



CAN WE BUILD SOFTWARE THAT NEVER EVER CRASHES?

MARJAN SIRJANI, ASSOCIATE PROFESSOR
SCHOOL OF COMPUTER SCIENCE | RU LECTURE MARATHON

- Does software crash?
- Why? Why so often?
- What do we do about it?

Windows

An exception 06 has occurred 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

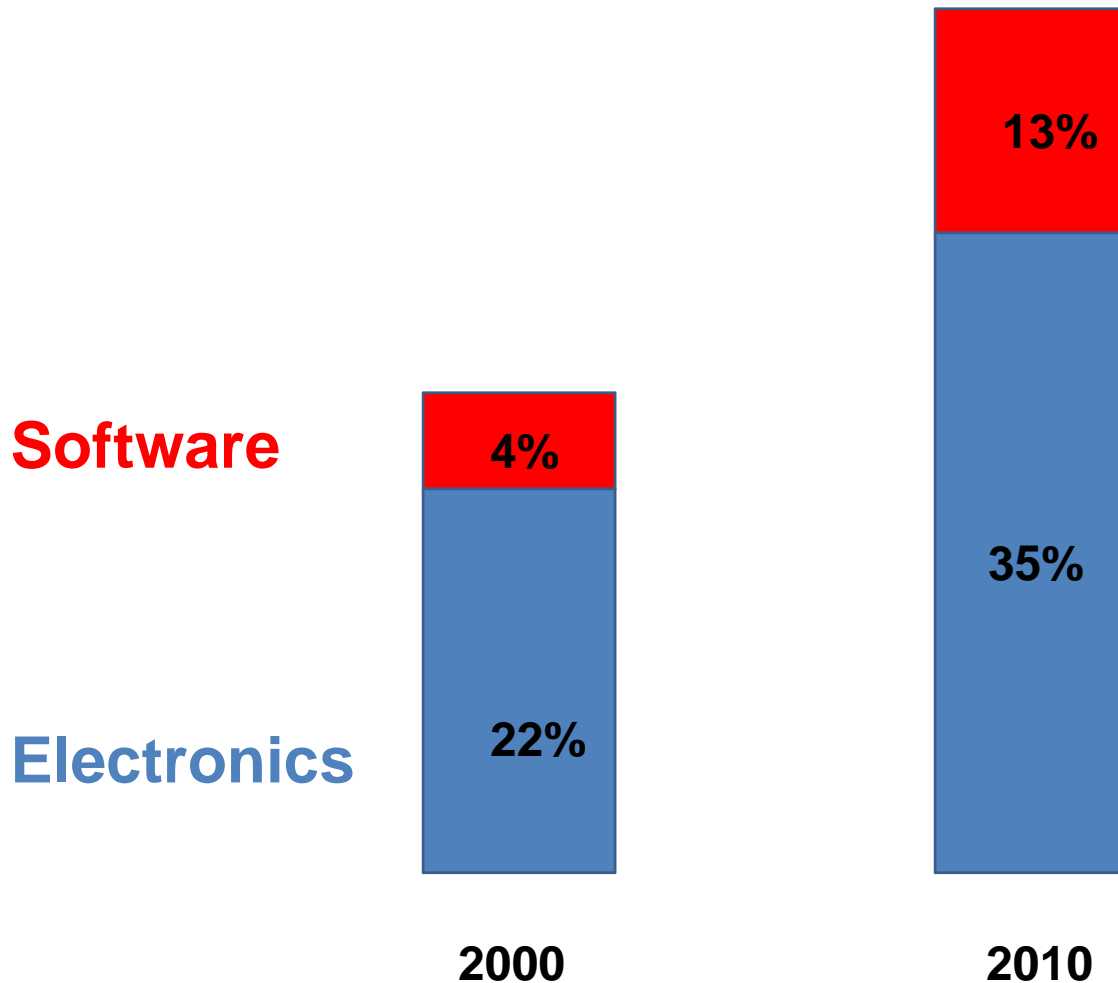


June 4, 1996

The European Ariane5 rocket explodes 40sec after launch, due to a software bug.



Production Cost of Automobiles



[MIT Tech Review]

- December 4, 2006
- The NHTSA said DaimlerChrysler is recalling 128,000 Pacifica sports utility vehicles because of a problem with the software governing the fuel pump and power train control. The defect could cause the engine to stall unexpectedly.
[Washington Post]

It's the Software!!

The value is in the software:

Microsoft is one of the three most valuable companies in the world.

The bugs are in the software:

What is more likely to crash: your modem or your browser?

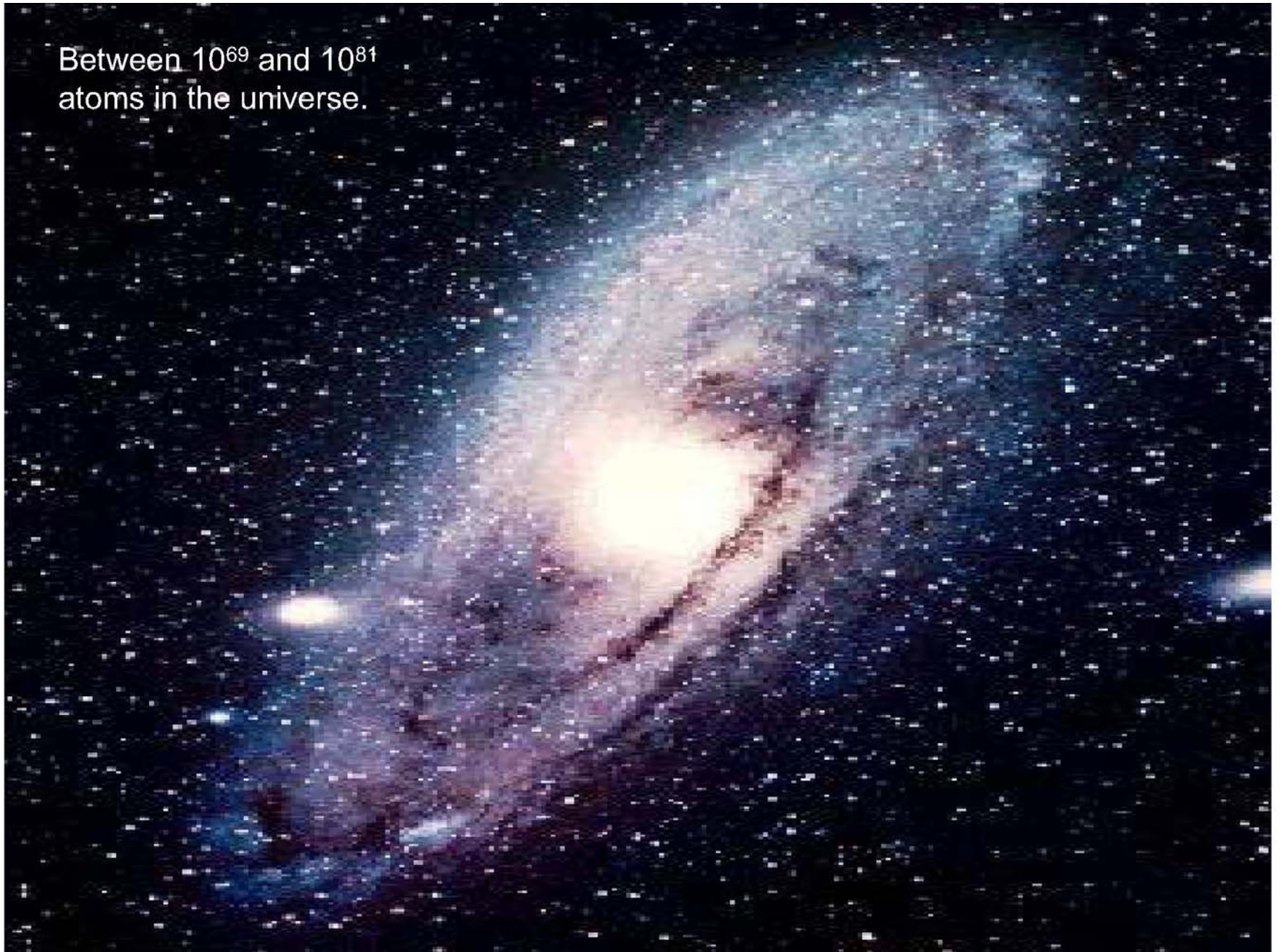
The challenges are in the software:


Is it that no smart people go into software engineering, or is building software really *that difficult*?

Software truly is the most complex artifact we build routinely. It's not surprising we rarely get it right.

Tom Henzinger, 2006

Between 10^{69} and 10^{81}
atoms in the universe.



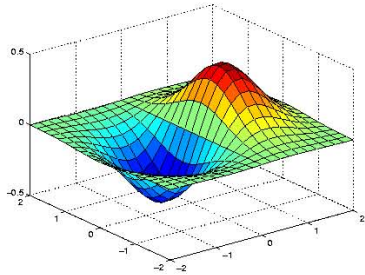


Between 10^{69} and 10^{81}
atoms in the universe.



10 MB cache >
 $10^{20,000,000}$ states.

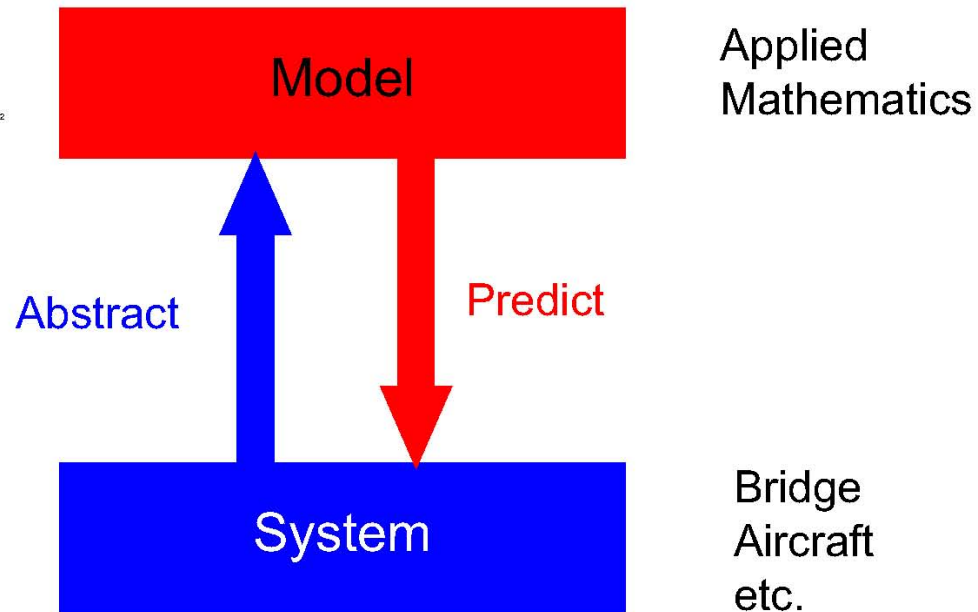
Complexity Management in Engineering



Calculate



Build & test



Mathematical Modeling: A Tale of Two Cultures

Engineering

Computer Science

Differential Equations

Linear Algebra

Probability Theory

Mathematical Logic

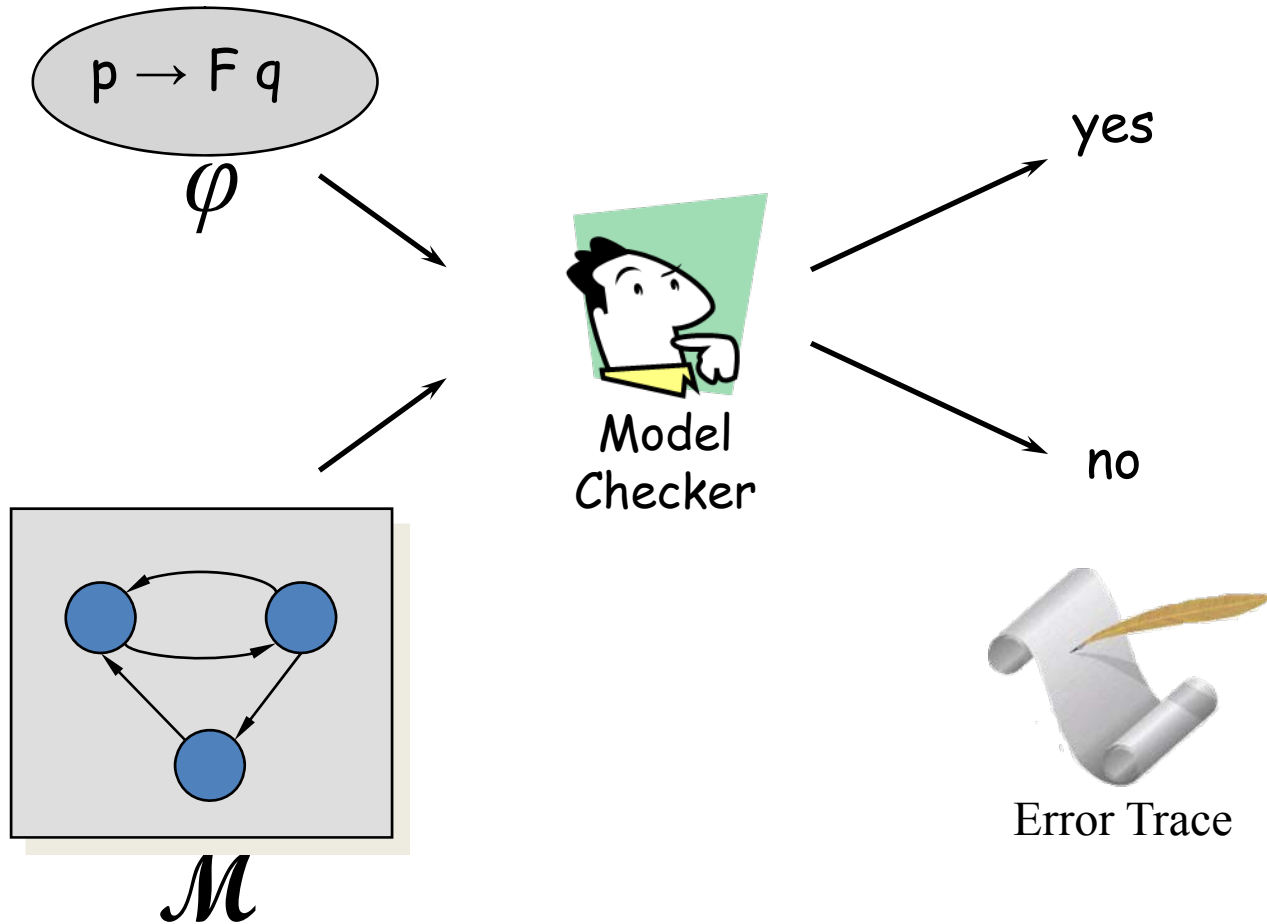
Discrete Structures

Automata Theory

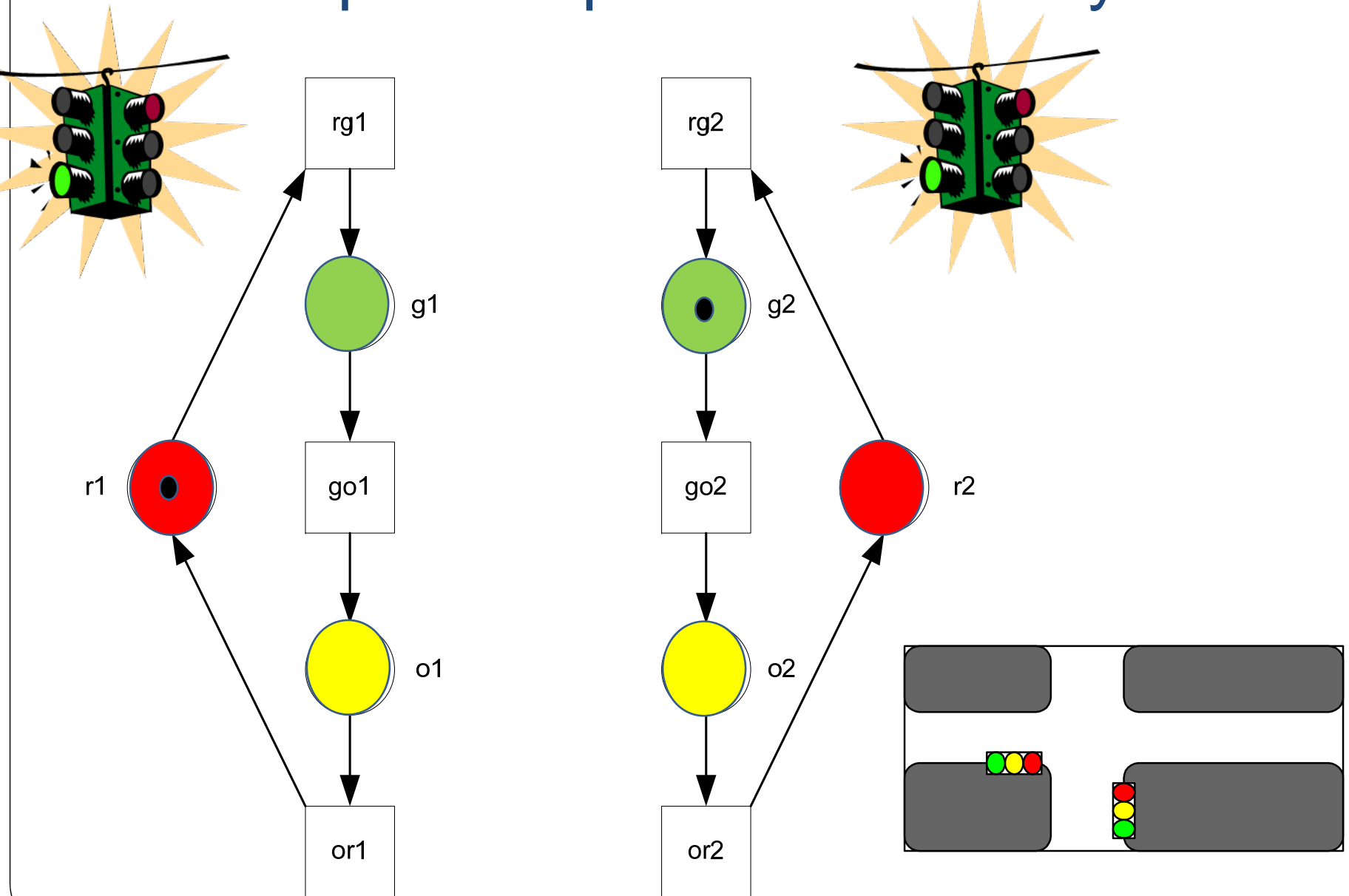
Our methodology in building software

- **Model Building: capture relevant aspects of the system formally (using logic and automata)**
- **Model Checking: implement algorithms for model analysis** [Clarke/Emerson; Queille/Sifakis1981]

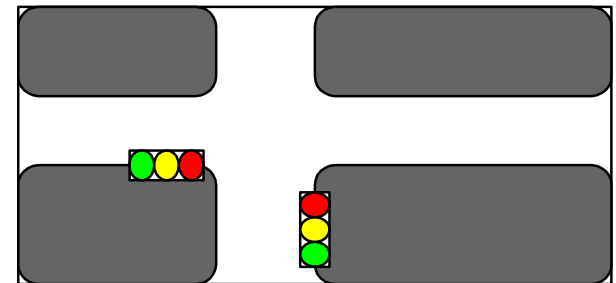
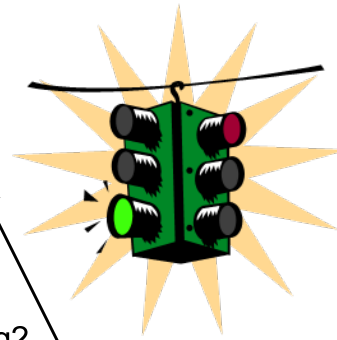
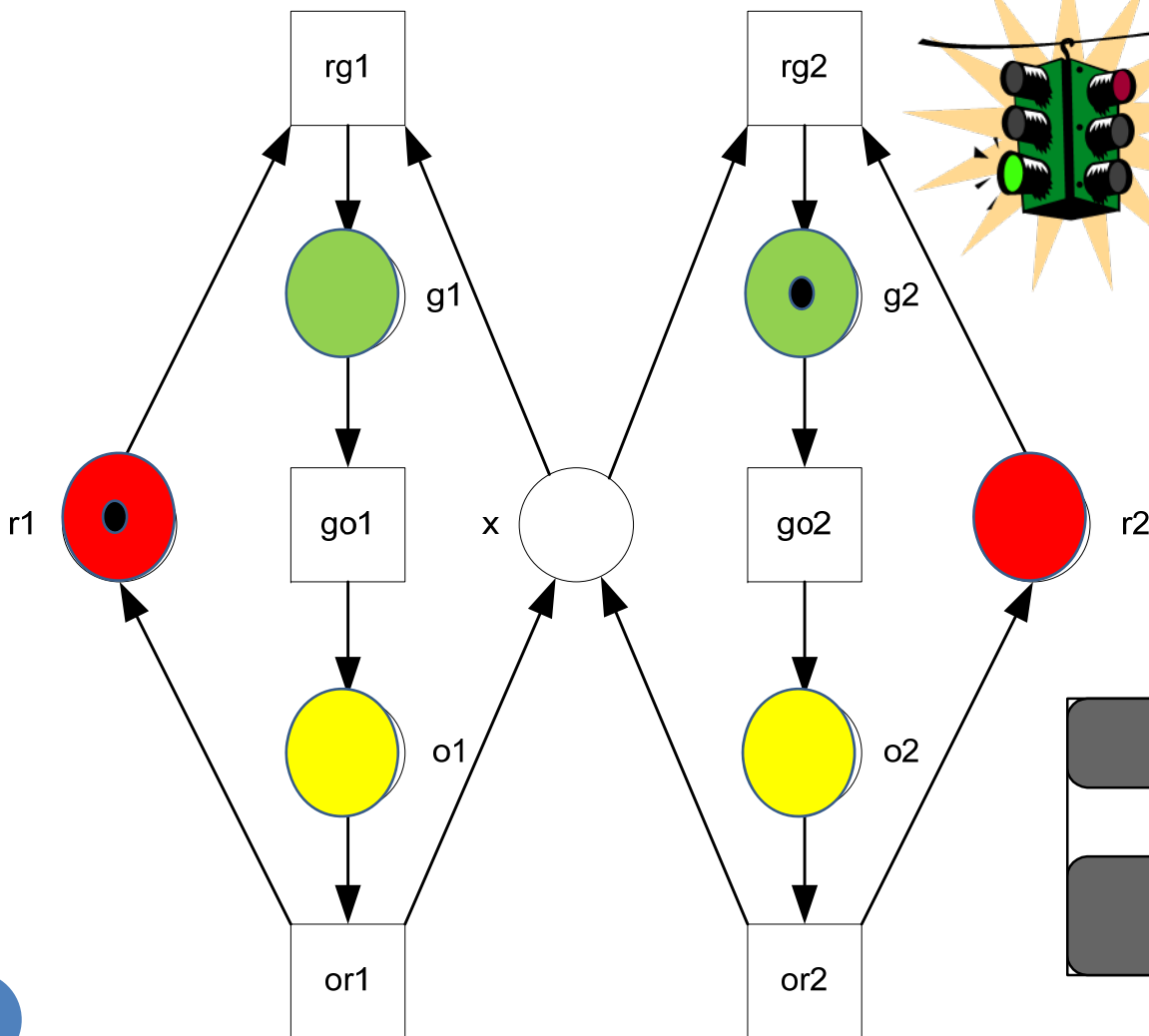
Model checker



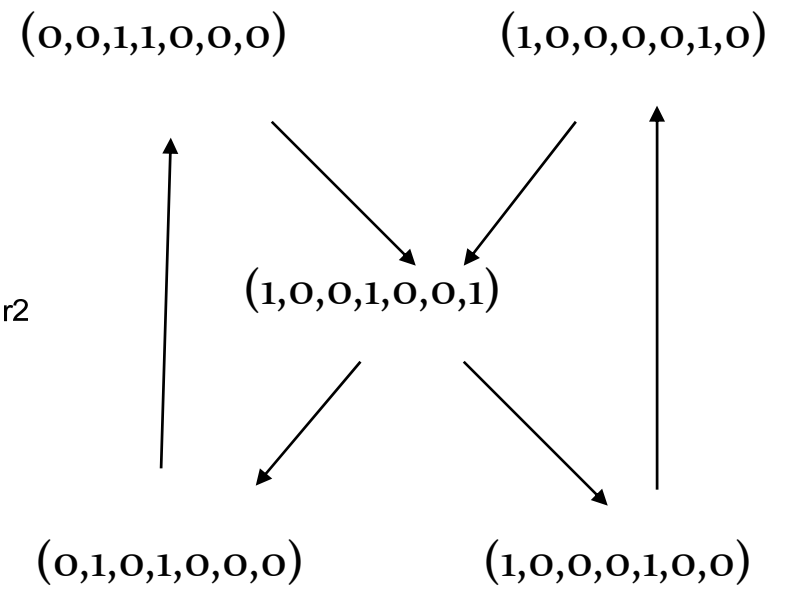
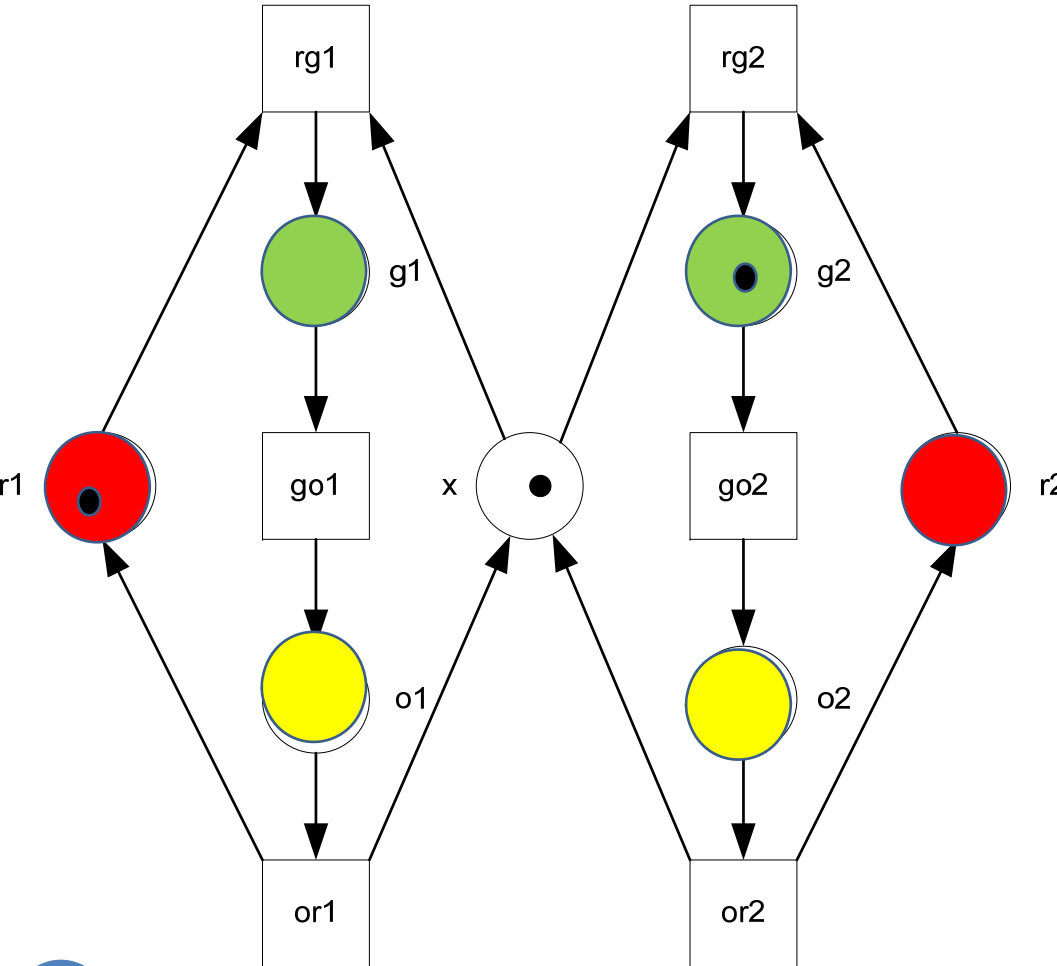
Example: simple concurrent system



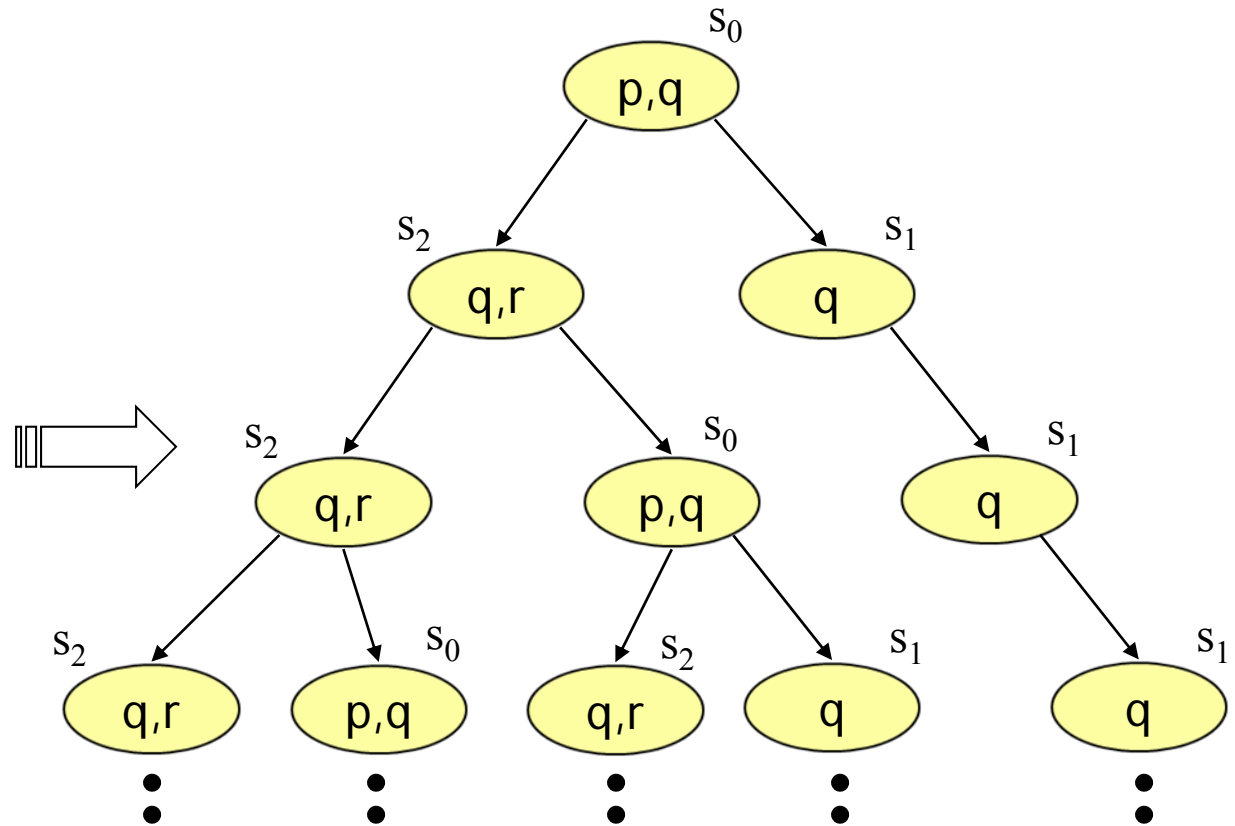
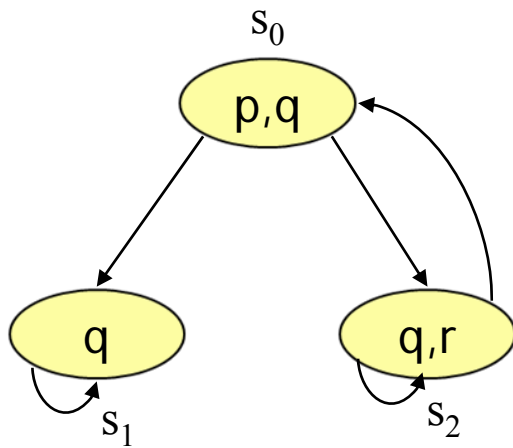
Keep the crossing safe



Traffic light: transition system



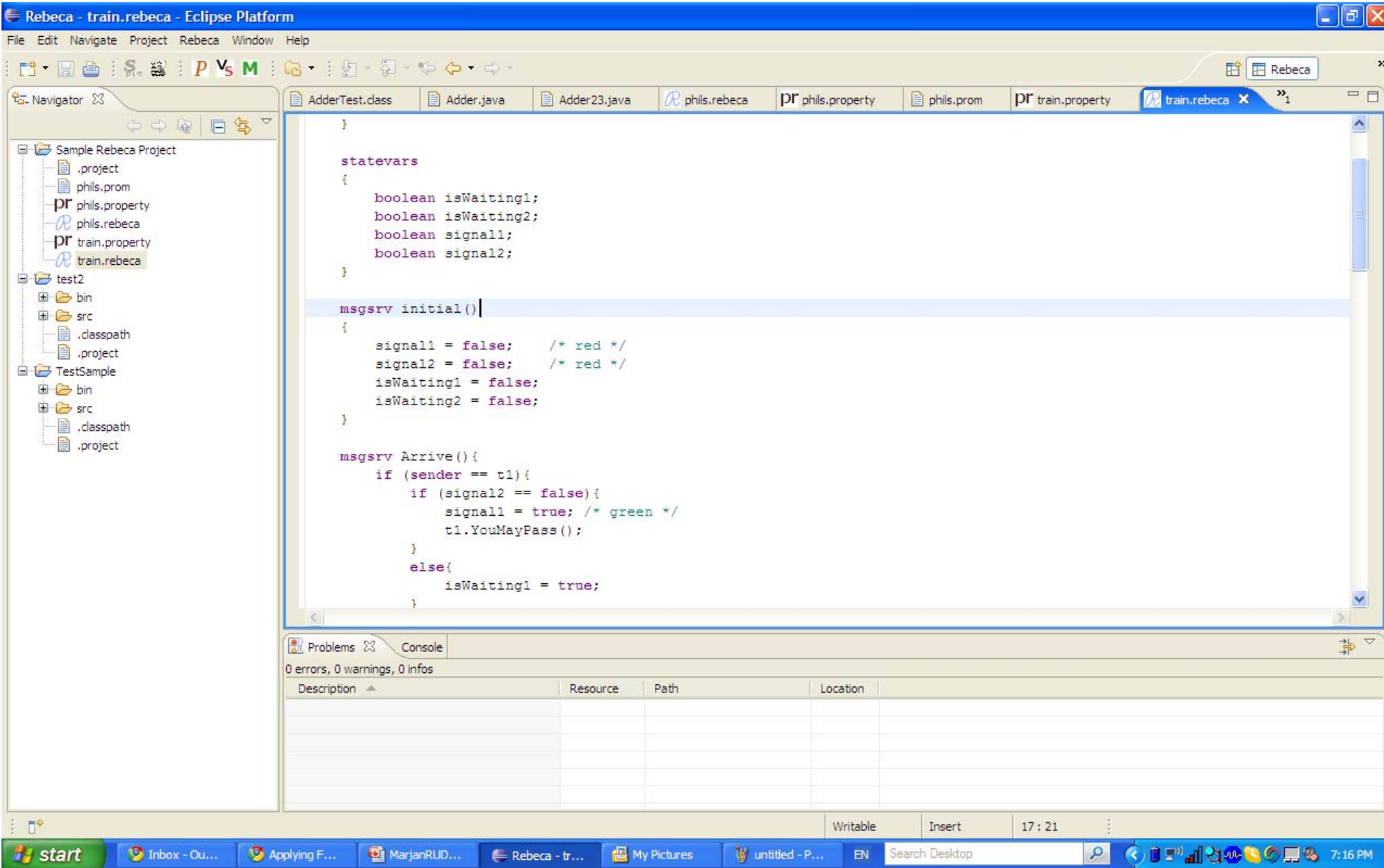
A sample of a model



- We check the model for required properties
 - Mutual exclusion
 - Deadlock freedom
 - No starvation

- Success stories of formal methods...
 - The fact that industry (**INTEL, IBM, MOTOROLA**) is starting to use model checking is encouraging.
 - Microsoft is applying different formal methods
 - Turing awards
 - ...

A screen-shot of our tool Afra



Acknowledgement

- Many of the slides are from
 - Tom Henzinger inaugural talk at EPFL 2006
 - <http://mtc.epfl.ch/~tah/Lectures/EPFL-Inaugural-Dec06.pdf>