

CS777 - Forensics

Spring 2009

Instructor: Dr. Olly Gotel (ogotel@pace.edu; Room: 212)

There have been a number of well-publicised software-based system failures, of which the London Ambulance Computer-Aided Despatch System is an example (discussed fully in CS775). You have each been allocated an example of an engineering failure to research. You are asked to provide a succinct report of the failure and the events leading up to it (remember, you are unlikely to find a system in which the software is *entirely* to blame for the failure). Try to answer the following questions:

- What happened?
- In what way was the system unreliable?
- What realistic level of reliability would be anticipated for a system of this nature? I.e., what would be an acceptable failure rate? How would this be determined?
- In what ways does this example exhibit either good or poor quality practices?

This exercise requires that you do some research. A good source of material is the Risks Electronic News Group (you can access archives on line at <http://catless.ncl.ac.uk/Risks/>). I have provided you with one reference on each incident to get you going, but I expect you to use your initiative! You are to hand in a 2-page summary of the incident (typewritten) at the start of the next class, being sure to attempt to answer the above questions. Please also email me a copy. You will give a brief 5 minute in-class presentation on the incident.

Incident List

These have been chosen due to the wealth of documentation available on-line:

1. Space Shuttle Challenger Accident (Flight STS51-L) in 1986
<http://history.nasa.gov/rogersrep/51lcover.htm>
2. Loss of NASA's Mars Polar Lander and Deep Space 2 Mission in 1999
<http://www.spaceref.com/news/viewnews.html?id=105>
3. Loss of NASA's Mars Climate Orbiter in 1999
<http://www.geocities.com/CapitolHill/Parliament/2191/MCO2.htm>
4. Denver International Airport Baggage Handling System Fiasco (1989-1995)
<http://www.geocities.com/kschottland/dia.html>
5. Therac-25 Accidents (1985-1987)
<http://sunnyday.mit.edu/papers/therac.pdf>
6. AT&T Network Crash of 1990 <http://www.dmine.com/phworld/history/attcrash.htm>
7. Abandonment of the London Stock Exchange Taurus Trading System in 1993
http://www.practicallaw.com/scripts/article.asp?Article_ID=4003
8. Patriot Missile Failure of 1991
<http://www.fas.org/spp/starwars/gao/im92026.htm>
9. Failure of the Aegis System on U.S.S. Vincennes in 1988
<http://www.cs.jcu.edu.au/ftp/web/teaching/Subjects/cp1500/1995/foils/may26/may26.html>
10. Failure of the Titan IV B-32 Mission in 1999 http://sunnyday.mit.edu/accidents/titan_1999_rpt.doc
11. Various Airbus failures over the years (select one) e.g. http://www.airdisaster.com/cgi_bin/view_details.cgi?date=09141993®=D-AIPN&airline=Lufthansa
12. Any other incident of your choosing...

Let me know if these links are no longer available – they were last time I looked! If you find another more recent incident you wish to explore, please discuss with me.