Automatic Verification — Model Checking

Sérgio Campos
Edmund Clarke, Ken McMillan

What are we going to talk about ?

- Motivation — Is it important ?
- Formal methods
  - Temporal Logic Model Checking and CTL
- Compositional Reasoning
- Examples
  - VoD server
  - Systems biology

Automatic Verification — Model Checking

Why ?

Imagine the implementation of a complex hardware or software system:

- A 100K gate ASIC perhaps 100 concurrent modules;
- A flight control system dozens of concurrent processes in multiple CPUs.

Under test the system fails approximately every 3 days.

- Failures is not repeatable – race conditions;
- Internal signals are hard to watch;
- Too much data;
- Heisenbug.

The reason could be:

- x and y happen simultaneously every 10^{10} times
- Assumed mutual exclusion.

Automatic Verification — Model Checking

A trivial example:

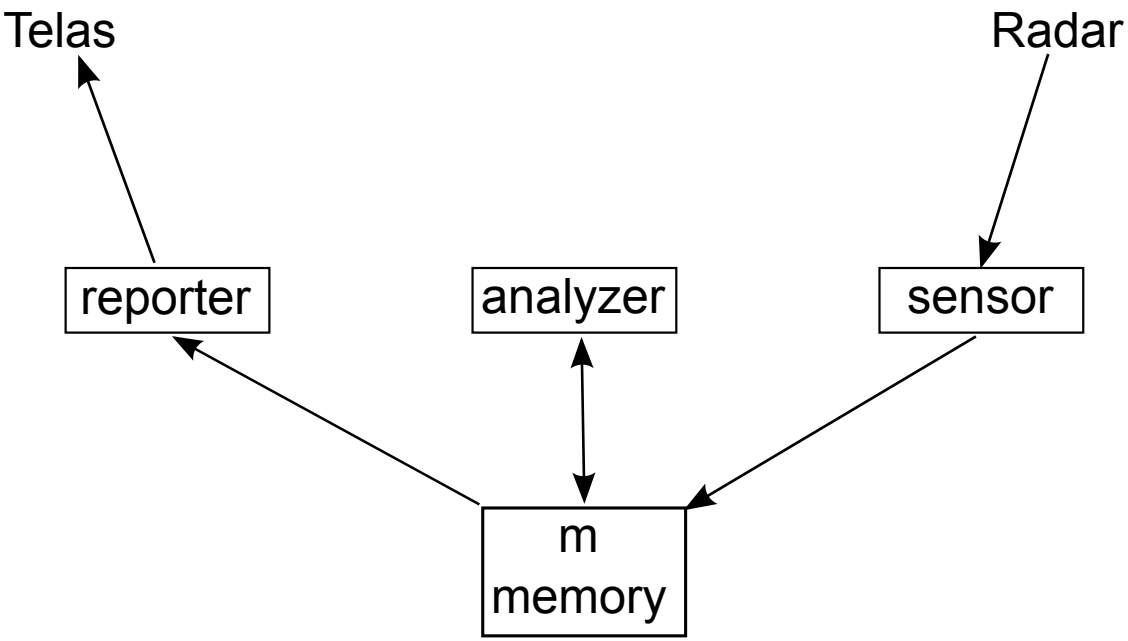
Process A	Process B
`...`	`...`
`x++;`	`x--;`
`...`	`...`

These errors can be prevented by good practice: semaphores, monitors, etc.

But other errors can be more subtle...

Priority Inversion

Consider a air traffic control system:



Processes communicate using shared memory.

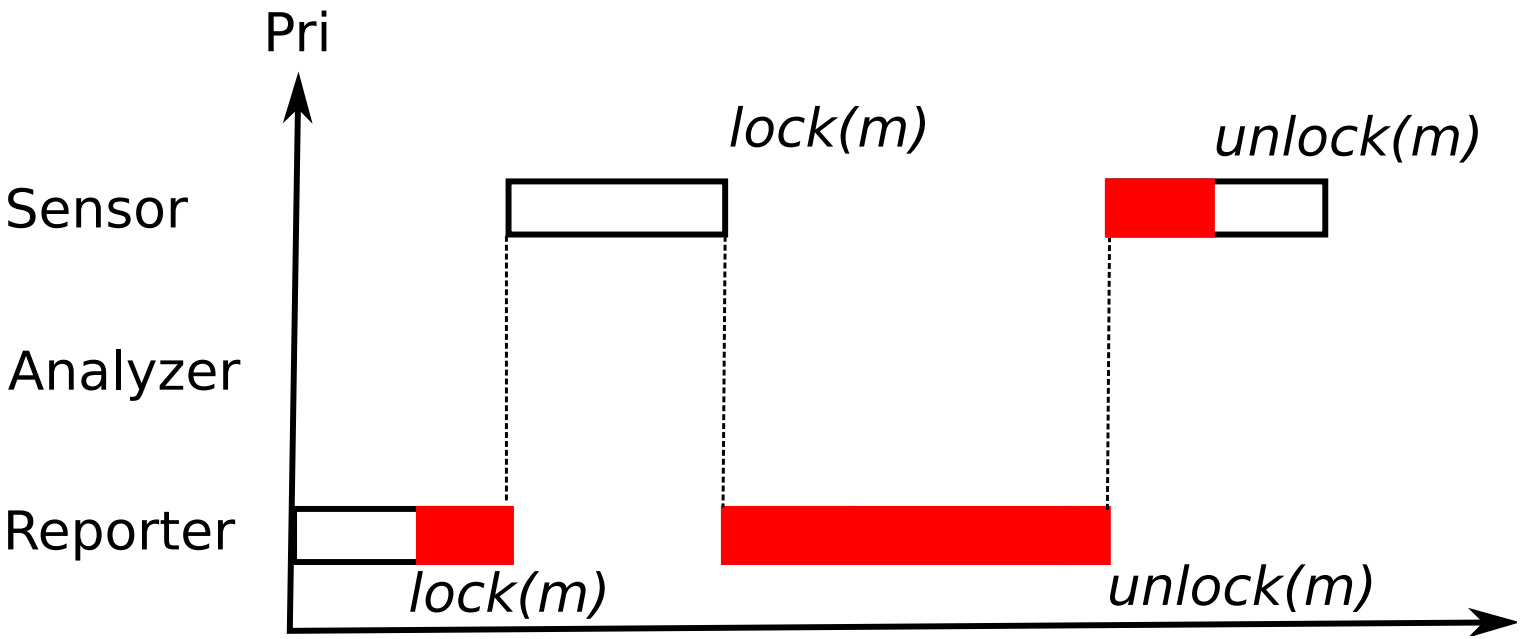
Priority order:

- Sensor (most important);
- Analyzer;
- Reporter;

Priority Inversion

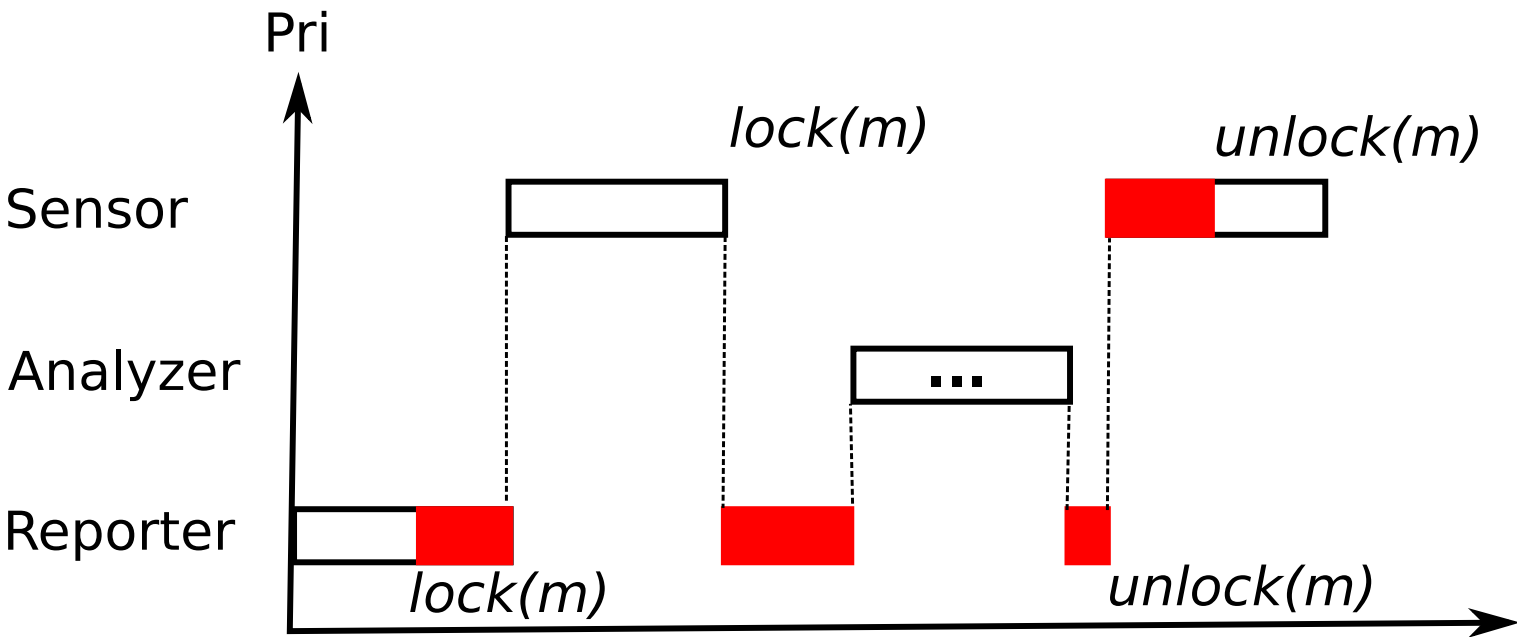
Sensor may never be blocked!

But the events below cause priority inversion:



Priority Inversion

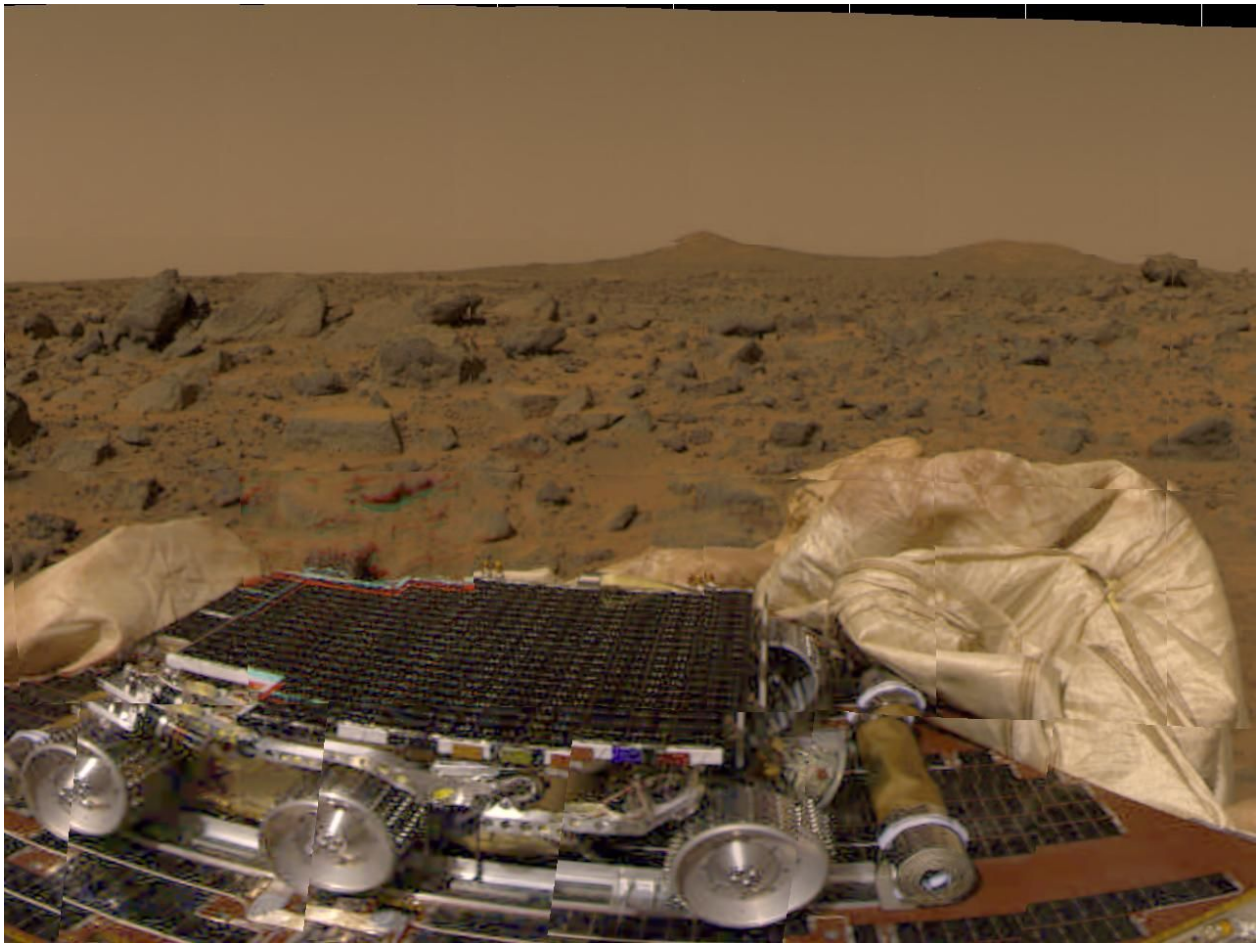
What if the Analyzer decides to run ?



The Analyzer does not see Sensor, and blocks Reporter *indefinitely*!

Priority Inversion

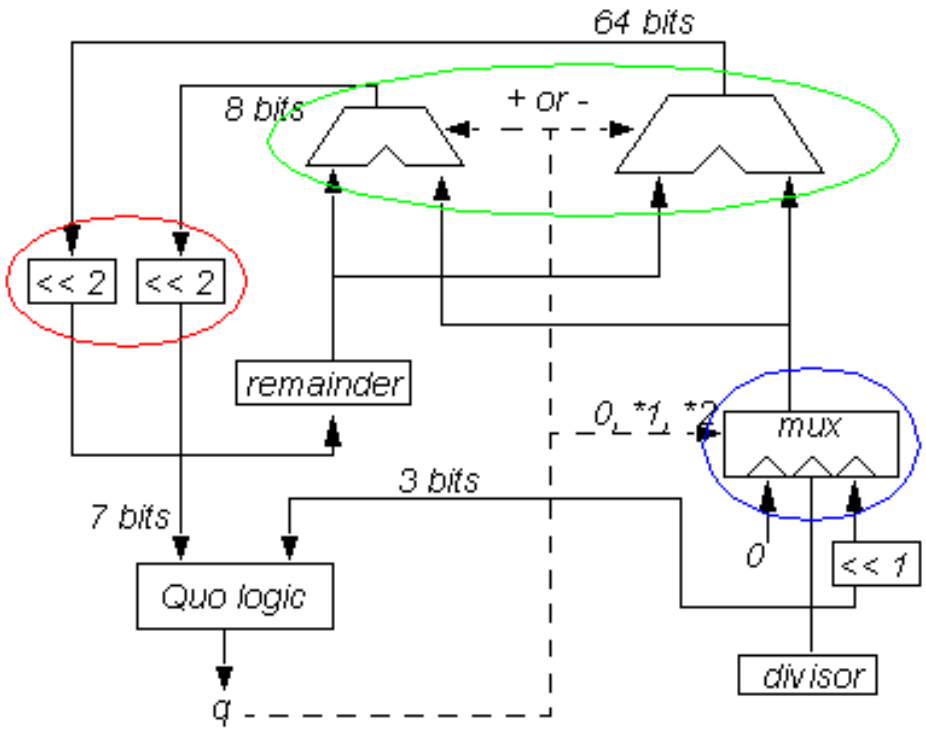
It happened! In Mars!!!
NASA Pathfinder, 1997:



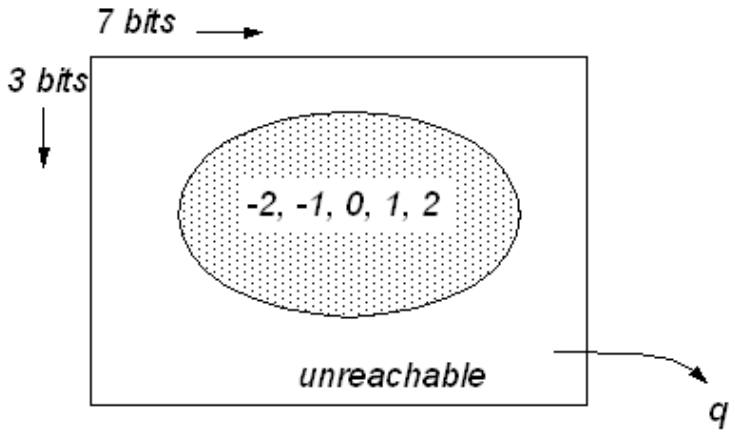
Pentium FDIV Bug

Pentium FDIV: SRT Division Circuit

- $P_0 = dividend/r$
- $P_{j+1} = r * P_j - q_{j+1} * divisor$
- $Q_{j+1} = r * Qj + q_{j+1}$



SRT Division Circuit



Quotient Logic:
Table was compressed to remove unreachable entries.

- reachable entries were considered unreachable and removed!

This caused an error only for operands that try to use those entries.

- Rare, but it sure happens!
- And it cost them US$500M!

We are Pentium of the Borg

Division is futile, you will be approximated...

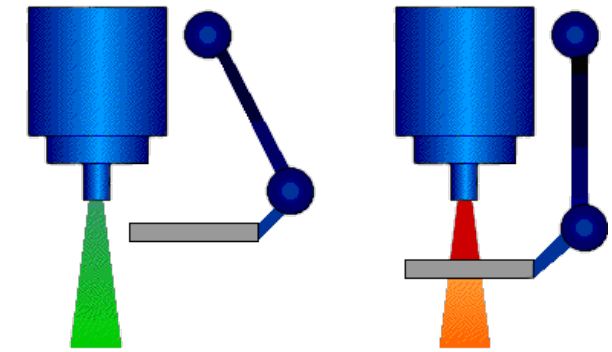
TOP TEN NEW INTEL SLOGANS FOR THE PENTIUM

- 9.9999973251 It's a FLAW, Dammit, not a Bug
- 8.9999163362 It's Close Enough, We Say So
- 7.9999414610 Nearly 300 Correct Opcodes
- 6.9999831538 You Don't Need to Know What's Inside
- 5.9999835137 Redefining the PC–and Math As Well
- 4.9999999021 We Fixed It, Really
- 3.9998245917 Division Considered Harmful
- 2.9991523619 Why Do You Think They Call It *Floating* Point?
- 1.9999103517 We're Looking for a Few Good Flaws
- 0.9999999998 The Errata Inside

Therac 25 Radiotherapy

Between 1985 and 1986 the Therac 25 radiotherapy machine *massively overdosed 6 patients* causing 2 deaths and worsening the other patients conditions severely.

Two modes of operation:

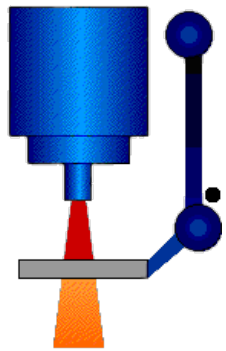


- After entering patients data, it is possible to edit this data.
- In some cases this causes a change in mode of operation, from x-ray to electron mode.

Therac 25

Error caused by:

- Race conditions in accessing shared variables.
- No hardware interlock: in this case, a pin holding the filter in place.



X-Ray Mode

The previous machine *had* a hardware interlock, but it was removed from the Therac 25!

- They used the same software, and they considered the software correct!

Ariane 5

- In June 4, 1996, the Ariane 5 rocket was launched for its first flight test
- 37 seconds after, it veered off its trajectory and was self-destructed.

The error:

- Software reused from Ariane 4
- But the previous rocket was much less powerful
- Navigation software detected a much stronger change in course than expected
- And the software that handled it *overflowed!!!*.

Ariane 5

One of the most expensive bugs in history:

- 10 years development
- at the cost of US$7.000.000.000,00 (7 billion!!!)