Day 21

Fatal Glitches
Ariane 5 Rocket
Antares
Therac-25
HRO structures
Failures & Errors

Common issue:

- Reuse of old software with new elements tacked on + insufficiently tested

Ariane 5 rocket (France)

- 1996 Test Launch: Data conversion error: old software subsystem used 16 bit integers, was not replaced – new software used 64 bit integers, resulting in an operand conversion error.
- Next launch was delayed until 2002
- No humans aboard (just ~$500 million in equipment)

Textbook p377
Reusing old software:

It is essential to reexamine the specifications and design of the software, consider implications and risks for the new environment, and retest the software for the new use.
Antares (2014)

- Used Soviet Era (1970s) engines and state of the art software

http://www.universetoday.com/115828/soviet-era-engines-likely-caused-antares-rocket-failure/
Medical devices

The software in a pacemaker may require over 80,000 lines of code, a drug-infusion pump 170,000 lines and an MRI (magnetic-resonance imaging) scanner more than 7m lines.

When code can kill or cure:
http://www.economist.com/node/21556098
Massive overdoses of radiation were given; the machine said no dose had been administered at all.

Caused severe and painful injuries; + the death of six patients.

Manufacturer, computer programmer, and hospitals/clinics all have some responsibility.

http://www.ccnr.org/fatal_dose.html
1 issue with Therac-25: Race Condition Bug
Other issues

○ Re-used software from older systems, unaware of bugs in previous software
○ Inadequate test plan
○ Bugs in software
  ○ Allowed beam to deploy when table not in proper position
  ○ Ignored changes and corrections operators made at console
○ Error messages not descriptive

Textbook p380-383
Why so many deaths?

0 Hospitals had never seen such massive overdoses before, were unsure of the cause

0 Manufacturer said the machine could not have caused the overdoses and no other incidents had been reported (which was untrue)

0 The manufacturer made changes to the turntable and claimed they had improved safety after the second accident. The changes did not correct any of the causes identified later.
Why so many deaths? (cont’d)

- Recommendations were made for further changes to enhance safety; the manufacturer did not implement them.
- The FDA declared the machine defective after the fifth accident.
- The sixth accident occurred while the FDA was negotiating with the manufacturer on what changes were needed.

http://www.ccnr.org/fatal_dose.html
Some observations and perspective:

- Minor design and implementation errors usually occur in complex systems; they are to be expected.
- The problems in the Therac-25 case were not minor and suggest irresponsibility.
- Old problem, new context → In the past, technicians...
  - Left a patient after treatment started to attend a party.
  - Did not properly measure the radioactive drugs.
  - Confused micro-curies (1/1,000,000) and milli-curies (1/1,000).
Lessons learned

- Stress importance of good software engineering and **professional responsibility** in the tech sector
- Redundancy & Testing
  - Include **real world testing** with real users + IV&V
Redundancy

- Multiple computers capable of same task; if one fails, another can do the job.
- Voting redundancy: multiple programming languages used to write modules for same purpose.
Lessons Learned

0 User interfaces should:

✓ provide **clear instructions and error messages**

✓ be **consistent**

✓ include appropriate **checking of input to reduce major system failures caused by typos or other errors a person will likely make**
Professional Techniques

Management and communication principles:

- **Preoccupation with failure**
- **Loose structure** (no strict or intimidating hierarchy between programmers and others)

An HRO is an organization that avoids disasters in a setting where catastrophes would seem common due to high risk and complexity.
“Part of our engineering culture is that you should work through your chain of command. I will regret, always, why I didn’t break the door down by myself [to stop the launch].”

Quoted to NY Times regarding Columbia explosion, 2003

Safety Critical

- Require a convincing case for safety, not just the apparent absence of danger.
- Define boundaries of acceptable risk and do not extend them.
10th Challenger - 1986

O-ring failure

Rubber O-rings, nearly 38 feet (11.6 meters) in circumference; 1/4 inch (6.4 mm) thick.

Estimated launch temperature 29°

https://www.space.com/31732-space-shuttle-challenger-disaster-explained-infographic.html

Columbia Cont’d
Columbia Cont’d
More lessons

- Even small changes need thorough testing
- Independent verification and validation (IV&V)
- Beta testing
Lion Air flight carrying 188 passengers crashes minutes after takeoff from Jakarta

A plane has reportedly crashed near Jakarta minutes after takeoff. The Lion Air flight had 188 passengers on board, according to the Indonesian Transport Ministry.

The pilot union for American Airlines, which also flies the new version of the 737, the Max 8, said Tuesday that the emergency system in question had not been included by Boeing in the standard operating manual. In addition, the flight check list — which contains information for manually overriding the emergency system — was incorrect, the union said.

The emergency system is intended to maneuver the plane out of a stall, when its nose is often angled too sharply upward. The system automatically pushes the nose down. If activated incorrectly, it could have sent the plane into its fatal dive, especially if the pilots were not properly trained on how to deal with such a situation.

In addition, he said, the onboard checklist that pilots had been carrying gave what now appears to be incorrect instructions for pulling out of the emergency condition that apparently confronted the Lion Air pilots.
Ethiopian Airlines Crash Kills at Least 150; 2nd Brand-New Boeing to Go Down in Months

Are There Problems With the Boeing 737 Max? A Second Deadly Crash Raises New Questions

New York Times, March 2019
“Pilots were comfortable flying it, while airlines didn’t have to invest in costly new training for their pilots and mechanics. For Boeing, it was also faster and cheaper to redesign and recertify than starting anew....

But the strategy has now left the company in crisis, following two deadly crashes in less than five months. The Max stretched the 737 design, creating a patchwork plane that left pilots without some safety features that could be important in a crisis — ones that have been offered for years on other planes. It is the only modern Boeing jet without an electronic alert system that explains what is malfunctioning and how to resolve it. Instead pilots have to check a manual.”
Trust the human?

**TRAFFIC COLLISION AVOIDANCE SYSTEM (TCAS)**

Automated system that directs pilots in case of imminent collision.

- Computers in some airplanes prevent certain pilot actions
- Near misses and accidents
In 2011, FAA officials and then-Transportation Secretary Ray LaHood promised reforms after a nearly a dozen incidents in which air traffic controllers were discovered sleeping on the job or didn’t respond to calls from pilots trying to land planes late at night. In one episode, two airliners landed at Washington’s Reagan National Airport without the aid of a controller because the lone controller on the overnight shift had fallen asleep.

https://www.pbs.org/newshour/nation/faa-controllers-working-exhausting-schedules
http://www.slideshare.net/JLGChico/Analysis-of-OE-and-interaction-to-TCASPaper-131Final-Presentation-808974