Understanding & Applying the New Mandatory ARP4761A, with ARP4754A

Vance Hilderman
Nazan Gozay Gurbuz

About AFuzion & Taos

* 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.

Purpose of this Technical Webinar

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.

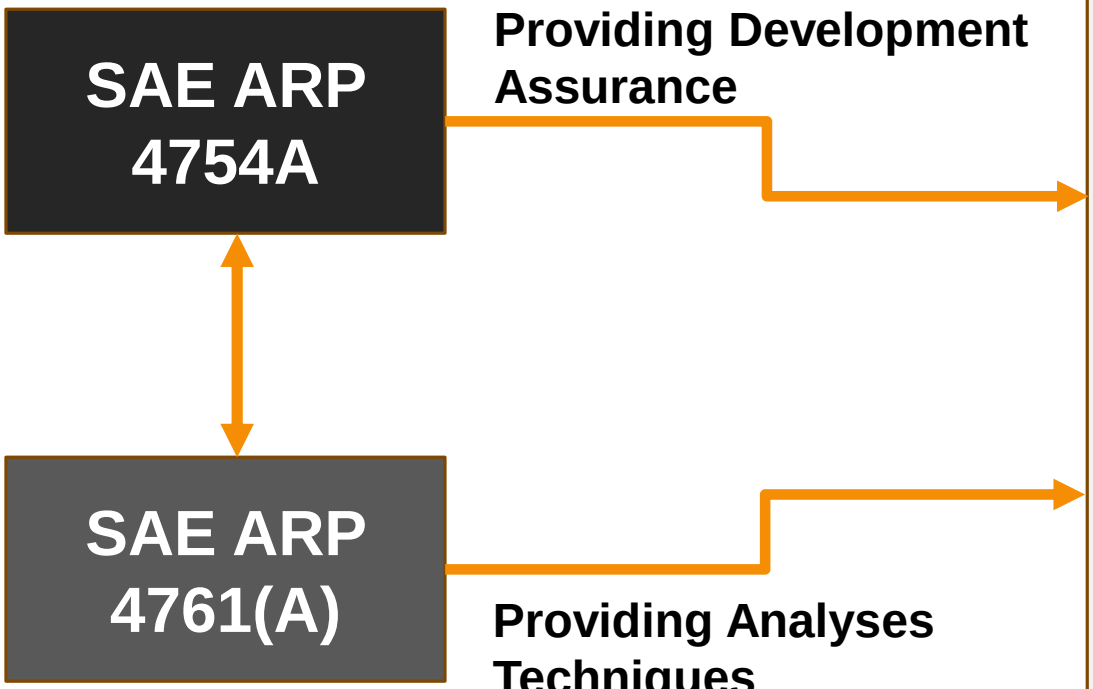
4. T/F: Development Assurance Level (DAL) is assigned to the effort of mitigating systematic errors which could lead to failures.

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.

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)

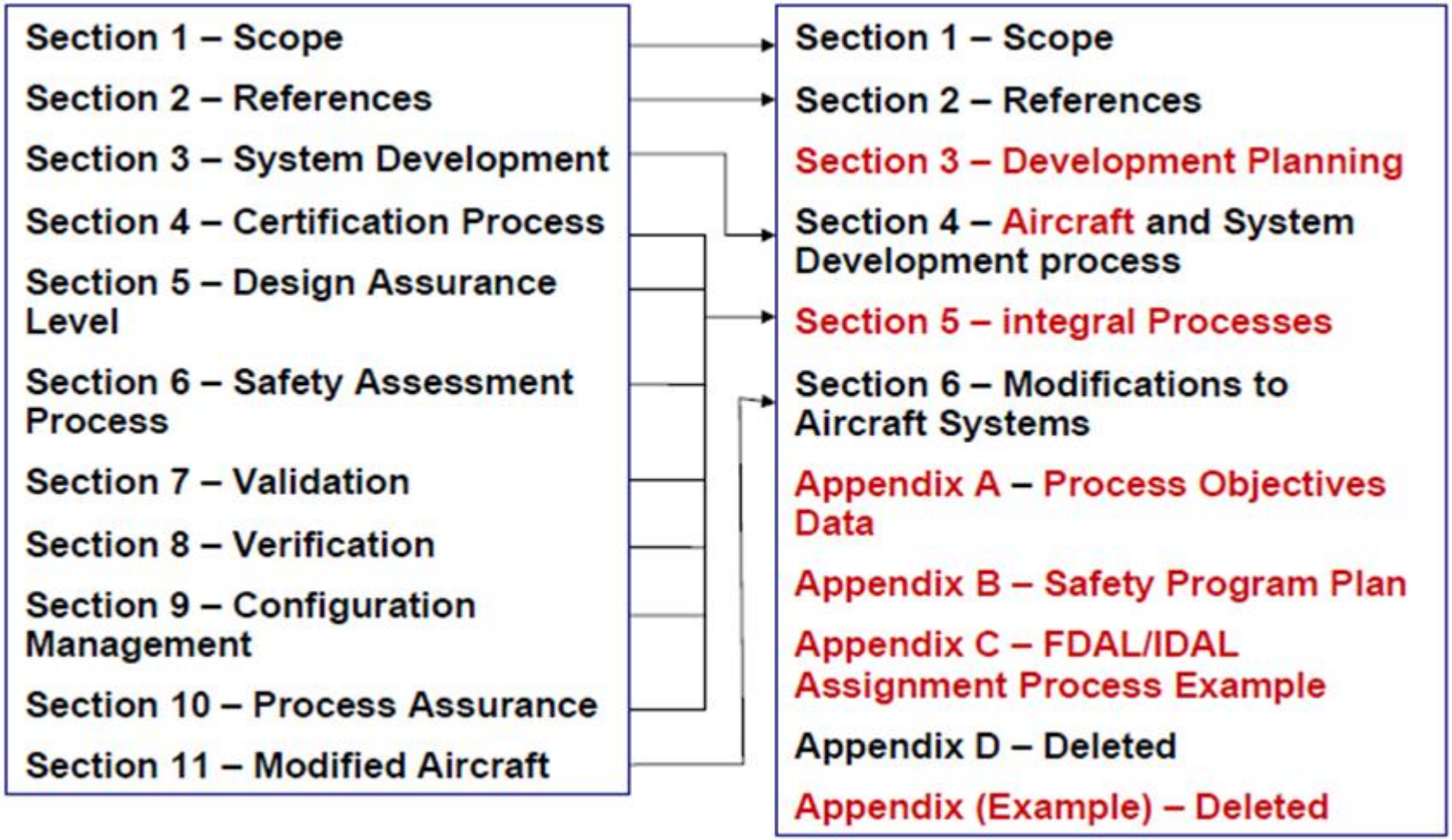
ARP 4754A Overview

SAE ARP 4754	Certification Considerations for Highly-Integrated Or Complex Aircraft Systems	1996
SAE ARP 4754A	Guidelines for Development of Civil Aircraft and Systems	2010

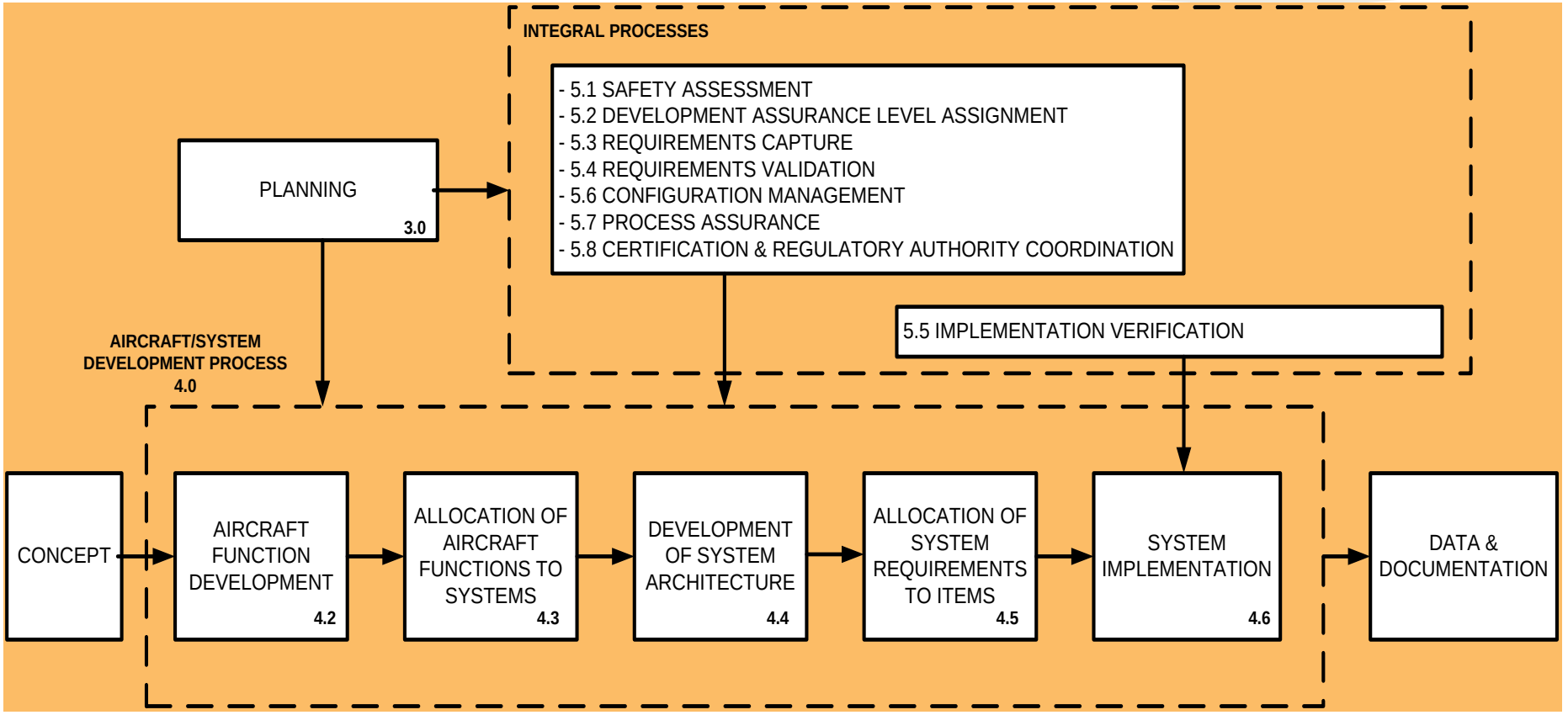
ARP 4754A: guidelines for aircraft/systems development processes considering overall aircraft operating environment and functions with system safety assessment process.

Includes validation of requirements and verification of the design implementation for certification and process assurance.

Compare: ARP4754 to ARP4754A

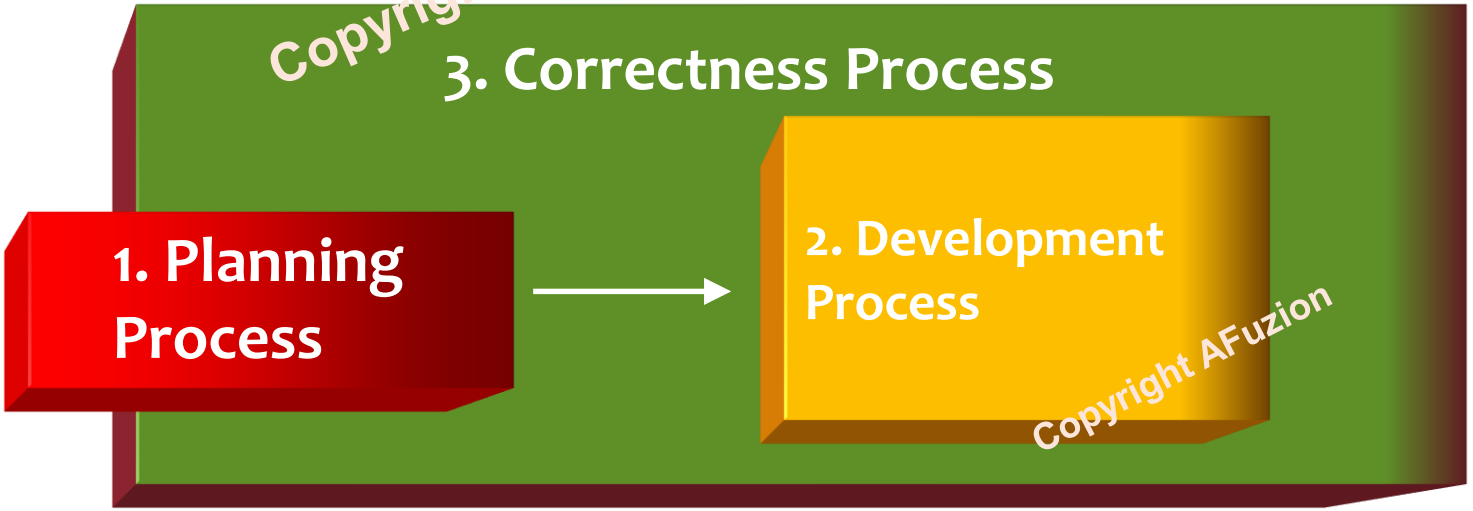


4754A Development Process Model



Safety-Critical Development: Three Key Processes

* Planning Process – *Occurs first*
* Development Process – *Follows Planning*
* Correctness Process – *Continuous Throughout Project*



ARP4754A: The Six Basic Steps

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;
6. Implement Process Assurance and prove Transition Criteria.

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

4754A Development Planning Elements

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

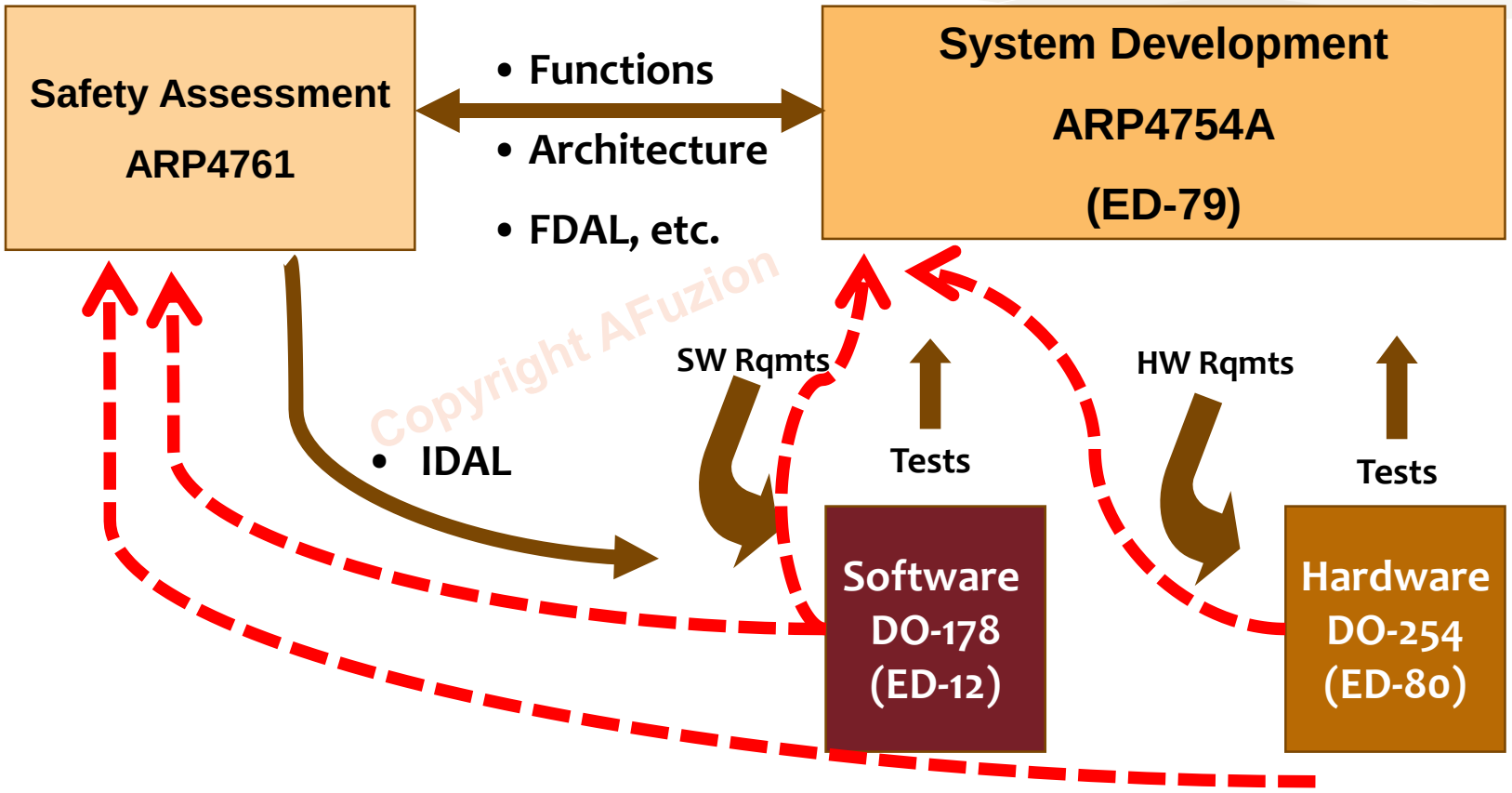
7. Process Assurance

Define independent activities used to ensure development activities follow processes and plans

8. Certification

Define how certification is to be achieved

ARP4754A Interactions



ARP 4761(A) Overview

SAE ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment	1996
SAE ARP 4761(A)	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment	Will be issued in 2019 Q3

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.

Compare: ARP4761 to Draft ARP4761(A)

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

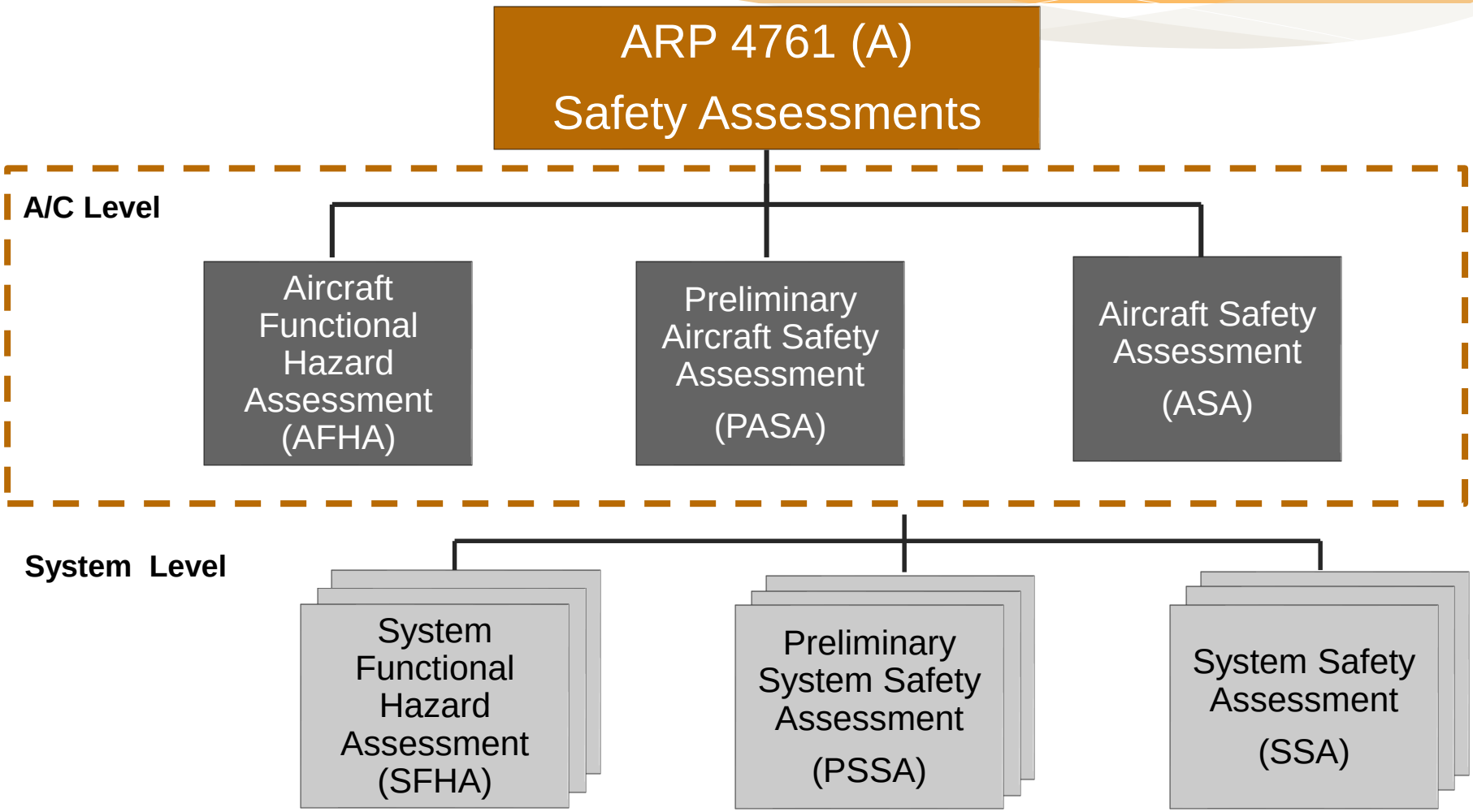
A – Functional Hazard Assessment (FHA)
B – Preliminary System Safety Assessment (PSSA)
C – System Safety Assessment (SSA)
D – Fault Tree Analysis (FTA)
E – Dependence Diagrams (DD)
F – Markov Analysis (MA)
G – Failure Modes and Effects Analysis (FMEA)
H – Failure Modes and Effects Summary (FMES)
I –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

ARP 4761(A) Overview

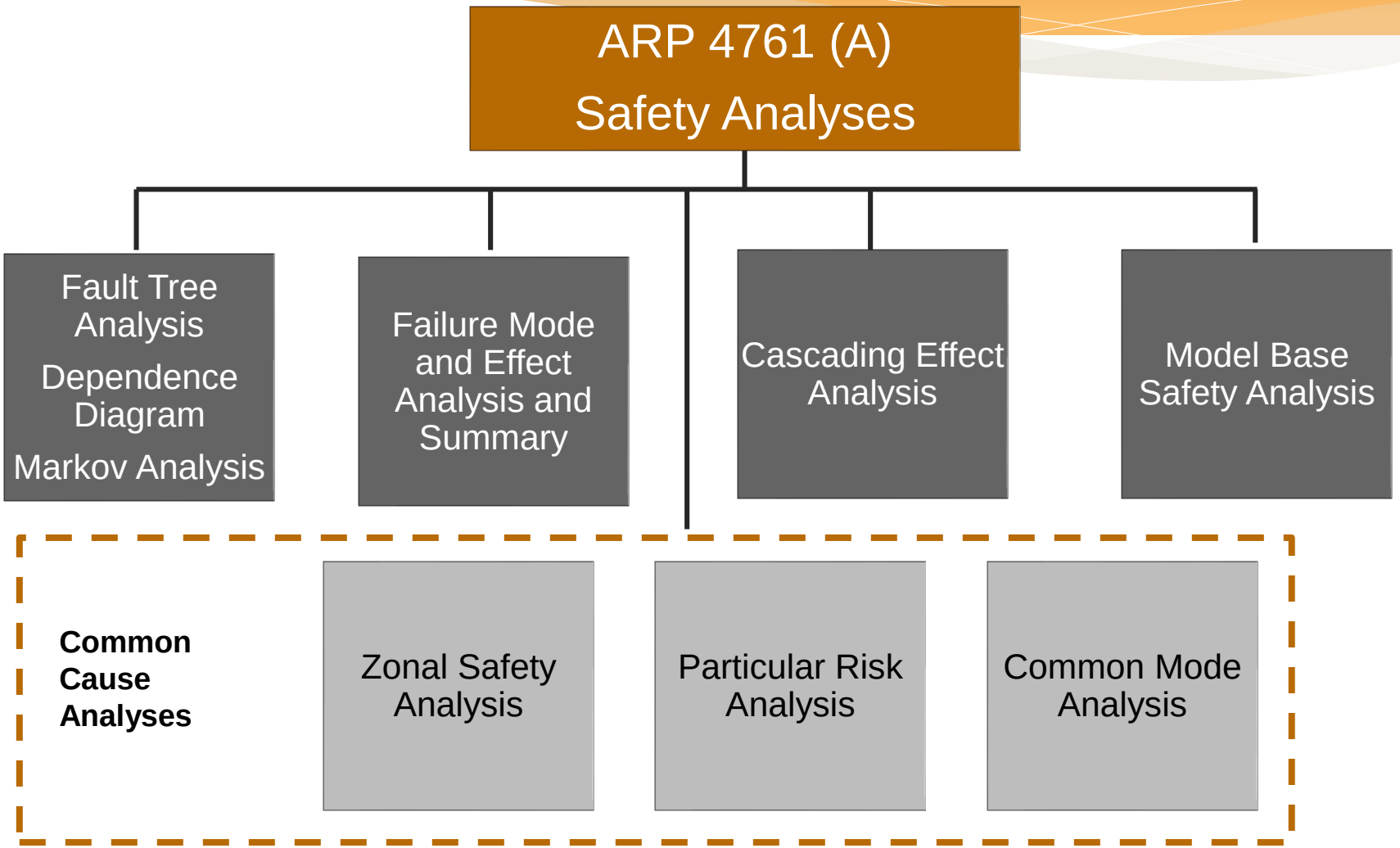
Intended users include:

- Airframe manufacturers
- System integrators
- Equipment suppliers
- Certification authorities

ARP 4761(A) Overview



ARP 4761(A) Overview



Development Assurance

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.

Development Assurance Level

Two type of Development Assurance Level in ARP 4754A

ARP4761 identifies **FDAL and IDAL**

ARP4754A defines the processes to be applied for **FDAL**

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).

Development Assurance Level Assignment

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.

Development Assurance Level Assignment

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.

Development Assurance Level Assignment

1- Without architectural consideration:

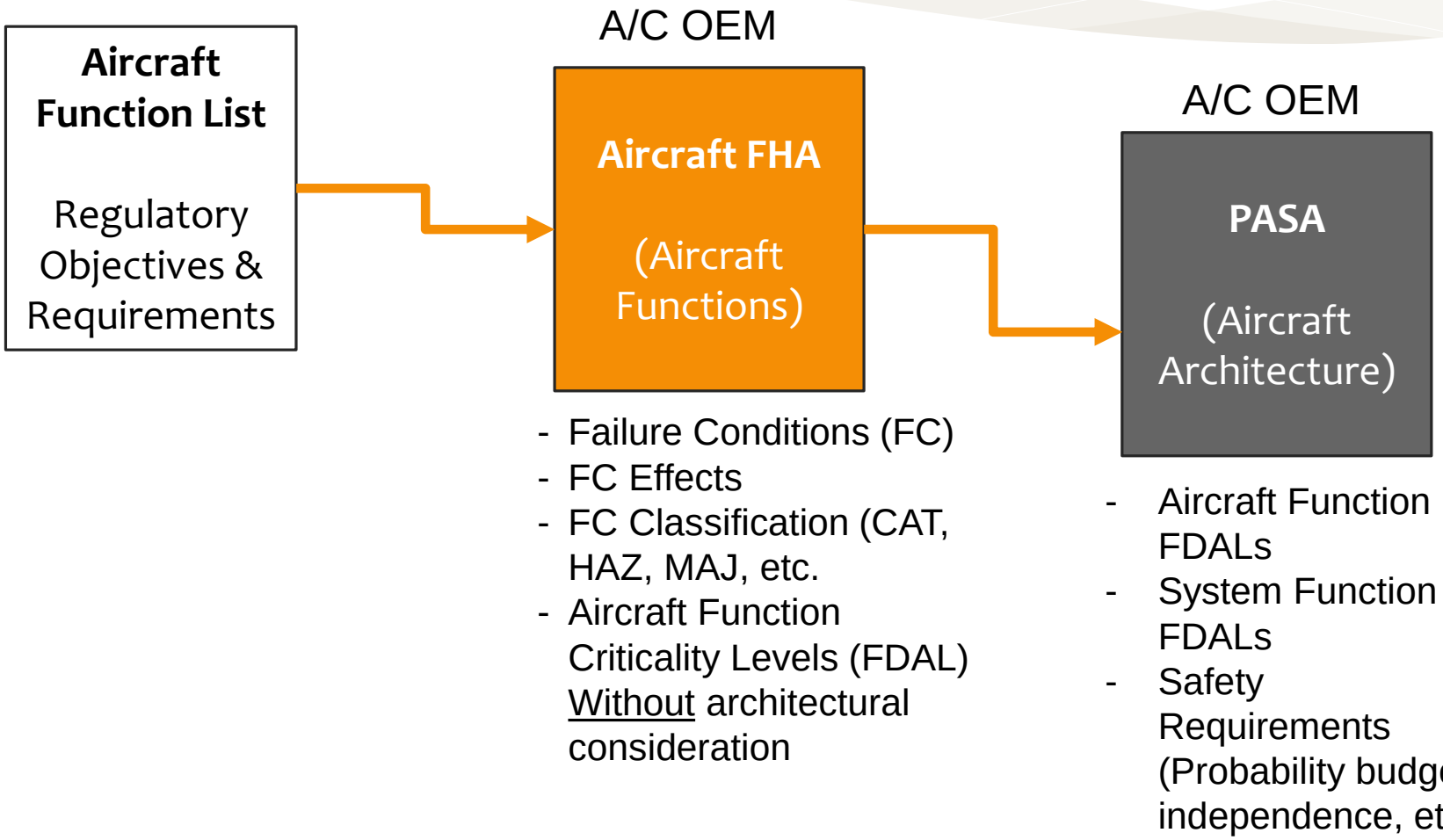
FHA's Failure Condition Severity Classification	FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Development Assurance Level Assignment

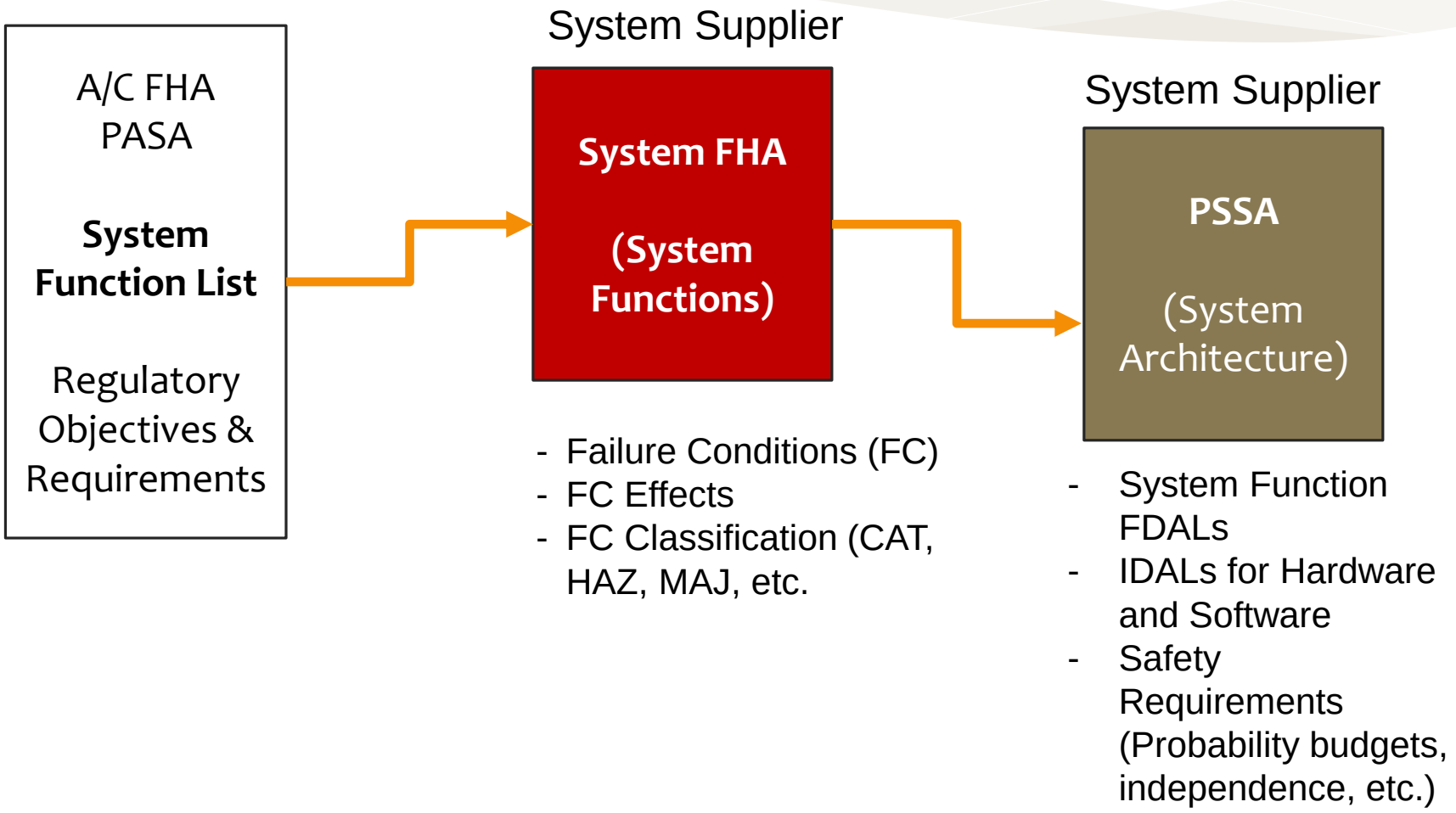
2- With architectural considerations:

Top-level Failure Condition Classification	Functional Failure Sets with a Single Member	Functional Failure Sets with Multiple Member	
		OPTION 1	**OPTION 2**
Catastrophic	**FDAL A**	**FDAL A** for one Member Additional Member(s) no lower than **FDAL C**	**FDAL B** for two Members Additional Member(s) no lower than **FDAL C**
Hazardous/ Severe Major	**FDAL B**	**FDAL B** for one Member Additional Member(s) no lower than **FDAL D**	**FDAL C** for two Members Additional Member(s) no lower than **FDAL D**
Major	**FDAL C**	**FDAL C** for one Member	**FDAL D** for two Members
Minor	**FDAL D**	**FDAL D** for one Member	
No Safety Effect	**FDAL E**	FDAL E	

Development Assurance Level Assignment



Development Assurance Level Assignment



DAL Example

Aircraft Function List (Example)	
1	Control aircraft energy
1.1	Maintain or increase aircraft energy
1.1.1	Provide thrust
1.1.2	Reduce drag
1.2	Reduce aircraft energy
1.2.1	Provide controlled aerodynamic drag
1.2.2	Provide high lift capability
1.2.3	**Provide Deceleration on Ground**

DAL Example

Aircraft FHA						
Function	**Failure Condition**	**Phase of Flight**	**Effects of Failure Condition**	**Classification**	**DAL**	**Verification**
Provide Deceleration on Ground	**Total loss of deceleration capability**	Landing	Crew is unable to decelerate aircraft resulting in a high speed overrun	**Catastrophic**	**FDAL A**	Fault Tree Analysis
	Inadvertent deceleration	Take off after V1	Crew cannot take of resulting in a high speed overrun	**Catastrophic**	**FDAL A**	Fault Tree Analysis

DAL Example

Preliminary Aircraft Safety Assessment (PASA)

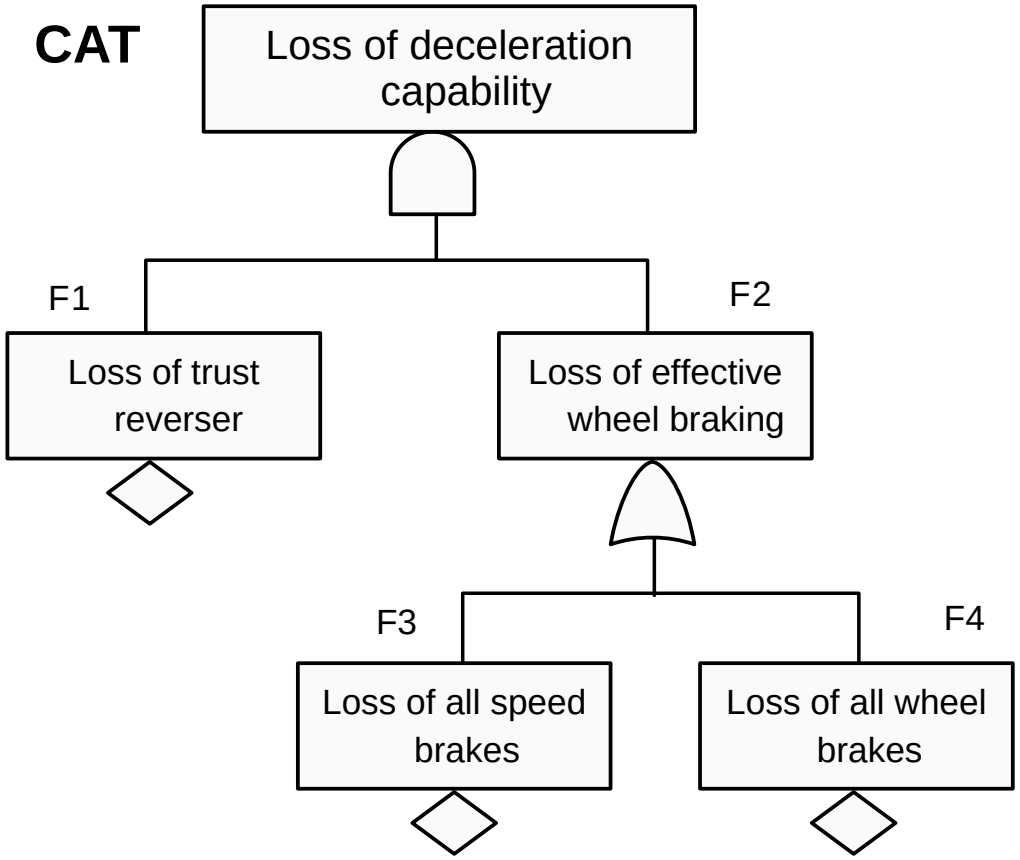
Provide Deceleration on Ground

- **Thrust Reverser System**

- **Ground Spoiler System**

- **Wheel Brake System**

DAL Example



FFS/Min. Cut Sets

Trust Rev **AND** Speed Brakes,

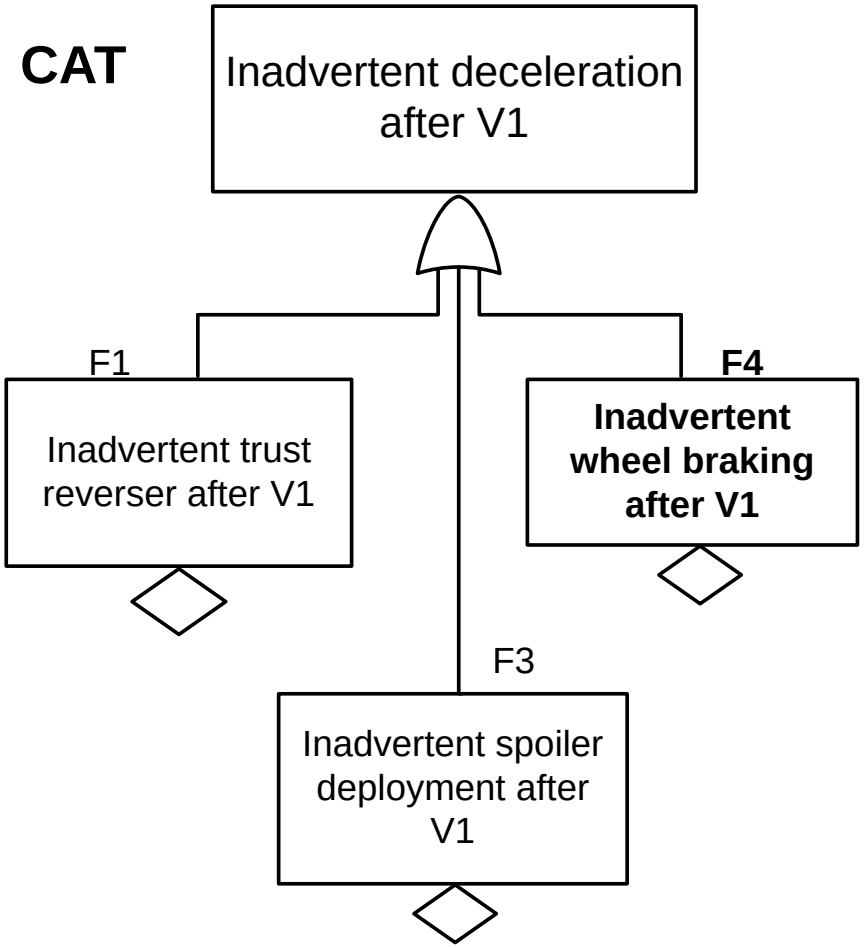
OR

Trust Rev **AND** Wheel Brakes

Functional Failure	FDAL	
Trust Reverse	C	B
Speed Brakes	A	B
Wheel Brakes	**A**	**B**

ARP-4754A Section 5.2. DAL Assignment
With architectural consideration

DAL Example



FFS/Min. Cut Sets

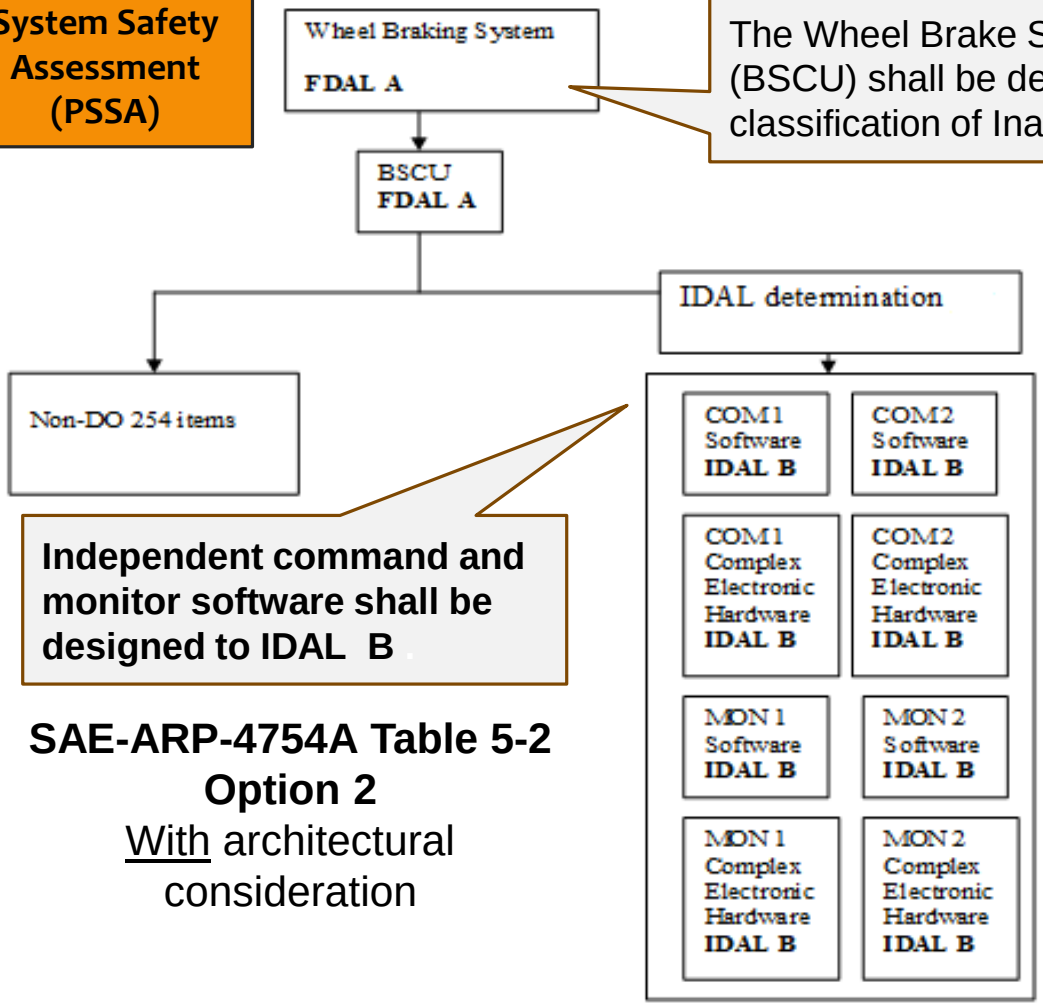
Trust Reverse **OR** Spoiler **OR** Wheel Brake

Functional Failure	FDAL
Trust Reverse	A
Spoiler	A
Wheel Brake	**A**

ARP-4754A Section 5.2. DAL Assignment
With architectural consideration

DAL Example

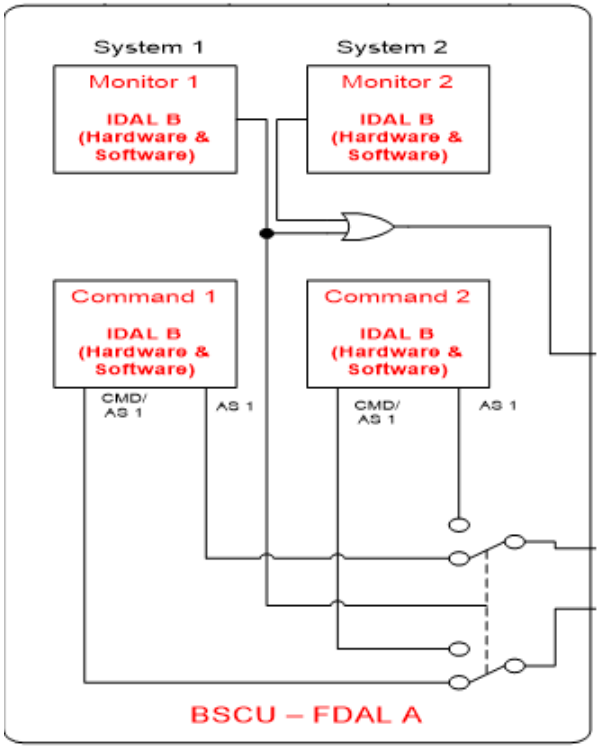
Preliminary System Safety Assessment (PSSA)



The Wheel Brake System and Breaking System Control Unit (BSCU) shall be designed to FDAL A based on the Catastrophic classification of Inadvertent braking

Independent command and monitor software shall be designed to IDAL B

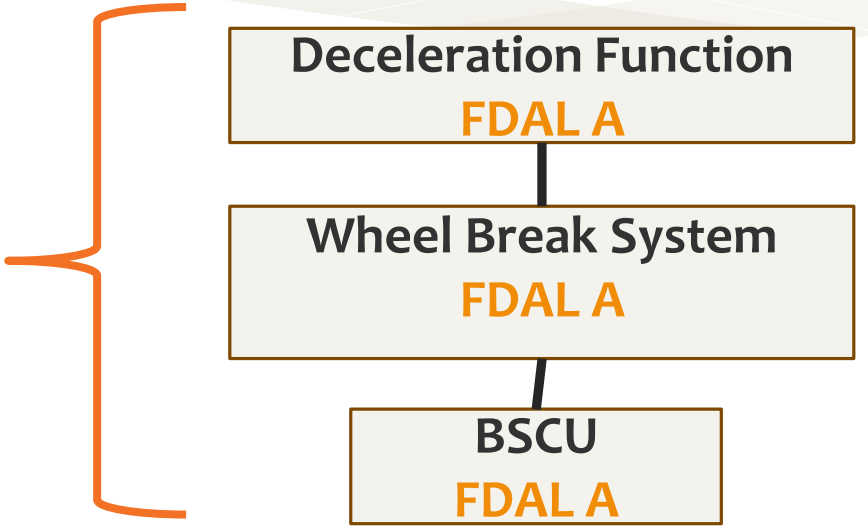
SAE-ARP-4754A Table 5-2 Option 2
With architectural consideration



DAL Assignment Results

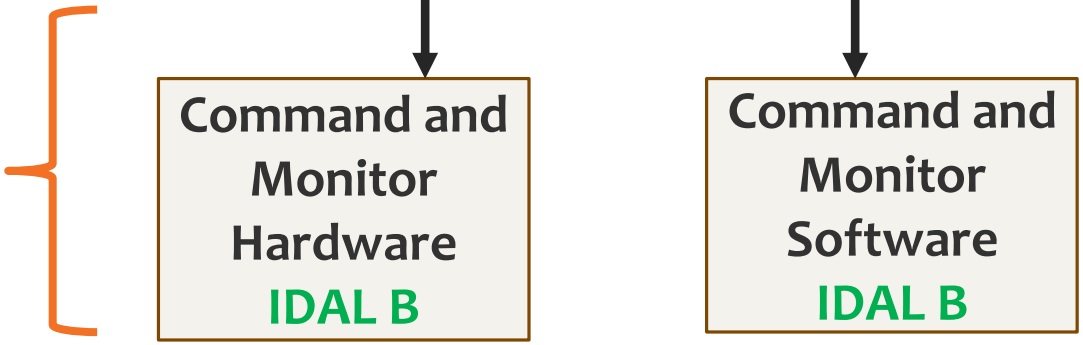
FDAL

SAE- ARP-4754A



IDAL

RTCA-DO-178C
RTCA-DO-254



Development Assurance Process Objectives

ARP-4754A Appendix A- Process Objectives Data

Planning Process Objectives		
Objective Outputs	**FDAL A**	**FDAL B**
Development Plan	Recommended	Recommended
Certification Plan	Recommended	Recommended
Safety Program Plan	Recommended	Recommended
Validation Plan	Recommended	Recommended
Verification Plan	Recommended	Recommended
Configuration Management	Recommended	Recommended
Process Assurance Plan	Recommended	Recommended

Development Assurance Process Objectives

Safety Assessment Process Objectives		
Objective Outputs	**FDAL A**	**FDAL B**
Aircraft FHA	Recommended*	Recommended*
System FHA	Recommended*	Recommended*
PASA	Recommended*	Recommended*
PSSA	Recommended*	Recommended*
SSA	Recommended*	Recommended*
ASA	Recommended*	Recommended*
Particular Risk Assessment	Recommended	Recommended
Common Mode Analysis	Recommended*	Recommended*
Zonal Safety Analysis	Recommended	Recommended

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

Development Assurance Process Objectives

Requirement Validation Process Objectives		
Objective Outputs	**FDAL A**	**FDAL B**
Validation Results Aircraft, system, item requirements are complete and correct.	Recommended*	Recommended*
Validation Results Assumptions are justified and validated	Recommended*	Recommended
Validation Results Derived requirements are justified and validated.	Recommended*	Recommended*
Validation Results Requirements are traceable.	Recommended	Recommended
Validation Summary and Matrix Validation compliance substantiation is provided	Recommended	Recommended

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

Development Assurance Process Objectives

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

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**

Wrap-up / Questions & Answers

- *Questions & Answer Session*

- *For additional information:*

Taos:

www.taoscertification.com

nazan.gurbuz@taoscertification.com

AFuzion Incorporated:

www.afuzion.com

info@afuzion.com