Understanding & Applying the New Mandatory ARP4761A, with ARP4754A

Vance Hilderman
Nazan Gozay Gurbuz
* Working together to provide aviation systems and safety engineering on four continents.
* Expertise in DO-178C, ARP4761/A, DO-254, ARP4754A, DO-278A, DO-200B, and DO-326A
* Training, Mentoring, Gap Analysis, Consulting: Aviation Systems, Safety, Software, Hardware
* World’s largest collection of whitepapers and aviation development process frameworks for clients
* Worked with 300 of the world’s largest 500 aviation companies

* Not yet a client? Easy: one-hour free technical consultation available for those companies not yet clients.
About AFuzion’s Presenter – Vance Hilderman

* BSEE, MBA, MSEE (Hughes Fellow)
* Founder of three of the world’s largest avionics and aviation development services companies
* Has personally trained over 19,500 persons; more than all other instructors in the world, combined.
* Has successfully contributed to over 300 diverse aviation projects for 200 clients.
* Author of the world’s best selling books and technical papers on aviation development.
* Contact: info@afuzion.com
About TAOS’s Presenter – Nazan Gozay Gurbuz

- BSME, MSME, MBA
- Founder of TAOS Certification and Engineering
- Has worked in both Industry and Military Authority side for more than 20 years in aircraft development and modification projects
- Has provided training and consultancy to many companies for establishment of their design assurance system
- Active member of SAE International S-18 Aircraft & Systems Development and Safety Assessment Committee for more than 10 years and has provided key contributions to development of SAE-ARP-4754A Aircraft Development Processes and SAE-ARP-4761(A) Safety Assessment Processes.
The purpose of this 1-hour technical training webinar is to:

* Understand why those ARPs are important and why we call them “Mandatory”
* Gain an overall view of ARP-4754A and ARP4761(A)
* Understand interaction of ARP-4754A and 4761(A) in DAL assignment and management
* Help you make better aircraft/avionics faster/cheaper while achieving new ARP4754A/4761(A) compliance!
First, A Quiz: True or False?

1. T/F: ARP4754A & ARP4761 are generally optional for aircraft & systems.

2. T/F: ARP4754A applies directly to avionics software and hardware.

3. T/F: ARP4754A Process Assurance performs system testing and also manufacturing & maintenance inspections.

4. T/F: Development Assurance Level (DAL) is assigned to the effort of mitigating systematic errors which could lead to failures.

5. T/F: DAL assignments depend on the failure condition classification, the number of independent failure paths, and their associated independence attributes.

6. T/F: ARP4761 provides methods for safety assessments to show compliance with certification requirements.

(Answers will be provided at the end of this Webinar)
Why “Mandatory”?

Certification Process

Showing compliance with 14CFR/CS 25.1309(b);
The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -
(1) Any catastrophic failure condition
   (i) is extremely improbable; and
   (ii) does not result from a single failure; and
(2) Any hazardous failure condition is extremely remote; and
(3) Any major failure condition is remote.

SAE ARP 4754A

Providing Development Assurance

SAE ARP 4761(A)

Providing Analyses Techniques
Why “Mandatory”? 

**FAA AC 20-174, dated 2011**
Recognizes SAE ARP 4754A as an acceptable method for establishing a development assurance process for compliance to 25.1309 (b)

**FAA AC 25-1309 (Arsenal version)**
…. These methods (in ARP 4754 and 4761), when correctly applied, are recognized by the FAA as valid for showing compliance with § 25.1309(b).

**EASA AMC 25.1309**
Recognizes SAE ARP 4754A and 4761 as an acceptable method for compliance with CS 25.1309(b)
SAE ARP 4754A Overview

<table>
<thead>
<tr>
<th>SAE ARP 4754</th>
<th>Certification Considerations for Highly-Integrated Or Complex Aircraft Systems</th>
<th>1996</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAE ARP 4754A</td>
<td>Guidelines for Development of Civil Aircraft and Systems</td>
<td>2010</td>
</tr>
</tbody>
</table>

ARP 4754A: guidelines for aircraft/systems development processes considering overall aircraft operating environment and functions with system safety assessment process.

Includes validation of requirements and verification of the design implementation for certification and process assurance.
Compare: ARP4754 to ARP4754A

- Section 1 – Scope
- Section 2 – References
- Section 3 – System Development
- Section 4 – Certification Process
- Section 5 – Design Assurance Level
- Section 6 – Safety Assessment Process
- Section 7 – Validation
- Section 8 – Verification
- Section 9 – Configuration Management
- Section 10 – Process Assurance
- Section 11 – Modified Aircraft

- Section 1 – Scope
- Section 2 – References
- Section 3 – Development Planning
- Section 4 – Aircraft and System Development process
- Section 5 – integral Processes
- Section 6 – Modifications to Aircraft Systems
  - Appendix A – Process Objectives Data
  - Appendix B – Safety Program Plan
  - Appendix C – FDAL/IDAL Assignment Process Example
  - Appendix D – Deleted
  - Appendix (Example) – Deleted
4754A Development Process Model

INTEGRAL PROCESSES

- 5.1 SAFETY ASSESSMENT
- 5.2 DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT
- 5.3 REQUIREMENTS CAPTURE
- 5.4 REQUIREMENTS VALIDATION
- 5.6 CONFIGURATION MANAGEMENT
- 5.7 PROCESS ASSURANCE
- 5.8 CERTIFICATION & REGULATORY AUTHORITY COORDINATION

PLANNING

AIRCRAFT/SYSTEM DEVELOPMENT PROCESS

CONCEPT

AIRCRAFT FUNCTION DEVELOPMENT

ALLOCATION OF AIRCRAFT FUNCTIONS TO SYSTEMS

DEVELOPMENT OF SYSTEM ARCHITECTURE

ALLOCATION OF SYSTEM REQUIREMENTS TO ITEMS

SYSTEM IMPLEMENTATION

DATA & DOCUMENTATION

3.0

4.0

4.2

4.3

4.4

4.5

4.6
* Planning Process – *Occurs first*
* Development Process – *Follows Planning*
* Correctness Process – *Continuous Throughout Project*
The Six Basic Steps of ARP4754A:

1. Plan your aircraft/system’s development lifecycle ecosystem;
2. Implement Safety activities per ARP4761/A;
3. Define and justify Development Assurance Levels;
4. Define system architecture and requirements; and Validate;
5. Perform Verification and Configuration Management;
4754A Development Planning Elements

1. **Development**
   Define process/methods for establishing architecture development, integration, and implementation

2. **Safety**
   Define Safety scope applicable to aircraft or system

3. **Requirements Management**
   Define the acquisition and management of requirements

4. **Validation**
   Define methods used to ensure requirements and assumptions are correct
5. Implementation Verification
Define processes and criteria used to assess if implementation meets requirements

6. Configuration Management
Define processes/activities to manage development configuration items/versions throughout lifecycle

7. Process Assurance
Define independent activities used to ensure development activities follow processes and plans

8. Certification
Define how certification is to be achieved
ARP4754A Interactions

Safety Assessment
ARP4761

• Functions
• Architecture
• FDAL, etc.

System Development
ARP4754A
(ED-79)

• IDAL

Software
DO-178
(ED-12)

Hardware
DO-254
(ED-80)

Tests

Copyright 2018
 ARP 4761(A) Overview

<table>
<thead>
<tr>
<th>SAE ARP 4761</th>
<th>Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment</th>
<th>1996</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAE ARP 4761(A)</td>
<td>Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment</td>
<td>Will be issued in 2019 Q3</td>
</tr>
</tbody>
</table>

ARP4761/A describes guidelines and methods of performing the safety assessment for certification of civil aircraft. Used for showing compliance with certification requirements (e.g., 14CFR/CS Parts 23, 25, 27, and 29, primarily sections 1309 and 1709). May also apply to 14CFR Parts 33, CS-E and CS-P.
Draft ARP-4761A Content

A – Aircraft Functional Hazard Assessment (AFHA)
B – Preliminary Aircraft Safety Assessment (PASA)
C – System Functional Hazard Assessment (SFHA)
D – Preliminary System Safety Assessment (PSSA)
E – System Safety Assessment (SSA)
F – Aircraft Safety Assessment (ASA)
G – Fault Tree Analysis (FTA)
H – Dependence Diagrams (DD)
I – Markov Analysis (MA)
J – Failure Modes and Effects Analysis (FMEA)
K – Zonal Safety Analysis (ZSA)
L – Particular Risk Analysis (PRA)
M – Common Mode Analysis (CMA)
N – Model Based Safety Analysis (MBSA)
O – Cascading Effects Analysis (CEA)
P – FDAL/IDAL Assignment
Q – Contiguous Safety Assessment Process Example

Current ARP-4761 Content

A – Functional Hazard Assessment (FHA)
B – Preliminary System Safety Assessment (PSSA)
C – System Safety Assessment (SSA)
D – Fault Tree Analysis (FTA)
E – Dependence Diagrams (DD)
F – Markov Analysis (MA)
G – Failure Modes and Effects Analysis (FMEA)
H – Failure Modes and Effects Summary (FMES)
I – Zonal Safety Analysis (ZSA)
J – Particular Risk Analysis (PRA)
K – Common Mode Analysis (CMA)
L – Contiguous Safety Assessment Process Example

Compare: ARP4761 to Draft ARP4761(A)
Intended users include:

- Airframe manufacturers
- System integrators
- Equipment suppliers
- Certification authorities
ARP 4761(A) Overview

ARP 4761 (A) Safety Assessments

A/C Level

- Aircraft Functional Hazard Assessment (AFHA)
- Preliminary Aircraft Safety Assessment (PASA)
- Aircraft Safety Assessment (ASA)

System Level

- System Functional Hazard Assessment (SFHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)
ARP 4761(A) Overview

ARP 4761 (A)
Safety Analyses

- Fault Tree Analysis
- Dependence Diagram
- Markov Analysis
- Failure Mode and Effect Analysis and Summary
- Cascading Effect Analysis
- Model Base Safety Analysis

- Common Cause Analyses
  - Zonal Safety Analysis
  - Particular Risk Analysis
  - Common Mode Analysis
Development Assurance confirms the planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected so system satisfies applicable certification basis.

- The mitigation of **Failures** is performed by setting safety qualitative and/or quantitative requirements.

- **Error** is a potential source of failure and mitigated by implementation of a Development Assurance Process.
Two type of Development Assurance Level in ARP 4754A

Function Development Assurance Level (FDAL)

The level of rigor of development assurance tasks performed to Functions.

Item Development Assurance Level (IDAL)

The level of rigor of development assurance tasks performed on Items (hardware and software).

ARP4761 identifies FDAL and IDAL

ARP4754A defines the processes to be applied for FDAL
ARP 4754A defines two ways to assign DALs:

1- Assignment without considering the system’s architecture

2- Assignment considering the architecture. With this option, independence between systems and components must be assessed.
Important elements for DAL assignment;

- Functional Failure Set (FFS)
- Members
- Independence

**FFS** is equivalent to a Fault Tree Minimal Cut Set.

**Minimal Cut Set:** The smallest combination of basic events which, if they occur, will cause the top event to occur.

**Member:** An aircraft/system function or item that may contain an error causing its loss or anomalous behavior.
1- Without architectural consideration:

<table>
<thead>
<tr>
<th>FHA’s Failure Condition Severity Classification</th>
<th>FDAL Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>A</td>
</tr>
<tr>
<td>Hazardous/Severe Major</td>
<td>B</td>
</tr>
<tr>
<td>Major</td>
<td>C</td>
</tr>
<tr>
<td>Minor</td>
<td>D</td>
</tr>
<tr>
<td>No Safety Effect</td>
<td>E</td>
</tr>
</tbody>
</table>
### 2- With architectural considerations:

<table>
<thead>
<tr>
<th>Top-level Failure Condition Classification</th>
<th>Functional Failure Sets with a Single Member</th>
<th>Functional Failure Sets with Multiple Member</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPTION 1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catastrophic</td>
<td>FDAL A</td>
<td>FDAL A for one Member</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional Member(s) no lower than FDAL C</td>
</tr>
<tr>
<td>Hazardous/Severe Major</td>
<td>FDAL B</td>
<td>FDAL B for one Member</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional Member(s) no lower than FDAL D</td>
</tr>
<tr>
<td>Major</td>
<td>FDAL C</td>
<td>FDAL C for one Member</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>FDAL D</td>
<td>FDAL D for one Member</td>
</tr>
<tr>
<td>No Safety Effect</td>
<td>FDAL E</td>
<td>FDAL E</td>
</tr>
</tbody>
</table>
Aircraft Function List

Regulatory Objectives & Requirements

A/C OEM

Aircraft FHA
(Aircraft Functions)

- Failure Conditions (FC)
- FC Effects
- FC Classification (CAT, HAZ, MAJ, etc.)
- Aircraft Function Criticality Levels (FDAL)
  Without architectural consideration

PASA
(Aircraft Architecture)

- Aircraft Function FDALs
- System Function FDALs
- Safety Requirements
  (Probability budgets, independence, etc.)
Development Assurance Level Assignment

A/C FHA
PASA
System Function List
Regulatory Objectives & Requirements

System FHA
(System Functions)
- Failure Conditions (FC)
- FC Effects
- FC Classification (CAT, HAZ, MAJ, etc.)

System Supplier

PSSA
(System Architecture)
- System Function FDALs
- IDALs for Hardware and Software
- Safety Requirements (Probability budgets, independence, etc.)
## Aircraft Function List (Example)

<table>
<thead>
<tr>
<th></th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control aircraft energy</td>
</tr>
<tr>
<td>1.1</td>
<td>Maintain or increase aircraft energy</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Provide thrust</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Reduce drag</td>
</tr>
<tr>
<td>1.2</td>
<td>Reduce aircraft energy</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Provide controlled aerodynamic drag</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Provide high lift capability</td>
</tr>
<tr>
<td>1.2.3</td>
<td><strong>Provide Deceleration on Ground</strong></td>
</tr>
<tr>
<td>Function</td>
<td>Failure Condition</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Provide Deceleration on Ground</td>
<td>Total loss of deceleration capability</td>
</tr>
<tr>
<td>Inadvertent deceleration</td>
<td>Take off after V1</td>
</tr>
</tbody>
</table>
Provide Deceleration on Ground

Thrust Reverser System

Ground Spoiler System

Wheel Brake System

Preliminary Aircraft Safety Assessment (PASA)
Loss of deceleration capability

Loss of trust reverser

Loss of effective wheel braking

Loss of all speed brakes

Loss of all wheel brakes

FFS/Min. Cut Sets
Trust Rev AND Speed Brakes, OR
Trust Rev AND Wheel Brakes

CAT

Functional Failure | FDAL
---|---
Trust Reverse | C
Speed Brakes | A
Wheel Brakes | A

ARP-4754A Section 5.2. DAL Assignment With architectural consideration
Inadvertent deceleration after V1

Inadvertent trust reverser after V1

Inadvertent wheel braking after V1

Inadvertent spoiler deployment after V1

Trust Reverse OR Spoiler OR Wheel Brake

Functional Failure

<table>
<thead>
<tr>
<th>Functional Failure</th>
<th>FDAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Reverse</td>
<td>A</td>
</tr>
<tr>
<td>Spoiler</td>
<td>A</td>
</tr>
<tr>
<td>Wheel Brake</td>
<td>A</td>
</tr>
</tbody>
</table>

ARP-4754A Section 5.2. DAL Assignment
With architectural consideration
The Wheel Brake System and Breaking System Control Unit (BSCU) shall be designed to FDAL A based on the Catastrophic classification of Inadvertent braking.

SAE-ARP-4754A Table 5-2
Option 2
With architectural consideration
FDAL
SAE- ARP-4754A

Deceleration Function
FDAL A

Wheel Break System
FDAL A

BSCU
FDAL A

IDAL
RTCA-DO-178C
RTCA-DO-254

Command and Monitor Hardware
IDAL B

Command and Monitor Software
IDAL B
# Development Assurance Process Objectives

ARP-4754A Appendix A- Process Objectives Data

## Planning Process Objectives

<table>
<thead>
<tr>
<th>Objective Outputs</th>
<th>FDAL A</th>
<th>FDAL B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Certification Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Safety Program Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Validation Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Verification Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Process Assurance Plan</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
</tbody>
</table>
### Development Assurance Process Objectives

#### Safety Assessment Process Objectives

<table>
<thead>
<tr>
<th>Objective Outputs</th>
<th>FDAL A</th>
<th>FDAL B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft FHA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>System FHA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>PASA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>PSSA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>SSA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>ASA</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Particular Risk Assessment</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Common Mode Analysis</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Zonal Safety Analysis</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
</tbody>
</table>

* Independence is achieved when the safety activity is performed by a person(s) other than the developer of the system/item.
## Requirement Validation Process Objectives

<table>
<thead>
<tr>
<th>Objective Outputs</th>
<th>FDAL A</th>
<th>FDAL B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation Results</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Aircraft, system, item requirements are complete and correct.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Results</td>
<td>Recommended*</td>
<td>Recommended</td>
</tr>
<tr>
<td>Assumptions are justified and validated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Results</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Derived requirements are justified and validated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Results</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Requirements are traceable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Summary and Matrix</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Validation compliance substantiation is provided</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Independence is achieved when the validation activity is performed by a person(s) other than the developer of the requirement.
## Development Assurance Process Objectives

<table>
<thead>
<tr>
<th>Objective Outputs</th>
<th>FDAL A</th>
<th>FDAL B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Procedures</td>
<td>Recommended*</td>
<td>Recommended</td>
</tr>
<tr>
<td>Test or demonstration procedures are correct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification Procedures/Results</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Intended function and confidence of no unintended function impacts to safety.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification Procedures/Results</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Product implementation complies with aircraft, and system requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification Procedures/Results</td>
<td>Recommended*</td>
<td>Recommended*</td>
</tr>
<tr>
<td>Safety requirements are verified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification Summary/Matrix</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Verification compliance substantiation is included</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification Summary/Problem Reports</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Deficiencies and their related impact on safety is identified.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Common Safety Process Mistakes

Administration And Process Problems

- Company does not provide adequate support for safety assessment or development assurance activities
- Safety Processes are not incorporated to the system development processes
- Late identification of failure conditions
- Using inappropriate analysis methods
- Insufficient control of vendor safety processes
- No independent validation and verification of safety assessments
QUIZ ANSWERS

1. ARP4754A & ARP4761 are generally optional for aircraft & systems: FALSE

2. ARP4754A applies directly to avionics software and hardware: FALSE

3. ARP4754A Process Assurance performs system testing and also manufacturing & maintenance inspections: FALSE

4. Development Assurance Level (DAL) is assigned to the effort of mitigating systematic errors which could lead to failures: TRUE

5. DAL assignments depend on failure condition classification, number of independent failure paths, and their associated independence attributes: TRUE

6. ARP4761 provides methods for safety assessments to show compliance with certification requirements: TRUE
Questions & Answer Session

For additional information:

Taos:
www.taoscertification.com
nazan.gurbuz@taoscertification.com

AFuzion Incorporated:
www.afuzion.com
info@afuzion.com