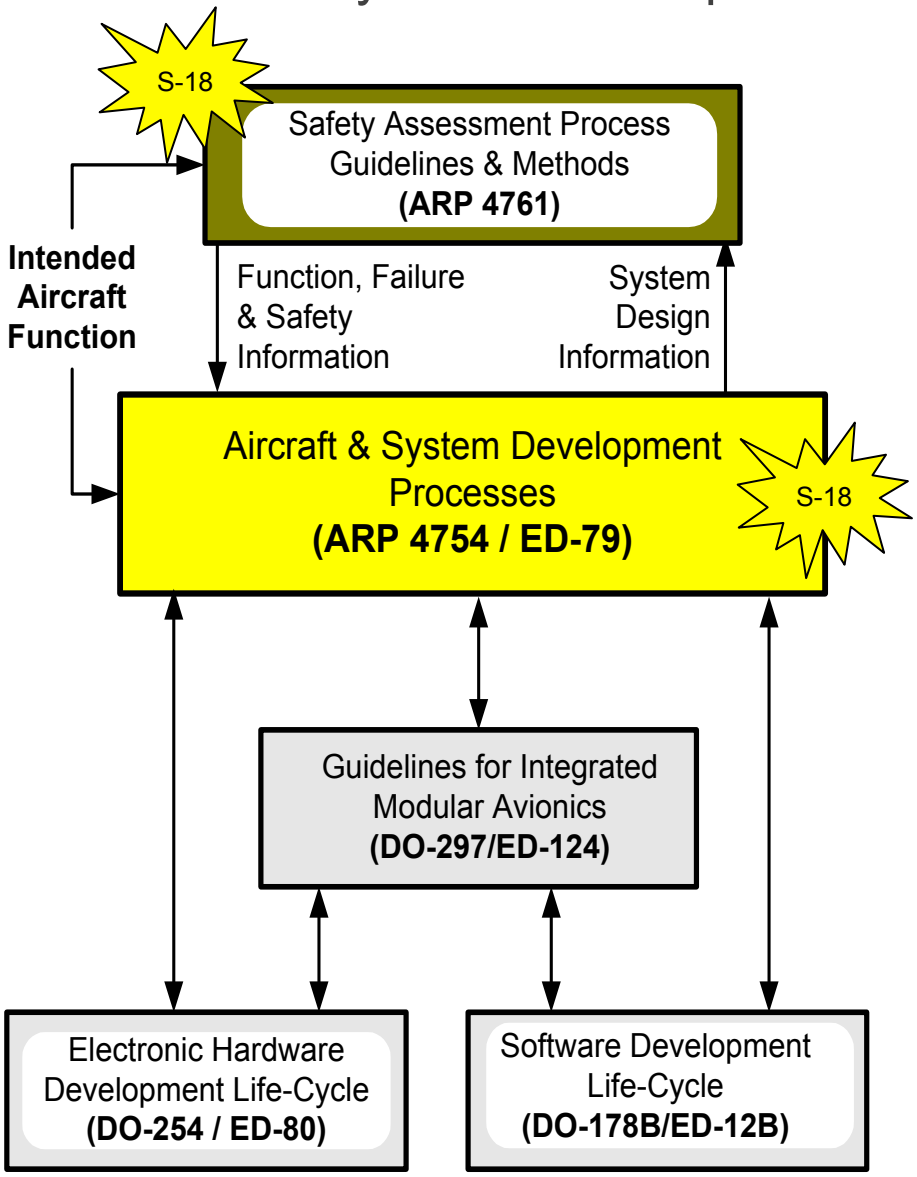
Role of STPA in Aircraft Standards (SAE S-18)

Steve Beland
Associate Technical Fellow – BCA Flight Controls; Authorized Representative (FAA)
March 27, 2014

SAE S-18 Committee

Aircraft and Systems Development and Safety Assessment Committee



SAE ARP4754A Figure 1

ADDITIONAL DOCUMENTS::

ARP5150 – Safety Assessment of Transport Airplanes in Commercial Service

ARP5151 – Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service

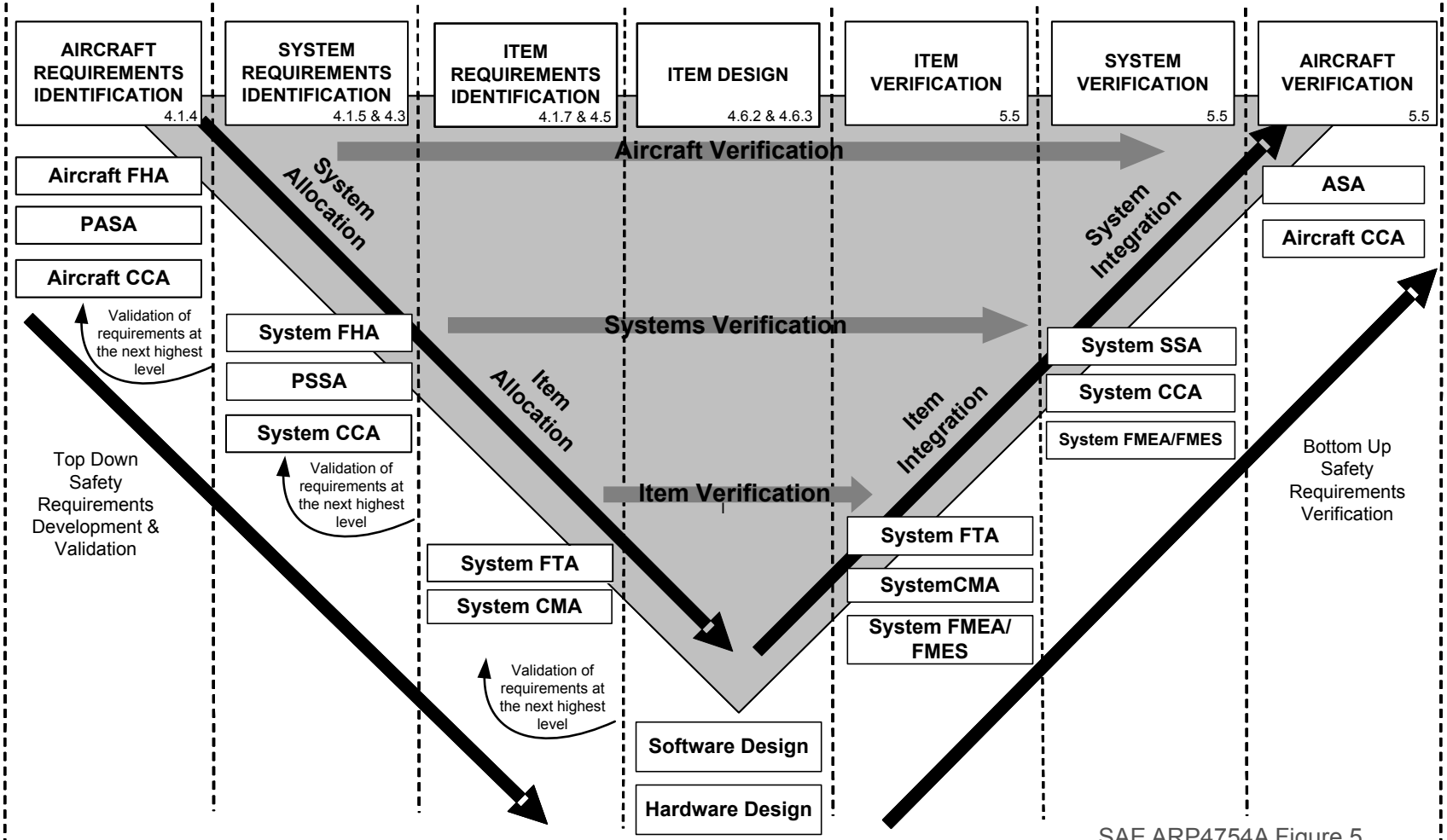
AIR6110 – Contiguous Aircraft/System Development Process Example

AIR6218 – Constructing Development Assurance Plan for Integrated Systems

AIR6219 – Incorporation of Atmospheric Neutron Single Event Effects Analysis into Safety Assessment (balloted)

AIR6276 - Use Of Modeling And Tools For Aircraft Systems Development (in work)

Interaction Between Safety & Development Processes ARP4761 & ARP4754



ARP4761A Outline

1. Scope
2. References
3. Safety Assessment Process
4. Safety Analysis Methods
5. Safety Related Maintenance Tasks & Intervals
6. Master Minimum Equipment List
7. Time Limited Dispatch
8. In-service Safety Assessment

SAFETY ASSESSMENTS:

App A Aircraft Functional Hazard Assessment (AFHA)
App B Preliminary Aircraft Safety Assessment (PASA)
App C System Functional Hazard Assessment (SFHA)
App D Preliminary System Safety Assessment (PSSA)
App E System Safety Assessment (SSA)
App F Aircraft Safety Assessment (ASA)

May use STPA in PASA & PSSA

ANALYSIS METHODS:

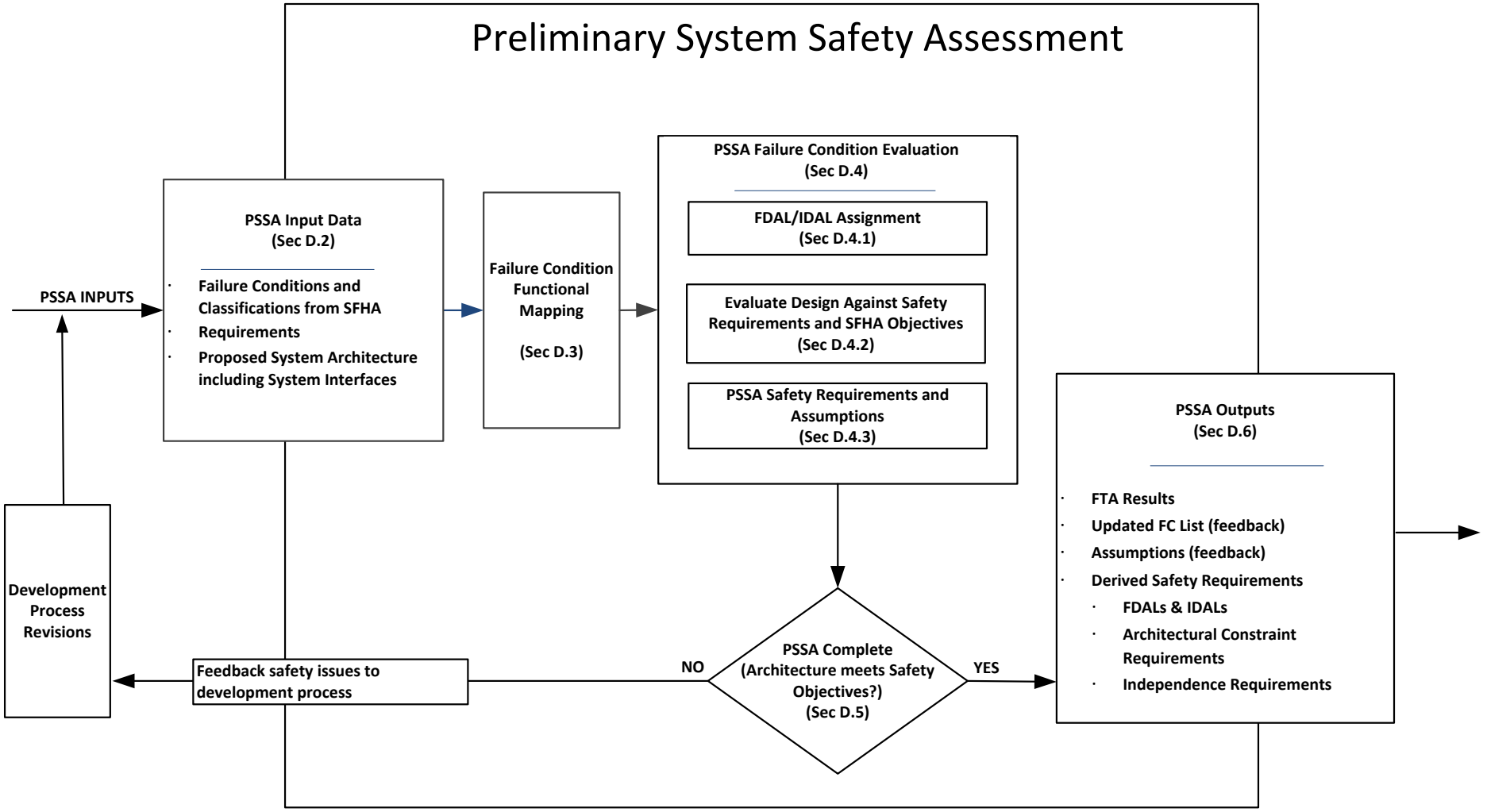
App G Fault Tree Analysis (FTA)
App H Dependence Diagrams (DD)
App I Markov Analysis (MA)
App J Failure Modes & Effects Analysis (FMEA)
App K Zonal Safety Analysis (ZSA)
App L Particular Risks Analysis (PRA)
App M Common Mode Analysis (CMA)
App N Model Based Safety Analysis (MBSA)
App O Cascading Effects Analysis (CEA)
App P FDAL/IDAL Assignment

App Q Contiguous Safety Assessment Process Example (Wheel Braking System)

Blue = New for Rev A

Preliminary System Safety Assessment

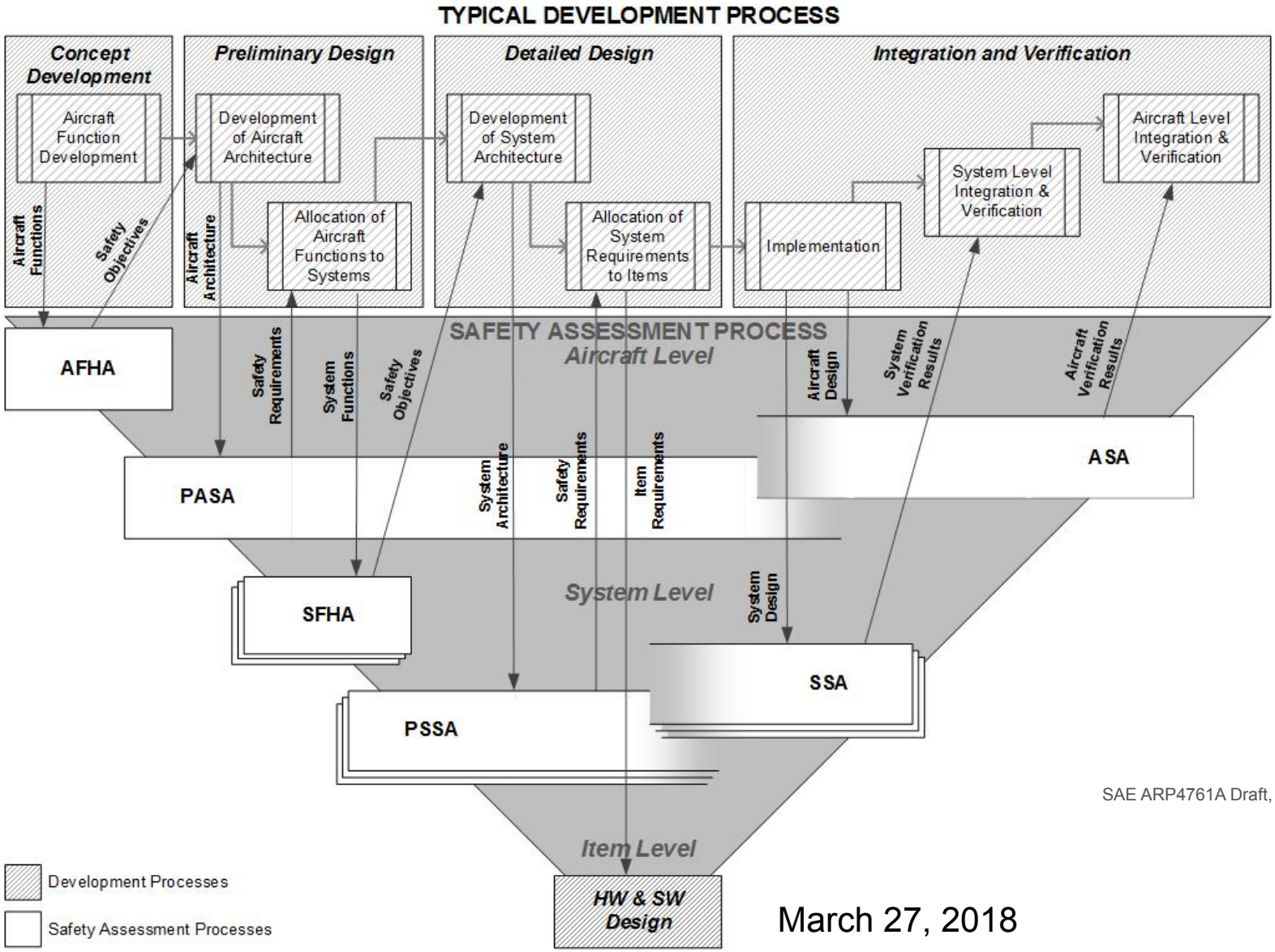
Asks if proposed architecture can meet objectives & captures safety requirements



SAE ARP4761A Draft, Figure D-1

ARP4761A Safety Assessment Process

Layers of safety assessments interact with the development process



SAE ARP4761A Draft, Figure 2

Role for STPA use with ARP4754A and ARP4761

The ARPs have included benefits similar to those in STAMP

STPA may fill an open area in these ARPs for some aspects such as complex automation and human interactions

Use of STPA is not (yet) deemed mature enough to include in these ARPs

Enable STPA as another tool in the overall safety assessment process:

- Create requirements, catch missing/incorrect requirements in development
- Anticipate safety issues in early stages of design / concept
- Improve effectiveness of safety analysis for preliminary architectures

Authorities and companies are independently evaluating STPA for potential means of compliance with regulations (e.g. 14 CFR 25.1309)

An AIR will help standardize the usage and provide a common understanding of STPA relationship to ARP4761 & 4754.

Chartered a new Aerospace Recommended Practice

Recognizing role for STPA use with ARP4754A and ARP4761

Goal: capture how STPA can be applied to the development and safety assessment of civil aircraft:

- Show how STPA relates to the ARP4754 and ARP4761 framework
- Provide a basic understanding of STPA and its strengths and limitations for aerospace industry and the potential uses of STPA for certification credit
- Same intended audience as ARP4761 and ARP4754 (system & engineers)
- Will assume working knowledge of these ARPs
- Provide the STPA basics to achieve AIR goals, referring out to detailed sources

Describe how STPA can be used and include an example; an AIR is generally not used to provide “guidance”

New Aerospace Information Report charted by S-18 for STPA (Jan 2018)

S-18’s main ARPs are about to be updated, so will tie to these updates

Plan is to have the AIR closely follow release of ARP4761A & ARP4754B

SAE S-18's STPA AIR6913 Working Outline

Using STPA During Development and Safety Assessment of Civil Aircraft

1) **Introduction**
   a) Purpose
   b) Definitions
2) **STPA Overview** (keep short, few pages)
   a) STPA High-Level Overview
      i. STPA Inputs / Outputs
   b) STPA Strengths / Limitations
   c) STPA Steps
      i. Defining STPA Scope
      ii. Control Structure
      iii. Identify Unsafe Control Actions
      iv. Identify Scenarios
      v. Creating Objectives & Requirements
3) **Relationship between STPA and ARP4761**
4) **Relationship between STPA and ARP4754**
5) **STPA Example Application**
   a) Example of STPA in aircraft development and safety assessment context

Finally……

S18 Committee Website:
http://www.sae.org/servlets/works/committeeHome.do?comtID=TEAS18

EUROCAE: http://www.eurocae.net/

More Questions? steven.c.beland@boeing.com


BOEING