**Test**	**Trace**	**Validation Artifact Reference**	**Reqt Valid (Y/N)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	AVACFT-R-1464	X		X		X	CN-1465	Y
AVSYS-R-xxx		N	Derived	X		X			CN-1465	Y
AVSYS-R-xxx		N	Assumption	X					ECM-SAABEII-CompA-14	Y
AVSYS-R-xxx		N	AVACFT-R-1490	X		X		X	CN-1465	Y
AVSYS-R-456										
Matrix Coding:										
Safety – Y if requirement is safety related.										
Requirement Sources: Parent Reqt ID, Derived, Assumption										
Validation Methods: Inspect – Inspection; Analysis – Analysis (Modeling); S – Similarity; Test – Test; Trace -Traceability;										
Reqt Valid – Y if requirement has completed validation effort and artifact has found requirement valid.										

CN = Change Notice
ECM = Engineering Communication Memo

A.1 SDP100 5.3 Requirements Verification:

- Verification of requirements and specific assumptions is the process of ensuring that the completed system has successfully implemented the requirements.
- Verification is a structured process for ensuring implementation complies with the set of captured requirements.
- Verification activities will be tracked using a matrix containing the requirements and their verification status.
- Verification activities accomplished and the completed verification matrix will be included in the Avionics System Validation and Verification Summary Report.
- Deviations from the verification process will be captured and reported in the Summary Report.

A.1 SDP100 5.3.1 Requirements Verification Methods & Process:

- Requirements will be verified using structured process accomplishing objectives of ARP4754A.
- Requirements will be verified using combination of methods:
- Methods of verification include:
    - Test,
    - Analysis (Modeling),
    - Service Experience or,
    - Inspection (engineering review).
- It is anticipated that the bulk of the avionic systems requirements will be verified through test.
- Artifacts will be generated as demonstration of the verification process for all requirements.
- Verification artifacts will be managed appropriate for the function development assurance level.

- Requirements supporting functions with FDAL A will be verified with independence.
- Requirements supporting functions with FDAL B & C will be verified with independence as a process goal but may be verified by requirement originators as necessary.
- For simplicity of process, verification test procedures supporting FDALs A thru C will be managed using change management control level 1.
- Requirements supporting FDALS A thru C will be summarized in a verification matrix.
- This matrix tracks the verification status of each requirement and captures the verification method(s) used to establish the verification result and artifact references capturing the verification evidence.
- An example verification matrix shown in Table 19.

Table 19 Example Completed Verification Matrix

					Verification Method(s)						
Unique ID	**Requirement Text**	**Safety**	**FDAL**	**Associated Function**	**Inspect**	**Analysis**	**Test**	**Service**	**Verification Procedure Reference**	**Verification Artifact Reference**	**Pass / Fail (P/F)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	A	Displays		X			NA	Avionic System SSA	P
AVSYS-R-xxx											
AVSYS-R-xxx											
AVSYS-R-xxx											
AVSYS-R-456											

Matrix Coding:

Safety – Y if requirement is safety related.

Verification Methods: Inspect – Inspection; Analysis – Analysis (Modeling); Service – Service Experience; Test – Test (Demonstration)
NA – not applicable

A.1 SDP100 6 Avionic System Configuration & Change Management:

- Configuration management of development artifacts are the responsibility of the originating group.
- The central Company “A” CM organization provides tools, services and process to assist in this task.
- Artifacts created during the development and used as part of the certification process will be managed per the detailed process described in the “Company A Configuration Management Plan” appropriate to the level of rigor established for the artifact.
- Artifacts to be managed include:
    - Avionic System Development Plan (this document),
    - Avionic system requirements documentation,
    - Avionic system safety assessments,
    - Avionic system validation evidence,
    - Avionic system verification procedures,
    - Avionic system verification evidence,
    - Avionic system validation & verification accomplishment summary.
- Requirements, safety assessment and verification procedure artifacts will be managed using detail change management process (Change control level 1 aka CM Level 1)
- All other program artifacts will be managed using version control change management process (change control level 2 aka CM Level 2).

A.1 SDP100 7 Avionic System Process Assurance:

- Process assurance is integral to the development activities to ensure that the system development and supporting processes are appropriate, maintained, and followed.
- Process assurance is performed by the Company “A” Quality Assurance (QA) organization.
- Process assurance is evaluated against:
    - ARP4754A objectives based on development assurance rigor (FDAL)
    - DO-178 objectives based on development assurance rigor (IDAL). See PSAC for specific details.
    - DO-254 objectives based on development assurance rigor (IDAL). See PHAC for specific details.

------- End of SDP100 Avionic System Development Plan excerpt -------

Appendix A.2 Study Architecture 1 (aka SAAB-EII 200)

Introduction

An example of planning specific change activities to avionics system hosted functionality being used on the same airplane as was previously certificated. Legacy avionic system (IMA) developed per ARP4754.

Example project ARP4754A artifacts developed include:

Airplane Level

Airplane Project Specific Certification Plan (PSCP200)

Systems Level

Avionic System Development Plan (ASDP200)

Item Level

None – not a feature of study

NASA Study Architecture 1	SAAB-EII 200 Project Specific Certification Plan			
ARP4754A, 6.2(a)(b)(c)	SIZE A	FSCM NO	DWG NO PSCP200	REV -
6.6.1, 6.6.4	SCALE 1 : 1		SHEET 1 of 1	

REVISIONS				
CN No.	REV	DESCRIPTION	DATE	APPROVED
-	-	Initial release	06 Mar 2015	J Allen
	A	Revised per Change Request 165.	03 Jul 2015	

Editor Note: Configuration control of certification plan document is per system control category 1, under full problem report/change management process control.

A.2 PSCP200 1 Plan Purpose:

- This project specific certification plan (PSCP) defines the certification activities planned as part of a modification to the IMA avionics platform on the SAAB-EII 200 airplane.
- The plan will highlight the specific modifications planned for the Company “A” IMA avionics system, the implementation strategy for the modification and the safety aspects of the planned changes.

A.2 PSCP200 2 Project Background:

- Legacy airplane certificated under 14CFR Part 25 Transport Category airplane
    - Legacy airplane certificated per conventional development processes

Editor Note: Conventional development processes denotes that no ARP4754A process artifacts were created.

- Company “A” provided Integrated Modular Avionics (IMA – ATA 42) using the architecture presented in Figure 12.

- IMA developed to ARP4754, DO-178B, DO-254 & DO-297
- IMA includes the following functions:
    - Autopilot/autoflight (ATA 22),
    - Communications (ATA23),
    - Displays (ATA31),
    - Navigation/Flight Management (ATA34) and,
    - Maintenance (ATA 45).

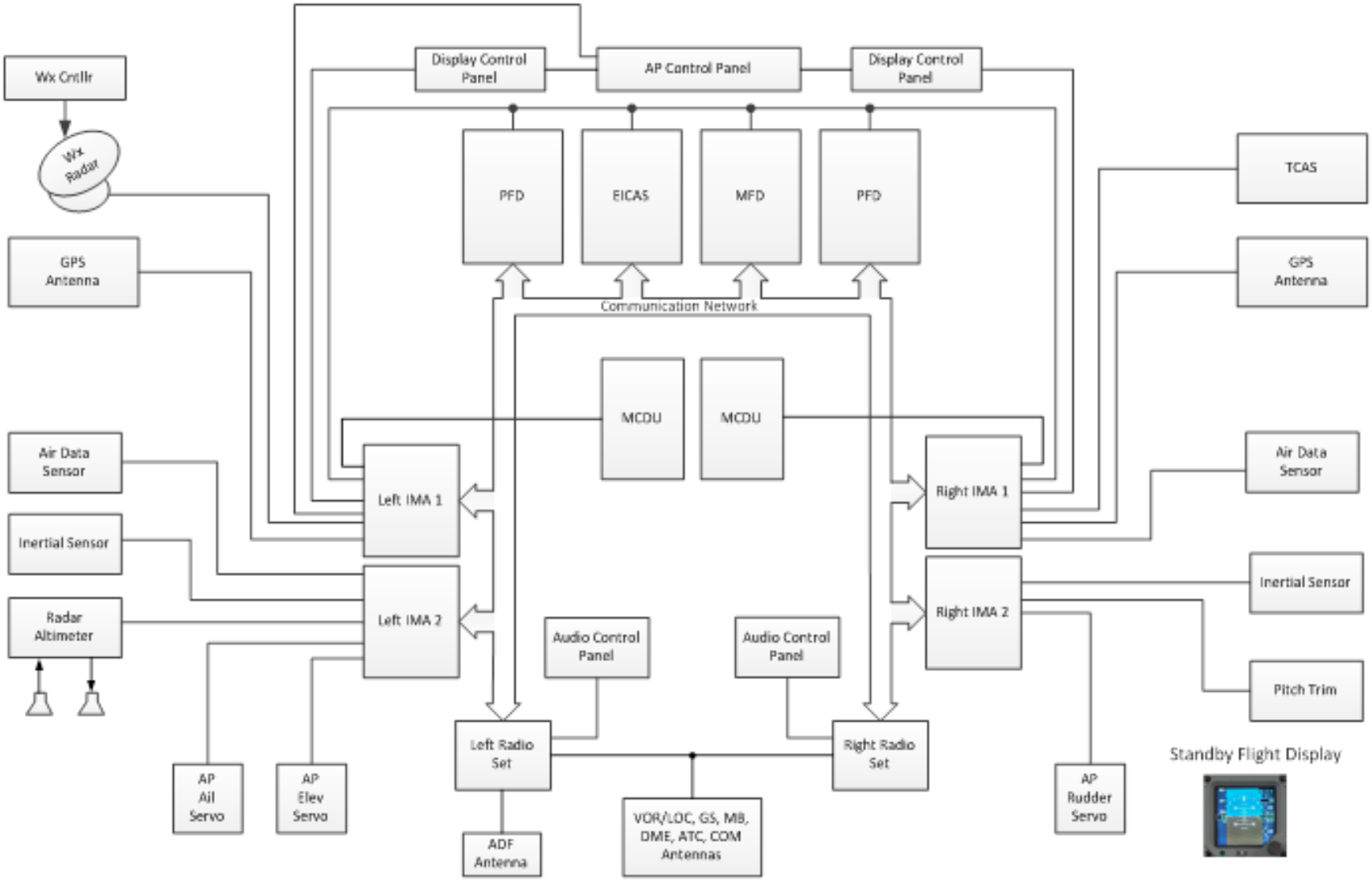


Figure 12 SAAB-EII 200 Avionics Architecture

A.2 PSCP200 3 Planned Modifications:

- Changes under this plan are limited to the flight deck avionics, i.e. no aircraft level modifications are planned.
- Existing Avionics (IMA), Part Number IMA100, will have the following changes incorporated:
  - Existing IMA Fight Management System (FMS) function will be revised to correct for deficiencies and enhance performance.
  - A new IMA function “ABC” will be added to the IMA platform to provide enhanced situational awareness of system status and configuration.
- Modifications will be accomplished using existing and evolved supplier system, software and hardware development processes satisfying ARP4754A objectives.
- Modification activity milestone summary is presented in Table 20.
- A high level modification process flow diagram is presented in Figure 13.

Table 20 SAAB-EII 200 Avionics Modification Milestones

Change Activity	**Projected Completion Schedule**
FMS Deficiency/Enhancements	Per change notice tracking timeline
“ABC” Requirement Capture	Function “ABC” CDR
Validation Matrix Update	Function “ABC” CDR
IMA Software Revisions Complete	See IMA100V1 PSAC[1]
Verification Procedures Update	Completion of HW-SW Integration (see IMA100V1 PSAC)
Verification Testing	Two weeks prior to submittal of certification package
V & V Summary Report	System Certification Package

[1] Individual PSACs for each software component may be developed or a combined IMA PSAC plan developed for all software modifications as selected for this scenario example.

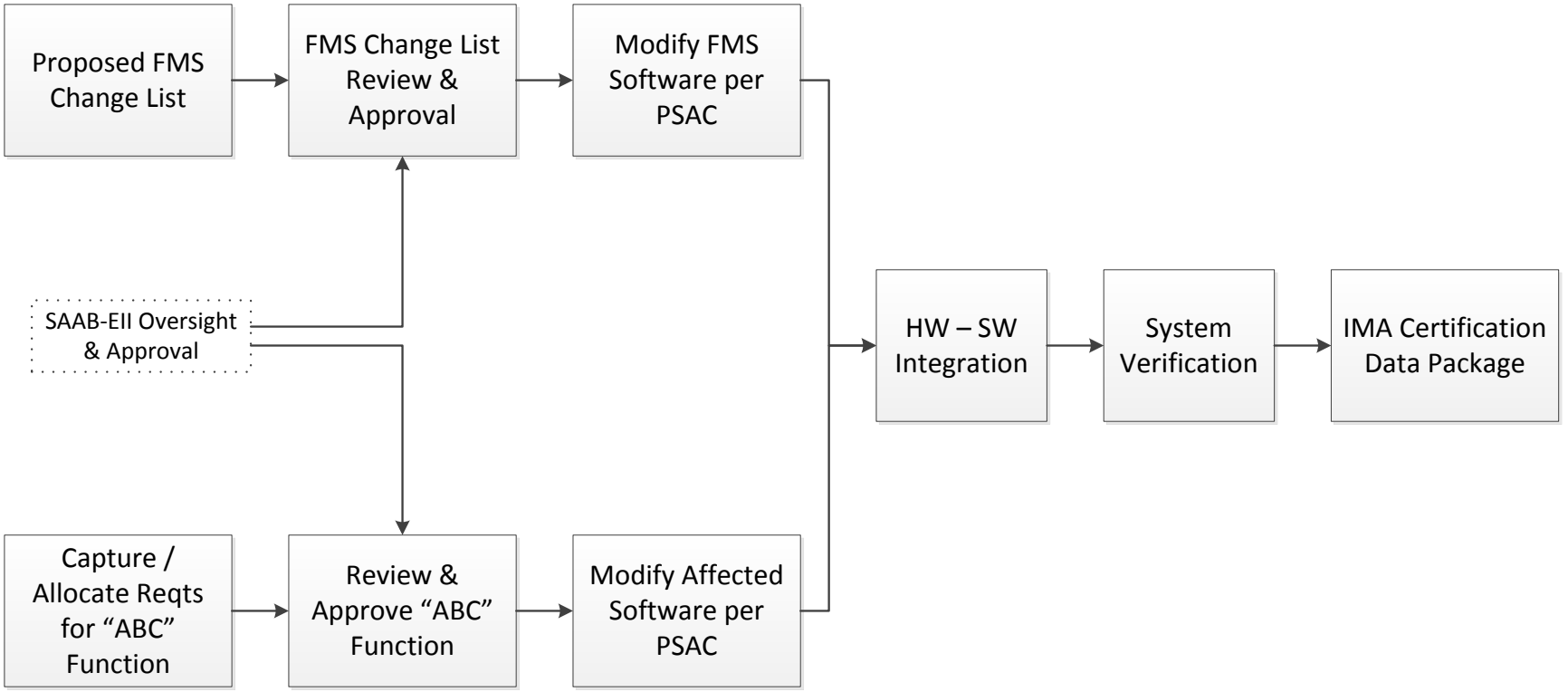


Figure 13 SAAB-EII 200 Avionics Modification Plan

A.2 PSCP200 4 Modification Impact Analysis Summary:

A.2 PSCP200 4.1 Change Description Summary:

- Modifications to FMS function do not impact airplane level functionality.
- Addition of function “ABC” provides additional capabilities to Provide Operational Awareness and Maintenance hosted airplane level function.
- Table 21 summarizes the IMA functional areas impacted by the change and the most sever failure condition classifications for that function.

Table 21 SAAB-EII 200 IMA Impact Summary

IMA Function	Change Y/N	Impact Description	Failure Condition Classification
Autopilot/Autoflight (ATA22)	N	No new or changed autopilot functions.	Catastrophic
Communications (ATA23)	N	No new or changed communication functions.	Catastrophic
Displays (ATA31)	Y	Addition of maintenance messages to support new function “ABC”	Catastrophic*
Navigation/Flight Management (ATA34)	Y	Open system problem reports on FMS function deficiencies and FMS function performance will be implemented.	Hazardous
Maintenance (ATA45)	Y	New maintenance messages and test instructions added.	Hazardous
Platform	N	No new or changed aircraft level platform functions.	Catastrophic
Sensors	N	No new or changed sensing functions.	Various
“ABC”	Y	New aircraft configuration monitoring and reporting function using existing available sensor data	Hazardous

*Note: Legacy Displays IMA function implementation is partitioned to support multiple software function criticalities.

A.2 PSCP200 4.2 Change Classification Analysis:

- The modifications have been evaluated per AC 21.101-1 and found to be non-significant.
  - The legacy certification basis for Legacy SAAB-EII 200 will be maintained.
- The planned modification has been evaluated per AC 21-40A for classification of the change as either major or minor:
  - Changes have been found to have no appreciable effect on:
    - Weight,
    - Balance,
    - Structural strength,
    - Reliability,
    - Characteristics affecting airplane airworthiness.
  - Changes have been found to have a minor impact on the operational characteristics of the flight deck maintenance displayed information.
  - Therefore, the changes planned in this plan are anticipated classified as *Minor* and will be approved using the SAAB-EII FAA approved "Minor Airplane Change Process".

- Legacy airplane level development used conventional development techniques and as such did not create ARP4754A objectives evidence.
  - FDAL for Avionics functions were not developed.
  - Airplane function development evidence was not created (Requirements, Validation and Verification).
- Creation of ARP4754A airplane level artifacts for the changes identified in this plan is not advantageous or practical and is therefore not planned. Conventional airplane certification activities will be used.

A.2 PSCP200 4.3 Safety Impact of Planned Changes:

- Review of legacy IMA functional failure conditions indicates that:
  - FMS Loss or Erroneous operation classified as Hazardous
  - Modifications planned for the FMS function do not affect the functional hazard failure condition description or severity
  - Modifications planned for the FMS function do not affect any other IMA or external functionality.
- Added IMA function "ABC" adds software function to provide new aircraft configuration advisories to enhance flight crew situational awareness
  - New function "ABC" adds two new failure conditions.
  - Preliminary FHA of function "ABC" indicates a hazardous (II) classification for erroneous operation and major (III) classification for loss of function.
  - Displays functionality is partitioned between caution/warn display and maintenance.
- The System FHA will be revised to add function "ABC" failure conditions and classification.
- FDAL for the modification activities will be assigned directly based on the most sever aircraft-level failure condition supported by the modified and new functionality.

A.2 PSCP200 4.4 Modification Implementation Strategy:

- All modifications planned under this change effort are contained to the IMA Avionics platform and impact only IMA avionic software
- See Company "A" **Avionics System Development Plan** for details of planned modification.

A.2 PSCP200 5 Compliance Methods:

- Compliance to the regulations will be shown by analysis, inspection and test.
- Summary for 14CFR 25.1309, Systems, equipment and installations:
  - IMA avionic system development process per AC20-174 using ARP4754A at assigned FDAL
  - Airborne electronic hardware development per AC20-152 using DO-254 at assigned IDALs
  - Airborne software development per AC20-115C using DO-178B at assigned IDALs
  - Safety assessments(FHA, PSSA, SSA) per ARP4761
- IMA development per AC-148 and AC-170.
- See Company "A**" Avionics System Development Plan** for details of modification process.

----- End of PSCP200 Project Specific Certification Plan excerpt -----

Title	Avionic System Development Plan	Doc No.	ASDP200	Date	7/03/2015

NASA Study Architecture 1	Company A Avionic System Development Plan			
	SIZE A	FSCM NO	DWG NO ASDP200	REV A
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
	REV	DESCRIPTION	DATE	APPROVED
	-	Initial release	01 March 2015	
	A	Revised for customer review commens.	03 July 2015	

Editor Note: Configuration control of avionics system development plan document is per system control category 2, using version change management process control.

A.2 ASDP200 1 Introduction:

- This Plan describes the system development process for modifications planned for the IMA hosted functionality installed on the SAAB-EII 200 airplane.
- Plan addresses engineering life cycle evolution from ARP4754 to ARP4754A including function design, requirements generation, analysis, requirements validation, function verification for re-used functionality and modified functionality.
- Plan includes the identification and assignment of the appropriate Functional Development Assurance Level (FDAL) rigor to be performed for changed or new systems functions as well as Item Development Assurance (IDAL) assignment for airborne software development of new functionality.
- Plan fulfills the intent of ARP4754A objectives planning for:
    - Development (section 4),
    - Requirements Management (section 5.3),
    - Validation (section 5.4),
    - Verification (section 5.5).

A.2 ASDP200 2 Avionics System Description:

The Company “A” IMA100 Avionics Flight Deck integrates multiple avionic functions into a single Integrated Modular Avionic (IMA) system implementation:

- The Integrated Modular Avionics (IMA – ATA 42) includes the following functions:
    - Baseline IMA includes the following system functions:
        - Autopilot/autoflight (ATA 22),
        - Communications (ATA23),
        - Displays (ATA31),
        - Navigation/Flight Management (ATA34), and
        - Maintenance (ATA 45).

A.2 ASDP200 3 Avionics System Development Overview:

- The legacy Company “A” IMA100 avionics system was developed in accordance with ARP4754, DO-178B, DO-254 & DO-297.
- The avionics ARP4754 system development process will be evolved and structured to ensure satisfaction of ARP4754A objectives commensurate with a developed function development assurance level (FDAL) for revised and new functions.
- FDAL/IDAL will be assigned directly based on the most sever aircraft-level failure condition supported by the modified and new functionality.

- This plan responds to the following ARP4754A planning objectives:
    - Requirements Management,
    - Requirements Validation,
    - Requirement Verification,
    - Configuration Management,
    - Process Assurance.

- The avionics system development process is based on re-using an integrated avionic implementation previously certificated on the SAAB-EII 200 airplane.
- The SAAB-EII 200 avionics system development process will use a combination of similarity/service experience to previous program ARP4754 objective data and the generation of new ARP4754A objective evidence for the changed IMA functionality to satisfy the SAAB-EII 200 ARP4754A development life cycle.

- Figure 14 presents a high level summary of the Avionics System development activities.

    - Changed FMS function:
        - Capture requirements associated with changed FMS functionality per newly assigned FDAL.
        - Validate new FMS requirements per ARP4754A compliant process
        - Validate unchanged FMS requirements per ARP4754A similarity to certificated functionality
        - Verify old and new FMS implementation meets intended FMS function requirements.

    - New “ABC” function:
        - Capture requirements associated with “ABC” functionality per assigned FDAL.
        - Validate new “ABC” requirements per ARP4754A compliant process.
        - Verify “ABC” implementation meets intended “ABC” function requirements.
        - Capture requirements in Displays (ATA 31) and Maintenance (ATA45) associated with changed IMA functionality per newly assigned FDAL.
        - Validate new IMA requirements per ARP4754A compliant process.
        - Validate unchanged IMA requirements per ARP4754A similarity to certificated functionality.
        - Verify old and new IMA implementation meets intended IMA function requirements.

    - Table 22 summarizes the objective evolution and highlights new configuration management (CM) system control (SC) category.
    - Modifications are anticipated to affect software only. Should hardware modifications be required, the necessary PHAC(s) will be created and approved for the modification.

Table 22 ARP4754 Objectives & Configuration Evolution Summary

4754 Objective / Evidence	Legacy CM CC Category	4754A Objective / Evidence	4754A CM CC Category
Requirements captured (FMS System Requirements Document)	NA	Requirements changes captured - FMS System Requirements Document	SC1
Requirements Validation - FMS (validation matrix, summary)	NA	Requirements Validation – FMS per assigned FDAL	SC2
NA	NA	Requirements captured – “ABC” Function Requirements Document	SC1
NA	NA	Requirements Validation – “ABC” per assigned FDAL	SC2
Requirements captured (Display System Requirements Document)	NA	Requirements changes captured - Display System Requirements Document	SC1
Requirements Validation – Display (validation matrix, summary)	NA	Requirements Validation – Display per assigned FDAL	SC2
Verify IMA function requirements (Test Procedures)	NA	Modify existing IMA function Test Procedures per assigned FDAL	SC1
Verify IMA function requirement implementation (verification matrix, summary)	NA	Verify changed and unchanged IMA function requirement implementation (verification matrix, summary)	SC2

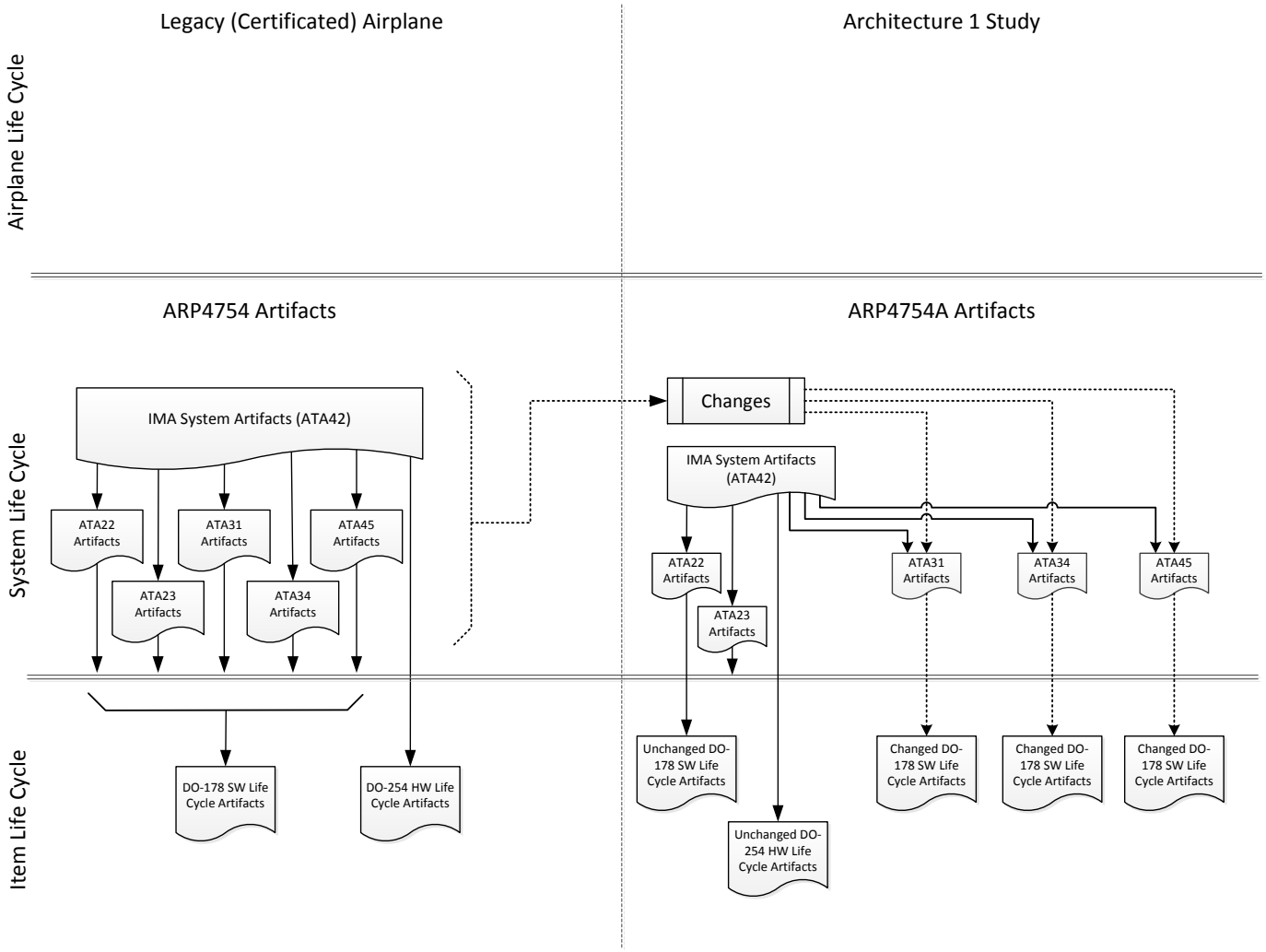


Figure 14 SAAB-EII 200 Avionics System Change Implementation Development Plan

A.2 ASDP200 3.1 Reuse Analysis Plan:

- Table 23 presents the top level SAAB-EII 200 Avionics Development plan and strategy for reuse of baseline avionic system functionality.
- Table 24 presents the planned program strategy nomenclature descriptions.

Table 23 SAAB-EII 200 Avionics Reuse Strategy

1	2	3	4	5	6
System Functional Area	**System Func or Item**	**Existing FDAL /IDAL**	**New FDAL /IDAL**	**Rigors Differ**	**Program Strategy**
Autopilot/Autoflight (ATA 22)	Sys	NA	NA	NA	Reapply
SW - AFCS App	Item	A	A	No	Reuse
HW - AP Control Panel	Item	B	B	No	Reuse
HW - Pitch servo	Item	B	B	No	Reuse
HW - Roll Servo	Item	B	B	No	Reuse
HW - Yaw Servo	Item	B	B	No	Reuse
HW - Pitch Trim Servo	Item	B	B	No	Reuse
Communications (ATA 23)	Sys	NA	NA	NA	Reapply
SW - Radio Tune App - Comm	Item				Reuse
HW - Radio Set - Comm	Item				Reuse
HW - Radio Set - Datalink	Item				Reuse
HW - Antennas - Comm	Item				Reuse
HW - Audio Control Panel	Item				Reuse
HW - TCAS	Item				Reuse
Displays (ATA 31)	Sys	NA	A	Yes	Adapt
SW - PFD Graphics Common App	Item	A	A	No	Reuse
SW - PFD Graphics Instrument "T" App	Item	B	B	No	Reuse
SW - Warn Function App	Item				RWC
SW - Warn Function Common App	Item				Reuse
SW - WX Graphics App	Item				Reuse
HW - Display Control Panel	Item	B	B	No	Reuse
HW - Standby Instrument	Item				Reuse
HW - Display Unit - PFD	Item	A	A	No	Reuse
HW - Display Unit - EICAS	Item	A	A	No	Reuse
HW - Display Unit - MFD	Item	B	B	No	RWC
Navidation/Flight Management (ATA34)	Sys	NA	B	Yes	Adapt
SW - Flight Management App	Item		B	No	RWC
SW - Take off Performance App	Item		B	No	RWC
SW - MCDU Host App	Item				Reuse
SW - GPS Nav App	Item				Reuse
SW - Radio Tune App - Nav	Item				Reuse
HW - Inertial Sensor	Item				Reuse
HW - Radio Set - Nav	Item				Reuse
HW - Antennas - Nav	Item				Reuse
HW - GPS Antenna	Item				Reuse
HW - MCDU	Item				Reuse
Maintenance (ATA45)	Sys	NA	C	Yes	Adapt
SW - CMC App	Item	D	C	Yes	RWC
IMA Platform	Sys	NA	A	Yes	Adapt
SW - Operating System App	Item	A	A	No	Reuse
SW - Middleware Apps	Item	A	A	No	Reuse
SW - HW Abstraction Layer App	Item	A	A	No	RWC
SW - Comm Network Core App	Item	A	A	No	RWC
SW - Comm Network Messaging App	Item	A	A	No	RWC
SW - Dataload App	Item	A	A	No	Reuse
HW - Power Supply	Item	A	A	No	Reuse
HW - Cabinets	Item	A	A	No	Reuse
HW - Multipurpose computers	Item	A	A	No	Reuse
HW - Comm Network	Item	A	A	No	Reuse
Sensors	Sys	NA	D	No	Reapply
HW - Weather Radar	Item				Reuse
HW - Weather Radar Controller	Item				Reuse

Editor's Note: Reused HW and SW implementations not impacted by the changes included in this example retain the legacy development assurance level (though not identified).

Table 24 Reuse Strategy Nomenclature

Determining the Item Change Type	
Program Strategy (Column 6)	**Description**
Reuse	Reusing an item (SW Application or HW element) from another aircraft program or previous certification without modification to the item itself.
Reuse with Change (RWC)	Reusing an item from another airplane program or previous certification with modifications to the item.
New	Develop a new item; i.e. this is the first instance of this function implementation.

Determining the System Change Type	
Program Strategy (Column 6)	**Description**
Reapply	Select Reapply if the entire system is being reused from another/same airplane program (i.e., all of the items in the system are identified as Reapply). The activities are related to adding traceability from existing system requirements to new airplane program/revised Function requirements and integration of the system.
Adapt	Select Adapt if one or more of the items is identified as Reuse with Change (RWC) with other items are identified as Reuse.
New	Select New if all or nearly all items are New

A.2 ASDP200 4 Avionic System Safety:

- The system safety process includes requirements development as well as implementation verification activities that support the avionic system development.
- This process provides a methodology to evaluate airplane function failure conditions and the avionic system design performing these functions to establish that the identified hazards have been properly addressed.

- The avionics systems development process will include the following safety activities:

  - Avionic System Functional Hazard Analysis
    - Updated hazard evaluation for new function “ABC”,
  - Preliminary Avionic System Safety Assessment Supplement
    - Supplement IMA100V1 PSSA will be created to evaluate planned implementation of function “ABC” against new system FHA failure condition(s).
    - Safety requirement development as necessary to support “ABC” implementation
    - FDAL / IDAL assignment (assignment substantiation) for FMS revisions & “ABC” development
  - Avionic System Safety Assessment (revision to existing analysis to incorporate applicable FMS changes and addition of “ABC” failure condition analysis result),
  - Avionic System Common Cause Analysis (update as necessary to support PSSA/SSA revisions),

Editor’s Note: IMA100V1PSSA not created as part of the example development.

A.2 ASDP200 5 Avionic System Requirements Development, Validation & Verification:

- Requirements development, validation and avionic system requirement verification plans are discussed in this section.
- Figure 15 presents the high level avionics system development process flow.
- Any changes in FDAL or IDAL assignments between the established baseline artifact level of rigor and the modification program assigned level will be evaluated on a case-by-case basis for a negotiated development approach.

A.2 ASDP200 5.1 Requirements Development & Management:

- The IMA100 Avionic System "X.Y" requirements set will form the baseline for the SAAB-EII 200 Avionic System modification program.
- The baseline requirements were developed to the level of rigor commensurate with the level of assurance assigned to the implementing software (though not identified as FDAL) as shown in Table 23.
- Each requirement includes the following information:
  - Unique requirement identifier,
  - Requirement text,
  - Rationale (reason for having the requirement if requirement was derived),
  - Parent trace link (if requirement traceable to a parent),
  - Safety related attribute.

- As part of the SAAB-EII 200 development process, the baseline Company "A" avionic system FMS and Display requirement sets will be evolved from the "X.Y" baseline to new IMA100V1.
- See Figure 16 for an artifact evolution plan.

- Requirements that need to be modified will be managed through the configuration management process to ensure traceability to the baseline.
- Changed requirements will be revalidated using the requirement validation process.
- New requirements (function "ABC") will be introduced to the baseline requirement set using the CM process and validated using the validation process.
- An illustration of the requirement levels and tracing between these levels is shown in Figure 17.

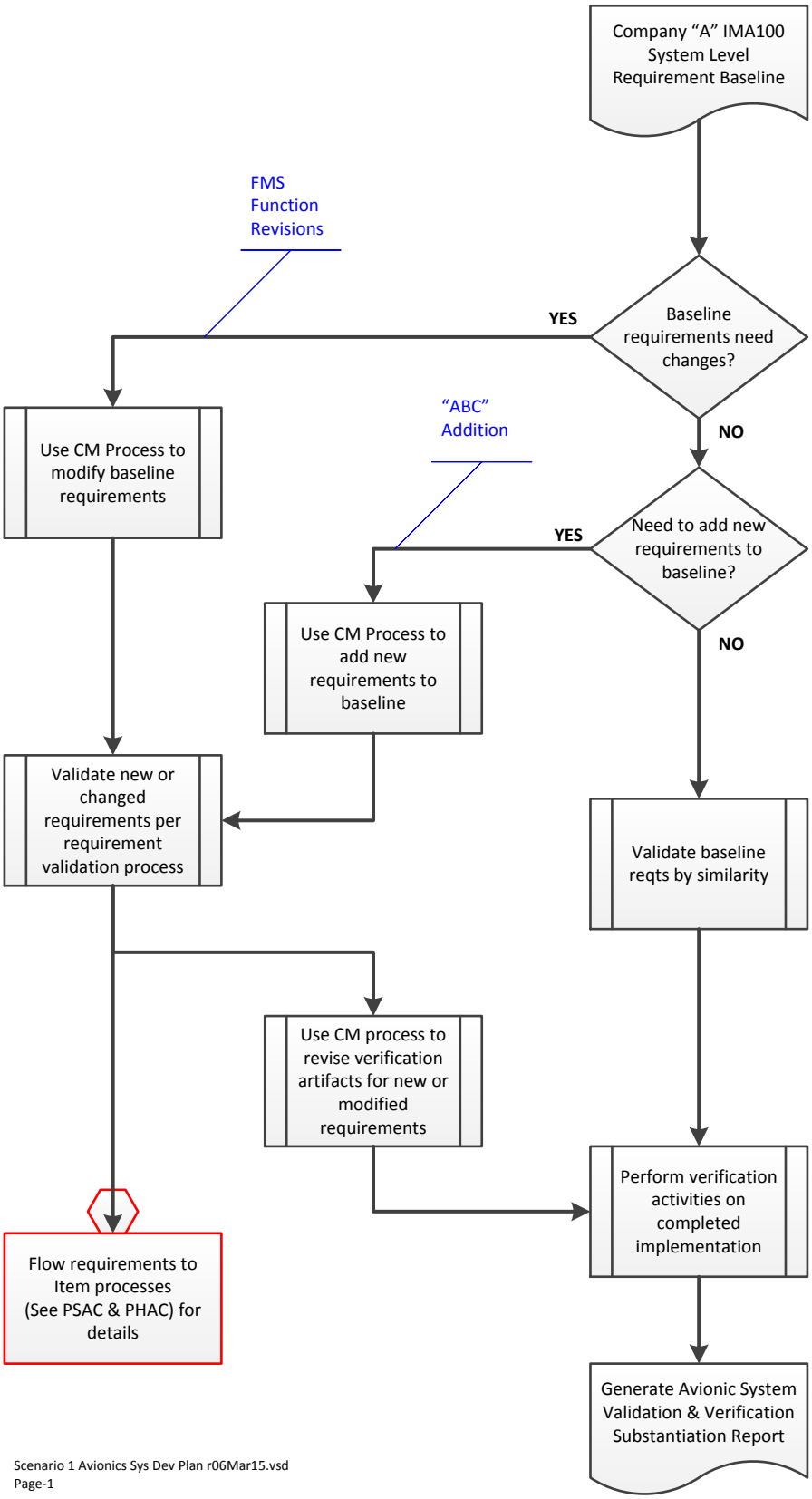


Figure 15 SAAB-EII 200 System Requirements Activity Plan

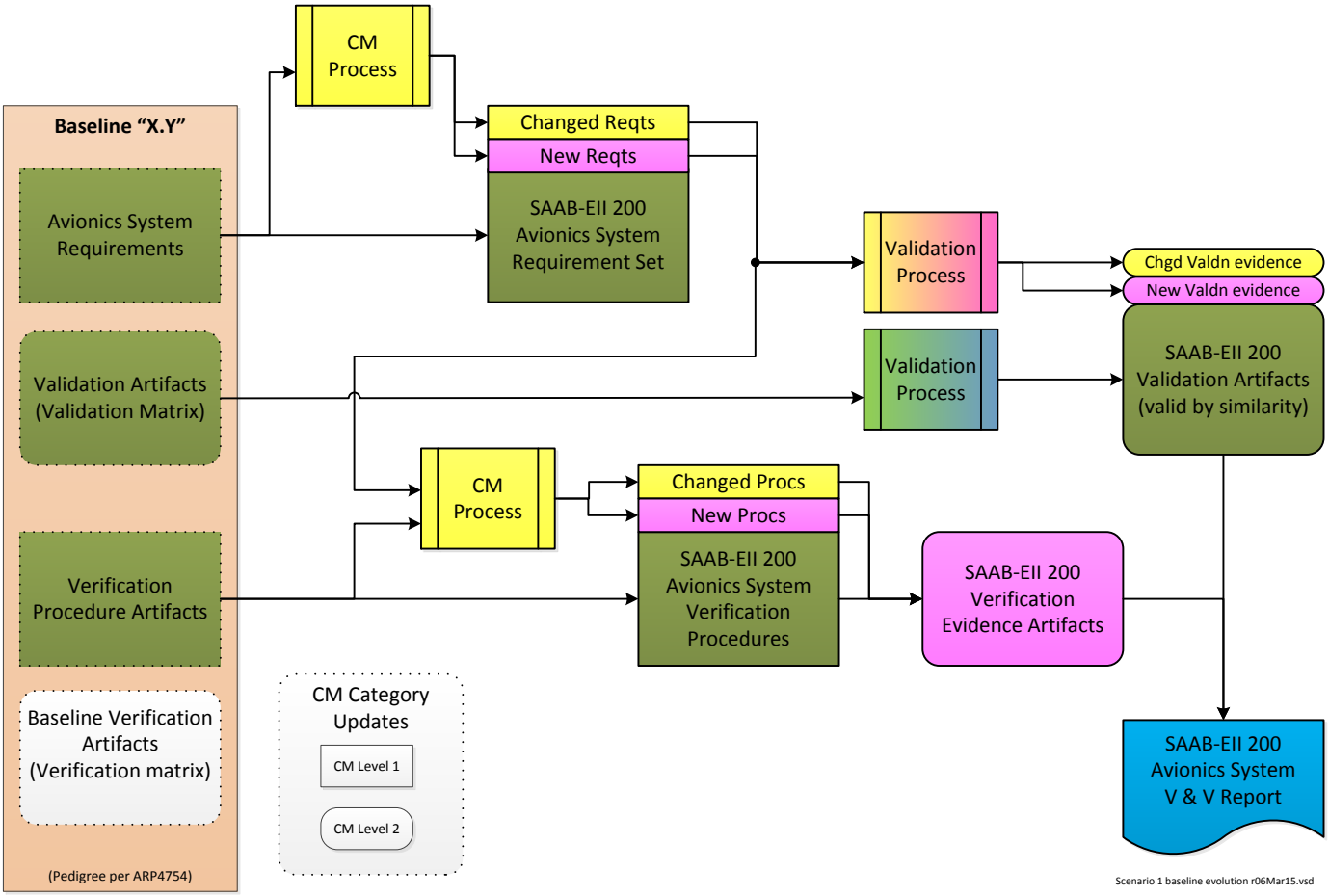


Figure 16 Baseline X.Y Evolution on SAAB-EII 200

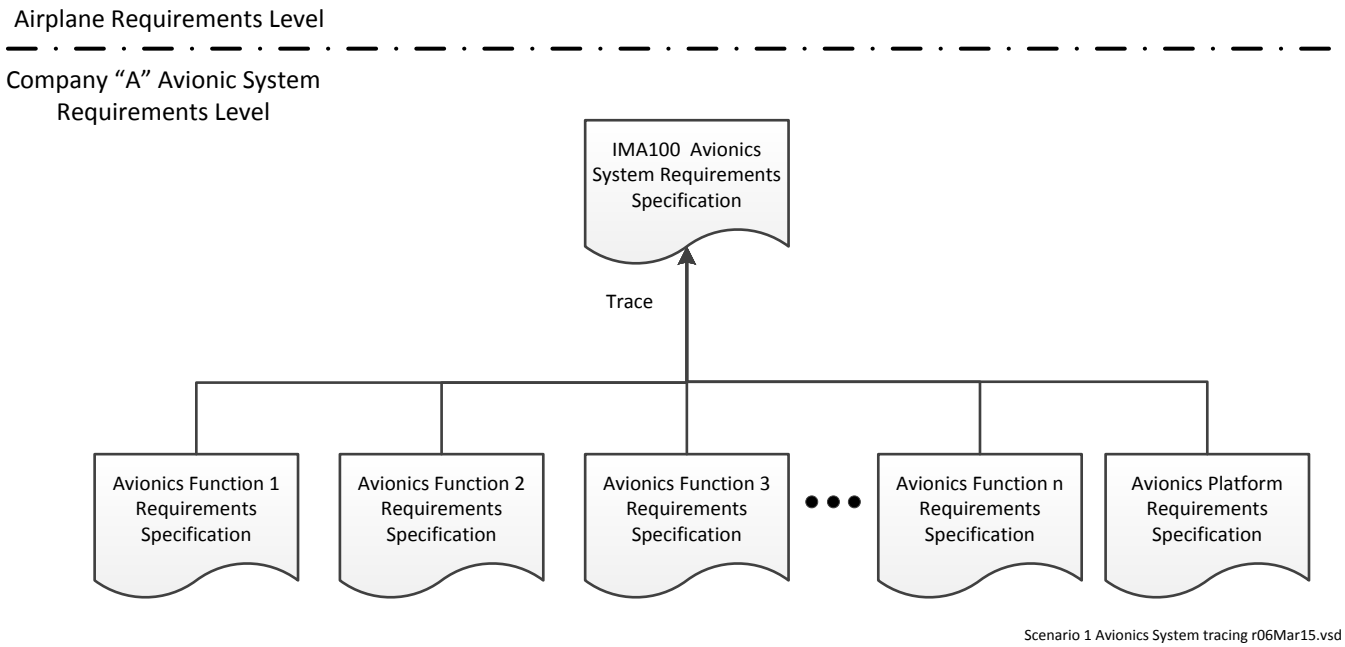


Figure 17 SAAB-EII 200 Baseline Requirements and Tracing

A.2 ASDP200 5.2 Requirements Validation:

- The validation of requirements and specific assumptions ensures that the specified requirements are sufficiently correct and complete so that the developed product will provide the intended functionality.
  - Validation is a structured process for ensuring the correctness and completeness of the set of captured requirements.
  - The validation process also includes capture and evaluation of assumptions made during the requirement capture process to ensure:
    - Assumptions have been explicitly stated,
    - Assumptions are appropriately disseminated, and
    - Assumptions are justified by supporting data.

- Validation activities will be tracked using a matrix containing the requirements and their validation status.
- Validation activities accomplished and the completed validation matrix will be included in the Avionics System Validation and Verification Summary Report.
- Deviations from the validation process will be captured and reported in the Summary Report.
- A comparison of the ARP4754 legacy validation process and the objectives outlined for validation in ARP4754A to identify any areas of the legacy validation process in need of revision.
- The validation process will be revised as appropriate based on the results of this analysis (no revision is anticipated to be required).

A.2 ASDP200 5.2.1 Requirements Validation Methods & Process:

- Requirements will be validated using structured process accomplishing objectives of ARP4754A.
- Requirements will be validated using combination of methods.

- Methods of validation include:
  - Traceability,
  - Analysis (Modeling),
  - Test,
  - Similarity or,
  - Inspection (engineering review).

- The bulk of the avionic systems requirements will be validated through similarity to the certificated baseline, “X.Y”.
- Artifacts will be generated as demonstration of the validation process for all changed or new requirements.
  - Artifacts generated based on validation method used. May include requirement inspections, analysis reports, test procedures or similarity (reuse) analysis.
- Validation of requirements will be accomplished with independence commensurate with the assigned FDAL.

- Requirements and validation status will be summarized in a validation matrix.
- This matrix tracks the validation status of each requirement or assumption and captures the validation methods used to establish the validation result and artifact references capturing the evidence.
- The requirements validation process is invoked as part of the change management process for changed or addition of new requirements.
- An example of validation matrix content shown in Table 25.

Table 25 Example Completed Validation Matrix

				Validation Method						
Unique ID	**Text (Requirement or Assumption)**	**Safety**	**Requirement Source**	**Inspect**	**Analysis**	**Similarity**	**Test**	**Trace**	**Validation Artifact Reference**	**Reqt Valid (Y/N)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	Derived	X	X	X		X	Insp-104	Y
AVSYS-R-xxx		N	Derived	X		X			Insp-517	Y
AVSYS-R-xxx		N	Assumption	X					ECM-SAABEII-CompA-25	Y
AVSYS-R-xxx		N	AVACFT-R-1490	X		X		X	CN-1465	Y
AVSYS-R-456		N	Derived	X	X				CN-5137	Y
Matrix Coding:										
Safety – Y if requirement is safety related.										
Requirement Sources: Parent Reqt ID, Derived, Assumption										
Validation Methods: Inspect – Inspection; Analysis – Analysis (Modeling); S – Similarity; Test – Test; Trace -Traceability;										
Reqt Valid – Y if requirement has completed validation effort and artifact has found requirement valid.										

CN = Change Notice
ECM = Engineering Communication Memo
Insp = Inspection
Reqt = Requirement

A.2 ASDP200 5.3 Requirements Verification:

- Verification of requirements and specific assumptions is the process of ensuring that the completed system has successfully implemented the requirements.
- Verification is a structured process for ensuring implementation complies with the set of captured requirements.
- Verification activities will be tracked using a matrix containing the requirements and their verification status.
- Verification activities accomplished and the revised IMA100V1 verification matrix will be included in the new Avionics System Validation and Verification Summary Report.
- Deviations from the verification process will be captured and reported in the Summary Report.

A.2 ASDP200 5.3.1 Requirements Verification Methods & Process:

- Requirements will be verified using structured process accomplishing objectives of ARP4754A.
- Requirements will be verified using combination of methods:

- Methods of verification include:
  - Test,
  - Analysis (Modeling),
  - Service Experience or,
  - Inspection (engineering review).

- It is anticipated that the bulk of the avionic systems requirements will be verified through test.
- Artifacts will be generated as demonstration of the verification process for all requirements.
- Verification artifacts will be managed appropriate for the function development assurance level.

- Changed or New requirements supporting functions with FDAL A will be verified with independence.
- Changed or New requirements supporting functions with FDAL B & C will be verified with independence as a process goal but may be verified by requirement originators as necessary.
- Changed or New verification test procedures supporting FDAL A will be managed using change management control category 1.
- All unchanged functions and their requirements will be re-verified through execution of legacy verification methodologies so as to ensure unchanged and revised capabilities provide all intended functionality.
- The IMA100 X.Y baseline verification matrix will be updated for completed verification activities and status.
- This matrix tracks the verification status of each requirement and captures the verification method(s) used to establish the verification result and artifact references capturing the verification evidence.

- An example verification Matrix shown in Table 26.

Table 26 Example Completed Verification Matrix

					Verification Method(s)						
Unique ID	**Requirement Text**	**Safety**	**FDAL**	**Associated Function**	**Inspect**	**Analysis**	**Test**	**Service**	**Verification Procedure Reference**	**Verification Artifact Reference**	**Pass / Fail (P/F)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	A	Displays		X			NA	Avionic System SSA V1	P
AVSYS-R-xxx		N	B	FMS	X	X	X		FMS1275	VVTest1275 V1	P
AVSYS-R-xxx		N	A	ABC	X		X		ABC101	VVTest1476 V1	P
AVSYS-R-xxx		N	-	Autopilot	X		X		AP37	VVTest37	P
AVSYS-R-456											

Matrix Coding:
Safety – Y if requirement is safety related.

Verification Methods: Inspect – Inspection; Analysis – Analysis (Modeling); Service – Service Experience; Test – Test (Demonstration)
NA – not applicable

A.2 ASDP200 6 Avionic System Configuration & Change Management:

- Configuration management of development artifacts are the responsibility of the originating group.
- The central Company “A” CM organization provides tools, services and process to assist in this task.
- Artifacts created during the development and used as part of the certification process will be managed per the detailed process described in the “Company A Configuration Management Plan” appropriate to the level of rigor established for the artifact.
- Artifacts to be managed include:
    - Avionic System Development Plan (this document),
    - Avionic system requirements documentation,
    - Avionic system safety assessments,
    - Avionic system validation evidence,
    - Avionic system verification procedures,
    - Avionic system verification evidence,
    - Avionic system validation & verification accomplishment summary.

- Current ARP4754A CM objective satisfaction will be compared to ARP4754A CM objectives for areas of difference identification.
- Any CM process differences will be noted for discussion and negotiated evolution.
- Requirements, safety assessment and verification procedure artifacts will be managed using detail change management process (Change control category 1 aka CM Level 1).
- All other program artifacts will be managed using version control change management process (change control category 2 aka CM Level 2).

A.2 ASDP200 7 Avionic System Process Assurance:

- Process assurance is integral to the development activities to ensure that the system development and supporting processes are appropriate, maintained, and followed.
- Process assurance is performed by the Company “A” Quality Assurance (QA) organization.
- Process assurance is evaluated against:
    - ARP4754A objectives based on development assurance rigor (FDAL),
    - DO-178 objectives based on development assurance rigor (IDAL). See PSAC for specific details.

A.2 ASDP200 8 Certification:

- Certification artifacts to be developed for the IMA100V1 changes include:

    - Avionic System Development Plan (ASDP200 – this document),
    - IMA100 Validation and Verification Summary Report for V1 Configuration,
    - System Safety Assessment (SSA) for IMA100V1 as Installed on the SAAB-EII 200 Airplane,
    - IMA100V1 Plan for Software Aspects of Certification,
    - IMA100V1 Version Description Document,
    - Other DO-178 life cycle documents as necessary.

Editor Note: Only Avionic System Development Plan developed as part of the study.

------ End of ASDP200 Avionic System Development Plan excerpt -----

Appendix A.3 Study Architecture 2 (aka SAAB-EII 300)

Introduction

An example of planning specific change activities for the addition of equipment covered by TSO to a certificated airplane with IMA hosted avionics functionality.

Editor Note: The example scenario provides insight into satisfying ARP4754A development for the modification and may not address all of the certification aspects for the scenario.

Example documentation developed:

Airplane Level

Airplane Project Specific Certification Plan (APSCP300)

Systems Level

Avionic System Development Plan (ASDP300)

Item Level

None – not a feature of the study.

NASA Study Architecture 2	SAAB-EII 300 Project Specific Certification PLan			
ARP4754A, 6.2(a)(b)(c)	SIZE A	FSCM NO	DWG NO APSCP300	REV -
6.6.3	SCALE 1 : 1		SHEET 1 of 1	

REVISIONS				
CN No.	REV	DESCRIPTION	DATE	APPROVED
-	-	Initial release	06 Apr 2015	J Allen

Editor Note: Configuration control of certification plan document is per system control category 1, under full problem report/change management process control.

A.3 APSCP300 1 Plan Purpose:

- This airplane project specific certification plan (PSCP) defines the certification activities planned as part of an equipment addition and modification to the IMA avionics platform on the SAAB-EII 300 airplane.
- The plan will highlight the specific modification activities planned for the addition of a TSO-092C Airborne Ground Proximity Warning System (AGPWS) line replaceable unit (LRU) to the SAAB-EII 300 airplane and integration of the AGPWS into Company "A" IMA100 avionics system. This plan will describe the development and implementation strategy for the modification and the safety aspects of the planned changes.

A.3 APSCP300 2 Project Background:

- Legacy SAAB-EII 300 airplane certificated under 14CFR Part 25 Transport Category airplane
  - Legacy airplane certificated per conventional development processes

Editor Note: Conventional development processes means no specific ARP4754A artifacts were created as part of the development effort.

- Company "A" provided Integrated Modular Avionics (IMA) Model 100 based flight deck functionality (IMA – ATA 42) (see Figure 1)
  - IMA developed to ARP4754, DO-178B, DO-254 & DO-297
  - IMA includes the following functions:
    - Autopilot/autoflight (ATA 22),
    - Communications (ATA23),
    - Displays (ATA31),
    - Navigation/Flight Management (ATA34) and,
    - Maintenance (ATA 45).

A.3 APSCP300 3 Planned Modifications:

- Airplane modification for installation of Company "R" TSO-092C AGPWS LRU
  - Addition of GPWS situational awareness airplane function
    - Includes additional wiring, installation tray,
    - Connection to airplane 28vdc electrical power.
- Existing Avionics platform (IMA), Part Number IMA100, will have the following changes incorporated:
  - AGPWS functional changes to IMA hosted functions:
    - Activation of provisioned AGPWS software function,
    - Activation of included spare digital (ARINC 429), discrete and analog interfaces,
    - Activation of IMA communication network for AGPWS information,
    - Activation of IMA annunciation function for display of AGPWS cautions and warnings.
- Modifications to the IMA100 will be accomplished using existing Company "A" supplier system, software and hardware development processes.
- System architecture modifications presented in Figure 18.
- Modification activity schedule is presented in Table 27.

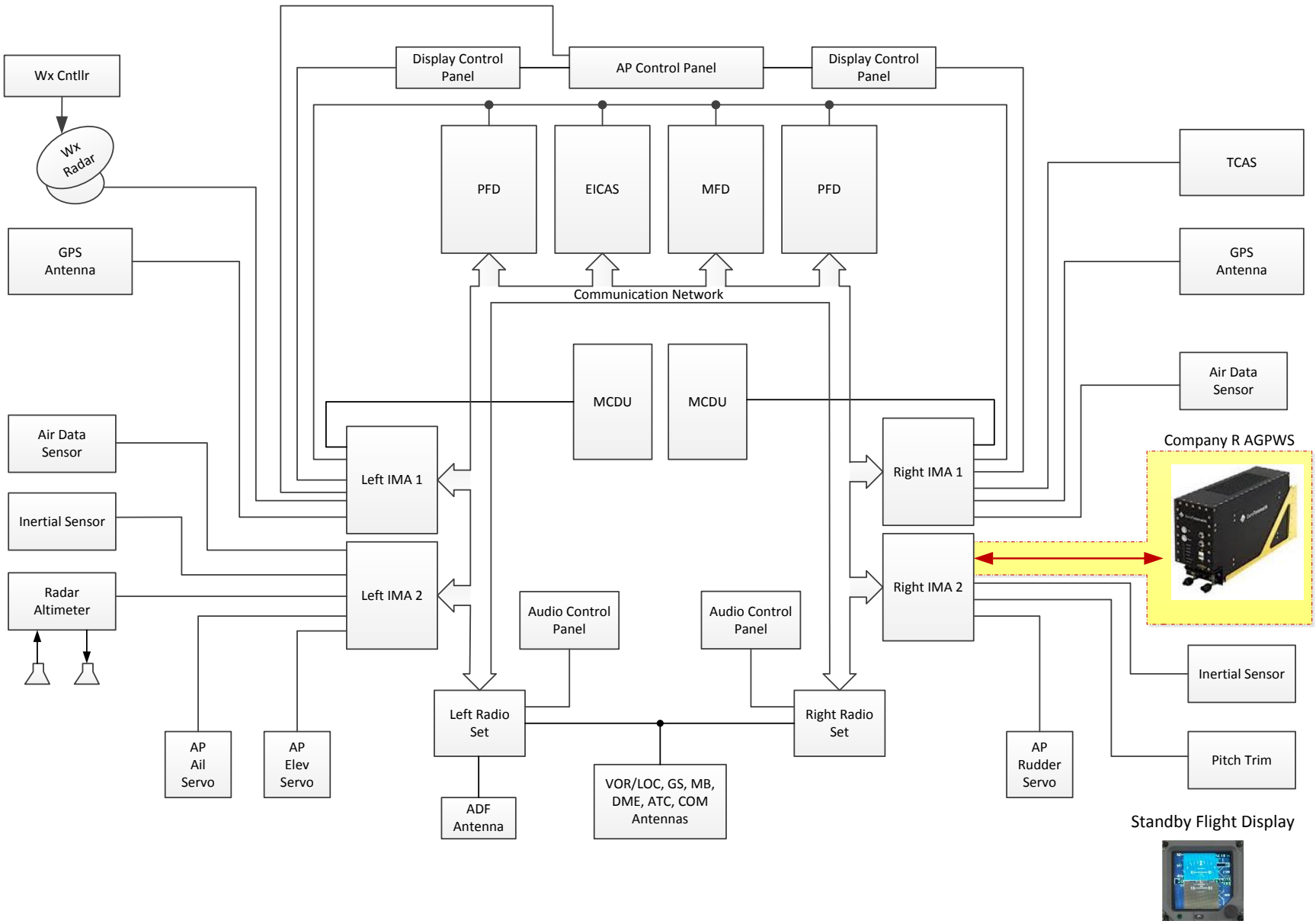


Figure 18 SAAB-EII 300 Modification

Table 27 SAAB-EII 300 Modification Schedule

Change Activity	Projected Completion Schedule
Installation modification drawings & wiring definitions	Airplane Project CDR
Initial Detailed IMA Changes Plan	Company “A” Avionics PDR
Final Detailed IMA Changes Plan	Company “A” Avionics CDR
IMA Implementation Verification	IMA Integration Verification Testing
Airplane Installation Verification	Airplane Ground/Flight Testing
PSCP Compliance Summary	Airplane Certification Package Delivery

A.3 APSCP300 4 Modification Impact Analysis Summary:

A.3 APSCP300 4.1 Change Description:

- SAAB-EII 300 Airplane:
  - AGPWS mounting tray installation in forward EE bay.
  - Addition of AGPWS circuit breaker in forward EE bay electrical panel #2
  - Addition of AGPWS wire harness:
    - AGPWS circuit breaker to Essential 28vdc Power Bus 2,
    - AGPWS circuit breaker to AGPWS mounting tray connector,
    - AGPWS ARINC 429 Output to Right IMA #2,
    - AGPWS Audio Output to Right IMA #2,
    - AGPWS Monitor Output to Right IMA #2,
    - Right IMA #2 Airplane status discretes (AGPWS Inhibit, Gear up/down, Flaps up/down) to AGPWS,
    - Right IMA #2 ARINC 429 Output to AGPWS (Radio Altitude, Glide Slope Deviation, Barometric Data).
- Figure 19 presents preliminary aircraft wiring installation modification.

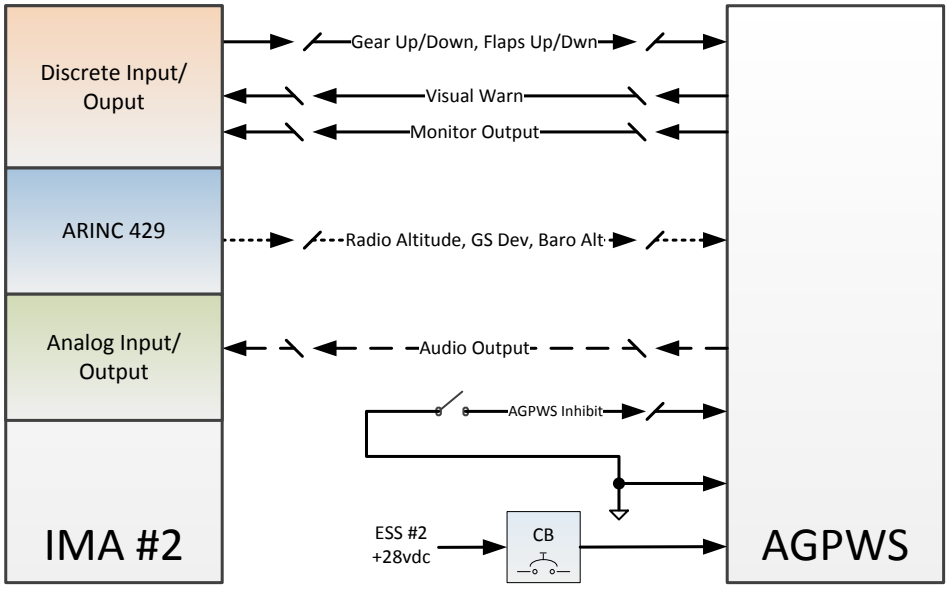


Figure 19 Preliminary SAAB-EII 300 AGPWS Wiring Updates

- IMA-100 Avionic System
  - Table 28 summarizes the IMA functional areas impacted by the change and the most severe failure condition classifications for that function.

Table 28 SAAB-EII 300 IMA Impact Summary

IMA Function	Change Y/N	Impact Description	FC Class.
Autopilot/Autoflight (ATA22)	N	No planned new or changed autopilot functions.	I
Communications (ATA23)	N	No planned new or changed communication functions.	I
Displays (ATA31)	Y	Activation of provisioned AGPWS alerts and warnings.	I*
Navigation/Flight Management (ATA34)	Y	Activation of provisioned AGPWS software function.	III
Maintenance (ATA45)	N	No planned new or changed maintenance functions.	II
Platform	Y	Modification of IMA communication network to add AGPWS communications. Activation of provisioned spare digital (ARINC429), discrete and analog interfaces to/from AGPWS	I
Sensors	N	No planned new or changed Sensor function.	III

*Note: Legacy Displays IMA function implementation is partitioned to support multiple software function criticalities.

A.3 APSCP300 4.2 Change Classification Analysis:

- The planned modifications described in section 4.1 herein have been evaluated per AC 21.101-1 and found to be non-significant.
  - The legacy certification basis for Legacy SAAB-EII 300 will be retained.
- The planned modification outlined in section 4.1 herein has been evaluated per AC 21-40A for change classification, i.e. major or minor:
  - The planned changes have been analyzed and found to have no appreciable effect on:
    - Weight,
    - Balance,
    - Structural strength,
    - Reliability,
    - Characteristics affecting airplane airworthiness.
  - Changes have been found to have a minor impact on the operational characteristics of the flight deck displayed information.
  - Based on the limited impact of the planned changes, the modification is preliminarily classified as *Minor* and will be approved using the SAAB-EII FAA approved "Minor Airplane Change Process" upon certification authority agreement.

- Legacy airplane level development used conventional development techniques and as such did not create ARP4754A objectives evidence.
  - FDAL for Avionics functions was not developed.
  - Airplane function development evidence was not created (Requirements, Validation and Verification).

- Creation of ARP4754A airplane level artifacts for the changes identified in this plan is not advantageous or practical and is therefore not planned. Conventional airplane certification activities will be used. SAAB-EII engineers will review and approve that the activated IMA-100 GPWS avionic functionality meets airplane level functional objectives.

Editor Note: The non-development of ARP4754A airplane artifacts is situationally based. As the IMA-100 already has deactivated functionality for the AGPWS there is little error mitigation benefit in creating ARP4754A development process artifacts as the function and implementation already exists. SAAB-EII review of the Avionics system level artifacts is sufficient to assure the implemented function will be what is desired (validation). If the IMA functionality did not exist or if the added TSO equipment was more than flight crew supplemental information, then a more rigorous satisfaction of ARP4754A objectives may be warranted.

A.3 APSCP300 4.3 Safety Impact of Planned Changes:

- AGPWS is an aid to aircrew intended to supplement existing flight instrument data annunciating the onset of conditions leading to inadvertent contact with the ground.
  - As a supplement, the loss of this warning function is classified as "No Effect".
  - Erroneous warning by the AGPWS function is "Minor" due to in slight increase in crew workload to validate warning through a crosscheck flight instruments and silence erroneous warning using added AGPWS inhibit capability.

- Review of legacy IMA functional failure conditions indicates that:
  - Modifications planned for the Display function do not affect the functional hazard failure condition description or severity. However, the System FHA will be revised to add the AGPWS function failure conditions.
  - Modifications planned for the Platform function may affect other IMA functionality due to added information on communication backbone. IMA backbone communications hardware and software were developed to Level A. Changes to these implementations will follow a Level A change process and be fully analyzed and tested.

A.3 APSCP300 4.4 Modification Implementation Strategy:

- Airplane installation drawings, wiring diagrams will be created by SAAB-EII for the modification of the SAAB-EII 300 airplane.

- All modifications planned to the IMA Avionics platform will be accomplished by Company “A”.
- See Company “A” Avionics System Development Plan for details of planned modification.

A.3 APSCP300 5 Compliance Methods:

- Compliance to the regulations will be shown by analysis, inspection and test.

- Summary for 14CFR 25.1309, Systems, equipment and installations:
  - Installation and design appraisals will be accomplished to establish that the AGPWS installation supports the safety objectives.
  - IMA avionic system development process will be per AC20-174 using ARP4754A at assigned FDAL for activation of AGPWS functionality Similarity and service experience are planned for use in accomplishing the IMA design evolution.
  - Airborne electronic hardware development will be per AC20-152 using DO-254 at assigned IDALs.
  - Airborne software development will be per AC20-115C using DO-178B at assigned IDALs.
  - Safety assessments (FHA, PSSA, SSA) per ARP4761.
- IMA development per AC-148 and AC-170.
- See Company “A” **Avionic System Development Plan** for details of modification process.

Title	Avionic System Development Plan	Doc No.	ASDP300	Date	5/28/2015

NASA Study Architecture 2	Company A Avionic System Development Plan			
	SIZE A	FSCM NO	DWG NO ASDP300	REV -
	SCALE 1 : 1		SHEET 1 OF 1	

REVISIONS				
	REV	DESCRIPTION	DATE	APPROVED
	-	Initial release		

Editor Note: Configuration control of avionics system development plan document is per system control category 2, using version change management process control.

A.3 ASDP300 1 Introduction:

- This Plan describes the system development process for the AGPWS installation modifications planned for the IMA hosted functionality installed on the SAAB-EII 300 airplane.
- Plan addresses engineering life cycle evolution from ARP4754 to ARP4754A including function design, requirements generation, analysis, requirements validation, function verification for re-used functionality and modified functionality.
- Plan includes the identification and assignment of the appropriate Functional Development Assurance Level (FDAL) rigor to be performed for changed or new systems functions as well as Item Development Assurance (IDAL) assignment for airborne software development of new functionality.
- Plan fulfills the intent of system development objectives planning for:
    - Development (ARP4754A section 4),
    - Requirements Management (ARP4754A section 5.3),
    - Validation (ARP4754A section 5.4),
    - Verification (ARP4754A section 5.5).

A.3 ASDP300 2 Avionic System Description:

- The Company “A” IMA100 Avionics Flight Deck integrates multiple avionic functions into a single Integrated Modular Avionic (IMA) system implementation:

    - The Integrated Modular Avionics (IMA – ATA 42) includes the following functions:
        - Baseline IMA includes the following system functions:
            - Autopilot/autoflight (ATA 22),
            - Communications (ATA23).
            - Displays (ATA31),
            - Navigation/Flight Management (ATA34), and
            - Maintenance (ATA 45).

A.3 ASDP300 3 Avionic System Development Overview:

- The legacy Company “A” IMA100 avionic system was developed in accordance with ARP4754, DO-178B, DO-254 & DO-297.
- The avionics legacy ARP4754 system development process will be evolved and structured to ensure satisfaction of ARP4754A objectives commensurate with a developed function development assurance level (FDAL) for revised and new functions.

- This plan responds to the following ARP4754A planning objectives:
    - Requirements Management,
    - Requirements Validation,
    - Requirement Verification,
    - Configuration Management,
    - Process Assurance.

- The avionics system development process is based on re-using an integrated avionic implementation previously certificated on the same SAAB-EII 300 airplane type.
- The SAAB-EII 300 avionics system development process will use a combination of similarity/service experience to previous program ARP4754 objective data and the generation of new ARP4754A objective evidence for the changed IMA functionality to satisfy the SAAB-EII 300 ARP4754A development life cycle.

- Figure 20 presents a high level summary of the Avionics System development activities.
- Table 29 summarizes the objective evolution and highlights new configuration management (CM) system control (SC) category.

    - Changed Display function (ATA31):
        - Capture requirements associated with changed Display functionality (activation of AGPWS provisional function) per newly assigned FDAL.
        - Validate new or changed Display requirements per ARP4754A compliant process.
        - Validate unchanged Display requirements per ARP4754A similarity to certificated functionality.
        - Verify old and new Display implementation meets intended Display function requirements.

    - Activate AGPWS function (ATA34)
        - Activate provisional AGPWS function requirements per newly assigned FDAL.
        - Validate new or changed AGPWS requirements per ARP4754A compliant process.
        - Validate unchanged AGPWS requirements per ARP4754A similarity to certificated functionality.
        - Verify old and new AGPWS implementation meets intended function requirements.

    - Changed Platform function (ATA42):

        Input/Output (I/O)-
        - Capture I/O requirements for added AGPWS digital (ARINC 429), analog (audio), and discrete (landing gear status, warning, monitor) interfaces
        - Validate new or changed I/O requirements per ARP4754A compliant process.
        - Validate unchanged I/O requirements per ARP4754A similarity to certificated functionality.
        - Verify old and new I/O implementation meets intended AGPWS function requirements.

        Communication (Comm) Network-
        - Capture Comm network requirements for added AGPWS digital (ARINC 429), analog (audio), and discrete (landing gear status, warning, monitor) interfaces
        - Validate new or changed Comm requirements per ARP4754A compliant process.
        - Validate unchanged Comm requirements per ARP4754A similarity to certificated functionality.
        - Verify old and new Comm implementation meets intended AGPWS function requirements.

Table 29 ARP4754 Objectives & Configuration Evolution Summary

4754 Objective / Evidence	Legacy CM SCC Category	4754A Objective / Evidence	4754A CM SCC Category
Display Function (ATA31)			
Display Function Requirement Set	NA	New and Changed Display Function Requirement Set	SC1
Requirements Validation (validation matrix, report)	NA	Requirements Validation per FDAL	SC2
Requirements Verification (verification matrix, report)	NA	Requirements Verification per FDAL	SC2
AGPWS Function (ATA34)			
AGPWS Function Requirement Set	NA	Changed AGPWS Function Requirement Set	SC1
Requirements Validation (validation matrix, report)	NA	Requirements Validation per FDAL	SC2
Requirements Verification (verification matrix, report)	NA	Requirements Verification per FDAL	SC2
IMA Platform			
I/O Requirement Set (A429, Analog, Discrete)	NA	New and Changed I/O Requirement Set	SC1
Comm Requirement Set (A429, Analog, Discrete)	NA	New and Changed Comm Requirement Set	SC1
I/O & Comm Requirements Validation (validation matrix, report)	NA	Requirements Validation per FDAL	SC2
I/O & Comm Requirements Verification (verification matrix, report)	NA	Requirements Verification per FDAL	SC2

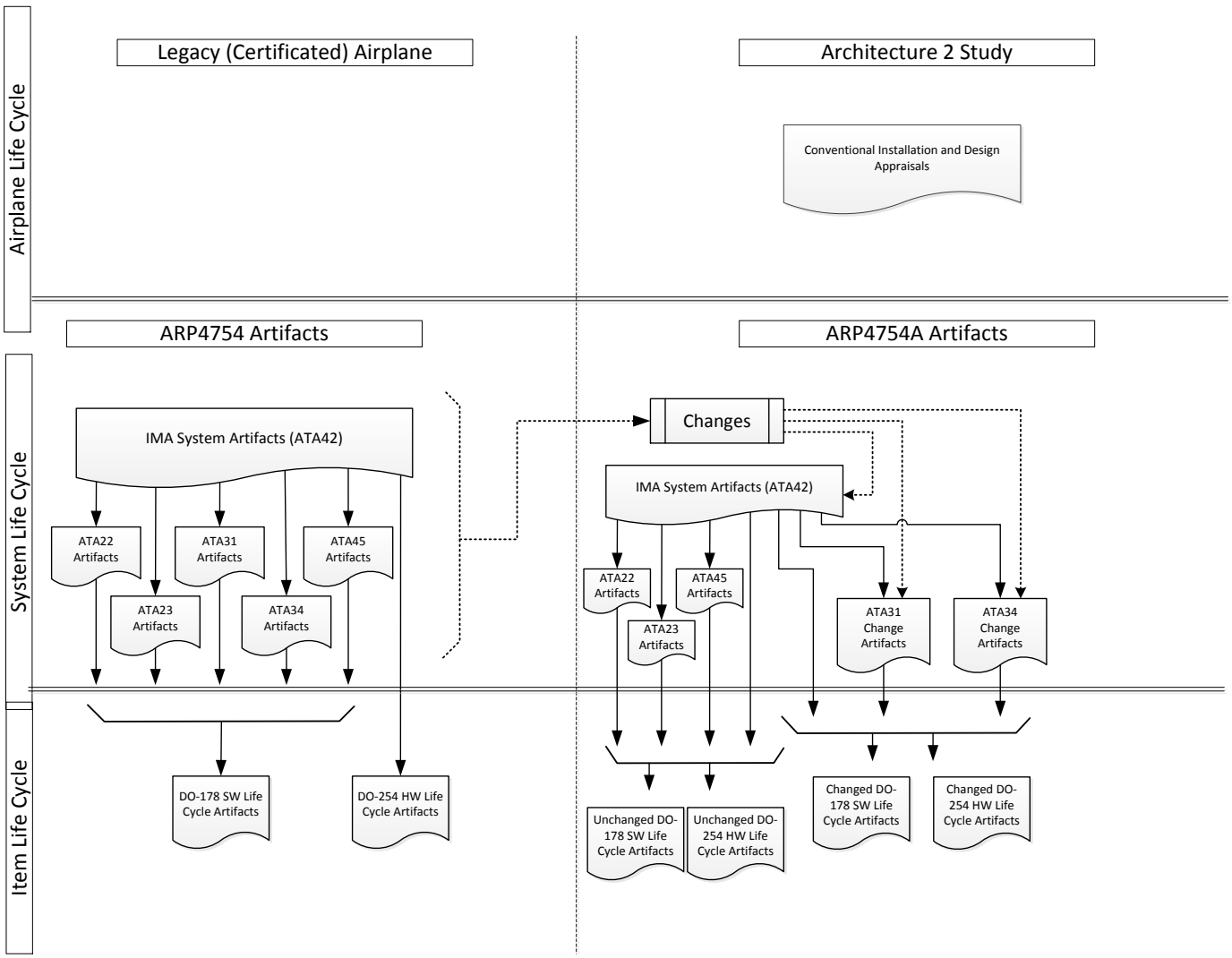


Figure 20 SAAB-EII 300 Avionics System Change Implementation Development Plan

A.3 ASDP300 3.1 Reuse Analysis Plan:

- Table 30 presents the top level SAAB-EII 300 Avionics Development plan and strategy for reuse of baseline avionic system functionality.
- Table 31 presents the planned program strategy nomenclature descriptions.

Table 30 SAAB-EII 300 Avionics Reuse Strategy

1	2	3	4	5	6
System Functional Area	**System Func or Item**	**Existing FDAL /IDAL**	**New FDAL /IDAL**	**Rigors Differ**	**Program Strategy**
Autopilot/Autoflight (ATA 22)	Sys	NA	NA	NA	Reapply
SW - AFCS App	Item	A	A	No	Reuse
HW - AP Control Panel	Item	B	B	No	Reuse
HW - Pitch servo	Item	B	B	No	Reuse
HW - Roll Servo	Item	B	B	No	Reuse
HW - Yaw Servo	Item	B	B	No	Reuse
HW - Pitch Trim Servo	Item	B	B	No	Reuse
Communications (ATA 23)	Sys	NA	NA	NA	Reapply
SW - Radio Tune App - Comm	Item				Reuse
HW - Radio Set - Comm	Item				Reuse
HW - Radio Set - Datalink	Item				Reuse
HW - Antennas - Comm	Item				Reuse
HW - Audio Control Panel	Item				Reuse
HW - TCAS	Item				Reuse
Displays (ATA 31)	Sys	NA	A	Yes	Adapt
SW - PFD Graphics Common App	Item	A	A	No	Reuse
SW - PFD Graphics Instrument "T" App	Item	B	B	No	Reuse
SW - Warn Function App	Item	A	A	No	RWC
SW - Warn Function Common App	Item	A	A	No	Reuse
SW - WX Graphics App	Item				Reuse
HW - Display Control Panel	Item	B	B	No	Reuse
HW - Standby Instrument	Item				Reuse
HW - Display Unit - PFD	Item	A	A	No	Reuse
HW - Display Unit - EICAS	Item	A	A	No	Reuse
HW - Display Unit - MFD	Item	B	B	No	Reuse
Navidation/Flight Management (ATA34)	Sys	NA	B	Yes	Adapt
SW - Flight Management App	Item		B	No	Reuse
SW - Take off Performance App	Item		B	No	Reuse
SW - MCDU Host App	Item				Reuse
SW - GPS Nav App	Item				Reuse
SW - Radio Tune App - Nav	Item				Reuse
SW - AGPWS	Item		C	No	New
HW - Inertial Sensor	Item				Reuse
HW - Radio Set - Nav	Item				Reuse
HW - Antennas - Nav	Item				Reuse
HW - GPS Antenna	Item				Reuse
HW - MCDU	Item				Reuse
Maintenance (ATA45)	Sys	NA	C	No	Reapply
SW - CMC App	Item	D	C	No	Reuse
IMA Platform	Sys	NA	A	Yes	Adapt
SW - Operating System App	Item	A	A	No	Reuse
SW - Middleware Apps	Item	A	A	No	Reuse
SW - HW Abstraction Layer App	Item	A	A	No	Reuse
SW - Comm Network Core App	Item	A	A	No	RWC
SW - Comm Network Messaging App	Item	A	A	No	RWC
SW - Dataload App	Item	A	A	No	Reuse
HW - Power Supply	Item	A	A	No	Reuse
HW - Cabinets	Item	A	A	No	Reuse
HW - Multipurpose computers	Item	A	A	No	Reuse
HW - Comm Network	Item	A	A	No	Reuse
HW - Input / Output	Item	A	A	No	RWC
Sensors	Sys	NA	D	No	Adapt
HW - AGPWS	Item	NA		No	New
HW - Weather Radar	Item				Reuse
HW - Weather Radar Controller	Item				Reuse

Table 31 SAAB-EII 300 Reuse Strategy Nomenclature

Determining the Item Change Type	
Program Strategy (Column 6)	**Description**
Reuse	Reusing an item (SW Application or HW element) from another aircraft program or previous certification without modification to the item itself.
Reuse with Change (RWC)	Reusing an item from another airplane program or previous certification with modifications to the item.
New	Develop a new item; i.e. this is the first instance of this function implementation.

Determining the System Change Type	
Program Strategy (Column 6)	**Description**
Reapply	Select Reapply if the entire system is being reused from another/same airplane program (i.e., all of the items in the system are identified as Reapply). The activities are related to adding traceability from existing system requirements to new airplane program/revised Function requirements and integration of the system.
Adapt	Select Adapt if one or more of the items is identified as Reuse with Change (RWC) with other items are identified as Reuse.
New	Select New if all or nearly all items are New

A.3 ASDP300 4 Avionic System Safety:

- The system safety process includes requirements development as well as implementation verification activities that support the avionic system development.
- This process provides a methodology to evaluate airplane function failure conditions and the avionic system design performing these functions to establish that the identified hazards have been properly addressed.

- The avionics systems development process will include the following safety activities:

  - Avionic System Functional Hazard Analysis
    - Updated hazard evaluation for activation of AGPWS on SAAB-EII 300 airplane.
  - Preliminary Avionic System Safety Assessment Supplement
    - Supplement IMA100V2 PSSA will be created to evaluate planned implementation of AGPWS function against system FHA failure condition(s).
    - Safety requirement development as necessary to support AGPWS implementation
    - FDAL / IDAL assignment (assignment substantiation) for AGPWS revisions development
  - Avionic System Safety Assessment IMA100V2 SSA (revision to existing analysis to incorporate applicable Display changes and addition of AGPWS failure condition analysis result),
  - Avionic System Common Cause Analysis (update as necessary to support PSSA/SSA revisions).

Editor Note: IMA100V2PSSA and IMA100V2 SSA were not developed as part of the example.

A.3 ASDP300 5 Avionic System Requirements Development, Validation & Verification:

- Requirements development, validation and avionic system requirement verification plans are discussed in this section.
- Figure 21 presents the high level avionics system development process flow.
- Any changes in FDAL or IDAL assignments between the established baseline artifact level of rigor and the modification program assigned level will be evaluated on a case-by-case basis for a negotiated development approach.

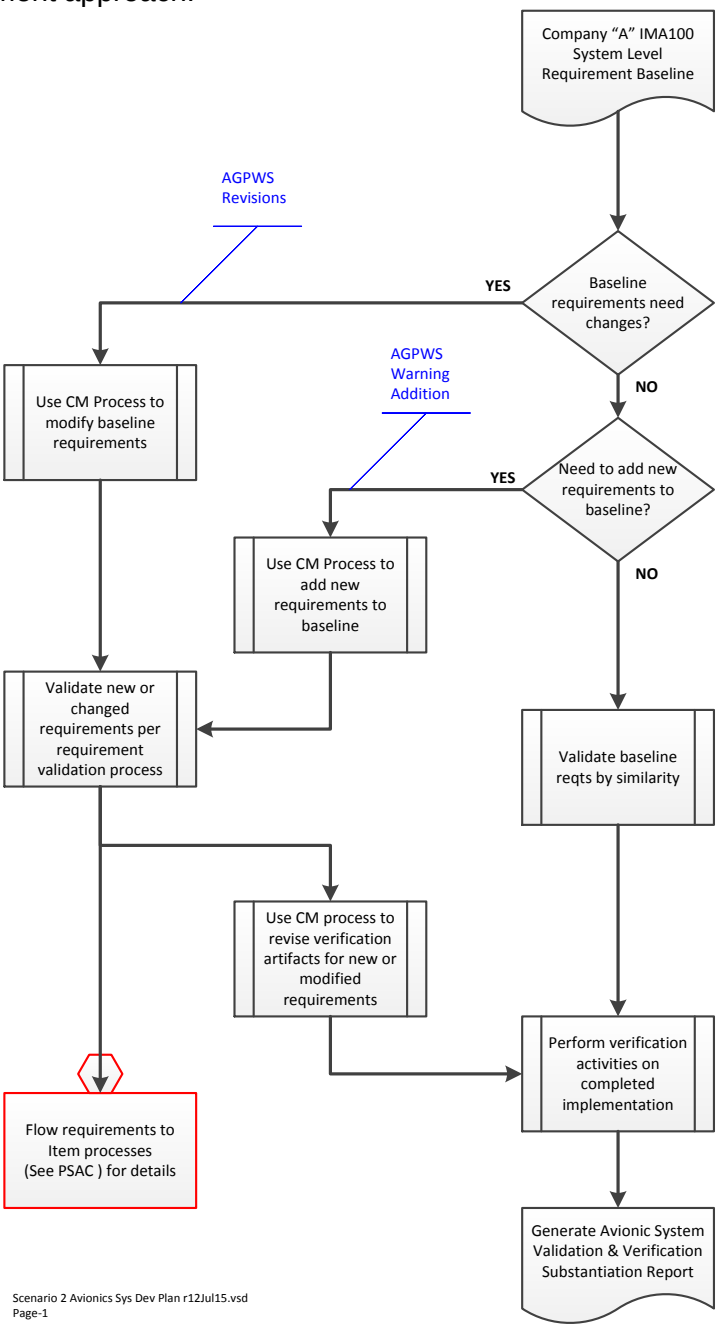


Figure 21 SAAB-EII 300 System Requirements Activity Plan

A.3 ASDP300 5.1 Requirements Development & Management:

- The IMA100 Avionic System "X.Y" requirements set will form the baseline for the SAAB-EII 300 Avionic System modification program.
- The baseline requirements were developed to the level of rigor commensurate with the level of assurance assigned to the implementing software (though not identified as FDAL) as shown in Table 30. Each requirement includes the following information:
  - Unique requirement identifier,
  - Requirement text,
  - Rationale (reason for having the requirement if requirement was derived),
  - Parent trace link (if requirement traceable to a parent),
  - Safety related attribute.

- As part of the SAAB-EII 300 development process, the baseline Company "A" avionic system Navigation and Display requirement sets will be evolved from the "X.Y" baseline to new IMA100V2.

- See Figure 22 for the artifact evolution plan.

- Requirements that need to be modified will be managed through the configuration management process to ensure traceability to the baseline.
- Changed requirements will be revalidated using the requirement validation process.
- New requirements (GPWS function) will be activated in the baseline requirement set using the CM process and validated using the validation process.

- An illustration of the requirement levels and tracing between these levels is shown in Figure 23.

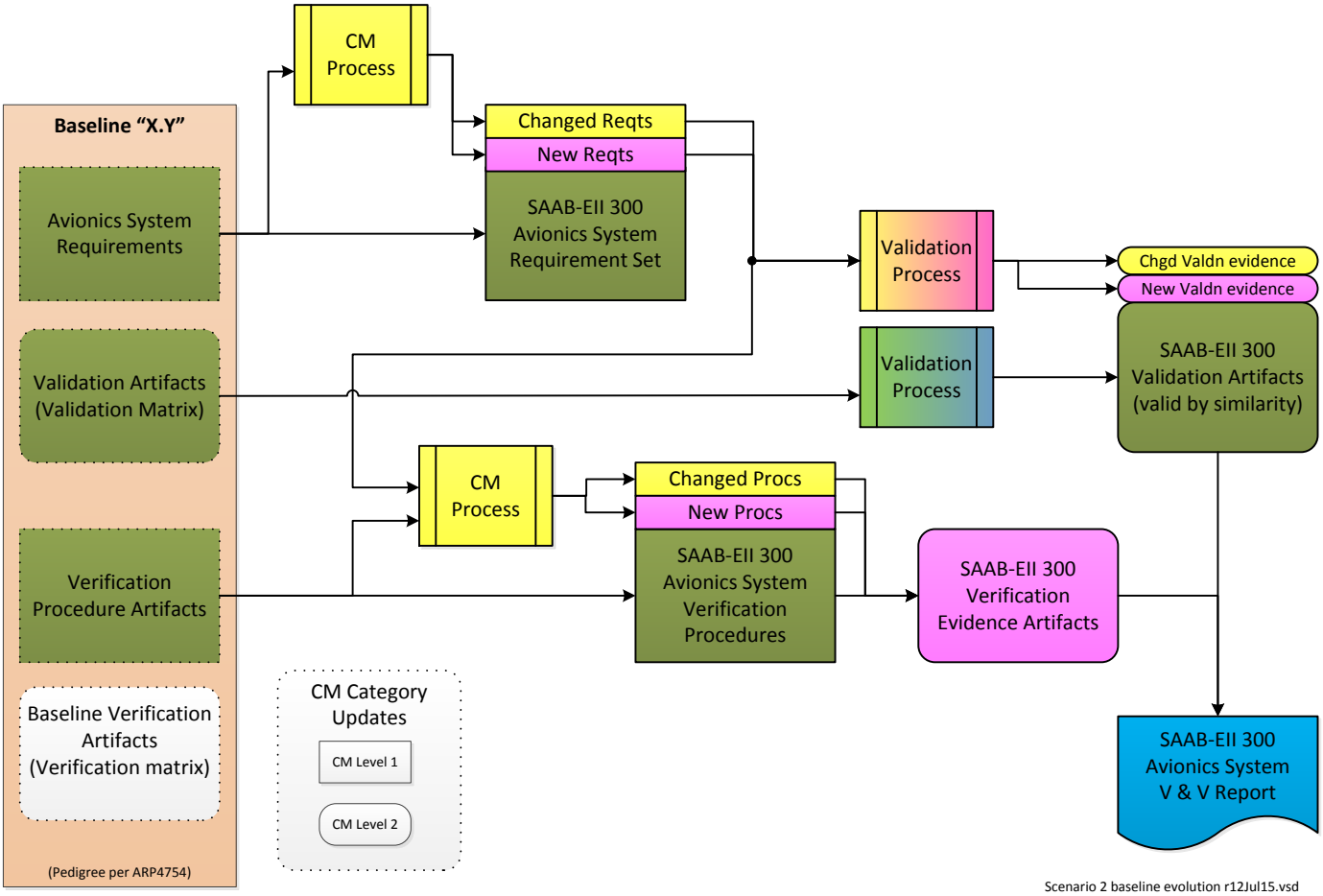


Figure 22 Baseline X.Y Evolution on SAAB-EII 300

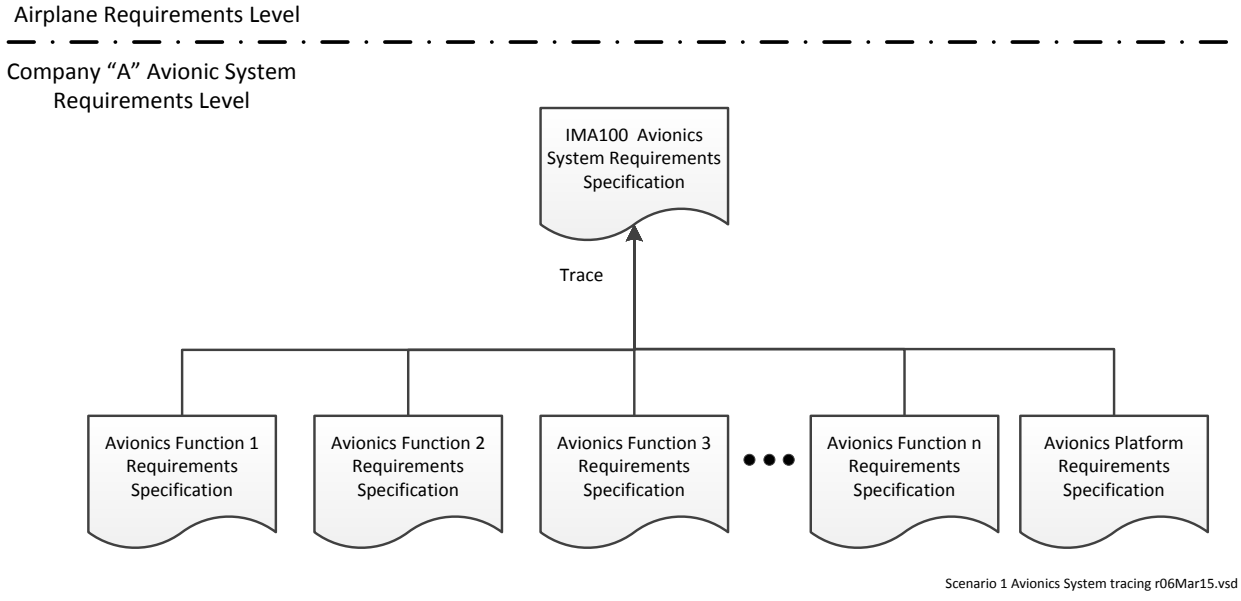


Figure 23 SAAB-EII 300 Baseline Requirements and Tracing

A.3 ASDP300 5.2 Requirements Validation:

- The validation of requirements and specific assumptions ensures that the specified requirements are sufficiently correct and complete so that the developed product will provide the intended functionality.
    - Validation is a structured process for ensuring the correctness and completeness of the set of captured requirements.
    - The validation process also includes capture and evaluation of assumptions made during the requirement capture process to ensure:
        - Assumptions have been explicitly stated,
        - Assumptions are appropriately disseminated, and
        - Assumptions are justified by supporting data.
- Validation activities will be tracked using a matrix containing the requirements and their validation status.
- Validation activities accomplished and the completed validation matrix will be included in the Avionics System Validation and Verification Summary Report.
- Deviations from the validation process will be captured and reported in the Summary Report.
- A comparison of the ARP4754 legacy validation process and the objectives outlined for validation in ARP4754A to identify any areas of the legacy validation process in need of revision.
- The validation process will be revised as appropriate based on the results of this analysis (no revision is anticipated to be required).

A.3 ASDP300 5.2.1 Requirements Validation Methods & Process:

- Requirements will be validated using structured process accomplishing objectives of ARP4754A.
- Requirements will be validated using combination of methods:

- Methods of validation include:
    - Traceability,
    - Analysis (Modeling),
    - Test,
    - Similarity or,
    - Inspection (engineering review).

- The bulk of the avionic systems requirements will be validated through similarity to the certificated baseline, “X.Y”.
- Artifacts will be generated as demonstration of the validation process for all changed or new requirements.
- Validation of requirement sets will be accomplished with independence commensurate with the assigned FDAL.
- Requirements will be summarized in a validation matrix.
- This matrix tracks the validation status of each requirement or assumption and captures the validation methods used to establish the validation result and artifact references capturing the evidence.
- The requirements validation process is invoked as part of the change management process for changed or addition of new requirements.

- An example validation Matrix shown in Table 32.

Table 32 Example Completed Validation Matrix

				Validation Method						
Unique ID	**Text (Requirement or Assumption)**	**Safety**	**Requirement Source**	**Inspect**	**Analysis**	**Similarit**	**Test**	**Trace**	**Validation Artifact Reference**	**Reqt Valid (Y/N)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	Derived	X	X	X		X	Insp-104	Y
AVSYS-R-xxx		N	Derived	X		X			Insp-517	Y
AVSYS-R-xxx		N	Assumption	X					ECM-SAABEII-CompA-25	Y
AVSYS-R-xxx		N	AVACFT-R-1490	X		X		X	CN-1465	Y
AVSYS-R-456		N	Derived	X	X				CN-5137	Y
Matrix Coding:										
Safety – Y if requirement is safety related.										
Requirement Sources: Parent Reqt ID, Derived, Assumption										
Validation Methods: Inspect – Inspection; Analysis – Analysis (Modeling); S – Similarity; Test – Test; Trace -Traceability;										
Reqt Valid – Y if requirement has completed validation effort and artifact has found requirement valid.										

CN = Change Notice
ECM = Engineering Communication Memo
Insp = Inspection
Reqt = Requirement

A.3 ASDP300 5.3 Requirements Verification:

- Verification of requirements and specific assumptions is the process of ensuring that the completed system has successfully implemented the requirements.
- Verification is a structured process for ensuring implementation complies with the set of captured requirements.
- Verification activities will be tracked using a matrix containing the requirements and their verification status.
- Verification activities accomplished and the revised IMA100V2 verification matrix will be included in the new Avionics System Validation and Verification Summary Report.
- Deviations from the verification process will be captured and reported in the Summary Report.

A.3 ASDP300 5.3.1 Requirements Verification Methods & Process:

- Requirements will be verified using structured process accomplishing objectives of ARP4754A.
- Requirements will be verified using combination of methods:
- Methods of verification include:
    - Test,
    - Analysis (Modeling),
    - Service Experience or,
    - Inspection (engineering review).
- It is anticipated that the bulk of the avionic systems requirements will be verified through test.
- Artifacts will be generated as demonstration of the verification process for all requirements.
- Verification artifacts will be managed appropriate for the function development assurance level.
- Changed or New requirements supporting functions with FDAL A will be verified with independence.
- Changed or New requirements supporting functions with FDAL B & C will be verified with independence as a process goal but may be verified by requirement originators as necessary.
- Changed or New verification test procedures supporting FDAL A will be managed using change management system control category 1.
- All unchanged functions and their requirements will be re-verified through execution of legacy verification methodologies so as to ensure unchanged and revised capabilities provide all intended functionality.
- The IMA100 X.Y baseline verification matrix will be updated for completed verification activities and status.
- This matrix tracks the verification status of each requirement and captures the verification method(s) used to establish the verification result and artifact references capturing the verification evidence.

- An example verification Matrix shown in Table 33.

Table 33 Example Completed Verification Matrix

					Verification Method(s)						
Unique ID	**Requirement Text**	**Safety**	**FDAL**	**Associated Function**	**Inspect**	**Analysis**	**Test**	**Service**	**Verification Procedure Reference**	**Verification Artifact Reference**	**Pass / Fail (P/F)**
AVSYS-R-010	The primary display system and the standby display shall be independent.	Y	A	Displays		X			NA	Avionic System SSA V2	P
AVSYS-R-xxx		N	C	AGPWS	X	X	X		AGPWS1275	VVTest1275 V2	P
AVSYS-R-xxx		N	A	Platform	X		X		Platform101	VVTest1476 V2	P
AVSYS-R-xxx		N	-	Autopilot	X		X		AP37	VVTest37	P
AVSYS-R-456											

Matrix Coding:
Safety – Y if requirement is safety related.

Verification Methods: Inspect – Inspection; Analysis – Analysis (Modeling); Service – Service Experience; Test – Test (Demonstration)
NA – not applicable

A.3 ASDP300 6 Avionic System Configuration & Change Management:

- Configuration management of development artifacts are the responsibility of the Company “A” originating group.
- The central Company “A” CM organization provides tools, services and process to assist in this task.
- Artifacts created during the development and used as part of the certification process will be managed per the detailed process described in the “Company A Configuration Management Plan” appropriate to the level of rigor established for the artifact.
- Artifacts to be managed include:
  - Avionic System Development Plan (this document),
  - Avionic system requirements documentation,
  - Avionic system safety assessments,
  - Avionic system validation evidence,
  - Avionic system verification procedures,
  - Avionic system verification evidence,
  - Avionic system validation & verification accomplishment summary.
- Current ARP4754 CM objective satisfaction will be compared to ARP4754A CM objectives for areas of difference identification.
- Any CM process differences will be noted for discussion and negotiated evolution.
- Requirements, safety assessment and verification procedure artifacts will be managed using detail change management process (Change control level 1 aka System CM category 1)
- All other program artifacts will be managed using version control change management process (change control level 2 aka System CM Category 2).

A.3 ASDP300 7 Avionic System Process Assurance:

- Process assurance is integral to the development activities to ensure that the system development and supporting processes are appropriate, maintained, and followed.
- Process assurance is performed by the Company “A” Quality Assurance (QA) organization.
- Process assurance is evaluated against:
  - ARP4754A objectives based on development assurance rigor (FDAL),
  - DO-178 objectives based on development assurance rigor (IDAL). See PSAC for specific details.
  - DO-254 objectives based on development assurance rigor (IDAL). See PHAC for specific details.

A.3 ASDP300 8 Certification:

- Certification artifacts to be developed for the IMA100V2 changes include:
  - Avionic System Development Plan (ASD300 – this document),
  - IMA100 Validation and Verification Summary Report for V2 Configuration,
  - System Safety Assessment (SSA) for IMA100V2 as Installed on the SAAB-EII 300 Airplane,
  - IMA100V2 Plan for Software Aspects of Certification,
  - IMA100V2 Version Description Document,
  - Other DO-178 life cycle documents as necessary,
  - Other DO-254 life cycle documents as necessary.

Editor Note: Only the Avionic System Development Plan developed as part of the study.

------ End of ASDP300 Avionic System Development Plan excerpt -----

Appendix B Industry Survey Response Data

B.1 1 Introduction

This appendix summarizes the ARP4754A application lessons learned sought out from industry in order to augment the experiences of the case study data in Appendix A.

B.1 2 Gathering Additional Information

Two approaches were undertaken as part of the project to augment the lessons learned from the case studies presented in Appendix A. First, a questionnaire was developed around the specific project task study interest areas and then disseminated to the aviation industry for response.

A second, a group discussion roundtable was also accomplished to obtain additional ARP application information in three specific focus areas.

The following subsections present the characteristics of each of these information gathering activities and the summarized themes resulting from the received data responses.

B.1 2.1 Questionnaire Data

A set of approximately 50 questions was developed to solicit individual or company lessons learned in the application of ARP4754A. Section B.2 presents the disseminated questionnaire and format. The questions were grouped so as to obtain a number of different perspectives on a specific ARP application area. The following application experience groupings were used:

- General,
- Certification,
- Planning,
- Development Process,
- Safety,
- ARP4754A Document and Authority guidance Material and,
- Respondent Characteristics.

Eleven (11) responses were received to the questionnaire. Responses were received from:

- Regulatory authority,
- Aircraft Manufacturer,
- Engine Manufacturer,
- System Supplier,
- Aviation Consultant.

B.1 2.2 Roundtable Discussion

Additional industry experience was solicited through a roundtable discussion held with twenty (20) ARP4754A experienced SAE S18 Committee members. Three different focus areas were discussed:

1) Lessons learned in applying ARP4754A (e.g. DAL assignment, objective satisfaction),
2) Engineering judgment in ARP4754A (where used, how leveraged, making up for a lack of experienced engineering judgment),
3) Certification lessons learned on application of ARP4754A (e.g. issues with guidance, issues with ARP application, issues with certification policies).

Discussion Participants have been encoded in the notes as follows:

- AC – Aircraft manufacturer,
- SYS – System manufacturer,
- EQ – Equipment manufacturer,
- REG – Regulatory authority.

Section B.3 contains the captured notes from the roundtable discussion.

B.1 2.2.1 Discussion Area 1: Lessons Learned Summary

Three basic themes were identified in the lessons learned and DAL assignment area. The themes include:

- Users are having difficulty in applying concepts of FDAL/IDAL assignment especially where non-complex items are involved.
- Users are experiencing AC/System FDAL escalation due to assignment of IDAL using alternate means.
- Users found new ARP contains improved wording that is different from original ARP and first impressions of “extra” work were mitigated through better understanding of the objectives vs what was already being accomplished.

B.1 2.2.2 Discussion Area 2: Engineering Judgment

The primary themes identified during the engineering judgment discussions include:

- Validation activity needs domain knowledge and experience history in order to review requirements. Two ways to obtain domain knowledge: buy it or experience it over time.
- Regulatory authority also needs experience in order to apply appropriate engineering judgments.
- Company cultures influence specific judgments made during the process (culture is safety focused- the judgments will be safety focused, culture is cost focused – judgments will be influenced to minimize expenditures).

B.1 2.2.3 Discussion Area 3: Certification Lessons

The primary themes identified during the certification discussions include:

- Industry should not have to spend time educating the regulatory authority on the process objectives.
- Variability in regulatory expectations by individual and location. Difficult for industry to determine appropriate program scope when there are significant differences in satisfying the ARP objectives program to program.
- Variability in establishing the means of evaluating the means of ARP satisfaction. Some regulatory authorities look for intent of accomplishing objectives while others look for checklist style compliance.

B.2 – Study Questionnaire

NASA ARP4754A Study Questionnaire

Background

This questionnaire is being circulated in the commercial aviation industry to gather and expand the experiences, issues and lessons learned on the application of ARP4754A. Questionnaire responses will be consolidated and analyzed to provide additional inputs to the SAE ARP4754A industry document revision process and published as part of NASA Contract NNL13AA06B, Task NNL14AB74T, "Application of SAE ARP-4754A to the Development of Complex and Safety-Critical System".
Please use this opportunity to relate your experiences on the application of ARP4754A system development objectives on a specific project or within your organization. Your experienced based comments provide a valuable perspective on the clarity and application of current industry development assurance objectives. Please be as descriptive in your responses as time allows. It is anticipated that you may require 30-45 minutes to complete this questionnaire.
Raw response data will only be seen by EII researchers. All questionnaire responses will be held in confidence and all sources de-identified prior to response consolidation and final report development activities.

General:

1	**Describe the extent and circumstances of your ARP4754A application (e.g. TC, ATC, STC project(s), other).**
	Click here to enter text.
2	**Describe any prior experience with the legacy ARP4754 systems development document that your organization may have had.**
	Click here to enter text.
3	**Based on your current work environment, how does your management interpret the scope and purpose of ARP4754A?**
	Click here to enter text.
4	**If your company has (or had) a system development process equivalent to ARP4754A, please describe how the equivalency was determined, validated and accepted?**
	Click here to enter text.
5	**If the application of ARP4754A required and/or resulted in a change to an established business process, please provide examples of any significant process changes your company initiated.**
	Click here to enter text.
6	**Please describe any aspects of ARP4754A that your company determined were unnecessary or impractical to apply.**
	Click here to enter text.

7	**Please describe any benefits you discovered in applying ARP4754A.**
	Click here to enter text.
8	**What type of training, if any, did you receive to better understand ARP4754A?**
	Click here to enter text.
	What type of training, if any, did you develop to implement ARP4754A?
	Click here to enter text.
9	**In your opinion, how does the application of ARP4754A result in better products and systems?**
	Click here to enter text.
	In your opinion, how does the application of ARP4754A adversely impact products and systems?
	Click here to enter text.
10	***In what ways would/did the application of ARP4754A impact program cost and schedule?***
	Click here to enter text.

Application Experience - Certification

11	**Describe your experience of ARP4754A process negotiation with the certification authorities or OEM, i.e. what was considered necessary to show "compliance" to ARP4754A?**
	Click here to enter text.
12	**What key issues(s) was/were the subject of any certification authority or OEM negotiation?**
	Click here to enter text.
13	**What data/documentation do/did you submit to your certification authority or OEM to support ARP4754A?**
	Click here to enter text.
14	**How many Designated Engineering Representatives (DERs) or Authorized Representatives (ARs), who specialize in ARP4754A objectives, does your company have?**
	Click here to enter text.
15	**What, if any, concerns do you have with the current regulatory policies governing development and assurance?**
	Click here to enter text.
16	**What, if any, concerns do you have with the regulatory guidance for development and assurance?**
	Click here to enter text.
17	**If you are or have been involved in Part 23 certification programs – what has the ARP4754A application relationship been on your development program?**
	Click here to enter text.

Application Experience – Planning

18	**Please identify any area(s) of ARP4754A that you have had the most difficulty in applying (i.e. Planning, Requirements (management, validation, verification), Configuration Management, Process Assurance or Safety Assessment)?**
	Click here to enter text.
19	**Please describe any ARP4754A planning difficulties encountered.**
	Click here to enter text.

20	**Please describe issues, if any, that you may have experienced with the roles and responsibilities for the development identified in the program plans.**
	Click here to enter text.

Application Experience – Development Process

21	**Please describe how the airplane manufacturer was involved in the requirement management processes at the system and lower tier equipment supplier levels, as applicable.**
	Click here to enter text.
22	**Please describe any ARP4754A requirements capture/ management issues encountered.**
	Click here to enter text.
23	**Please describe your experience with the adequacy of system design tools in the ARP4754A development process.**
	Click here to enter text.
24	**Please describe any ARP4754A requirement validation issues encountered.**
	Click here to enter text.
25	**Please describe any ARP4754A requirement verification issues encountered.**
	Click here to enter text.
26	**Please describe any ARP4754A configuration management issues encountered.**
	Click here to enter text.
27	**Please describe any ARP4754A processes assurance issues encountered as it related to your development activities.**
	Click here to enter text.
28	**With regard to ARP4754A and engineering judgment, what, if any, difficulties did your company experience?**
	Click here to enter text.
29	**Please describe any boundary definition issues, between systems and items, that were encountered and how they were manifested.**
	Click here to enter text.

Applications Experience – Safety

30	**How was your company's safety focal involvement on the project(s) defined and managed?**
	Click here to enter text.
31	**Please elaborate on your experience of airplane manufacturer management of ARP4754A safety process activities, as applicable.**
	Click here to enter text.
32	**Please describe any safety process activity issues you or your organization experienced.**
	Click here to enter text.
33	**Describe the ARP4754A safety process activity issue(s) (e.g. FHA, PASA, PSSA, FTA, CCA).**
	Click here to enter text.
34	**Please describe any issues associated with definition or assignment of "safety related requirements".**
	Click here to enter text.
35	**Please describe the context of any architectural mitigation strategies successfully used in the assignment of Functional Development Assurance Levels (FDALs).**
	Click here to enter text.
36	**Please describe the context of any architectural mitigation strategies successfully used in the assignment of Item Development Assurance Levels (IDALs).**
	Click here to enter text.
37	**What, if any, tools have you used to assign FDALs?**
	Click here to enter text.
38	**What tools, if any, have you used to assign IDALs?**
	Click here to enter text.
39	**What FDAL assignment levels were assigned and satisfied?**
	Click here to enter text.
40	**Please describe any issues or difficulties in selecting between ARP4754A Option 1 or 2 in Table 3 for FDAL or IDAL assignments that were encountered.**
	Click here to enter text.
41	**Briefly describe any Table 3, Note 1 issues encountered during the assignment of FDAL or IDAL on the project.**
	Click here to enter text.
42	**Looking back, how did your understanding of Functional/Item DAL assignment process evolve throughout the project.**
	Click here to enter text.

ARP4754A Document and Authority Guidance Material

43	**What, if any, concerns do you have with the current ARP4754A industry guidelines for development and assurance?**
	Click here to enter text.
44	**What, if any, additional guideline material(s) would help to satisfy regulatory expectations?**
	Click here to enter text.

45	**How did SAE AIR6110, the industry application example for ARP4754A, aid your understanding of the development process described in ARP4754A?**
	Click here to enter text.
46	**What information or issues in AIR6110, contributed to confusion in satisfying ARP4754A objective expectations?**
	Click here to enter text.
47	***What, if any,* issues or concerns do you have with the current certification authority guidance material for application of development and assurance?**
	Click here to enter text.
48	***What, if any,* issues or concerns do you have with the current certification authority policies related to the application development and assurance?**
	Click here to enter text.
49	***What additional case study application examples would be helpful in understanding development process expectations? Why would these examples be helpful?***
	Click here to enter text.

Respondent Characteristics

Please describe the sector of the industry in which you work (e.g certification authority, airplane manufacturer, integrated system supplier, equipment supplier, etc.)
Click here to enter text.
Please describe which regulatory framework you normally address (e.g. Transport (Part 25), Normal, Utility (Part 23), Rotorcraft (Part 27-29), other, etc).
Click here to enter text.
Please discuss (in general terms) any current or future ARP4754A applications?
Click here to enter text.

B.2 1 Questionnaire Response Data

01 Describe the extent and circumstances of your ARP4754A application (e.g. TC, ATC, STC).

R1 STC- Avionic modernization program

R2 As regulators, we generally encourage companies to apply ARP4754A.

R3 Skip

R4 Landing Gear System Development-ATA Chapter 32 e.g. MLG/NLG Structure, Steering System, Ext&Ret System, Position Indication and Warning System, Brake Control System.

R5 TC project

R6 I have read 4754A and compared it to 4754.

R7 Development of FCS and LGS and related Equipment. Compliance to ARP4754(A) part of work process as per company standard and work flow process required by TC holder. Application of ARP4754A or equivalent/derived integral processes from project start (Aircraft Manufacturer input requirements) throughout Systems and Equipment requirements definition, validation and verification to final steps of certification by TC-holder. Problem reporting, configuration management and safety considerations tied to the process.

R8 We apply ARP in our avionic and weapon systems development activities which are generally supplied to Military Aircrafts (fighters, trainers, rotorcrafts, UAVs). Application of ARP4754 or ARP4754A is being specified as requirement in our contracts by the aircraft manufacturer or main contractor responsible from aircraft. Although these are the military system development projects, civil certification requirements are in place to adhere. The authority is not a civil authority like FAA or EASA but a military certification authority established by the acquisition.

R9 Two TC projects under development.

R10 TC

R11 My company is the airborne equipment supplier, we use ARP4754A mainly for TSO.

02 Describe any prior experience with the legacy ARP4754 systems development document that your organization may have had.

R1 Skip

R2 As regulators, we had only seen applicants use the legacy document in the areas of DAL (more specifically IDAL in current 4754A) assignments.

R3 The development process was mostly following the ARP 4754 as it is a clear proceeding; however it was not reflected in whole detail in the internal development process

R4 ARP4754, was applied in our organization for the development of control units for landing gear systems, flight control systems and environmental control system as the level above RTCA DO254 and 178B

R5 Small gas turbine FADEC development project for helicopters, and turbine engine development for civil aircraft

R6 The PROGRAM NAME was developed under 4754. This covers a product line for the PROGRAM NAME and the development of four different applications.

R7 Airplane 1 LGS, Airplane 2 & 3 LGS, Airplane 4 & 5 LGS, Airplane 1 FCS

R8 Application of ARP 4754 was a contractual requirement in many of our current and previous development programs.

R9 Three TC projects and type design changes (post-TC) in one of them.

R10 Don't know

R11 We do not have formal prior experience with ARP4754, but we have followed the idea of the ARP4754 in some project.

03 Based on your current work environment, how does your management interpret the scope and purpose of ARP4754A?

R1 I think benefit of using this standard is not well understood by management. We need to measure some metrics during application process.

R2 As regulators, we generally view 4754A as state-of-the-art guidelines

R3 Skip

R4 Initially after the release of the DRAFT ARP4754A and the request, by our customers, apply the ARP for new development programs, it created confusion, as interpretation of the ARP content was varying inside the organization heavily. It was not clear how the existing development processes have to be tuned in order to show compliance. The management accepted the ARP as a burden in the beginning, which changed with the first projects ARP4754A has been applied to the common consensus that the application of the ARP adds maturity to all development phase. (brings our products closer to first time right).

R5 Comply with Rev A for new design. Airframer got Issue Paper to follow rev A.

R6 Concerned that any extra work to become 4754A compliant was not in the original budget and is not easily

R7 Necessary and acceptable mean to ensure development process of complex systems and product quality. Reference and link to cost for extensive application of integral process not defined and measurable yet despite development planning and transition criteria guidelines.

R8 Management knows the importance of application of ARPs since they are stated in the contracts in military projects. Also the aim is to get TSO in the near future for our products meeting civil certification requirements so they know ARPs are part of this process.

R9 A kind of certification requirement and, to some extent, and under certain conditions, good practices for product quality and maturity assurance. Recently, due to a certain inflation in number of requirements being captured either due to situation described in q. 22 below or because those recommended practices being carried for non-direct engineering requirements at product high level specification (like maintenance, operational and customer support requirements – see also q.5), there is also the perception that it represents a burden activity.

R10 It's understood within management that the application of ARP4754A is needed in any system development

R11 The CAAC authority may take the ARP4754A as the certification requirement for the system product, though there is no formal AC for it. My company management use ARP4754A as guidance to improve the development process rather than only for certification.

04 If your company has (or had) a system development process equivalent to ARP4754A, please describe how the equivalency was determined, validated and accepted?

R1 Military applicants have used system engineering processes defined in ISO/IEC standards. They also started to organize their processes according to 4754A. Especially safety related processes that are not well defined in system engineering standards.

R2 Skip

R3 Skip

R4 The development process in our company was reworked in 2010 with respect to the AIRPLANE PROGRAM NAME development guidelines. So with the release of ARP4754A, an assessment was done in order to identify if there are discrepancies existing to be corrected, adjusted. Further on we stepped into new development programs where our customers had different approaches to show compliance to the ARP4754A. One customer required for example a line to line compliance matrix to the ARP4754A. The comparison ARP4754A versus our development process was made and adjustments applied to the process where necessary. One beneficial task prior to the assessment was the ARP4754A training at our company done by Eric Peterson to reach a common understanding of the ARP.

R5 Closest that comes to mind was PROGRAM NAME. No equivalency established

R6 As far as I know there isn't one.

R7 Skip

R8 We are trying to update our system development process to make it fully compliant with ARP 4754A. In order to determine the gaps between ARP process and our existing processes we conducted gap analyses performed by an independent consultant.

R9 Company has adapted its engineering processes across projects. For the projects under development this question is not applicable (all systems/functions are covered by ARP4754A based processes). The last project' TC adopted ARP4754 (legacy version) based processes, with some features from version A; and for the first two projects' TC, there were a scope analysis based on complexity, level of integration and criticality of systems/functions to identify which ones would be covered by each process (company equivalent and ARP4754 based).

R10 Don't know

R11 We have established a development process followed ARP4754A at the LRU level, we have internal review and approval procedure to check against the ARP4754, but there is no way to determine the equivalency by the third party at the moment in Chinese case.

05 If the application of ARP4754A required and/or resulted in a change to an established business process, please provide examples of any significant process changes your company initiated.

R1 Especially requirement validation and safety assessment processes needed to be updated.

R2 From the regulatory perspective, the “business change” is our recognition that 4754A has a role in the certification process, via our ACs and other vehicles.

R3 It was not really a fundamental change rather than a determination of the process in more detail

R4 The application of the ARP4754A resulted in a change of the Requirements Based Engineering process, with correction of the validation and verification process steps and content. The result was the implementation of a generic Validation and Verification Plan for the company.

R5 NA

R6 NA

R7 1) Introduction and application of requirements engineering

2) Establishment and application of System Development Plan, Requirements Validation Plan, Requirements Verification Plan, Process Assurance Plan, Configuration Management.

R8 Requirement validation process had to be improved considering ARP. Safety requirements generation and flow down to SW/AEH had to be improved. In general system requirements management process and requirement decomposition structure had to be improved.

R9 No change at business level was identified in the projects so far (considering the application of ARP4754A in the strict sense of technical scope of the projects and in the level of airframe and systems development). There are, however, two points to highlight: The first: those recommended practices were somewhat spread out to higher-level product definitions, outside the usual product definition engineering areas (like maintenance, operational and customer support areas), which have more impacts and visibility in business process (through data like direct operation cost, direct maintenance cost, etc.) – this point contributes, to some extent, with the perception described in q.3. Second point: there is the possibility to move toward on introducing more detailed criteria, metrics and indicators based on requirements management practices in the project development framework, refining the decision and risk assessment processes around project phases and gates.

R10 The verification and validation processes between requirements owners and implementers have been reviewed completely under the guidance or ARP4754A.

R11 My company established business process is the general requirements for airborne product development, the rigor is the average level which means it is more rigor than DAL D but is less rigor than DAL B. So the DAL allocation process and control in different rigor impact the process significantly.

06 Please describe any aspects of ARP4754A that your company determined were unnecessary or impractical to apply.

R1 DAL allocation Table 3. Using option 1 and 2 is not as easy in real environment as it is described in 4754A in terms of showing compliance to independence requirements.

R2 Skip

R3 FDAL-determination: it is not fully clear, down to what level this should be performed
Validation: It was understood, that for requirements with FDAL A or B two means of verification should be applied. This is in some cases not feasible or impossible

R4 FDAL and IDAL Assignment Process created discussion and inconsistency within our development process. As our customers do not identify FDAL's in their specifications In consequence we used the SFHA as done in legacy projects. The further item difficult to handle was the issue how to determine complex versus noncomplex equipment mainly for structural or hydro-mechanical equipment. For electronic HW and SW it was clear. This was a discussion with our customers, as well the authorities as it was not clear from ARP how to handle non electronic equipment. During audits with customers and authorities it was not clear at all how to deal with para 5.5.5.4 b. "unintended functions " of ARP4754A.

R5 NA

R6 NA

R7 1) Ambiguous explanation (e.g. Table 6 Requirements Validation Methods and Data) often leads to mismatching interpretation and expectation with Regulatory Authorities and TC-holder. This concerns both the process to be in put in place and the acceptable level and extent of data/results to be provided.

2) The concept of eliminating "unintended function" during verification and/or integration activities gained wider popularity and some acceptance with ARP4754A. It is however too summarily defined to provide assistance or guideline: some interpretation might be unintended function = "everything that is not required from the system", thus any attempt to define a process gets out of hand.

3) Formal allocation FDAL A/B/C sufficient to address failure criticalities affecting development process. Focus is usually put on FDAL A/B investigation and assurance.

R8 Section 6

R9 Although some aspects have been controversial issues, both internally and externally in discussions with cert. authorities and suppliers, we could not find, to the extent of application we've exercised so far, anyone that we could firmly say it's unnecessary or impractical.

R10 Don't know.

R11 Because we are the LRU supplier, so most of the safety assessment process except FMEA is unnecessary to us. Typically we follow the requirement from the customer, including DAL and safety requirement.

07 Please describe any benefits you discovered in applying ARP4754A.

R1 It provides companies a structure way to develop their processes. Giving a systematic path to follow in design and development.

R2 From the regulatory perspective, the benefits are better understanding of applicants' development process which in turn helps us provide better guidance to applicants toward showing compliance

R3 Clear relationship between safety, requirements capture process and (system) design

R4 Guideline for development process development and predecessor to RTCA DO 178 and 254

R5 More rigorous requirements traceability

R6 NA

R7 1) Possibility and opportunity to apply a single development process for complete System 2) Compatibility with other standards or guidelines already established in the Company, such as DO254x,DO178x, ARP47613) Compatibility with Company Business Process, though adjustment might be necessary 4) Wider acceptance among development and verification engineering.

R8 ARP is a key tool when applied logically and in an organized manner because it is a detailed guideline which provides a bridge between the civil certification requirements and SW development (DO 178)/AEH development (DO-254). Since all our existing programs requires SW developed according to DO 178 and in recent programs DO 254 is also required, the appliance of system level development processes according to ARP is very crucial. ARP gives a detailed guideline starting from deriving system functions to implementation. While doing this, the focus is system level development (for our usage) and system safety assessment but the relations with other levels like aircraft level, item level, SW level, HW level are very well established. The flow of information between these layers and the borders of each layer has been drawn to clarify top-down approach that has been adapted. Hence it is good to know when adapting company processes to ARP, which pieces of information is related with systems engineering or SW engineering or HW engineering and what should we expect from aircraft level.

R9 The ones that highlight are: # is to set up a framework to perform a requirements-oriented development, which provides means to correlates program/development phases/events with key processes activities that allow us to set up and to measure product quality and maturity expectations.

R10 Structured and controlled V&V activities throughout the development process

R11 The work is well ordered and well controlled. Though we have taken more time for the design, less iterations are required for the verification process, etc.

08a What type of training, if any, did you receive to better understand ARP4754A?

R1 Skip

R2 As a member of the S18 committee, I have no need for this training. However, we continually find ways to train our engineers in the agency.

R3 Skip

R4 We got training by E. Peterson, two days for general walk through and another two days for dedicated question session.

R5 Presentations on introduction of Rev A. Organized workshops

R6 None

R7 Skip

R8 We received a 2-day training for ARP 4761 and 4754A, a couple of years ago. Also we conducted a gap analysis to reveal what has to be done in order to make our processes compliant with ARP4754A and ARP 4761.

R9 The great majority of people had no formal training; we have got understanding across projects from interacting with cert. authorities and suppliers, taking part in S-18 meetings and “on the job training” during the projects, exchanging internally experiences and lessons learned.

R10 Three days course on ARP4754A.

R11 We did not have formal training to understand ARP4754A. We do this by group discussion within the company.

08b What type of training, if any, did you develop to implement ARP4754A?

R1 We develop trainings related to 4754A and 4761 for our engineers (military authority certification specialists).

R2 We have internally developed a training course and a webinar.

R3 Skip

R4 Based upon the training and company development process adaptation to ARP4754A we developed a one day training session for company employees in order to make them aware of ARP4754A and respectively the company development process which is in line with ARP4754A. We also established training sessions for the company guidelines Requirements Engineering Policy and Requirements Engineering Process.

R5 NA

R6 None

R7 Skip

R8 We implemented internal System Safety and Development training covering ARP 4761 and ARP4754A processes.

R9 We developed a corporate introductory, overview, training (for version A and relevant changes from legacy) and project specific trainings focusing on operational aspects of each process implementation (functions list / requirements capture, validation & verification and related aspects of configuration management).

R10 None

R11 We did not have formal training to implement ARP4754A. We do this by group discussion and dry run the sample project within the company.

09a In your opinion, how does the application of ARP4754A result in better products and systems?

R1 4754A gives us a good understanding of what to do. I think companies should develop their own procedures according to their scope of work and criticality of the systems. Finding the best way that fits to company is important to get the benefit of applying 4754A.

R2 From the regulatory perspective, the learning curve for industry and ACO is still fairly steep at the present time. But for those who have gone through it once, the benefit is better/smoother certification in the next program.

R3 The clear relationship between safety, requirements capture process and (system) design will help to avoid errors and late detection of non-compliance to safety requirements

R4 Identification of gaps in the forward path of the development with validation “are we building the right thing” and with verification “did we build the right thing”.

R5 Better requirements definition and management

R6 Higher levels of configuration management and control practices. Also, the alignment with DO-178B/C makes it easier to work with the software group.

R7 1) Methods to ensure correctness, completeness and traceability provide more confidence at every single step of development process and problem management, more visibility is given for documentation during development and for/post-certification.

2) ARP4754A is not depending on the software tool adapted for its application.

R8 I think before ARP, it is not clear how to relate our system safety engineering and other system development activities with the SW and AEH level. ARP provides a means of filling the gap between civil certification requirements and implementation in SW and AEH through the use of DAL assignment process, requirement validation and verification process. Since DO-178 or DO-254 for SW and AEH are not sufficient to produce a safe product without a systematic approach followed in system level, ARP serves as a “systems aspect of certification” standard to follow for developing better airborne products and systems.

R9 Anticipating issues as early as possible in the development and Entry Into Service (EIS), helping risk identification / mitigation and providing a systematic mean (requirements-oriented development) to analyze, assessing and solving issues from the deployment of business / high level requirements into implementation, during the development, framework for communication with suppliers (e.g. requirements and interface control data), EIS and operation. Additionally, it helps in the product change impact analysis; without the traceability framework its application provides, impact analysis requires much time (having to analyze the entire database and test data) and that is subject to much more errors.

R10 All the engineers participating in the system development have a better idea of the whole process. The life cycle of requirements from initial state to implementation and testing is better controlled, reducing the risk of missing steps during the development that would result in costly redesigns at a later stage in the program.

R11 Less remained errors, better controlled data for modification and duplication, it is also good for reuse.

09b In your opinion, how does the application of ARP4754A adversely impact products and systems?

R1 Documentation effort as output of 4754A may lead some delay in project. Common understanding is important. I don't think both authority and applicant personnel are in same understanding level.

R2 From the regulatory perspective, there should not be adverse impact to the safety of products and systems.

R3 Skip

R4 I see no adverse impact on products and systems

R5 Increase cost via Engineering hours

R6 No – it contains good engineering practices.

R7 Extensive application of ARP4754A as per the document for whole System and its Equipment often impacts cost and schedule.

R8 None

R9 One possible adverse impact is the pitfall of believing that setting down the processes, with checklists, activities workflow, etc., one could execute that without an engineering judgment and technical background with regarding the content being evaluated. For instance, a requirement captured by a beginner engineer, validated by another beginner engineer may not be of good quality, even though we have a checklist approved in a plan, fulfilled with independence and assured by another person that has no good knowledge on that technology area. The risk here is to believe that the processes can replace people knowledge about the artifacts being worked out under those process.

R10 Cost and effort is increased, mainly in the initial stages of the development process. Generally the initial investment pays off during the whole program. However, in some cases it is difficult to see the benefit.

R11 The cost.

10 In what ways would/did the application of ARP4754A impact program cost and schedule?

R1 We couldn't apply all sections 100% in our military project. No metrics were measured. Therefore no objective evidence about the impact on cost and schedule.

R2 From the regulatory perspective, cost and schedule impacts should be neutral for the first application (i.e. pays for itself due to mitigation of late surprises) and then improved for the next project.

R3 Additional effort in development, requirements capture process and verification. Application in development process in some cases not clear - see also response to question 6.

R4 In the beginning for the first time application of the ARP4754A it was an increase of the cost of about 25% and a schedule impact of about 3-4 month, clearly owed the fact that the ARP4754A process common understanding was not given with a set of repetitions required. With the improved practice and mature and trained process, the impact is reduced to 10% cost and 4 weeks schedule. But consider that the maturity of the final system/product is heavily improved.

R5 Higher cost, longer development plan

R6 A small potential for addition hours to support the higher levels of CM

R7 1) Reviews might need to involve more resources, effort or loops before being deemed completed. However, this is usually the case for FDAL A/B and safety related items.

2) Validation process is generally understood to need time, which is acceptable with regards to the final target. Often times, this process is being complicated when organizations/stakeholders to be involved are further apart (e.g. Customer/Supplier in different countries). Release of documents might take longer, or rework is necessary if validation is not directly performed with all stakeholders.

R8 There is no sufficient data for this evaluation in our hand since our experience is relatively low, newly developing. But I think the application of ARP should not adversely affect the cost and schedule when applied correctly because the real cost comes from SW development (appliance of DO 178) and AEH development (appliance of DO 254). On the other hand, appliance of ARP should serve for cutting cost and schedule in the appliance of these processes by timely identifying safety objectives, safety requirements and development assurance levels which are used as the main inputs and in fact are the main drivers for cost and schedule factors.

R9 Increase schedule and cost in early phases of projects (due to greater effort concentrated in requirements capture, discussion and validation, when compared to non-ARP4754 based processes) and across all phases due to formalization of several data, process assurance activities and support for Cert. Authorities on-site reviews.

R10 Don't know.

R11 In my opinion, to apply ARP4754A, we need qualified engineers to support the engineering activities, so cost more for the human resource. As for the schedule, it may take more time for design, but it may save time for the verification.

11 Describe your experience of ARP4754A process negotiation with the certification authorities or OEM, i.e. what was considered necessary to show "compliance" to ARP4754A?

R1 As military authority side we more focused on planning (especially certification plan and safety program plan), safety assessment and verification processes outputs.

R2 From the regulatory perspective, if an applicant is applying the ARP for the 1st time, regulators expect the company to have the infrastructure (and management support) to be able to perform the entire set of the "integral process". Depending on the scope of the project, I have advised our ACOs to focus oversight on certain aspects of the integral process. In all cases, the requirement validation aspect is at the forefront.

R3 Skip

R4 The negotiation with authorities was in a way that it was presented to the customer and authorities how the company's interpretation and implementation is. Audits, by the authorities and customer during the developments process, reviewed whether the presented ARP4754A process was applied as per initial presentation.

R5 NA

R6 NA

R7 1) General agreement on application and aim of ARP4754A

2) Key divergence is related to the extent and depth of the process application itself and also the acceptable evidence to be provided.

3) Negotiations are often affected by different or non-consistent interpretations among representatives of same organizations or roles (e.g. among Suppliers, or among Regulatory Authorities). Very personal interpretation of ARP4754A, in this case, is rather a barrier to come to an agreement than an added value.

R8 The implementation of safety requirements (FDALs, IDALs) are required to be in compliant with ARP4754A.

R9 In general, submittal of Certification and Development Plans, and Certification Summary / Compliance Report, along with on-site audits performed by CAs, usually regulated by agreement in an specific issue paper and / or Certification Action Item, usually covering us as OEM (system level) and our suppliers (sub-systems / equipment

R10 It has been well valued by the certification authorities the compliance to ARP4754A. No important points of discussion have taken place with the authorities so far.

R11 Certification support Plan, Safety Assessment data, identification and change control process and data, Requirements documents, Design documents and verification documents.

12 What key issues(s) was/were the subject of any certification authority or OEM negotiation?

R1 It was a modification project so as authority side we tried to follow section 6 of 4764A but some issues raised to agree on impact analyses and output documentation. I think section 6 should provide more information to manage the modification of an aircraft. Also modifications are mostly performed by companies rather than TC holder and those companies usually don't have enough information about aircraft to assess the modification impact (for example no original safety assessments).

R2 Looking from the regulatory perspective, the main concern I have is the "ARP4754A process specialists" at the companies are too busy designing the processes, they are removed from the development itself (which often runs concurrently) and consequently there can be disconnects between what they think is done vs what is actually done. Thus the full spectrum of benefits of applying the ARP is not realized until the next program (cost/schedule/quality of product/smoother cert).

R3 Skip

R4 Compliance to ARP was one of the mandatory subjects.

R5 NA

R6 NA

R7 1) Amount of validation/verification methods to be applied;

2) Involvement of Safety Engineer in reviews, problem and change assessment.

R8 Item DAL levels.

R9 Their level of involvement and the rigor in the compliance demonstration, considering the systems that is introducing any new technology or whose architecture is highly integrated and complex, or, yet, if the supplier has few previous experience either in the development of the sub-system or equipment being supplied or in the ARP4754 compliance demonstration for it.

R10 Don't know.

R11 DAL allocation.

13 What data/documentation do/did you submit to your certification authority or OEM to support ARP4754A?

R1 As military authority side we incorporated all documents that we required in the contract. We also referenced 4754A in the contract but Contract Data Requirement List took priority.
R2 Skip
R3 As system supplier we submit validation and verification plans, system development plan, safety and reliability plan to the aircraft manufacturer
R4 Compliance Matrix, System Development Plan, Process Assurance Plan, Validation and Verifcation Plan
R5 SSA
R6 NA
R7 System Development Plan, Requirements Validation Plan, Requirements Verification Plan, Process Assurance Plan, Configuration Management, System Requirements Document, System Validation Summary Report including matrix, System Verification Summary Report including matrix
R8 System Safety Program Plan, Certification Plan, FHA, PSSA, SSA.
R9 See 11.
R10 System Description Documents, Test Procedures, Test Results
R11 Certification support Plan, FHA/PSSA/SSA data, Verification plan, summary report.

14 How many Designated Engineering Representatives (DERs) or Authorized Representatives (ARs), who specialize in ARP4754A objectives, does your company have?

R1 We have trained our specialist to understand the objectives of 4754 but it takes time to specialize in this guideline.
R2 Skip
R3 Skip
R4 None
R5 Don't know.
R6 NA
R7 Skip
R8 None
R9 Eleven (11) registered in Certification Authority records and, so far, four (4) had effectively acted in reviewing ARP4754() data for compliance.
R10 Two
R11 There are 2 DERs (system and equipment) in my company, in CAAC policy there is no specialized DER for ARP4754A objective, neither for SW or E HW.

15 What, if any, concerns do you have with the current regulatory policies governing development and assurance?

R1 Skip
R2 Skip
R3 Skip
R4 None
R5 Need more experience on Assurance
R6 NA
R7 Regulatory policies or boundaries, especially data to be provided for certification submission, need to be defined latest by PDR. Any communication or new insights and perceptions beyond this milestone impacts product design,
R8 None
R9 Not clear what question means by “policies”… Considering, for instance, the FAA AC 20-174 / ARP4754(), there is no concern so far, because, it seems to us, they are somewhat “new” (considering an airplane development cycle) and were not exercised sufficiently so far (like the ones regarding integrated modular architectures, the FA AC 20-170 and DO-297, for instance). However, based on similar question in other technologies (software and AEH, for instance), the concerns are not directly related to the policies themselves, but to some lack of alignment of agencies personal (both internally to each agency, and between agencies) about the understanding of their application and how to follow them: depending on the person the applicant faces in the room, or the one that reviews the data the applicant sent out, what has being done can be acceptable or not.
R10 None
R11 Skip

16 What, if any, concerns do you have with the regulatory guidance for development and assurance?

R1 Skip

R2 Skip

R3 Skip

R4 There is one issue, recognized that the ARP4754A, which is similar to the experience made within our organization that different organizations (authorities) and also personal in these organizations show different interpretations of how things of the ARP shall be applied to the development process. (e.g. recommendation equals requirement).

R5 Guidance need to be part of training.

R6 NA

R7 Different references are generally mentioned for development and assurance guidance: Regulatory's, OEM's and Supplier's business process. All of those might be based on ARP4754A or were considered when creating it. But since regulatory authorities' guidance is determining, more effort for communication and at times discussion with SAE ARP4754A working group and the general industry is required on regular basis.

R8 None

R9 See 15 – for us, the distinction between a regulatory "policy" and "guidance" is not clear.

R10 None

R11 Skip

17 If you are or have been involved in Part 23 certification programs – what has the ARP4754A application relationship been on your development program?

R1 We involved in CS 23 Cat III aircraft development process with EASA. But in this project EASA didn't require the application of 4754A.

R2 Skip

R3 Skip

R4 Since ARP4754A was released we have not be working on a Part 23 projects, but on Part 29 programs. We as a company decided to follow the ARP4754A respectively ours company development process guidelines for Part 23/25/27/29 applications.

R5 NA

R6 NA

R7 None yet.

R8 We have ARP4754A requirement in our Part 23 aircraft system development programs. The activities are the same but it is difficult to classify failure conditions and substantiate them since most AC and TSO material include classifications made considering Part 25 airplanes.

R9 Involvement occurred only with legacy version (ARP4754), through a Certification Action Item for the Type

R10 In my personal experience, the application of ARP4754A has been similar in Part 23 and Part 25 programs I've

R11 Skip

18 Please identify any area(s) of ARP4754A that you have had the most difficulty in applying (i.e. Planning, Requirements (management, validation, verification), Configuration Management, Process Assurance or Safety Assessment)?

R1 Each process has its own methodology and tool to apply. I think the biggest problem we had is communication and timely information flow between and within the processes.

R2 Skip

R3 FDAL-determination: it is not fully clear, down to what level this should be performed
Validation: It was understood, that for requirements with FDAL A or B two means of verification should be applied. This is in some cases not feasible or impossible

R4 Safety Assessment (FDAL assignment); Verification process philosophy

R5 Config Management

R6 NA

R7 1) Challenging if not problematic involvement of Verification entities, i.e. Verification Engineers, during the development process starting during first validation reviews. The difficulties encountered partly reside in their theoretically "passive" role during development, in order for the independence policy to be ensured.

2) Minor mismatch between currently valid items baseline (e.g. document or design build standard) and the items actually being investigated or used for further activities.

R8 Requirement validation was the most difficult area since engineers are used to define and perform verification work rather than validation of the requirements they are developing. Hence it was difficult to manage and complete validation work.

R9 Planning, Verification and Process Assurance. Regarding safety assessment, the scope of the ARP4754A and the relationship with the certification process (final full review versus early involvement accepting the process).

R10 Process Assurance and Safety Assessment integration with system requirements.

R11 I think the Process Assurance is the most difficult part, we know the basic idea, but we do not know how to guide the QA to do the work effectively. The same for other activities, though we know what we expected to do, we are lack of experience on how to write good engineering documents, etc.

19 Please describe any ARP4754A planning difficulties encountered.

R1 Safety assessments should be started very early stage of the project. Because system criticality effects some planning activities. Without knowing system criticality we couldn't plan some activities in detail.

R2 Skip

R3 Skip

R4 None, after the generic validation and verification plans have been established in the development process

R5 When to introduce Config Management

R6 NA

R7 1) "Old school" verification, just like design, certainly still relies on experience and sees requirements engineering as subordinated.

2) Beyond configuration management own issues, keep track of all currently valid items' baselines in a way to coordinate complex actions and interactions is nearly impossible. E.g.: By the time of its delivery, the qualification procedures for the release of equipment might not be complete in its entireness. Written Evidence or Design Justification supporting applicability and minor/none effect of remaining portion to be qualified must be produced.

R8 It is difficult to plan the completion of requirement validation work.

R9 The most relevant difficulties were related to:

a) timely definition and application of clear transition criteria and guidelines related to deviations from the plans (section 3.2);

b) to set up process related to architecture / design definition and requirements allocation (sections 4.1.6/7, 4.4 and 5.8.4.4). Additionally, about this last, in despite of figure 6 suggests the existence of sub-systems, related sections suggest that systems are, at the same time, the entity to which aircraft level functions are allocated and from which software and hardware items are deployed (section 4.6). This situation does not match with real environment and introduce difficulties in planning requirements organization and integral processes.

R10 None

R11 The plans for all the projects seem similar, but it does not have too much help to the project. We do not know how to write a good plan to guide the specific project working effectively.

20 Please describe issues, if any, that you may have experienced with the roles and responsibilities for the development identified in the program plans.

R1 As military authority side we had some problem related to owning of 4754 processes by our system certification specialist. They mostly focus on their certification requirements. We realized that we need to provide more trainings related to 4754A in order to make them understand they have to manage whole processes related to their systems.

R2 Skip

R3 Skip

R4 None

R5 NA

R6 NA

R7 1) For a requirement with identical validation method and verification method, for instance Stress Analysis, independency is not guaranteed since often the same Stress Analysis report would be used as a reference. Assessment whether the analysis results are sufficient to cover both purposes would need to be done by another engineer.

2) Involving Senior Engineers' (Chief, Airworthiness, Specialists, …) in reviews and decision pertaining FDAL A/B/C should certainly be a general aim, though application due to restricted number of Senior Engineer is not always possible.

R8 The responsibilities for the documentation and verification of safety requirements. The means for communicating derived requirements between the item level and system level.

R9 The most relevant issue was related to responsibilities of process definition (internal agreements and planning), communication (training) and Process Assurance execution being performed by the same team.

R10 None

R11 CCB, different people think differently about CCB. Some think it as a fixed organization, some think it as a meeting for the change.

21 Please describe how the airplane manufacturer was involved in the requirement management processes at the system and lower tier equipment supplier levels, as applicable.

R1 Skip

R2 As an observation, airplane manufacturers currently have limited practical influence at lower tiers supplier levels, although most have processes to manage system-level requirements.

R3 Skip

R4 The airplane manufacturer was involved in the system requirements by discussion and agreement to the compliance matrix to the customer specification as well as the participation in the system validation audits.

R5 Airframer review engine safety requirement, offer workshop

R6 The normal interaction with the airframer is through the publication of the ICD. This process is the same under both versions of the ARP so there is no difference seen in this area.

R7 1) System Requirements Document is a child of the airplane manufacturer's requirements documents. Traceability to the document

2) Validation activities with airplane manufacturer to ensure completeness and coverage are part of standard process.

3) System Validation/Verification Summary Reports including matrices containing agreed information are part of deliverables.

4) Airplane manufacturer representatives witness verification activities on request.

R8 In some projects airplane manufacturer or main contractor gives us not only FDALs but also IDALs for system items that we are developing without validation evidence. This complicates the safety assessment process, requirement development and management.

R9 In our experience as airplane manufacturer, suppliers are involved in two moments, with two approaches. In the first moment, in the preliminary studies of a new project, before its formally launched, through interviews and procurement preliminary discussions (requests for information / proposal). Next, we set up a supplier oversight plan, based on a risk assessment and level of involvement processes. Those processes end up with activities similar to the ones defined for "Stage Of Involvement" reviews performed for software when finding compliance to DO-178() ("SOIs"), which the highest rigor is to have on-site development and verification reviews after the planning review performed for all cases. In general, we've observed the suppliers of are not familiar with fulfilling ARP4754() objectives, usually because either their primary regulatory compliance does not require include ARP4754A as a means of compliance or that compliance is requested to be demonstrate by the airplane manufacturer only.

R10 Aircraft level requirements and supplier requirements are traces and controlled by the airplane manufacturer.

R11 Skip

22 Please describe any ARP4754A requirements capture/ management issues encountered.

R1 4754 tells us what kind of requirement can be captured and what methods can be used to validate them. But I think this phase mostly depend on the knowledge of each party (customer, manufacturer, etc) at the time of requirement review. We had to face incomplete and ambiguous requirements required by customers.

R2 Skip

R3 Skip

R4 Not configured customer documentation e.g. specification plus a set of Change Requests, not formally validated on parent level. Missing requirements links, missing equipment allocation, incorrect means of validation/verification, duplication of verification tasks e.g. at equipment and system level the verification of the same functionality.

R5 Nacelle, TRU requirements capture and flowdown by engine manufacturer

R6 NA

R7 1) Linguistic difficulties and conflicts aside, requirements capture is rarely satisfying to an organization or an engineer during the course of the development. Different insights and realizings will always come down the way, sometimes leading most drastic action such as complete rework. This might be related to the general approach, the layout of information capture, the acceptability of a wording across diverse disciplines.

2) Tool available for requirements capture/management not always satisfying every requirement and process within one organization or outside the organization. Misuse or mishandling of the tool and the ARP4754A process to comply with one aspect, e.g. document layout containing information deemed necessary to assess certifiability need to be produced although multiple relations on a single level are not to be managed.

R8 It was difficult to capture and manage system requirements in a consistent manner without a requirement standard employed like in DO178 and DO254 but ARP doesn't call out for such type of standardization. Hence different type of requirements, in different granularities and different composition makes harder to evaluate them.

R9 The most relevant issue is related to engineers capturing as "requirements" information that may not represent indeed a "requirement" (like a design standard or assumptions) and having difficulties in validating it. This situation sometimes leaded to a requirements database bigger than the product actually needs.

R10 Suppliers don't all work following the same processes and requirements capture and management worked well with some and not so well with others.

R11 We have DOORS for requirement management, but it is not clear for us how to connected the requirement management with the development process.

23 Please describe your experience with the adequacy of system design tools in the ARP4754A development process.

R1 Skip

R2 Skip

R3 Skip

R4 DOORS is used as a standard for the validation and verification process. What is required is unambiguous defined process and therefore the verification and validation plan must be in place.

R5 NA

R6 NA

R7 As per Q22, available tools (e.g. Team Center, IBM DOORS) correspond closely to the expectation and application of ARP4754A development process. Inadequacy or possibly misuse results from expectations beyond process application, implementation and reasonable management effort.

R8 None

R9 Not sure what the question means by “system design tools”. Assuming the restrict sense of “design” provided in sections 4.1.6 and 4.4, and Simulink as one example of such tools, they have been widely used in supporting requirements validation through the usage of modeling and simulation cases as part of validation evidences.

R10 DOORS is the tool typically used. In some ways this tool is deficient and can be improved significantly.

R11 DOORS, Synergy, PDM, integrated development tools, verification tools.

24 Please describe any ARP4754A requirement validation issues encountered.

R1 The issue was that companies didn't set a systematic correctness and completeness check process. Also only review process as a validation method was preferred by companies. Test and analysis methods were found as a

R2 Skip

R3 Implementation during development process needed to be established, e. g. with respect to determination of disciplines to participate and resources planning

R4 Organization of the validation process, having the required people available for the validation process. Re-visit of already validated requirements with different results. Non availability of Verification engineering for validation, causing additional effort during verification back in the validation process. In complete requirements baseline from parent documentation means spread of requirements over a set of documents. We made the decision in the company to apply validation process as well for complex and non complex systems and equipment's, as we recognized by doing so having a robust development process and less discussions with customers/authorities.

R5 Not covered yet

R6 NA

R7 1) Rationale of requirement often understood as self-explaining or "based on experience" is also often hard to formulate.

2) Different linguistic backgrounds within one project, whether within one organization or outside, sometimes build a barrier for clear formulation and precise wording choice. Even the most skilled specialist might encounter this problem if not expressing himself in his native language or language of education.

R8 The responsibility of requirement validation work is not clearly described in ARP.

R9 Additionally to comment provided in question 22 above, recently we realized that sections 5.4.3 and 5.4.4 (Correctness and Completeness Checks) seem to provide much more details than the current practices actually demands to address. Additionally, one of the most controversial issue is regarding the prevention of unintended function through validation methods and activities – usually, for textual requirements, this issue is explicitly addressed in the verification process only.

R10 Requirement owners don't always understand the need to validate their requirements during the process. It is important to involve everyone in the process.

R11 One of the objective of the requirement validation is its integrity, but it is difficult to prove it.

25 Please describe any ARP4754A requirement verification issues encountered.

R1 Verification process was more structure than validation process. Because seeing the results/outputs were the concern of each party therefore more attention was paid for this process. But documenting of what was done as guided by 4754A was an issue.

R2 Skip

R3 Implementation during development process needed to be established, e. g. with respect to determination of disciplines to participate and resources planning Verification rigor sometimes unclear.

R4 Traceability and coverage becomes a high effort, if the verification engineering was not deeply involved within the validation process, causing inconsistencies in the verification either verification of requirements was not done or duplicated at different levels.

R5 Not covered yet

R6 NA

R7 1) First issue roots back to requirement capture and validation process: misinterpretation might raise on what needs to be verified, or possibly how it should be verified.

2) For Verification Method “similarity”, it is unclear how much of the “similar” equipment or system need to be shown. The main issue is due to disclosure obligation with a third party airplane manufacturer.

3) Combination of numbers of Verification Method to be applied (e.g. 2), FDAL classification (e.g. A) and mandatory method (e.g. test) as per System Verification Plan might not be feasible. Negotiation with Regulatory Authorities and Airplane Manufacturer is not avoidable.

R8 We are confused with the need to prepare a separate verification plan, the need for the plan and the content of this plan is not clear in ARP.

R9 Some minor issues were related to credits from verification performed at different levels of systems and items development; to the level of formalization of verification environment in the verification procedures and results; and to the definition of criteria for verification methods others than test. Some other issues were related to independence for verification activities with regarding design activities and to the level of details in description of test objectives and test cases, when considering the requirements set covered.

R10 None

R11 According to ARP475A, the requirement verification not only refers test after the prototype, to verify the design data against the requirement is also part of the requirement verification. But at moment we do not have good way for this except review.

26 Please describe any ARP4754A configuration management issues encountered.

R1 Mostly issues were raised in change control and problem reporting. Evaluating the effect of changes on each processes, systems, etc. was a challenging process. And ensuring the timely transfer of design data to all parties

R2 Skip

R3 Skip

R4 None

R5 PSSA goes through several iterations before final issue

R6 NA

R7 1) Short cuts and full run processes are defined based upon criticality of configuration or change. Still, short cut process would suffice in many cases, e.g.: correction of typos in a System Requirements Document would mean among others building a team of at least 5, alerting the Airplane Manufacturer for the upcoming update. If the typo affects understanding or design, this process is correct. However, removal of a misspelling or transposed word should be allowed to be done at any time, which is then likely to be at the opportunity of a major rework.

2) Sensitization of every single member of a development team in the necessity of configuration and change management needs time to take effect.

R8 The time when the configuration baselines are established can be described more clearly giving example milestones in the certification process.

R9 Some issues occurred were related to the inclusion of design data in the configuration item identification for CM activities and to criteria procedures for archive and retrieval (applicability of SC2). Although there is some practices in place, not clear in the document what are the guidelines regarding interim and design completion configurations (figure 14).

R10 None

R11 The CM is too general in the ARP4754A. We need more specific guidance for the relationship between Part No, Mod, version, document id, etc. Also, the definition for CC1 and CC2 is not clear, I think a criteria is needed for classifying the CC1 and CC2, so the engineers can judge CC for the data by themselves.

27 Please describe any ARP4754A processes assurance issues encountered as it related to your development activities.

R1 Process assurance activities was performed as part of independent system monitoring activities. But stand-alone assessment according to 4754A (with a 4754A questionnaire) should have been performed to assure better compliance.

R2 Skip

R3 Skip

R4 None

R5 NA

R6 NA

R7 Skip

R8 None

R9 Some issues identified: #1. Not clear which level, or at least, which kind of, independence section 5.7 talks about, e.g.: who performs the assurance activities versus who defines the process versus who performs development activities? Individuals or organization level? Most of practices are based on experience from software domain… what about that "portability" – adequate? Too rigorous?

#2. Unclear guidelines regarding deviation from plans when considering the Process Assurance: section 3.2.1 (bottom line for all planning elements) has a general statement about that, but further guidelines are defined only for validation, verification and certification planning elements.

#3. Sometime we have some difficulty in performing assurance due to supplier's data access limitation, like Intellectual Property or ITAR restrictions.

R10 Requirements were initially written based on preliminary system design data which leads to a lot of changes during validation and verification process. Requirements traces have to be reviewed regularly in order to keep them up to date. High level requirements are also an area that causes difficulties, since they are written at the beginning of the program and not updated, with the risk of becoming obsolete and making the traces invalid.

R11 We know the basic idea PA, but it is not quite clear how to make the PA work effectively and typically what kind of person is qualified for the PA.

28 With regard to ARP4754A and engineering judgment, what, if any, difficulties did your company

R1 Skip
R2 Skip
R3 Skip
R4 For engineering judgment, the point is that you have to have a proven database either from previous developments/lessons learnt or R&D programs/testing etc. which are documented to underline the engineering judgment position.
R5 NA
R6 NA
R7 Documentation of engineering judgment, possibly taken as an assumption, encounters reluctance, sometimes resistance. This is often explained as follows: Capturing the judgment as a requirement would make it necessary to be validated. The validation method used will confirm the “judgment”, changing its character to “analyzed” or “reviewed and assessed”.
R8 For military platforms, it is difficult to justify DAL requirement for some mission functions.
R9 Requirements using "engineering judgment" present evidence and documentation with very sparse quality (high and low) being very dependent, of course, on the person who is judging. And as previously spoken (see q. 9, adverse impacts), there may be cases when that person does not have more experience or knowledge than who wrote the evidence, leading to a possible loss of knowledge or even errors that may have consequences on the next project phase. In general, we think that engineering judgment should be avoided. Methods such as analysis and simulation are more scientific and less subject to opinions as engineering judgment. Nevertheless, there may be ways to increase the quality of engineering judgment, like for example training, use of best practices records, etc.
R10 Don't know.
R11 We are lack of the experienced engineers or experts to make good engineering judgment.

29 Please describe any boundary definition issues, between systems and items, that were encountered and how they were manifested.

R1 Especially LRUs were treated as item (hardware) by the companies rather than a part of system. Therefore problem raised to apply 4754A for development process of equipment.

R2 Skip

R3 Skip

R4 None real boundary conditions, one point to mention to define in an early stage to what level of completion the validation must be done and released prior to the transition to the next level, that means for example SW development may need at an earlier stage validated requirements than a hydraulic valve block during the during the development phase.

R5 e.g., Boundary overlap between engine Controls and Installations

R6 NA

R7 The systems and items definition issues are not related to the boundary definitions but more to activities applicable on multiple levels: Credit is sometimes taken on a higher level from verification activities of sub-level items. Attempt to influence the verification activities on these sub-levels to cover both their and the one above might occur. Also, it is possible to have conflicting means of verification on two levels.

R8 The means for communicating derived requirements between the item level and system level.

R9 We are facing difficulties in the usage of REQUIREMENTS MODEL; boundaries when applying DO-331 (Model Based Development and Verification supplement to DO-178C) for such requirements are not clear and ARP4754A guidelines are not considering that supplement.

R10 Tracing requirements between the system and the individual components is difficult and sometimes not possible. Items are developed by suppliers, sometimes with different processes. It is particularly a problem when integrating COTS items in the system.

R11 Actually, the term “boundary” is not clear when I read the ARP4754A.

30 How was your company's safety focal involvement on the project(s) defined and managed?

R1 As military authority we set a safety panel for the project and assigned panel coordinator. Safety panel was a transversal panel. It was responsible for setting the high level safety objectives, approving applicant's safety program plan and aircraft level safety analyses and ensuring (by attending the system certification panels) that all system panels/experts are working according to that methodology set by Safety Panel. Also safety panel organized safety trainings during the project to ensure a certain level of understanding for safety by all authority's system certification experts.

R2 Skip

R3 The company process description defines the involvement of the safety specialists in the projects. Several internal trainings make other disciplines' specialists aware of the safety involvement.

R4 The safety organization/focal is involved from the early beginning in the development process and plays one of the major roles in architecture/requirements based engineering together with system engineering and chief engineering.

R5 Develop the safety case observing Rev A.

R6 No comment

R7 Skip

R8 Safety Engineer has a key role in projects and the responsibilities are defined in System Safety Program Plans.

R9 The safety team participated as other technologies in the project definition and management.

R10 He prepared the PSSAs and reviewed system requirements.

R11 My company provides computer to the customer following their requirements, including DAL and safety requirements, we do not do much work on the safety assessment, typically we provide FMEA data to the customer to support their SSA, So I leave this table blank.

31 Please elaborate on your experience of airplane manufacturer management of ARP4754A safety process activities, as applicable.

R1 Skip

R2 Skip

R3 As system supplier we submit validation and verification plans, system development plan, safety and reliability plan to the aircraft manufacturer .The aircraft manufacturer reviewed and approved these plans. The aircraft manufacturer participated in technical meetings and reviewed and approved all safety documentation.

R4 What we have experienced so far it is poor from airplane manufacturer's side, what we get is mainly the SFHA for the contracted systems that's it. One other experience is that airplane manufactures contract consulting agencies, to review the ARP4754A processes at supplier level but at airplane manufactures level they do it differently (they cook their own soup as we say in country).

R5 NA

R6 No comment

R7 Skip

R8 Airplane manufacturers tend to give more stringent requirements than the actual required ones.

R9 The process describe in the ARP4754A regarding safety were similar to those described in ARP4761 and therefore applicable in several new type designs and modifications. Specifically on ARP4754A no project were fully certified although two current programs are under development following those safety intent of ARP4754A and one, the last project' TC adopted ARP4754 (legacy version) based processes, with some features from version A. Regarding DAL allocation the intent, which were already in ARP4754, were considered in the last 7 new clean sheet developments, and FDAL allocation in the current 2 programs . It's worth to mention that all relevant considerations during the revision of ARP4754A and ARP4761A discussed during the S18 meetings were applied in the product development of several programs whenever applicable.

R10 PSSA tracing to system requirements has been difficult.

R11 Skip

32 Please describe any safety process activity issues you or your organization experienced.

R1 Skip
R2 Skip
R3 The relationship between safety, requirements capture process and (system) design needs to be better established for development programs.
R4 None
R5 Resource issues
R6 No comment
R7 Skip
R8 Derived requirement analysis is always an issue. Who should initiate this analysis and how it should be carried out always a problem.
R9 See 33.
R10 PSSA tracing to system requirements has been difficult.
R11 Skip

33 Describe the ARP4754A safety process activity issue(s) (e.g. FHA, PASA, PSSA, FTA, CCA).

R1 We had issues related to Common Mode Analysis outputs especially when applicant use architectural mitigation for DAL assignment. Companies didn't want to show independence for DAL assignment (for HAZ and MAJ FC) by CMA. They provided evidence of CMA for only CAT failure conditions (for no single failure requirements).

R2 Skip

R3 As a system supplier we have always been involved in the whole V&V process form PSSA to SSA incl. FTA, CMA, PRA, FMEA. No special issues were experienced due to the ARP 4754A.

R4 None

R5 All above necessary for Safety Case development

R6 No comment

R7 Skip

R8 We had confusion on whether the probabilistic requirement should match with the DAL assigned to lower level events in a Fault Tree. We had confusion about how to transform the results of CMA into safety requirements.

R9 In general, the systematic and complete analysis performed for FHA, PASA, PSSA, FTA, CCA are generated late in aircraft development when the definitions are almost freeze due to the lack of resources in the early phases. This causes some rework late in design after the throughout analysis is completed for final certification. Also, due to the different mindset the communication between safety specialist to project management and the project designers.

R10 PSSA tracing to system requirements has been difficult.

R11 Skip

34 Please describe any issues associated with definition or assignment of "safety related requirements".

R1 Safety related requirements are defined in different sections of 4754A. We required from applicant to mark safety related requirements (related to Flight Operation, Maintenance Tasks, function, independence, etc.) with kind of tag on requirement management tool to take everyone attention on critical requirements. But some management issues raised to assign and trace the requirements.

R2 Skip

R3 A detailed definition had to be established, when a requirement is safety related. In the process it must be ensured, that this determination can only be made by a safety specialist

R4 None

R5 Safety requirements developed by Safety. Safety related may come from a Sub-System SSDD.

R6 No comment

R7 Skip

R8 We had difficulty when to flow down FDAL requirements (i.e. right after FHA completion or in PSSA stage) but we de *[Ed note: response was incomplete.]*

R9 The link/traceability between safety analysis and artifacts generated for safety (following the methodologies already in place for years in the industry such as ARP4761) and the development requirements and artifacts is a challenge, especially during the early design phases and across the suppliers chain. Also, as the number of requirements increase, the safety requirements, or the safety driven requirements are sometimes "lost" in the middle of the numerous requirements decreasing its priority over other requirements, especially when a function , which is considered critical (FDAL A, B), could not be decoupled from other non-critical functionalities or goals. An example is an aircraft performance function which has critical goals (such as maintain positive climb gradient) but also not safety driven goals (market driven) such as time to climb. All the requirements related to this function might be FDAL A and therefore threated in similar way.

R10 PSSA tracing to system requirements has been difficult.

R11 Skip

35 Please describe the context of any architectural mitigation strategies successfully used in the assignment of Functional Development Assurance Levels (FDALs).

R1 Skip
R2 Skip
R3 Redundant and dissimilar functions, Separation of functions
R4 Introduction of dissimilar control- monitor channel control architectures; dissimilar control architectures etc.
R5 NA
R6 No comment
R7 Skip
R8 Independent systems performing same function.
R9 Independent functions allocated to different system and suppliers. Independent functions allocated to totally dissimilar technologies (ex: electronics versus mechanical).
R10 Redundancy and independence of control and monitoring functions has been used throughout the system development. Protection functions external to the system have also be used in limited cases.
R11 Skip

36 Please describe the context of any architectural mitigation strategies successfully used in the assignment of Item Development Assurance Levels (IDALs).

R1 Skip
R2 Skip
R3 On Control Computers: Partitioning, Multiple Version Dissimilar SW, Safety Monitoring.
R4 None
R5 NA
R6 No comment
R7 Skip
R8 Different items having same output data.
R9 Low level dissimilarity (SW, AEH, HW - processors, A/D converters, sensors...) in some critical functions, hardwire solutions, relay logics, implementation of monitors in a different system or a specific dissimilar monitor for a specific failure mode and service experience for similar non-novel solutions with a significant accumulated field experience were used as mitigation strategies.
R10 Same as 35.
R11 Skip

37 What, if any, tools have you used to assign FDALs?

R1 FTA
R2 Skip
R3 Fault Tree Analysis, Event Trees
R4 None
R5 FHA
R6 No comment
R7 Requirements database, same used for requirements capture and management
R8 None
R9 Error trees, PASA activities.
R10 Don't know.
R11 Skip

38 What tools, if any, have you used to assign IDALs?

R1 FTA
R2 Skip
R3 Fault Tree Analysis, Event Trees
R4 None
R5 FTA
R6 No comment
R7 Requirements database, same used for requirements capture and management.
R8 None
R9 Error trees, CMA (common mode analysis) internal process.
R10 Don't know.
R11 Skip

39 What FDAL assignment levels were assigned and satisfied?

R1 FDAL A and B were satisfied in our project
R2 Skip
R3 Up to FDAL A
R4 FDAL A,B,C,D
R5 DAL A
R6 No comment
R7 Focus on FDAL A/B addressing Catastrophic/Hazardous failure condition.
R8 All levels.
R9 A to E.
R10 All system functions.
R11 Skip

40 Please describe any issues or difficulties in selecting between ARP4754A Option 1 or 2 in Table 3 for FDAL or IDAL assignments that were encountered.

R1 Skip

R2 Skip

R3 For a combination of failures of mechanical items and electronic items leading to cat. failures: Can credit be taken of the mechanical item being DAL A, thus reducing the DAL of the electronic item to C?

R4 None

R5 NA

R6 No comment

R7 Skip

R8 When deciding the sufficiency of functional independence and item development independence. The intent and relationship with DAL assignment process of Common Mode Analysis should be updated to support this crucial part of ARP.

R9 Functional independence is always a difficult discussion, especially the same system or supplier team is used. The independence attributes are not clear variable/criteria and may vary from authorities and people mindset.

R10 Don't know.

R11 Skip

41 Briefly describe any Table 3, Note 1 issues encountered during the assignment of FDAL or IDAL on the project.

R1 For FDAL A single member function (software was assigned IDAL A too), we wanted from applicant to show evidence that SW architecture is robust enough to deal with errors. We also required software fault tree analysis to support the evidences.

R2 Skip

R3 None

R4 None

R5 NA

R6 No comment

R7 Skip

R8 Note 1 does not give a clear idea for what is required extra in this type of situation, because if we have FDAL A system, the development rigor required in ARP demands maximum independent process in terms of validation and verification.

R9 The current authorities criteria/vision has been more restricted than the method proposed in the ARP4754A. The authorities still discuss in a case by case despite the process. The previous version of ARP4754 with the potential acceptable examples were more likely to be useful for aircraft development.

R10 Don't know.

R11 Skip

42 Looking back, how did your understanding of Functional/Item DAL assignment process evolve throughout the project.

R1 We had to deal with CAT function with DAL A software. Same software run on both computers. During the process the discussion was weather two independent level B software developed by different teams is better or not in terms of error. Some research say two different SW generates more errors. Benefit of using of Option 2 was another question.

R2 As a regulator, an observation is that because the company's process specialists don't do safety assessment, they often are not aware of how Table 3 is used.

R3 It was not fully clear, down to what level FDAL-determination should be performed: Down to each single requirement or only for top-level functions and thus one FDAL for the whole specification. In the process the latter was finally applied On IDAL determination there were discussions about combination of failures of mechanical items and electronic items leading to cat. Failures: Can credit be taken of the mechanical item being IDAL A, thus reducing the IDAL of the electronic item to C? The decision was, not to take credit of the mechanical item being IDAL A, however there is no clear substantiation for it.

R4 We faced lots of discussion how to evaluate FDAL if not assigned form the parent documentation, which was the case in our previous and actual running programs. Discussions lead to the point that in case of a system is identified with one Top Level Failure conditions "Catastrophic" the entire system is dealt as FDAL on System level. At equipment level we differentiated the architecture then to cover the FDAL A with dedicated IDAL's for the electronic control units to show compliance.

R5 NA

R6 No comment

R7 Skip

R8 It is in close relationship with the customer requirements (in A/C level), system functions, their allocations to subsystems and system architecture. We observed that since there are lots of factors driving DAL assignment process it is difficult to manage the changes. Because you have to catch up with or provide output beforehand the item level development processes. There are always schedule pressure, since all the activities performed concurrently, DAL assignment process or safety assessment process needs to be performed as early as possible but in practice it is difficult to complete these when you don't have enough data for substantiation of results to derive safety requirements.

R9 For the common developer, it has been very difficult concept to be understood and applied. For most the users IDAL is a more straightforward concept but the FDAL itself and the mixing with IDAL in a FFS approach is a very confusing and complex to operationalize method. Even for a specialist it still causes misunderstanding and misalignment all across the company.

R10 It has improved, allowing to reduce the FDAL and IDAL in some particular cases.

R11 Skip

43 What, if any, concerns do you have with the current ARP4754A industry guidelines for development and assurance?

R1 4754A set a systematic approach to development. As a result of this, it increases documentation effort by applicants and assessment/acceptance effort by Authority. Concerns were mostly related to cost and schedule.

R2 The line between system engineering and safety engineering is vague, consequently the scope of application widely varies between aircraft manufacturers.

R3 Skip

R4 The ARP provides recommended practice with recommendations, but it seems that our customers and respectively the authorities interpreted recommendation as a “shall” required and are not open to accept a different approach.

R5 More work, not enough experience

R6 No comment

R7 Skip

R8 Transition criteria between the activities within the development processes and integral processes can be defined with an example.

R9 Besides the ones provided in questions 15/16, 19, 24, 27 and 29, we have the following:
#1. Section 1 (SCOPE) is unclear in the following points: in the upper bound of product specification, it explicitly excludes from these guidelines some activities and technologies, like aircraft structural development. Nevertheless other aircraft level technologies, like the ones related to aeronautics, e.g. flight mechanics, performance, aeroelasticity, etc. remain undefined, once they are neither explicitly excluded nor can be fit the area of “…development of aircraft systems…” stated in the first paragraph of that section. In the lower bound of product specification, once ARP4754A define it boundary where software and hardware start, it is not clear if a single “equipment” is part of its scope. Around this issue, it’s not clear as well how ARP4754A and DO-297 guidelines work together for the case of an “Integrated Modular Architecture” (IMA).

#2. There is a perception that the compliance plans (both internal and from the suppliers) are somewhat inefficient to promote product improvement by themselves. From one hand, it seems that ARP4754A has too open guidelines in such a way that any plan can be compliant with that; on the other hand, there may be too much rigor depending on who define, apply and oversight the plans and artifacts, to clearly identify the improvements desired (similar to situation described in q. 15). We have tried to mitigate that situation, both internally and at suppliers (see q. 21) through planned process reviews, similar to the software “SOIs” reviews. We are working on an internal policy to perform those process reviews on a regular basis in all programs and contracts, covering not only process aspects but also the related technology aspects (e.g., requirements validation and rational fundamentals and design choices) by involving people with good knowledge and experience in the technologies reviewed.

R10 Too long and complicated in some areas.

R11 1.The interface with DO178, DO254, DO297, etc, needs to be more clearly defined. 2. Some terms in definitions and the main body are not consistent, for example, the some context, the term “item” refers to LRU, in other context, “item” refers to single piece of SW or HW.

44 What, if any, additional guideline material(s) would help to satisfy regulatory expectations?

R1 Skip

R2 Prioritize the following 4 aspects of the integral process: Planning, Safety Assessment, Requirement Validation, Implementation Verification.

R3 More detailed explanations to the questions/issues raised in point 6, 18, 40 and 42 above.

R4 Training of the ARP4754A would help to understand the aim end reduce the window of interpretations

R5 Training

R6 No comment

R7 Skip

R8 The details of the flow of information between guideline documents (ARP 4754, ARP 4761, DO-178, DO-254) can be presented with an example containing SW and AEH development.

R9 Although we have neither exercised nor studied them yet, we feel that the following FAA documents can be helpful on this matter: DOT/FAA/AR-08/34, Requirements Engineering Management Findings Report, May 2009. DOT/FAA/AR-08/32, Requirements Engineering Management Handbook, June 2009.

R10 Don't know.

R11 I understand that ARP4754A do not want to limit the applicant or suppliers, but I think it will be helpful if providing good Checklist and document template as examples.

45 How did SAE AIR6110, the industry application example for ARP4754A, aid your understanding of the development process described in ARP4754A?

R1 It helps for better understanding of 4754A but I think It is not well known by industry. When it becomes an appendix of 4754, it will make more sense.

R2 Skip

R3 Skip

R4 None

R5 NA

R6 No comment

R7 Skip

R8 Examples given in AIR are very helpful to understand the application of the system development process described in ARP. It provides very valuable examples for all the activities defined in the process thus complements the application of ARP. Especially requirement validation example tables.

R9 We have neither exercised nor studied in deep that document up to now.

R10 I didn’t use it.

R11 I think current AIR6110 will be a great help for us to understanding the development, but I think besides the development process, it would be more help if the document includes the example for Process Assurance, Configuration Management process, requirement management, etc.

46 What information or issues in AIR6110, contributed to confusion in satisfying ARP4754A objective expectations?

R1 Skip
R2 Skip
R3 Skip
R4 None
R5 NA
R6 No comment
R7 Skip
R8 None, detailed description of process output data was helpful to understand ARP descriptions.
R9 See 45.
R10 None
R11 I am not quite understand the meaning of “contributed to confusion”. Is it required to identify the inconsistent between the AIR6110 and ARP4754A?

47 What, if any, issues or concerns do you have with the current certification authority guidance material for application of development and assurance?

R1 Skip
R2 Skip
R3 The guidance of ARP 4754A is required by the authorities and may in some cases be over-interpreted and result in unnecessary effort and impractical tasks due to unclear interpretation of the original spirit of the guidance.
R4 None
R5 NA
R6 No comment
R7 Skip
R8 None
R9 See 15 and 16.
R10 None
R11 Skip

48 What, if any, issues or concerns do you have with the current certification authority policies related to the application development and assurance?

R1 Skip
R2 Skip
R3 Skip
R4 None
R5 NA
R6 No comment
R7 Skip
R8 None
R9 See 15 and 16.
R10 None
R11 Skip

49 What additional case study application examples would be helpful in understanding development process expectations? Why would these examples be helpful?

R1 Skip
R2 Skip
R3 Skip
R4 None
R5 FADEC Case Study
R6 No comment
R7 Skip
R8 The example system assesses in 4761, 4761A and AIR6110 are all the same, Wheel Brake System. This can be another system like cockpit display and flight management system since this type of systems are more interface with other systems and have more items to be integrated it will provide good guidance in understanding the DAL assignment process.
R9 A case of MBDV (Model Based Development and Verification), aligned with guidance of DO-331, top-down from aircraft level through system design and reaching software boundary. This would be helpful due to the lack of guidelines in using model both as requirements and as part of design data and the newness of usage of guidance provided by DO-331, raising difficulties on defining the boundaries. Another case that would be interesting and helpful due to similar reasons would be development of a system through the usage of an IMA (see q. 43).
R10 Don't know.
R11 Requirement management procedure. We have DOORS in the company, but we do not know how to use it affectively, what’s the relationship between the DOORS and CM tools, etc.

50 Please describe the sector of the industry in which you work (e.g certification authority, airplane manufacturer, integrated system supplier, equipment supplier, etc.).

R1 Military Certification Authority
R2 Certification authority
R3 Skip
R4 Integrated system supplier for landing gear systems (ATA 32), primary and secondary flight control systems.
R5 Turbine engine manufacturer
R6 Engine supplier
R7 Integrated system and equipment supplier
R8 Integrated system supplier, equipment supplier.
R9 Airplane manufacturer
R10 Airplane manufacturer
R11 Equipment supplier

51 Please describe which regulatory framework you normally address (e.g. Transport (Part 25), Normal, Utility (Part 23), Rotorcraft (Part 27-29), other, etc).

R1 Part 25, MIL-HNBK-516
R2 Part 25
R3 Skip
R4 The main focus is on Part 25 and Part 29, with random activities on Part23 and Part 27
R5 Part 25 and 27
R6 AC 33.28
R7 Part 25, Part 23, Part 27-29
R8 Part 23, Part 27-29.
R9 Part 25 (mainly), Part 23.
R10 Utility (Part 23)
R11 We provide the computers for the different kind of customers, including Part 25, 23, 27,39, 33,etc.

52 Please discuss (in general terms) any current or future ARP4754A applications?

R1 4754A is also a good guideline for military projects when it is tailored according to the scope of the project. There is no appropriate guidance material in military regulations/standards that integrates system development and safety processes together and no clear guideline to determine DALs.

R2 As regulators, we expect aircraft companies and systems suppliers will establish and maintain infrastructures apply the ARP and we anticipate that over time their activities will be streamlined to be more efficient than the first application. As the ACOs gain understanding and confidence in their applicants' processes, we anticipate reduced involvement, and oversight will also be streamlined as a function of the scope/complexity/novelty of the product

R3 Skip

R4 Long Range Wide Body Commercial Aircraft Landing Gear (Part 25); Helicopter Landing Gear System (Part 29)

R5 Control systems for turbine engine

R6 None

R7

R8 Avionic system (primary flight displays, navigation sensors, internal communication systems) development for utility helicopter program. Avionic system(mission computers, display systems, navigation and communication equipment), and weapon systems (integration of various weapons to platform) development for fighter jet program. Equipment (mission computers, displays, communication and navigation equipment) development for a trainer aircraft program. Avionic system development for civil transport category airplane.

R9 See q. 1 – in one of the first program, certification authority requested ARP4754A as one of the means of compliance with 25.1309 through an issue paper; in the second program, they understood that an issue paper is not needed – the compliance with 25.1309 would require to follow ARP4754A, based on the AC 20-174.

R10 Currently applying it in a Part 23 airplane.

R11 Compliance mean for System, LRU, SRU Guidance for the companies to improve their development process.

B.2 2 Roundtable Discussion Notes

Facilitator Introduction:

This is an informal System Development Process discussion with SAE S18 Committee Members to enhance the SAAB-EII NASA ARP4754A study project with additional industrial experience inputs through round table discussions. The discussion commentary, with only aircraft, system, equipment or regulatory identification nomenclature will be attempted. The assembled SAE S18 participants should provide their individual opinions and experiences on lessons learned. The inputs should fulfill the guidance and process materials on the white spaces without pointing the problems on recommended practice.

Discussion Area 1: Lessons learned in applying ARP4754A: Are there any difficulties in DAL assignments or satisfying the objectives? Is there any difficulty to assign the DAL? Are they all level A or B? Any FDAL lower than B?

AC A: I have not seen many DAL assignments at level B. Most of the assignments fall into category A or C.

SYS B: I actually have seen many assignments at level B. Functional Decomposition is the key. It is dependent on how the functionality is assigned to FDALs and allocated to IDALs. The problem is derived requirements. When you derive requirement at the system level, how to allocate to item level and assign DALs. A good allocation make the program management have less DAL assignment arguments.

AC A: This is based on the requirement flow down. I agree that in the SW level or box level assignment that was passed down to avionic suppliers. However, in the system level we always do one level better, so it will result in a hazardous assignment increasing to be catastrophic [level A].

EQ A: There is a great sense of impact and argument of ARP4754A since the management knows it will directly impact the DAL assignments; however, it seems to be getting easier to deal with DAL assignment argument recently.

I believe Section 5.2 of ARP4754A is written in such a way that it is clearer than the original ARP4754 for DAL allocation. People are assuming ARP4754A is the same as ARP4754, but we have enough to go back to them and say: “No your DAL location breakdown happens once” and it is very clear once you show them the recommended practice. They will go back and say: “Oh! We missed that”.

AC B: We try to make it as objective as possible. Something that is fundamentally a subject of process.

EQ A: There are a couple people want to further reduce down, but once we show them Section 5.2 of ARP4754A then the arguments are done.

Sys B: The only issue I have seen is that we have 18 level “As” and I want to do one to level D. We cannot do that anymore based on the written in the table.

AC A: Let me tell you another experience. When you go back and go to item level, and people say, I have so much more work to do. We set down and talk about what Validation means and the activity we just done is called owner engineering course of action. We realized that the validation was done in the past, and the only thing that was not done is to take credit. I ask them to take

schematic, Simulink, engineering review and test cases and call them validation as done with independence. The credit has never received in the past with those Validation while they are already DAL A and B, but now we can get the credit with the improved guideline.

It is not difficult to assign DAL assignments, but the assignment might result in additional work. The ARP4754A has a clear comparison to show the differences with ARP4754; however, people are assuming they are the same, while it is not true. The subject of objective allocation needs to be further broken down. It is incorrect while people assigning 18 level A with only one level D. There needs to be an explanation for each process to evaluate the work; otherwise, there is too much work to be done. The Validation will take credit on ARP4754A, but we do want to avoid extra work that is not going to take credit.

SYS B: One of the challenges I have is to understand what is an IDAL. An IDAL applies to the whole life. It divides the concepts to where you are applying to. I have a single item that has mixed many IDALs. There become a discussion on the level A has a level D coding SW behind it internally. It shows it is being activated appropriately, so I have an FDAL.

SYS C: It is the problem that we have a DAL A partition and a DAL D in there. You cannot do it by looking at the table. The case is like, you have a simple switch in the hardware; therefore, by ARP4754A, it is DAL A. I used DAL A switch to detect DAL B. We cannot do that either per table, but common sense it is OK. Those are common sense that we can fix in ARP 4754A.

SYS B: The other one that I dislike with is that by definition DAL C is not catastrophic. We programming in the wrong time. I do not know if I need to do anything or not, but it has to be DAL C according to the system because the wording in the ARP. However, I cannot proof confidentially and I cannot stop either because catastrophic by definition.

There needs to be a good understanding of IDAL. IDAL is for the whole item, so the single item may have mixed items. Per ARP4754A table, it is incorrect to have a level A partition with a level D allocation, but sometimes it seems to be fine in common sense. An example for a level A assign to mechanical devise is like a simple DAL A switch to detect DAL B.

AC A: By definition, DAL C is not catastrophic; however, the combination of DAL in mechanical and electrical objectives in each level may result of level increasing.

SYS B: It is an issue that if there was no agreement up front. Every hazardous failure condition has something not making sense or misleading, which cause argument and rework.

AC A: When you look at the aircraft level if I go to PASA to talk about DAL assignment. Not a big deal since they use DO178, 254. When I go to ECS for flight control systems that has never done this before, they do not know what to do, and I will have to explain them the concept and let them know that they have done it before, and now you can get credit for it. It is depend on who your audience is.

SYS B: It is documenting what you actually did to satisfy the objectives. We did many things and we cannot know what we did, so we document it to now to know the steps.

AC A: It is important to know who you are talking to and understand from their stand point. If I talk to an ACO regulator it will be smooth, but if I talk to a purely mechanical flight control system or ice protection system specialist, and they will be asking: Why are you giving this material to me? We need to have the local regulator training to resolve cross ways.

It is depend on who your audience is. While interfacing organization that is using DO178B and DO 254, they are audit friendly. The documents are actually mentioning what you actually did. You

only need to explain your concepts. There can be issues while dealing with purely mechanical flight control system or ice protection system specialist that are not familiar with DAL assignments.

AC A: Question on satisfying objectives while we wrote the ARP 4754A material. The regulator looked at appendix A and told me that I gave him a prescriptive checklist, which he can go around to ask for evidences on the checklists. There was a regulator challenge stuff on ARP4761 CMA stuff and told me that things are missing. I explained to them that this is a guideline, but the regulator told me that we need to follow ARP 4761 appendix.

AC B: Tell him to go back and read page one. There are also many places in the documents telling you that is not true. They chose to interpret that way then they are blinding themselves how the ARP works.

AC A: The result was that it went into debate and I had to go back and propose a deviation for compliance. I have to re-adjust to show the deviation is still compliant to ARP 4761.

AC B: You are then non-compliant to a non-compliance document.

Facilitator: In DO we use compliant, but we should use satisfying the objectives in ARP because it is only a guideline and there is no rule there.

AC B: Shall and must do not exist in the ARP guideline.

It is possible that the regulatory authority to use the appendix as a prescriptive checklist and enforce the company to be compliant while the goal is supposed to be only on satisfying the objectives. The incorrect usage on the recommended practice may result of providing additional deviation in order to show the compliance.

EQ B: I had an experience that we were forced to do a DAL A in Software. The FDAL becomes a level A while we do not want to mess with it, so we will just do them all. This is a gray area while we are mandated from the bottom.

Facilitator: One thing that we learned by comparing ARP and DO is that if the DO is assigned as level A then it also migrated to systems to the same level. Even though ARP4754A level is not A, but be get stuck with it by the lower level bottom up. It turns out that it's OK while the objectives for A and B in ARP4754A are the same.

AC A: While dealing with the engine supplier, FADEC were B on two of them. The suppler had identical FADEC channel with no independence and they thought they can have B on them per using the table in ARP4754A.

In order to show compliance to DO and satisfy the objectives of ARP, the recommended practice of FDAL may end up required even if it is not. There are cases the lower level A forces ARP to comply while most likely there is a bottom up impact.

Discussion Area 2: Engineering Judgment

Facilitator: What are your experiences with regards to engineering judgment? What should developers do if they have no experience? How do you accomplish if you have never done it before? How to fill in the blanks?

EQ B: By reading ARP, there are 3 levels of decomposition. There is no reason that we cannot take the principle of the ARP and increase the layer for higher complexity. We are not going to commit and assume the small layer of decomposition is enough.

REG A: There is a need to have background of domain knowledge to ask the correct questions to review the documents. The process depends on experience people who have the history of lessons learned.

AC C: There needs to be better definition on the objects to support engineering judgment if there is not enough history or lessons and learned. The assumptions are not based on technical activity, but by the objectives and principle that you want to archive. This is challenge to write the policy and guidance to help the engineers to understand the objectives to achieve.

AC D: There are extreme cases that the certification authority needs experience to do something first. Maybe the training for certification authority is needed.

SYS B: While assuming something is the same and consistent, the assumption is also engineering judgment.

AC D: How do people start? They build experience from something that does not need to be certified first to build up their domain knowledge. After they get their experiences then they can move to a Part 23 then Part 25 aircraft. All those experiences are engineering judgment, and there is no way to skip all that unless hiring the talent people.

SYS C: If we look at the basic, there is not much differences when a good functional allocation is needed. If you have a system development knowledge background then it will help support facilitate engineering judgment. If we do not have the experience then we hire experience people, which can do good functional allocation.

SYS B: There is a dependency of company culture differences. Some companies focus on safety, but some of them want the minimum cost. The requirements are driven by the company behavior on their culture differences. The company culture philosophy will drive the engineers to make some decisions, which are engineering judgments.

AC A: We have never been good systems engineering organization. Since 1927, we have been able to design build and certified aircraft in local office. Now we have a hiccup on AC20-174. In ARP there are all kinds of engineering judgment for the reviews that we can take credit for. Somehow locally for my experience is to that if you are not compliant of 8110-3 or 8100-9 and unable to show the engineering judgment from experience people, it will be hard to take credit from them.

REG A: Can I just clarify something? The AC is about development assurance process for complex systems. The ARP is a means, but not the only means. We only use it to design and build a better aircraft. Maybe we need to have a development assurance process for company start up.

The engineering judgment should focus on strict objectives to in accordance with the planning. If you can go back and show what you should do, and what you need to add on due to any unresolved problems. That would be great. We do not need everything to be blindly compliant to ARP4754A.

AC A: There is no good way to maintain or archive lessons learned information. In some cases, they (lessons learned) are only captured in an engineer's note book. The experienced people who have the knowledge are behind the story. For the process now the certification plan should control the roles, responsibility, negotiation and planning. We do want to follow the objectives, but we also need engineering judgment to set the priority of the objectives in order to improve the "selling" of the process.

Item 3: Certification lesson learned on application of ARP4754A

Facilitator: ARP is a means of compliance. Map how you accomplish the objective in the ARP.

System B: The ARP is a mean of compliant to the regulations. Where is the compliance matrix for the regulation? It is difficult to map the requirement and the matrix.

Facilitator: ARP 4754A Appendix A is a summary only. In order to approach the satisfaction of ARP, we need to read the text for detail objectives. There maybe 30 objectives in the appendix, but 90 objectives in the ARP content. Another approach is like, Do you understand the *[ARP]* objectives? Have you setup to accomplish your plan? Understanding ARP and include in your plan is necessary. The DOs are easier to audit since it tells you what to do.

Person ?: It is possible to fall into strictly compliant to ARP with no background on what the purpose is. Good planning is needed to find problems if they need to be compliant with real values. It is not a good practice to blindly to be compliant to all the artifacts.

REG A: Enough or not enough is an engineering judgment from regulatory stand point, which needs artifacts to support process in order to comply only on necessary objective and avoid negotiation during the audit.

AC A: ACO specialist scope is different than each other and also cause differences on different programs. It is hard to determine when or when not to exercise the particular aspect.

EQ B: Develop partnership is needed to handle disagreements. The agreement between you and the ACO management can resolve different cases under different levels, which can be refer to PSP.

SYS B: Fundamentally, the higher level authority does not have good understanding on the lower level sub-system. It is common that the system get overworked while certifying the sub-system by reading the guidance with checking boxes.

Facilitator: There is a lack of consistency for interpreter side for certifying. It may be recommended instead of revising the ACs we can create some standards or guidance for people doing evaluation. Kind of like a lessons learned for regulatory standpoint.

Person ?: There is a battle on training our own people or training the regulatory authority. There needs to be a trust of each other in order to have a smooth certification.

REG B: Pre-audit can resolve problems. The pre-audit can have the supplier understand the objectives and where they come from. Try to meet the intent of assigning DALs. For example, to perform more robustness testing to meet the intent of unintended function. In this case, the audit will go smoother.

AC A: There are problems on the AC 8110.15. Need experience on brand new process. This issue has grown locally, but there were no people to support it. There is culture shift for individual authority, which does not support locally while the ARP get interpreted locally. The lack of process understanding needs to be addressed in FAA manual.

There was a case that ACO get questioned if they overviewed the AC before the audit. Only one out of a few ACO confirmed while they even think the AC is only the few sentences presented in the FAA page.

EQ B: There was a case that DO178B get audited for the project for 15+ times. The level of FAA involvement on carry the assurance is needed to minimize the times of re-auditing.

Appendix C Objectives Correlation Study

C 1 Introduction

During the project kick-off meeting, additional questions were identified for project study. This appendix responds to establishing a justification for the ARP4754A aircraft and system level process objectives and guidelines question. The study herein approaches this question with two considerations;

1. How are ARP4754A guidelines used for regulatory compliance support? And,
2. How do the guideline objectives in ARP4754A compare to the other industry development life cycle objectives?

C 2 ARP4754A Support of Regulatory Compliance

The authors of the 2002 Arsenal Draft proposed 14CFR Part 25.1309 rule and advisory circular noted a concern regarding the ability to adequately address the safety assessment of "highly" integrated systems. They noted that traditional design and analysis techniques may be inadequate for complex systems due to non-deterministic risks and inadequate safety coverage. To address these concerns the Authors noted that a systematic use of assurance techniques increases the confidence that errors are adequately identified and corrected. These "assurance techniques" should consider:

- Development assurance using a combination of process assurance & verification coverage criteria,
- Structured analysis,
- Airplane-level assessment techniques, and
- Inter & Intra system interactions.

The application of these "assurance methods" would help ensure errors, which may cause failures, are mitigated to an extent practical.

AC20-174, Development of Civil Aircraft and Systems, recognizes that ARP4754A establishes an acceptable method for instituting a development assurance process to support compliance to §25.1309. Figure 24 presents the overall summary then for showing compliance to the regulation using a combination of safety assessments of the final implementation and development process satisfying the objectives of ARP4754A and the other "DO" life cycle processes.

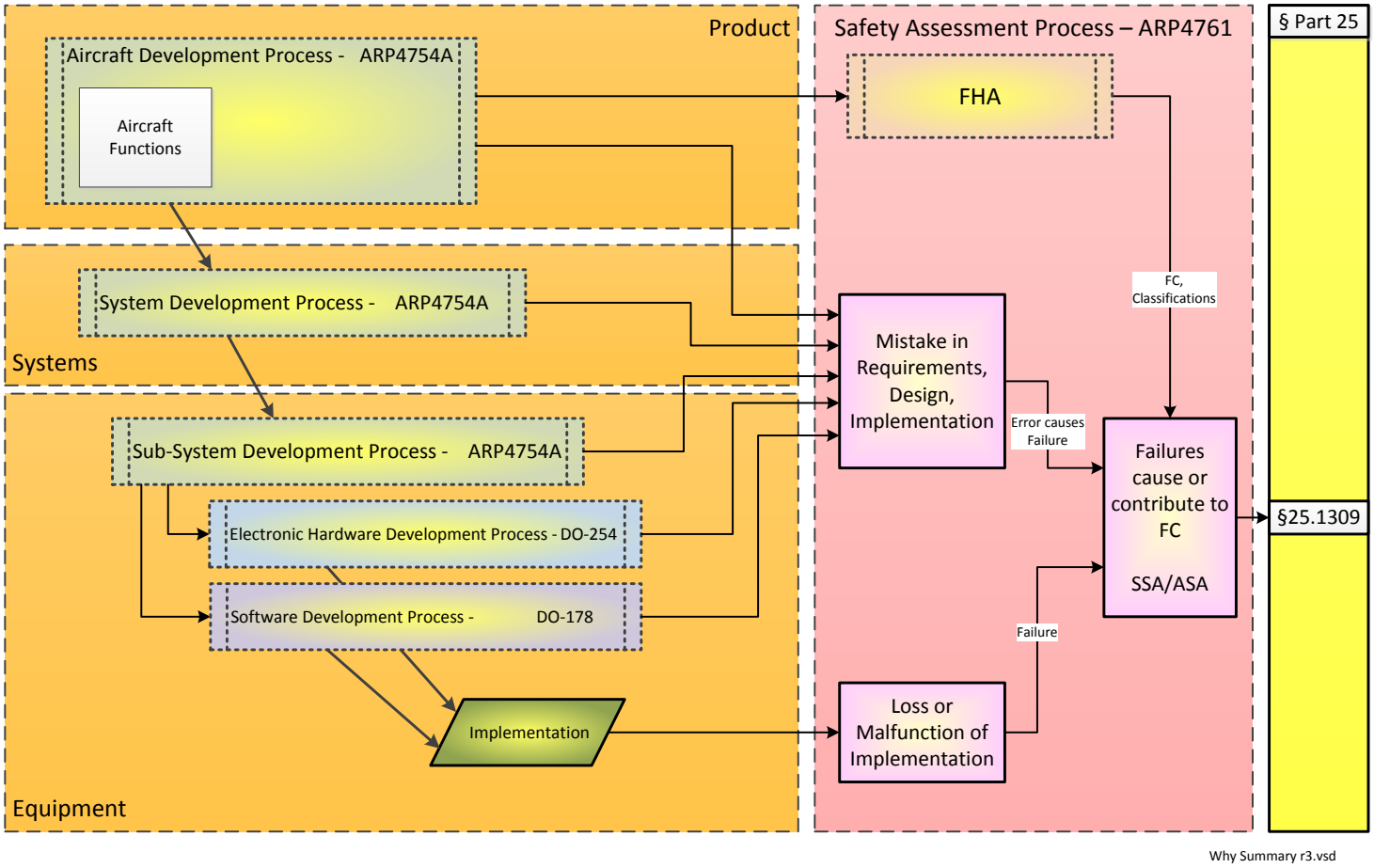


Figure 24 ARP4754A Certification Support Summary

C 2.1 Development Process – Historical Perspective

A look at the timeline associated with the creation of the various industry development process documents helps establish a basic consideration as to what and why ARP4754A objectives were established. Figure 25 presents a synopsis of guideline/guidance document publications over the last 23 years. It is reasonably safe to assume that a synergy with DO-178, published in 1992, was established for the systems objectives published in ARP4754 in 1996.

The rationale for the resultant objectives and guidelines in ARP4754 and subsequently ARP4754A, are thereby primarily based on similarity to those objectives that were established earlier in time by DO-178B.

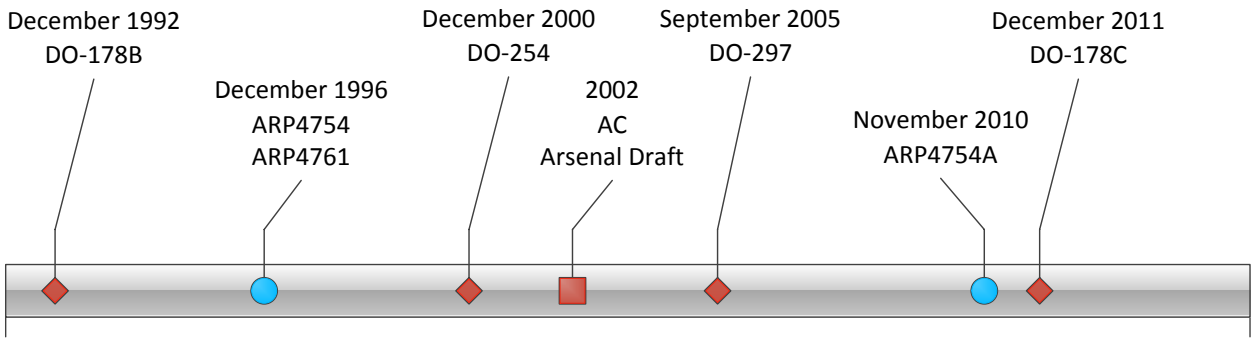


Figure 25 Development Processes Historical Timeline

C 3 ARP4754A to Other Industry Development Documents

This section performs a comparison analysis of the objectives identified in Appendix A of ARP4754A, "Guidelines for Development of Civil Aircraft and Systems" with the corresponding objectives identified in the software (DO-178 B/C Considerations in Airborne Systems and Equipment Certification) and hardware (DO-254 Design Assurance Guidance for Airborne Electronic Hardware) life cycle process guidance documents. The high-level ARP development process objectives are highlighted in Figure 26. This two-dimensional graphic summarizes the objective areas identified in ARP4754A Appendix A, including the recommendations as well as the configuration management data control categories.

In order to provide an "apples to apples" comparison, the ARP objectives were arranged so that an effective comparison between the life cycle activities, data and configuration management control could be achieved. The following process objective areas of Figure 26 are compared:

- Planning,
- Development process (requirements capture, management),
- Validation process,
- Verification process,
- Configuration Management and,
- Process Assurance.

The safety process activities (FHA and general safety process) are acknowledged as applicable only to the airplane/system development levels, so were omitted from the comparison activities.

Section 4 provides the comparison results for the above selected process objective areas.

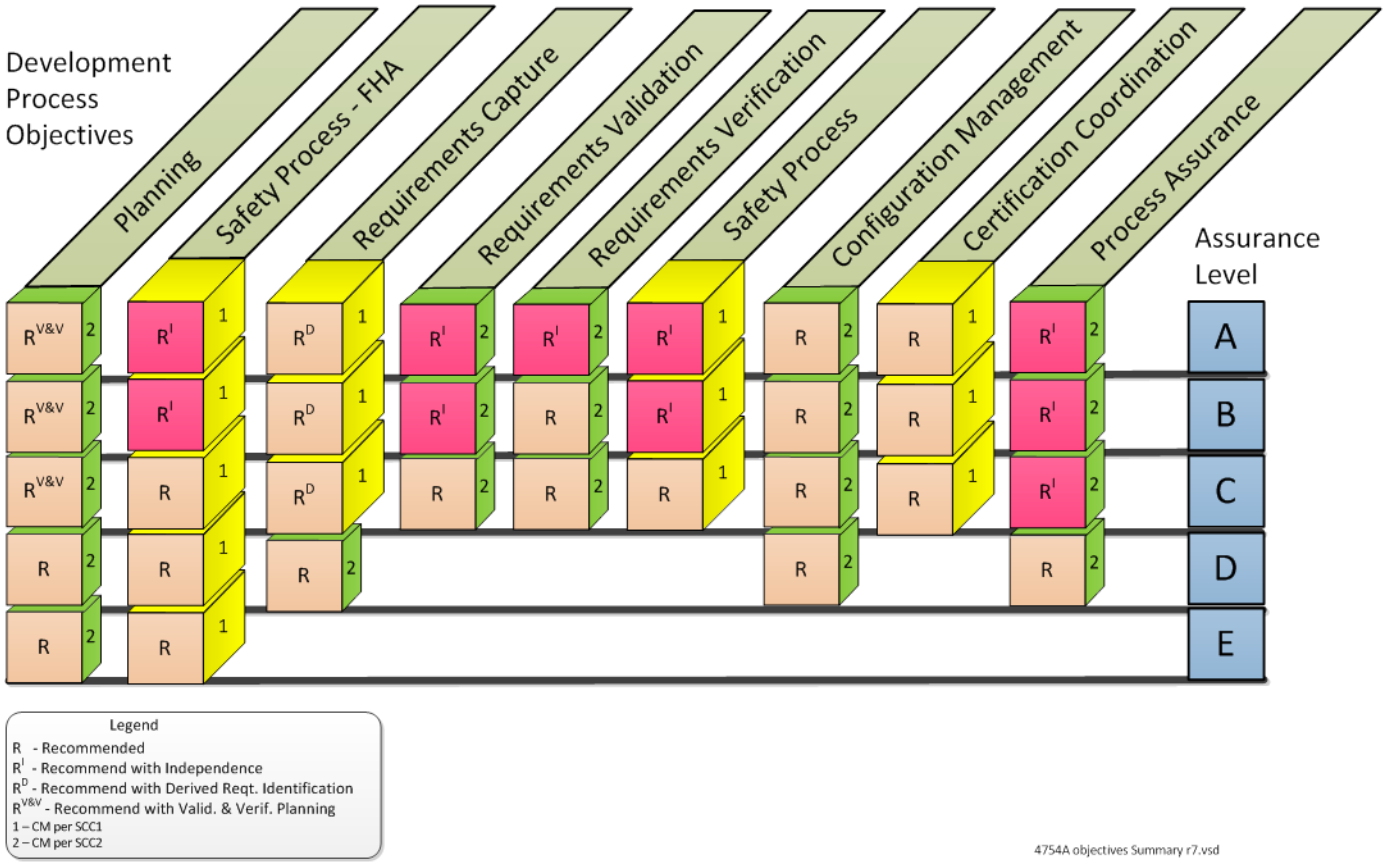


Figure 26 ARP4754A Objective Areas & CM Categories by Assurance Level

C 3.1 References

The documents listed in Table 34 were used in performing the life cycle process (LCP) comparison study presented in section C 4.

Table 34 Reference Document List

Document No.	Document Title
ARP4754A	Guidelines for Development of Civil Aircraft and Systems
DO-178B	Software Considerations in Airborne Systems and Equipment Certification
DO-178C	Software Considerations in Airborne Systems and Equipment Certification
DO-254	Design Assurance Guidance for Airborne Electronic Hardware
DO-297	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

C 3.2 Definitions

The definitions captured in Table 35 are noteworthy for the life cycle objective comparison activity.

Table 35 Noteworthy Comparison Definitions

Term	Definition
Guidance	Recommended procedure for complying with regulations.
Guideline	Supporting information that can be helpful but is not considered to be guidance.
Independence	The separation of responsibilities that assures the accomplishment of objectives evaluation (e.g. validation activities are not performed solely by the developer of a requirement for a system or Item (ARP4754A))

C 4 Life Cycle Objective Comparisons

This section presents the comparison of objectives identified in ARP4754A and the equivalent objectives identified in DO-178 and DO-254. Each sub-section provides analysis description highlights of the major commonalities, and the significant activity objective or configuration control category differences. The following process objective areas are compared:

- Planning,
- Development process (requirements capture, management),
- Validation process,
- Verification process,
- Configuration Management and,
- Process Assurance.

C 4.1 Planning Process Objectives Comparison

Figure 27 graphically summarizes the objectives and control categories for planning between ARP4754A and the DO LCPs. The Planning objectives are consistent across the processes for assurance levels A through D; with only differences of CM control categories depending upon the planning data. There are significant CM control differences highlighted between the software LCPs and ARP4754A.

Objective Commonality:

1. The Planning Objectives across the different life cycle domains are consistent, with each LCP recommending objectives at assurance levels A through D for:
    - Certification planning,
    - Development planning,
    - Verification planning,
    - Configuration management planning and,
    - Process assurance planning.

Figure 27 Planning Objectives Comparison Summary

Differences Summary:

Table 36 summarizes the noted differences between the ARP and DO processes.

Table 36 Planning Process Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Validation Plan	X		A-D D	DO178B/C DO254
Verification Plan	X		D	
Development Plan		X	A-B	DO178
Verification Plan		X	A-B	DO178
Configuration Management Plan		X	A-B	DO178/DO254
Process Assurance Plan		X	A-B	DO178

Objective Differences:

1. As highlighted in Table 36, the software LCP does not identify the need to accomplish a validation plan for any assurance level. And AC/Sys validation planning is "As Negotiated" for assurance level D without a corresponding objective in the DO life cycles.

Analysis: *A more detailed review of the software LCP finds that the corresponding objectives to those identified in AC/SYS LCP for validation planning can be found under the Verification Planning activities. So even though planning for a specific set of planning data is not called out, the objectives are to be accomplished. The "As Negotiated" identification for AC/SYS LCP versus no entries for the DO LCPs is not a real difference since accomplishment is as negotiated on all projects. The analysis conclusion is that the objectives for validation planning are consistent across the LCPs for assurance levels A-D.*

2. The AC/Sys LCP Verification Planning objectives are noted as "As Negotiated" for assurance level D while "Recommended" for the DO LCPs.

Analysis: *As a consequence of this difference, it is conceivable for the AC/SYS LCP assurance level D, verification planning objectives may need to be accomplished in order to have consistent development processes across a project containing all of LCPs.*

The AC/Sys LCP authors should consider revising ARP4754A Verification Planning to "Recommended" for assurance level D for process consistency.

Data CM Category Differences:

1. The CM control categories for assurance level A and B differ between the software LCPs and AC/SYS and hardware LCP. All of the software planning objectives are managed using CM category 1 while hardware and AC/Sys planning data is managed using CM category 2.

Analysis: *It is unclear why the software life cycle manages the planning activities for assurance levels A and B to the CM category 1 stringent criteria. The certification equivalent documents between the life cycles are managed consistently at CM category 1 and it is these data artifacts that are specifically used to plan the regulatory certification compliance criteria. CM category 1 increases the burden on industry without justification or benefit since the certification planning data artifacts would need to be revised commensurate with any subordinate plan revision.*

The software LCP authors should consider relaxing the software configuration management control category for development, verification, configuration management and quality assurance as the more rigorous activities are unnecessary for certification or for the mitigation of development errors.

C 4.2 Development Process Objectives Comparison

Figure 28 graphically summarizes the objectives and control categories for development process between ARP4754A and the DO LCPs. In general, the basic Development Process objectives are consistent across the processes for assurance levels A through C; with only minor differences of CM control categories. There are significant differences highlighted between the four LCPs at assurance level D for both the objective recommendations and CM category assignments.

Objective Commonality:

The Development Process Objectives across the different life cycle domains are consistent, with each LCP recommending objectives at assurance levels A through C for:

- Identifying and capturing requirements,
- Identifying system architectures and,
- Performing integration.

The Development Process objectives for identifying requirements and architectures are consistent with "Recommended" for development assurance levels A and B, with the data managed per CM category 1. There are objective differences identified at assurance levels C and D (see Objective Differences). There are also CM data control category differences identified at development assurance levels A and B for performing integration objectives (see CM Differences).

No Development Process Objectives are identified for development assurance level E across all four LCPs.

Differences Summary:

Table 37 summarizes the noted differences between the ARP and DO processes.

Figure 28 Development Process Objectives Comparison Summary

Table 37 Development Process Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Perform integrations		X	A-D	
Perform integrations	X		D	
Architecture defined		X	C	DO178C/DO254
System Reqts / LL Reqts defined		X	C	DO178B
Derived Reqts defined	X	X[1]	D	[1] Differs by HL/LL
Architecture defined	X	X	D	
Allocate Reqts to Items / LL Reqts	X[2]	X[3]	D	[2] DO178C /[3] DO254

Objective Differences:

1. As highlighted in Table 37, there are three objectives which are "Recommended" by the hardware/software LCPs but are "As Negotiated" for the AC/Sys LCP for the Level D assurance level. These "As Negotiated" objectives include:
    - Defining derived requirements,
    - Defining architecture, and
    - Performing system integrations.

Analysis: *As a consequence of this difference, it is conceivable that the system level "As Negotiated" objectives would be de-facto considered as "Recommended" in order to have consistency with the HW and SW LCPs on the same project.*

Data CM Category Differences:

1. The Development Process CM objectives for performing integration in AC/SYS LCP differ from the other LCPs for assurance levels A-D. AC/SYS system integration data is managed per CM category 2 while in the other LCPs, the data is managed per CM category 1.

Analysis: *As a consequence of this difference, it is conceivable for the AC/SYS LCP assurance levels A through D CM category may need to be escalated to use CM category 1 in order to have consistent development processes across a project containing all of LCPs.*

2. The CM category for development of system/software or hardware architecture data across the LCPs is inconsistent across assurance levels C and D. ARP4754A and DO-178B are category 2 for both levels while DO-254 maintains level 1 across all levels. DO-178C controls the SW architecture data, for assurance level C, at CM category 1 and at category 2 for level D.

Analysis: *It is unclear why the architecture data, which is identified to be captured in all life cycles by the Design Description, needs the category 1 level of CM management and attention for Levels C and D as prescribed in DO178C and DO254. This difference could be due to a nomenclature or an objectives mapping issue. The SW "Design Description" is actually a low level requirements document where the system level design description is as titled, a system description narrative.*

3. At assurance level C, the DO-178B objective to define low level requirements managed by CM category 2 was inconsistent with the ARP4754A and the other life cycle assignments of CM category 1. This difference is mitigated on forward projects using DO-178C.
4. The derived requirement output data CM management across the LCPs for level D is mixed. System derived requirements are maintained at category 2 while the DO LCPs maintain this data is maintained using CM category 1.

Analysis: *It is unclear why the software and hardware derived requirements data is so rigorously maintained for Level D. As a consequence of this difference, it is conceivable that AC/SYS LCP CM category may need to be escalated to use CM category 1 in order to have consistent development processes across a project containing all of LCPs.*

The LCP authors should establish consistency and revise the LCPs accordingly.

5. DO254 maintains all requirement data at assurance level D to CM category 1. ARP4754A and DO178B are consistent at CM category 2. DO178C maintains only HL requirement data to category 1.

Analysis: *Again, it is unclear why the requirements data is so rigorously maintained for Level D. As a consequence of this difference, it is conceivable that AC/SYS LCP CM category may need to be escalated to use CM category 1 in order to have consistent development processes across a project containing all of LCPs.*

The LCP authors should establish consistency and revise the LCPs accordingly.

C 4.3 Validation Process Objectives Comparison

Figure 29 graphically summarizes the objectives and control categories for validation of requirements between ARP4754A and the DO LCPs. In general, the basic Validation objectives are consistent across the processes for assurance levels A through C; with only minor differences at assurance level D. The caveat however, is that the AC/Sys LCP objective to validate and justify assumptions which has no equivalent objective in either of the software or hardware LCPs.

Objective Commonality:

Establishing the completeness and correctness of requirements is a consistent objective across all of the LCPs. Assurance levels A and B are consistent for AC/Sys and software LCP as “Recommending” this objective being satisfied with independence. Derived requirement validity and requirement traceability are also consistent at “Recommended” across all of the LCPs for assurance levels A and B.

Differences Summary:

Table 38 summarizes the noted differences between the ARP and DO processes.

Table 38 Validation Objectives Process Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Reqts complete & correct	X		A-B	Lack of independence in DO254
Reqts complete & correct	X		D	DO178/DO254
Assumptions	X		A-D	DO178/DO254
Derived reqts	X		A-B	Lack of independence in DO178/DO254
Derived reqts	X		C-D	DO178/DO254
Validation records	X		A-D	DO178/DO254

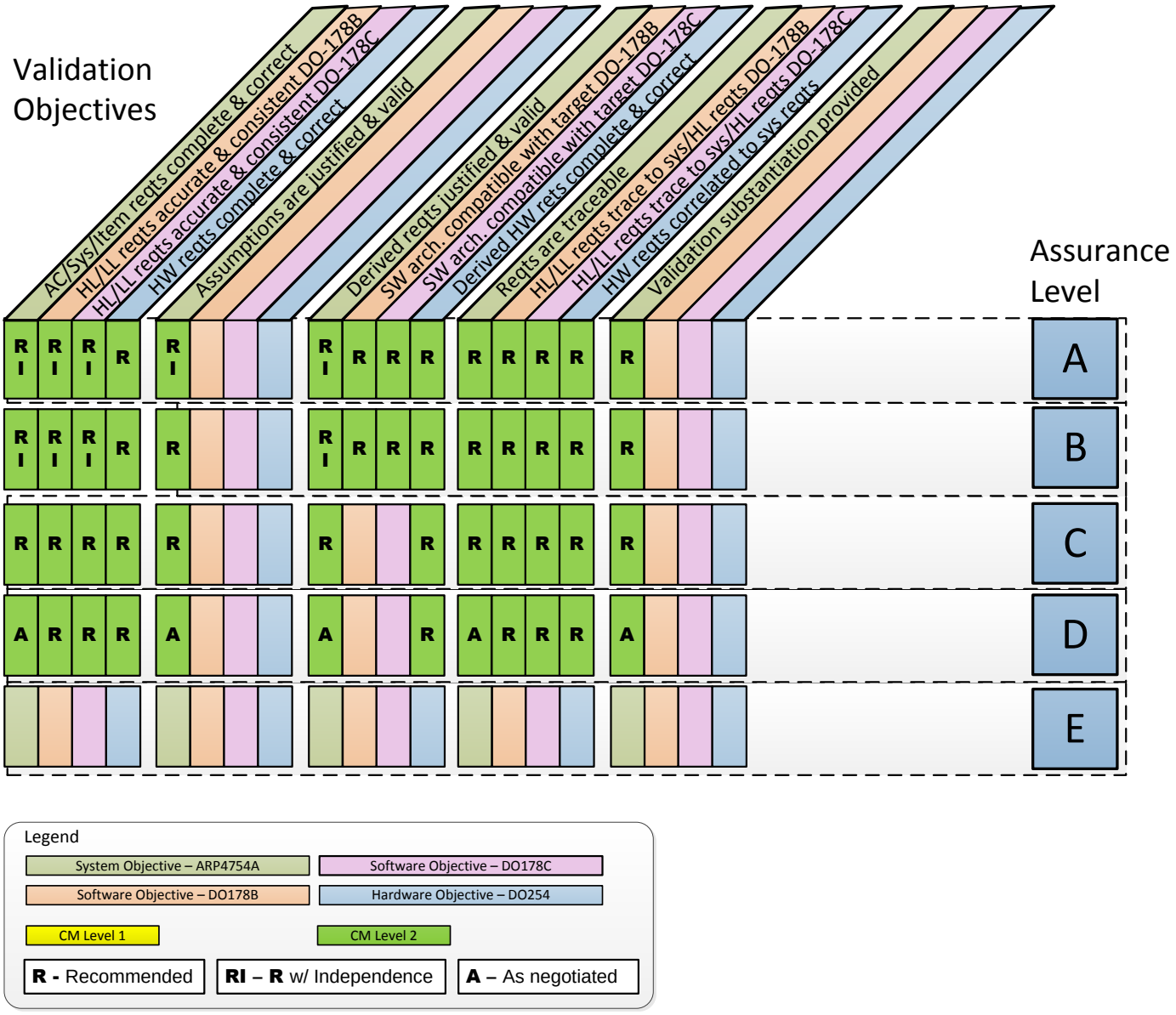


Figure 29 Validation Objectives Comparison Summary

Objective Differences:

1. The DO254 LCP "Recommends" ensuring hardware requirements are complete and correct but is inconsistent with the AC/Sys and software LCPS in not accomplishing the objective with independence for assurance levels A and B. The AC/Sys LCP also has "As Negotiated" for validation of requirements at assurance level D, while the DO LCPs maintain "Recommended".

Analysis: *It is unclear why the hardware requirements validation is not accomplished with independence similarly to AC/Sys and software LCPs. As a consequence of this difference, it is conceivable that hardware validation activities would be adapted to implement independence in order to have consistent development processes across a project containing all of LCPs.*

Similarly, if the HW and SW LCPs recommend validation of requirements for assurance level D, the AC/SYS LCP would need to be negotiated to "Recommended" to maintain project consistency.

The AC/Sys and hardware LCP authors should establish consistency and revise the LCPs accordingly.

2. Validation of assumptions has no equivalent objective identified in the DO LCPs.

Analysis: *This seems to be a set of "missing" (or at least not highlighted in the guidance material) objectives from the DO life cycle processes regarding assumptions. Many assumptions are made at these lower levels of development which may experience the same benefits experienced at the aircraft and system levels had the validity been tracked and/or validated prior project completion.*

The DO LCP authors should consider adding objective or highlighting validating assumptions made during hardware and software development and revise the LCPs accordingly.

3. Derived requirement objectives vary across the LCP with different accomplishment criteria or by not having any objectives. For assurance levels A and B, all of the LCPs "Recommend" accomplishing validating captured requirements. The AC/Sys LCP recommends accomplishing this object with independence whereas the DO LCPs do not. Additionally, the recommendation disappears for validation of software requirements for assurance levels C and D.

Analysis: *It is unclear why some categories of derived software requirements are not validated with independence. It is also unclear as to why the software LCP varies the objectives within the domain based on high and low level requirement definitions.*

The software LCP authors should identify the rationale that validates high software requirements with independence yet validates the traced children low level requirements without independence.

4. Validation records generation has no equivalent objective identified in the DO LCPs.

Analysis: *This result is probably due to the comparison strategy used in this analysis. The hardware and software DO LCPs contain the generation of validation data, as noted by the common satisfaction of establishing requirement completeness and correctness. The DO LCPs do not call this out as a separate or unique completion objective.*

Data CM Category Differences:

There were no configuration management category differences identified for validation objectives between the ARP and DO LCPs.

C 4.4 Verification Process Objectives Comparison

Figure 30 graphically summarizes the objectives and control categories for verification of requirements between ARP4754A and the DO LCPs. In general, the basic Verification objectives are consistent across the processes for assurance levels A through D; with only minor differences at assurance level D.

Objective Commonality:

The verification of requirements is a consistent objective across all of the LCPs. Each of the life cycles has assurance level A thru C objectives "Recommended" for:

- Ensuring verification test procedures are correct,
- Verifying intended function,
- Verifying implementation meets requirements, and
- Safety requirements are verified.

Differences Summary:

Table 39 summarizes the noted differences between the ARP and DO processes.

Table 39 Verification Objectives Process Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Test Procedures Correct	X		B	With independence for DO254
Test Procedures Correct	X		D	DO178/DO254
Verify intended function	X		B	With independence for DO178
Safety requirements	X	X	A-C	DO178/DO254
Verification evidence	X			DO178/DO254
Safety impact identified	X			DO178/DO254

Objective Differences:

1. The DO254 LCP "Recommends" ensuring hardware test procedures are correct at assurance Level B with independence which is inconsistent with the AC/Sys and software LCPs recommendations. The hardware also "Recommends" test procedure correctness at assurance level D where the software LCP has no similar objective and the AC/Sys LCP has "As Negotiated".

Analysis: *It is unclear why the hardware test procedure verification is accomplished with independence at assurance level B. As a consequence of this difference, it is conceivable that AC/System process activities may need to be adapted to implement independence in order to have consistent development processes across a project containing both LCPs.*

The hardware LCP authors should establish consistency with the AC/System and software LCPs.

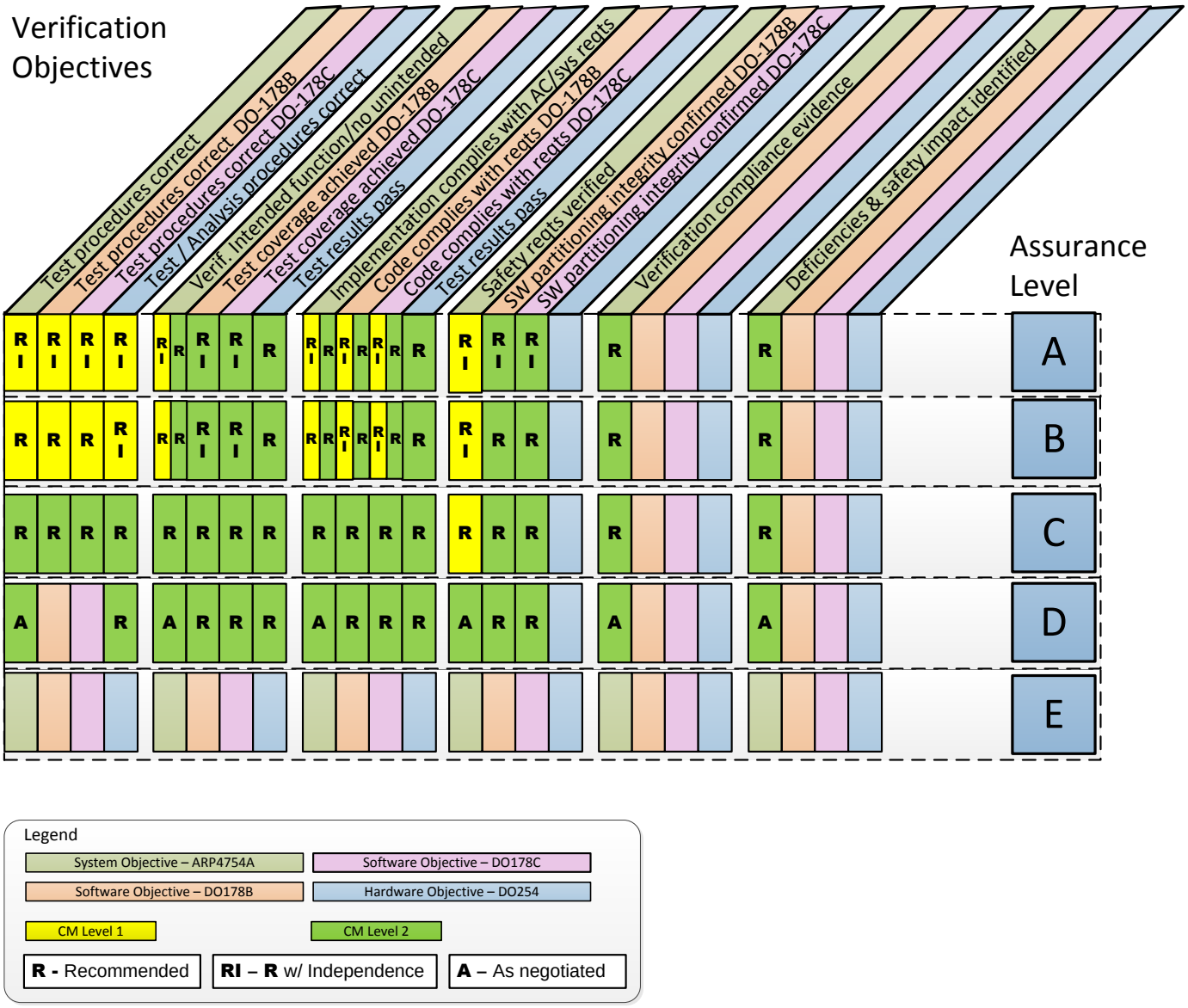


Figure 30 Verification Objectives Comparison Summary

2. The Verify intended function and Verify implementation software objectives have accomplishment with independence for the software LCP in difference to the AC/Sys and HW LCPs.

Analysis: *It is unclear why the software verification is accomplished with independence at assurance level B inconsistently with the other LCPs. As a consequence of this difference, it is conceivable that AC/System and HW process activities may need to be adapted to implement independence in order to have consistent development processes across a project containing all LCPs.*

The software LCP authors should establish consistency with the AC/System and hardware LCPs.

3. Specific safety requirement verification is “Recommended with Independence” at the AC/Sys LCP assurance levels A and B only software LCP assurance level A having a similar objective.

Analysis: *It is unclear why the hardware LCP does not have a specific objective to ensure safety requirement verification. It is also unclear why the software LCP does not maintain the verification with independence to assurance level B.*

Since safety is predominately an aircraft and/or system activity, it is conceivable that the authors of the hardware and software LCPs had a more narrow definition of “safety requirements” than that of the ARP authors. The discrepancy may also be attributed to the comparison strategy used in this analysis. The hardware LCP contains the generation of verification data but does not call the objective out as a separate or unique completion objective.

Further detailed comparison analysis should be completed so that LCP authors can establish consistency in objective completion.

4. The AC/Sys life cycle has two objectives identified where there is no comparative hardware or software LCP objective

Analysis: *A more detailed comparison analysis would undoubtedly find that these two objectives are inherent in the activities of the HW and SW LCPs though they are not highlighted in the summary matrices in each process.*

Further detailed comparison analysis should be completed so that LCP authors can establish consistency in objective completion.

Data CM Category Differences:

1. Safety requirement verification is maintained using CM category 1 in the AC/Sys LCP for assurance levels A thru C which differs from the software LCP at CM category 2 at those levels (the HW LCP has no safety verification objectives).

Analysis: *Since safety is predominately an aircraft and/or system activity, it is conceivable that the authors of the hardware and software LCPs envisioned that CM of true “safety” data would be accomplished in the AC/Sys life cycle. The “safety data” created by the subordinate HW and SW life cycles would be effectively managed for certification purposes at the higher levels.*

Further detailed comparison analysis should be considered so that LCP authors can establish consistency across the LCPs in objective completion.

C 4.5 Configuration Management Process Objectives Comparison

Figure 31 graphically summarizes the objectives and control categories for configuration management processes between ARP4754A and the DO LCPs. The basic configuration management objectives are consistent across the processes for assurance levels A through D; with only minor differences with the software LCP due to non-equivalent objectives.

Objective Commonality:

All of the development process documents have consistent “Recommended” CM objectives for:

- Defining configuration items,
- Establishing baselines and derivatives,
- Establishing change control,
- Establishing archive and control capabilities.

Differences Summary:

Table 40 summarizes the noted differences between the ARP and DO processes.

Table 40 CM Process Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Baselines & derivatives	X		D	
Baselines & derivatives		X	C,D	

Objective Differences:

1. The AC/Sys objective to establish configurations and baselines is "As Negotiated" for assurance level D which differs from the HW and SW LCP which have this objective as "Recommended".

Analysis: *It is unclear why the HW and SW LCPs find it a necessary objective to maintain control of implementations with such a minor impact on aircraft safety. As a consequence of this difference, it is conceivable that the system level "As Negotiated" objectives would be de-facto considered as "Recommended" in order to have consistency with the HW and SW LCPs on the same project.*

The software and hardware LCP authors should explore the rationale for the present recommendation to establish baselines at assurance level D when the AC/System LCP indicates there isn't a need.

Data CM Category Differences:

1. The configuration and baseline data is maintained using control category 1 in the HW and SW LCPs for assurance levels C and D but at category 2 for the AC/Sys LCP.

Analysis: *It is unclear why the HW and SW LCPs find it a necessary to maintain such stringent control of implementations with such a minor impact on aircraft safety. As a consequence of this difference, it is conceivable that the system level would be de-facto considered as category 1 in order to have consistency with the HW and SW LCPs on the same project.*

The software and hardware LCP authors should explore the rationale for the present control category assignment when the AC/System LCP indicates there isn't a need. The software and hardware LCP authors establish consistency with the AC/System LCP.

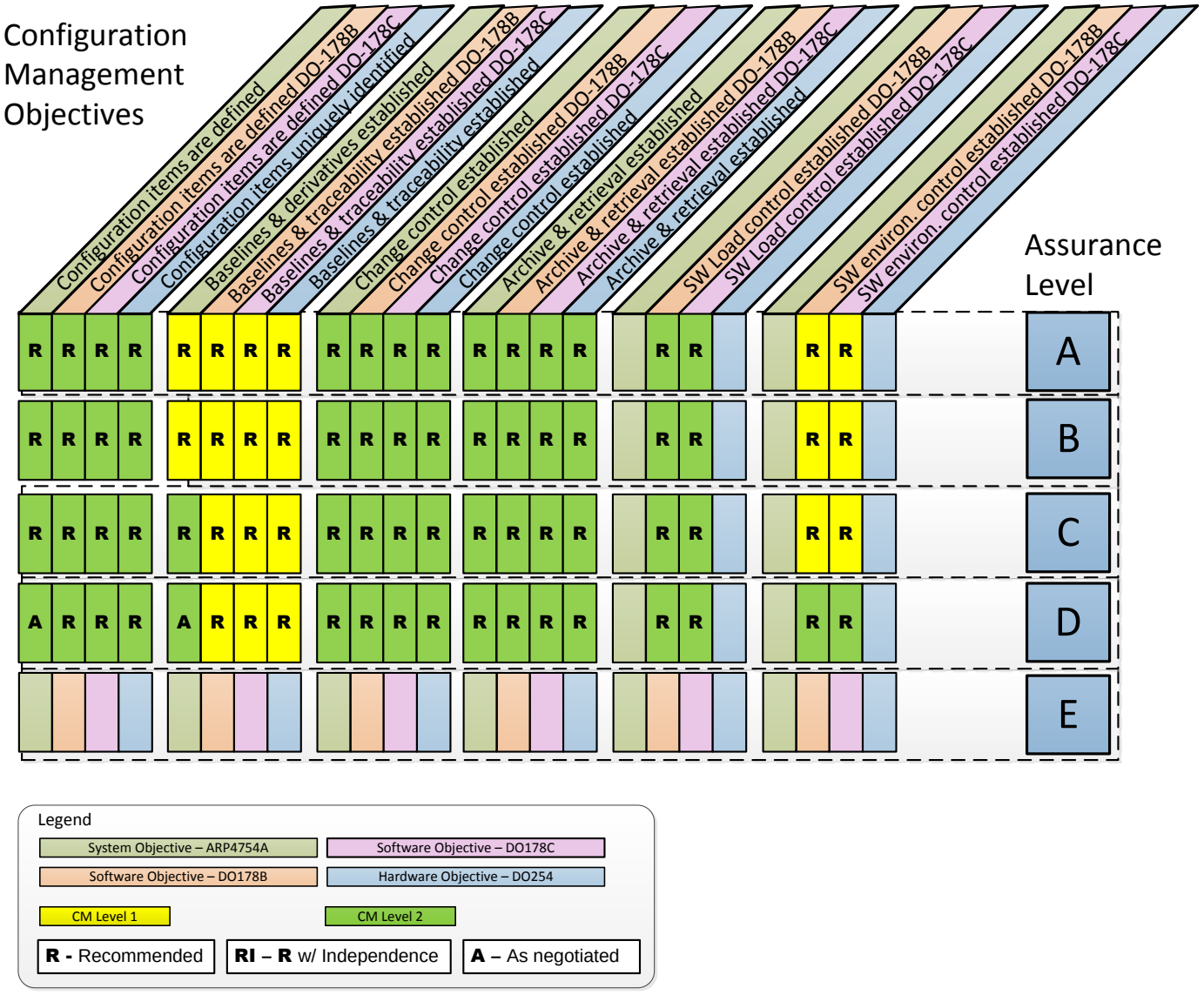


Figure 31 Configuration Management Objectives Comparison Summary

C 4.6 Process Assurance Objectives Comparison

Figure 32 graphically summarizes the objectives and control categories for process assurance between ARP4754A and the DO LCPs. The Process Assurance objectives are consistent across the processes for assurance levels A through C; with minor differences at assurance level D.

Objective Commonality:

All of the development process documents have consistent “Recommended” PA objectives for:

- Evaluating process activities and processes in accordance with developed plans.

Differences Summary:

Table 41 summarizes the noted differences between the ARP and DO processes.

Table 41 Process Assurance Differences

Objective	Accomplish	CM Category	Assurance Level	Comment
Plans developed & maintained	X		A-D	DO178/DO254
Data complies with plans	X		A-C	DO178/DO254
Implementation conforms to data	X		A-D	DO178/DO254

Objective Differences:

1. The AC/Sys LCP directly identifies creating and maintaining the development plan data while the DO LCPs do have an equivalent objective.

Analysis: *In this case, it is obvious that the DO LCPs contain this objective since the remainder of the process assurance activities are based on evaluating compliance to these plans. So even though there appears to be a gap in objectives, it is predominately a depth of comparison analysis study issue.*

It would be advantageous though for the software and hardware LCP authors to explore adding an equivalent objective to enhance process consistency.

2. There are differences in evaluating the process activities for assurance level D. The software LCP maintains a "Recommended with Independence" for assurance levels A thru D while the AC/Sys LCP identifies only "Recommended" and DO254 has no equivalent objective.

Analysis: *It is unclear why the SW LCP recommends the additional burden of activity monitoring with independence for functions which have such a limited impact on product safety.*

The software and hardware LCP authors should explore the rationale for the present recommendations or lack thereof at assurance level D when the AC/System LCP indicates there isn't a safety need.

3. The hardware and software LCPs contain objectives evaluating the implementation against program standards and specific project documentation. There is not an equivalent AC/Sys LCP objective.

Analysis: *This is an acceptable difference. The DO LCPs define the items that are used to implement systems and aircraft. It is reasonable therefore to have a process objective to establish that the actual implementation matches its documentation, since that documentation will be used at each successive level to establish compliance.*

Data CM Category Differences:

There were no configuration management category differences identified for the process assurance objectives between the ARP and DO LCPs.

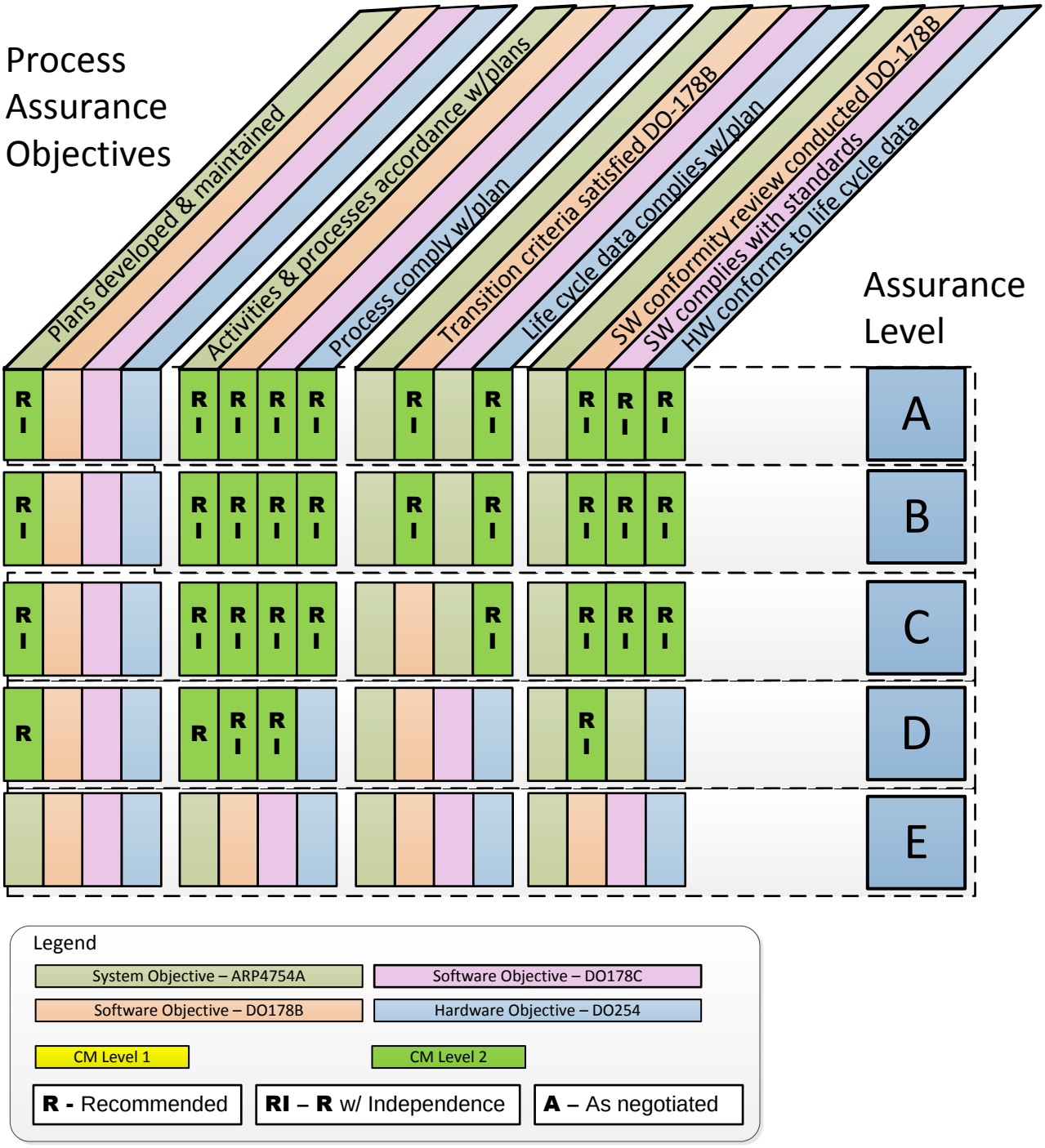


Figure 32 Process Assurance Objectives Comparison Summary

C 5 ARP4754A to DO-297 Objectives Comparison

This section summarizes a comparison of the objectives and control categories between ARP4754A and DO297. DO-297 does not vary satisfaction of objectives or CM control category by assurance level within its guidance. All objectives identified are "Recommended" for accomplishment at the assigned configuration control category due to the Integrated Modular Avionic (IMA) system construction.

There is no Development Assurance Level specified under DO-297; therefore, the comparison will focus on ARP4754A assignment level A for objective coverage and CM category.

Objective Commonality:

1. The Development Process Objectives for identifying requirements and architectures are consistent per CM category 1 between ARP4754A and DO297. There are differences identified at A/C level objectives (see Objective Differences 2 & 3).
2. The Validation Objectives for V&V data are consistent to be CM category 2 between ARP4754A and DO297. There are differences in terms of having objectives (see Objective Differences 4).
3. The Verification Objectives for V&V data are consistent between ARP4754A and DO297 with minor considerations (see Objective Differences 5).
4. In general, CM objectives and control categories are consistent between ARP4754A and DO297. The CM objectives are always control categories 2 unless related to baseline (configuration) or environment (platform).
5. In general, Process Assurance objectives are consistent between ARP4754A and DO297 and managed under control category 2 with single exception (see Objective Differences 6).

Objective Differences

The ARP4754A objectives differ from DO297 objectives in a few notable areas.

1. Certification Plan objectives for ARP4754A and all the Planning Objectives for DO297 are maintained under CM category 1 while the remaining Planning objectives for ARP4754A are maintained under CM category 2.

Analysis 1: As a result of this discrepancy, it is conceivable that DO297 Planning Objectives may need to align with ARP4754A objectives to have all the objectives to be maintained under CM category 2 except for Certification Plan.

2. The ARP4754A Development Process Objectives of A/C & system integration is maintained under CM category 2 while in DO297, most of the objectives of A/C & system integration data managed per CM category 1. DO297 also have platform integration and V&V results data controlled at CM category 2.

Analysis 2: As a result of this discrepancy, it is conceivable that ARP4754 Integration Objectives may need to align with DO297 objectives to have most of the objectives to be maintained under CM category 2 except for platform integration and V&V results.

3. Based on Objective tables under DO297, it is unclear if the Development Process Objectives of identifying A/C requirements and allocating A/C functions to systems are covered or not. The A/C function allocation objectives are actually mixed with system function allocation objectives under DO297 section 3.2, but DO297 A/C requirements identification equivalent objectives is not identified.

Analysis 3: As a result of this discrepancy, it is conceivable that DO297 objectives of A/C function allocation and identification may need to be independent from system objectives in Chapter 3.

4. The ARP4754A contains two additional Validation Objectives, justifying assumptions and providing validation substantiation which do not have DO297 equivalent objectives.

Analysis 4: After the analysis under DO297, it is conceivable that DO297 objectives justifying assumptions and providing validation substantiation may have already been covered as the of V&V record. However, the V&V record of the two objectives are only listed in Section 4.7.6.2 for reuse of module and application. It is recommended for DO297 to have the same objectives under the other V&V sections.

5. It is not always clear to compare Verification Objectives between ARP4754A and DO297 while DO297 is mixing Validation and Verification under objectives. In ARP4754A, the Verification Objectives are controlled by CM category 2 unless related to procedure or safety, where in DO297, V&V Objectives are managed per CM category 2 unless related to planning or safety analysis.

Analysis 5: This discrepancy is resulted as different terminology in each guideline document. The overall objectives are still consistent if the terminologies are considered to be equivalent. It is suggested to have DO297 distinguish the objectives of Validation and Verification independently.

6. The ARP4754A and DO297 Process Assurance Objectives for developing and maintaining plans, differ in terms of control category of the data. ARP4754A data is managed per CM category 2 and in DO297 the data is managed per CM category 1.

Analysis 6: As a result of this discrepancy, it is conceivable that DO297 objectives of developing and maintaining plans may reconsider to be controlled by CM category 2 to align with ARP4754 objectives.

Appendix D Additional Study Areas

D 1 Introduction

This appendix summarizes various additional ARP4754A study results for questions identified during the project kick-off meeting. The following topic objectives are included:

- Development Assignment levels in AC23.1309.1E vs ARP4754A (AC 20-174), Differences – Why? Are the levels assigned equivalent?,
- Insight as to why Options 1 / 2 of ARP4754A Table 3 are equivalent,

D 2 ARP4754A & AC23.1309-1E

Figure 33 captures a synopsis of the functional and item development assurance level assignments afforded by ARP4754A in support of Part 25 and the equivalent development assurance level assignments allowed by the guidance in AC23.1309-1E.

As summarized in Figure 33, AC23.1309 does not advocate applying development assurance activities at the airplane or system function level (FDALs) for any of the Class I-IV airplane types. It is apparent that the Authors of the AC are primarily interested in mitigating errors within the software and airborne electronic hardware domains. Information as to why this emphasis was implemented was not publicly available.

Within the assignment levels for the hardware and software domains (IDALs), the AC23 assignments are consistently more rigorous than those that would be allowed for Part 25. This revelation means that the airborne electronic hardware and software developed to support Normal and Utility Category aircraft may be more rigorous than that developed for Commercial Category. Therefore it is safe to extrapolate that the development assurance levels are not based on safety concepts and may be higher to compensate for the fact that there isn't any rigor associated with the system development.

Key Attributes	Aircraft - System Function					Software (Item)			Electronic Hardware (Item)		
	Qualitative				Quantitative	Qualitative		Quantitative	Qualitative		Quantitative
	FC Classification	Development Process W/O Independence	Development Process With Independence	Airplane Class	Probability Criteria	Development Process W/O Independence	Development Process With Independence	Probability Criteria	Development Process W/O Independence	Development Process With Independence	Probability Criteria
§ Part 25 (per AC20-174/ ARP4754A)	Catastrophic	A	AC or BB	NA	≤10-9	A	AC or BB	NA	A	AC or BB	≤10-9
	Hazardous	B	BC or CC		≤10-7	B	BC or CC	NA	B	BC or CC	≤10-7
	Major	C	CC, CD, CE or DD		≤10-5	C	CC, CD, CE or DD	NA	C	CC, CD, CE or DD	≤10-5
	Minor	D	DD or DE		≤10-3	D	DD or DE	NA	D	DD or DE	≤10-3
	No Effect	E	E		NA	E	E	NA	E	E	NA
§ Part 23 (per AC23.1309-1E)	Catastrophic	None Required		IV	≤10-9	AB		NA	AB		≤10-9
				III	≤10-8	BC		NA	BC		≤10-8
				II	≤10-7	CC		NA	CC		≤10-7
				I	≤10-6	CC		NA	CC		≤10-6
	Hazardous			IV	≤10-7	BC		NA	BC		≤10-7
				III	≤10-7	CC		NA	CC		≤10-7
				II	≤10-6	CC		NA	CC		≤10-6
				I	≤10-5	CD		NA	CD		≤10-5
	Major			IV	≤10-5	CD		NA	CD		≤10-5
				III	≤10-5	CD		NA	CD		≤10-5
				II	≤10-5	CD		NA	CD		≤10-5
				I	≤10-4	CD		NA	CD		≤10-4
	Minor			IV	≤10-3	D		NA	D		≤10-3
				III	≤10-3	D		NA	D		≤10-3
				II	≤10-3	D		NA	D		≤10-3
				I	≤10-3	D		NA	D		≤10-3
	No Effect			NA	NA	NA		NA	NA		NA

Figure 33 Part 23-25 Development Assurance Assignment Comparison

D 3 ARP4754A Option 1/2 Equivalence

ARP4754A establishes that, should independence in the functional failure set be established, the functional or item development assurance level assignment may be accomplished using either of two options, 1 or 2. How do the two options compare?

Fault tree representations of functional failure sets (FFS) supporting catastrophic, hazardous and major failure conditions, respectively, were created to evaluate the options. Each representative graphic summarizes the assurance objectives for a functional failure set, having a single member (i.e. no independence development attributes satisfied) as the leftmost branch and then the option 1 or option 2 assurance assignment options with their objective attributes, left to right respectively. Note that for Option 1 or 2, the minimum allowable assignment pair from ARP4754A Table 3 is considered.

D 3.1 Catastrophic Failure Condition FFS

Figure 34 presents the FFS fault tree for a catastrophic failure condition. A review of Figure 34 shows that satisfying the ARP4754A Level A objectives establishes sufficient rigor of process results to support the catastrophic Failure Condition.

Option 1: Option 1 provides for assurance assignments of Level A in combination with Level B or C to support the catastrophic Failure Condition. Since a Level A process alone is sufficient to satisfy the development process objectives, the addition of an independent error migration path at either level B or C provides additional error mitigation properties. It is noted that even though the additional independent element may be accomplished as low as level C, the only significant deviation in objectives from level A is the requirements management activities are not accomplished with in-line independence. This is certainly acceptable since any error is mitigated by the Level A development path.

Option 2: Option 2 provides for two independent level B assurance assignments to support the catastrophic FC. When the objectives of Level B are compared to those of Level A, the only difference is the lack of in-line requirement verification in each independent Level B process. In this case, the independence is achieved by having two independent level B processes accomplishing independent and different requirement verifications.

It is important to remember that Function F1 and F2 must have functional or Item development independence attributes satisfied in order to consider Option 1 or 2. The establishment of these attributes by a safety analysis assures minimization of common mode errors in the development process.

From a practical standpoint, these independence attributes mean that Function F1 and F2 have an acceptable level of differences in their requirement sets and development processes such that the independence attribute is true. A comparison of the single member FFS with Option 2 at this lower level may look like Figure 35. For the Single Member FFS on the left, we see that we have independent in-line requirements validation and independent in-line requirement verification to satisfy the objectives of the ARP and mitigate errors. In the Option 2 case (on the right of Figure 35) we have two independent requirement sets and development processes. Each process still has an independent in-line validation activity with non-independent (but different between F1 and F2) verification activity.

The independent in-line validation of two different requirement sets as well as the verification of two different requirement sets, using the equivalent configuration management and process assurance rigor, assures that the equivalent level of common mode error mitigation as the single member FFS case is achieved.

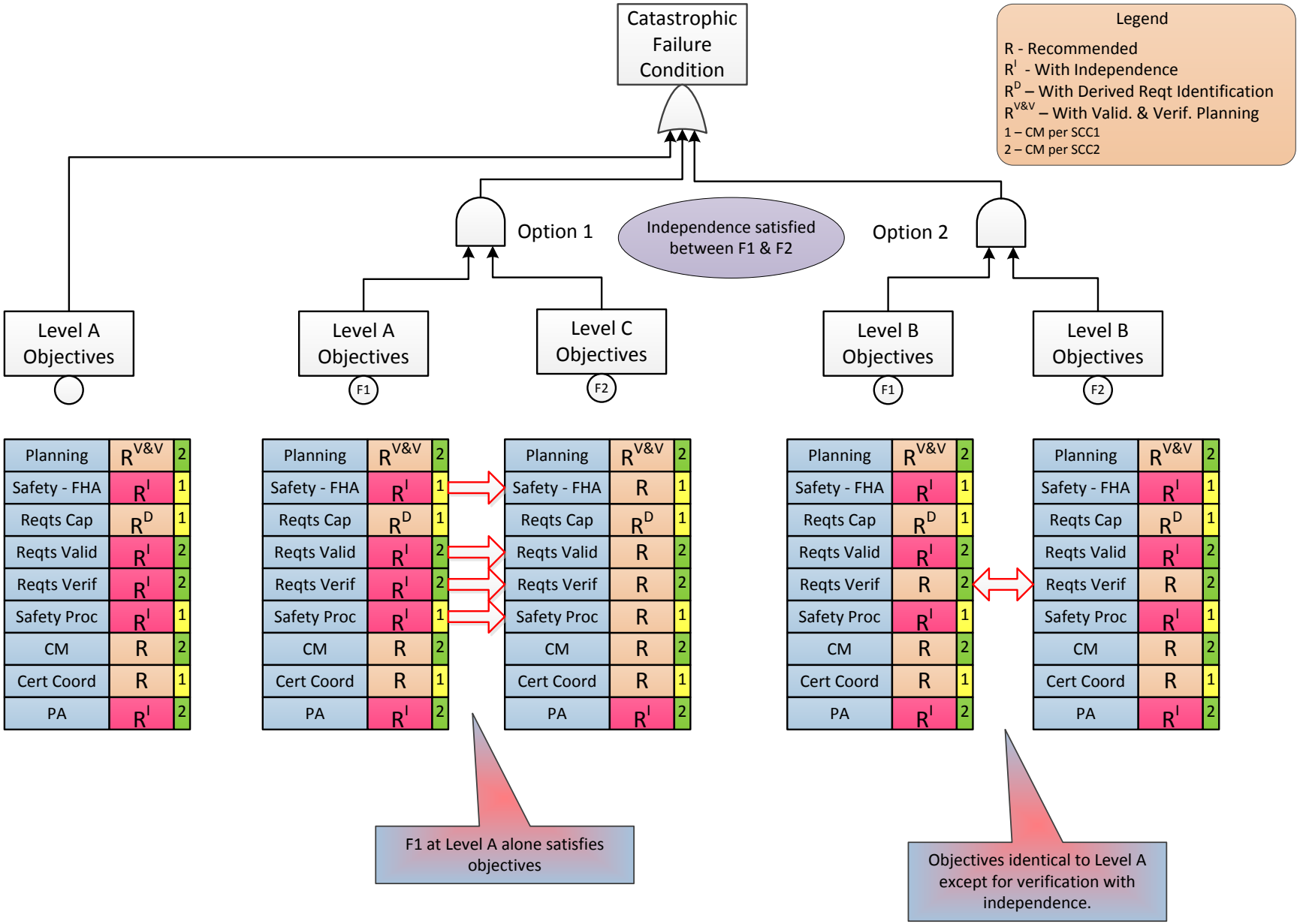
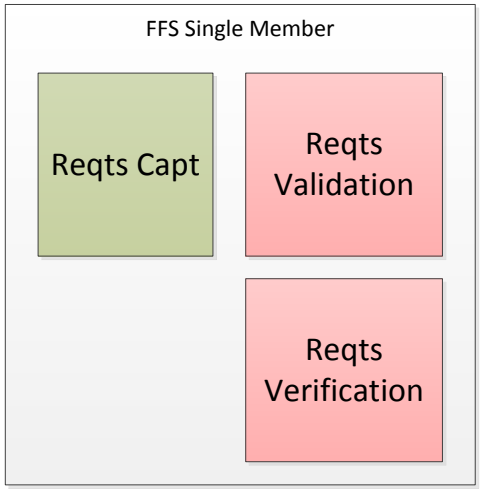
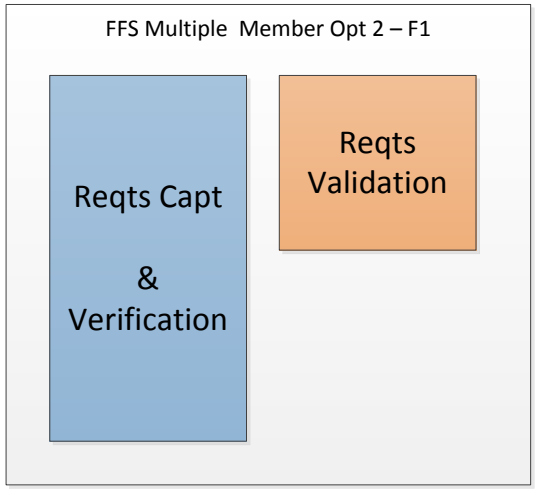
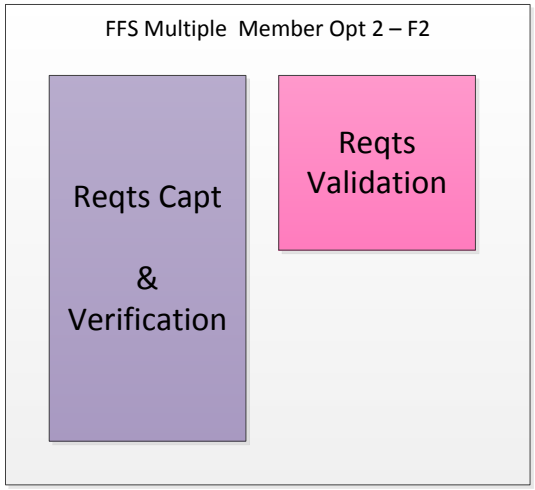


Figure 34 Option 1-2 Comparison for Catastrophic FC







Requirement/development errors mitigated through:

1. independent of validation &
2. independent verification
3. configuration & process rigor

Requirement/development errors mitigated through:

1. different requirement sets &
2. independent validation of different requirement sets &
3. independent verification of each different requirement set
4. configuration & process rigor

Figure 35 Option 2 Error Mitigation Equivalence to Single Member

D 3.2 Hazardous Failure Condition FFS

Figure 36 presents the FTA showing the single and multiple member FFS that may be used to satisfy a hazardous Failure Condition.

The single member FFS objectives that support a Level B assignment are summarized under the leftmost branch.

Option 1: Option 1 provides a single level B in combination with additional members at any level but not lower than Level D (objectives shown). In this option, there is significant difference between the Level B and Level D processes but the single level B alone would be sufficient to address the safety needed for the hazardous failure condition. The addition of the independent development process supporting the same functional failure set provides a measure of error mitigation properties since both the level B and level D must contain the same error to result in the failure condition.

Option 2: Option 2 establishes two independent level C processes to support the hazardous FC. In this case, the small difference from the single Level B process is the lack of independence in-line for safety and requirement validation of Level C process. In this case, the independence is achieved by having two independent level C processes accomplishing independent and different safety and requirement verifications. The independent Level C processes are therefore equivalent to the single Level B process.

D 3.3 Major Failure Condition FFS

Figure 37 presents the FTA showing the single and multiple member FFS that may be used to satisfy a major Failure Condition.

The characteristics and analysis presented for the catastrophic and hazard failure conditions also apply to major.

The single level C process, or a level C process in combination with any other assurance level (option 1) or two level D processes provide equivalent error mitigation.

D 3.4 Equivalence Analysis Summary

As discussed and visually compared herein, both of the ARP4754A Table 3 options provide equivalent error mitigation capabilities through almost identical objectives. Option 1 provides an unquantifiable level of development rigor “goodness” over the single member FFS by having an independent development path. Option 2 lacks in-line independence assurance objective characteristics but still accomplishes the overall error mitigation goals through the multiple (independent) member FFS paths.

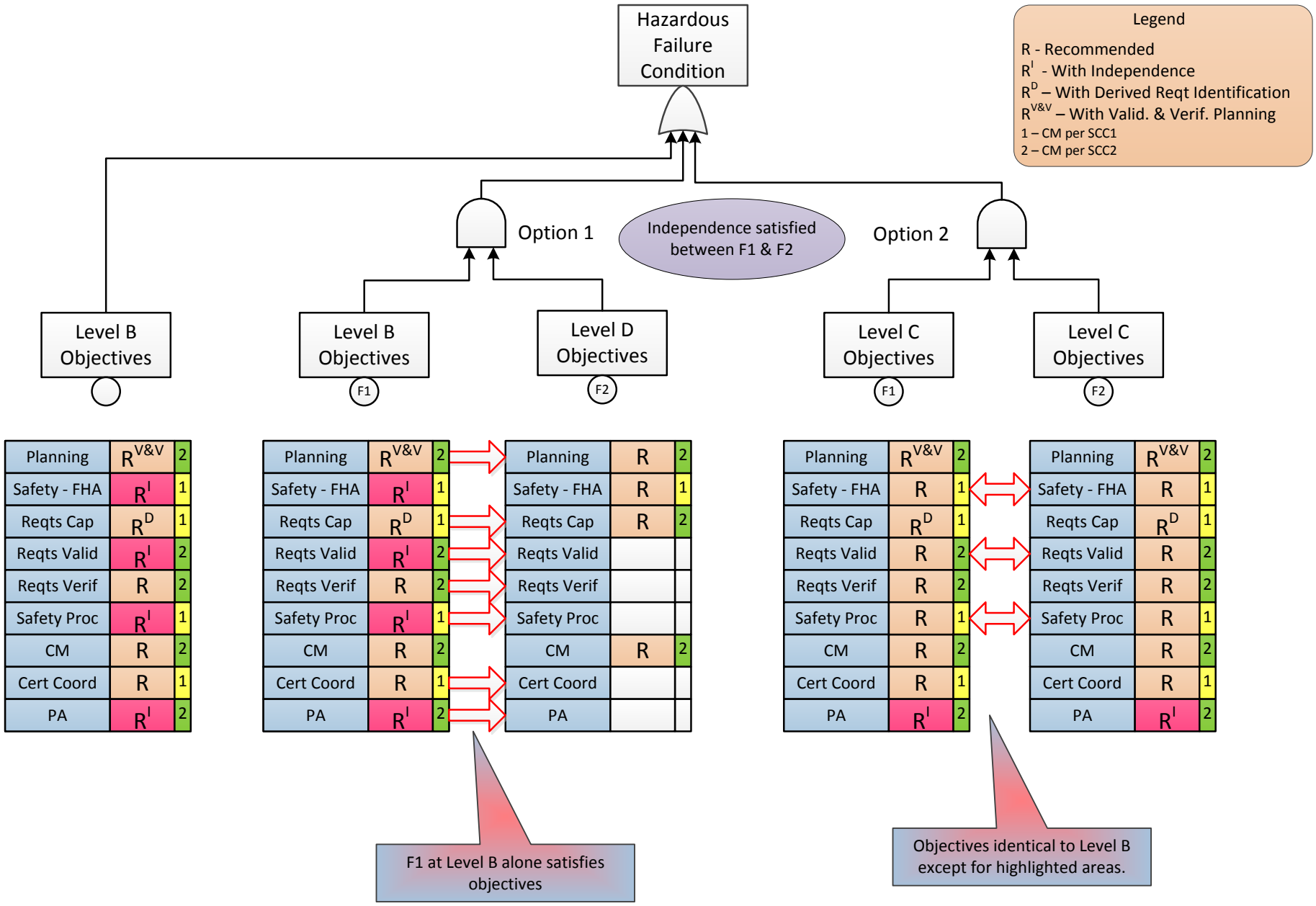

Hazardous Failure Condition
Legend
R - Recommended
R^I - With Independence
R^D – With Derived Reqt Identification
R^V&V – With Valid. & Verif. Planning
1 – CM per SCC1
2 – CM per SCC2
Option 1
Independence satisfied between F1 & F2
Option 2
Level B Objectives
Level B Objectives
F1
Level D Objectives
F2
Level C Objectives
F1
Level C Objectives
F2
Planning R^V&V 2
Safety - FHA R^I 1
Reqts Cap R^D 1
Reqts Valid R^I 2
Reqts Verif R 2
Safety Proc R^I 1
CM R 2
Cert Coord R 1
PA R^I 2
Planning R 2
Safety - FHA R 1
Reqts Cap R 2
CM R 2
F1 at Level B alone satisfies objectives
Objectives identical to Level B except for highlighted areas.

Figure 36 Option 1-2 Comparison for Hazardous FC

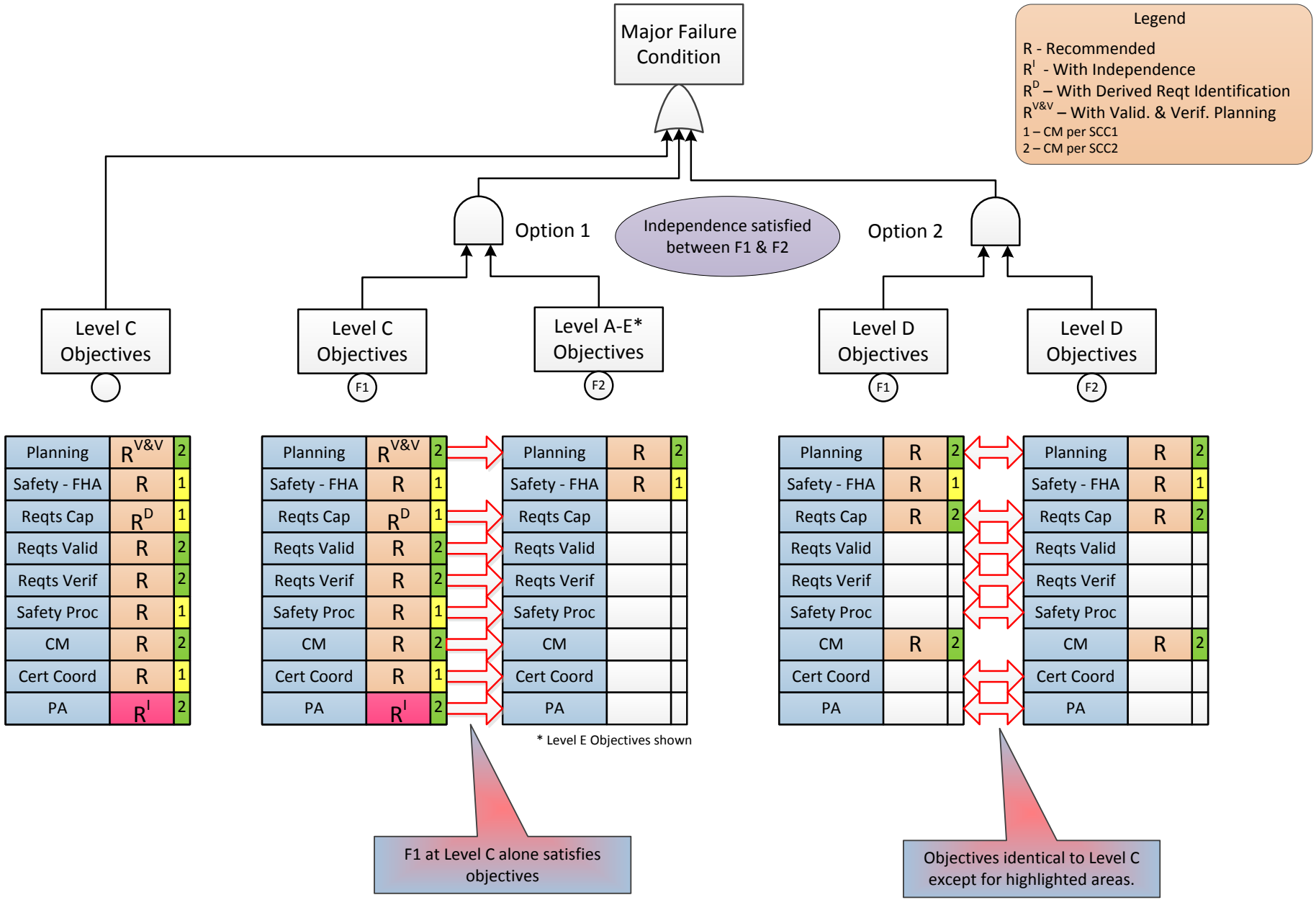

Major Failure Condition
Legend
R - Recommended
R^I - With Independence
R^D – With Derived Reqt Identification
R^V&V – With Valid. & Verif. Planning
1 – CM per SCC1
2 – CM per SCC2
Option 1
Independence satisfied between F1 & F2
Option 2
Level C Objectives
Level C Objectives
F1
Level A-E* Objectives
F2
Level D Objectives
F1
Level D Objectives
F2
Planning R^V&V 2
Safety - FHA R 1
Reqts Cap R^D 1
Reqts Valid R 2
Reqts Verif R 2
Safety Proc R 1
CM R 2
Cert Coord R 1
PA R^I 2
Planning R 2
Safety - FHA R 1
Reqts Cap
Reqts Valid
Reqts Verif
Safety Proc
CM
Cert Coord
PA
* Level E Objectives shown
Planning R 2
Safety - FHA R 1
Reqts Cap R 2
Reqts Valid
Reqts Verif
Safety Proc
CM R 2
Cert Coord
PA
F1 at Level C alone satisfies objectives
Objectives identical to Level C except for highlighted areas.

Figure 37 Option 1-2 Comparison for Major FC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 11 - 2015	Contractor Report	

4. TITLE AND SUBTITLE

Application of SAE ARP4754A to Flight Critical Systems

5a. CONTRACT NUMBER

NNL13AA04B

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Peterson, Eric M.

5d. PROJECT NUMBER

5e. TASK NUMBER

NNL14AB74T

5f. WORK UNIT NUMBER

999182.02.50.07.02

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, Virginia 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA/CR-2015-218982

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified
Subject Category 62
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES

Phase II Final Report

Langley Technical Monitor: Wilfredo Torres-Pomales

14. ABSTRACT

This report documents applications of ARP4754A to the development of modern computer-based (i.e., digital electronics, software and network-based) aircraft systems. This study is to offer insight and provide educational value relative to the guidelines in ARP4754A and provide an assessment of the current state-of-the-practice within industry and regulatory bodies relative to development assurance for complex and safety-critical computer-based aircraft systems.

15. SUBJECT TERMS

Avionics; Certification; Guidelines; Life-cycle; Safety

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	230	(757) 864-9658