Little Faults, Big Failures

Software bugs and project mismanagement

Prof. Thomas Huckle

22.04.2013
Critical Software
Bugs in the News I

• Delay in delivery of new ICE trains, (Nov. 2012)


The command for stopping the train „strays“ for nearly a second through the computer before it is conducted. For a speed of 250 km/h and full application of the break the stop therefore needs around 70 m more.
Bugs in the News II


The computer was not ready to accept the freak occurrence of successive throws of exactly the same distance and wiped out Heidler's fifth throw of 77.12 meters, which came after Russia's Tatyana Lysenko - who went on to take gold - had also thrown 77.12m.
Flash Crash last week

Sinking gold price provokes stockbrokers to modify their algo-trading codes to react more sensitive on sinking stock prices → 180 points drop of DAX in a few minutes. Risks of “high frequency trading”
Mars Rover Curiosity

Since late February, Curiosity's computing needs have been served by its B-side computer after a memory issue affecting the A-side computer prompted NASA engineers to 'flip' active computers.

On Sunday 16 March Curiosity went into a precautionary standby status after a "command file failed a size-check by the rover's protective software", allowing it to append an unrelated file which then caused a file size mismatch.

Curiosity initiated this automated fault-protection action, entering 'safe mode' at about 8 pm PDT (11 pm EDT) on March 16, while operating on the B-side computer, one of its two main computers that are redundant to each other. It did not switch to the A-side computer, which was restored last week and is available as a back-up if needed.
Murphy‘s Law

- Anything that can possibly go wrong, does.
- If there is a possibility of several things going wrong, the one that will cause the most damage will be the one to go wrong
- Enough research will tend to support whatever theory
- The light at the end of the tunnel is a train
- In any collection of data, the figure most obviously correct, beyond all need of checking, is the mistake.
Ariane 5  (4.6.1996)
Ariane 5

- 40 seconds after launch: Explosion
- Loss: ca. 500 million $ (€) for rocket and freight (4 satellites).
- Development expenses: ca. 7 billion $.
Cause of the crash

- Crash of the on-board computer 36.7 sec. after launch:
- Cast of 64 bit floating point number into 16 bit signed integer format in binary representation $\pm b_1 b_2 \ldots b_{15}$, $b_i \in \{0, 1\}$
- The related number was larger than $2^{15} = 32768$ and caused an overflow = register overflow.
- Collapse of the guiding system, flight getting unstable, and jet engines were breaking off.
- Self-destruction
• Origin of the software: Ariane 4, but the related number represented the horizontal speed. Ariane 5 was much faster!!!

• Software was superfluous during the flight, it was only useful for restart in case of countdown interruption

• Backup computer used the same code and crashed earlier!

• The cast was not protected!!! Nobody believed, that the horizontal speed would get so large!
I cannot solve problem two.

Choose "eleven" and don't bother.
I did the same.

"x" is usually 11 and "y" mostly 9

One thing I have already learned about Algebra:
Don't take it too serious.
Pentium Processor Bug (1994)

Example for the division error:

\[ x = 4195835.0 \]
\[ y = 3145727.0 \]

Compute \[ z = x - (x / y) \cdot y \]

Exact result: \[ z = 0 \]
With Intel Pentium: \[ z = 256 \]
Reason

- For Division Intel uses an implementation of the Radix-4 SRT algorithm:
  - Collect significant digits in divisor and dividend, resp. the remainder of the division
  - Search in lookup table for an estimate of the next digit in the quotient
  
  .....
Advantage: Gives 2 bit of the quotient per cycle.

Look-up table should have 1066 entries to cover all possible combinations.

Erroneously (possibly too short FOR-loop or damaged mask) it contained only 1061 entries and in this form it was used for manufacturing the chips.
MoR = 2/3 Measure of Redundancy

\([DVSR]_5\) 5 MSBs of divisor

\([rP]_7\) 7 MSBs of shifted partial remainder

+2D

5/3 D

+2D +1D

4/3 D

+1D

2/3 D

+1D 0D

1/3 D

0D

1/3 D

0000.000

1.0000 1.0001 1.0010 1.0011 1.0100 1.0101 1.0110 1.0111 1.1000 1.1001 1.1010 1.1011 1.1100 1.1101 1.1110 1.1111

Divisor

Shifted Partial Remainder (rP)
Impact of the bug

- Division error at fourth digit
- Occurrence of the error:
  - Once in 27000 years (Intel)
  - Once every 24 days (laut IBM)

Financial loss of Intel > 400 million dollar.
Patriot Missile (1991)
Irak War I (resp. II)
Patriot failure

• Febr. 25th 1991 the Patriot system missed an attacking Irakian Scud missile.
• The Scud missile hit an American barrack in Saudi Arabia killing 28 American soldiers.
Reason

• The internal clock of the control unit uses time in one-tenth of a second
• The control program is based on seconds
• Conversion by dividing by 10
• Implementation of this conversion by multiplying with 0.1, but in binary form with finite number of bits!!!
Error Analysis

\[
\frac{1}{10} = 2^{-4} + 2^{-5} + 2^{-8} + 2^{-9} + 2^{-12} + 2^{-13} + ... 
\]

As binary fixed-point number with 24 bit:

\[
\frac{1}{10} \approx (0.00011001100110011001100)_{2}
\]

Obvious round-off error:

\[
2^{-25} + 2^{-26} + ... \approx 0.000000095 = 9.5 \cdot 10^{-8}
\]
Impact of the rounding error:

- After 100 operating hours there results a difference between actual and computed time of
  \[(9.5 \cdot 10^{-8}) \cdot 3.6 \cdot 10^6 \text{s} = 0.34 \text{s}\]

- Scud speed: 1.676km/s=6034km/h, hence the Scud-missile covers in 0.34 seconds a distance of around 0.57 km and resides already outside the range of the tracking system of the Patriot!

- Real story: Patriots mostly hit only the stern of the Scud resulting in increased damage on the ground by the patriot missiles and the parts of the attacking Scud (including the warhead)

- Compare SDI!
National Missile Defense program

Decoys | Warhead

X-band radar
(Accurate tracking)
National Missile Defense program

Decoys  Warhead

Kill vehicle (Hit-to-kill)

Command center
SDI Difficulty:

Is it possible to bring down an attacking nuclear intercontinental missile safety by a computerized defense system?

- time frame
- multiple warheads, mock-ups, second rocket stage
- precision (hit the nuclear warhead!)
- decision fully computerized or manually?
- length of code ↔ error-proneness
- test only in the case of emergency?
Friendly Fire

Irak war: Shooting of a british airplane, April 2003
Falkland war 1982: Sinking of the Sheffield by an Argentine Exocet with Nato identification.
The Boomerang

There once was a boomerang
That was a little bit too long.

The boomerang flew somewhat
But it didn't come back.

The public, for hours long,
Waited for that boomerang.

J. Ringelnatz
“One mile is 1609 meter, and ignoring 9 meter therefore the conversion is 5:8.
The unit for fluid is american gallon (3.785 Liter), which correlates roughly like 1:4.
The mileage of a car in USA is given as miles per gallon, and transforming this to Kilometer pro Liter requires some luck.”

“...The tire pressure is given in pounds per square inch, and each attempt to relate this to Atmosphären is in my opinion a waste of effort.”

Paul Watzlawick in Gebrauchsanweisung für Amerika Directions for USA
Mars Climate Orbiter (1999)
Mars Climate Orbiter

Launch: 11.12.1998

Goal: - reach orbit
    - map the surface
    - establish relay station for *Mars Polar Lander*

Crash 23.9.1999 approaching Mars orbit
Reason:

Use of different measuring units:

Lockheed delivered device, specifying the force in 'Pound(-force)'

NASA (resp. Jet Propulsion Lab in Pasadena) had commissioned a device using 'Newton'.

'Imperial' versus 'metric' units!
Soliloquy of a Snail

Shall I dwell in my shell?
Shall I not dwell in my shell?
Dwell in shell?
Rather not dwell?
Shall I not dwell?
Shall I dwell,
dwell in shell,
shall I shell,
shallIshhIsallIshellIshallI...?

Christian Morgenstern
Sojourner (1997)
Sojourner Error

Mars rover Pathfinder successfully explored the Mars surface (1997) -

except for a tiny bug:

The airborne computer sometimes restarted without apparent cause, incl. loss of data and time.
Bus for data exchange between different modules:

- Highest priority: (H) Bus management (often)
- Medium priority: (M) communication task, sending collected data to the ground control (long reigning)
- Low priorität: (L) recording of meteorological data; (L) only brief, therefore it is allowed to block (H) (but not (M))!
Mars Rover Spirit Bug (January 2004)

Flash Memory formatted in FAT format (File Allocation Table).
Changes in the file system result in an update of the allocation table:

Write table in main memory, do the changes, and write new table back into memory.

Bug:

The table is getting longer and longer because deleted data are marked by a flag in the table!

At arrival on the mars the file system was so big that the table didn’t fit in the RAM memory.

→ Repeated rebooting until battery was nearly empty.
Light

people believe
reft and light
cannot be
mixed up.

what an ellol.

E. Jandl
Various Money Bugs:

- Wall Street crash 19.10.1987
- US Federal Reserve System (Zentralbank): Erroneous money transfer of 28 billion $ conducted by new computer system; back transfer of only 24 billion $!
- Vancouver stock exchange: round-off errors
- High frequency trading
- Algorithmic trading
- Mathematical finance (discontinuous, parameter, right predictions)
Jeopardy:

By erroneous allocation it could happen, that the treatment starts with strong electron beam **without** metal foil!

Electron modus                       X-ray modus
A special example out of a long list of bugs:

1 byte variable C used as counter for the number of faulty manual inputs.

\[ C = 0: \] Everything is correct: Start treatment.

First wrong input: \[ C = (00000001)_2 \]

Second wrong input: \[ C = (00000010)_2 \]

…..

After 256 wrong inputs C gets

\[ 256 = (1|00000000)_2 \Rightarrow (00000000)_2 = 0 \]

and the radiation treatment is applied in spite of erroneous and dangerous alignment!
By wrong display and keyboard implementation it could happen, that subsequent corrections of wrong entries could appear on the screen but were not accomplished:

<table>
<thead>
<tr>
<th>PATIENT NAME</th>
<th>TEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>TREATMENT MODE</td>
<td>FIX</td>
</tr>
<tr>
<td>BEAM TYPE: X</td>
<td>ENERGY (MeV): 25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNIT RATE/MINUTE</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITOR UNITS</td>
<td>0</td>
<td>200</td>
</tr>
<tr>
<td>TIME (MIN)</td>
<td>0.27</td>
<td>1.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GANTRY ROTATION (DEG)</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COLLIMATOR ROTATION (DEG)</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>359.2</td>
<td>359</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COLLIMATOR X (CM)</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14.2</td>
<td>14.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COLLIMATOR Y (CM)</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>27.2</td>
<td>27.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WEDGE NUMBER</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACCESSORY NUMBER</th>
<th>ACTUAL</th>
<th>PRESCRIBED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATE</th>
<th>84-OCT-26</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>12:55:8</td>
</tr>
<tr>
<td>OPR ID</td>
<td>T25V02-R03</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>BEAM READY</td>
</tr>
<tr>
<td>OP. MODE</td>
<td>TREAT AUTO</td>
</tr>
<tr>
<td>TREAT</td>
<td>TREAT PAUSE</td>
</tr>
<tr>
<td>X-RAY</td>
<td>173777</td>
</tr>
<tr>
<td>COMMAND:</td>
<td></td>
</tr>
</tbody>
</table>
A number of patients were seriously harmed. Some died after the treatment.

The code was written by one single software developer without comments or meaningful error messages.

Computer euphoria 1980: Software can not fail!
Airport Baggage Transport
Denver International Airport 1993-95
Transport by carts
Dynamic Loading

- Barcode Reader
- Array
- Conveyor
- RF/ID tag
- Baggage cart
- RF/ID reader
Design:

- 300 PC (486) in 8 control rooms
- Raima Corp. Data base on Netframe NF250 Server
- High-Speed glass fiber net
- 14 million feet cable
- 56 laser units (Bar Code reader)
- 400 frequency reader
- 22 miles tracks, 6 miles conveyor
- 3100 standard carts and 450 oversize carts, radio-controlled
- 60 „Destination Coded Vehicles“ (DCV) per minute/track
- 10000 engines and 92 PLC‘s (Programmable Logic Controller) for controlling engines and switches
Bugs:

- narrow curves in tunnel → derailing and damages
- problems with head wind
- faulty locks at carts
- badly printed labels
- adjustment of Barcode scanner
- contamination of photocell
- bumper interfere with photocells
- power blackouts
Reason:

- Combination of different programming languages
- Faulty timing of carts and loading canons
- Faulty timing for release of printed labels
- Difficult debugging: Trial & Error, no radio in tunnel
- Components were working under maximal loading
- **Complexity of the control problem growing exponentially:**
  - Line Balancing: Controlling the carts such that
    - there are no overstrained conveyors and
    - there is no need of a lot of empty carts on the tracks
    - every cart reaches the right gate as fast as possible
Solution
by German company Logplan:
Reduce baggage transport to small part of the airport.
Meanwhile this system has been totally removed

Compare Heathrow T5 (2008):
- Testing with private baggage or confusing with proper flights
- Distribution of lost suitcases to other countries for sorting

Is this your luggage by Luna Laboo:
http://www.isthisyourluggage.com/lost_luggage/LANDING.html
Delay of large-scale Projects

Toll collect
Airbus 380 wiring
Gesundheitskarte (health insurance card)
Digital radio communication for the police
Berlin airport
Railway station Stuttgart 21
Elbphilharmonie Hamburg
…
Nedelin Disaster

1960 for the anniversary of the October revolution a new missile R-16 should be launched. General Nedelin pushed the project pressed for time.

Explosion caused by wrong use of a rotary switch:

„Before launch – Manual Ignition – After Launch“
Winter storm Lothar, Xmas 1999

Wrong weather prediction by DWD. Outcome: 100 dead and nearly 6 billion € damage. Reason: data assimilation for deriving initial weather data. Ill-conditioned, prediction)

‘Im Fall "Lothar" versagte aber nicht etwa das GME-Modell an sich, sondern die Datenassimilation zur Initialisierung des GME. Es kursieren Gerüchte, wonach einige Messdaten, für Messfehler gehalten, gestrichen wurden oder anderen Messungen nicht die richtige Zeit zugeordnet wurde. Solche vermeintlich kleine Vergehen könnten sich gravierend auswirken im komplexen Gebilde Wettervorhersage.’
• USS Yorktown: Division by 0, 1998
• Atomic attack alarm in Russia, 1983
• 180 degree bugs (torpedo, F16, missile)
• Railway control center in Altona,
• Downing of Iranian airbus, 1988
• Überlingen, TCAS (traffic collision avoiding system)
• Qantas, Air France (ADIRU-altimeter)
Airbus reverse thrust, Warshaw, 1993
Airbus Fly-by-wire

A320, Airshow in Habsheim, Mulhouse, 1988

The pilot tells the computer that he wants to climb but the software decides! Delay or blocking!
- Paper retractions
- Ozone hole: Analysing output data
- EXCEL rounding
- Heisenbug, Lance Armstrong bug
- Space Shuttle, first start: synchronization
- Airbag: deactivating
- Bridge over Rhein, train tracks

Switzerland Germany

Railway track removal

Altitude above sea level

Removing the right track
Nuclear Disaster

- Windscale, 1957
- Majak, Kyschtym, Ural, 1957
- Harrisburg, Three Mile Island, 1979
- Chernobyl, 1986
- Fukushima, 2011

\[ E(\text{damage}) = \text{damage} \times \text{number}_F \times \text{prob}_F \]
You have mounted the mirror arse about face
Classical „Bugs“
Meidum Pyramid and Dahschur bent pyramid
Firth-of-Tay Bridge, Scotland, 1879
Tacoma Bridge (1940)

DISASTER! The Greatest Camera Scoop of all time!
London Millenium Bridge (2000)
London Millenium Bridge
Suspension bridge

Shutdown on third day because of wobbling.
Test runs
Sailor’s walk - swagger
Loss of Oil Rig Sleipner (1991)

Simulation by FEM code: underestimation of the effective shear forces by 47%
Software Bugs

• According to INTEL: 80-90 bugs in Pentium and in all other processors

• Normal Software: 25 bugs per 1000 lines of code.
• Good Software: 2-3 bugs per 1000 lines.
• Space Shuttle Software: less than 1 bug per 10000 lines (acc. to NASA)
• Mobile phone:
  200 000 lines of code → ca. 500 bugs
• Space Shuttle Software:
  3 mill. lines → ca. 300 bugs
• Windows 2000:
  27 mill. lines → ca. 50 000 bugs
• SDI (missile defense, USA):
  25-100 mill. lines → 10 000 bugs

Banana software:
Let the software ripe at the customer!

It´s not a bug, it´s a feature!

Quelle: Ingolf Giese, GSI Darmstadt
Personally I believe, it's the chemicals in the food
Reasons of Software Bugs

- Obvious errors (typo~ , design~ )
- Lack of safety checks (unexpected cases: division by 0, casts,. )
- Interface~ (different code doesn’t fit together)
- Misinterpretation of input/output data
- Untested recycling of old code
- Software and Hardware do not fit together (anymore)
- Progress in computer technology to fast
- Numerical round-off errors
- Insufficient testing
- Large-scale projects, gigantismus, complexity
- Underestimation of the task
Softwarebug at the „Bundesagentur für Arbeit“

Many Unemployed have to wait for their money
Wrong bank account numbers for transferring unemployment benefits

Berlin.- Kurz vor Inkrafttreten der Arbeitsmarktreform ist bei der Bundesagentur für Arbeit eine schwere Computerpanne aufgetreten……
Der Programmierfehler führte dazu, dass das Computerprogramm in den Überweisungsformularen für das Arbeitslosengeld leere Felder anstatt am Anfang am Ende der Kontonummern automatisch mit Nullen auffüllte. …..

(10-digit mask for bank account numbers
Sometimes also 9-digit numbers have to be inserted and extended to 10 digits by 0: Left-aligned with additional 0 on the rightmost position instead of right-aligned!)
• Leap second ➔ crash (July 2012)

On Saturday, at midnight Greenwich Mean Time, as June turned into July, the Earth’s official time keepers held their clocks back by a single second in order to keep them in sync with the planet’s daily rotation, and according to reports from across the web, some of the net’s fundamental software platforms — including the Linux operating system and the Java application platform — were unable to cope with the extra second.
Crash of CryoSat, 2005

ESA mission: Measure the thickness of the ice cap.

Launch with Russian SS19 intercontinental ballistic missile, October, 8th 2005: “... the second stage performed nominally until main engine cut-off was to occur. Due to a missing command from the onboard flight control system the main engine continued to operate until depletion of the remaining fuel. As a consequence the separation of the second stage did not occur. Thus, the combined stack of the two stages and the CryoSat satellite fell into the nominal drop zone north of Greenland...