System Safety

Dr Steve Burrow

Why Aerospace System Safety?

- Aircraft are complex machines and the consequences of failure are severe.
- Safety is the number 1 concern of passengers.
- There is a legal requirement for aircraft to be designed to operate within certain safety parameters.
- Assessment of aircraft system safety is also enshrined within legally defined process.
- Poor safety impacts profitability at all levels of the aircraft industry.

What is Safety?

- OED: ‘Being safe; freedom from danger’
- DoD MIL-STD-882D: ‘Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment’
- SAE ARP 5744: ‘The state in which risk is lower than the boundary risk. The boundary risk is the upper limit of acceptable risk’
- Regulation through;
  - CAA SRG, Civil Aviation Authority Safety Regulation Group (UK)
  - EASA, European Aerospace Safety Agency (Europe)

Definitions

- Hazard
  - A ***hazard*** is any situation or condition resulting from failures, malfunctions, external events or errors, that has the potential to cause adverse consequences.
  - A ***hazard identification process*** is the formal means of collecting, recording, analysing, acting on and generating feedback about hazards that affect the safety of the operational activities of the organisation.
- Risk
  - ***Risk*** is the assessed potential in terms of severity and likelihood of the consequences of a ***hazard*** considering the worst case scenario.
  - A ***hazard*** has the potential to cause harm while ***risk*** is the likelihood of that harm being realised within a specific time-scale.

Definitions

- Failure
  - The inability of an item to perform its intended function
- Integrity
  - The attribute of a system or an item indicating that it can be relied upon to work correctly on demand
- Availability
  - The probability that a system or an item is in a functioning state at a given point in time

Definitions

- System safety
  - The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

- System safety engineering
  - An engineering discipline that employs specialised professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

Hazard and Risk Assessment process

Hazard identification

↓

Risk Assessment 1: severity of occurrence

↓

Risk Assessment 2: likelihood of occurrence

↓

Acceptability of Risk

Accept risk or Take action to reduce risk

Severity (CAA)

Negligible
Little consequence to the operation of the aircraft

Minor effect
Slight increase in crew workload. Slight reduction in safety margins.
Physical effects, but no injury to occupants. A reportable occurrence only.

Major effect
Significant reduction in safety margins or functional capabilities.
Significant increase in crew workload or in conditions impairing crew efficiency.
Some injury to occupants.

Hazardous effect
Large reduction in safety margins or functional capabilities.
Higher workload or physical distress.
Serious injury to, or death of, a relatively small proportion of the occupants.

Catastrophic effect
All failure conditions which would prevent continued flight and landing.
Consequence is a multi-fatal accident and/or loss of the aircraft.

Likelihood (CAA)

'Frequent'
Likely to occur many times, 1 - $1x10^{-3}$ per hour

'Occasional'
Likely to occur sometimes, $1x10^{-3}$ - $1x10^{-5}$ per hour

'Remote'
Unlikely, but may possibly occur, $1x10^{-5}$ - $1x10^{-7}$ per hour

'Improbable'
Very unlikely to occur, $1x10^{-7}$ - $1x10^{-9}$ per hour

'Extremely improbable'
Almost inconceivable that the event will occur, $>1x10^{-9}$ per hour

Severity and likelihood

- JAR* aerospace definitions of acceptable likelihoods for failures of various severity;

Severity	*Probability*	*Analysis*
Minor	Reasonably probable	1 $\times 10^{-3}$ per flight hour
Major	Remote	1 $\times 10^{-5}$ per flight hour
Hazardous	Extremely remote	1 $\times 10^{-7}$ per flight hour
Catastrophic	Extremely improbable	1 $\times 10^{-9}$ per flight hour

** JAR (Joint Aviation Requirements) - standards defined across several European aviation authorities*

What do these figures mean?

Minor *= $1x10^{-3}$ per hour = Once in 1000 hours.*
Physical effects, but no injury to occupants. A reportable occurrence only.
~ Once in a lifetime for regular passenger.

Major *= $1x10^{-5}$ per hour = Once 100,000 hours*

Significant increase in crew workload or in conditions impairing crew efficiency. Some injury to occupants.
~ Once in career of 3 pilots or life of an individual aircraft.

Catastrophic *= $1x10^{-9}$ per hour = Once in a thousand million hours*
Consequence is a multi-fatal accident and/or loss of the aircraft.

~ Once in lifetime of the entire fleet of 737 (most numerous civil aircraft - ~7000 built, over 1000 flying at any moment).

Types of Failure

- Systematic Failure
  - These failures will always occur for a given set of conditions. Repeatable and *potentially* predictable.
  - Software ‘bugs’ are a good example: once the ‘buggy code’ is written the potential for the failure is intrinsic to the system and occurrence depends only on the conditions.
  - These are hard to mitigate for and difficult to analyse with rigor.
    - In very many cases accidents happen because of events or behaviour that were not foreseen
  - The primary approach is to try and ‘design out’ this type of fault.

Types of Failure

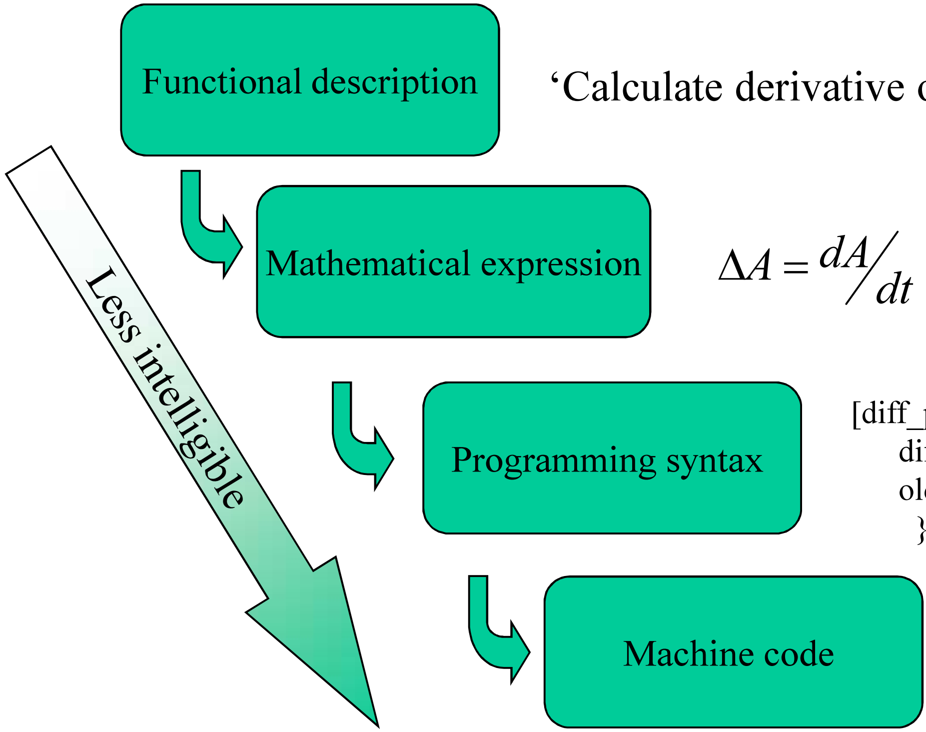
- Random Failures
  - These failures occur during normal operation and are not repeatable or predictable, but can be dealt analytically using probability.
  - Blowing of bulbs is an example, or failure from fatigue within design limits.
  - Once extensive testing has determined the probability of failure then ‘reliability analysis’ can be used to ensure the probability of failure is within acceptable bounds.

Types of failure and severity…

- *A pixel fails on the navigation display after two years of aircraft service*?
- An aircraft skids off the runway due to ice on the tarmac?
- An aircraft skids off the runway because a tire bursts on landing?
- *A computer driving the attitude indicator produces a blank screen if an input data value is greater than expected?*
- *A computer driving the attitude indicator produces a zero-valued output because a capacitor in the electronics failed?*

Design Safety features: process assurance

- Involves rigorous checking and a development process designed to minimise the potential for systematic failures. Software example;



'Calculate derivative of air pressure'

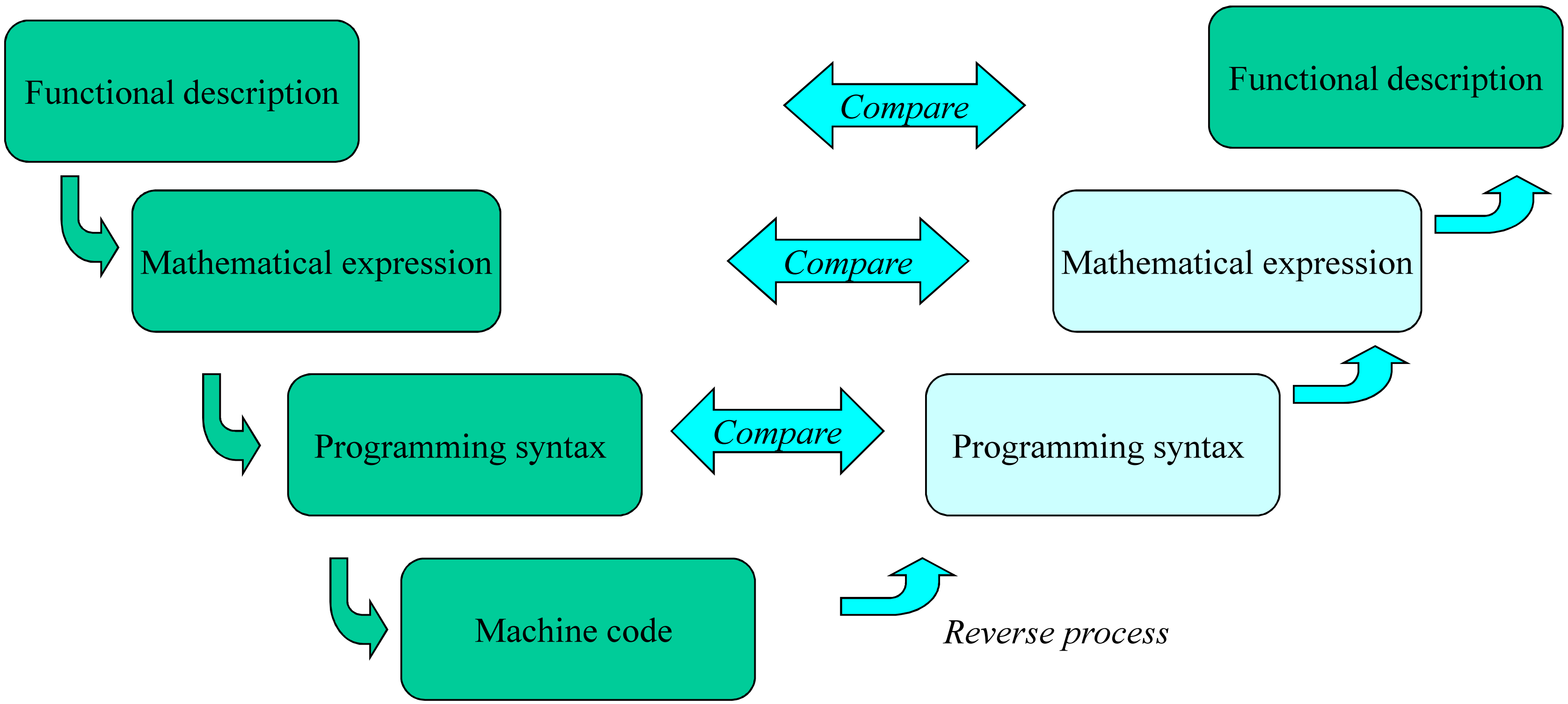
$$\Delta A = {dA}/{dt}$$

```
[diff_press] =  diff(air_press, t_step) {
     diff_press = (air_press – old_press) ./t_step
     old_press = diff_press
      }
```

```
0011 1110
1001 0001
0101 0101
0000 1001
```

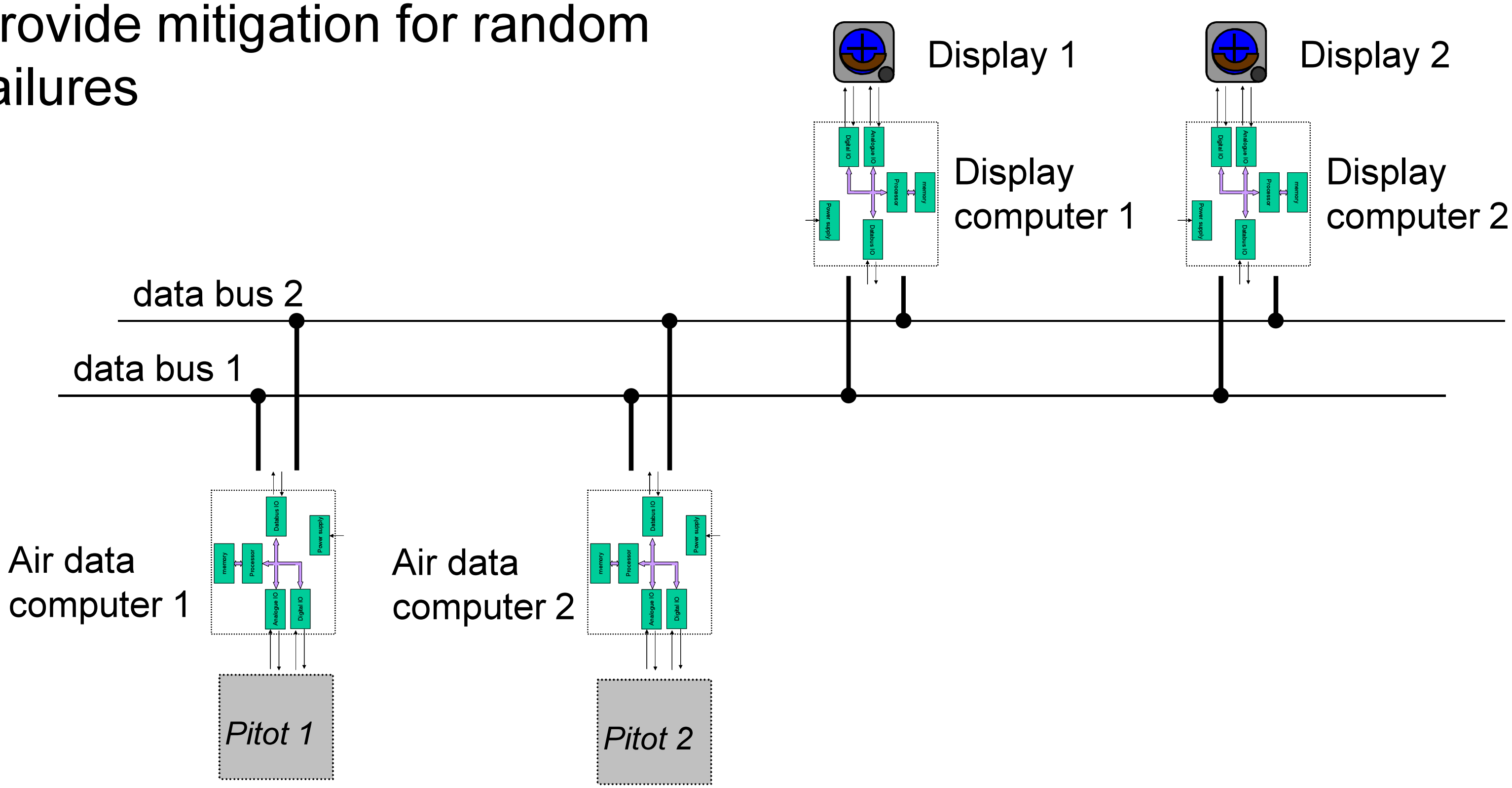
Design Safety features: process assurance

- By providing cross checking in the development process, systematic errors can be uncovered.

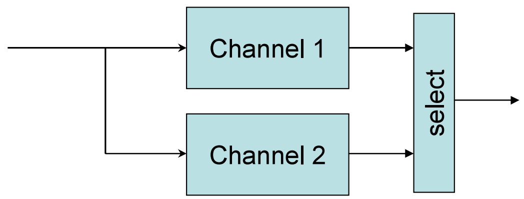


Architectural safety features: Redundancy

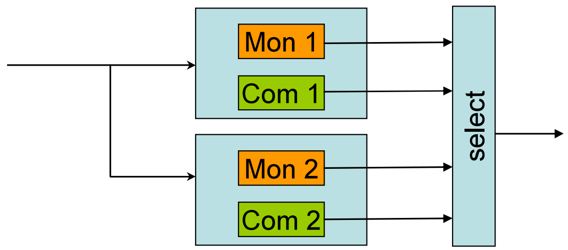
- Redundant architectures provide mitigation for random failures



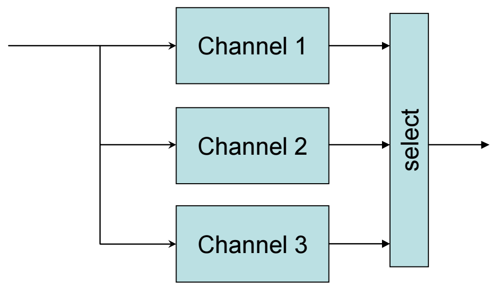
Redundancy



Duplex *- systems have two lanes. A duplex system can detect faults by cross-comparison between lanes. System operation can only continue after a single fault by pilot selection of the "good" remaining lane, assuming that this can be identified. This may be done by the pilot.*



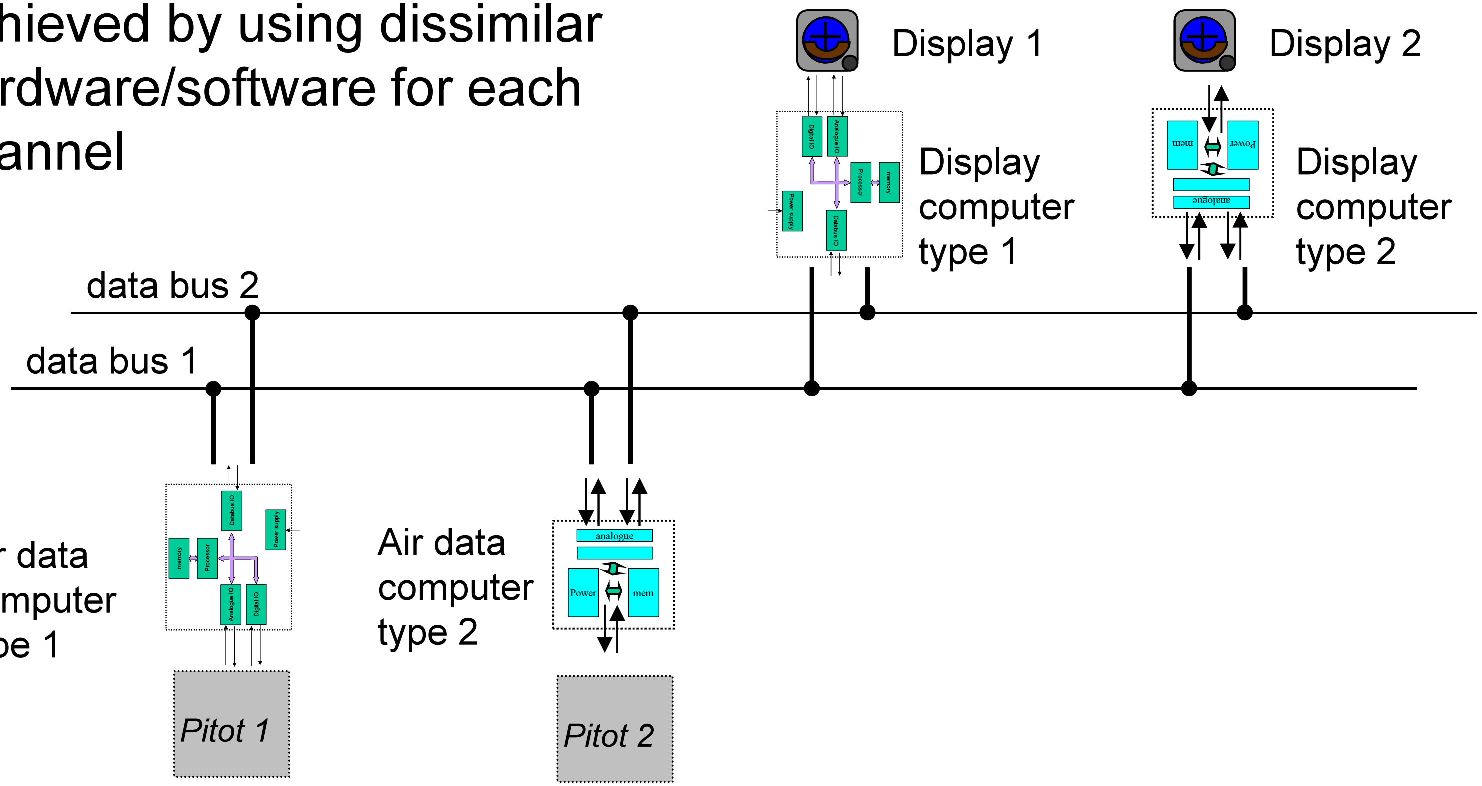
Dual-duplex *- systems have two operating lanes, with two more lanes independently monitoring them. System operation can continue after a single fault, which can be detected and isolated by the monitoring lane. The system can do this automatically*



Triplex systems *- have three operating lanes. System operation can continue after a single fault by cross-comparison between all three lanes, and voting out a failed lane. Again this can be automatic*

Dissimilar redundancy

- Mitigation for ‘common mode’ systematic failures can be achieved by using dissimilar hardware/software for each channel



Example dissimilar systems

- Wheel brakes and thrust reversers……..

- Flight control surfaces………

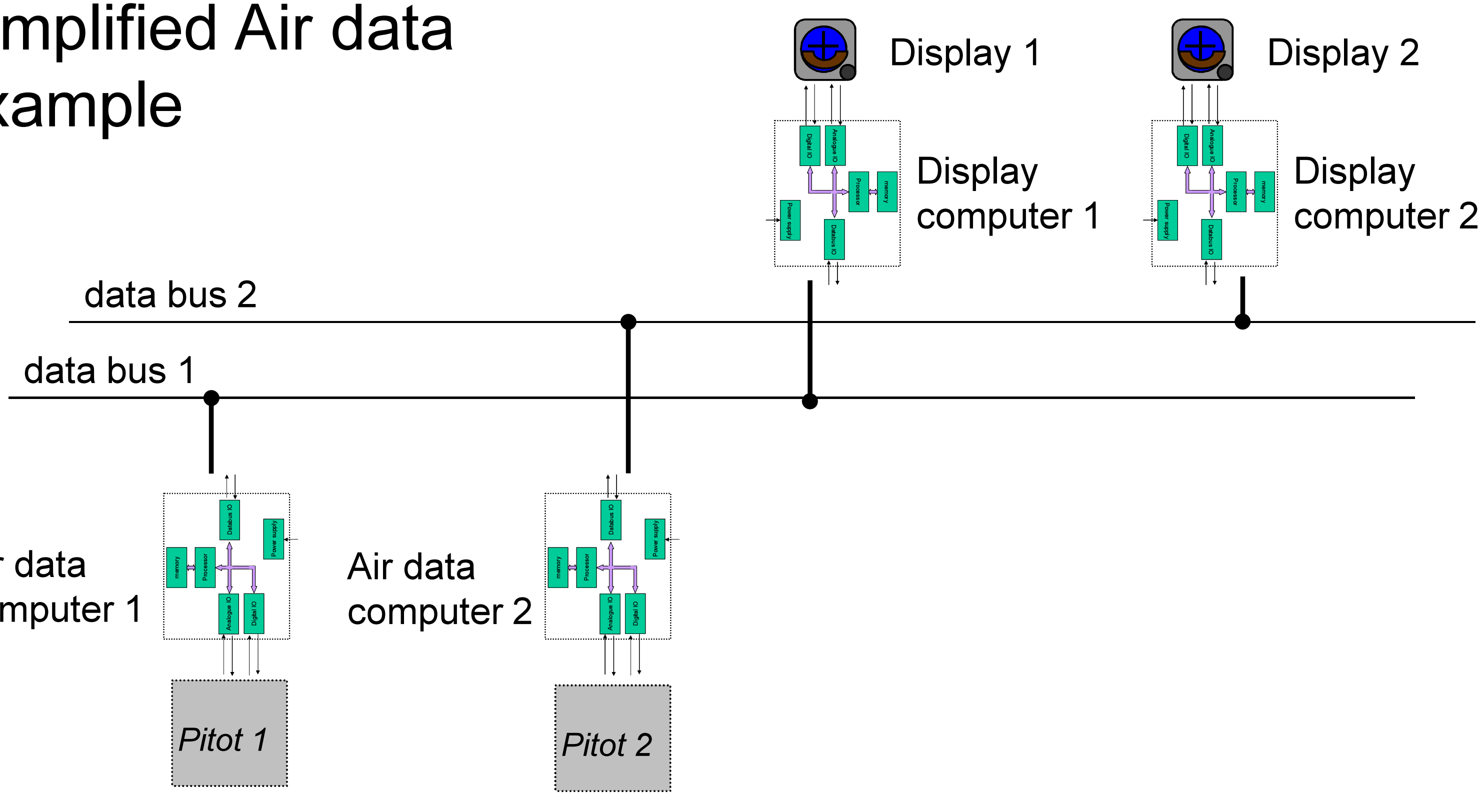
- Engine driven generators, auxiliary power unit, and batteries…..

Analysis

- Where failure rates can be determined for a component, probability theory can be used to quantitatively assess system safety and demonstrate system compliance with regulations.
- These techniques are applicable to random failures only, and where accurate data to quantify the availability of the system exists.
- This data might come from extensive testing or from flight experience.

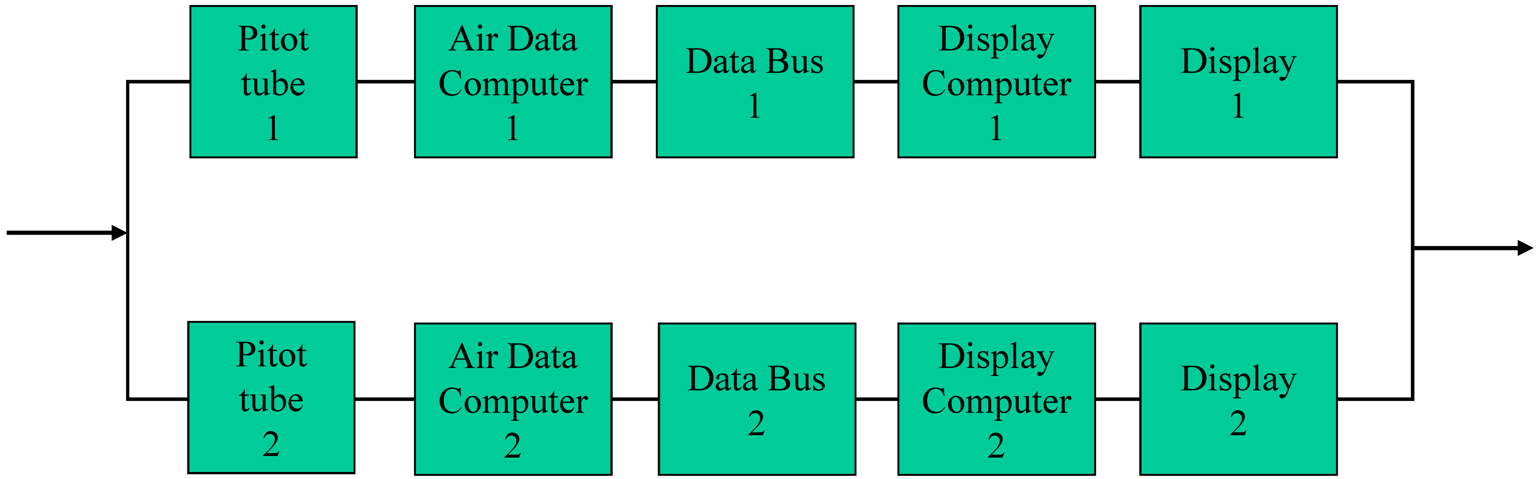
Analysis

Simplified Air data example



Analysis

- From Air data example, a 'redundancy diagram' will look like;

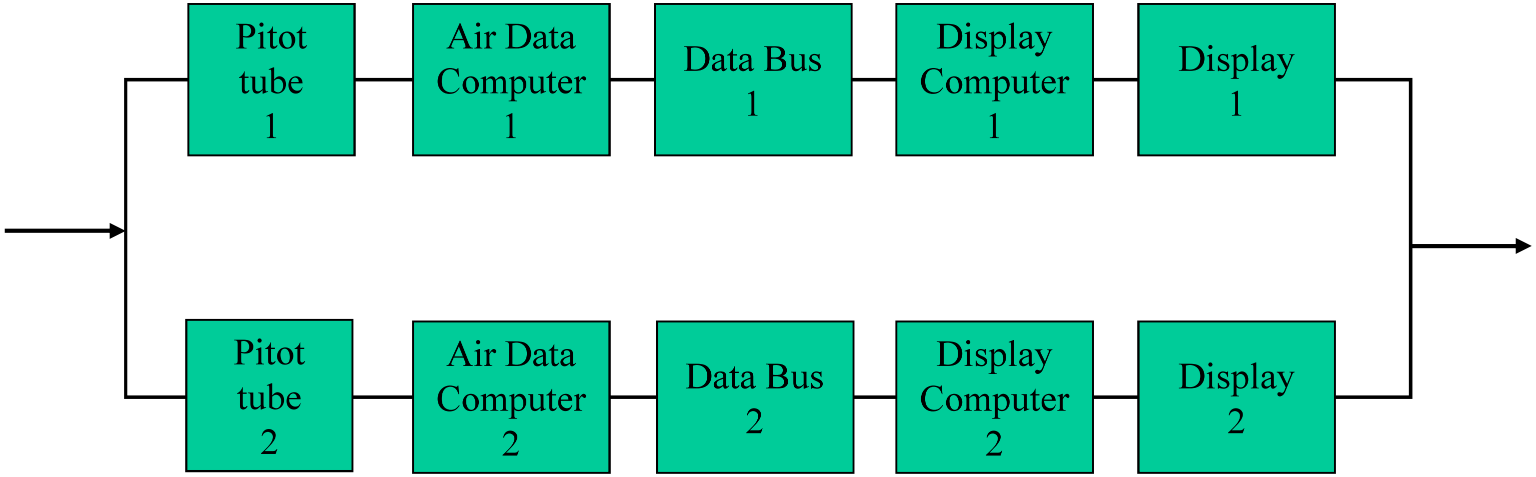


System fails if channel 1 fails **and** channel 2 fails

Channel 1 fails if pitot 1 ***or*** air data 1 ***or*** data bus 1 ***or*** display computer 1 ***or*** display 1 fails

Analysis

- From Air data example, a ‘redundancy diagram’ will look like;



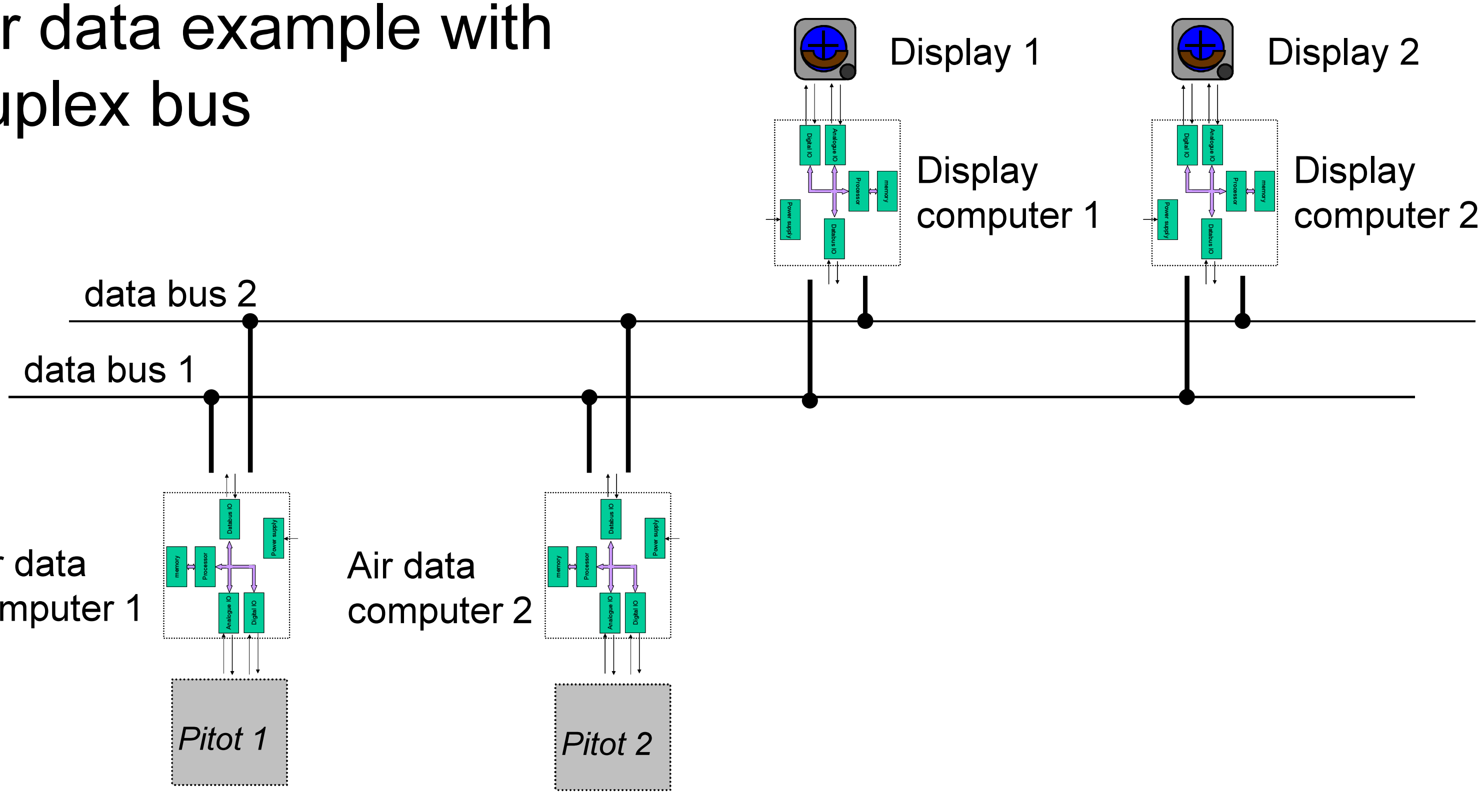
System failure probability = P(channel 1) * P(channel 2)

$$P(\text{channel 1}) = P(\text{channel 2}) = P_p + P_{adc} + P_{db} + P_{dc} + P_d$$

$$\text{System failure probability} = (P_p + P_{adc} + P_{db} + P_{dc} + P_d)^2$$

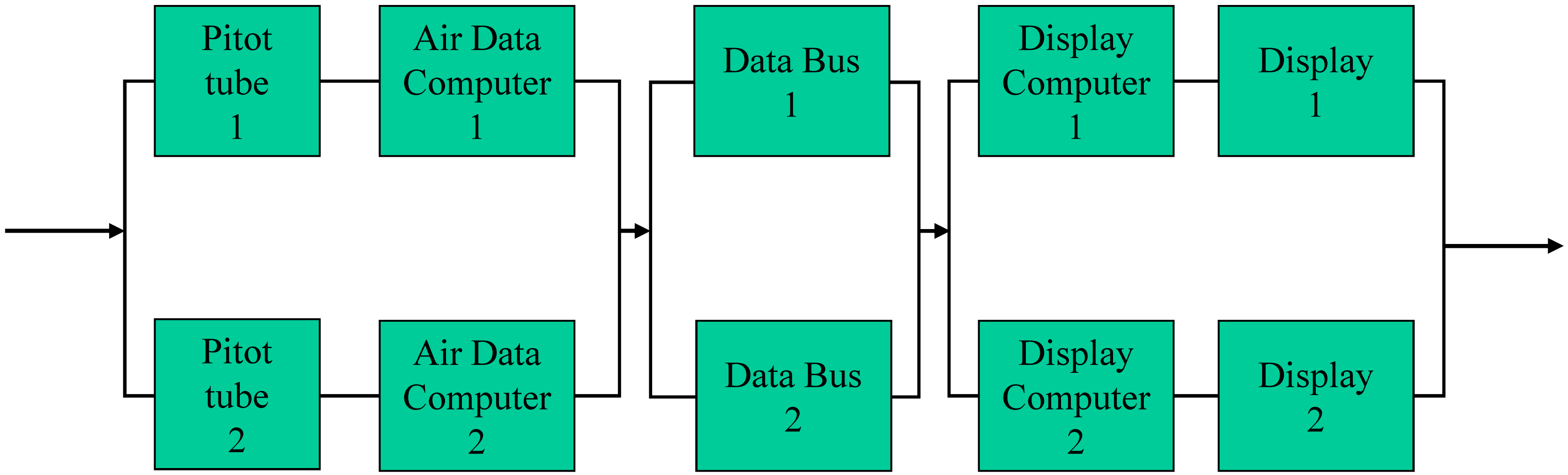
Analysis

Air data example with duplex bus



Analysis

- The new redundancy diagram will look like;



System fails if ?

Analysis

- For random failure, failure rate per hour is normally assumed constant and denoted by λ

- A component may be quoted as having a failure rate per hour (λ) or a Mean Time Between Failure (MTBF), $1/\lambda$

- The probability of a failure is an exponential and given by;

$$p = 1 - e^{-\lambda t}$$

Where t is exposure time

- Exposure time (~hours) is generally much smaller than MTBF (~10000's hours) so we can approximate $p = \lambda t$

Analysis

- For the air data system assume;

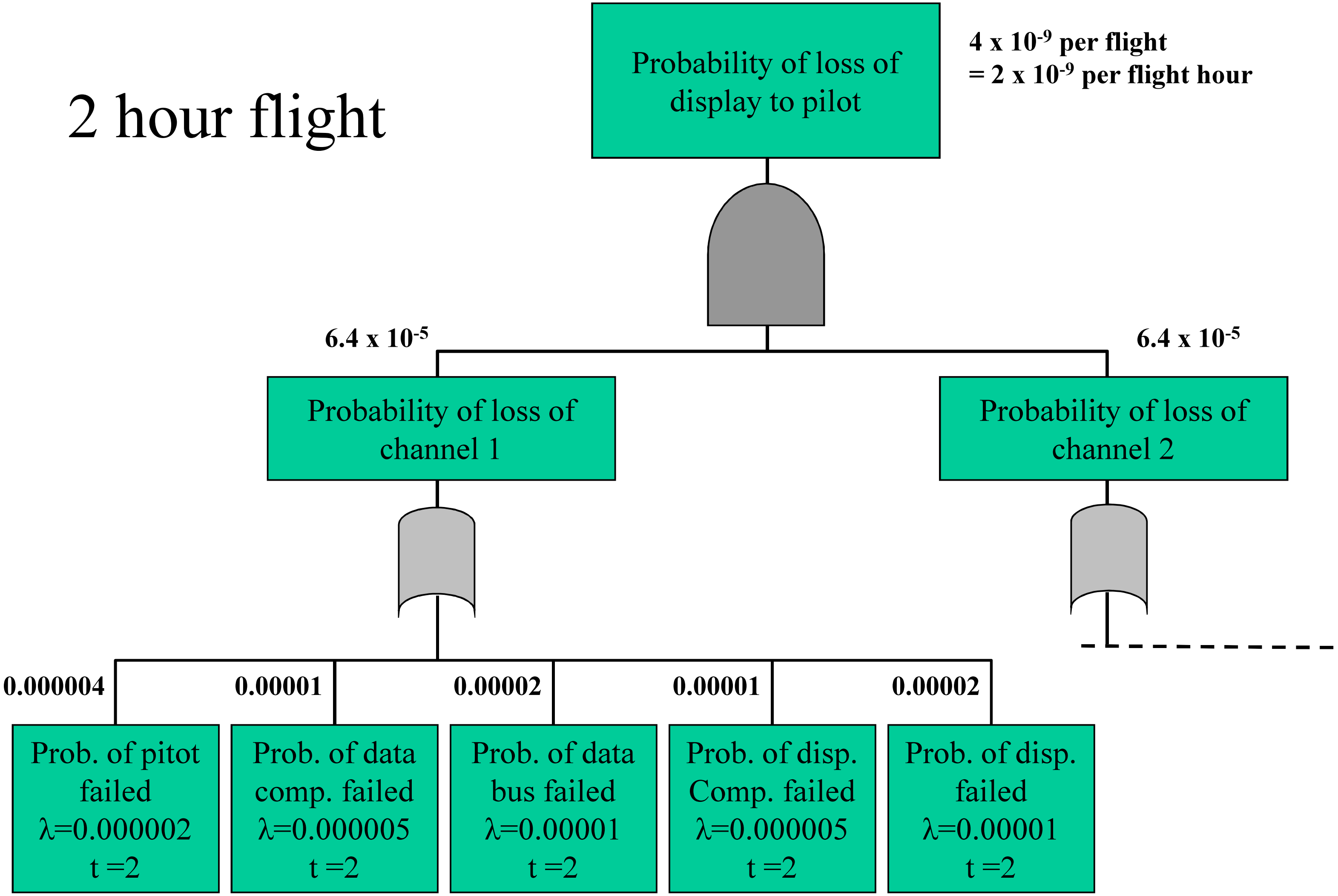
- MTBF pitot = 500,000 hours
- MTBF air data computer = 200,000 hours
- MTBF data bus = 100,000 hours
- MTBF display computer = 200,000 hours
- MTBF display = 100,000 hours

(note these are not necessarily representative of a real components)

- First consider a short flight of 2 hours, then the same system on a 13 hour long haul flight.

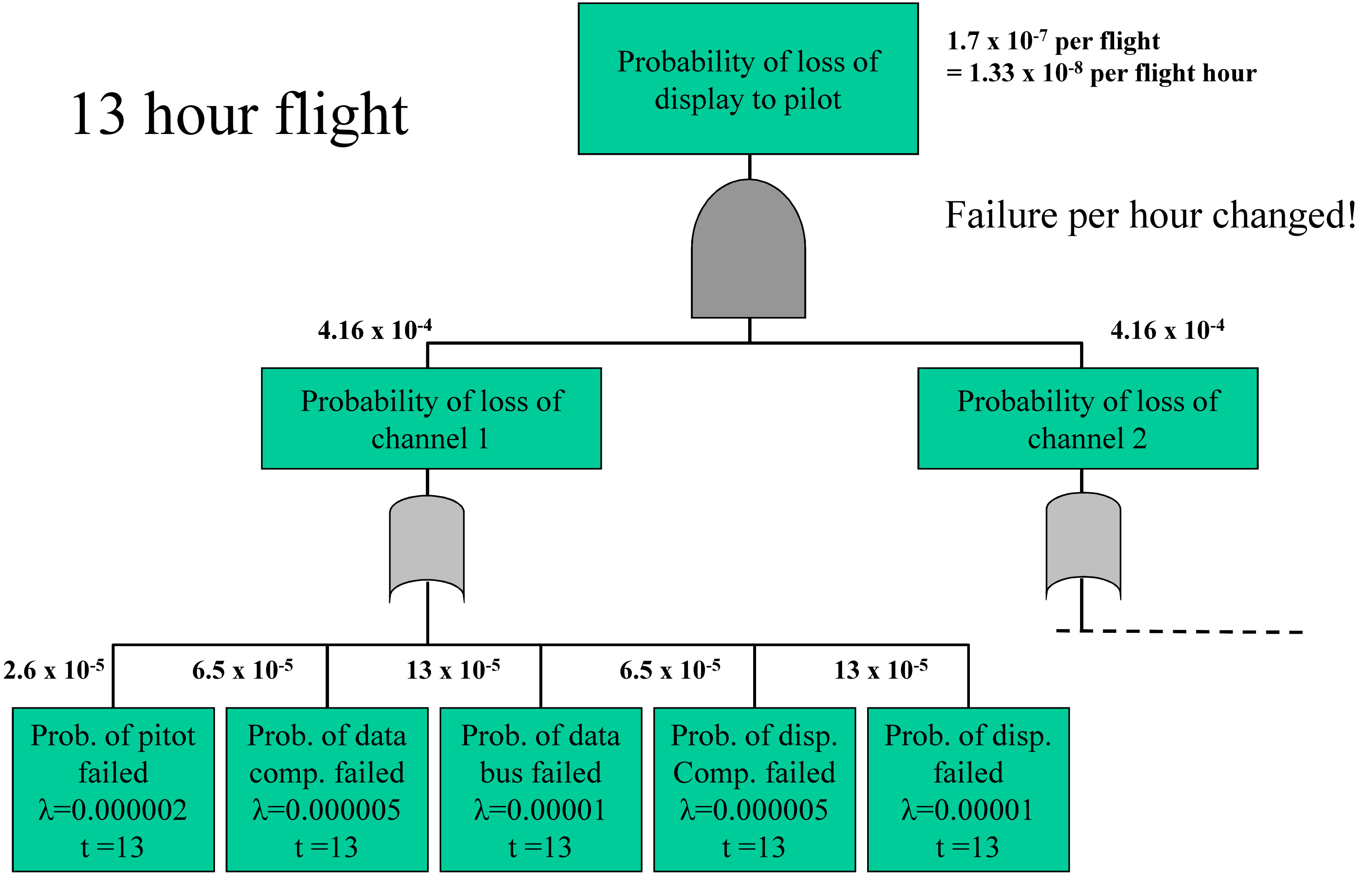
Analysis – fault tree

2 hour flight



Analysis – fault tree

13 hour flight



Summary

- System Safety Assessment is a well developed and defined discipline.
- It is heavily regulated by various national and international organisations.
- Both the system itself and the process used to assess safety need to comply with regulation.

Summary

- Failures can be random or systematic
- Process assurance is the main tool to mitigate for systematic failures.
- Probability is used to assess random failures.
- Redundant architectures are used to mitigate for random failures and make systems meet typical safety requirements
- Dissimilar components in a redundant architecture can mitigate for some systematic failures

Further reading

- Look at ‘SPARK’ programming language - (suggest Wikipedia)
- Read CAA document ‘Safety management systems – guidance to organisations’ (available through blackboard)