Software Accidents and Disasters

Bernd Schoeller

Zurich, October 4th 2005
Overview

- Ariane 5
- Mars Climate Orbiter
- Los Angeles air control system
- USS Yorktown
- Patriots vs. SCUTs
- Homework: Therac 25
Ariane 5: about

- New carrier rocket for ESA
- Weight: 740t
- Carrying capacity: 7 - 18t
- Duration of development: 10 years
- Cost of development: 6'700 Million Euros
Ariane 5: event

- June 4, 1996 maiden flight
- After 36.7 seconds: back-up inertial reference system (SRI) becomes inoperative
- 0.05 seconds later: active SRI fails → no longer correct guidance and attitude information
- active SRI transmits essentially diagnostic information to launcher’s main computer, where it is interpreted as flight data and used for flight control calculations
- main computer commands booster nozzles and main engine nozzle to make a large correction for an attitude deviation that had not occurred
- 39 sec. after start: Ariane 5 self-distructs
Ariane 5: what happened?

- Ariane 5 used same software as Ariane 4
- For Ariane 4: proved that horizontal velocity cannot exceed certain limit
- BUT: build-up of horizontal velocity was five times more rapid than for Ariane 4
- Higher horizontal velocity of Ariane 5 caused exception during execution of a data conversion from 64-bit floating point to 16-bit signed integer value
Mars Climate Orbiter: about

- Mars Climate Orbiter was planned to be the first weather satellite to orbit a foreign planet.
- Total cost: $125 million.
- Engine controlled by the NASA JPL (Jet Propulsion Laboratory).
- Used engines from Lockheed Martin Astronautics Co., Denver, Colo.
Mars Climate Orbiter: event

- September 23, 1999
- 100 km off course
- Entered the atmosphere and burned
- CFIT (controlled flight into terrain)
Mars Climate Orbiter: what happened?

- Caused by a design flaw, the flight had to have constant corrections

- The corrections were calculated in Newton by JPL

- Based on numbers provided by Lockheed Martin in Pound Force

- Factor of 4.45 between two units

- Major management issues in detecting and correcting the errors

- Reviews were impossible because of 30 year old code - “cannot be run, see or verified”
Los Angeles Air Control System: about

- The Voice Switching and Control System (VSCS) manages voice communication between pilots and air traffic controller.
- Deployed since the mid-1990s.
- Uses touchscreens.
- Connects nearly 160 ATCs on about 100 channels.
- „Complex System“
Los Angeles Air Control System: event

- September 14, 2004, 5pm
- Without warning, the system stopped working
- 400 planes in the air
- Many on collision course
- 5 incidents of planes coming within minimum separation distance
- ATCs used mobile phones to call up aircraft companies and other ATC-centers to inform planes about collisions
- Real hero: Collision Avoidance System
Los Angeles Air Control System: what happened?

- VSCS has an update system called VCSU
- This update system has a counter
- Counter is initialized with $2^{32}$
- Counts down to measure time every millisecond
- Runs out after ~50 days
- Normally the system should have a full reboot every 30 days
- Caused a crash one week later in Seattle
- Bug was known to the producer, but not to the customer
USS Yorktown

Event:
- 1998
- Ship was dead in the water for several hours

What happened:
- A crew member mistakenly entered a zero for a data value, which resulted in a division by zero.
- The error cascaded and eventually shut down the ship's propulsion system.
- The program didn't check for valid inputs!
Patriot Missile

About:
- Surface-to-air missile system
- Used to intercept enemy Scud missiles

Event
- February 25, 1991
- Gulf war in Iraq
- US Patriot Missile battery fails to intercept Iraqi Scud
- Scud hits US-barracks in Dharan killing 28 soldiers
Patriot Missile: what happened?

- Internal clock advances every 1/10 of a second
- Time since reboot: internal clock * 1/10
- System uses 24bit fixed point register to calculate 1/10 → rounding error of 0.000000095
- Time error after 100 hours of operation: 0.342 sec
- Scud missile travels ~600m in 0.342 sec !!!!
- Patriot missile system detected the Iraqi Scud missile but then LOST it because it was looking in the wrong part of the sky!
References

http://www.imam.edu/~arnold/disasters/ariane.html

http://www-aix.gsi.de/~giese/swr/ariane5.html

http://infotech.fanshawec.on.ca/gsantor/Computing/FamousBugs.htm

http://www.imam.edu/~arnold/disasters/patriot.html
Exercise For Next Week

- Therac-25

- Search for information on the incident

- Give a short (max 1 page) summary:
  - Why did the error happen?
  - Why wasn’t the flaw in the software detected before?
  - What could be done (with software engineering) to prevent such mistakes in the future?