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

Cody Fleming

March 27, 2014

MIT 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

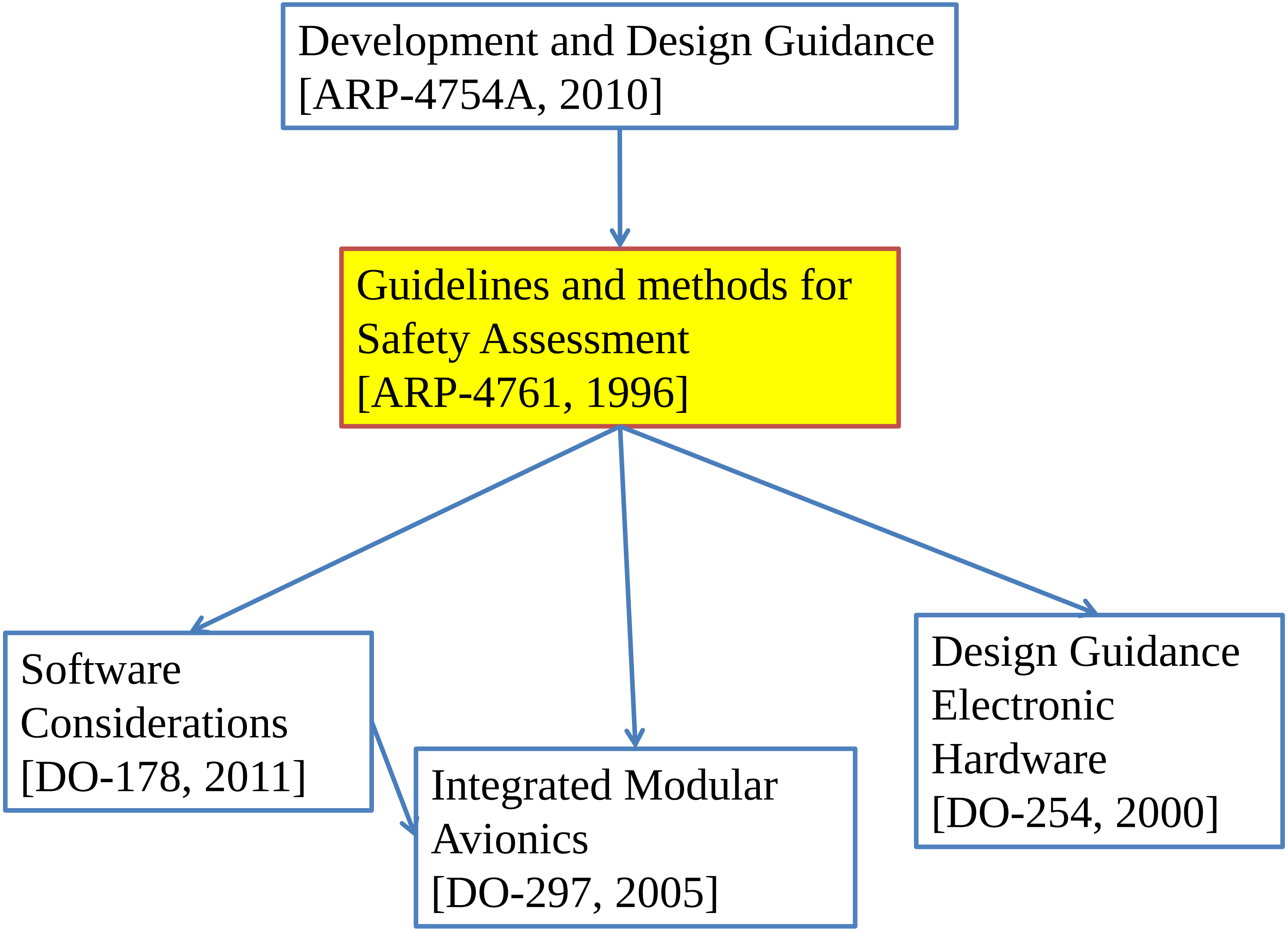
- ARP4761 Process
- ARP4761 Application
- STPA Results
- 4761 and STPA
- Future

ARP 4761

- What is ARP 4761???

- "Describes guidelines and methods of performing safety assessment for certification of civil aircraft" [SAE 1996]

Development & Certification Process



Safety Assessment Elements

- Functions, Design Constraints, Reqs, …

FHA

- *Functional Hazard Assessment*
- Identify failure, error conditions according to severity
- Aircraft level & System level

PSSA

- *Preliminary System Safety Assessment*
- Complete failure conditions list
- Generate safety requirements

SSA

- *System Safety Assessment*
- Comprehensive analysis of implementation

Development Assurance Levels

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

4761 Basics

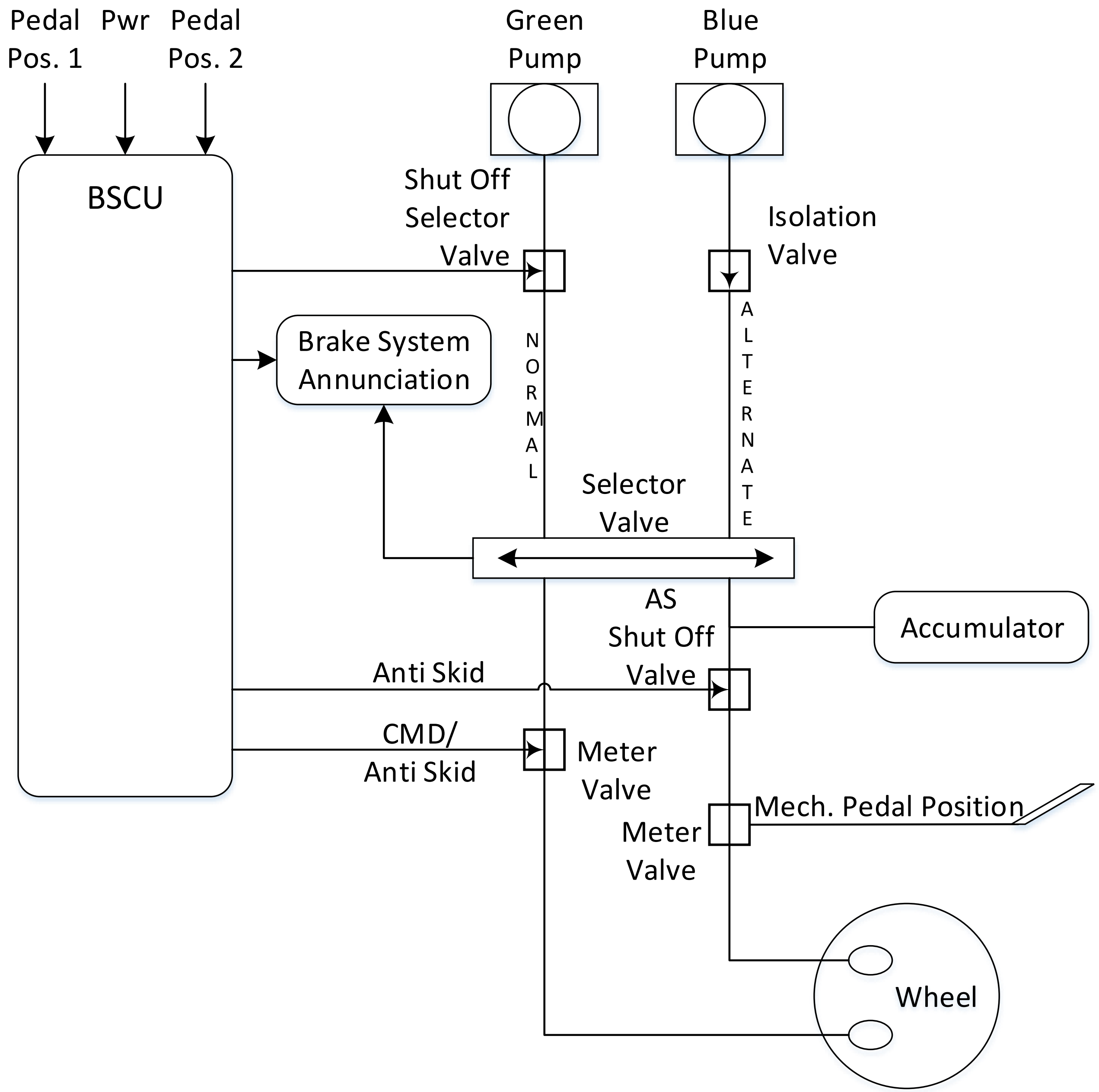
- PRA
  - Some requirements leveled in terms of probabilities
  - Not all requirements are leveled in terms of Pe
    - E.g. software assumed as Pe=0
    - Level A failures cannot be argued probabilistically

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

Agenda

- ARP4761 Process
- ARP4761 Application
- STPA Results
- 4761 and STPA
- Future

4761 – Wheel Brake System



Aircraft FHA

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

Aircraft FHA

1 Function	2 Failure Condition (Haz Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classificat'n
Decelerate Aircraft on the Ground	d. Annunciated loss of deceleration	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs	No Safety Effect

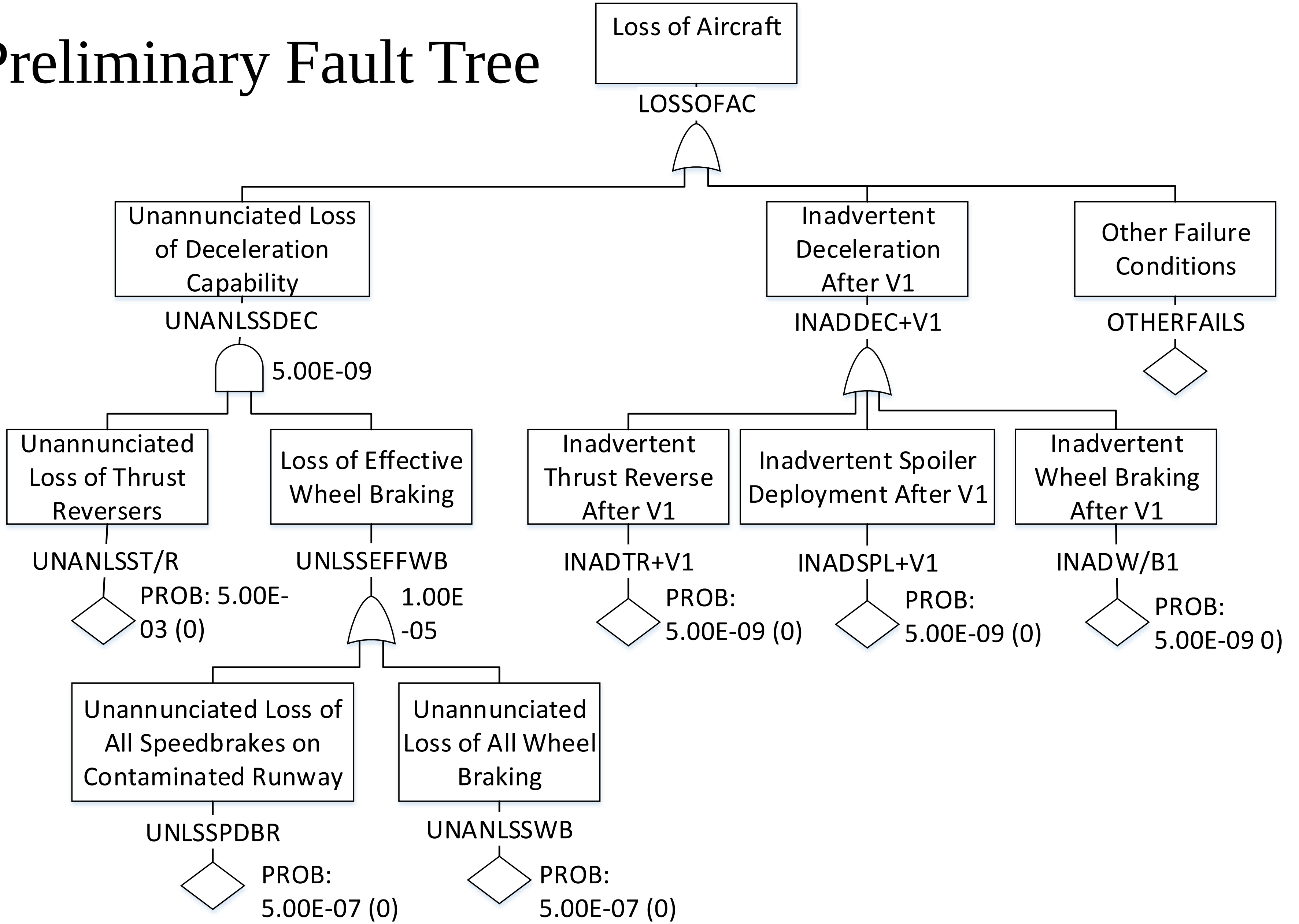
PSSA

- Continuation of FHA on “systems”

- Refined requirements, refined failure assessments, …

PSSA

Preliminary Fault Tree



Derived Safety Requirements

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

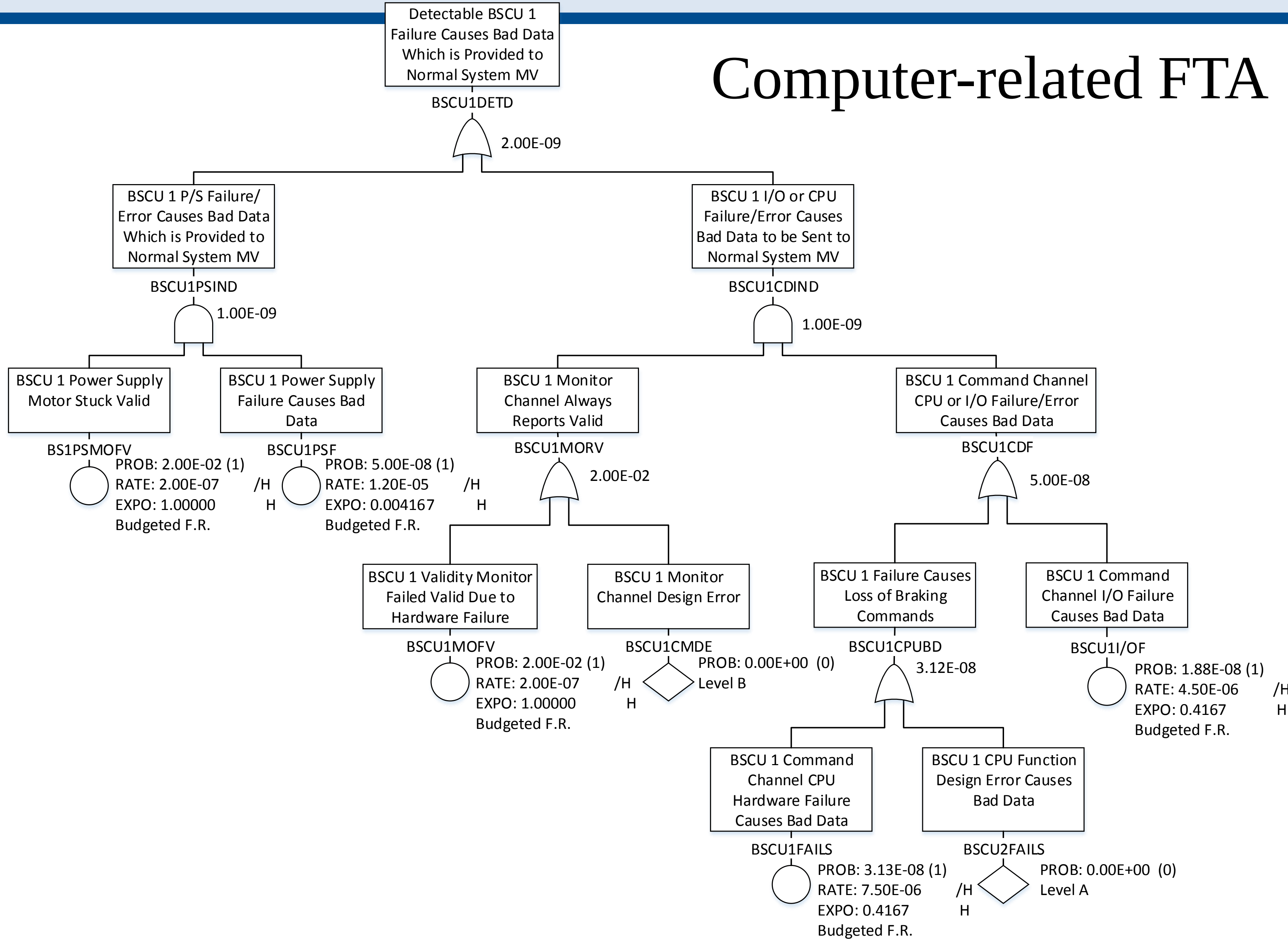
Derived Safety Requirements

Safety Requirement	Design Decisions	Remarks
1. The primary and secondary system shall be designed to preclude any common threats (tire burst, tire shred, flailing tread, structural deflection).	Install hydraulic supply to the brakes in front and behind the main gear leg.	Compliance will be shown by ZSA and PRA. *(Editor's Note: In this example only for the main gear bay zone and the tire burst particular risk.).*
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.).	Choose two different hydraulic systems to supply the brakes, emergency braking without electrical power.	Compliance will be shown by CMA.

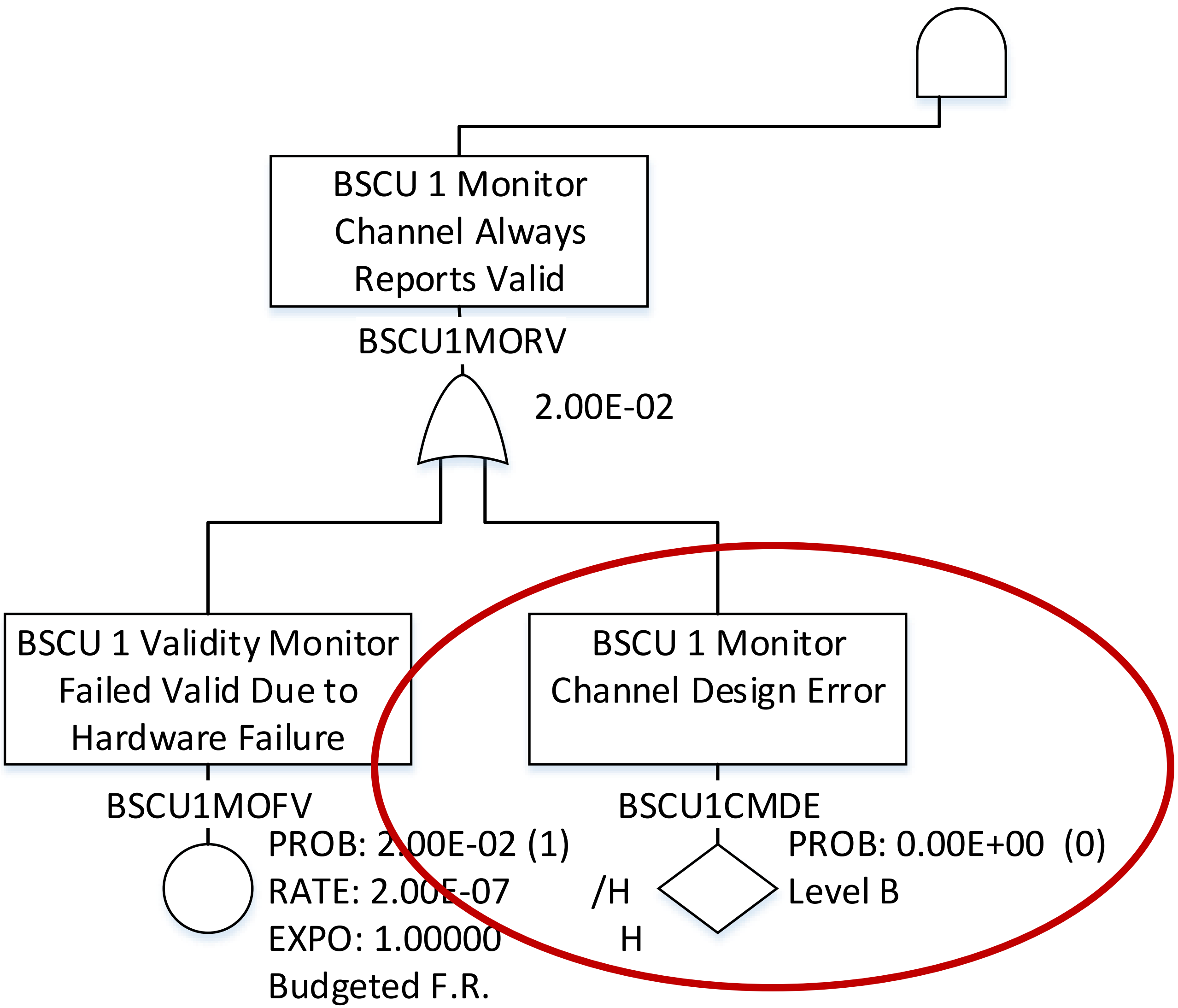
SSA

- Continuation from PSSA
- Based on final designs and implementations

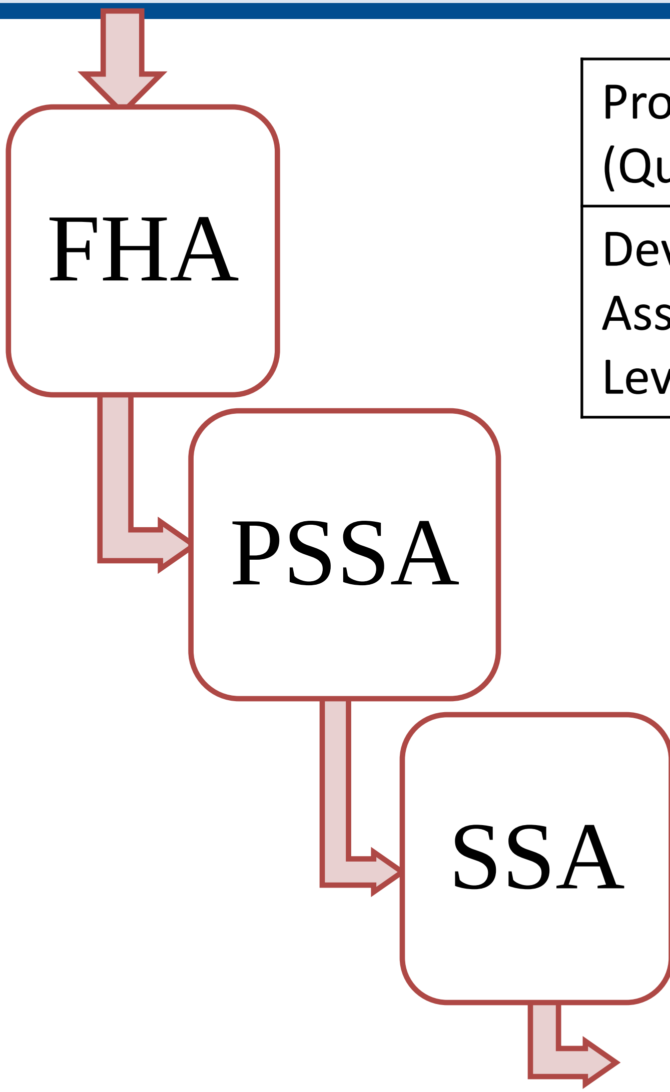
Computer-related FTA



Computer-related FTA



Safety Assessment Elements



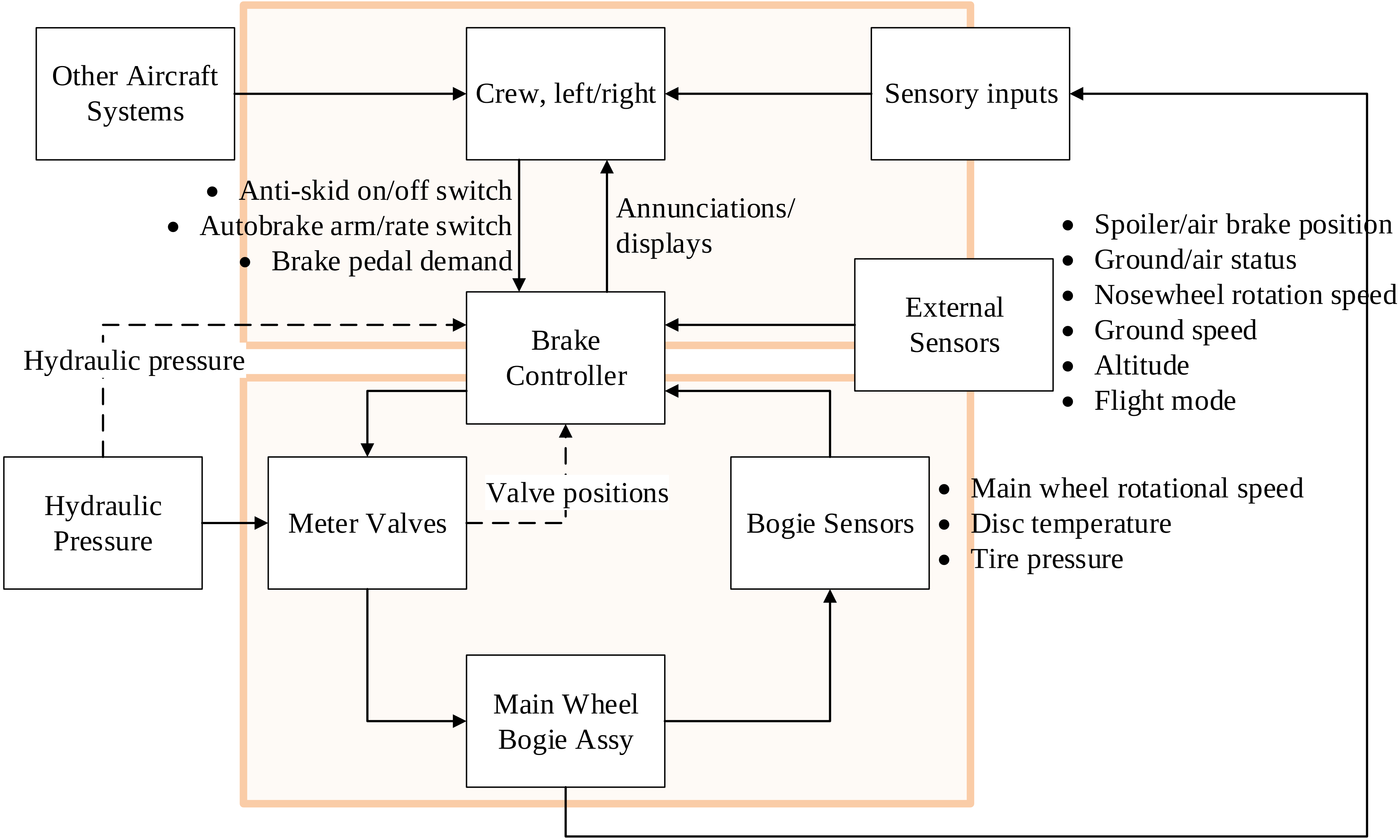
Probability (Quantitative)	1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Development Assurance Level	Level D		Level C	Level B	Level A

- 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



Unsafe Control Actions

Control Action Flight Crew:	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
CREW.1 Manual braking via brake pedals	CREW.1a1 Not providing manual braking during landing or RTO while autobrake not providing braking (or insufficient braking), leading to overshoot	CREW.1b1 Manual braking provided with insufficient pedal pressure, resulting inadequate deceleration during landing	CREW.1c1 Manual braking applied before touchdown causes wheel lockup, loss of control, tire burst	CREW.1d1 Manual braking stopped too soon before safe taxi speed reached, resulting in over-speed or overshoot
		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	CREW.1c1 Manual braking applied too late to avoid collision or conflict with another object	CREW.1d2 Manual braking applied too long, resulting in stopped aircraft on runway or active taxiway

Unsafe Control Actions

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

BSCU (Brake Comp.) Analysis

SERL
MIT AEROASTRO

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

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

Controller: BSCU

Flawed Control Algorithm:
Algorithm for determining when it is too late to apply brakes during takeoff is incorrect, i.e. incorrect computation of V_1 speed

Flawed Control Algorithm:

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

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)

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

* Meter valve position incorrectly read

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

Caliper pressure given
Hydraulic pressure higher than valve capability

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

Caliper pressure not detected

BSCU (Brake Comp.) Analysis

SERL
MIT
AEROASTRO

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

Flawed Control
Algorithm:
Alg

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

speed incorrect or misread
ound/airspeed incorrect or misread
ght mode incorrect or misread

lismatch in data format;
lismatch in units (Eng v
let)
ensor readings are too
ow (BSCU computes at
00Hz but sensor
pdates at 1Hz)

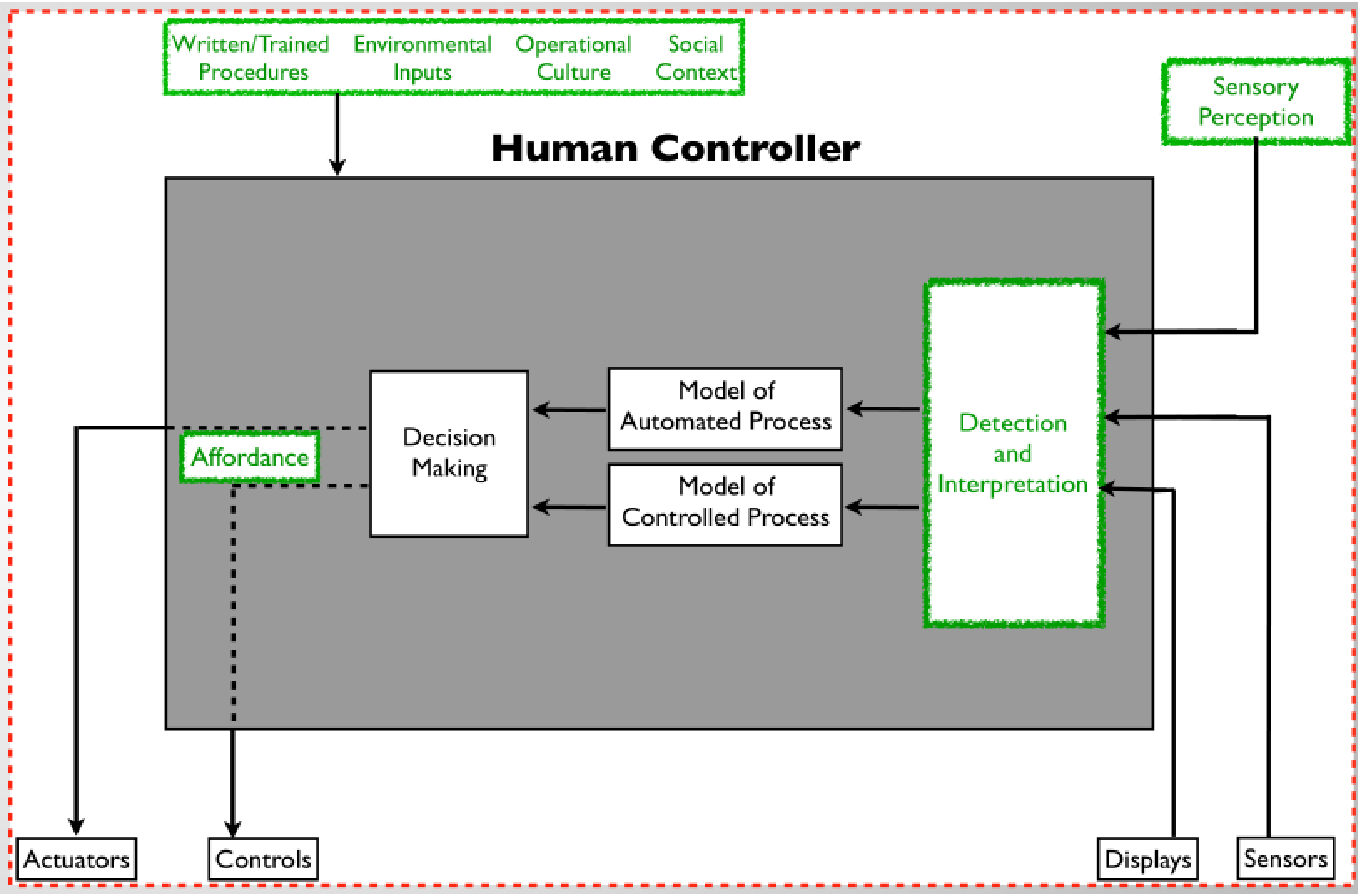
d WOW Sensors

measurement error
ncorrect or misread
g. due to winds)
stent weight-on-
nts
lose calibration
weather

pressure not detected

mechanism cannot overcome latent
hydraulic pressure

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 annunciations prior to crash

[Telegraph/Getty Images 2012]

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 annunciated,
  - 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 ≈ 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 ARP4761***<u>A</u>*** 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?
3. Boeing 787 Wikipedia page (accessed 20 March 2014) http://en.wikipedia.org/wiki/Boeing_787_Dreamliner
4. ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Warrensdale: SAE International, 1996. Print.
5. 787 picture
6. The Unwanted Blog, http://up-ship.com/blog/?p=6045, May 01, 2010
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

SERL MIT AEROASTRO

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

__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

Contr

Fla
Alg
Alg
det
late
dur
inc
cor

Fla
Alg

read

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

__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

__Actuator:__ **Meter valves**

Signal to release brakes mis-read/n received
Meter valve stuck open upon initia takeoff
Meter valve incompletely closed

Caliper pressure given
Hydraulic pressure higher than valve capability

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

Caliper pressure not detected

BSCU (Brake Comp.) Analysis

SERL
MIT AEROASTRO

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

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

Manual braking pressure incorrectly applied or misread

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

* Meter valve position incorrectly read

Sensor: C

Hydrauli
Weight o
Aircraft p
resulting
wheels m
Sensors c
Sensors e

takeoff
Meter valve incompletely closed

Caliper pressure given
Hydraulic pressure higher than valve capability

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

wheels measurements
Sensors degrade or lose calibration
Sensors effected by weather

Caliper pressure not detected

Definitions

- 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

Definitions

- 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?

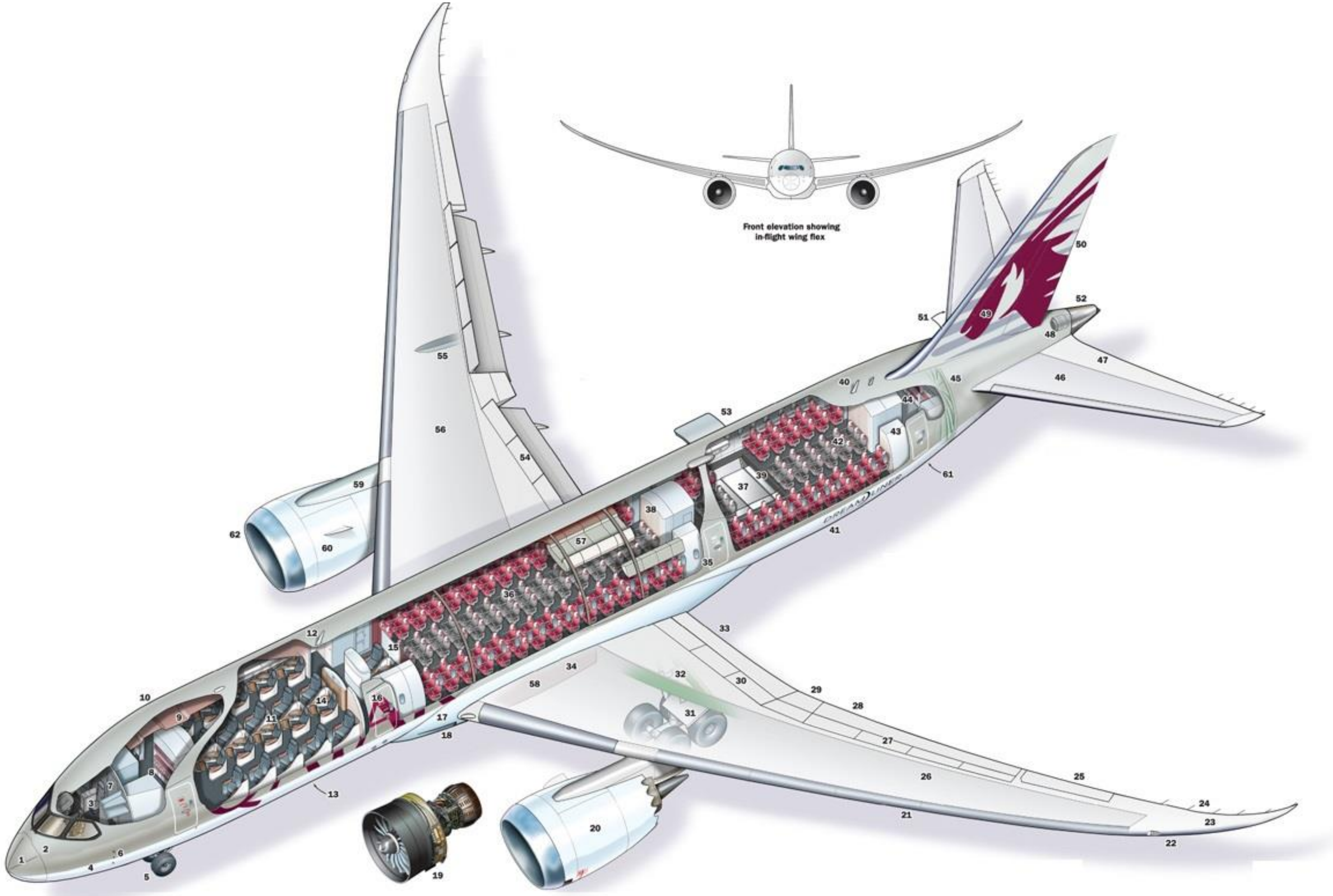
Past, Present, and Future

- 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

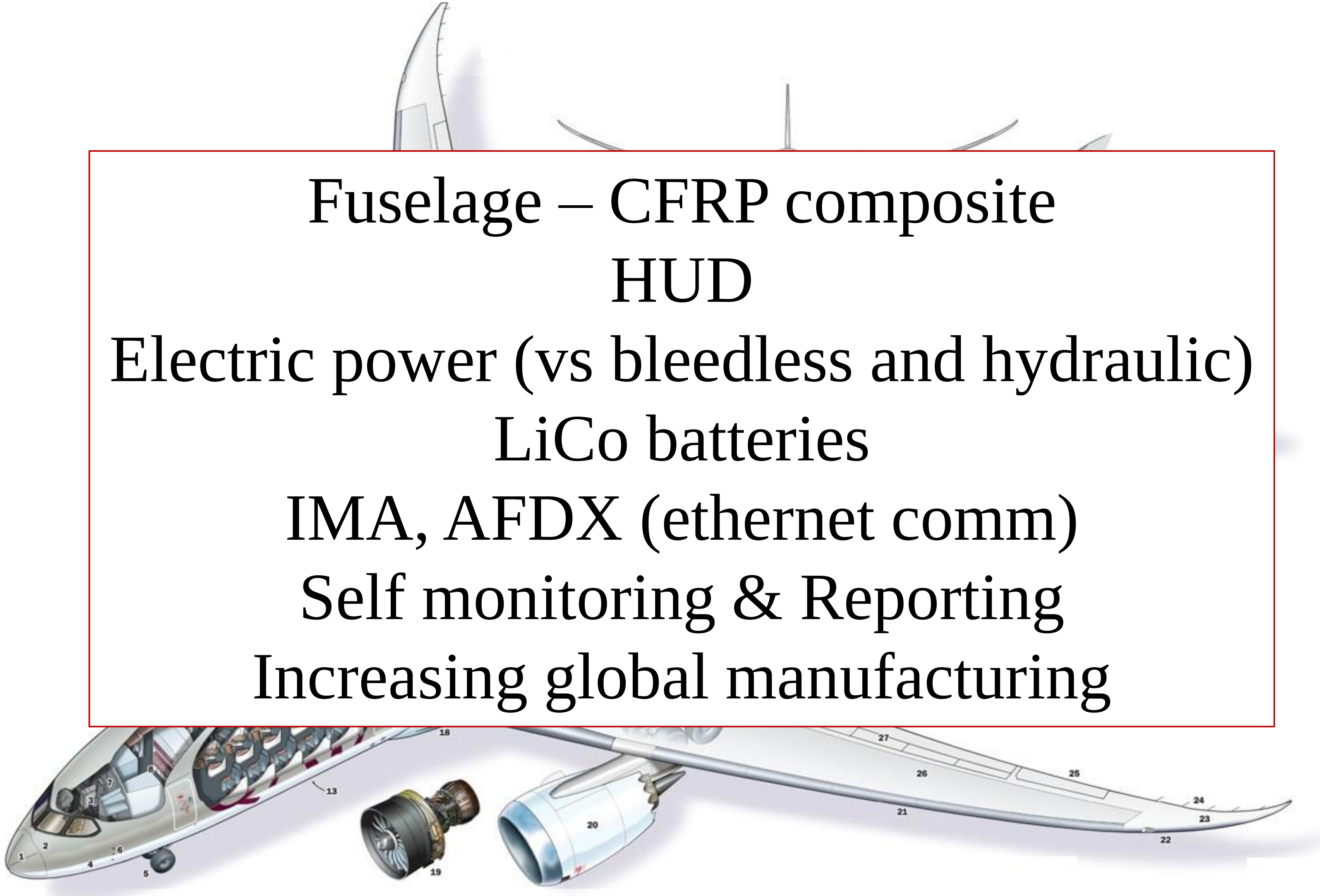
[UWB, 2010]

Present



[Bicheno-Brown, 2012]

Present



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

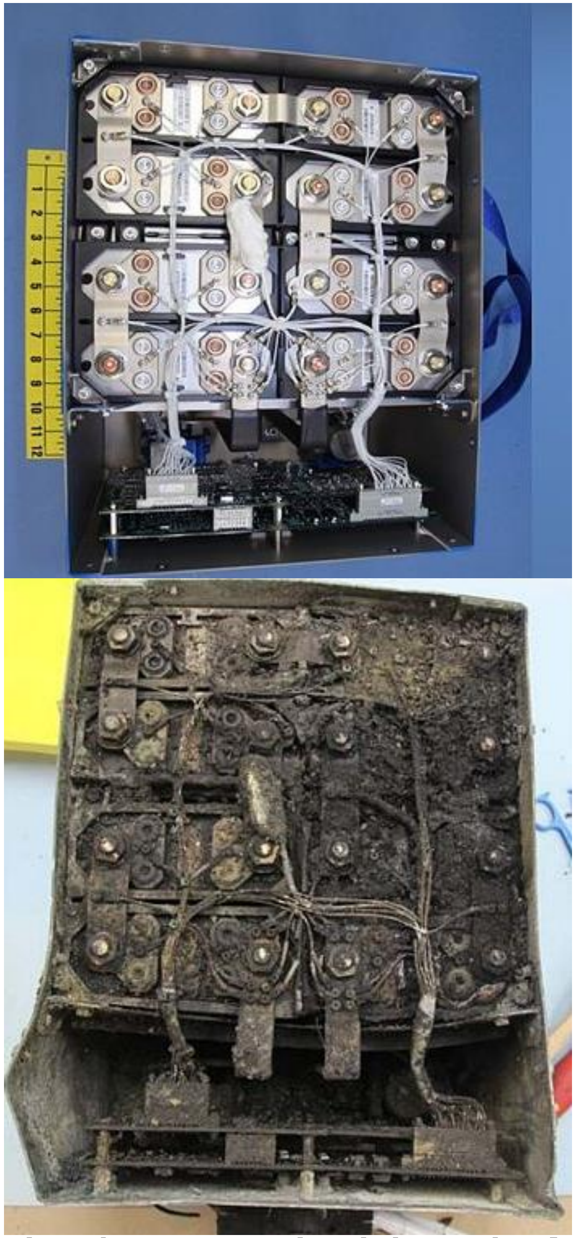
[Bicheno-Brown, 2012]

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
  - 2.6×10^4 flight hours [NTSB 2013]



[http://upload.wikimedia.org/wikipedia/commons/9/95/Boeing_Dreamliner_battery_original_and_damaged.jpg]

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?