Lecture 22: Software Disasters

Kenneth M. Anderson
Software Methods and Tools
CSCI 3308 - Fall Semester, 2004

Today's Lecture

- Discuss several different software disasters to provide insights into
  - the types of errors that can occur
  - the costs associated with them
- Examples
  - Mars Climate Orbiter
  - Mars Polar Lander
  - Patriot Missile Defense System
  - Ariane 5

Mars Climate Orbiter

- Science Objectives
  - Monitor climate changes
  - Serve as relay for Mars Polar Lander
- Costs for Climate Orbiter and Polar Lander combined
  - Spacecraft Development - 193.1 million
  - Launch - 91.7 million
  - Mission and Operations - 42.8 million
  - Total - 327.6 million

Mars Climate Orbiter, continued

- Supposed to enter Martian atmosphere "at a high trajectory" and "lightly aerobrake" to achieve orbit, which uses less fuel
- Due to a conversion error in which commands to the spacecraft were sent in English units rather than metric units, the spacecraft entered the atmosphere at "a trajectory 170km lower than planned"
  - The spacecraft hit the atmosphere earlier than was planned and was thus traveling too fast; this led to the destruction of the spacecraft
  - Since the Polar Lander was also lost, the combined cost of the project stands at 327.6 million dollars
  - Compare to Mars Observer (lost in 1989): 4 billion dollars!
- Unofficially, the problem had been detected but due to politics between the development team and JPL, a fix was never deployed

Mars Climate Orbiter, continued

- The official report cited the following "contributing factors" to the loss of the spacecraft
  - undetected errors in ground-based models of the spacecraft
  - the operational navigational team was not fully informed on the details of the way that Mars Climate Orbiter was pointed in space
  - a final, optional engine firing to raise the spacecraft's path relative to Mars before its arrival was considered but not performed

Mars Climate Orbiter, continued

- Contributing Factors, continued
  - the systems engineering function within the project that is supposed to track and double-check all interconnected aspects of the mission was not robust enough
    - this was exacerbated by the first-time handover of a Mars-bound spacecraft by the team that constructed and launched the vehicle to a new multi-mission operations team (this is the "politics" part!)
  - some communications channels among project engineering groups were too informal (e.g. not documented!)

Mars Climate Orbiter, continued

- Contributing Factors, continued
  - the small mission navigation team was oversubscribed and its work did not receive peer review by independent experts
  - personnel were not trained sufficiently in areas such as the relationship between the operation of the mission and its detailed navigational characteristics, or the process of filing formal anomaly reports
  - the process to verify / validate certain engineering requirements and the technical interfaces between some project groups, and between the project and its prime mission contractor was inadequate

Mars Climate Orbiter, summary

- One Technical Problem
  - failed conversion of units
- Many Process and Social Problems
  - No review (e.g. verification), insufficient training, informal processes in place, formal processes ignored
- Led to a destroyed spacecraft

Mars Polar Lander

- Part of the same project as the Mars Climate Observer
- Last communication with spacecraft occurred just prior to its entry into the Martian atmosphere
- Loss of spacecraft can be attributed to the lack of integration testing
  - e.g. the failure was not detected by "module" testing
  - an integrated test across subsystems was required to detect the problem

Details

- Module Test 1
  - Give command to deploy spacecraft's legs
    - Legs deploy
      - Test Passed!
- Module Test 2
  - When spacecraft detects "jolt" of landing on the surface of Mars, turn engine off
    - Simulated "jolt" detected, engine shuts off
      - Test Passed!

Details, continued

- What actually happened
  - Spacecraft enters atmosphere
  - Legs deploy and "jolt" the craft
  - "Jolt" detected and engine shuts off
- The problem
  - Spacecraft was still miles above the surface of Mars!
  - Spacecraft crashes into Mars and is destroyed

Mars Polar Lander, summary

- Clear demonstration of the importance of integration testing
  - If the team testing the deployment of the legs had conducted the test while also testing the flight software, the "bug" may have been detected
  - Unfortunately, with the "faster, better, cheaper" philosophy of NASA at the time, integration testing was deemed too expensive and was not conducted in a comprehensive fashion