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

Presented to: 2011 SW & AEH Conference
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

**4754A Development Assurance**
Validates that the requirements are **correct** and **complete**

**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

System A Requirements

Requirements Allocated to Software

Requirements Allocated to AEH

Input

Requirements

Input
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

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

<table>
<thead>
<tr>
<th>Objective No.</th>
<th>Objective Description</th>
<th>Section</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>System Control Category by Level (see 5.6.2.6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0 Safety Assessment Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>The aircraft/system functional hazard assessment is performed</td>
<td>5.1.1, 5.2.3, 5.2.4</td>
<td>R*</td>
<td>R*</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>Aircraft FHA System FHA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>3.2</td>
<td>The preliminary aircraft safety assessment is performed</td>
<td>5.1.2, 5.2.3, 5.2.4</td>
<td>R*</td>
<td>R*</td>
<td>R</td>
<td>A</td>
<td>N</td>
<td>PASA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>3.3</td>
<td>The preliminary system safety assessment is performed</td>
<td>5.1.2, 5.1.6, 5.2.3, 5.2.4</td>
<td>R*</td>
<td>R*</td>
<td>R</td>
<td>A</td>
<td>N</td>
<td>PSSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ARP 4754A</th>
<th>DO-178B</th>
<th>DO-254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>Planning</td>
<td>Planning</td>
</tr>
<tr>
<td>Development</td>
<td>Development</td>
<td>Design</td>
</tr>
<tr>
<td>- Function</td>
<td>- Requirements</td>
<td>- Requirements</td>
</tr>
<tr>
<td>- System</td>
<td>- Design</td>
<td>- Conceptual</td>
</tr>
<tr>
<td>Architecture</td>
<td>- Coding</td>
<td>- Detailed</td>
</tr>
<tr>
<td>- Allocation</td>
<td>- Implementation</td>
<td>- Implementation</td>
</tr>
<tr>
<td>- Implementation</td>
<td></td>
<td>- Production</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transition</td>
</tr>
</tbody>
</table>
## ARP 4754A, DO-178B, and DO-254
### Integral/Supporting Processes

<table>
<thead>
<tr>
<th>ARP 4754A</th>
<th>DO-178B</th>
<th>DO-254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integral</td>
<td>Integral</td>
<td>Supporting</td>
</tr>
<tr>
<td>- Configuration Management</td>
<td>- Configuration Management</td>
<td>- Configuration Management</td>
</tr>
<tr>
<td>- Process Assurance</td>
<td>- Quality Assurance</td>
<td>- Process Assurance</td>
</tr>
<tr>
<td>- Certification &amp; AuthorityCoordination</td>
<td>- Certification Liaison</td>
<td>- Certification Liaison</td>
</tr>
<tr>
<td>- Requirements Validation</td>
<td>- Verification</td>
<td>- Validation &amp; Verification</td>
</tr>
<tr>
<td>- Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Safety Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Assurance Level assignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Requirements Capture</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• 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>