# 2º Simpósio Internacional de Confiabilidade e Gestão de Segurança Operacional

**09 a 11 de novembro de 2010**

DCA-BR

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

2nd Simpósio Internacional de Confiabilidade e
Gestão de Segurança Operacional
9 a 11 de novembro de 2010

# Aerospace Practices

## Just for Aviation?

Eric M. Peterson
Electron International, Inc.

SAE S18 Co-Chairman

SAE Aerospace
An SAE International Group

eii

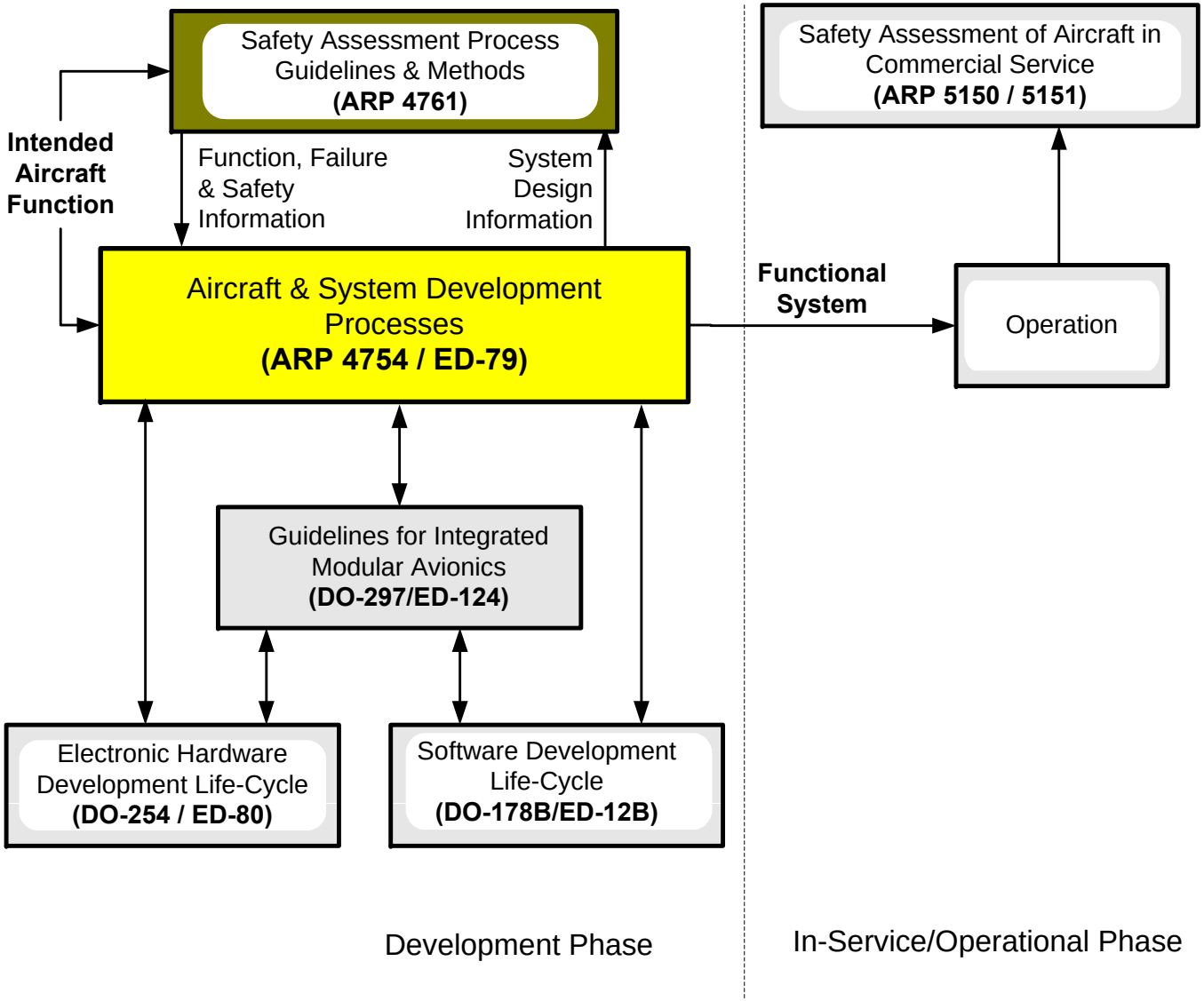
# What is SAE S-18

- Aircraft & Systems Development and Safety Assessment Committee
  - Active international committee
  - Representatives attend from > 25 companies and > 10 countries.
- Charter
  - Develop and maintain recommended practices for certification and product assurance of aircraft and systems from development and validation of requirements to verification of an implemented design.
  - Develop and maintain recommended practices for accomplishing initial design and in-service safety assessments of aircraft, systems and equipment to support effective safety management.

# Presentation Outline

- Document Overview and Relationships
  - ARP4754/4754A
  - ARP4761
  - ARP5150
- System Development (ARP4754)
- Safety Evaluation Methods (ARP4761)
- Monitoring Products in the Field (ARP5150)
- Closing Remarks

# Recommended Practices Relationships



# Overview

## ARP4754/4754A

- Discusses the development, validation and verification of aircraft & systems requirements.

## ARP4761

- Describes guidelines and methods of performing the safety assessment product assurance of aircraft.

## ARP5150

- Describes guidelines, methods and tools used to perform the ongoing safety assessment process for transport airplanes in commercial service.

## ARP5151

- Describes a process that may be used to perform the ongoing safety assessment for 1) GAR aircraft and components, & 2) commercial operators of GAR aircraft.

# ARP4754 Overview

## ARP4754

"Certification Considerations for Highly-Integrated or Complex Aircraft Systems"

## ARP4754A

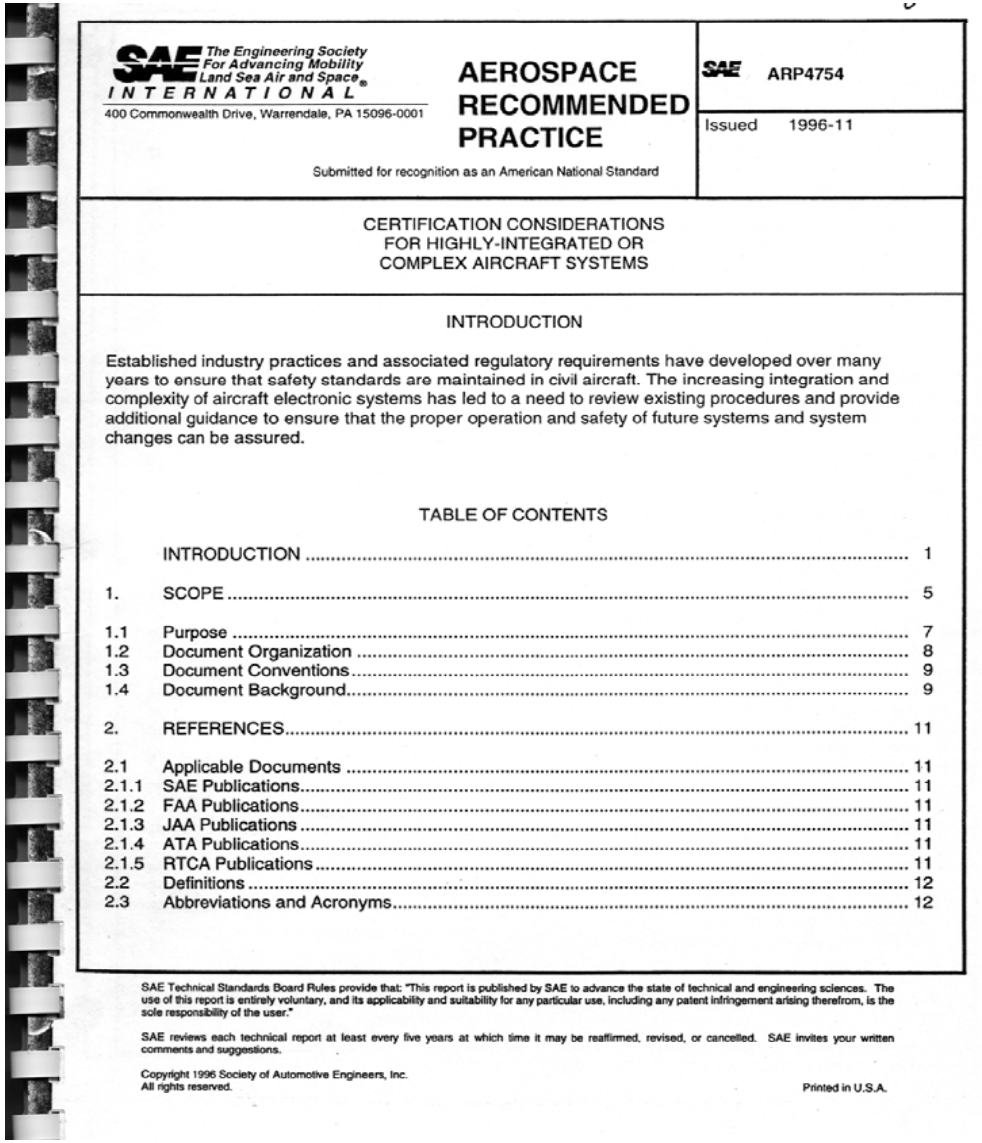
"Guidelines for Development of Civil Aircraft and Systems"

# ARP4754 /4754A Overview

- Aerospace Recommended Practice for the development and integration of aircraft systems
- Early treatment of airplane level integration
- Original document development team (SIRT) was dissolved after release of ARP4754 in 1996
- SAE S-18 revised to ARP4754A in 2010 (publication pending)

# ARP4754 Overview

- Structured Development Process
- Requirements Definition
- Introduces Development Assurance Levels
- Validation of Requirements
- Implementation Verification
- Tied to Safety Methodology (ARP4761)



SAE The Engineering Society For Advancing Mobility Land Sea Air and Space®
INTERNATIONAL
400 Commonwealth Drive, Warrendale, PA 15096-0001

**AEROSPACE RECOMMENDED PRACTICE**

Submitted for recognition as an American National Standard

SAE ARP4754

Issued 1996-11

CERTIFICATION CONSIDERATIONS FOR HIGHLY-INTEGRATED OR COMPLEX AIRCRAFT SYSTEMS

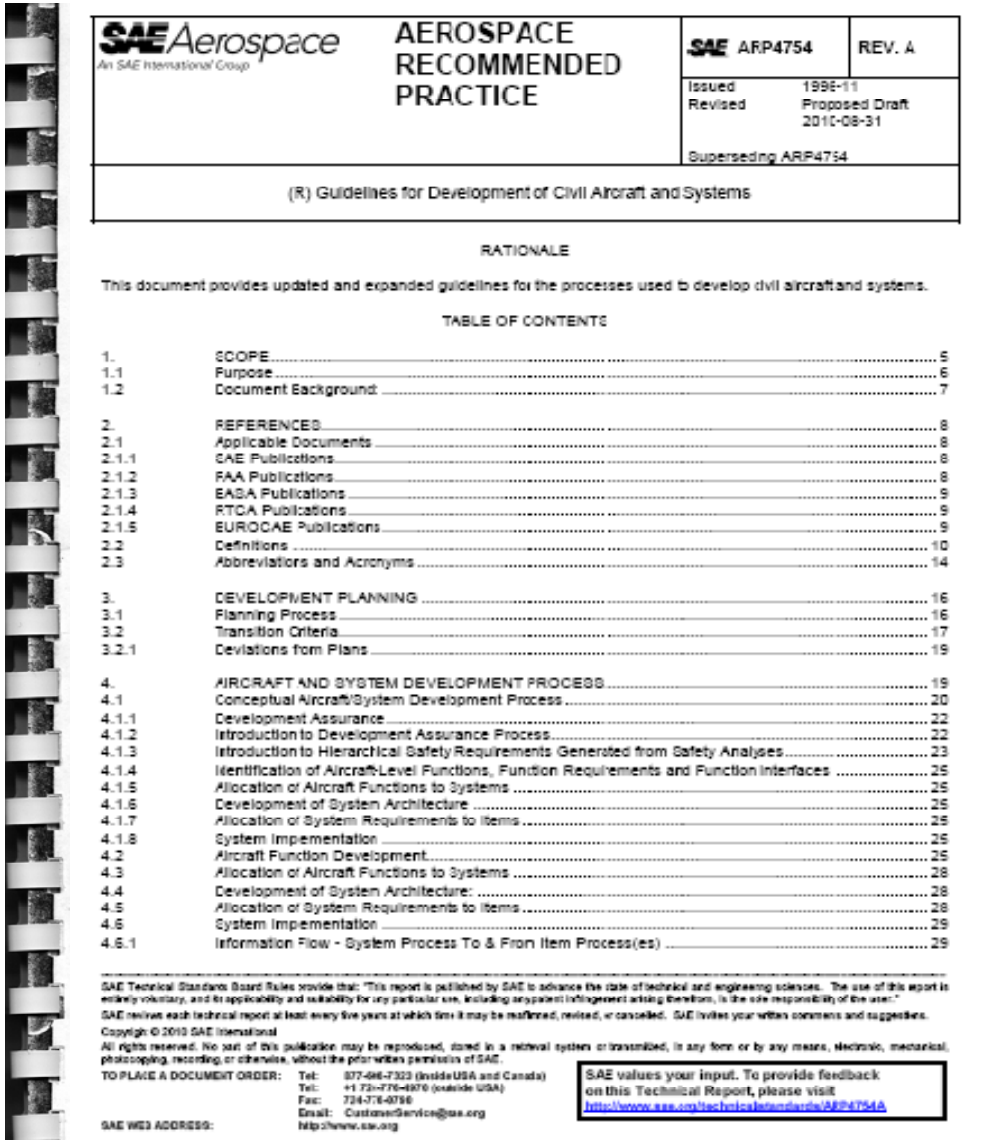
INTRODUCTION

Established industry practices and associated regulatory requirements have developed over many years to ensure that safety standards are maintained in civil aircraft. The increasing integration and complexity of aircraft electronic systems has led to a need to review existing procedures and provide additional guidance to ensure that the proper operation and safety of future systems and system changes can be assured.

TABLE OF CONTENTS

# ARP4754A Overview

- Structured Development Process
- Requirements Definition
- Introduction of **Functional & Item** Development Assurance Levels
- Validation of Requirements
- Implementation Verification
- Tied to Safety Methodology (ARP4761)



SAE Aerospace
An SAE International Group

AEROSPACE RECOMMENDED PRACTICE

SAE ARP4754 REV. A

Issued 1996-11
Revised Proposed Draft 2010-08-31

Superseding ARP4754

(R) Guidelines for Development of Civil Aircraft and Systems

RATIONALE

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

TABLE OF CONTENTS






TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org


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

# ARP4754 / 4754A Overview

- The Recommended Process has its roots in Systems Engineering but with an emphasis on Safety
- Calls for a Structured Process which includes Requirements Definition, Requirements Validation and Design Implementation Verification
- Describes a Top Down Development Process using Safety as the Rationale
- Increases the Role and Responsibilities of Systems Engineering at each Hierarchical Level
- Calls for improved process integration between Systems Engineering and Safety Engineering
- Difficult to apply to derivative airplane / system developments based on Minor changes to existing systems
- Results in increased exposure of Development Plans to Regulators, but allows internal processes to be used

# ARP4761

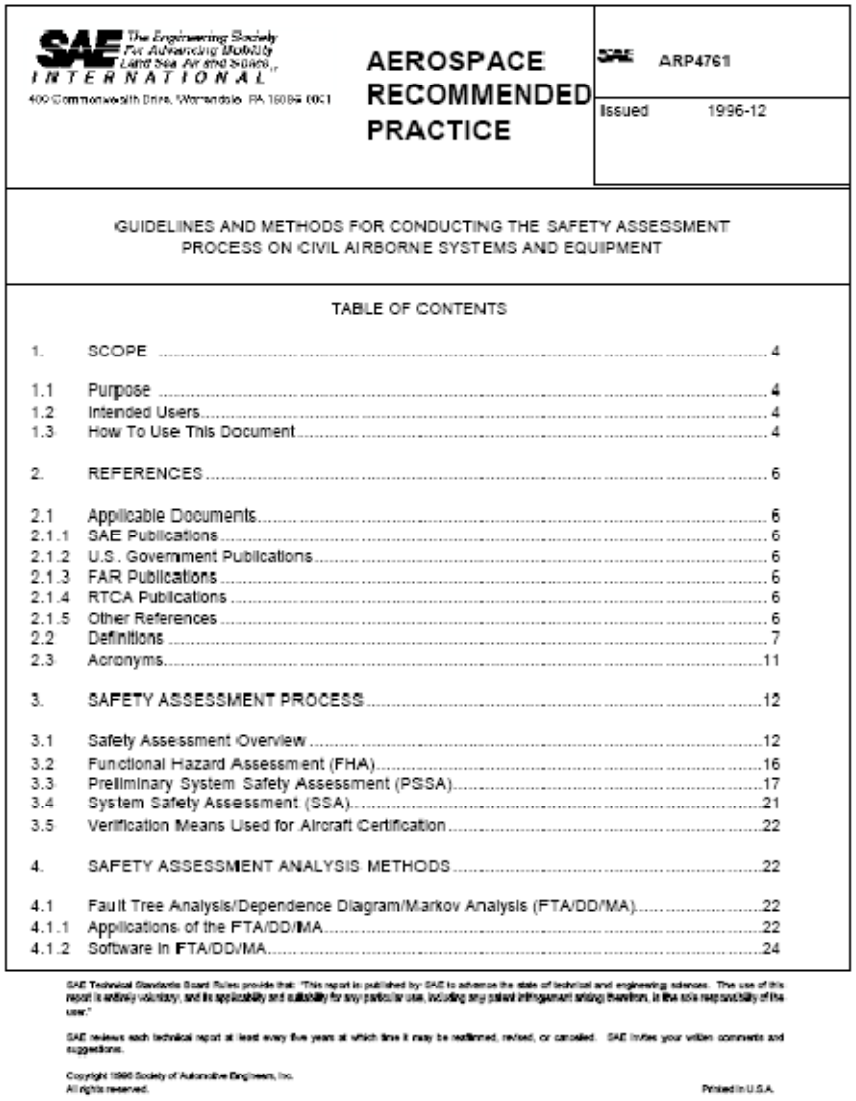
"Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"

# ARP4761 / 4761A Overview

- Aerospace Recommended Practice for performing safety assessments for civil aircraft
- Guidelines for conducting industry accepted safety assessments consisting of:
  - Functional Hazard Assessment (FHA)
  - Preliminary Safety Assessment (PSSA)
  - System Safety Assessment (SSA)
- SAE S-18 authored document in 1996
- SAE S-18 revising to ARP4761A in 2012

# ARP4761/4761A Background

- Chapter 6 of ARP4754 (5.1 of ARP4754A) tells “what to do” for airplane safety assessment
- ARP4761 tells “how to do it”
- ARP4754 & 4761 (and revisions) were developed in parallel
- Effort coordinated
  - Definitions consistent
  - Are to be used together



SAE INTERNATIONAL
400 Commonwealth Drive, Warrendale, PA 15096-0001

**AEROSPACE RECOMMENDED PRACTICE**

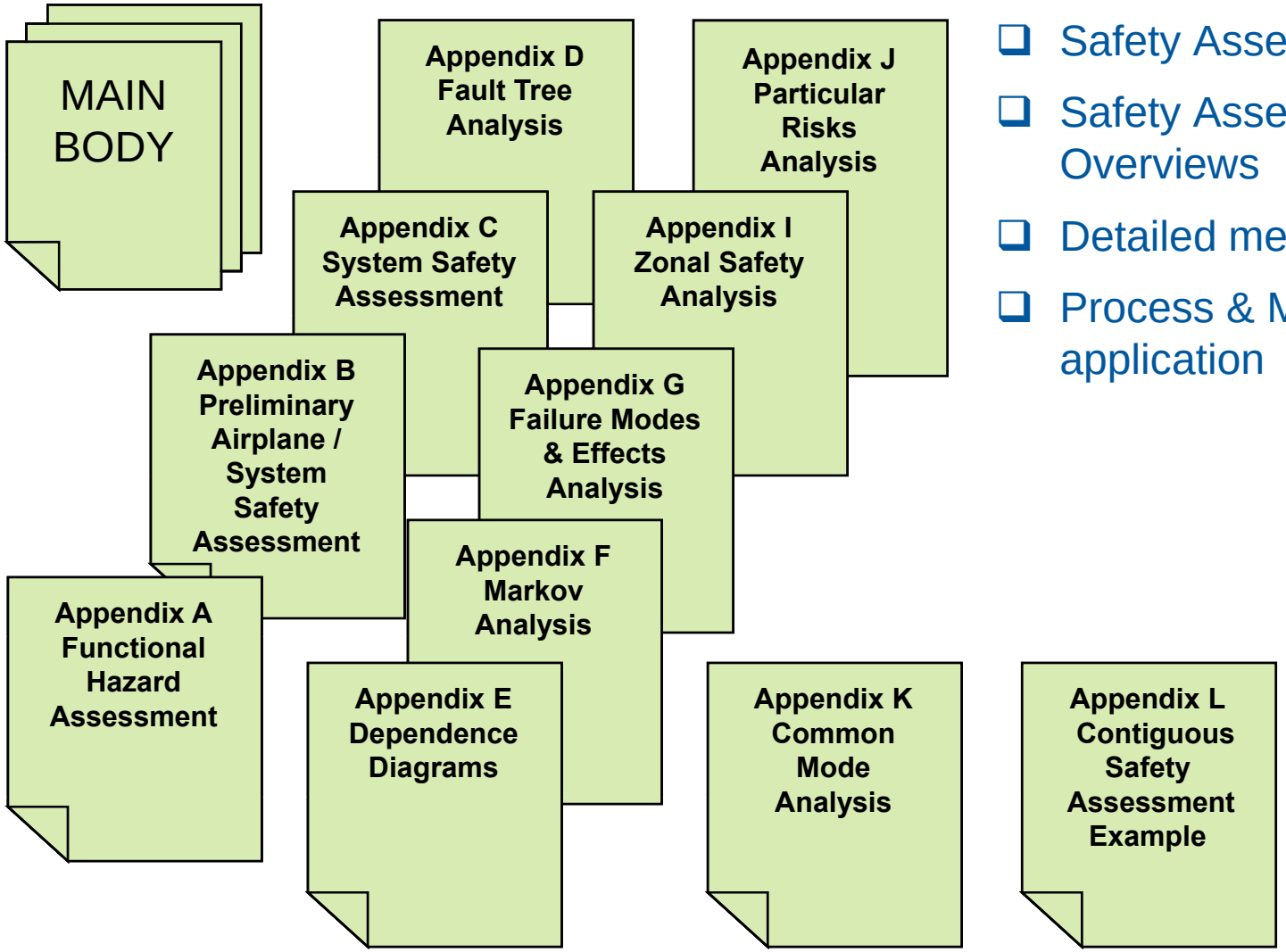
SAE ARP4761

Issued 1996-12

GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT

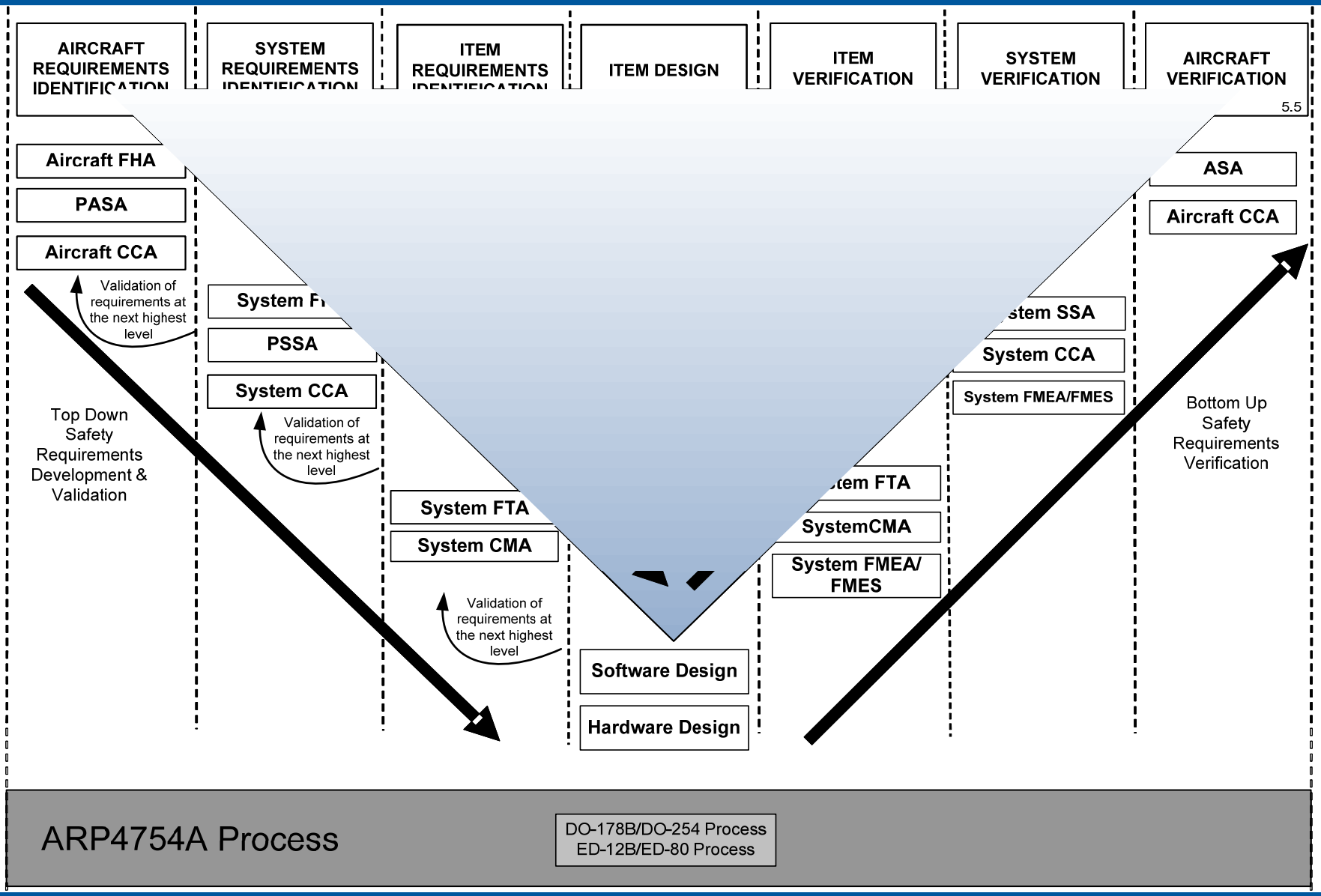
TABLE OF CONTENTS

# ARP4761/4761A Document Organization




- Safety Assessment Process
- Safety Assessment Methods Overviews
- Detailed method guidelines
- Process & Methods application

# Systems Development – Safety Interrelationship



# ARP5150 Overview

## ARP 5150

"Safety Assessment of Aircraft in Commercial Service"

# ARP5150 Overview

- Developed by SAE S-18 committee
- Published in Dec 2003
- Ongoing safety assessment process for transport commercial airplanes
  - Guidelines
  - Methods
  - Tools
- Systematic process to measure and monitor safety elements to help determine safety priorities and focus resources

# ARP 4754

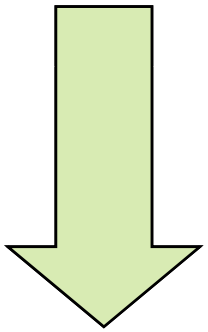
"Certification Considerations for Highly-Integrated or Complex Aircraft Systems"

# ARP 4754A

"Guidelines for Development of Civil Aircraft and Systems"

# System Development (ARP4754)

- "Certification Considerations for Highly-Integrated or Complex Aircraft Systems"
  - circa 1996



  - Eight years of international revision support
    - SAE S-18 (~40 members)
    - EUROCAE WG-63 (~20 members)

- "Guidelines for Development of Civil Aircraft and Systems"
  - circa 2010 (publication pending by SAE/EUROCAE)

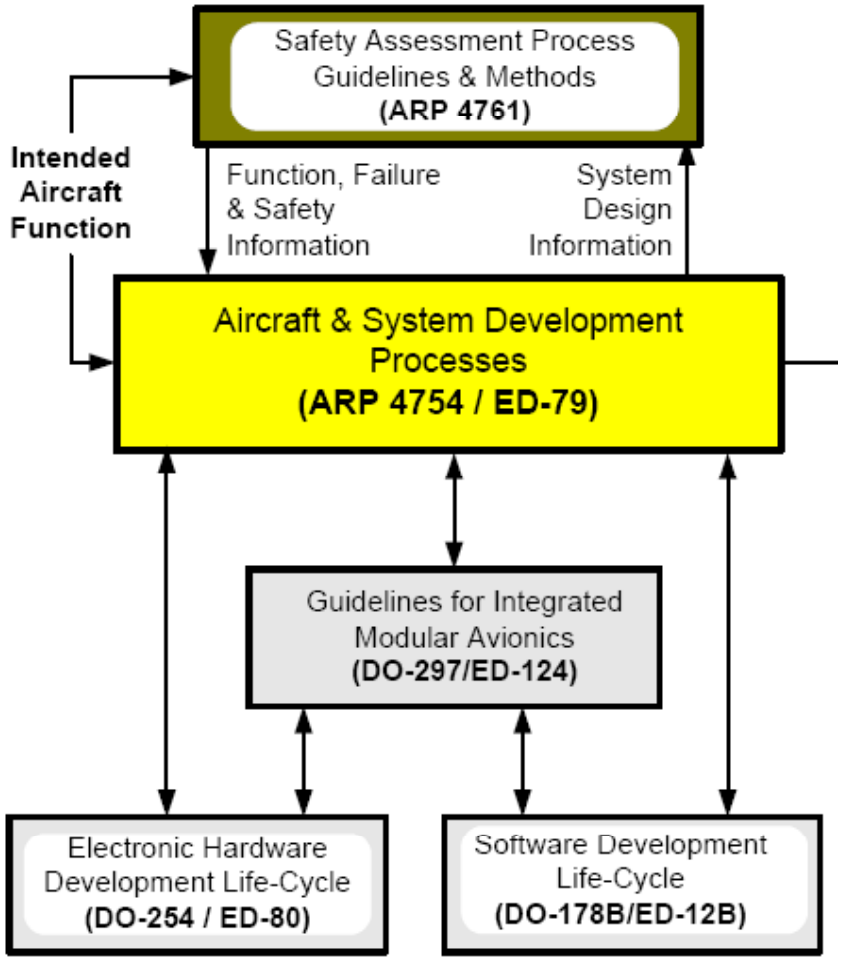
# ARP4754A Book Outline

## Table of Contents

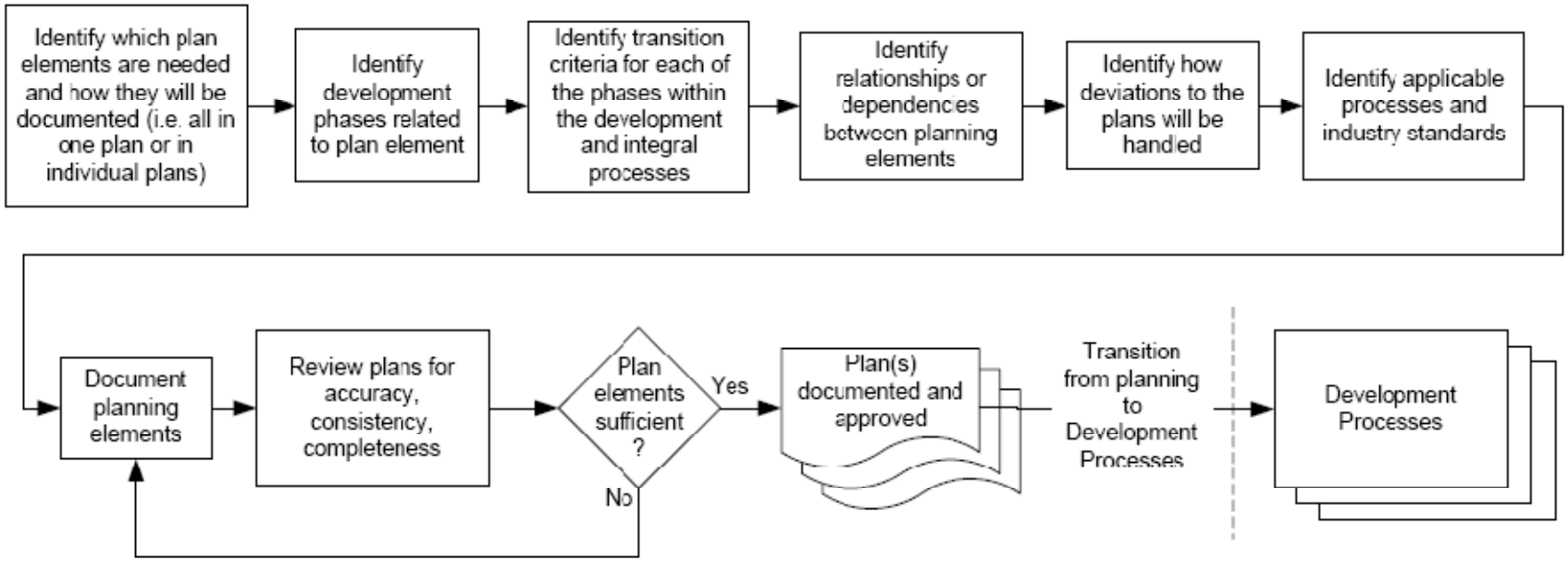
1. Scope
2. References
3. Development Planning
4. Aircraft and System Development Process
5. Integral Processes
6. Modifications to Aircraft or Systems
7. Notes

# Multiple Parallel Processes

- Input Is Intended Functions
- Process integral with ARP 4761
- Output is development rigor for HW & SW
- Output Is Functioning System

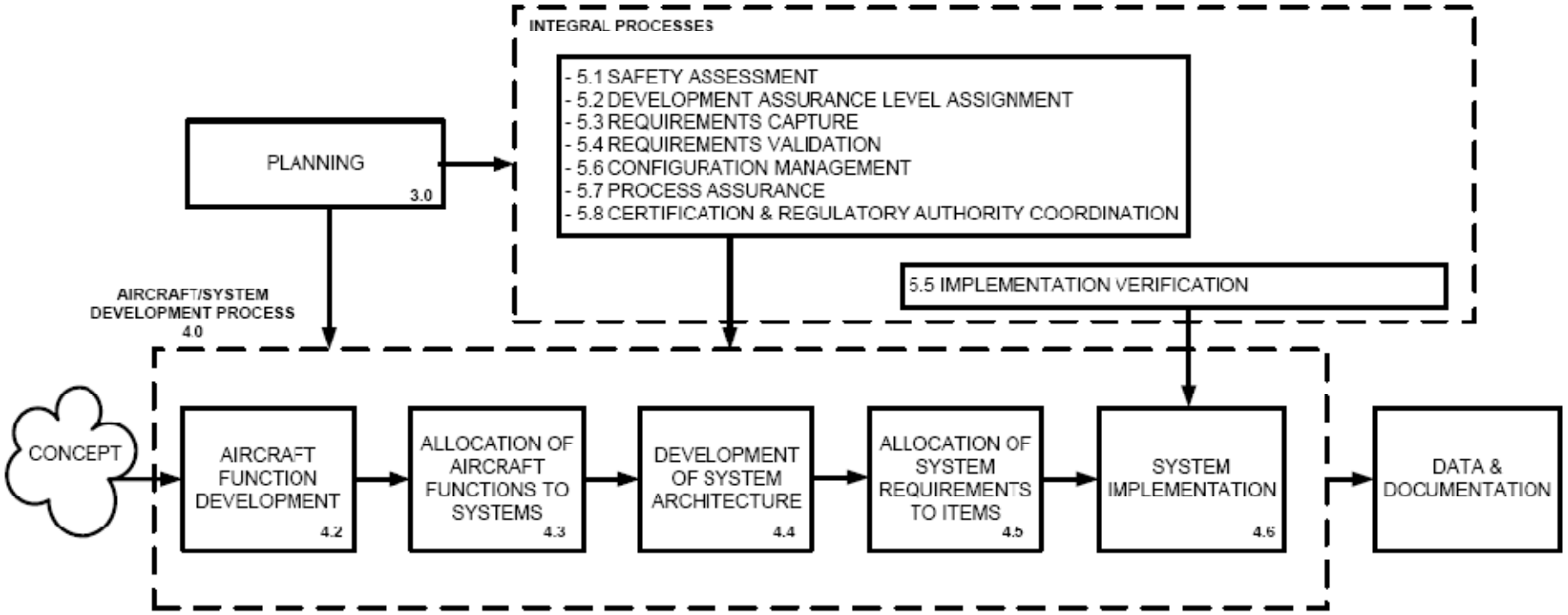


# ARP4754A Planning




- Objective of planning process is to define the means that will be used to produce the aircraft or system.
  - Define the activities used to address the requirements, functional development assurance levels, item development assurance levels.
  - Define the development life cycle including process interrelationships and transition criteria.
  - Define the development standards to be used
  - Define the development life cycle including methods and tools to be used for the activities in each life cycle process.

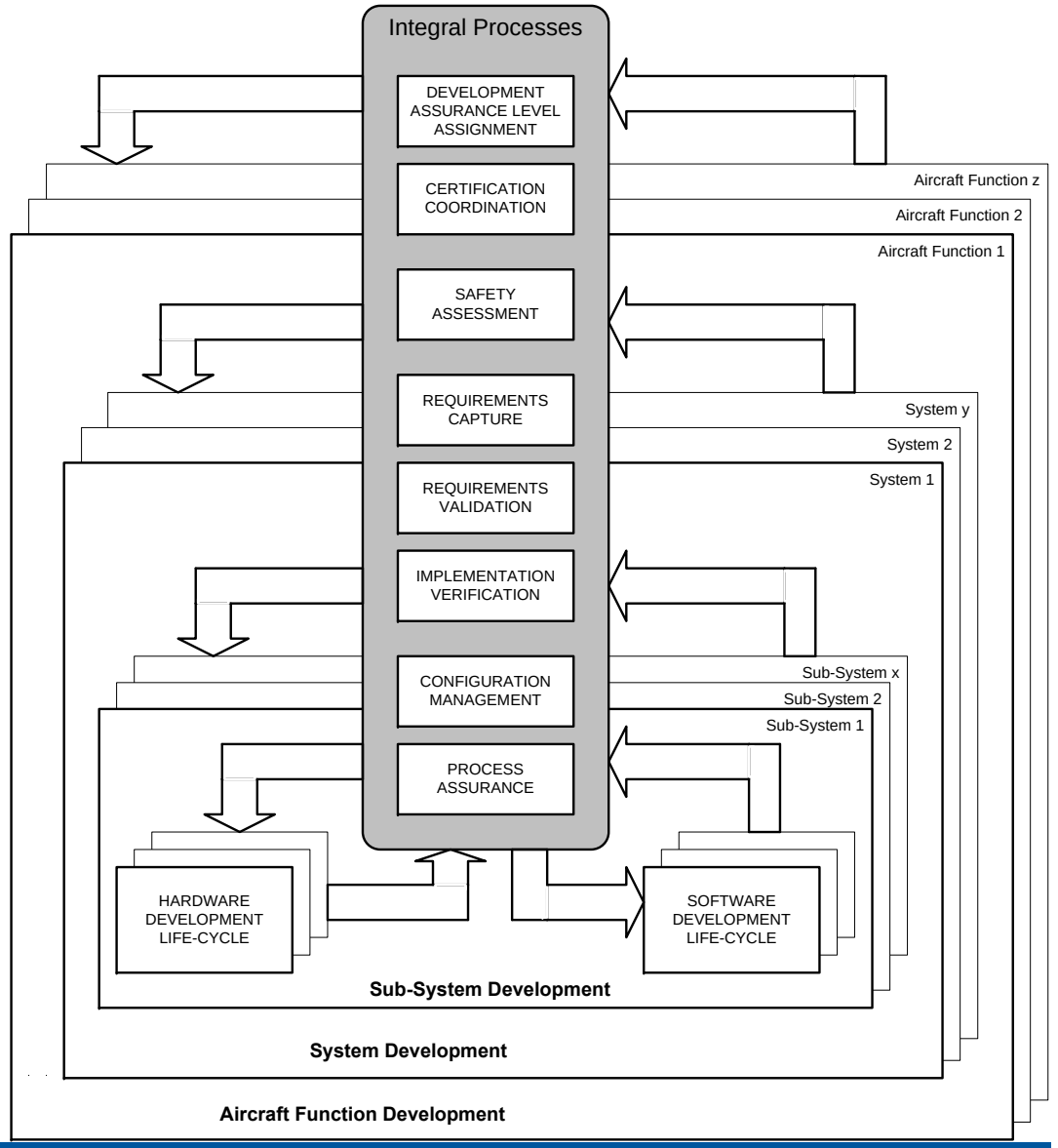
# Aircraft or System Development Process Model




- Generic development process to establish a frame for discussing the process.
- Emphasis is focused on top-down development strategy since it provides the necessary links between safety and system development.
- No organizational structures, preferred methods or processes implied.

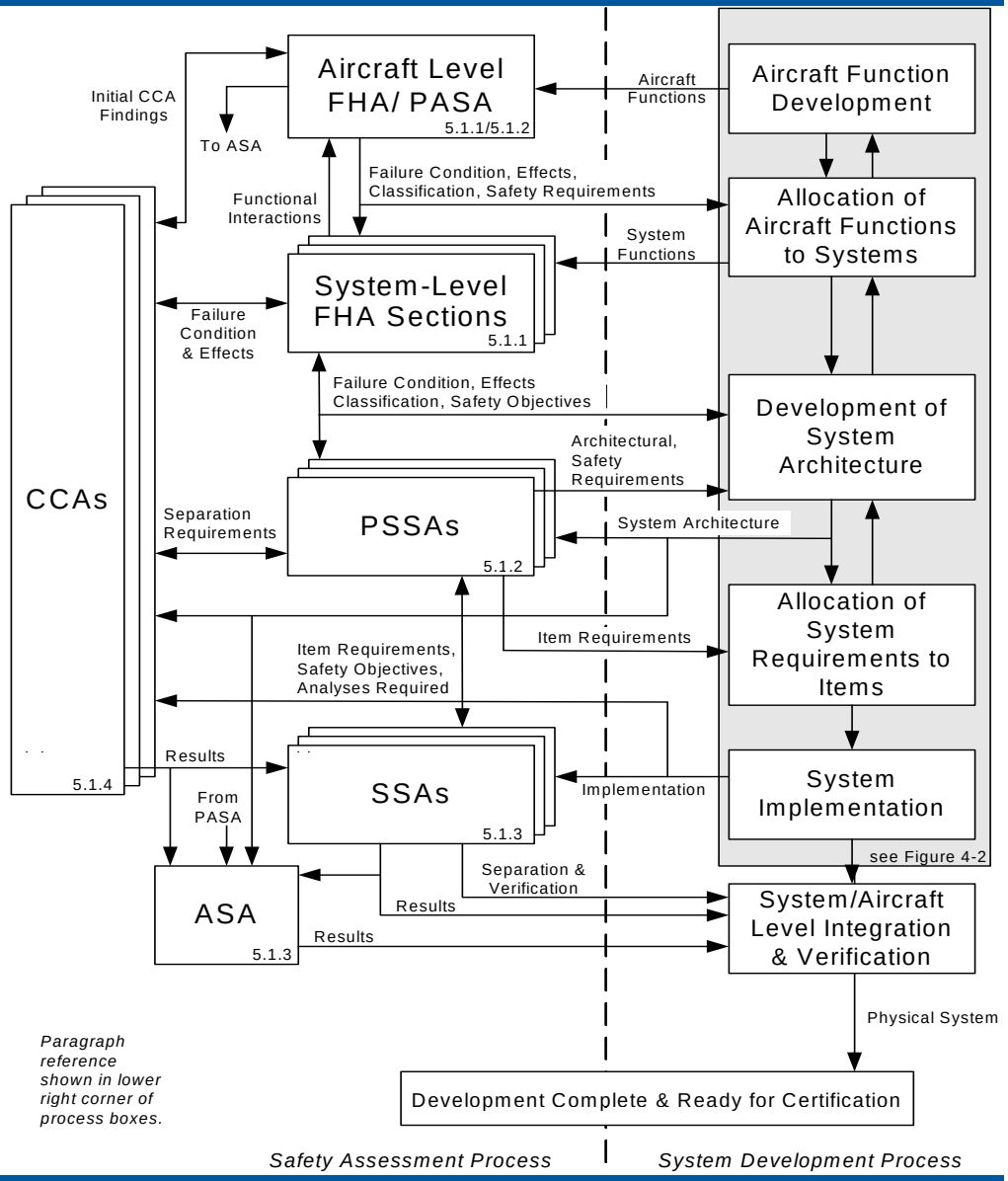
# System Development Process

- Process includes Top-Level Requirements
- Allocation To Systems
- Architecture Development
- Further Allocation To HW/SW (Items)
- System Implementation
- Parallels Safety Assessment Process



# Safety Assessment Process

- Process Includes Airplane Level FHA
- Preliminary Airplane Safety Assessment
- System Level FHAs
- Preliminary System Safety Assessments
- Airplane Safety Assessment
- System Safety Assessments
- Common Cause Assessments
- Parallels System Development Process
- Processes Lead to Certification



# ARP4754 Revision Change Rationale

- ☑ Initial DAL was not always based on rigorous safety analysis
- ☑ Delineation of the architectural containment boundaries were not always properly defined
- ❑ Items are not always wholly contained within the architectural boundary
- ❑ Difficult to delineate the subtleties between “independence” and “dissimilarity”
- ❑ Probabilities have often been improperly linked to development assurance levels
- ❑ No top level development assurance level definition

  - SAE 5 year revision cycle.

# Approach to Assigning Levels

- Existing ARP4754 explicitly addresses system level (with only some mention of airplane level)
  - Level assignment/reduction applied to items defined from the at the system architecture
- Revised ARP4754A addresses airplane & system levels explicitly
  - FDAL is effectively new for the revised ARP and should be assigned to the systems from the aircraft architecture using the PASA
  - IDAL assignment should be similar to existing ARP
- Discusses “independence” rather than “dissimilarity”
- Emphasize assigning levels rather than reducing levels
  - “Reduction” is a misnomer, but arises when a function has a level lower than its parent function

# Independence Attributes

- Functional: different functions & requirements
  - Common requirements errors
  - Requirements interpretation errors
- Design: different designs
  - Hardware component errors
  - Software language or HDL errors
  - Requirements interpretation errors
  - Quality errors
- Other: do not influence FDAL/IDAL assignment
  - Physical
    - Redundancy, installation
  - Process
    - Between independent designs or functions
    - Between development/design vs. verification/validation

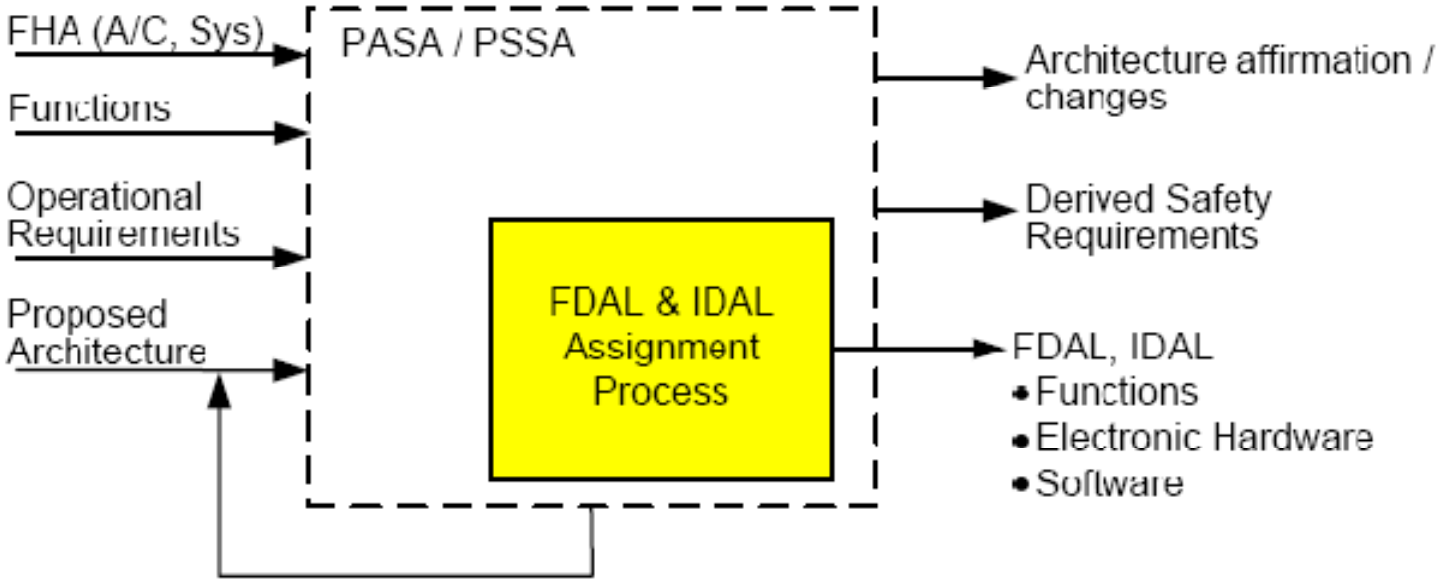
# Independence Attributes

- FDAL considers the functional independence of the aircraft (or system) functions.
- IDAL considers the design independence of items
- Once the IDALs are assigned to items, they should be fed back to the system and aircraft processes to ensure that no common mode is inadvertently introduced that violates any claimed functional independence.
- The assertion of independence needs to be substantiated & address potential common modes.
- One type of independence does not necessarily imply the other.

# FDAL/IDAL Assignment Process

- Development Assurance Level (FDAL)
  - Assigned per Aircraft Level FHA & PASA
  - Validated per Aircraft and System level Safety Analysis
- Design Assurance Level (IDAL)
  - Assigned per System Level FHAs & PSSAs
  - Validated per System level Safety Analysis and Component Functional Failure Analysis
  - Must trace up to upper level functions' FDAL so that it is not decomposed/assigned more than once (e.g. keeps 4 Level D items from assuring a Level A function).
  - Non-complex items that are fully and deterministically tested and analyzed may be considered Level A

# FDAL / IDAL Assignment



# Development Assurance Levels

**PSSA evaluates most severe top-level Failure Condition Classification**

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

Assigned FDAL sets the rigor of the process

# FDAL & IDAL Assignment Process

- Top down process that starts with a Failure Condition Classification for a Function.
- To be applied when developing new functions or systems.
- Allows for consideration of independence attributes to assign development assurance levels.

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

NOTE 1: When a FFS has a single Member and the mitigation strategy for systematic errors is to be FDAL A alone, then the applicant may be required to substantiate that the development process for that Member has sufficient independent validation/verification activities, techniques and completion criteria to ensure that potential development error(s) having a catastrophic effect have been removed or mitigated.

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

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

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

# FDAL/IDAL Results

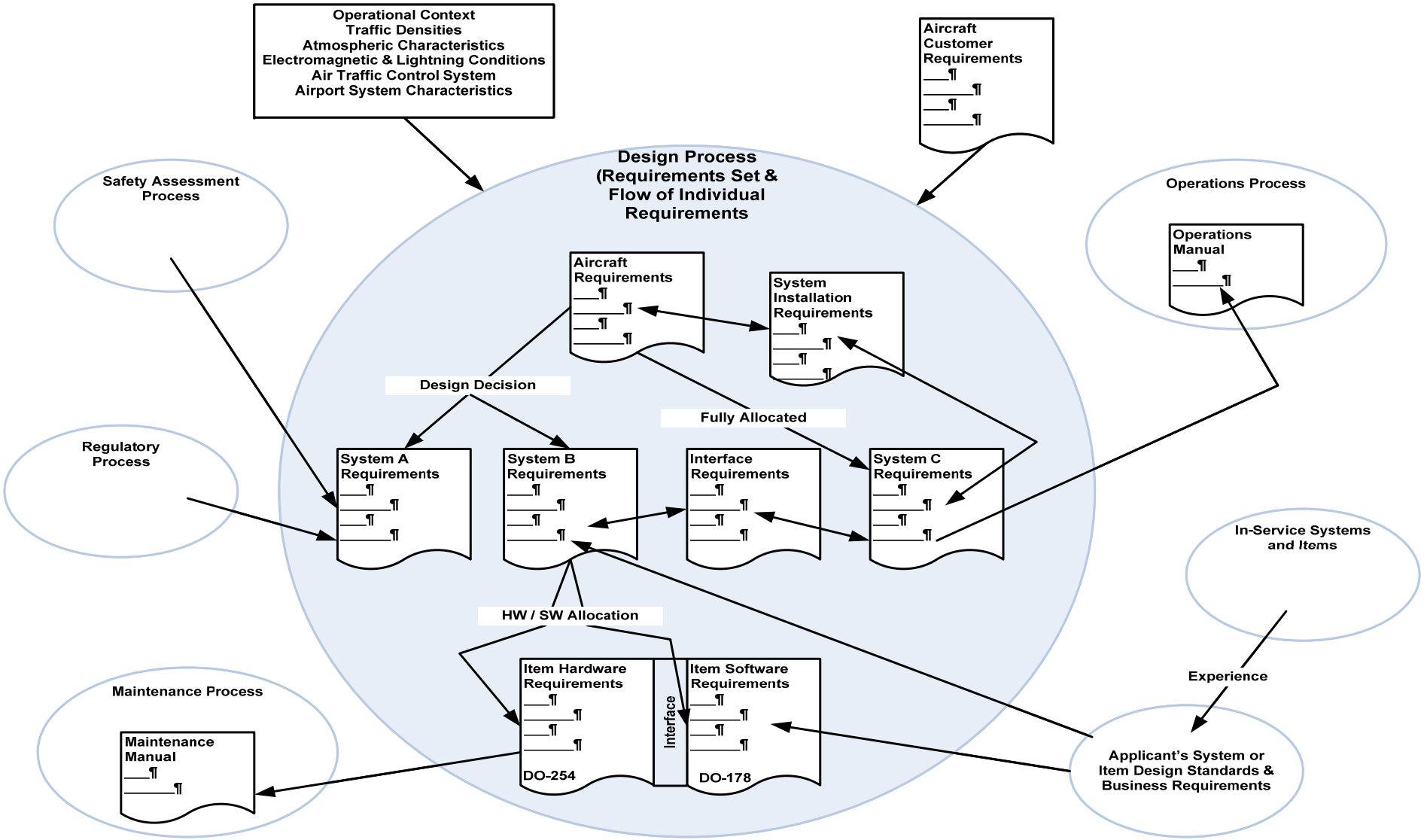
- FDAL and IDAL are based on safety analyses; do it early (and often)!
- PASA and PSSA can be used to derive requirements including FDAL/IDAL
- Development Assurance can be an enabler to focus resources on the aspects that matter most.
- The IDAL assigned per the ARP4754A process is used in the software or hardware processes.
  - Coordinated with SC-205 generation of DO-178C

# Integral Processes

- Requirements Capture
- Requirements Validation
- Requirements Verification
- Configuration Management*
- Process Assurance*
- Regulatory Liaison*

* Omitted for brevity

# Integral Process – Requirements Capture



# ARP4754A Requirements Capture

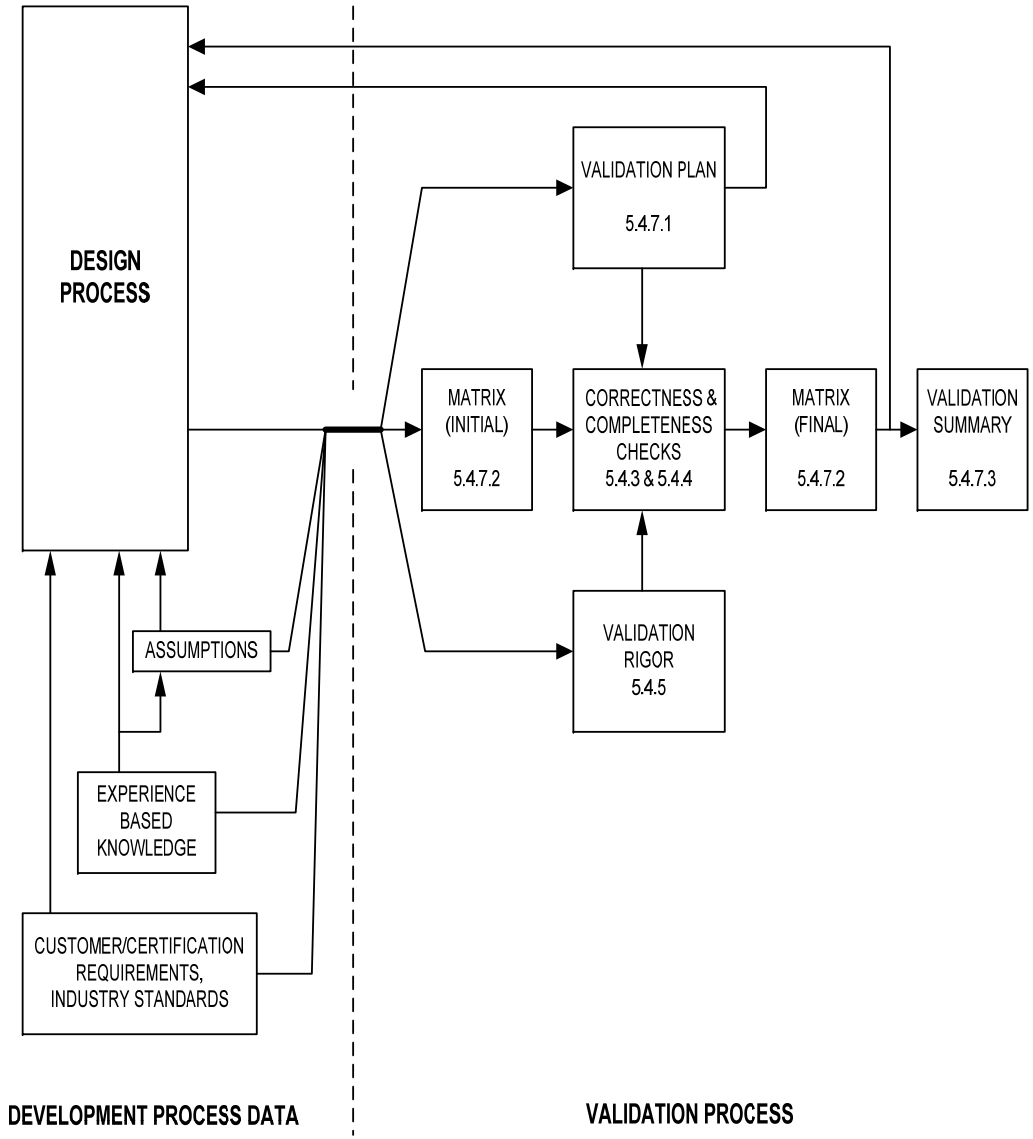
- Common basis for integral processes.
- Requirements may be captured in many different formats but standards should be developed to establish consistency across the requirement set and ensure accurate communication across the development team;
  - Textural
  - Graphical

# Integral Process – Requirements Validation

- Process for ensuring that the specified requirements are sufficiently correct and complete to meet the needs.
  - "Are we building the right thing?"
- Planned activities documented in the Validation Plan
- Requirements evaluated against various attributes -
  - Is the requirement correctly stated?
  - Is the requirement necessary for the set of requirements to be complete?
  - Is the requirement set better suited to be contained in a single requirement?
  - Does the requirement set correctly reflect the safety analyses?

# Requirements Validation

- Requirements Validation Includes a Validation Plan
- Includes an Initial Validation Matrix
- Includes the Validation Activities
- Includes a Validation Matrix
- Completed with the Validation Summary Report



# Validation Rigor

- **The level of validation rigor for the aircraft or system is determined by the assigned FDAL and IDAL.**

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

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

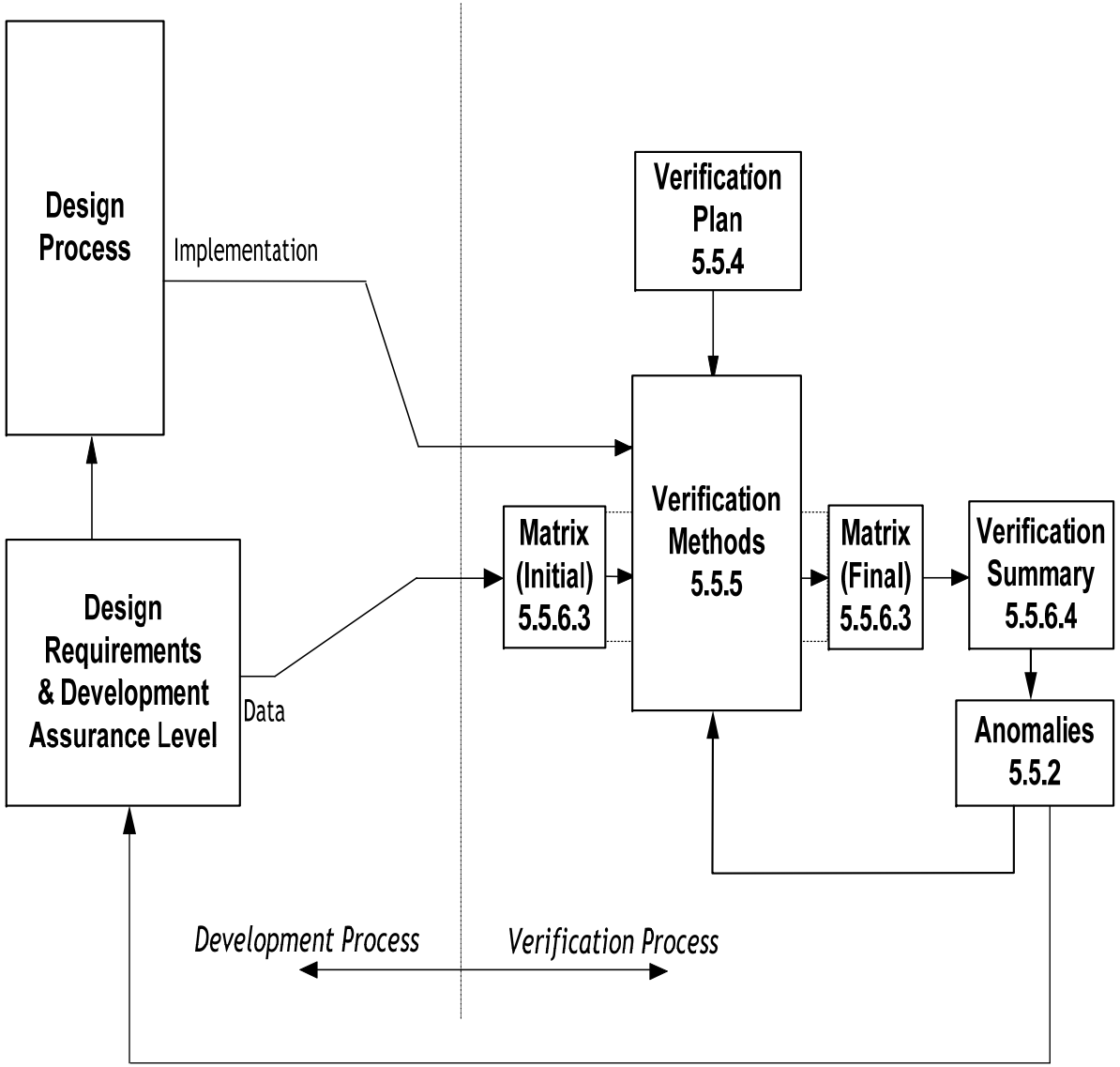
For each requirement, a combination of the recommended and allowable methods necessary to establish the required confidence in the validation of that requirement, should be identified and then applied.

# Integral Process – Requirements Verification

- Process to ascertain that the implementation meets the specified requirements.
  - "Have we built the right thing?"
- Planned activities documented in the Verification Plan
- Requirements evaluated using various methods -
  - Inspection, Reviews
  - Analyses
  - Tests
  - Service Experience

# Integral Process – Requirements Verification

- Implementation Verification Includes a Verification Plan
- Includes an Initial Verification Matrix
- Includes the Verification Activities
- Includes a Final Verification Matrix
- Completed with the Verification Summary



# Verification Rigor

- **The level of verification rigor for the aircraft or system is determined by the assigned FDAL and IDAL.**

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

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

# ARP4754A

- “Updated and expanded guidelines for the processes used to develop civil aircraft and systems.”
- Layered development rigor that is now applied at the aircraft level.
- Principle based development rigor assignment (FDAL & IDAL)
- Reorganized to improve process and description flow.

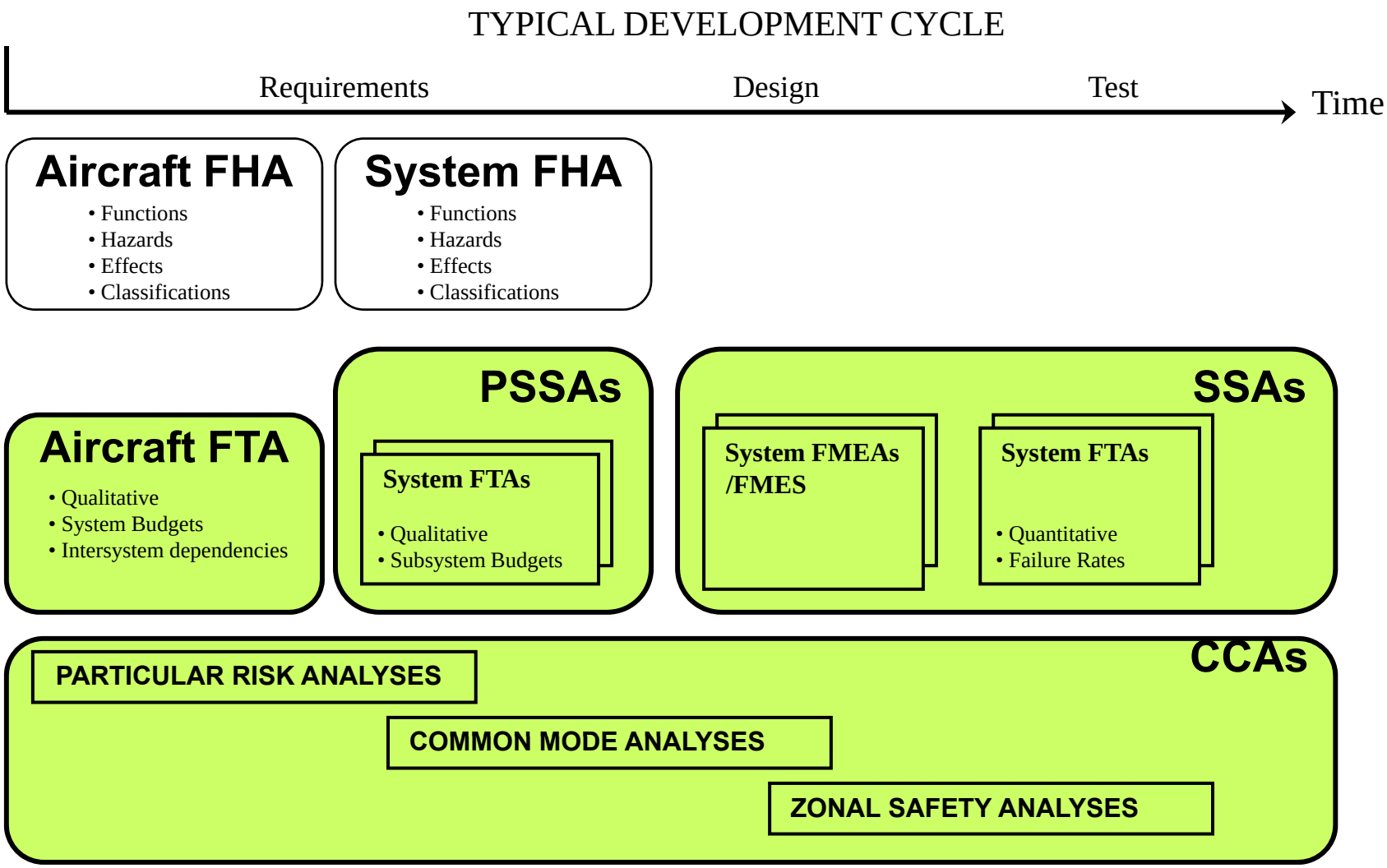
# ARP4761

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

# ARP4761 Outline/Contents

- Functional Hazard Assessment
  - Aircraft
  - System
- Safety Assessments
  - Preliminary Aircraft Safety Assessment
  - Preliminary System Safety Assessment
  - Aircraft Safety Assessment
  - System Safety Assessment
- Methods
  - Fault Tree Analysis
  - Dependency Diagrams
  - Markov Analysis
  - Failure Modes & Effects Analysis
- Common Cause Analysis
  - Particular Risk Analysis
  - Common Mode Analysis
  - Zonal Safety Analysis

# Safety Assessment Process Overview



# Functional Hazard Assessments

- Airplane FHA
  - Qualitative assessment which identifies & classifies the failure conditions and their severity rationale associated with aircraft level functions.
- System Level FHA
  - Qualitative assessment which considers single or combination of system failures that affect an aircraft function and becomes the starting point for generation and allocation of safety requirements.

# System Safety Assessments

- PSSA
  - An iterative analysis which evaluates a proposed implementation to derive and capture system & item safety requirements, protective strategies and complete failure conditions list.
- SSA
  - A systematic & integrated analysis which verifies that the implemented design meets both qualitative and quantitative safety requirements.

# Safety Assessment Methods

- Fault Tree Analysis / Dependence Diagrams / Markov Analysis
  - Top down analysis techniques to establish failure model associated with FHA failure condition.
- Failure Modes & Effects Analysis
  - Bottoms up method of identifying failure modes of a system, item or function.
  - Failure Modes & Effects Summary
    - Grouping of single failure modes which produce the same failure effect.

# Common Cause Analyses

- Provide tools to verify independence between functions, systems, items
- Identifies individual failure modes or external events which can lead to catastrophic or hazardous/severe major failure conditions.
- Common Cause Analysis Types
  - Particular Risks Analysis (PRA)
  - Zonal Safety Analysis (ZSA)
  - Common Mode Analysis (CMA)

# Particular Risk Analysis

- Focus is on Airplane Architectural definition to provide mitigation for identified internal and external threats
  - Accomplished through a cross-functional skill team
- Internal and external threats are identified:
  - Impact of Objects external to the airplane
  - Includes Bird strike
  - Impact of Objects that are part of the airplane, but not part of the system being identified
    - Uncontained Rotating Parts
      - Rotor burst
      - Flailing shaft
    - Tire and Wheel Threats

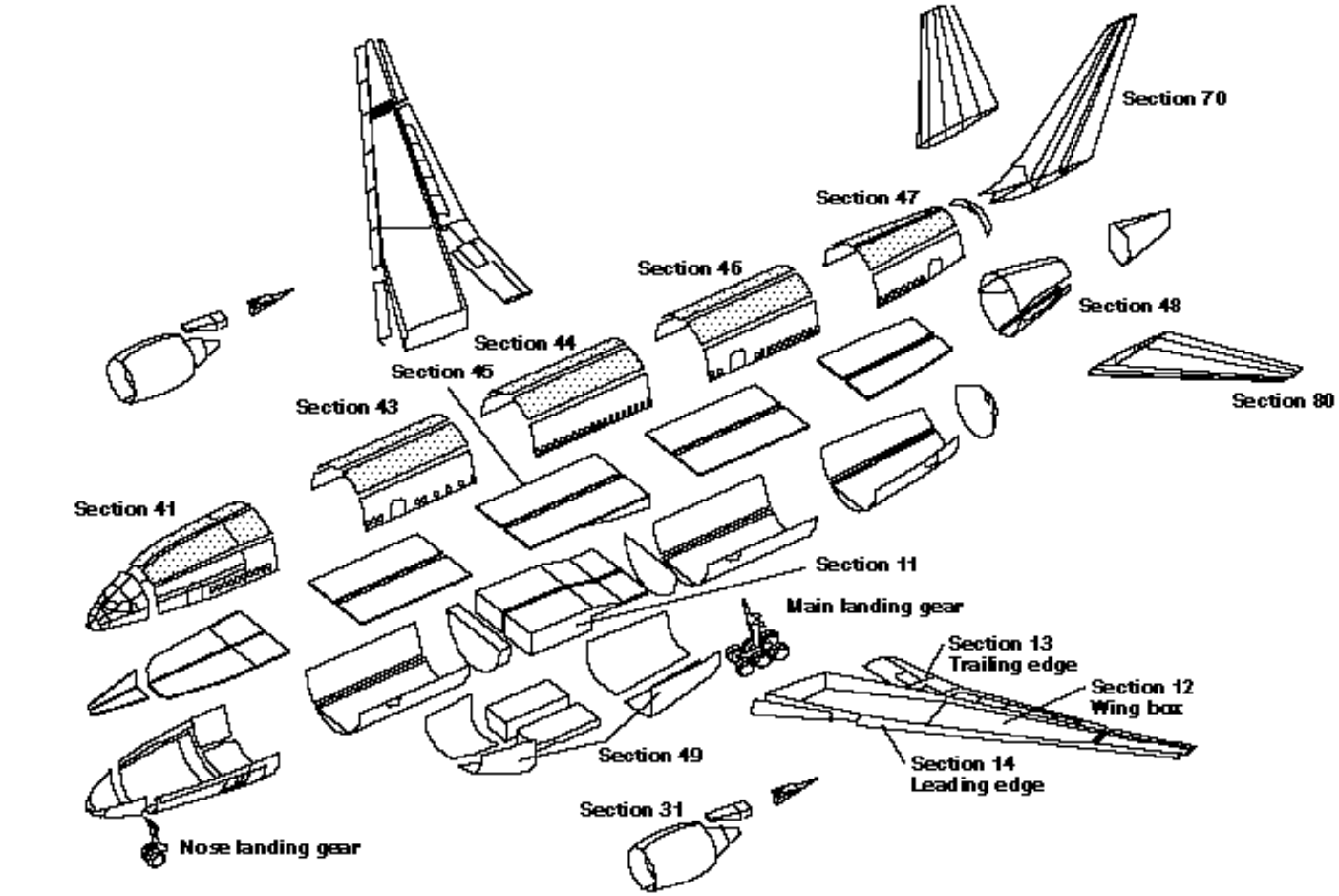
# Particular Risk Analysis (continued)

- Particular Risk Analysis internal and external threats identified:
  - Energy Release
  - Fan Blade Out/ Windmilling
  - Fire/Thermal Overheat
  - Fluid Spillage or Leakage
  - Structural Damage
  - Electromagnetic and Weather Threats

# Zonal Safety Analysis

- Objective - Ensure equipment installation meets safety requirements with respect to:
  - Basic Installation
  - Interference between systems
  - Maintenance errors
- ZSA accomplished by a cross-functional Team to evaluate verification activities

# Example of Aircraft Zones




- Crown-ECS–Distribution
- Flight Deck-Flight Deck-Panels & Modules
- Passenger Compartment-Payloads–Linings
- Floors-Elec–Wiring Installation
- E/E Bay-Elec–Panels & Cargo Handling
- Cargo Compartment-Payloads–Systems
- A/C & Mix Bay-ECS–A/C, Temp Control, etc.
- Landing Gear-Mech/Hyd Systems–Landing Gear Actuation
- Wings/Wheel Well-Mech/Hyd Systems–Hydraulic Installation
- Propulsion/APU-Propulsion-Propulsion and APU
- Empennage-Elec–Antenna

# Common Mode Analysis

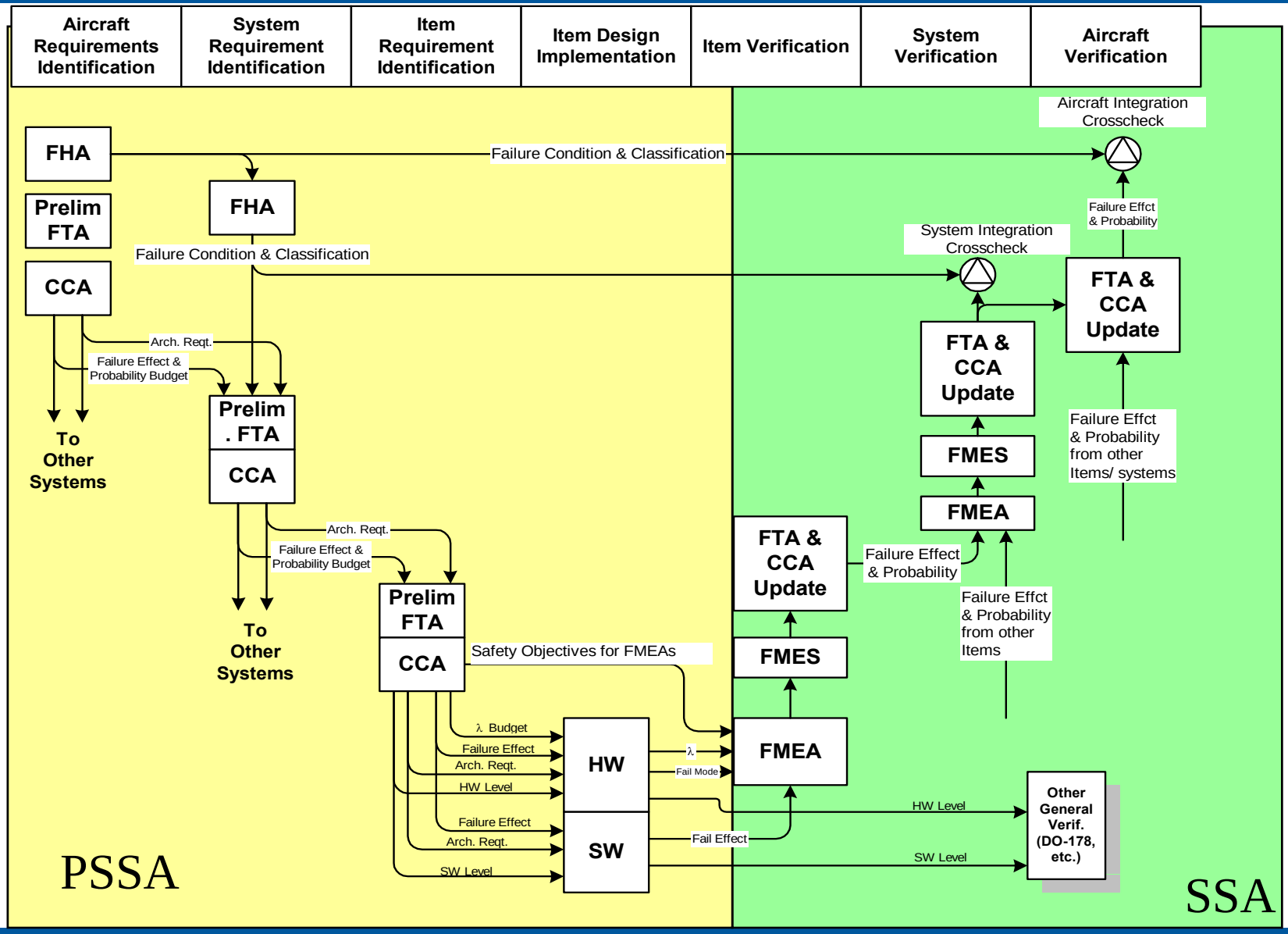
- Primary objective is to verify independence of redundant functions:
  - Verify that ANDed events in FTA/DD/MA are truly independent
  - Some of the effects reviewed include:
    - Design implementation
    - Manufacturing Erros
    - Maintenance Errors
    - Component failures which may defeat redundant design principles

- Qualitative evaluation using checklists

# CMA Checklist Example

| Common Mode Types | Common Mode Sources | Common Modes Failure /Errors |
|---|---|---|
| CONCEPT & DESIGN | | |
| DESIGN ARCHITECTURE | External Sources | Electrical Power Distribution failure<br>Data Source (input) Failure |
| TECHNOLOGY, MATERIAL, EQUIPMENT TYPE | Redundant, Similar Hardware:<br><br>Redundant, Similar Software: | Hardware development errors<br>Component failures<br>Verification tools<br><br>Software development errors<br>Verification tools |
| MANUFACTURING | | |
| MANUFACTURER | Common manufacturer | Common manufacturing error |
| PROCEDURES | Common build procedure | Incorrect manufacturing procedure |
| PROCESS | Common build process | Incorrect manufacturing process |
| INSTALLATION / INTEGRATION & TEST | | |
| FITTER & PROCEDURES | Common installation | Incorrect installation |
| LOCATION & ROUTING | Common installation location | Common environmental failure |
| MAINTENANCE | | |
| STAFF | Common maintenance staff | Error due to inadequately trained staff. |
| PROCEDURES | Common maintenance procedures | Faulty operating procedures, omission of action, etc. |
| TEST | | |
| STAFF | Common test staff | Error due to inadequately trained staff. |
| PROCEDURES | Common test procedures | Faulty test procedures, omission of action, etc. |
| CALIBRATION & RIGGING | | |
| STAFF | N/A | N/A |
| PROCEDURES | Common calibration & rigging procedures | Erroneous operation due to faulty calibration or rigging procedures. |
| ENVIRONMENTAL | | |
| MECHANICAL & THERMAL | Temperature, vibration, pressure, humidity, moisture, etc. | Common erroneous response to environmental conditions.<br>Failure of common cooling function. |
| ELECTRICAL & RADIATION | EME & HIRF | Common erroneous response to EME & HIRF environment. |
| CHEMICAL | Fluid contamination – fuel, coffee, blue water, etc. | Common erroneous response to fluids, chemicals, etc. |
| MISCELLANEOUS | NA | NA |

# Safety Assessment Process Diagram



# ARP5150

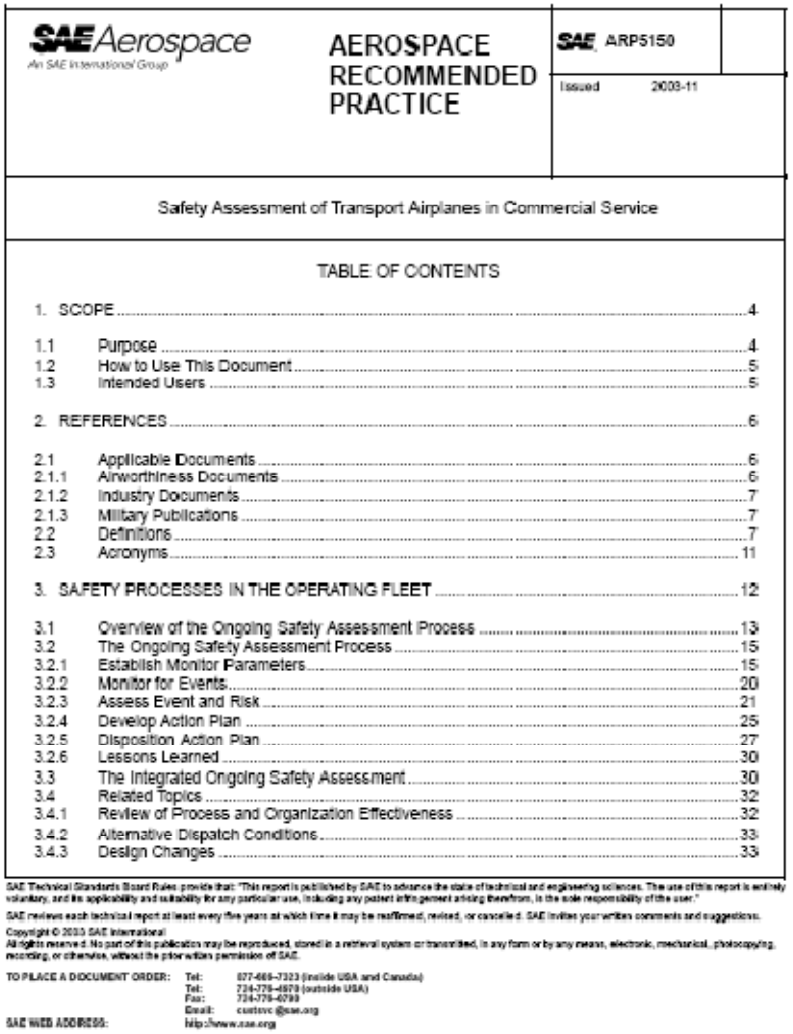
"Safety Assessment of Transport Airplanes in Commercial Service"

# ARP5151

"Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service"

# Monitoring Products in the Field (ARP5150)

- 3 Safety Processes in the Operating Fleet
  - Overview of the ongoing Safety Assessment Process
- 4 In-Service Data
  - Systematic view of safety information
  - Sources of safety data
- 5 Methods & Tools
  - Multiple methods or tools including Root Cause, Weibull, Monte Carlo, & CAAM.
- 6 Being Involved in the Aviation Safety Community



SAE Aerospace
An SAE International Group

AEROSPACE RECOMMENDED PRACTICE

SAE ARP5150

Issued 2003-11

Safety Assessment of Transport Airplanes in Commercial Service

TABLE OF CONTENTS

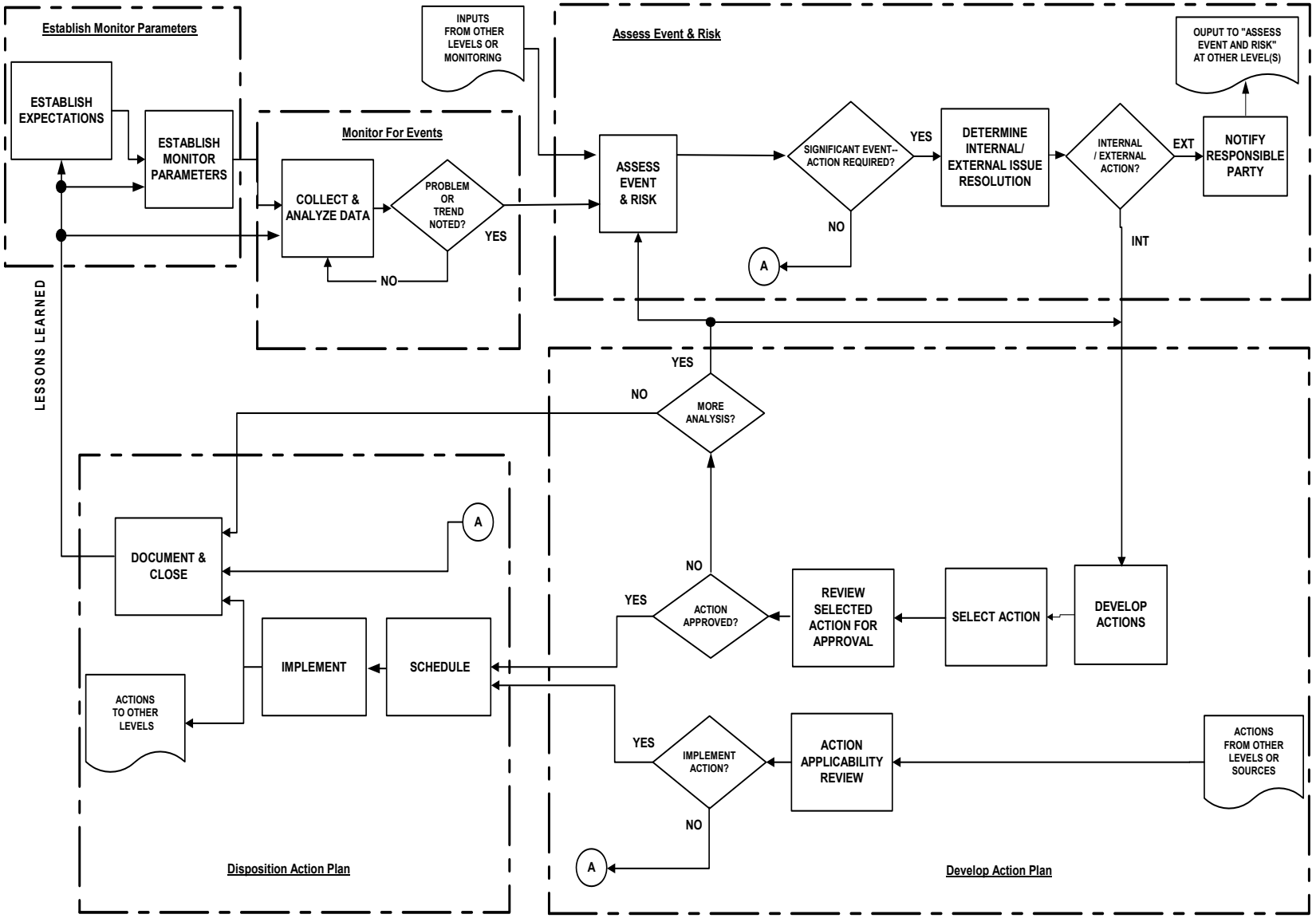




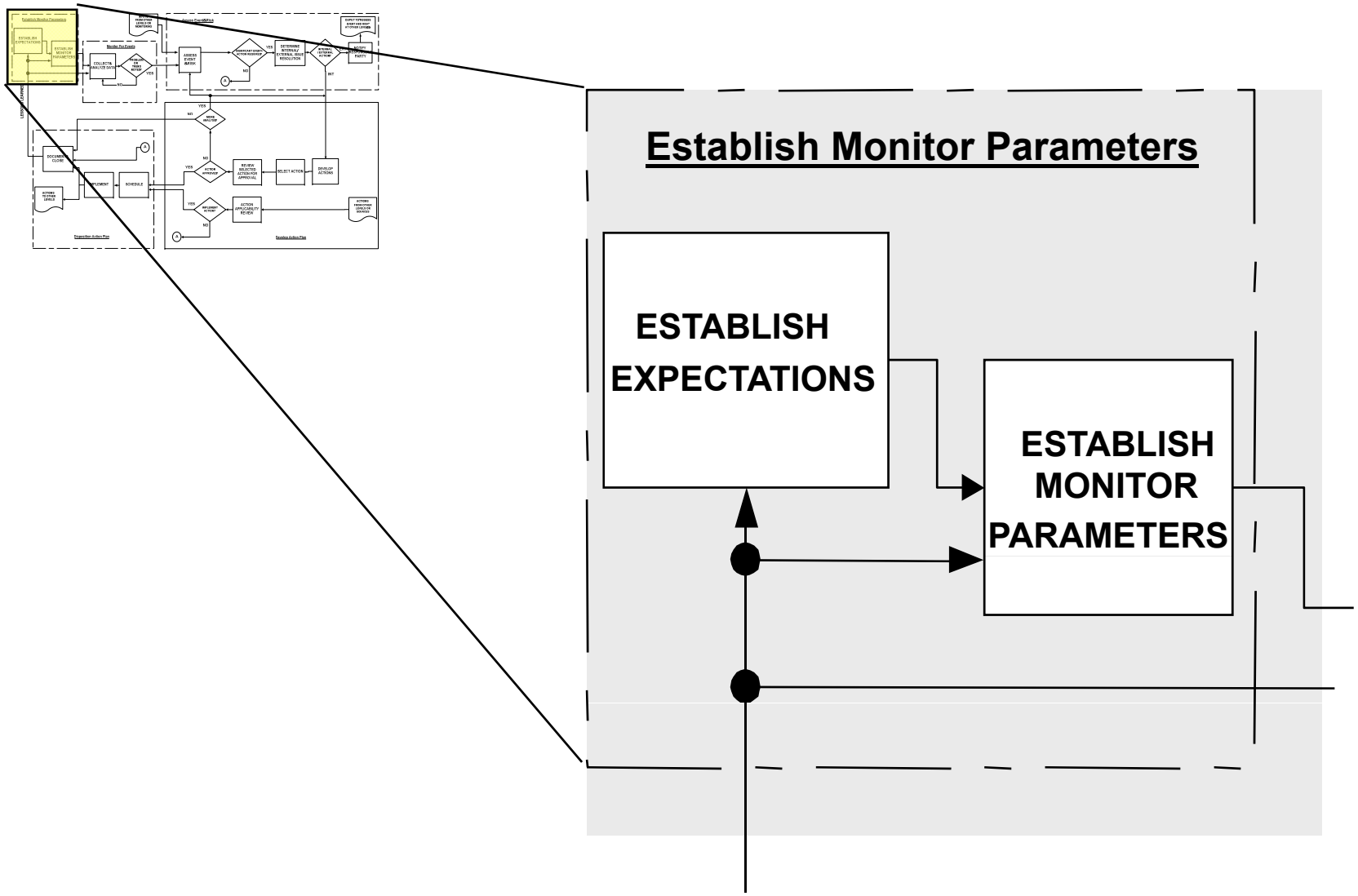

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: custsvc@sae.org
SAE WEB ADDRESS: http://www.sae.org

# Overview of Ongoing Safety Assessment Process

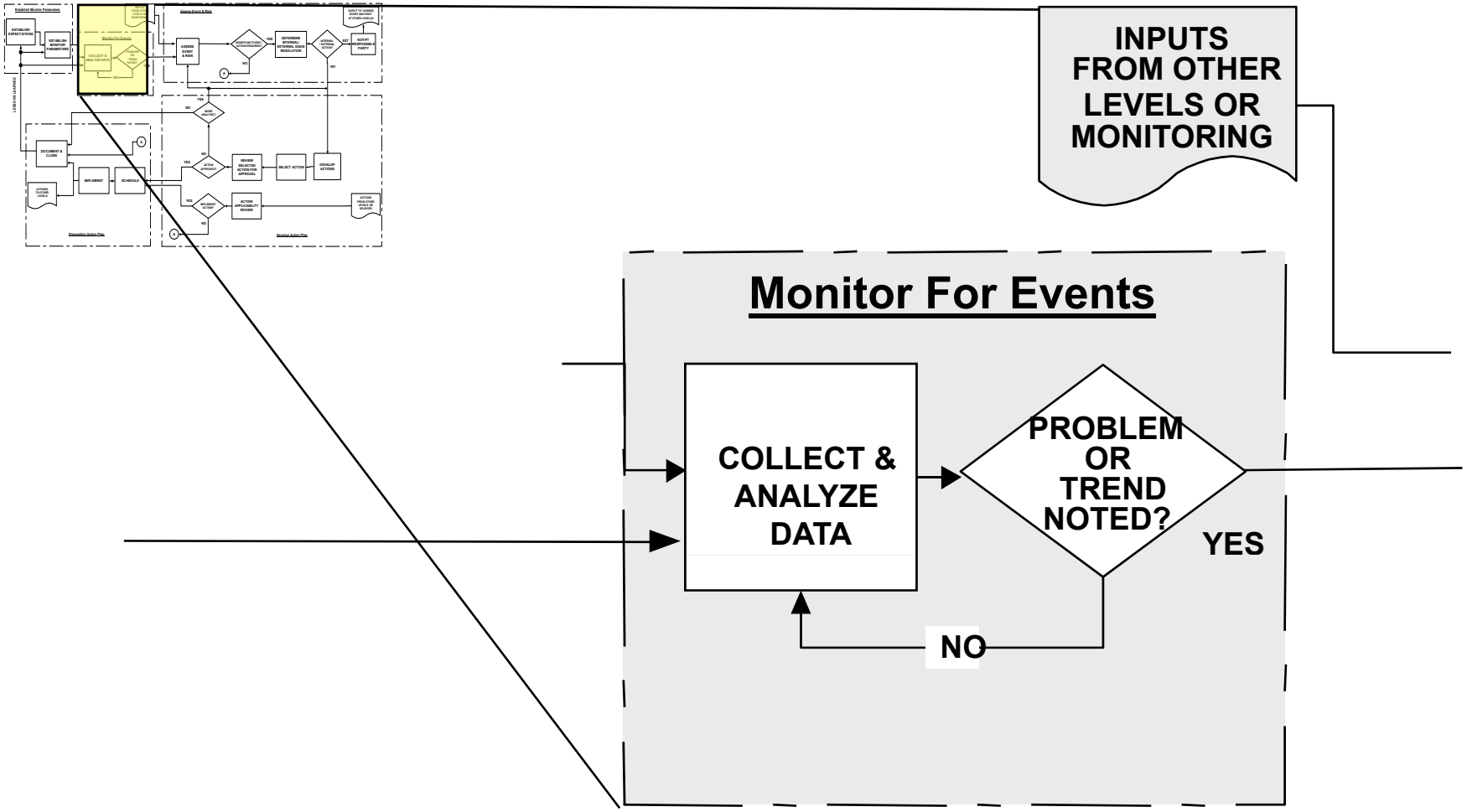
# ARP5150 Detailed Process Flow



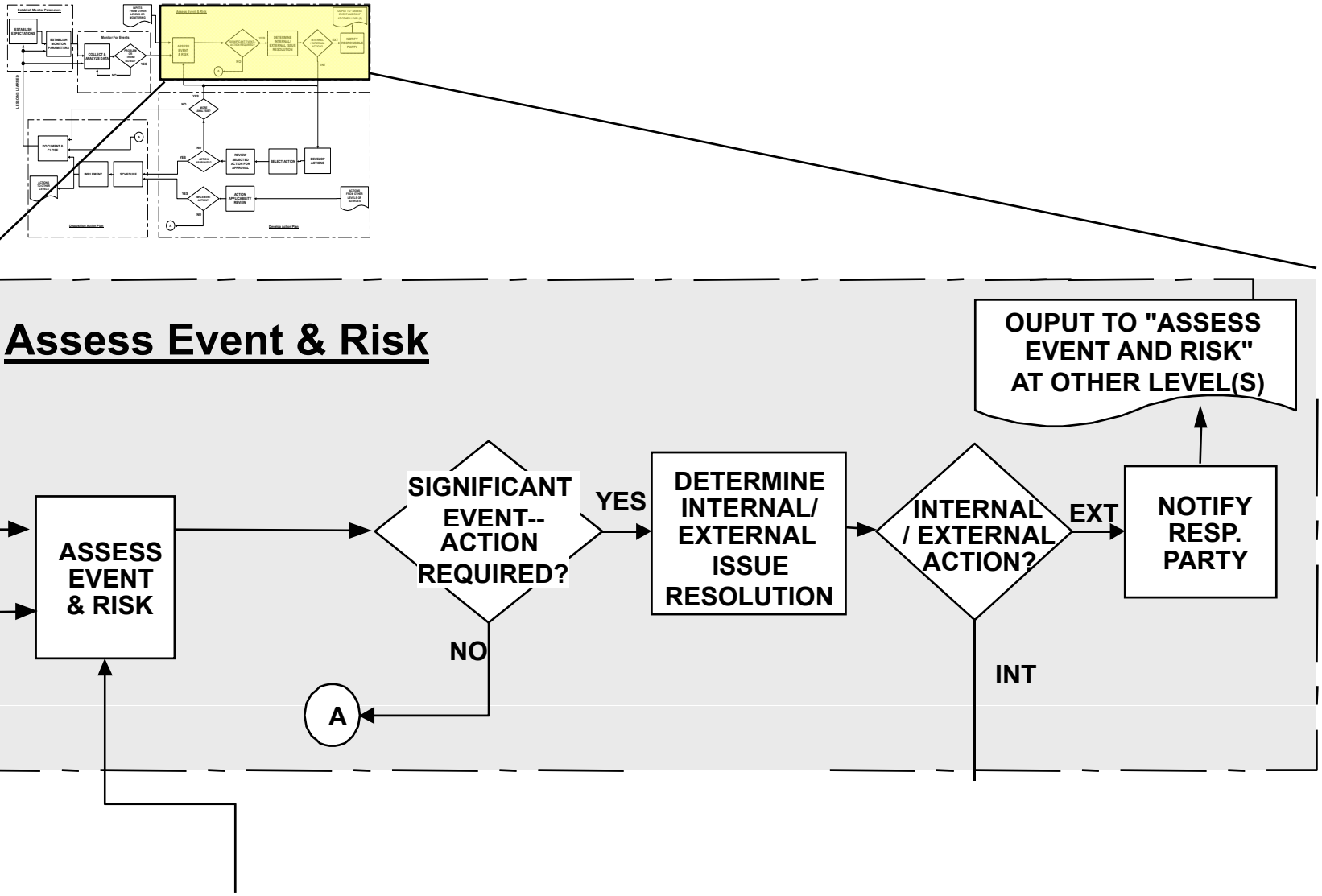
# ARP5150 Process Flow



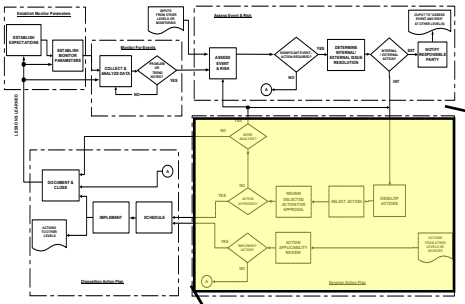
# ARP5150 Process Flow

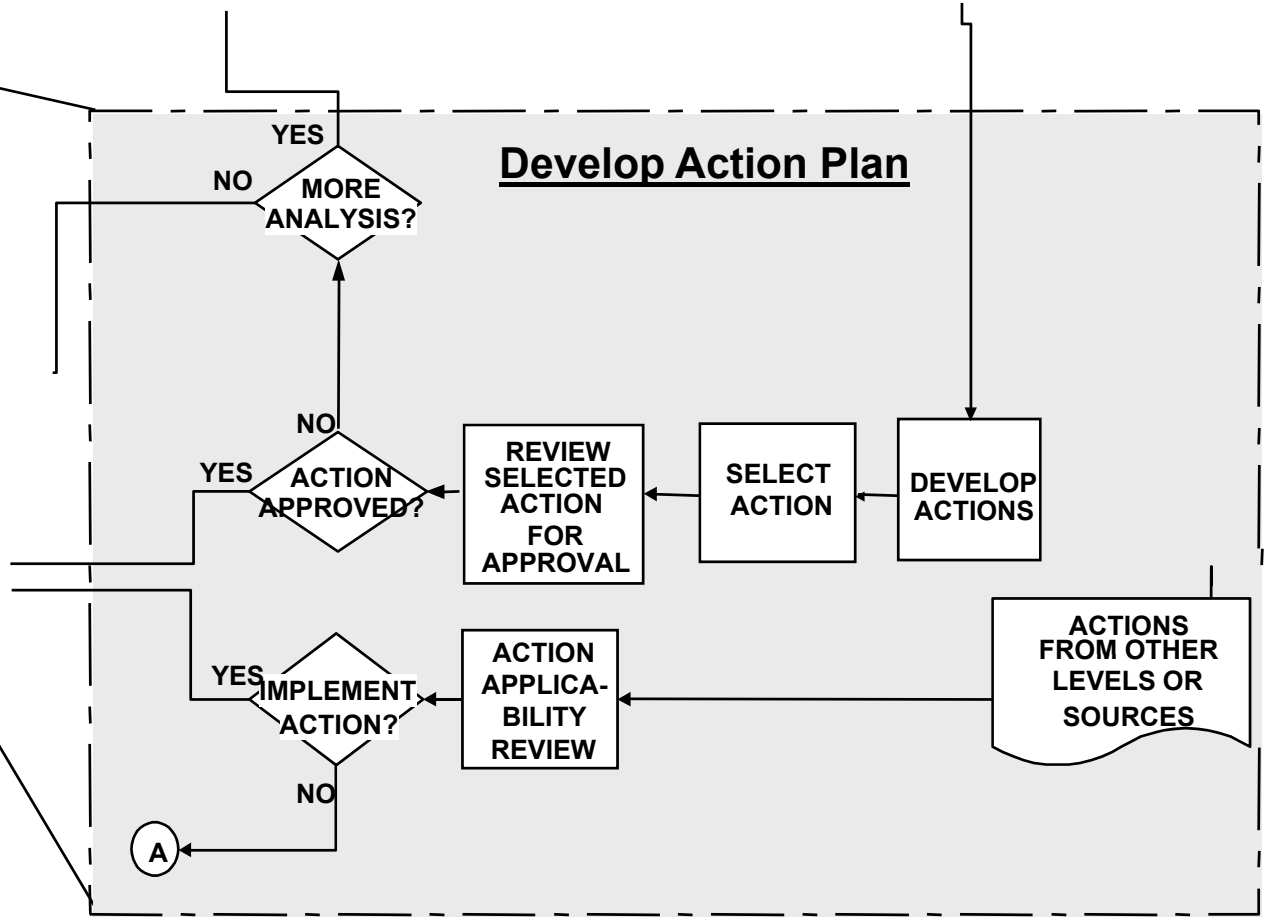


# ARP5150 Process Flow

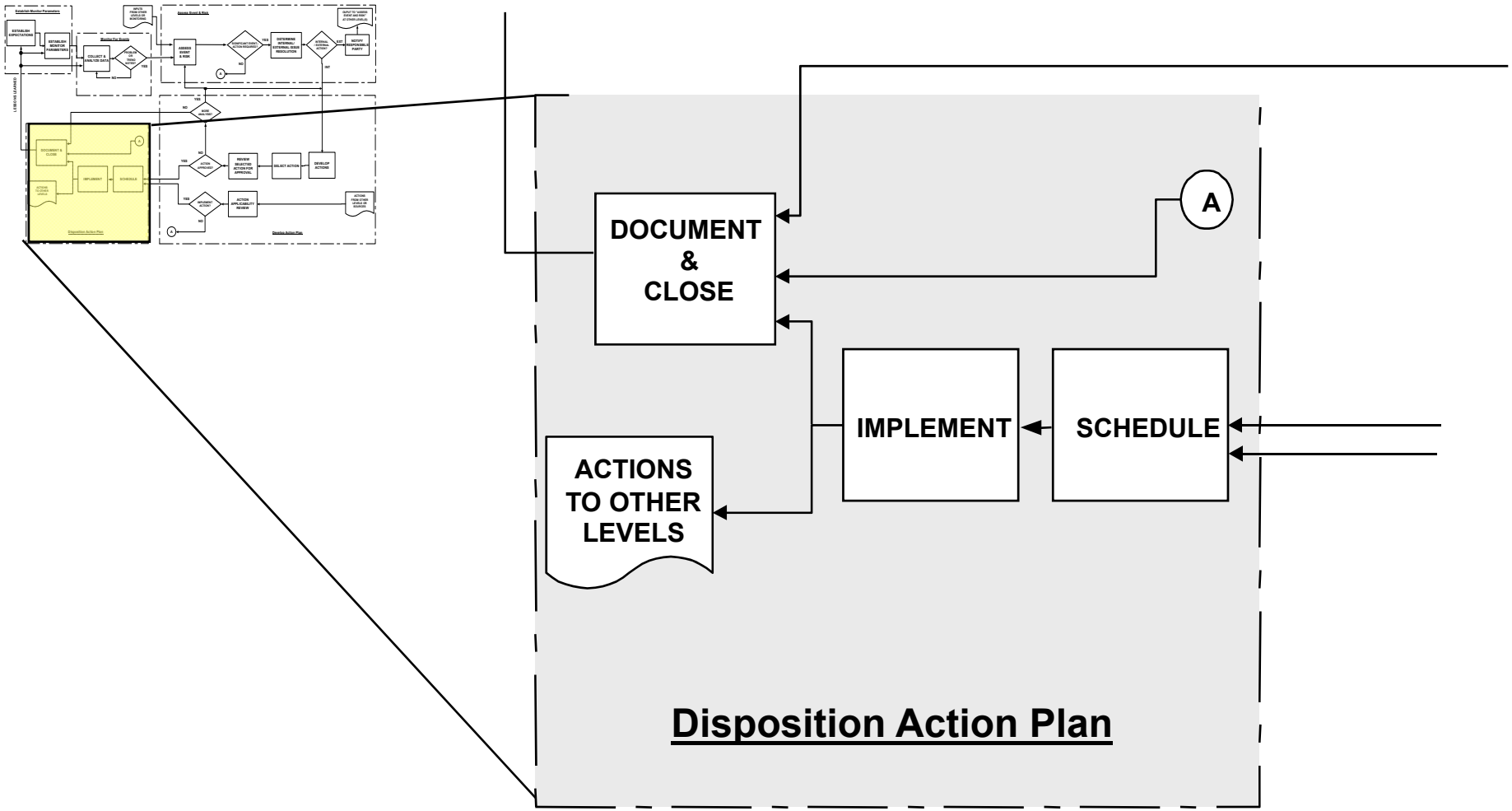


# ARP5150 Process Flow





# ARP5150 Process Flow



# Closing Remarks

- ARP4754, ARP4761, ARP5150 written with aviation regulatory environment in mind but ….
- The recommended practices are based on system engineering concepts applicable to many industries.
- The methods and tools are easily transferrable to other industry areas.

- These premises are supported by evidence
  - ARP4761 is the 3rd best selling SAE document.

# Acronym List

- ARP – Aerospace Recommended Practice
- CCA – Common Cause Analysis
- CMA – Common Mode Analysis
- FDAL – Function Development Assurance Level
- FHA – Functional Hazard Assessment
- FMEA – Failure Modes & Effects Analysis
- GAR – General Aviation and Rotorcraft
- IDAL – Item Development Assurance Level
- PASA – Preliminary Aircraft Safety Assessment
- PRA – Particular Risks Analysis
- PSSA – Preliminary System Safety Assessment
- SAE – Society of Automotive Engineers
- SSA – System Safety Assessment
- WG – Working Group
- ZSA – Zonal System Analysis