Avionics Systems Evolution

- Early Aviation: mainly mechanical equipment
- 1960’s: increased electronic controls
- 1970’s: analog equipment supported by low level, simple software
- 1980’s: integrated digital systems
- 1990’s: PLDs, ASICs, FPGAs and other CEHs
- 2000’s: highly integrated & complex systems
SAE ARP4754 Background

- During preparation of DO178B, it was determined that system level information was needed as input to Software Development process.
- FAA requested SAE to prepare an ARP for demonstrating regulatory compliance for highly-integrated or complex avionics systems.
- A Systems Integration Requirements Task group (SIRT) was formed to draft the ARP, which became ARP4754.
SAE ARP4754 Background

• Since harmonization was deemed highly desirable, representatives of both the FAA and JAA were engaged.

• Working group WG-42 was formed to coordinate European input to the SIRT group.

• The SIRT group members included those with direct design & support experience in:
  – Large commercial aircraft
  – Commuter aircraft
  – Commercial & general aviation avionics
  – Jet engines, and
  – Engine controls
SAE ARP4754 Background

- 14CFR/CS 25.1309 harmonization working group was involved.
- Decision to focus on fundamental principles of certification Vs providing a “very specific list of certification steps”
- ARP4754 published in 1996
SAE ARP4754A Background

• **Written / published in Dec 2010 by S-18 & WG-63 committees.**

• **S-18 & WG-63 committee members:**
  - AEC (1), Aero & Space USA (1), Aeroconseil (1), Airbus (4), ANAC (1), Bell Helicopter (1), Boeing (5), Bombardier (1), CAA UK (1), Cessna (1), CFSS LLC (1), CTA IFI (1), Dassault (2), Diehl (1), EASA (1), Electron International II (2), EMBRAER (1), FAA (3), GE Aviation (3), Goodrich (1), Gulfstream (1), Honeywell (2), Intertechnique (1), Lockheed Martin (1), Messier-Dowty (1), NIIAO (1), Omnicon (1), Pratt & Whitney (1), Rockwell Collins (4), Rolls Royce (4), STM (2), Thales (2), Transport Canada (1), Univ of York (1), Woodward Governor (1)

• **Provides guidelines for the development of systems and items that support aircraft level functions.**

• **This process is referred to as Development Assurance.**
What is Development Assurance?

- All of those \textit{planned and systematic actions} used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis.
Purpose of Development Assurance

- Development assurance establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.
SAE ARP4754A Scope

- The guidelines are primarily directed toward systems that support aircraft level functions. Typically, these systems involve significant interactions with other systems in a larger integrated environment.

- The contents are recommended practices and should not be construed to be regulatory requirements. Alternative methods to the processes described or referenced in this document may be used by an organization desiring to obtain certification.
# SAE ARP4754A Scope

**Included**

- Development of aircraft systems taking into account the overall A/C operating environment and functions
- Integral processes: Safety Assessment, DAL assignment, Validation, Verification, Configuration Control
- Compliance to regulations, where applicable
- Context Part 25 / CS 25
- Document = Guideline
- Document background (link with AMC 25.1309)

**Not Included**

- Development of A/C structure
- MMEL and CDL
- Software development (DO-178)
- Electronic hardware development (DO-254)
- Safety assessments detailed methods (ARP4761)
- Safety assessments in commercial service detailed methods (ARP5150)
SAE ARP4754A Scope
ARP4754A Integral Processes

- Please refer to ARP4754A Section 5 for further descriptions and information.

5.1 Safety Assessment

5.2 Development Assur. Level Assignments

5.3 Requirements Capture

5.4 Requirements Validation

5.5 Implementation Verification

5.6 Configuration Management

5.7 Process Assurance

5.8 Certification & Regul. Authority Coordination

System Safety

Systems Engineering

CM

Systems

PM

Introduction to ARP4754A
ARP4754A 5.1 Safety Assessment Process

- The following slides provide an overview of the safety assessment processes defined in ARP4754A, as it is recommended that they be applied on Throttle Quadrants, Pilot Controls and other safety critical aircraft components.
Safety Process During Development and in Operation

Safety Assessment Process
Guidelines & Methods (ARP 4761)

Intended Aircraft Function
Function, Failure System & Safety Design
Information Information

Aircraft & System Development Processes (ARP 4754 / ED-79)

Guidelines for Integrated Modular Avionics (DO-297/ED-124)

Electronic Hardware Development Life-Cycle (DO-254 / ED-80)

Software Development Life-Cycle (DO-178B/ED-12B)

Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)

Functional System
Operation
Relationship of Safety Assessment Process to System Development Process
Relationship of Safety Assessment Process to Aircraft / System Development Process
Functional Hazard Assessment (FHA)

• An FHA should be conducted at the Aircraft level and the System level.

• Goal of FHA is to clearly identify circumstances and severity of each failure condition, and the rationale for its classification.

• FHA should provide the following information:
  – Identification of related failure conditions.
  – Identification of the effects of the failure conditions.
  – Classification of each failure condition based on the identified effects.
  – A statement outlining what was considered and what assumptions were made (e.g. flight phase, adverse operating / environment, etc.)
## Aircraft FHA

<table>
<thead>
<tr>
<th>Function Failure Ref</th>
<th>Function</th>
<th>Phase</th>
<th>Failure Condition</th>
<th>Failure Effect</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1</td>
<td>Decelerate aircraft on ground</td>
<td>Landing / RTO</td>
<td>Loss of deceleration capability on the ground</td>
<td>Crew is unable to stop the aircraft on runway.</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Decelerate aircraft on ground</td>
<td>Landing</td>
<td>Unannunciated loss of all Automatic Stopping functions.</td>
<td>Crew must use manual procedures to stop the aircraft.</td>
<td>Major</td>
</tr>
</tbody>
</table>

## Brake System FHA

<table>
<thead>
<tr>
<th>Function Failure Ref</th>
<th>Function</th>
<th>Phase</th>
<th>Failure Condition</th>
<th>Failure Effect</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>36-40 1.1</td>
<td>Wheel Braking</td>
<td>Landing / RTO</td>
<td>Loss of all wheel braking.</td>
<td>Crew’s ability to stop the aircraft on runway is significantly reduced.</td>
<td>Hazardous</td>
</tr>
<tr>
<td>36-40 1.2</td>
<td>Auto-Braking</td>
<td>Landing / RTO</td>
<td>Unannunciated loss of Autobraking</td>
<td>Crew must use manual procedures to stop the aircraft.</td>
<td>Major</td>
</tr>
</tbody>
</table>
Preliminary System Safety Assessment (PSSA)

A PSSA is a systematic examination of a proposed architecture to determine how failures could cause the Failure Conditions identified by the FHA
Preliminary System Safety Assessment (PSSA)

• A PSSA is used to ensure completeness of the failure conditions list from the FHA and to complete the safety requirements of the design.

• It is also used to demonstrate how the proposed design will meet the qualitative and quantitative requirements for the various hazards (FCs) identified.

• Provides safety feedback to the design process to support trade off studies and evaluations of alternative designs.
PSSA – Typical Inputs / Analyses

- FHA (FCs & Classifications)
- Block diagrams, schematics, assembly drawings, detail parts, BOM
- Design meetings, plans, engineering coordination
- FMEA (Single point failures)
- Fault Tree Analysis (FTA) of CAT & HAZ FCs
- Common Mode Analysis (evaluates & determines need for additional independence (separation & isolation) requirements)
PSSA – Outputs

• Derived Safety Requirements (DSR) *(inputs for SRD, hardware and software requirements documents, and SSA)*

• Failure rate allocations for critical subassemblies

• Safety analysis (FTA & CMA) of alternative design approaches. *(feedback to design process)*

• Alternative protective strategy recommendations, *e.g.* partitioning, built-in-test, dissimilarity, monitoring, redundancy, safety maintenance task intervals, etc. *(feedback to design process)*
PSSA – Life Cycle

• Iterative Analysis (*ongoing process starting in the early phases of the development with the allocation of aircraft functions and their requirements to the system level*)

• Through Conceptual Design phase

• Through Detail Design phase

• Culminates with start of SSA, prior to CDR
System Safety Assessment (SSA)

• An SSA is a systematic, comprehensive evaluation of the implemented system to show that relevant safety requirements are met.

• The analysis process is similar to the activities of the PSSA, but different in intent.

• The PSSA is used to derive system and item safety requirements, whereas the SSA is used to verify that the implemented design meets those safety requirements.
Typical SSA Report Contents

• Compliance Summary
  – System Safety Conclusions
  – Flight Crew Procedures Required To Ensure Safety
  – Review of Significant Latent Failures
  – Maintenance Procedures Required To Ensure Safety
  – Safety Requirements/Compliance

• System Overview and Design for Safety

• Functional Hazard Assessment

• Failure Mode & Effects Analysis

• Design Assurance Assessment

• Fault Tree Analysis

• Common Cause Analysis (*including Particular Risks and CMA* )
Common Cause Analysis (CCA)

- Used to determine if ≥ 2 functions, systems or items are ‘independent’. If not independent, then whether the lack of independence is acceptable.

**Independence**

1. *A concept that minimizes the likelihood of common mode errors and cascade failures between aircraft / system functions or items.*

2. *Separation of responsibilities that assures the accomplishment of objective evaluation, e.g. validation activities not performed solely by the developer of the requirement of a system or item.*
Common Cause Analysis (CCA)

• Identifies the failure modes or external events that can lead to Catastrophic or Hazardous Failure Conditions.

• CCA is subdivided into the following areas of study:
  – Particular Risk Analysis (PRA)
  – Common Mode Analysis (CMA)
  – Zonal Safety Analysis (ZSA)

• CCA studies (PRA, CMA and ZSA) may be performed at any stage of the design process; however, they’re most cost effective early on.
Particular Risk Analysis (PRA)

- PRA is normally performed by the airframer.

- Particular Risks are events or influences which are outside the system or item(s) but which may violate independence claims.

- Examples of Particular Risks include:
  - Fire
  - High-pressure air duct rupture
  - Leaking fluids
    - Fuel
    - Hydraulic
    - Battery Acid
    - Water
Common Mode Analysis (CMA)

• CMA is normally performed by the system / item OEM.

• Used to determine if failure events from the PSSA / SSA are independent.

• Effects of development, manufacturing, installation, maintenance and crew errors, and failures of system elements that defeat independence should be analyzed.

• Independence of functions and their respective monitors; identical systems / items ...

• Results of preliminary CMA is input for DAL assignments.
Zonal Safety Analysis (ZSA)

• ZSA is normally performed by the airframer.

• ZSA should be performed on each zone of the A/C.

• Used to ensure the installation meets the safety requirements with respect to:
  – Basic installation
  – Interference between systems
  – Maintenance errors
Zonal Safety Analysis (ZSA)

Example of Aircraft Zones
Additional System Safety Data Items

- System Safety Program Plan (SSPP)
- Architectural Principles and Safety Rationales report
- SEU/MBU Susceptibility Analysis report
- Intrinsic & Environmental Hazards Analysis (IEHA) report
- Safety Accomplishments Summary report
5.2 Development Assurance Level Assignments

Prerequisites for a good understanding of DAL Assignments are the definitions of:

**Function**: Intended behavior of a product based on a defined set of requirements regardless of implementation.

**Failure Condition**: A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events (AMC 25.1309).

**Failure**: An occurrence which affects the operation of a component, part or element such that it can no longer function as intended (this includes both loss of function and malfunction). Note: errors may cause failures but are not considered to be failures.

**Error**: An omitted or incorrect action by a crew member or maintenance person, or a mistake in requirements, design or implementation (derived from AMC 25.1309).
5.2 Development Assurance Level Assignments

Prerequisites ...

**Independence:**

1.) A concept that minimizes the likelihood of common mode errors and cascade failures between aircraft / system functions or items.

2.) Separation of responsibilities that assures the accomplishment of objective evaluation, e.g. validation activities not performed solely by the developer of the requirement of a system or item.
5.2 Development Assurance Level Assignments

- A Failure Condition can be caused by 1 or more **Failures** or **Errors**.

- Failures are mitigated by establishing qualitative and quantitative safety requirements, including the fail-safe design concept of AC/AMC 25.1309.

- Errors are mitigated by implementing a Development Assurance process.
5.2 Development Assurance Level Assignments

- The Development Assurance process establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.

- The Development Assurance Level (DAL) is the measure of rigor applied to the development process.

- The DAL is assigned depending on the severity classification of Failure Conditions considering the possible independence between development processes that can limit the consequences of development errors.
5.2 DAL Assignment ~ General Principles

• **When a Catastrophic Failure Condition is involved:**
  – If a Catastrophic Failure Condition could result from a possible development error (in a function or item), the DAL assignment is Level A.
  – If a Catastrophic Failure Condition could result from combination of development errors between two or more independently developed aircraft / system functions or items then:
    • Either one Development Assurance process is assigned level A, or
    • Two Development Assurance processes are assigned at least level B.
    • The other independently developed aircraft / system functions or items are assigned no lower than DAL C.
    • The Development Assurance process used to validate the independence of the two or more items or functions should remain at level A.
• When a Hazardous Failure Condition is involved:
  – If a Hazardous Failure Condition could result from a possible development error (in an aircraft / system, function or item), the DAL assignment is Level B.
  – If a Hazardous Failure Condition could result from combination of development errors between two or more independently developed aircraft / system functions or items then:
    • Either one Development Assurance process is assigned level B, or
    • Two Development Assurance processes are assigned at least level C.
    • The other independently developed aircraft / system functions or items are assigned no lower than DAL D.
    • The Development Assurance process used to validate the independence of the two or more items or functions should remain at level B.
### 5.2 DAL Assignment ~ General Principles

- **Top Level Function DAL Assignment Matrix**

<table>
<thead>
<tr>
<th>Top-Level Failure Condition Classification</th>
<th>Associated Top-Level Function 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>
5.2.2 DAL Assignment ~ FDAL & IDAL

- FDAL & IDAL assignment is a top-down process beginning with the Failure Condition severity classification from the FHA and assigning the top level FDAL in the PSSA.

- After Decomposing the top level function into sub-functions, the sub-function FDALs are assigned.

- Each sub-function is allocated or decomposed into Items, and then IDALs are assigned.
Integrated Safety Process

**Aircraft Level**
- Concept & Architecture Development
- Aircraft FHA
  - Function Failure Ref.
  - Function
  - Phase
  - Failure Condition
  - Failure Effect
  - Classification
  - AFHA
    - 1.1.1: Decelerate Aircraft on Ground, Landing RTO
      - Loss of Deceleration Capability on the Ground
      - Crew is unable to stop aircraft on runway
      - Catastrophic
    - 1.1.2: Decelerate Aircraft on Ground, Landing
      - Unanticipated Loss of All Automatic Stopping Functions
      - Crew must use manual procedures to stop aircraft
      - Major
  - Aircraft FTAs
    - Loss of Deceleration Capability on the Ground
    - Loss of Effective Wheel Braking
    - Loss of all Speedometers on a Contaminated Runway
    - Loss of all Wheel Braking
    - Loss of Normal Braking
    - Loss of all Alternate Braking
    - Loss of Reserve Braking

**System Level**
- Preliminary Design
- System FHA
  - Function Failure Ref.
  - Function
  - Phase
  - Failure Condition
  - Failure Effect
  - Classification
  - SFHA
    - 30-40 1.1: Wheel Braking, Landing RTO
      - Loss of all Wheel Braking
      - Crew's ability to stop aircraft on runway to be significantly reduced
      - Hazardous
    - 30-40 1.2: Auto Braking, Landing RTO
      - Unanticipated Loss of Auto Braking
      - Crew must use manual procedures to stop aircraft
      - Major
  - System FMEAs
    - Electrical System
    - Hydraulic System
    - Speedbrake System
    - Thrust Reverser System
    - Brake System
  - PSSA
    - Loss of all Wheel Braking
    - Loss of Normal Braking
    - Loss of all Alternate Braking
    - Loss of Reserve Braking

**Item Level**
- Detailed Design
- Item FMEAs
  - SSA FTAs
    - Loss of all Wheel Braking
    - Loss of Manual Braking
    - Loss of Alternate Braking
    - Loss of Reserve Braking
  - SSA
    - Loss of Manual Braking
    - Loss of Alternate Braking
    - Loss of Reserve Braking
## 5.2.2 DAL Assignment

- **DAL Assignment to FFS Members**

<table>
<thead>
<tr>
<th>Top-Level Failure Condition Classification</th>
<th>Development Assurance Level (NOTES 2 &amp; 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column 1</strong></td>
<td><strong>Column 2</strong></td>
</tr>
<tr>
<td><strong>Column 3</strong></td>
<td><strong>Column 4</strong></td>
</tr>
<tr>
<td><strong>Catastrophic</strong></td>
<td>FDAL A (NOTE 1)</td>
</tr>
<tr>
<td><strong>FDAL A</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>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)).</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Hazardous/Severe Major</strong></td>
<td>FDAL B</td>
</tr>
<tr>
<td><strong>FDAL B</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>FDAL C</strong></td>
<td>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).</td>
</tr>
</tbody>
</table>
5.3 Requirements Capture
5.4 Requirements Validation
5.5 Implementation Verification
5.6 Configuration Management
5.7 Process Assurance
5.8 Certification & Regulatory Authority Coordination

- Performed by Applicant and Certification Authorities, i.e. not Mason unless we were pursuing a Supplemental Type Certification (STC)
- Mason may be asked to support, if needed, by:
  - Attending certification meetings, phone calls, etc.
  - Supplying evidence of development assurance activities, Qualification test plans, procedures, reports, analyses, etc.
  - Participating (i.e. hosting) development audits performed by our customer and the certification authorities.
- Mostly supported by Program Manager and/or Project Engineer
Thank you!

... Questions?