Uncommanded Engine Shutdown
19 kilometres North of Melbourne
B717-200 VH-AFR
3 February 2001

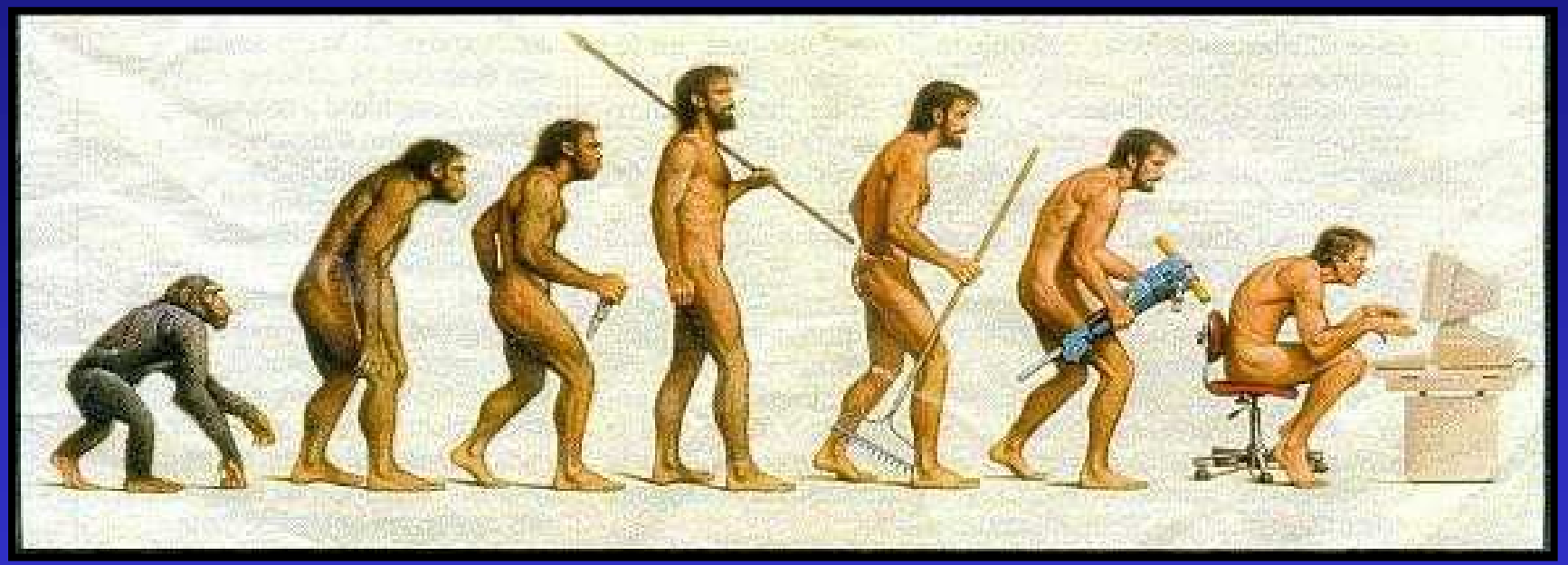
by L.S. (Sam) Webb
Senior Air Safety Investigator
Australian Transport Safety Bureau

Australian Transport Safety Bureau

To maintain and improve transport safety through excellence in:
- ‘no blame’ independent transport accident, incident and safety deficiency investigation,
- safety data, research, pro-active systemic analysis, communication and education, and
- leading development of national and international safety strategies.

Auckland ANZSASI 2002

Automation/Software Evolution in Aircraft Systems



Automation- allocation of functions to machines normally allocated to humans

Flight deck automation- machines on the flight deck which perform functions normally performed by pilots.

Examples- autopilots, flight management systems, electronic flight instrument systems, EECs, and warning and alerting systems.

Accident involving B757 N651AA near Cali on 20 December 1995

Contributing to the cause of the accident were:

1. Flight crew's efforts to expedite approach and landing to avoid potential delays.
2. Flight crew's execution of the GPWS escape manoeuvre with speed brakes deployed.

Accident involving B757 N651AA near Cali on 20 December 1995

3. FMS logic that dropped all intermediate fixes from the display(s) in the event of execution of a direct routing.
4. FMS-generated navigational information that used a different naming convention from that published.

B717-200 Engine Shutdown

Background

- Left turn holding pattern, descending through FL 230, when right engine uncommanded in-flight shutdown
- No advisories of any type prior to shutdown
- Flight crew received a vectored straight-in approach and landing

B717-200 Engine Shutdown

- Troubleshooting revealed fault codes in computer memory, related to Channel A of EEC
- FMU replaced 50 flight hours prior
- No maintenance manual requirements for an EEC stored faults check following engine run
- Fault codes cleared from computer memory and engine successfully test run

B717-200 Engine Shutdown

DFDR readout

- Allied Signal Digital Solidstate, 600 plus parameters
- No. 2 engine EGT spike 420>680 degrees C
- No. 2 engine N2 spike (of 15.35 %)
- EEC disagree, No. 1 & 2 engine out
- No. 2 EEC fail bit
- Airspeed 230-250 knots

B717-200 Engine Shutdown

Follow on actions

- FMU and EEC removed for testing
- EEC sent to the engine manufacturer for testing and operating on test bed engine

B717-200 Engine Shutdown

Results

- FMU manufacturer's testing found no faults
- Initial testing of EEC on the test bed engine could not duplicate
- Testing with fault codes entered into and simulated loss of Channel B, successfully repeated the failure and shutdown

B717-200 Engine Shutdown

The EEC

- Two-channel (A & B) electronic unit with system redundancy
- Controlled, start, engine power, temperature, turbine speeds, fuel flow, monitoring, and automatic relight
- Fault detection, storage, and readout capabilities, stored on EEPROM

B717-200 Engine Shutdown

EEC testing/ after action

- Testing revealed RAM parity errors in Channel B of EEC resulted in multiple resets
- Repeated resets caused loss of channel
- Tiger Team established (EEC manufacturer involved)
- BR715 Communication RRD/022/2001 issued

B717-200 Engine Shutdown

EEC software version

- Version 5.0 susceptible to engine surging causing EEC reset
- SB BR700-73-100993 upgraded software to version 6.0.3/ eliminated surging
- Rest of operators fleet upgraded to version 6.0.3
- Failure mode different than version 5.0 concerns

B717-200 Engine Shutdown

EEC Analysis

- EEC operating on Channel B only
- Channel B experienced RAM parity errors and resets
- EEC reverted to Channel A for primary control
- Channel A was degraded by pre-existing FMU electrical fault codes

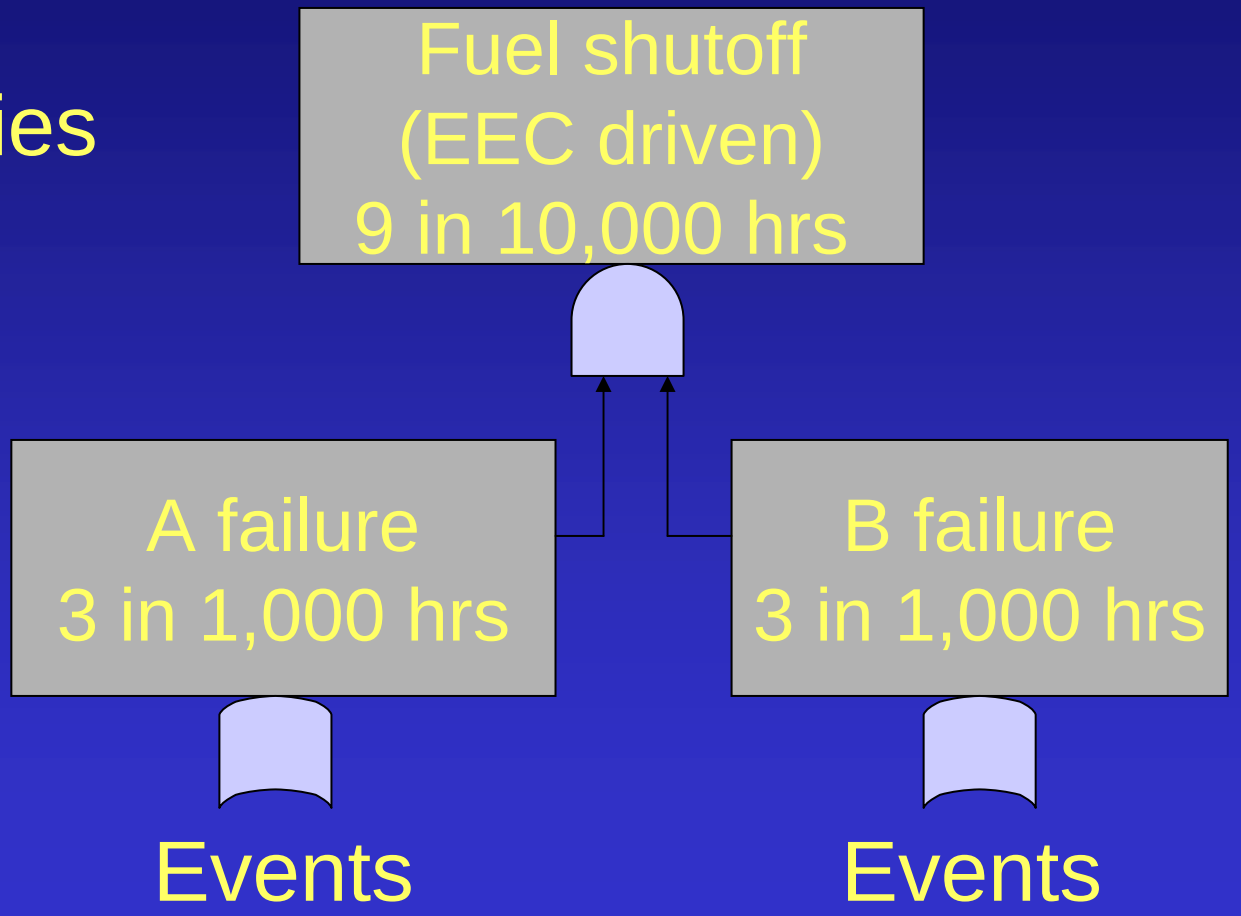
B717-200 Engine Shutdown

EEC Analysis

- Neither channel able to control the engine (redundancy lost)
- The fuel-control metering valve closed, resulting in fuel starvation and engine shutdown

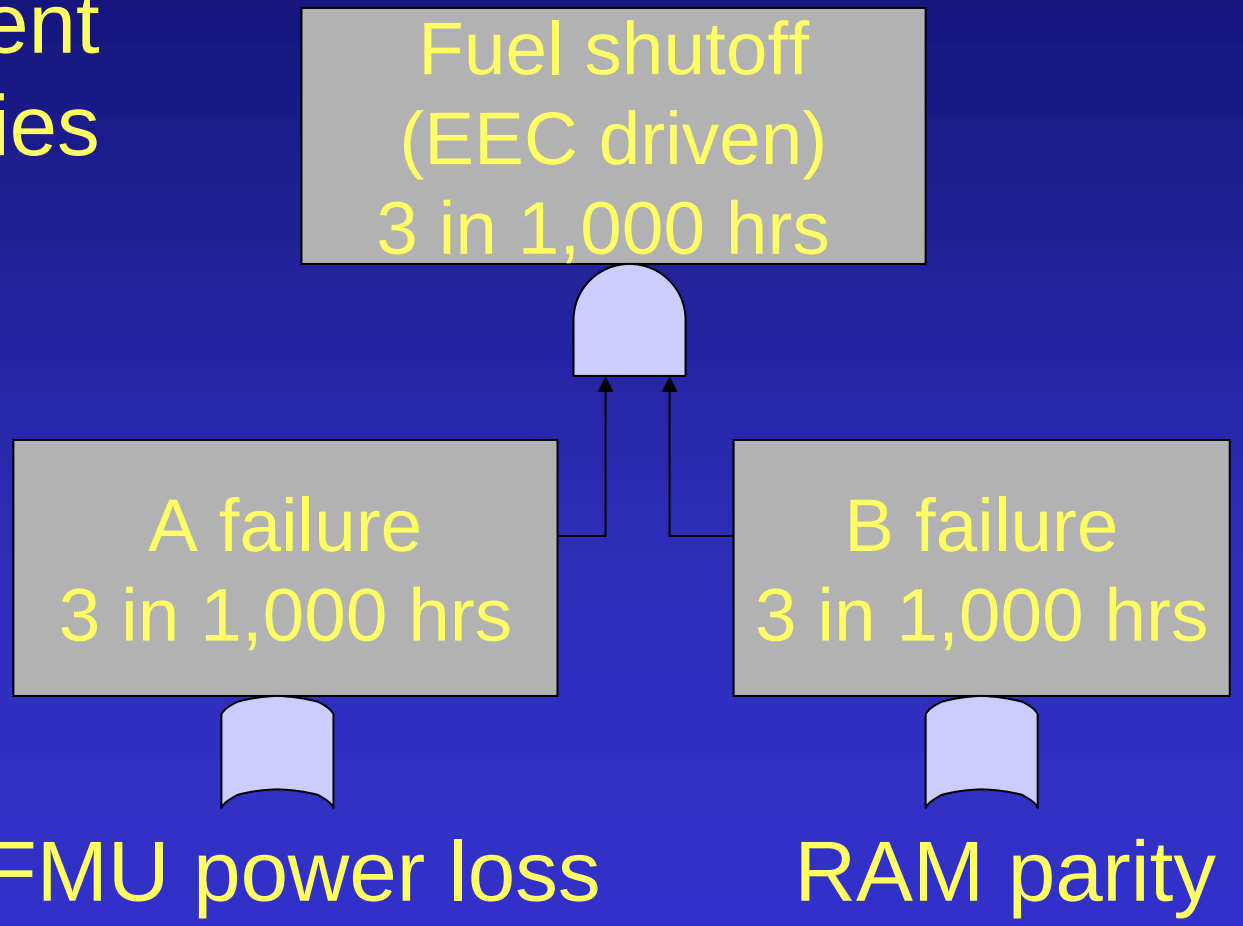
B717-200 Engine Shutdown

Projected (probabilities example only)



B717-200 Engine Shutdown

During event (probabilities example only)



B717-200 Engine Shutdown

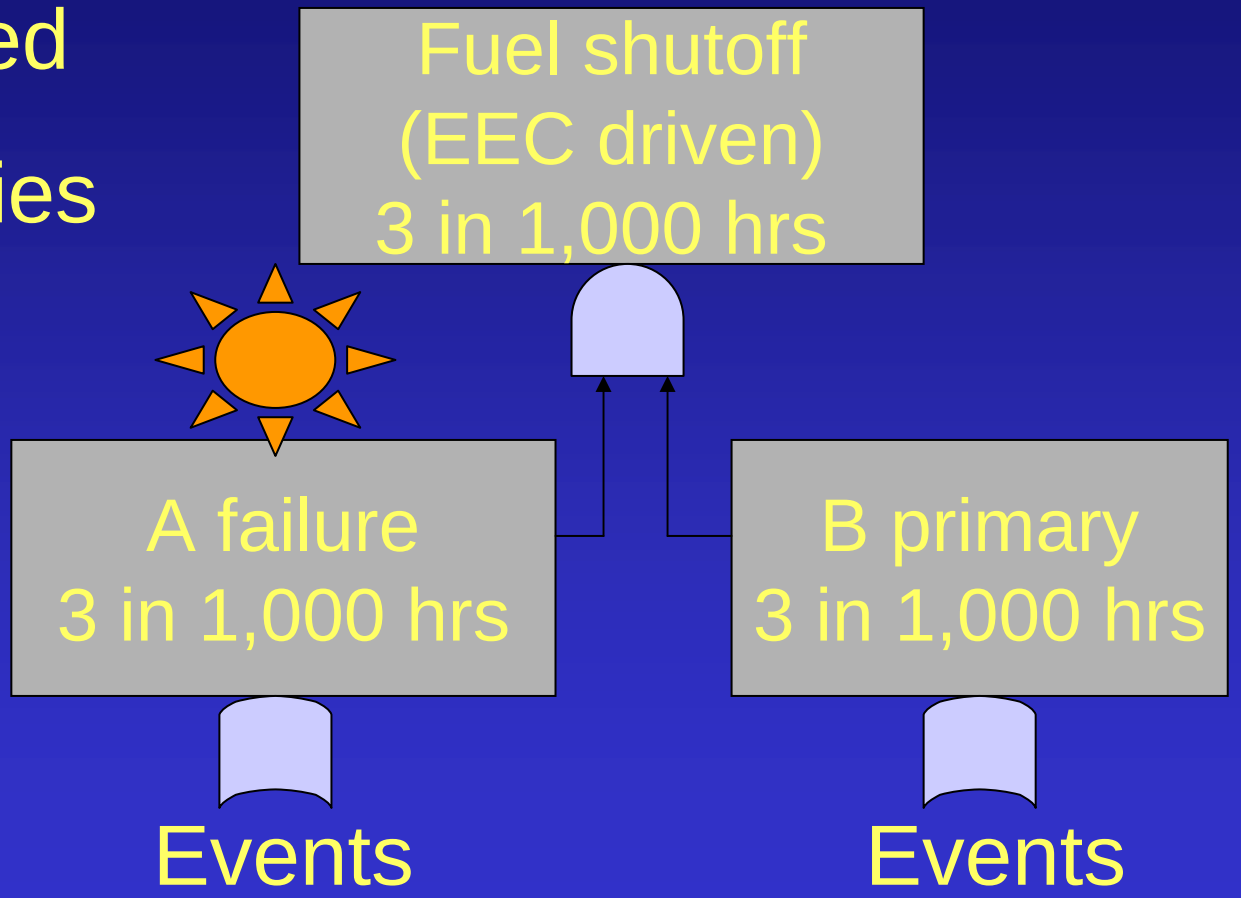
Safety action- engine manufacturer

- Revised FMU fault codes status raising priority from LTD to STD
- Software change to limit EEC susceptibility to RAM parity errors
- Maintenance manual change to introduce check for EEC FMU faults during engine run

B717-200 Engine Shutdown

Redesigned

(probabilities example only)



B717-200 Engine Shutdown

DFDR compliance

- When aircraft taxied to holding point and park brake set, stopped recording until brake released (not compliant to Australian CAOs)
- Information relating to operation of aircraft not recorded
- Recommendations to Australian Civil Aviation Safety Authority

B717-200 Engine Shutdown

Conclusion- the incident

- EEC was degraded, flight crew not “displayed” vital information concerning the status of EEC
- System redundancy safety factor removed, crew not advised
- Hindered their ability to isolate anomaly and take action

B717-200 Engine Shutdown

Conclusion- software issues

- Software technology/ design has advanced on a large scale
- Non-pilot rated design engineers determine what information will be display
- New requirement for “software sneak circuit analysis” to identify all the risks inherent in software system

B717-200 Engine Shutdown

Conclusion- software issues

- SS Engineers, may not have sufficient electronic software skills
- More responsibility placed upon the Electronic Software Design Engineers
- May not process skills and training required

Solutions

1. Training for engineering personnel in system safety principals
2. More involvement of SS Engineers in the software design process
3. More involvement by design engineering qualified pilots
4. Extensive testing of software systems prior to fielding to users

The Concern

- The behaviour of automated devices (based upon pilot input or other factors) may not be apparent to pilots, possibly resulting in reduced pilot awareness of automation behaviour and goals.

Thank you for your attention