SafetyInEngineering

Complex failure modes in complex systems, a case study:

Qantas A330 flight 72, Singapore-Perth, 7th October 2008

Jim Thomson, www.safetyinengineering.com

March 2015

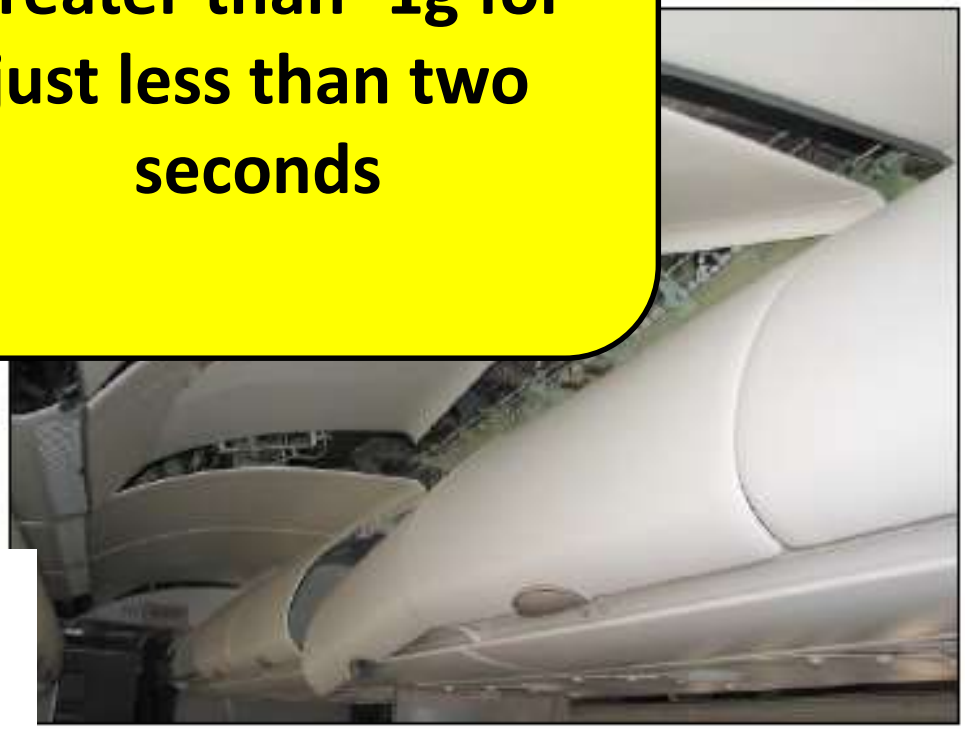
"Complex systems almost always fail in complex ways."
Columbia Accident Investigation Board Report, August 2003

QANTAS A330 ‘upset’, 7 October 2008

Figure 48: Example of damage to the fittings above passenger
section)

Greater than -1g for just less than two seconds

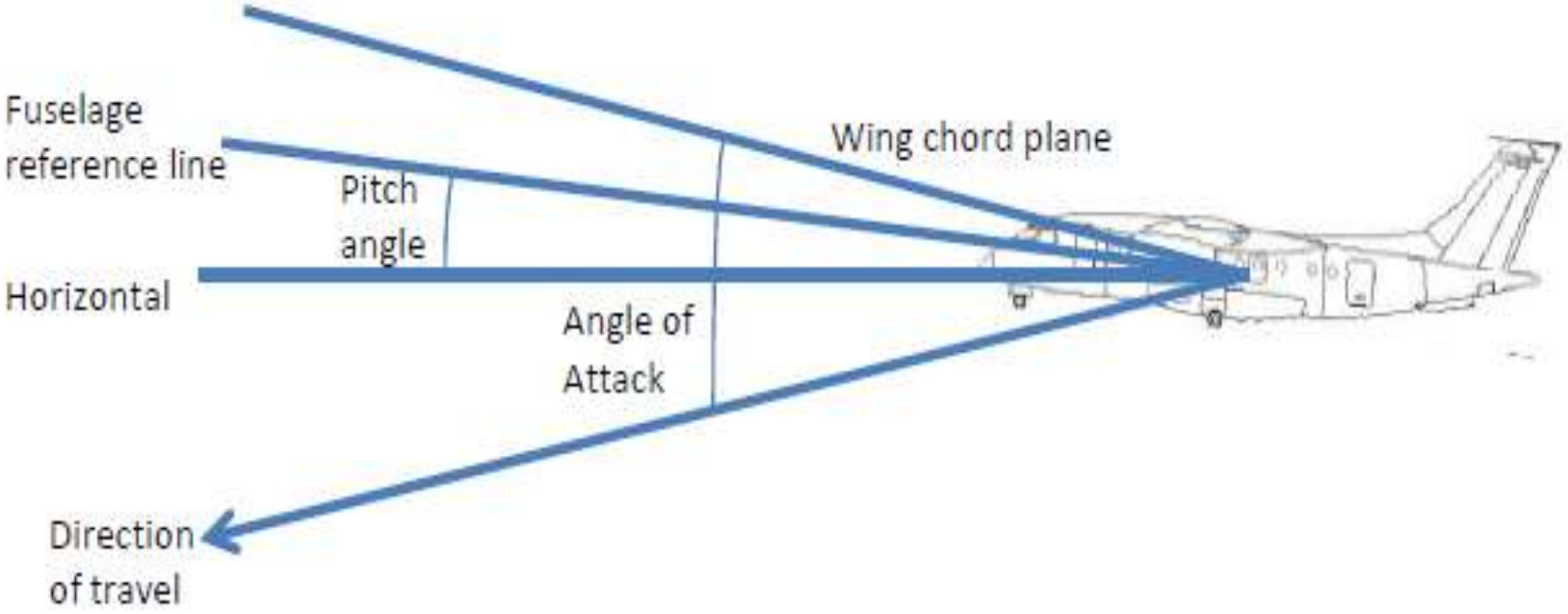
the aisle (rear section)



Injuries	Crew	Passengers	Total
Fatal	-	-	-
Serious	1	11	12
Minor	8	99	107
None / unknown	3	193	196
Total	12	303	315

See ATSB animation at
https://www.youtube.com/watch?v=3dpG7_2izXs

Angle of Attack (AOA) vs Pitch Angle



The pilot cannot readily sense the Angle of Attack – he relies on instruments.

ADIRUs: “ring-laser gyroscopes”

- Modern Inertial Reference Units use *ring laser gyroscopes* to provide raw data.
- A ring laser gyroscope consists of a ring laser having two counter-propagating modes over the same path in order to detect rotation (Sagnac effect).

Air Data Inertial Reference Units (ADIRUs)

Figure 7: ADIRU 1 (ADIRU 4167) from QPA

Northrop Grumman LTN-101 Flagship ADIRU

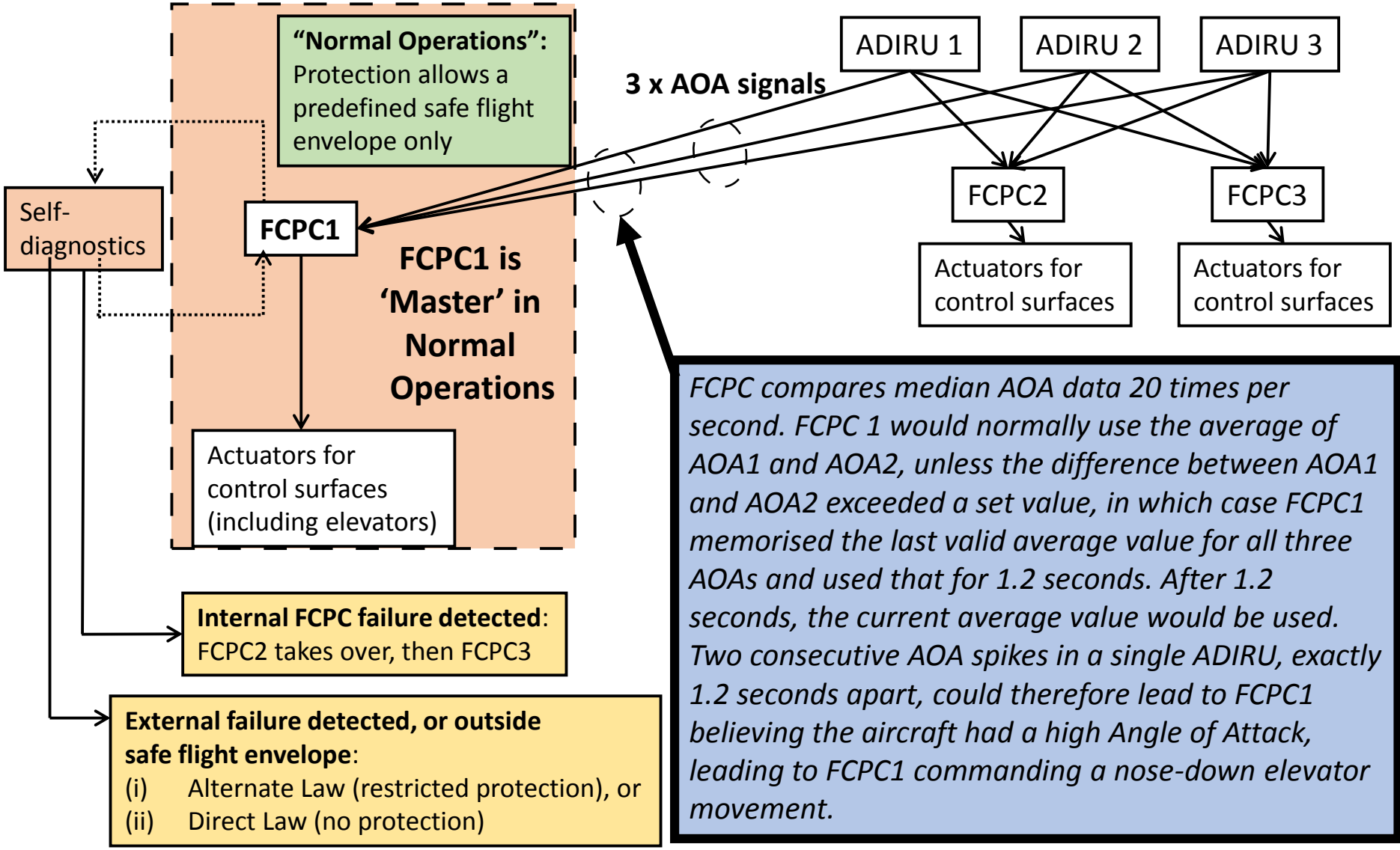
Angle Of Attack is a critical safety parameter for the EFCS, and the Flight Control Primary Computers use three independent AOA signals to check their consistency, signals AOA1, AOA2 and AOA3.

The AOA signals are created by Air Data Inertial Reference Units (ADIRUs), which use ring-laser gyroscopes, Pitot tube sensors, air temperature, and GPS data.

The AOA value is then fed into the flight control system and used, in particular, to drive signals to the elevators in the tailplane which control aircraft pitch.

Claimed MTBF 16000 hours. Weight 12.6 kg.

ADIRUs are "smart sensors" in nuclear terminology.



Acronyms:
AOA = Angle of Attack
ADIRU = Air Data Inertial Reference Unit
FCPC = Flight Control Primary Computer

Key factors from the in-flight upset of Qantas Airbus 330-303, 7th October 2008

(adapted from Australian Transport Safety Bureau report AO-2008-70)

Aircraft was in level cruise at 37000 feet

1240:26 ADIRU 1 started providing multiple intermittent spike signals. Crew received numerous warning messages (mostly spurious).

1242:27 Aircraft suddenly pitched nose down, max 8.4 degrees. The command lasted <2 seconds. At least 110 passengers and 9 crew injured, 12 seriously. A second less severe pitch down occurred at 1245:08.

"The data-spike failure mode……..involved intermittent spikes on air data parameters being sent to other systems as valid data without a relevant fault message being displayed to the crew."

"There was a limitation in the algorithm used by the A330/A340 FCPCs for processing AOA data. This limitation meant that, in a very specific situation, multiple AOA spikes from only one of the three ADIRUs could result in a nose-down elevator command. (Significant safety issue)"

"The FCPC algorithm was very effective but it could not correctly manage a scenario where there were multiple spikes in either AOA1 or AOA2 that were 1.2 seconds apart…….it is very unlikely that (this) FCPC design limitation could have been associated with a more adverse outcome……The occurrence fitted the classification of a 'hazardous' effect rather than a 'catastrophic' effect……only known case of the design limitation affecting an aircraft's flight-path in over 28 million flight hours……limitation was within the acceptable probability range……."

Key factors from the in-flight upset of Qantas Airbus 330-303, 7th October 2008

(adapted from Australian Transport Safety Bureau report AO-2008-70)

"……the development of the A330/A340 flight control system during 1991 and 1992 had many elements to minimise the risk of design error……None of these activities identified the design limitation in the FCPC's AOA algorithm……**Overall, the design verification and validation processes used by the aircraft manufacturer did not fully consider the potential effects of frequent spikes in data from the ADIRU."**

"….. the LTN-101 ADIRU's central processor unit (CPU) module combined the data value from one parameter with the label for another parameter. The failure mode was **probably initiated by a single, rare type of internal or external trigger event** combined with a marginal susceptibility to that type of event within a hardware component." **There were two other known occurrences of the ADIRU data-spike failure mode, on 12th Sept 2006 and 27th Dec 2008.**

On 15th January 2009 the EASA issued Emergency Airworthiness Directive 2009-0012-E to address the Northrop-Grumman ADIRU problem.

Mayday declared, flight diverted and landed successfully at 1332.

The Rare Event Fallacy, as demonstrated by Robin Williams

(*from 'The World According to Garp', 1982*)

Key points

Findings:

- A single failure in one ADIRU led to an accident in a redundant system.
- The ADIRU fault may have been caused by a single event upset due to cosmic rays.
- Airbus software was improperly specified for dealing with the ADIRU fault.

Key conclusion:

- Tricky FMEAs for complex systems using COTS smart sensors.

Other issues of note:

- Flimsy retrospective PRA justification?
- Regulatory xenophobia?