Learning From our Mistakes – Prospects for a Discipline of Software Forensics

Paul Bailes[1,2]
with
Christine Cornish[1,2], Toby Myers[1,2], Lou Rago[2], Nick Tate[3] and Mal Thatcher[4]

[1]School of ITEE ,The University of Queensland, QLD 4072 Australia
[2]BCI Technology, Level 2, 167 Eagle St, Brisbane, QLD 4000 Australia
[3]RDSI Project, The University of Queensland, QLD 4072 Australia
[4]Mater Health Services, Raymond Tce, South Brisbane, QLD 4101 Australia

The Message

If aeronautical engineering can be developed and matured “from scratch” within a century, there is no excuse for accepting the excuse of immaturity for scandalous outcomes of software development and procurement.

Overview

- Software Development Catastrophes
- Chaos not Order
- Aeronautical Engineering Lessons
- Towards SEFA
- Challenges
- Conclusions

Software Development Catastrophes

- USAF ERP - US$1B(illion)
  - http://www.cio.com/article/721628/Air_Force_scraps_massive_ERP_project_after_racking_up_1_billion_in_costs
- UK welfare - UK £ 300M(illion)
  - http://www.nao.org.uk/report/universal-credit-early-progress/
- Queensland (Aus) Health payroll AU$1.2535B(illion)
  - http://www.healthpayrollinquiry.qld.gov.au/__data/assets/pdf_file/0014/207203/Queensland-Health-Payroll-System-Commission-of-Inquiry-Report-31-July-2013.pdf
- UK NHS - UK £ 12B(illion)
  - http://www.theguardian.com/healthcare-network/2011/sep/22/npfit-ends-cfh-andrew-lansley-bt-csc?newsfeed=true
- Obamacare
  - http://www.businessweek.com/articles/2013-10-16/open-source-everything-the-moral-of-the-healthcare-dot-gov-debacle
- Charette's (2005) Hall of Shame – 9-figure losses unexceptional
  - http://spectrum.ieee.org/computing/software/why-software-fails
- More recently …
  - http://www.computerworld.com/s/article/9234581/The_scariest_software_project_horror_stories_of_2012

Chaos not Order

- Requirements: nat.lang. vs logic vs graphics
- Specification: model-based vs abstract; logic vs graphical; executable vs non.
- Design: TP vs OO vs …
- Implementation: C++ vs Java vs Scala vs …
- V&V: formal methods vs testing
- Overall: waterfall vs V vs agile

V vs agile

V

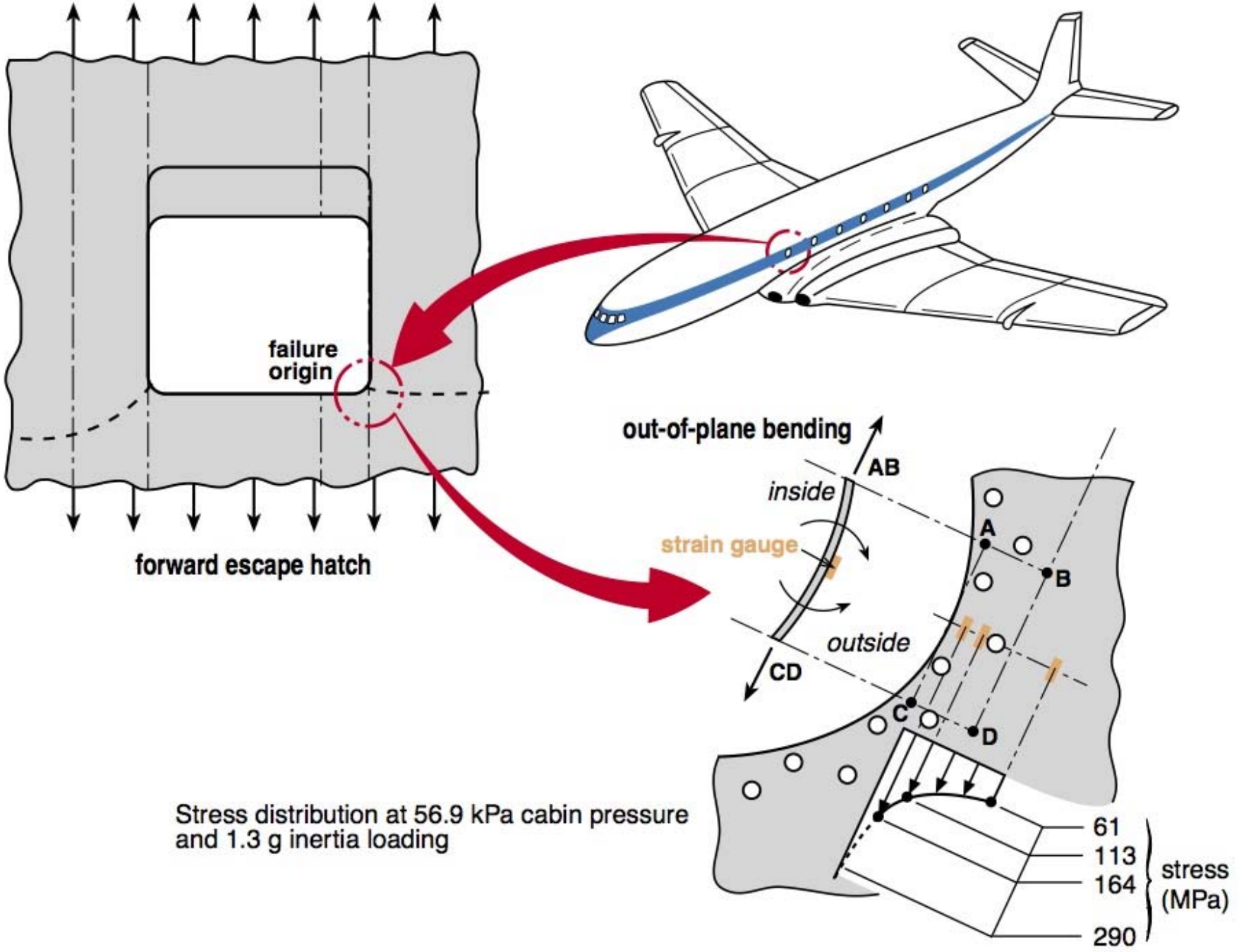
- Requirements
  - System Design
    - Architecture Design
      - Module Design
        - » Coding
      - Unit Test
    - Integration Test
  - System test
- Acceptance Test

Agile

- requirements refined from iterative coding

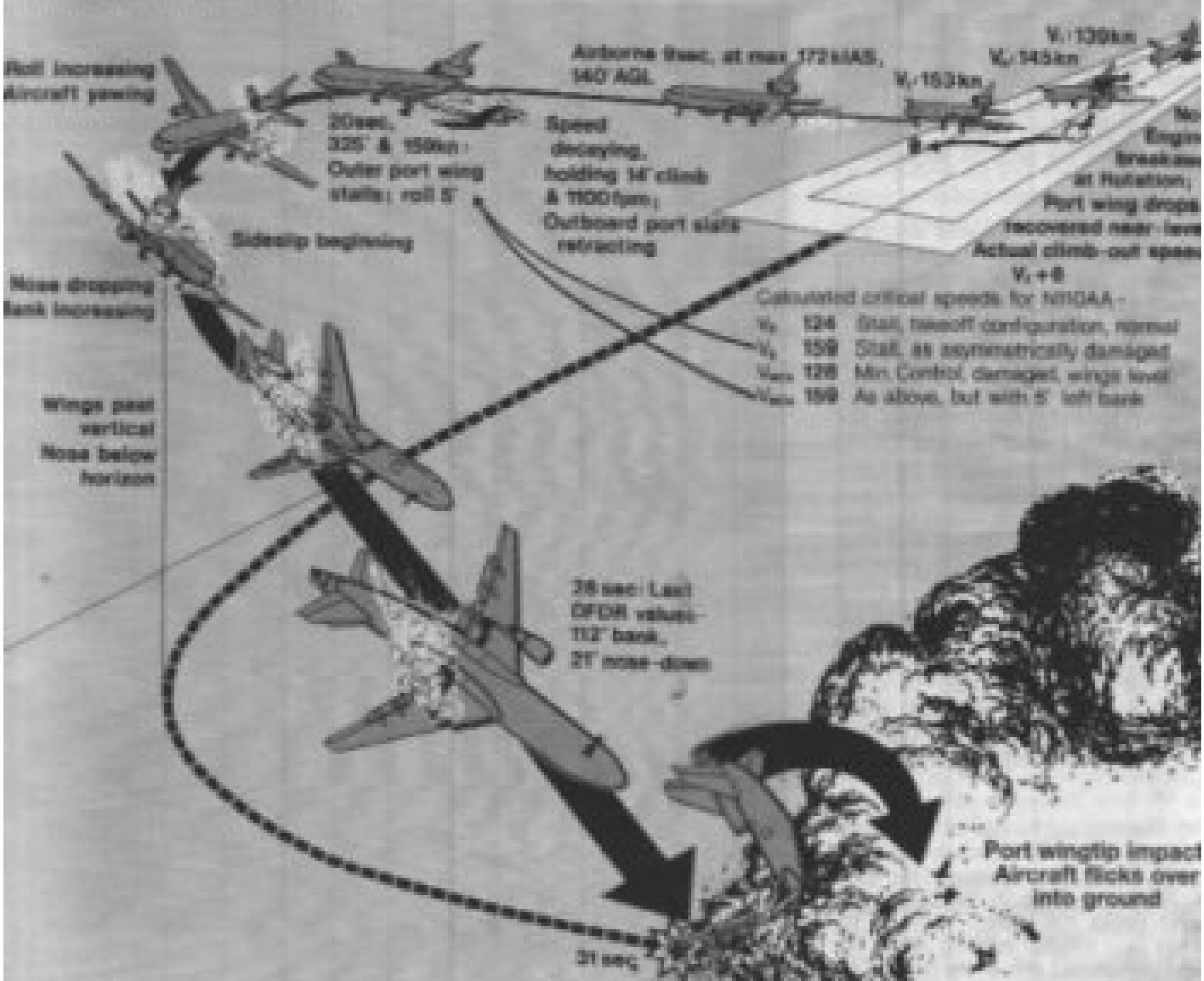
Aeronautical Engineering Failures

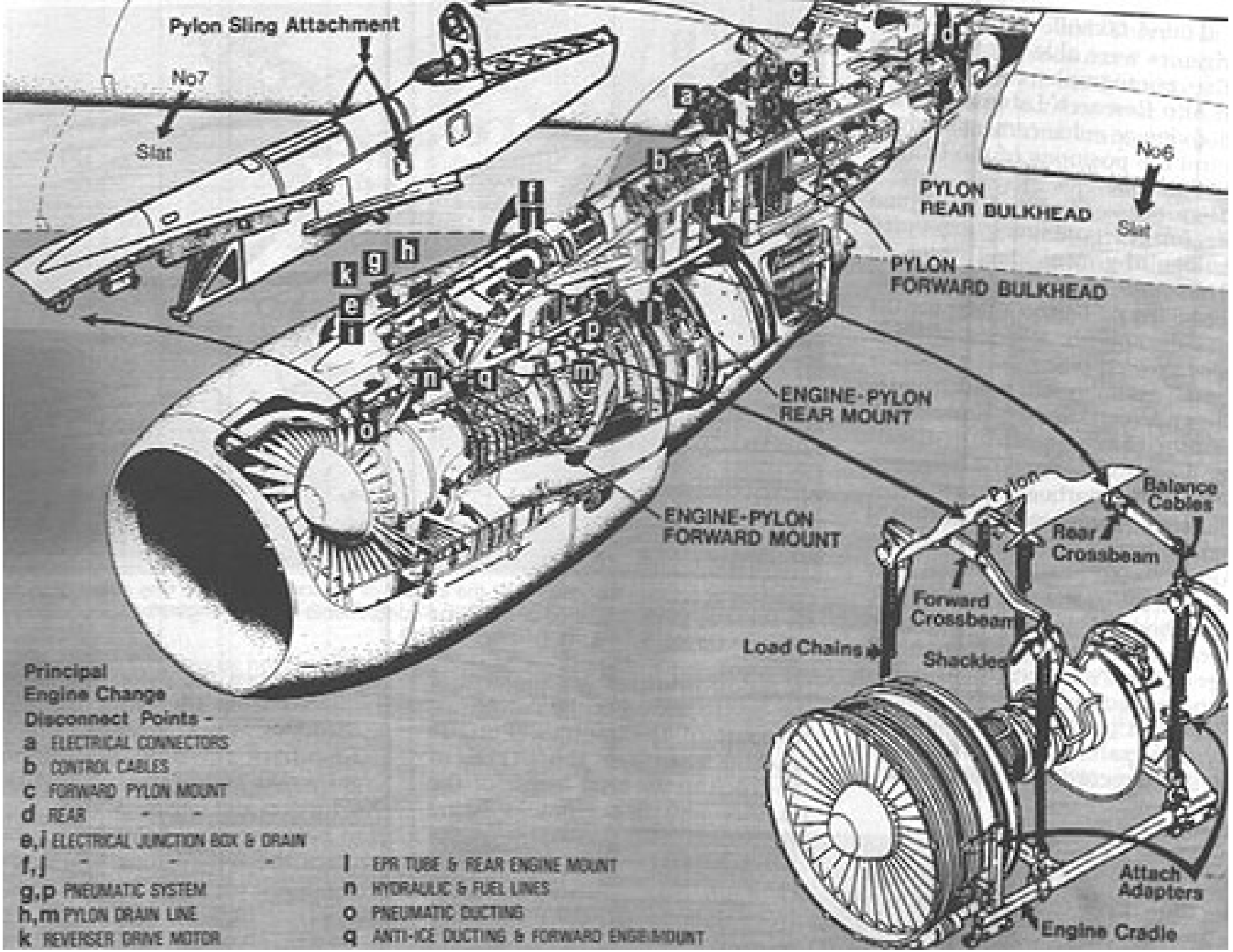
- very well-documented
  - http://en.wikipedia.org/wiki/Aviation_accidents_and_incidents
- ICAO Treaty (annex 13, since 1951)mandates investigative standards including national investigative bodies e.g.
  - http://www.aaib.gov.uk/home/index.cfm
  - http://www.aaib.gov.uk/cms_resources.cfm?file=/S2-2010%20Airbus%20A321-231,%20G-MEDJ%2012-10.pdf

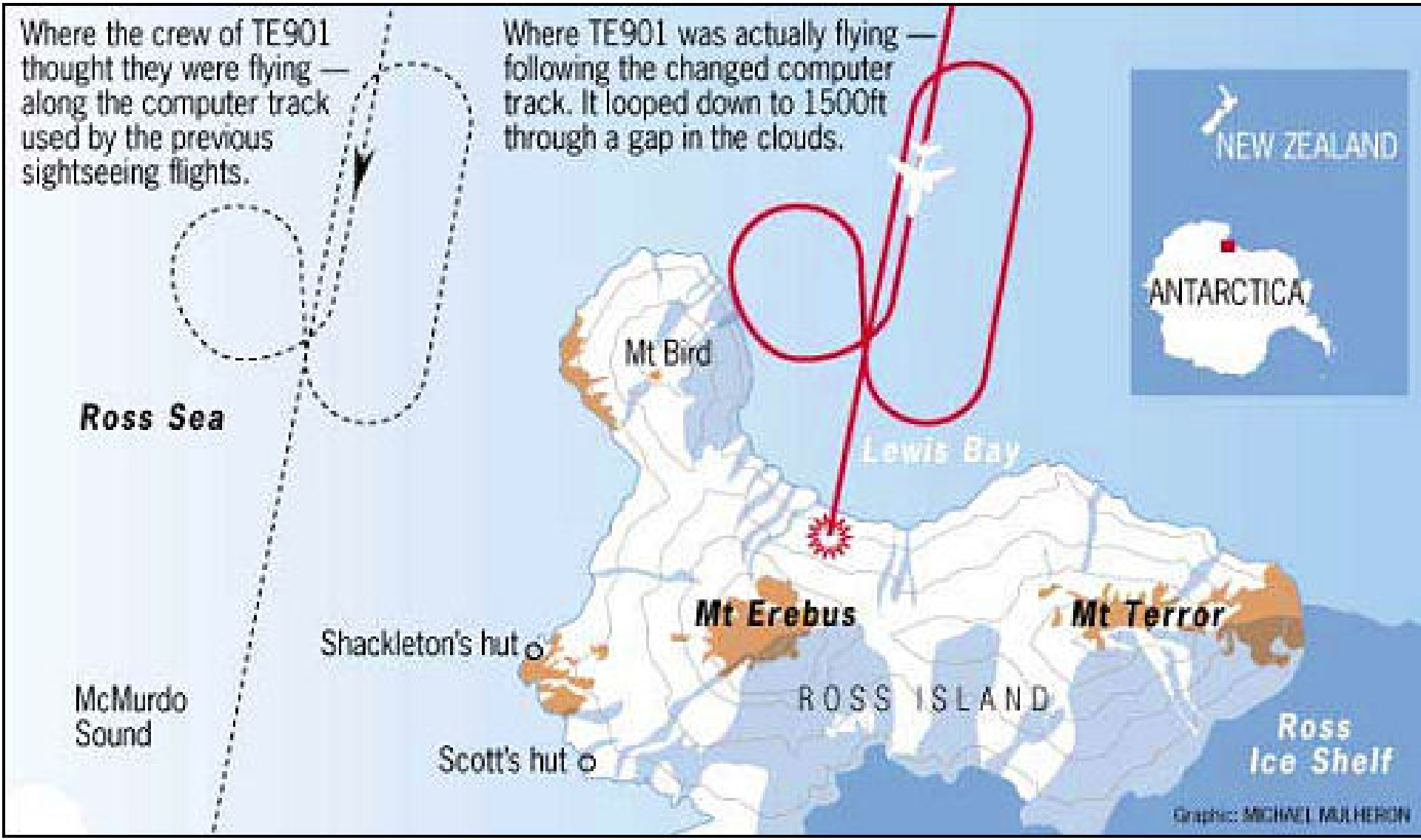


Stress distribution at 56.9 kPa cabin pressure
and 1.3 g inertia loading

Electra Wings Animation.htm


Roll increasing
Aircraft yawing
Airborne 9sec, at max 172 kIAS,
140' AGL
V1 139kn
VR 145kn
V2 153kn
20sec,
325' & 158kn:
Outer port wing
stalls: roll 5°
Speed
decaying,
holding 14° climb
& 1100fpm;
Outboard port slats
retracting
Sideslip beginning
Nose dropping
Bank increasing
Wings past
vertical
Nose below
horizon
Calculated critical speeds for N108AA -
VS 124 Stall, takeoff configuration, normal
VS 159 Stall, as asymmetrically damaged
VMCA 128 Min. Control, damaged, wings level
VMCA 159 As above, but with 5° left bank
26 sec: Last
DFDR values -
112° bank,
21° nose-down
Port wingtip impact
Aircraft flicks over
into ground
31 sec


Pylon Sling Attachment
No7
Slat
No6
Slat
PYLON
REAR BULKHEAD
PYLON
FORWARD BULKHEAD
ENGINE-PYLON
REAR MOUNT
ENGINE-PYLON
FORWARD MOUNT
Pylon
Balance
Cables
Rear
Crossbeam
Forward
Crossbeam
Load Chains
Shackles
Attach
Adapters
Engine Cradle
Principal
Engine Change
Disconnect Points -
a ELECTRICAL CONNECTORS
b CONTROL CABLES
c FORWARD PYLON MOUNT
d REAR - -
e,i ELECTRICAL JUNCTION BOX & DRAIN
f,j - - -
g,p PNEUMATIC SYSTEM
h,m PYLON DRAIN LINE
k REVERSER DRIVE MOTOR
l EPR TUBE & REAR ENGINE MOUNT
n HYDRAULIC & FUEL LINES
o PNEUMATIC DUCTING
q ANTI-ICE DUCTING & FORWARD ENGINE MOUNT


Where the crew of TE901 thought they were flying — along the computer track used by the previous sightseeing flights.
Where TE901 was actually flying — following the changed computer track. It looped down to 1500ft through a gap in the clouds.
NEW ZEALAND
ANTARCTICA
Mt Bird
Ross Sea
Lewis Bay
Mt Erebus
Mt Terror
Shackleton's hut
McMurdo Sound
ROSS ISLAND
Scott's hut
Ross Ice Shelf
Graphic: MICHAEL MULHERON

Aeronautical Engineering Lessons

- Evidence-based
  - fatigue
  - whirl mode → flutter
  - engine attachments
- Beyond technical
  - maintenance procedures
  - integrity of navigation parameters
  - ICAO treaty
    - *List the findings and causes established in the investigation. The list of causes should include both the immediate and the deeper systemic causes.*

Towards SEFA

- Knowledge
  - basic SE
  - legals
  - research (general and specific)
- Modes
  - preventive
  - corrective
  - investigative
- Structure
  - private “Software Forensics Institute”
  - AAIB/ATSB/NTSB

Challenges

- apprehend narrative record of specific projects
- assess against specific SE processes & techniques
- assess artefacts also
- what is the philosophical basis for making inferences
  - how do you really know if A caused B

Conclusions

SEFA raises hopes for the following:

- **an evidence-based, more specific understanding of the different circumstances under which different software processes and tools are more or less appropriate;**
- similarly for other variations from canonical process(es);
- meta-level tools and techniques to enable the above;
- more specific directions in software engineering education and training;
- incidentally, because software systems dominate aeronautical engineering, a formally-established “Software Forensics Institute” would discharge implicit ICAO obligations in software dimension of air accident investigations.

Some specific tech. issues

- “black boxes” for software developers
- integrated standards as bases e.g.
  - OGC Gateway
  - ISO standards (12207 & 15288)
- a rubric when “agile” methods are appropriate (or not)!
- meta-level considerations e.g.
  - recording of forensic investigators’ implicit assumptions

  = “black boxes” for software forensic investigators

Aims:

- to advance the theory and practice of software engineering through the analysis of software development projects by distinguishing between the characteristics of successful versus failed or failing projects;
- simultaneously, to develop tools and techniques to facilitate these analyses;
- equally, to foster the development of social institutions and practices (both voluntarily and by regulation/legislation, as appropriate) that will encourage the adoption and application of the above;
- thereby engendering improvements in the timeliness, cost and effectiveness of significant software procurement exercises;
- and thus, to achieve the economic and social benefits resulting from all the foregoing.