Avionics and Airborne Computers: What Could Possibly Go Wrong?

Dr Stephen Wright

University of the West of England
steve.wright@uwe.ac.uk
Birmingham University 1986-89
Steve Wright

- Rolls-Royce 1989-97
- STMicroelectronics 1997-2000
- Airbus 2001-14
- University of Bristol 2006-2009
Avionics I have known

- Rolls Royce Trent 700
- Airbus A400M
- Boeing 767
- Airbus A330
- BMW/Rolls Royce BR710
- Airbus A380
- Airbus A380
Programme

- How is avionics special?
- How does avionics fail?
- How does avionics *defend* against failure?
Avionics = Computer + Other

• Avionics not just a computer – hybrid with other electrical/electronics
  • Hard to differentiate avionics from aircraft system
In Position
In Action
How are Avionics Special?

- Operate in *hostile* environments
- Long *lifetimes*
- High cost of *failure*
- High *reliability*
Hostile Environments

- Vibration
- Low Temperature
- High Temperature
- Radiation
- Moisture
- Battle damage
- Engine burst
Long lifetimes

• Expected: 25 years
• B-52: 90 years?
• **Obsolescence** is a major issue
• How to test for wear-out?

Rolls-Royce RB211-535

Boeing B-52H
High Cost of Failure

• Catastrophic is obvious

• Financial – aircraft cannot dispatch
Types of Failure

- Design failure
- Runtime failure
- User failure
- Maintenance failure
High Reliability

- **Availability** (does what we want)
- **Integrity** (doesn’t do what we don’t want)
High Reliability

• Not perfect
• Design to a failure probability
• Particular probability decided by severity of outcome
Failures contained as well as prevented

• Avionics are reliable *not* because things never go wrong

• Reliable because failures reduced to acceptable level, then contained
Graceful degradation

- Reversionary modes
- Redundant units
- Load shedding
- Alternative methods for achieving functionality
Software

```html
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <p>Ok. Let's print some time-based greetings.</p>
    <button onclick="myFunction()">Try it!</button>
    <p id="demo"></p>
    <script>
      function myFunction()
      {
        var time = "";
        var hours = new Date().getHours();
        if (hours<12) {
          time = "Good morning";
        }
        else if (hours==12) {
          time = "Good day";
        }
        else {
          time = "Good evening";
        }
        document.getElementById("demo").innerHTML=time;
      }
    </script>
  </body>
</html>
```
Avionics Software Growth

- F-4A (1958) - 1000 lines-of-code
- F/A-18 (1978) – 1 million lines-of-code
- F-22 (1997) - 1.7 million lines-of-code
- F-35 (2006) - 8 million lines-of-code
Avionics Software Languages

- Multiple input formats
- Allows software development by non-programmers
- Integrated verification methods
Software dissimilarity

- Top-level design
- Coding
- Verification
- Compiler
- etc.
Reliable Software Development

DO178C = guidance to determine if software will perform reliably in an airborne environment (2012)

• Recommends some methods (e.g. Model-Based, Formal Methods)
Software Costs

• Software production:
  ~10 loc/day @
  ~$100/hour = $800M

• Full Authority Digital Engine Controller -
  $100,000 - $200,000
Hardware
Failures - Wiring

- Impact
- Corrosion
- Chafing
- Bad Maintenance

Qantas Flight 32
4 November 2010
Uncontained engine failure
Failures - Connectors

• Bad Maintenance
• Impact
• Corrosion
Failures – Inside the box

- Packaging failures
- Contact failures
- Printed circuit board failures
- Relay failures
- Semiconductor failures
- Manufacturing failures
Electromagnetic Sources

- Galactic
- Solar
- Lightening
- Other systems
- Components of same system
- Nuclear weapons
- Electronic Countermeasures
Radiation v Altitude

- Bad at 60,000 feet
- Much worse in Low Earth Orbit
- Much, much worse outside Earth’s magnetic field
Single Event Failures

- Transient “glitches”
- Caused by neutrons, protons, alpha particles, high energy gamma rays (ionising particles)
- Can indirectly lead to permanent damage by switching a gate into latched state
Component Failure Reduction

- Large “geometries”
- Consumer electronics use feature sizes of ~14 nanometre width
- Avionics electronics use feature sizes of ~65 nanometre width
- Space electronics use feature sizes of ~250 nanometre width

- Expensive and slow
Component Failure Reduction

- Silicon on Insulator (SOI)
- Insulating substrates instead of the usual semiconductor wafers
- Silicon on Sapphire (SOS) are commonly used
- Very expensive
Component Failure Reduction

• Protective packaging, doped with radiation-absorbing elements

• e.g. Boron-10 captures neutrons and breaks down to lighter elements
Box Failure Reduction

• Protective signal conditioning
• High specification connectors
• Unit location: avionics-bay pressure-vessel burst-zones
Failure Detection

- Write/read-back
- Parity Checks
- Watchdog timers
- etc.
Failure Recovery

• Channel reset
• Hand-over to other channel
• System shutdown

i.e. recover at architecture level
Architectures

- Simplex
- Duplex
- Dual COM/MON
- Triplex

Choice driven by reliability need
Simplex

- Low Availability
- Low Integrity
• Improved Availability
Channel Select

“Quis custodiet ipsos custodes?”

= "Who will guard the guards themselves?"

Juvenal, 2nd Century AD
Duplex COM/MON

- High Availability
- High Integrity
Triplex

- High Availability
- High Integrity
Architecture Dissimilarity (Flight Controls)

Boeing 777

Airbus A330/340
Failure... and success

• Air Transat A330 Flight 236

• Toronto-Lisbon, August 2001
Air Transat Flight 236 – System Failure

• Updated engine delivered
• Installation bodged with old version part
• Fitter questioned action but overruled by supervisor
• Fuel pipe rubbed against other pipe
Air Transat Flight 236 – More System Failure

- Fuel pipe ruptured over Atlantic
- Crew confused by oil temperature warning
- Crew disbelieved gauging
- Crew retreated to following procedure
Trans Air A330 Flight 236 – More System Failure

• Crew pumped fuel from good engine
• All fuel lost overboard 135 miles from land
• All-engine flameout
Trans Air A330 Flight 236 – System Failure Cascade

- All electrical power generation lost
- All hydraulics power lost
Air Transat Flight 236 – Avionics Success

- Ram Air Turbine deployed
- Backup battery (& hydraulics) power used
- Ordered shutdown of non-essential systems
- Reversionary avionics units used
Air Transat Flight 236 – Success

- 135 mile glide to Azores
- Heavy landing
- Zero deaths
Finally

• Avionics are very **reliable** – but not in the way people expect

• Failure is **reduced** then **contained**
Finally

It **works** – air transport is getting **much safer**
Finally

It works – air transport is getting much safer
Questions?

I make mistakes, I'm out of control, and at times hard to handle

Marilyn Monroe
Future Avionics

- General purpose processors in common computing resource
IMA Architecture

- Multiple avionics applications hosted on a common computing resource
Germanwings
Accident Causes

Root causes of plane accidents

- Flight crew: 56%
- Aircraft: 17%
- Weather: 13%
- Miscellaneous: 4%
- Maintenance: 4%
- Airport/Air traffic control: 6%
Getting Safer

- Deaths falling
- Crashes falling
- Flights rising
- Flight-hours rising
- Deaths/flight falling
- Crashes/flight falling