SAE ARP 4754A Linkage with DO-178 and DO-254

Presented to: 2011 SW & AEH Conference

Federal Aviation Administration

Outline

- **Key Linkages**
  - 14 CFR XX.1301, XX.1309
  - Development Assurance Level Assignment Process
  - Requirements
- **Assurance Process Similarities and Differences**
  - Objective based
  - Processes

14 CFR XX.1301 and XX.1309

- Means of compliance to 14 CFR XX.1301 and XX.1309
  - AC XX-1309
  - AC 20-XXX, SAE ARP 4754A
  - AC 20-115B, DO-178B
  - AC 20-152, DO-254

Outline

- **Key Relationships**
  - 14 CFR XX.1301, XX.1309
  - ➡ Development Assurance Level Assignment Process
  - Requirements
- **Assurance Process Similarities and Differences**
  - Objective based
  - Processes

Development Assurance Level Assignment

- **Starts with the FHA failure condition severity classification**
- **ARP 4754A provides a development assurance level assignment process**
  - Function Development Assurance Level (FDAL) are assigned to aircraft functions
  - Functions can be allocated to sub-functions
  - Sub-functions are allocated to hardware and software item
  - Item Development Assurance Level (IDAL) is assigned
  - Can consider the system architecture in the assignment process
    - Functional and development independence must be present
  - IDAL levels dictate the level of DO-178 and DO-254 process rigor for the software and AEH items

Outline

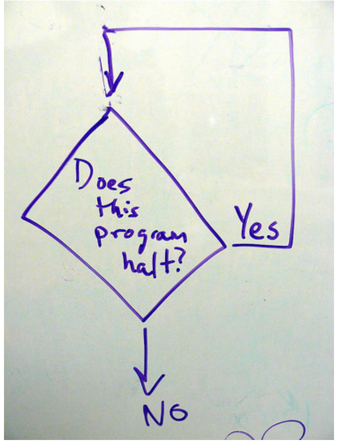
- **Key Relationships**
  - 14 CFR XX.1301, XX.1309
  - Development Assurance Level Assignment Process
  - ➡ Requirements
- **Assurance Process Similarities and Differences**
  - Objective based
  - Processes

Requirements

- Software versus Requirements Errors
- Relevant Incident
- Requirements Allocation
- Requirements Validation
- Derived Requirements

Software Versus Requirements Errors

Airborne system problems are reported as "*software problems, anomalies, bugs or glitches*"



Many are due to incomplete or incorrect *requirements and not to software coding errors*

Relevant Incident

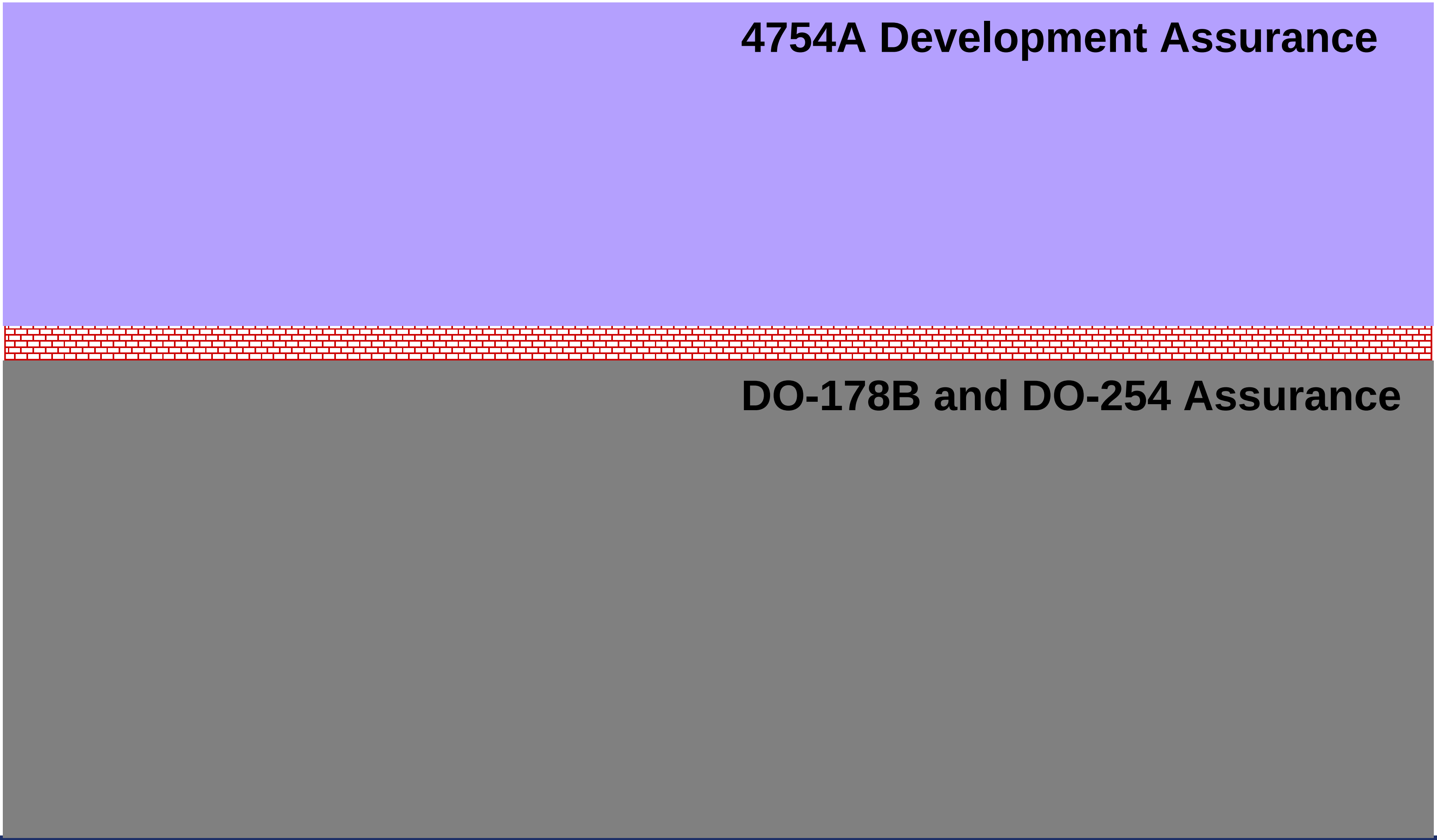
- **August 2005, a Malaysian Airlines Boeing 777-200ER suffered an in-flight upset en-route from Perth to Kuala Lumpur.**

"The Australian ATSB concluded that a contributing safety factor was that *an anomaly existed in the component software hierarchy that allowed inputs from a known faulty accelerometer to be processed by the air data inertial reference unit (ADIRU) and used by the primary flight computer, autopilot and other aircraft systems*."

- Example of a systems requirement error where the ADIRU would reinstate known failed accelerometers

- **Fault handling requirements need to be validated and verified**

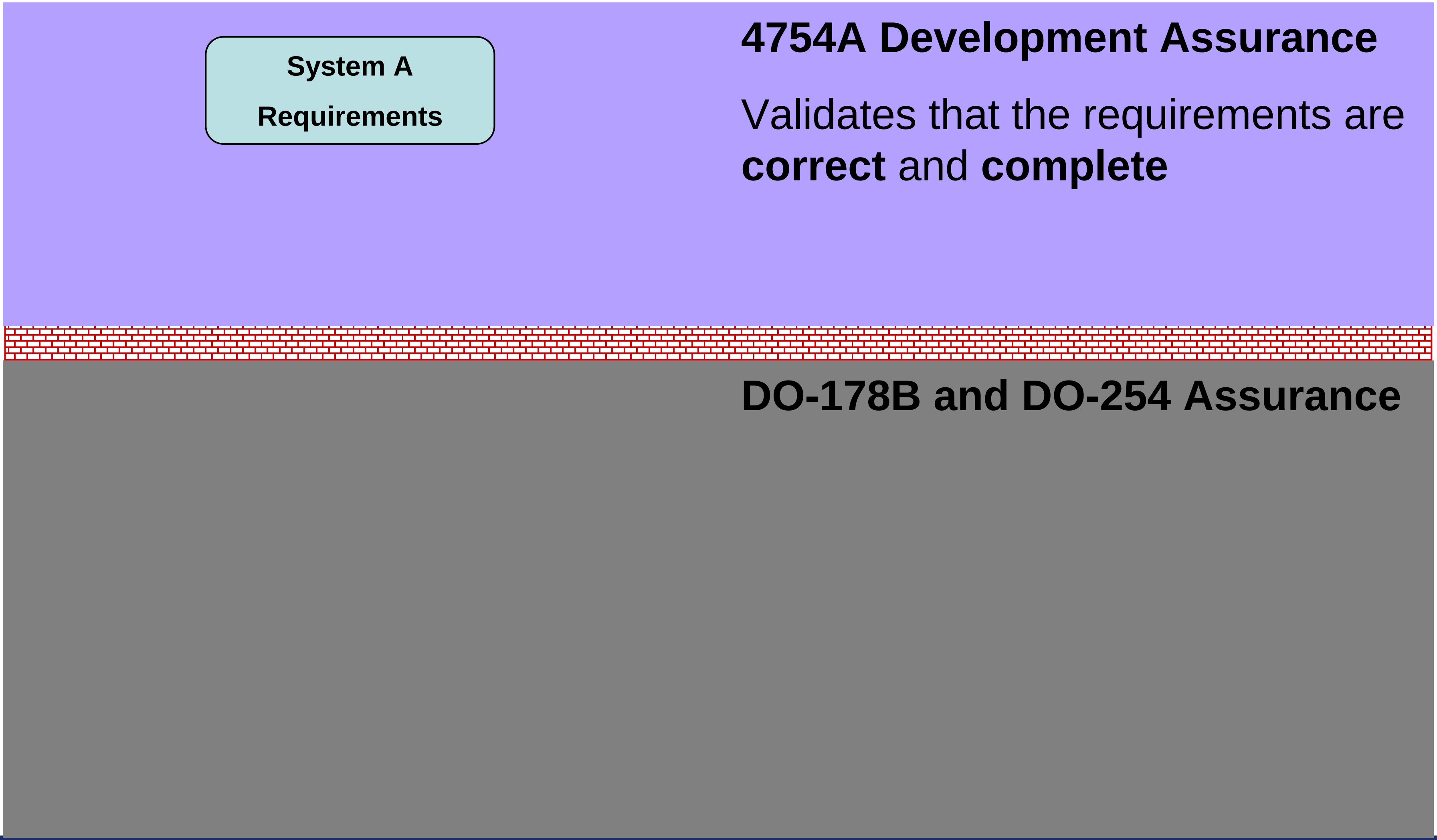
Requirements Allocation



4754A Development Assurance

DO-178B and DO-254 Assurance

Requirements Allocation



System A

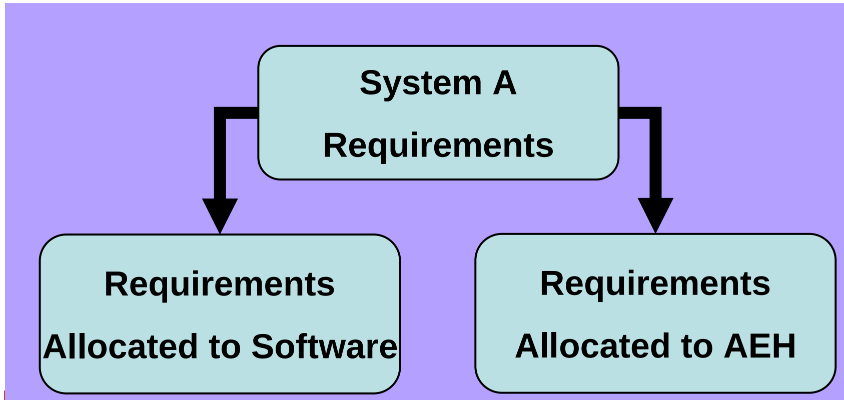
Requirements

4754A Development Assurance

Validates that the requirements are **correct** and **complete**

DO-178B and DO-254 Assurance

Requirements Allocation



System A Requirements

Requirements Allocated to Software

Requirements Allocated to AEH

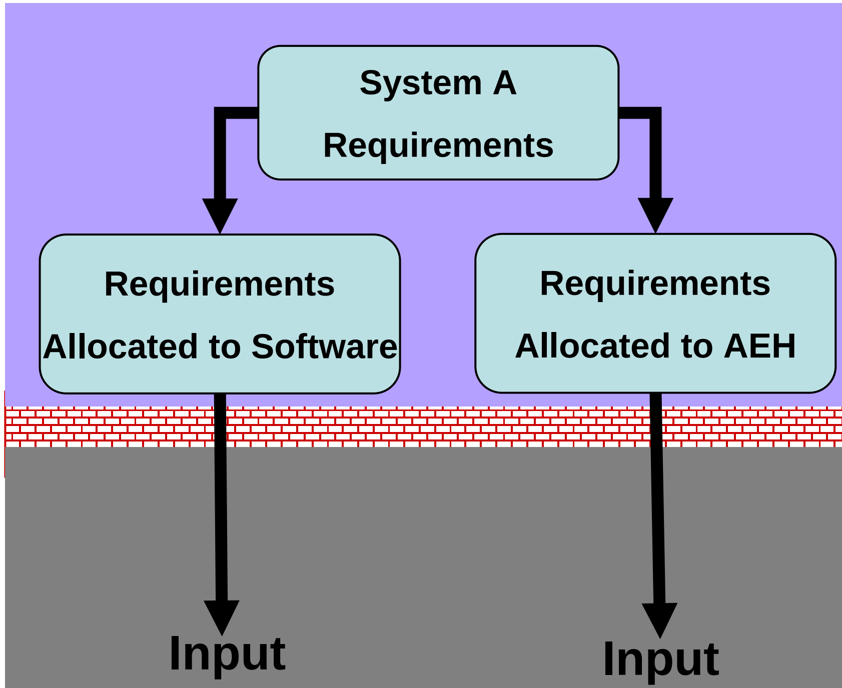
4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Requirements Allocation



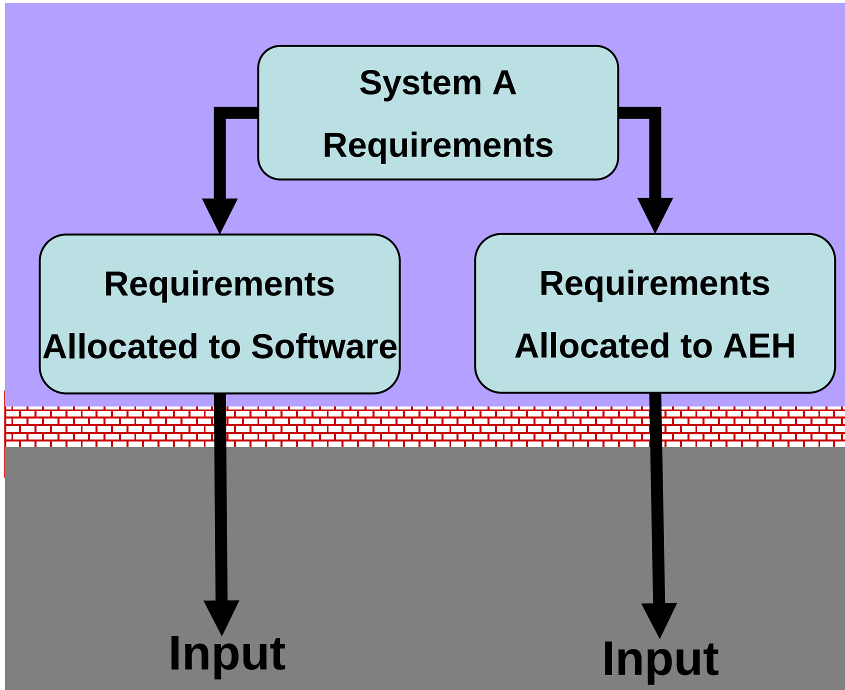
4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Requirements Allocation



4754A Development Assurance

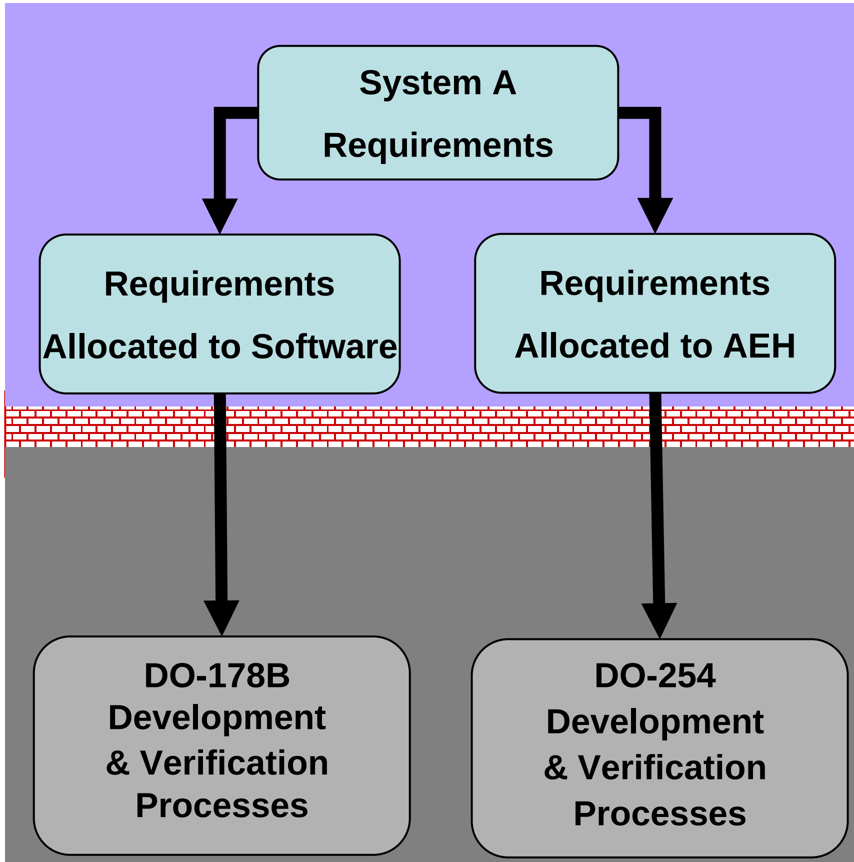
Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Assume the requirements are **correct** and **complete**

Requirements Allocation


System A Requirements
Requirements Allocated to Software
Requirements Allocated to AEH
DO-178B Development & Verification Processes
DO-254 Development & Verification Processes

4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Assume the requirements are **correct** and **complete**

Develop the software and AEH

Verify that the software and AEH meets their requirements

ARP 4754A Requirements Validation Process

- **Process of ensuring the requirements are sufficiently correct and complete**
  - Correct – unambiguous, verifiable, and consistent with other requirements
  - Completeness – degree to which the requirement satisfies users', maintainers', and certifiers' needs under all operating modes
- **Assumptions and derived requirements are justified and validated**
- **Requirements are traceable**
- **Use of scenarios and model prototypes to elicit user, operator, and maintainer input to help identify missing requirements**
- **Validation methods**
  - Traceability
  - Analysis
  - Modeling
  - Test
  - Review
- **Validation rigor and the need for independence is dependent on the assurance level**

Derived Requirements

- Requirements which are generated during the design processes that do not directly trace to a higher level requirement
- ARP 4754A, DO-254 and draft DO-178C highlight the need for systems to assess the potential system safety and system requirements impacts of the derived requirements

Outline

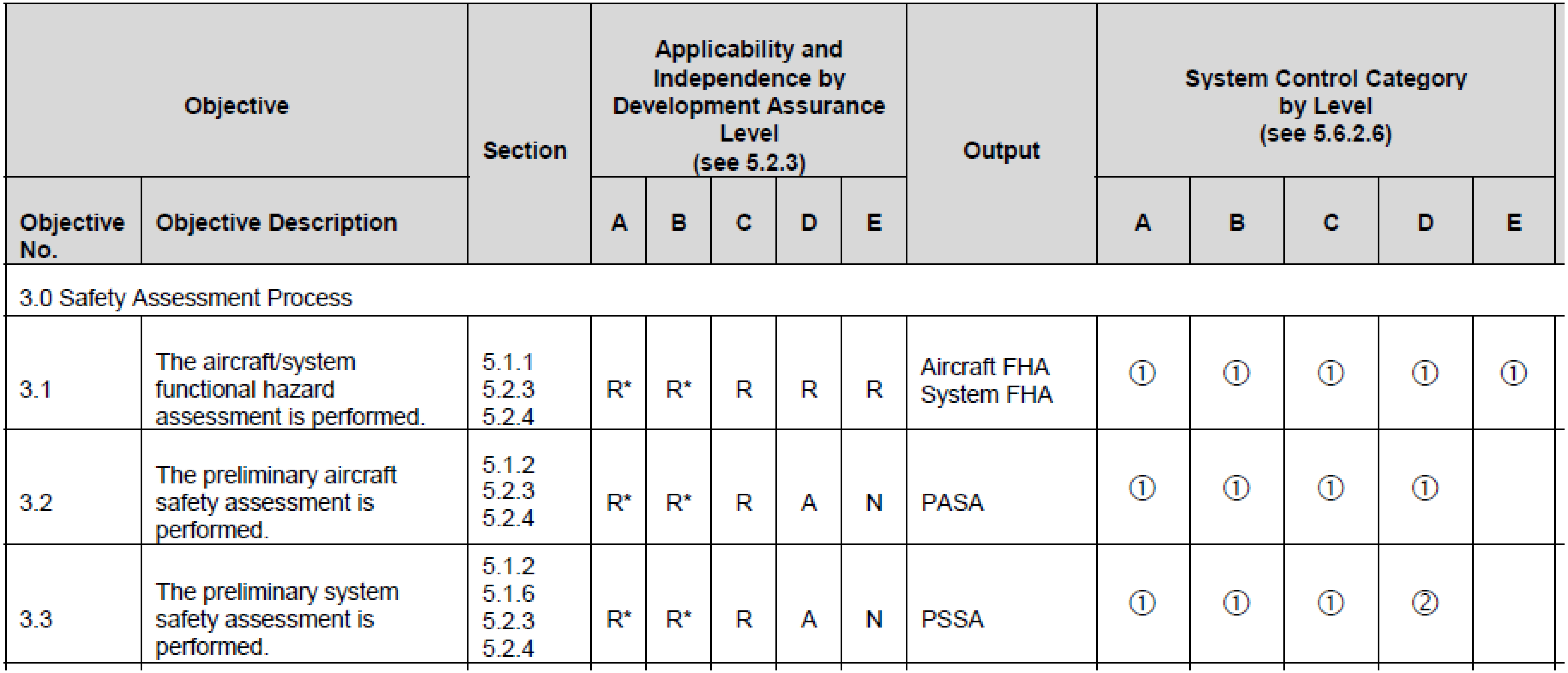
- **Key Relationships**
  - 14 CFR XX.1301, XX.1309
  - Development Assurance Level Assignment Process
  - Requirements

➔ **Assurance Process Similarities and Differences**
  - Objective based
  - Processes

Similarities

- **ARP 4754A, DO-178, and DO-254 are all assurance processes**
  - Establishes confidence that the development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety
  - Assurance level establishes the level of process rigor which is commensurate with the functional failure condition
  - They are all dependent on each other
- **Use objective based tables**

Sample of the ARP4754A Table A-1



Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)				
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E
3.0 Safety Assessment Process													
3.1	The aircraft/system functional hazard assessment is performed.	5.1.1 5.2.3 5.2.4	R*	R*	R	R	R	Aircraft FHA System FHA	①	①	①	①	①
3.2	The preliminary aircraft safety assessment is performed.	5.1.2 5.2.3 5.2.4	R*	R*	R	A	N	PASA	①	①	①	①	
3.3	The preliminary system safety assessment is performed.	5.1.2 5.1.6 5.2.3 5.2.4	R*	R*	R	A	N	PSSA	①	①	①	②	

R*- Recommended for certification with process independence

R - Recommended for certification

A - As negotiated for certification

N - Not required for certification.

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

ARP 4754A, DO-178B, and DO-254 Processes

ARP 4754A	DO-178B	DO-254
Planning	Planning	Planning
Development - Function - System Architecture - Allocation - Implementation	**Development** - Requirements - Design - Coding - Integration	**Design** - Requirements - Conceptual - Detailed - Implementation - Production Transition

ARP 4754A, DO-178B, and DO-254 Integral/Supporting Processes

ARP 4754A	DO-178B	DO-254
Integral	Integral	Supporting
- Configuration Management	- Configuration Management	- Configuration Management
- Process Assurance	- Quality Assurance	- Process Assurance
- Certification & Authority Coordination	- Certification Liaison	- Certification Liaison
- Requirements Validation	- Verification	- Validation & Verification
- Verification		
- Safety Assessment		
- Assurance Level assignment		
- Requirements Capture		

Summary Slide

- **ARP 4754A, DO-178B and DO-254**
  - Collectively can support a means of compliance to XX.1301 and XX.1309
  - All use an assurance process with the level of process rigor determined by the failure classification
  - All have similar processes, integral/supporting processes, and use objective based tables
  - All have a very important part in the overall systems development process

<Audience Questions>