ARP 4761 and STPA
(using the Wheel Brake Example in ARP 4761)

Cody Fleming

March 27, 2014

AEROASTRO
SYSTEMS ENGINEERING
RESEARCH LABORATORY
Goals of this Talk

1. How does regulation work in aviation?
   – ARP 4761, others

2. What are the objectives of 4761?
   – What methods, outputs, processes does it require?

3. Can STPA satisfy the 4761 objectives?

4. What is necessary for #3 to happen?
   – Do we have to re-write 4761, do we have to modify STPA, are they already compatible?
Agenda

• ARP4761 Process
• ARP4761 Application
• STPA Results
• 4761 and STPA
• Future
ARP 4761

• What is ARP 4761???

• “Describes guidelines and methods of performing safety assessment for certification of civil aircraft” [SAE 1996]
Development & Certification Process

Development and Design Guidance
[ARP-4754A, 2010]

Guidelines and methods for Safety Assessment
[ARP-4761, 1996]

Software Considerations
[DO-178, 2011]

Integrated Modular Avionics
[DO-297, 2005]

Design Guidance Electronic Hardware
[DO-254, 2000]
Safety Assessment Elements

- Functions, Design Constraints, Reqs, …
  - Functional Hazard Assessment
    - Identify failure, error conditions according to severity
    - Aircraft level & System level
  - Preliminary System Safety Assessment
    - Complete failure conditions list
    - Generate safety requirements
  - System Safety Assessment
    - Comprehensive analysis of implementation
# Development Assurance Levels

<table>
<thead>
<tr>
<th>Probability (Quantitative)</th>
<th>Per flight Hour</th>
<th>Probability (Descriptive)</th>
<th>Failure Condition</th>
<th>Severity Classification</th>
<th>Failure Cond. Effect</th>
<th>Development Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1.0E-3</td>
<td>Frequent</td>
<td>Minor</td>
<td>Minor</td>
<td>- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants</td>
<td>Level D</td>
</tr>
<tr>
<td>1.0E-5</td>
<td>Remote</td>
<td>Reasonably Probable</td>
<td>Major</td>
<td>Major</td>
<td>- significant reduction in safety margins or functional capabilities - ...</td>
<td>Level C</td>
</tr>
<tr>
<td>1.0E-7</td>
<td>Extremely Remote</td>
<td></td>
<td>Sever Major</td>
<td>Hazardous</td>
<td>- large reduction in safety margins or functional capabilities - ...</td>
<td>Level B</td>
</tr>
<tr>
<td>1.0E-9</td>
<td>Extremely Improbable</td>
<td></td>
<td>Catastrophic</td>
<td></td>
<td>- all failure conditions which prevent continued safe flight</td>
<td>Level A</td>
</tr>
</tbody>
</table>
4761 Basics

- **PRA**
  - Some requirements leveled in terms of probabilities
  - Not all requirements are leveled in terms of $P_e$
    - E.g. software assumed as $P_e=0$
    - Level A failures cannot be argued probabilistically

- **Methods**
  - FTA, FMEA
  - Zonal, CCA, DD, MA
Agenda

- ARP4761 Process
- ARP4761 Application
- STPA Results
- 4761 and STPA
- Future
4761 – Wheel Brake System

Pedal Pos. 1 → BSCU → Green Pump → Shut Off Selector Valve → Brake System Annunciation

Pedal Pos. 2 → BSCU → Blue Pump → Isolation Valve

BSCU

Brake System Annunciation

Green Pump

Blue Pump

Shut Off Selector Valve

Isolation Valve

Selector Valve

AS Shut Off Valve

Accumulator

Anti Skid

CMD/Anti Skid

Meter Valve

Mech. Pedal Position

Wheel
<table>
<thead>
<tr>
<th>Function</th>
<th>2 Failure Condition (Haz Description)</th>
<th>3 Phase</th>
<th>4 Effect of Failure Condition on Aircraft/Crew</th>
<th>5 Classificat’n</th>
<th>V&amp;V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decelerate Aircraft on the Ground</td>
<td>Loss of Deceleration Capability</td>
<td>Landing/RTO</td>
<td>See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unannunciated loss of deceleration capability</td>
<td>Landing/RTO</td>
<td>Crew is unable to decelerate the aircraft resulting In a high speed overrun</td>
<td>Catastrophic</td>
<td>Aircraft Fault Tree</td>
<td></td>
</tr>
<tr>
<td>b. Annunciated loss of deceleration capability</td>
<td>Landing</td>
<td>Crew selects a more suitable airport, notifies emergency ground support and prepares occupants for landing overrun.</td>
<td>Hazardous</td>
<td>Aircraft Fault Tree</td>
<td></td>
</tr>
<tr>
<td>c. Unannunciated loss of deceleration capability</td>
<td>Taxi</td>
<td>Crew is unable to stop the aircraft on the taxi way or gate resulting In low speed contact with terminal, aircraft, or vehicles</td>
<td>Major</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Annunciated loss of deceleration</td>
<td>Taxi</td>
<td>Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs</td>
<td>No Safety Effect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent Deceleration after V1</td>
<td>Takeoff</td>
<td>Crew is unable to takeoff due to application of brakes at the same time as high thrust settings resulting in a high speed overrun</td>
<td>Catastrophic</td>
<td>Aircraft Fault Tree</td>
<td></td>
</tr>
<tr>
<td>1 Function</td>
<td>2 Failure Condition (Haz Description)</td>
<td>3 Phase</td>
<td>4 Effect of Failure Condition on Aircraft/Crew</td>
<td>5 Classificat’n</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>Decelerate Aircraft on the Ground</td>
<td>d. Annunciated loss of deceleration</td>
<td>Taxi</td>
<td>Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs</td>
<td>No Safety Effect</td>
<td></td>
</tr>
</tbody>
</table>
PSSA

- Continuation of FHA on “systems”

- Refined requirements, refined failure assessments, ...
PSSA

Preliminary Fault Tree

- Loss of Aircraft (LOSSOFAC)
  - Unannunciated Loss of Deceleration Capability (UNANLSSDEC)
    - Prob: 5.00E-09
  - Inadvertent Deceleration After V1 (INADDEC+V1)
  - Other Failure Conditions (OTHERFAILS)
  - Inadvertent Thrust Reverse After V1 (INADTR+V1)
    - Prob: 5.00E-09
  - InadvertentSpoiler Deployment After V1 (INADSPL+V1)
    - Prob: 5.00E-09
  - Inadvertent Wheel Braking After V1 (INADW/B1)
    - Prob: 5.00E-09

- Unannunciated Loss of Thrust Reversers (UNANLSST/R)
  - Prob: 5.00E-03

- Loss of Effective Wheel Braking (UNLSSEFFWB)
  - Prob: 1.00E-05

- Unannunciated Loss of All Speedbrakes on Contaminated Runway (UNLSSPDBR)
  - Prob: 5.00E-07

- Unannunciated Loss of All Wheel Braking (UNANLSSWB)
  - Prob: 5.00E-07
## Derived Safety Requirements

<table>
<thead>
<tr>
<th>Safety Requirement</th>
<th>Design Decisions</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Loss of all wheel braking (unannunciated or annunciated) during landing or RTO</td>
<td>More than one hydraulic system required to achieve the objective (service experience). Dual channel</td>
<td>The overall wheel brake system availability can reasonably satisfy this requirement. See PSSA FTA below.</td>
</tr>
<tr>
<td>2. Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel</td>
<td>Separate the rudder and nose wheel steering system from the wheel braking system. Balance hydraulic</td>
<td>The wheel braking system will be shown to be sufficiently independent from the rudder and nose wheel</td>
</tr>
<tr>
<td>steering during landing shall be less than 5E-7 per flight.</td>
<td>supply to each side of the wheel braking system.</td>
<td>steering systems. System separation between these systems will be shown in the zonal safety analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and particular risk analysis</td>
</tr>
</tbody>
</table>
## Derived Safety Requirements

<table>
<thead>
<tr>
<th>Safety Requirement</th>
<th>Design Decisions</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The primary and secondary system shall be designed to preclude any common threats (tire burst, tire shred, flailing tread, structural deflection).</td>
<td>Install hydraulic supply to the brakes in front and behind the main gear leg.</td>
<td>Compliance will be shown by ZSA and PRA. <em>(Editor's Note: In this example only for the main gear bay zone and the tire burst particular risk.)</em>.</td>
</tr>
<tr>
<td>2. The primary and secondary system shall be designed to preclude any common mode failures (hydraulic system, electrical system, maintenance, servicing, operations, design, manufacturing, etc.).</td>
<td>Choose two different hydraulic systems to supply the brakes, emergency braking without electrical power.</td>
<td>Compliance will be shown by CMA.</td>
</tr>
</tbody>
</table>
• Continuation from PSSA

• Based on final designs and implementations
Detectable BSCU 1 Failure Causes Bad Data Which is Provided to Normal System MV

BSCU1DETD

2.00E-09

BSCU 1 P/S Failure/ Error Causes Bad Data Which is Provided to Normal System MV

BSCU1PSIND

1.00E-09

BSCU 1 Power Supply Motor Stuck Valid

BS1PSMOFV

PROB: 2.00E-02 (1)  
RATE: 2.00E-07   
EXPO: 1.00000  
Budgeted F.R.

BSCU 1 Power Supply Failure Causes Bad Data

BSCU1PSF

PROB: 5.00E-08 (1)  
RATE: 1.20E-05  
EXPO: 0.004167  
Budgeted F.R.

BSCU 1 Monitor Channel Always Reports Valid

BSCU1MORV

/ H

BSCU 1 Monitor Channel Design Error

BSCU1MOFV

PROB: 2.00E-02 (1)  
RATE: 2.00E-07  
EXPO: 1.00000  
Budgeted F.R.

BSCU 1 Failure Causes Bad Data To be Sent to Normal System MV

BSCU1CDIND

1.00E-09

BSCU 1 I/O or CPU Failure/Error Causes Bad Data

BSCU1CDF

5.00E-08

BSCU 1 Command Channel CPU or I/O Failure/Error Causes Bad Data

BSCU1OF

PROB: 1.88E-08 (1)  
RATE: 4.50E-06  
EXPO: 0.4167  
Budgeted F.R.

BSCU 1 Command Channel CPU or I/O Failure Errors Causes Bad Data

BSCU1CPUBD

3.12E-08

BSCU 1 Command Channel CPU Hardware Failure Causes Bad Data

BSCU1FAILS

PROB: 3.13E-08 (1)  
RATE: 7.50E-06  
EXPO: 0.4167  
Budgeted F.R.

BSCU 1 CPU Function Design Error Causes Bad Data

BSCU2FAILS

PROB: 0.00E+00  
H

Level A

Computer-related FTA
Computer-related FTA

- BSCU 1 Monitor Channel Always Reports Valid
- BSCU1MORV

BSCU 1 Validity Monitor Failed Valid Due to Hardware Failure
- PROB: 2.00E-02 (1)
- RATE: 2.00E-07
- EXPO: 1.00000
- Budgeted F.R.

BSCU 1 Monitor Channel Design Error
- PROB: 0.00E+00 (0)
- Level B
- 2.00E-02

BSCU 1 Monitor
- 2.00E-02

PROB: 0.00E+00 (0)
Safety Assessment Elements

<table>
<thead>
<tr>
<th>Probability (Quantitative)</th>
<th>1.0</th>
<th>1.0E-3</th>
<th>1.0E-5</th>
<th>1.0E-7</th>
<th>1.0E-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Assurance Level</td>
<td>Level D</td>
<td>Level C</td>
<td>Level B</td>
<td>Level A</td>
<td></td>
</tr>
</tbody>
</table>

- Flow into DO-178 (software) and DO-254 (hardware)
- Those documents provide guidance in how to achieve the different levels (a discussion for another time)
Agenda

• Motivation
• ARP4761 Process
• ARP4761 Application
• STPA Results
• 4761 and STPA
• Future
Control Structure

- Crew, left/right
  - Anti-skid on/off switch
  - Autobrake arm/rate switch
  - Brake pedal demand

- Sensory inputs
  - Spoiler/air brake position
  - Ground/air status
  - Nosewheel rotation speed
  - Ground speed
  - Altitude
  - Flight mode

- Brake Controller
  - Annunciations/displays
  - Valve positions

- Meter Valves
  - Hydraulic pressure

- Bogie Sensors
  - Main wheel rotational speed
  - Disc temperature
  - Tire pressure

- Main Wheel Bogie Assy

- Other Aircraft Systems

- External Sensors
  - Main wheel rotational speed
  - Disc temperature
  - Tire pressure

- Hydraulic Pressure
<table>
<thead>
<tr>
<th>Control Action Flights Crew:</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too soon, too late, out of sequence</th>
<th>Stopped too soon, applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREW.1 Manual braking via brake pedals</td>
<td>CREW.1a1 Not providing manual braking during landing or RTO while autobrake not providing braking (or insufficient braking), leading to overshoot</td>
<td>CREW.1b1 Manual braking provided with insufficient pedal pressure, resulting inadequate deceleration during landing</td>
<td>CREW.1c1 Manual braking applied before touchdown causes wheel lockup, loss of control, tire burst</td>
<td>CREW.1d1 Manual braking stopped too soon before safe taxi speed reached, resulting in overspeed or overshoot</td>
</tr>
<tr>
<td></td>
<td>CREW.1b2 Manual braking provided with excessive pedal pressure, resulting in loss of control, passenger/crew injury, brake overheating, brake fade or tire burst during landing</td>
<td>CREW.1c1 Manual braking applied too late to avoid collision or conflict with another object</td>
<td>CREW.1d2 Manual braking applied too long, resulting in stopped aircraft on runway or active taxiway</td>
<td></td>
</tr>
</tbody>
</table>
### Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too soon, too late, out of sequence</th>
<th>Stopped too soon, applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSCU.1 Command Braking Pressure</td>
<td>BSCU.1a1 Braking pressure not provided during RTO (to V1), resulting in inability to stop within available runway length</td>
<td>BSCU.1b1 Braking pressure commanded excessively, resulting in rapid deceleration and injury in pushback</td>
<td>BSCU.1c1 Braking pressure applied before touchdown, resulting in tire burst, loss of control, injury, other damage</td>
<td>BSCU.1d1 Reduced deceleration if brake pressure is released during landing roll before TBD taxi speed attained</td>
</tr>
<tr>
<td></td>
<td>BSCU.1a2 Brake pressure not provided during landing roll, resulting in insufficient deceleration and potential overshoot</td>
<td>BSCU.1b2 Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration</td>
<td>BSCU.1c2 Braking pressure applied too long after touchdown, resulting in insufficient deceleration and potential loss of control, overshoot</td>
<td>BSCU.1d2 Stop on runway if brake pressure not released during landing roll after TBD taxi speed attained</td>
</tr>
</tbody>
</table>
BSCU (Brake Comp.) Analysis

**Unsafe Control Action:** BSCU.1b2
Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration

- **Controller:** BSCU
- **Actuator:** Meter valves
- **Controlled Process:** Brake Caliper
- **Sensor:** Caliper and WOW Sensors

**Manual braking pressure incorrectly applied or misread**

**Flawed Control Algorithm:**
Algorithm for determining that aircraft has lifted off is incorrect
Due to...
Algorithm for determining pilot braking...

**Brake apply signal given during takeoff**
Command to close valve (and release brake) is given to incorrect valve; e.g., to Green sys, during alternate mode

**Actuator: Meter valves**
- Signal to release brakes mis-read/not received
- Meter valve stuck open upon initiation of takeoff
- Meter valve incompletely closed

**Controlled Process: Brake Caliper**
- Corroded brake piston causes caliper to stay engaged;
- Contaminated brake fluid causes caliper to remain engaged, even after valves are correctly closed;
- Fluid not released, or spring mechanism cannot overcome latent hydraulic pressure

**Sensor: Caliper and WOW Sensors**
- Hydraulic pressure measurement error
- Weight on wheels incorrect or misread
- Aircraft pitches (e.g., due to winds) resulting in inconsistent weight-on-wheels measurements
- Sensors degrade or lose calibration
- Sensors effected by weather

**Incomplete or inaccurate process model:**
- BSCU is unaware that aircraft is in takeoff phase (but may still have correct WOW and air/groundspeed readings and thus applies brakes)
  - **Proc Model Variables:** Flight Mode
- BSCU is unaware that aircraft has passed V₁ speed
  - **Proc Model Variables:** Groundspeed
- BSCU incorrectly assesses that aircraft has left ground
  - **Proc Model Variables:** Altitude, WOW

**Flawed Control Algorithm:**
Algorithm for determining when it is too late to apply brakes during takeoff is incorrect, i.e., incorrect computation of V₁ speed

V₁ speed incorrect or misread
Ground/airspeed incorrect or misread
Flight mode incorrect or misread

Mismatch in data format; Mismatch in units (Eng v Met)
Sensor readings are too slow (BSCU computes at 100Hz but sensor updates at 1Hz)
BSCU (Brake Comp.) Analysis

Flawed Control Algorithm:

Unsafe Control Action: BSCU.1b2
Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration

Incomplete or inaccurate process model:
- BSCU is unaware that aircraft is in takeoff phase (but may still have correct WOW and air/groundspeed readings and thus applies brakes)

**Proc Model Variables:** Flight Mode
- BSCU is unaware that aircraft has passed \( V_1 \) speed

**Proc Model Variables:** Groundspeed
- BSCU incorrectly assesses that aircraft has left ground

**Proc Model Variables:** Altitude, WOW

- Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration
- Incomplete or inaccurate process model:
  - BSCU is unaware that aircraft is in takeoff phase (but may still have correct WOW and air/groundspeed readings and thus applies brakes)
    **Proc Model Variables:** Flight Mode
  - BSCU is unaware that aircraft has passed \( V_1 \) speed
    **Proc Model Variables:** Groundspeed
  - BSCU incorrectly assesses that aircraft has left ground
    **Proc Model Variables:** Altitude, WOW

- Manual braking pressure incorrectly applied or misread
- \( V_1 \) speed incorrect or misread
- Ground/airspeed incorrect or misread
- Flight mode incorrect or misread

- Mismatch in data format;
  - Mismatch in units (Eng v Met)
- Sensor readings are too slow (BSCU computes at 100Hz but sensor updates at 1Hz)

- Flawed Control Algorithm:
  - Algorithm for determining when it is too late to apply brakes during takeoff is incorrect
  - Algorithm for determining that aircraft has lifted off is incorrect
  - Due to...

- Flawed Control Algorithm:
  - Algorithm for determining pilot braking...

- Hydraulic pressure higher than valve capability
- Caliper pressure not detected
- Mismatch in data format;
  - Mismatch in units (Eng v Met)
- Sensor readings are too slow (BSCU computes at 100Hz but sensor updates at 1Hz)

- Incomplete or inaccurate process model:
  - BSCU is unaware that aircraft is in takeoff phase (but may still have correct WOW and air/groundspeed readings and thus applies brakes)
  **Proc Model Variables:** Flight Mode
  - BSCU is unaware that aircraft has passed \( V_1 \) speed
  **Proc Model Variables:** Groundspeed
  - BSCU incorrectly assesses that aircraft has left ground
  **Proc Model Variables:** Altitude, WOW

- Mismatch in data format;
  - Mismatch in units (Eng v Met)
- Sensor readings are too slow (BSCU computes at 100Hz but sensor updates at 1Hz)
Crew Analysis

[Thornberry 2014]
Agenda

• ARP4761 Process
• ARP4761 Application
• STPA Results
• 4761 and STPA
• Future
A Note on “Annunciation”

• Air France 447 had plenty of annunciaciones prior to crash

[Image: Air France 447 accident scene]
STPA and 4761 FMEA

• Where is the pilot in 4761?
  – The only relevant thing to pilot is “unannunciated”,
  – What about when and why it is annunciacted,
  – Assumes that pilot will be able to account for and react to brake failures

• Why?
  – It is not just because FTAs and other methods
STPA and 4761

• What about software?

  – Software often “ends” with a failure node in a FTA

  – There are other tools in the suite of tools allowed by 4761 that we need to assess

  – Software development is (somewhat) out-of-scope for 4761

  – But STPA can help here!!!
STPA and 4761

• Can STPA find the things about hardware that are already in existing techniques?

  – How does it compare with FMEA & FTA?

  – Does it find things beyond what they find?

  – Does STPA help to achieve 4761 objectives?
Agenda

• ARP4761 Process
• ARP4761 Application
• STPA Results
• 4761 and STPA
• Future
Next Few Months

• STPA Analysis is ongoing
  – Fidelity of STPA analysis \( \approx \) fidelity of ARP analyses, examples

• More thorough analysis
  – of how STPA compares to existing techniques
  – of how STPA fits into (or doesn’t) ARP4761
Longer Term

• Can we get STPA into ARP4761?

• What will ARP4761A look like?

• Does STPA help to achieve 4761 (and 4754A) objectives?
Does the FAA want this?
References

1. NTSB Case Number: DCA13IA037, Interim Factual Report Boeing 787-8, JA829J, Japan Airlines (Boston, Massachusetts, January 7, 2013), National Transportation Safety Board, Office of Aviation Safety, March 7, 2013

2. Boeing 787 Program Information “About the Dreamliner” (accessed 20 March 2014)
   http://www.boeing.com/boeing/commercial/787family/background.page


5. 787 picture


7. Ross & Tweedie, The Telegraph, UK
   http://www.telegraph.co.uk/technology/9231855/Air-France-Flight-447-Damn-it-were-going-to-crash.html, April 28, 2012, Getty Images
BSCU (Brake Comp.) Analysis

Unsafe Control Action: BSCU.1b2
Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration

Sensor: Caliper and WOW Sensors

Hydraulic pressure measurement error
Weight on wheels incorrect or misread
Aircraft pitches (e.g. due to winds) resulting in inconsistent weight-on-wheels measurements
Sensors degrade or lose calibration
Sensors effected by weather

Control

Flawed Control Algorithm:
Algorithm for determining that aircraft has lifted off is incorrect
Due to…
Algorithm for determining pilot braking...

Brake apply signal given during takeoff
Command to close valve (and release brake) is given to incorrect valve; e.g. to Green sys. during alternate mode

Actuator: Meter valves
Signal to release brakes mis-read/mis-received
Meter valve stuck open upon initiation of takeoff
Meter valve incompletely closed

Caliper pressure given
Hydraulic pressure higher than valve capability

Caliper pressure not detected

Manual braking pressure incorrectly applied or misread

Manual braking pressure incorrectly applied or misread

Flawed Control Algorithm:
Flawed Control Algorithm:
Algorithm for determining when it is too late to apply brakes during takeoff is incorrect, i.e. incorrect computation of \( V_{1s} \) speed

Flawed Control Algorithm:
Algorithm for determining that aircraft has lifted off is incorrect
Due to…
Algorithm for determining pilot braking...
**BSCU (Brake Comp.) Analysis**

**Unsafe Control Action:** BSCU.1b2
Braking pressure applied inappropriately during takeoff, resulting in inadequate acceleration

**Controller:** BSCU

**Actuator:** Meter valves
- Signal to release brakes mis-read/not received
- Meter valve stuck open upon initiation of takeoff
- Meter valve incompletely closed

**Controlled Process:** Brake Caliper
- Corroded brake piston causes caliper to stay engaged;
- Contaminated brake fluid causes caliper to remain engaged, even after valves are correctly closed;
  Fluid not released, or spring mechanism cannot overcome latent hydraulic pressure

**Sensor:** Caliper and WOW Sensors
- Sensors degrade or lose calibration
- Sensors effected by weather
- Meter valve position incorrectly read

**Flawed Control Algorithm:**
- Algorithm for determining that aircraft has lifted off is incorrect
  Due to...
- Algorithm for determining pilot braking

**Manual braking pressure incorrectly applied or misread**

**Signal to release brakes mis-read/not received**

**Meter valve stuck open upon initiation of takeoff**

**Meter valve incompletely closed**

**Caliper pressure given**
- Hydraulic pressure higher than valve capability

**Caliper pressure not detected**
• Functions = intended behavior of a product based on a defined set of requirements regardless of implementation
Definitions

• Failures = loss of function or a malfunction of a system or a part thereof (different than 4754)
Definitions

- Errors = (1) an occurrence arising as a result of an incorrect action or decision by personnel operating or maintaining a system, (2) a mistake in specification, design, or implementation
• Hazards = potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof
Definitions

• These definitions present some hurdles in terms of communication

• But STPA can help with ARP4761…especially with identifying ‘errors’, why they might occur, how to generate requirements
4761 Objectives

• FHA Outputs
  – FHA input function list
  – Environmental and Emergency Configuration List
  – Derived safety requirements for the design at each level
  – FHA Report
    • Functions, failure conditions, phase of ops, …
4761 Objectives

• PSSA Outputs
  – Planned compliance with FHA requirements
  – Updated FHAs
  – Material supporting classification list
  – Failure condition list
  – Lower level safety requirements (including DALs)
  – Qualitative FTAs
  – Preliminary CCAs
  – Operational requirements
4761 Objectives

• SSA Outputs
  – Updated failure condition list or FHA which includes rationale showing compliance with safety requirements (qual and quant)
  – Documentation showing how req’s for the design of the system items’ installation have been incorporated (segregation, protection, etc.)
  – Materials used to validate the failure condition classification
  – Maintenance tasks
  – Documentation showing how system has been developed according to DAL
Background

• Aircraft are VERY safe

• Development & Certification process has been very successful

• This is due at least in part to ARP4761

• Accidents due to mechanical failure have decreased dramatically over the years…
Background

• Why has approach been so successful?

• Will the assumptions hold in the future?
Past, Present, and Future

- What do we see in the aircraft of ‘yesterday’?

- What do we see in the aircraft of ‘today’?

- What will we see in the aircraft of ‘tomorrow’?
Past

[UWB, 2010]
Present

[Bicheno-Brown, 2012]
Fuselage – CFRP composite
HUD
Electric power (vs bleedless and hydraulic)
LiCo batteries
IMA, AFDX (ethernet comm)
Self monitoring & Reporting
Increasing global manufacturing

[Bicheno-Brown, 2012]
Future
A Note on PRA

• Boeing 787 LiCo Batteries

• Prediction/Certification:
  – No fires within $10^7$ flight hours
  – Followed 4761 certification paradigm

• Actual experience:
  – Within 52,000 flight hours – 2 such events
  – $2.6 \times 10^4$ flight hours [NTSB 2013]
A Note on PRA

• I love the 787 and I continue to cheer it on!

• LiCo technology a fairly significant departure from yesteryear’s battery technology
  – More energy density, requiring more complexity to control it

• This is a battery – what will happen if/when we drastically change the role of software & humans?