

User Interface Risks



Matt Welsh

UCB CS260, 1 April 1998

Risks of Computers and Technology

Often an underlooked area

- 'Human error' often attributed
 - Assumption that engineers can design RISK-free systems
 - Finger-pointing and nose-thumbing
 - Lack of government, industry standards
-
- **Safety**
 - Threat of loss to life, limb, property
 - Airliner crashes, automobile safety, health-related computer systems, etc.
-
- **Privacy and Security**
 - Exposure of information to unintended parties
 - Online securities trading, credit card purchases, e-mail love letters
 - (Use of Safeway Card)

A Good Example of a user-interface risk

-- Laptop Automated Suicide System --

Do you not want to take your
own life now?

[YES]

[NO]

USS Vincennes Disaster

3 July 1988, USS Vincennes shot down Iran Air flight 655

- 290 people on board died
- During battle with surface boats
- Vincennes AEGIS system misread IFF from airliner as Mode II (military)
- Iran Air 655 was transmitting Mode III (civilian) squawk
- Mistake generally attributed to command confusion, and ...

Bad UI Design Points

- AEGIS display did not directly show altitude of tracked aircraft
- (Had to consult a printout to get altitude readings)
- Size of aircraft not displayed
- Radar assembly focused on airport with Iranian F-14s
- Mistaken Mode II squawk remained tagged with Iran Air 655

China Airlines A300/600 Disaster

26 April 1994, China Airlines Airbus A300/600 to Nagoya

- Crashed during landing, 264 people died
- During approach copilot accidentally sets autopilot to 'go-around' mode
- (Mode used to retry the landing approach; pulls up aircraft automatically)
- Pilot informs copilot of mistake
- Copilot tries to pitch down manually while autopilot pitches up
- Autopilot switched off, plane too high to land so switched back on
- Stall-prevention system kicked in
- (Increased thrust which increased climb to 52 degrees)
- Plane crashed tail-first

China Airlines A300/600 Disaster - Reasons

Copilot confusion over mode of autopilot

- GA mode switched on by accident
- Copilot trying to pitch down while autopilot engaged
- Pilot confused after taking control

Autopilot should have disengaged

- Manual control should have overridden GA on autopilot

Stall-prevention systems caused stall

- Thrust increased which increased the (already high) climb angle

American Airlines 965 Disaster

20 Dec 95: AA965 from Miami to Cali, Columbia

- Crashed into mountains during landing approach, 160 people died
- Approach path dog-legged through canyon via ROZO NDB and Tulua VOR
- Pilots confused about dogleg path and request direct landing
- Pass Tulua VOR then realize the mistake
- ATC operator confused and did not speak English well

Flight computer confusion

- Pilots enter direct route to Cali VOR ("CALI")
- Pilots enter "R" for ROZO
- (However "R" is both ROZO and ROMEO VOR, 150 nautical miles from ROZO)
- (Papers inconsistent with FMC database)
- Plane turns left towards ROMEO for 87 seconds
- Pilots then program for Tulua VOR which they already passed
- Plane turns right towards Tulua, crashes into mountain

Other HCI-related Airline Disasters

Northwest 255, 16 Aug 87, Detroit - 156 fatalities

- Warning system for flaps/slats disabled by pilot due to annoyance

Air Inter A320, 20 Jan 92, Strasbourg - 87 fatalities

- Pilot confusion over two descent modes

Birgenair B757, 6 Feb 96, ocean off Dominican Republic - 189 fatalities

- Speed indicator faulty; led pilot to believe speed was adequate

Las Vegas Lasers

- Luxor in Vegas had a laser which would blind pilots flying over
- Hilton installed TCAS(!) to shut off lasers if aircraft fly in their path
- FDA ordered a halt to laser shows within 20 miles of Vegas airports

THERAC-25 Accidents

3 June 85, Kennestone

Burn to patient's breast and arm, settled out of court

26 July 85, Ontario

'H-tilt' error and repeated 'P' 4 times

Patient died 3 Nov 95 of cancer but would have needed hip replacement

AECL suspected microswitch problem with turntable position

AECL reduces number of retries on dose malfunction from 5 to 3

December 95, Yakima

Overdose causes striped pattern on hip of patient

Not much done as THERAC-25 not suspected

THERAC-25 Accidents - 2

21 March 86, ETCC

Operator corrects 'x' to 'e'; 'Malfunction 54' errors; retries with 'P'

Patient gets up during second try and bangs on operator room door!

Machine used for rest of the day

Patient dies 5 months later; AECL suspects electrical problem

11 Apr 86, ETCC

Again 'x' to 'e' correction, 'Malfunction 54', patient dies 3 weeks later

Tyler physicist does experiments and discovers race condition

AECL reproduces the next day

THERAC-25 Accidents - 3

2 May 86: FDA requests first CAP from AECL

13 June 86: First CAP from AECL to FDA

12 November 86: AECL first CAP revision

22 December 86: AECL second CAP revision

17 January 87, Yakima

Patient receives two film-verification exposures

Operator moves turntable to field-light position and returns with 'set' button

Beam engaged; no dose shown; proceeds with 'P'; another shutdown

AECL thinks beam came on in field-light position? Patient dies in April.

10 Feb 87: FDA, Canada find THERAC-25 defective under law

Warning to customers from AECL until August 87

5 March 87: AECL third CAP revision

1 May 87: AECL fourth CAP revision

21 July 87: AECL final CAP revision

THERAC-25 Accidents - Reasons

Data-entry race condition

- User corrects data in under 8 seconds while beam magnets being set
- Editing changes shown on screen but not recognized by system
- In 'x' to 'e' case, X-Rays delivered instead of electrons

Turntable position problem

- 'Set' button pressed by operator when counter rollover occurred
- Beam engaged while turntable in field-light position

General software engineering and QA problems

- AECL not responsive to problem reports or lawsuits
- Entire CAP process: 2 May 86 - 21 July 87!
- AECL quality assurance shoddy
- Too many safety checks placed in software?

Risks - General Principles and Concerns

Lack of a system-wide approach

- Placing too much blame on one component of a system
- Was AEGIS designed for the Vincennes scenario?
- Was a single component failure to blame for THERAC-25 accidents?

Too much attribution to human error

- 'Everything' is human error
- Need to study interaction with humans and the system

Misunderstanding of software complexity

- Belief that software as good as hardware - if not better
- Inadequate testing and real-world verification
- Remember the Ariane 5!

Lack of an audit trail

- No way to determine behaviour of systems after-the-fact
- Example: AECL claimed that memory limitations made this impossible

Risks Resources

RISKS Digest, comp.risks

- Moderated by Peter Neumann
- Archives at <http://catless.ncl.ac.uk/Risks/>

Airline disaster sites

<http://mek.ml.org/~ladkin/Incidents/FBW.html>

<http://www.pongnet.nl/avnsafety/>

<http://www.webcom.com/~terps/cali/welcome.html>

<http://www.primenet.com/~kebab/>

Computer-Related Risks, Peter Neumann, Addison-Wesley/ACM Press

- Great overview book of many kinds of computer and technology risks