Famous Software Failures

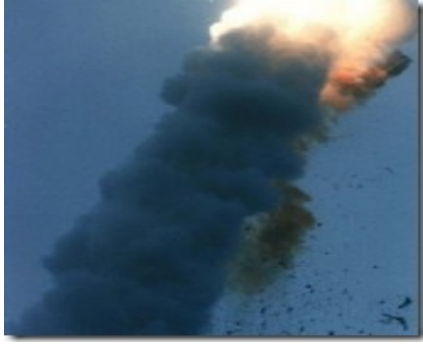
Ariane 5

- On June 4, 1996, the maiden flight of the European Ariane 5 launcher crashed about 40 seconds after takeoff. Media reports indicated that the amount lost was half a billion dollars -- uninsured.

- The CNES (French National Center for Space Studies) and the European Space Agency immediately appointed an international inquiry board, made of respected experts from major European countries, who produced their report in hardly more than a month

- It is a remarkably short, simple, clear and forceful document. Its conclusion: the explosion was the result of a software error -- possibly the costliest in history.

Software Failures



- **Ariane Rocket Goes Boom (1996)**
- **Cost:** €350 million
  - **Cause:** Shutdown occurred when the guidance computer tried to convert the sideways rocket velocity from 64-bits to a 16-bit format. The number was too big, and an overflow error resulted. When the guidance system shut down, control passed to an identical redundant unit, which also failed because it was running the same algorithm.

Ariane 5

- the error came from a piece of the software that was *not* needed during the crash. It has to do with the Inertial Reference System, (termed SRI in the report). Before lift-off certain computations are performed to align the SRI. It caused an exception, which was not caught after takeoff.

- There was no explicit exception handler to catch the exception, so it crashed the entire software, hence the on-board computers, hence the mission.

- It was a software reuse error. The SRI horizontal bias module was reused from a 10-year-old software: the software from Ariane 4.

F-16 Crossing the Equator

- An updated software in a F-16 was being tested by the US Air Force.
- When the plane flew across the equator (from the Northern Hemisphere to the Southern Hemisphere), the autopilot software inverted the plane.
- When the pilot righted the plane, the software informed him that he was flying upside down.
- When the pilot crossed back over the equator, everything returned to normal.

Therac-25

- The Therac-25 was a radiation therapy machine which caused massive radiation overdoses that resulted in the serious injury and death of patients.

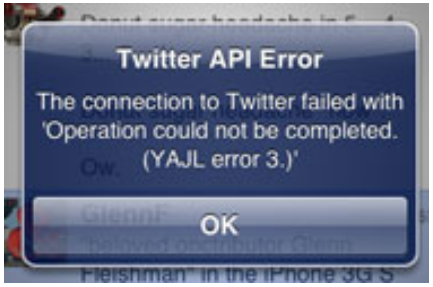
- Eleven Therac-25s were installed: five in the US and six in Canada. Six accidents involving massive overdoses to patients occurred between 1985 and 1987. The machine was recalled in 1987 for extensive design changes, including hardware safeguards against software errors.

Therac-25

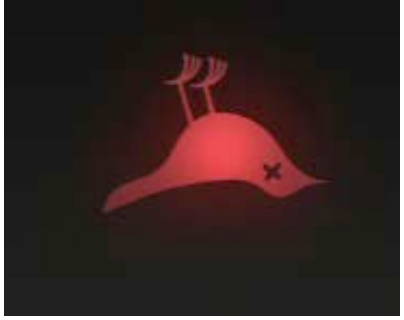
- the Therac-25 was designed with more attention on software interaction with the operator.

- In contrast to previous models, however, it was the software, not the hardware that was to provide the crucial safety precautions

- The overdoses have generally been attributed to the flaws in the software that would allow operators to override SW errors that would arise, many fatal to those patients being treated. The amount of the overdose was, more often than not, many times more than the recommended therapeutic dose that eventually culminated in severe trauma or death.



Twitpocalypse



- On June 12, 2009, in what was called a potential "Twitpocalypse", the unique identifier associated with each tweet exceeded the limit for 32-bit signed integers.
- The number of tweets exceeded 2,147,483,647
- While Twitter itself was not affected, some third-party clients found that they could no longer access recent tweets.
  - Iconfactory’s Twitterrific for iPhone stopped working immediately following the event

- **Y2K (1999)**
- **Cost:** €350 billion

  - **Disaster:** One man's disaster is another man's fortune, as demonstrated by the infamous Y2K bug. Businesses spent billions on programmers to fix a glitch in legacy software. While no significant computer failures occurred, preparation for the Y2K bug had a significant cost and time impact on all industries that use computer technology.
  - **Cause:** To save computer storage space, legacy software often stored the year for dates as two digit numbers, such as "99″ for 1999. The software also interpreted "00″ to mean 1900 rather than 2000, so when the year 2000 came along, bugs would result.

- **Mars Climate Orbiter (1998)**
- **Cost:** €100 million

  - **Disaster:** After a 286-day journey from Earth, the Mars Climate Orbiter fired its engines to push into orbit around Mars. The engines fired, but the spacecraft fell too far into the planet's atmosphere, causing it to crash on Mars.

  - **Cause:** The software that controlled the Orbiter thrusters used imperial units for force (pound-seconds), rather than metric units (Newton-seconds, defined in the Software Interface Specification (SIS)) for thrust instructions as specified by NASA and used in the software generating the instructions on the ground – ***a metric mixup***

- **Royal Bank of Scotland (2012)**
- **Cost:** €3.5 million/€56 million fine (Ireland/UK)
  - **Disaster:** A software update was applied on 19 June 2012 to RBS CA-7 software which controls the payment processing system. Customer wages, payments and other transactions were disrupted. Some customers were unable to withdraw cash using ATMs or see bank account details. Others faced fines for late payment of bills because the system could not process direct debits. It took until the 16th July before it was fixed.
  - **Cause:** The software upgrade was corrupted

RBS Software Upgrade Consequences

- People could not withdraw cash from the ATMs
- Bills could not be paid because direct debits could not be processed, furthermore, customers could face fines for not having bills paid on time
- Wages were not being paid into people's accounts
- Social welfare payments were not going through
- Completion of new home purchases were delayed
- others were stranded abroad
- A cancer charity was unable to transfer funds as arranged to a family whose daughter was on life support in a Mexican hospital and alternative arrangements had to be made with the bank for the transfer
- On Friday 22 June a man was granted bail at Canterbury Crown Court on condition a surety was to be paid before his release, but the computer failure prevented the transfer of his bail money, leading to him remaining in a remand cell over the weekend.

China Air Lines Flight 140

- On the night of April 26, 1994, China Air Lines flight 140 made its final approach to Nagoya, Japan. The weather over Nagoya was perfect, clear with light winds. The Airbus A300-600R was in top mechanical condition and had just been certified. The European built airliner was still very new in all aspects, having been added to the Taiwanese based air carrier only a few months before.

China Air Lines Flight 140

- As the airliner approached within feet of the runway it began to lurch back into the air, nosing up quickly as if it did not want to land. The pilot, an experienced flier, cursed as he fought with the jet, trying to force it back onto the runway. However, each time he pushed down to land, the jet bucked back into the air.

China Air Lines Flight 140

- Three times the pilot fought with the controls. Each time the modern airliner seemed to respond with a mind of its own, pulling up hard at the last second. On the third nose up maneuver the airliner lost almost all its speed. The Airbus hesitated for a moment, hanging motionless a thousand feet in the air over the runway, and then with a shuddering blast, crashed backwards onto the Nagoya airfield, killing all 231 aboard.

China Air Lines Flight 140

- What happened to CAL flight 140? According to information gathered by the flight data recorder, the pilot had placed the airliner into a computerized "touch and go" mode that forced the aircraft to pull up and away during landings. This maneuver is practiced by pilots, allowing the airliner to gently skip off the runway and back into the air.

China Air Lines Flight 140

- Unknowingly, the pilot attempted to override the computer by pushing the nose back down to land but never turned the computer off. In response to each landing attempt, the computer dutifully followed its preset program and pulled the jet back up. The pilot, determined to land the aircraft, engaged in a battle for control of the plane. The result was a classic computer "loop." Each time the pilot pushed the airliner down to land, the computer obediently pulled the jet back up to go around. On the third try the entire system, including the airliner, crashed.

Lufthansa Airbus Crash

- On Sept. 14, 1993, a Lufthansa Airbus A320-200 was landing in bad weather at Warsaw airport, Poland. The pilots had been warned of gusting cross winds, rain and possible wind shear conditions. In order to compensate for the bad weather problems the crew added 20 knots of speed to their landing approach and used a standard cross wind landing technique, keeping the right wing low and landing first on the right gear.

Lufthansa Airbus Crash

- However, because of the gusting winds and heavy rains, the wheels aquaplaned during the first nine seconds on the ground. The extra wind and water combined to fool the Airbus computer, indicating the big jet had not landed. The computer responded by disabling the aircraft braking systems. With no brakes, the Lufthansa jet skidded off the end of the Warsaw runway and struck a hill, killing the first officer, one passenger, and injuring 45 others. The A320 was totally destroyed in the crash.

Lufthansa Airbus Crash

- The crash report that followed indicated the flight crew followed the Airbus book on how to land the big jet in bad weather. Lufthansa, in response to the crash, changed the procedures against the advice of Airbus. No Lufthansa A320s have crashed since that change. Airbus, of course, insists there is no problem in their control software.

Other Examples

- In February 2003 the U.S. Treasury Department mailed 50,000 Social Security checks without a beneficiary name. A spokesperson said that the missing names were due to a software program maintenance error

- In July 2001 a “serious flaw” was found in off-the-shelf software that had long been used in systems for tracking U.S. nuclear materials. The software had recently been donated to another country and scientists in that country discovered the problem and told U.S. officials about it

Other Examples

- **Excel 2007:**
  - Ask people with calculators or slide rules to multiply 850 x 77.1, and they'll answer 65,535. But in September 2007, it was discovered that Excel 2007 answered 100,000.
  - **Cause:** According to Microsoft, this bizarre rounding-up occurred only in calculations that resulted in floating point numbers near 65,535 or 65,536 – but there was a *display-only* bug. What's more, Excel actually calculated the correct answer, but the bug prevented it from displaying properly.

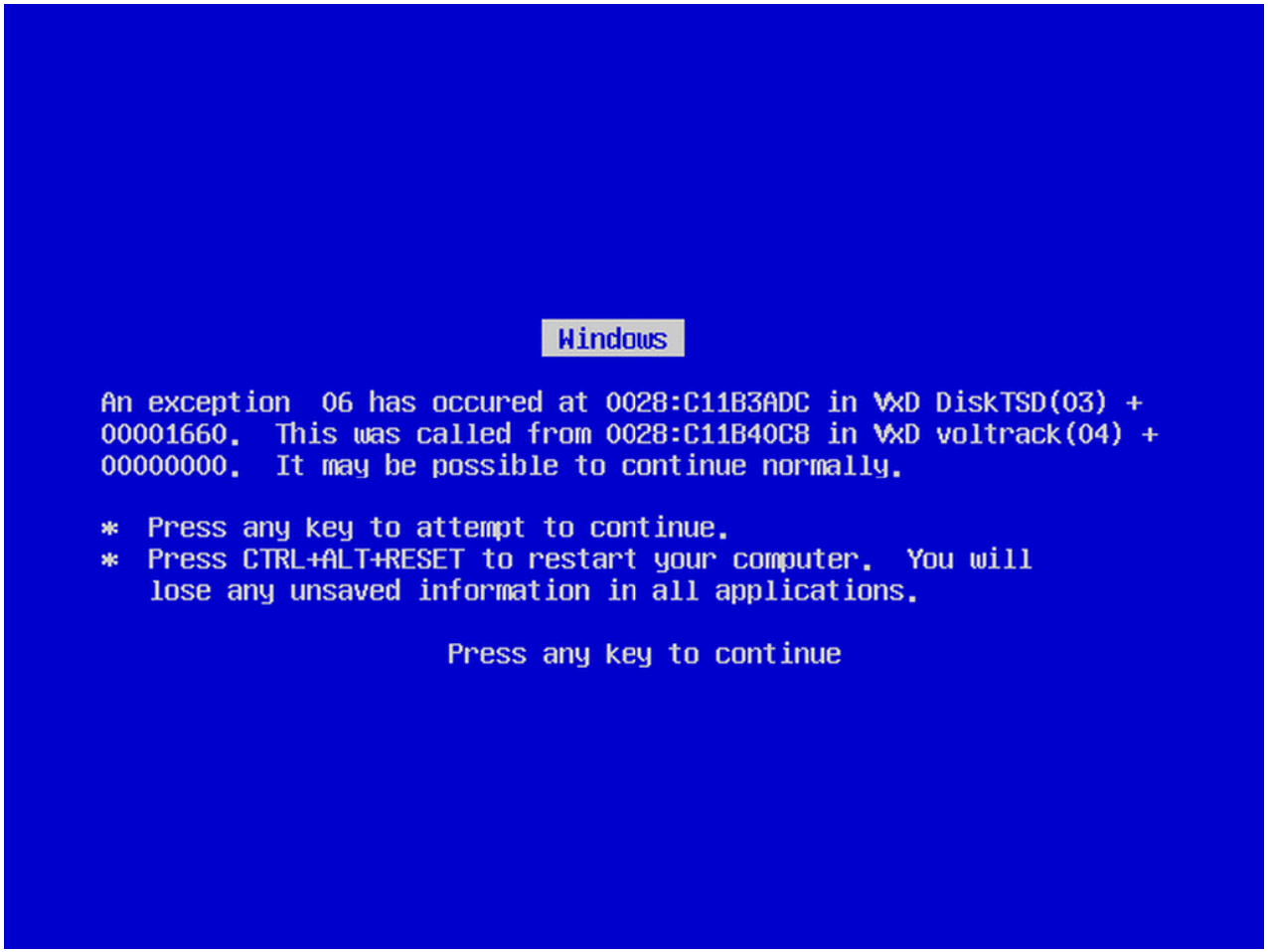
Interesting Quotes

- “If Microsoft made cars instead of computer programs, product-liability suits might now have driven them out of business.”

- if cars were like software, they would crash twice a day for no reason, and when you called for service, they’d tell you to reinstall the engine

- “Thank the programmer”, Airline pilot after a smooth landing

The BSOD


Windows
An exception 06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660. This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000. It may be possible to continue normally.
* Press any key to attempt to continue.
* Press CTRL+ALT+RESET to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue