

Amazon Cloud Outage - 2011

- Loss
 - difficult to quantify, but many Web 2.0 websites were affected for hours, days
- Description
 - Amazon EC2 services were unavailable for hours
 - Some permanent data loss
- Cause
 - “The trigger for this event was a network configuration change.”



IC4 Marslev incident - 2011

- Loss
 - Tens, maybe hundreds of millions DKK
- Description
 - On 14 November 2011 DSB stopped operations with all IC4 trains after an IC4 train overran a red stop signal at Marslev
- Cause
 - Slippery rails and “inefficient” braking system
 - See the “DTU report”



Ariane 5 Rocket Explosion - 1996

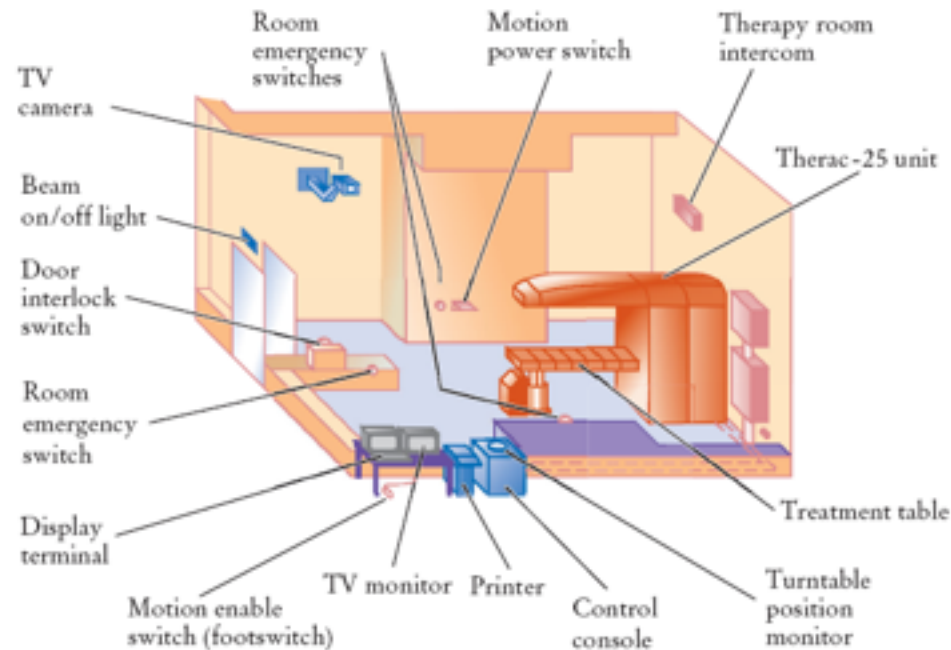
- Loss
 - rocket: \$500 million
 - project: \$7 billion
- Description
 - Intentionally destroyed 40 s after liftoff
- Cause
 - Variable overflow because of reuse of software module (from Ariane 4) related to horizontal velocity measurement.
 - This happened simultaneously in both the active and the back-up computer.



Therac-25

Radiation therapy machine - 1985

- Loss
 - 6 people injured
 - 3 dead
- Description
 - Severe overdose of X-Ray radiation
- Cause
 - Concurrency not properly tested, generating a race condition
 - Lack of hardware redundancy: hardware interlocks removed (replaced with software redundancy check)



Typical Therac-25 facility

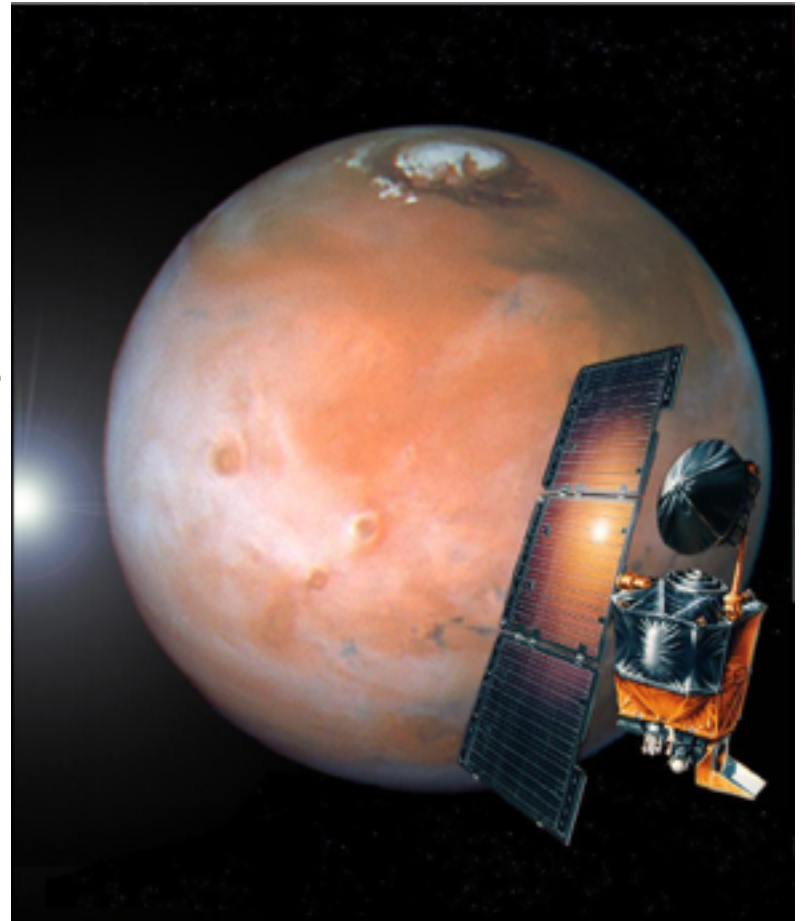
Patriot Missile System - 1991

- Loss
 - 28 soldiers dead
 - 100 injured
- Incident
 - The system failed to intercept an incoming missile
- Cause
 - Time is kept continuously by the system's internal clock in tenths of seconds but is expressed as an integer (e.g., 32, 33, 34...)
 - The Patriot battery had been up around 100 hours, resulting in a precision error of 0.34 seconds



Mars Climate Orbiter - 1998

- Loss
 - \$125 million
- Description
 - Spacecraft crashed on Mars falling too deep into its atmosphere
- Cause
 - Discrepancy in the usage of imperial units (pounds of force) and metric units (Newtons)



Infusion Pumps



“a medical device used to deliver fluids into a patient’s body in a controlled manner. There are many different types of infusion pumps, which are used for a variety of purposes and in a variety of environments.”



56,000 reports of adverse events associated with the use of infusion pumps, including numerous injuries and deaths (during 4 years).

Is new technology making our world riskier?

Risk: combination of the *likelihood* of an accident and the *severity* of the potential consequences.

- Industrialized society
 - **Appearance of new hazards:** atomic energy
 - **Increasing complexity:** component failures vs. interaction failures
 - **Increasing exposure:** larger planes, larger cities & factories
 - **Increasing amounts of energy:** higher energy sources
 - **Increasing automation of manual operations:** does not remove humans, redefines their roles (e.g., fighting the autopilot)
 - **Increasing centralization and scale:** larger plants, ships, planes
 - **Increasing pace of technological change:** not enough time to test