Northeast Blackout of 2003

50 million people
60 billion US$

… because of a computer software bug in General Electric Energy's Unix-based XA/21 energy management system that prevented alarms from showing on their control system. This alarm system stalled because of a race condition bug.
Restart and set the recovery options in the system control panel or the \CRASHDEBUG system start option.
this is the first time start your computer. If these steps:

check for viruses on your hard drives or hard drive make sure it is properly run CHKDSK /F to check for start your computer.
\[ x - \frac{x}{y} \times y = 0 \]

\[ 4195835.0 - \left( \frac{4195835.0}{3145727.0} \right) \times 3145727.0 = ? \]
\[
x - \frac{x}{y} \times y = 0
\]

\[
4195835.0 - \left(\frac{4195835.0}{3145727.0}\right) \times 3145727.0 = 256.0
\]
Autonomous Intelligent Vehicles
Mars Climate Orbiter 1998

1cm = 1 inch
Computers embedded into products

- Embedded Systems
- Cyber-Physical Systems

- Internet of Things
  - Ubiquitous Computing
  - Pervasive Computing
  - Ambient Intelligence

- Cognitive Technical Systems
  - Perception and Decision

Disruptive Technologies

wireless software updates

2008 paper: security threat
System Analysis by Model Checking

Program / HW or SW  Logical Specification

Validation / Counterexample
Transition Graphs

System Status

"State"

SIG = 1
ACK = 0
CNT = 13
REQ = 0
IRQ = 0
KRT = 0
MMM = 1

"Transition"

inc CNT

SIG = 1
ACK = 0
CNT = 14
REQ = 0
IRQ = 0
KRT = 0
MMM = 1

IRQ=1

IRQ=2

Transition systems: Automata, Kripke Structures, FSM, …
Transition Graphs

Transition systems: Automata, Kripke Structures, FSM, ...
The Triumph of Model Checking

1981  Clarke / Emerson: CTL Model Checking
      Sifakis / Quielle

1982  EMC: Explicit Model Checking
      Clarke, Emerson, Sistla

1990  Symbolic Model Checking
      Burch, Clarke, Dill, McMillan

1992  SMV: Symbolic Model Verifier
      McMillan

1998  Bounded Model Checking using SAT
      Biere, Clarke, Zhu

2000  Counterexample-guided Abstraction Refinement
      Clarke, Grumberg, Jha, Lu, V

2000+ Software Model Checking
      SLAM, BLAST, MAGIC, …

“Model checking is an acceptable crutch”
(Dijkstra)

Hardware Industry

Software Industry

Turing Award 2007
Emerson, Clarke, Sifakis
2000s: development of industrial strength C model checkers
• “… rivals theorem proving for many verification tasks” (Rushby)
• Microsoft product for Windows device driver verification
“... software verification, this has been the Holy Grail of computer science for many decades but now in some very key areas, for example, driver verification, we’re building tools that do actual proofs about the software and how it works in order to guarantee the reliability.” (2002)
The Triumph of Model Checking

Turing Award 2007
E. Clarke, A. Emerson, J. Sifakis 1981
Programs Analyzing Programs

Self-Reference
Psychology
Philosophy
Logic
Computer Science
Biology
Limitations of Machine Reasoning

Alan Turing 1936
Program analysis by programs not possible.
System Analysis by Model Checking

Program / HW or SW

Logical Specification

Validation / Counterexample
Why can I model a program as a finite state system?

C programs have fixed word size, e.g. 32 bit

→ 32 bit pointer
→ 32 bit address space
→ finite heap
System Analysis by Model Checking

Program / HW or SW  Logical Specification

State Explosion !!!
memory, concurrency
Exponential blow-up

Validation / Counterexample
“I know a bug when I see it.”

Example CTL Specifications
AG $\psi$ “$\psi$ is an invariant”
AF $\psi$ “$\psi$ will necessarily happen”
AGAF $\psi$ “$\psi$ will happen infinitely often”

Counterexample for AG $\neg$ green

Model checking
→ Reachability
→ (Nested) DFS
System Analysis by Model Checking

Program / HW or SW  Logical Specification

State Explosion !!!
memory, concurrency
Exponential blow-up

State Explosion
▸ Finite state systems
▸ Infinite state systems
▸ Parameterized systems

Central Challenge in Model Checking!

Validation / Counterexample
“I know a bug when I see it.”
The Triumph of Model Checking over State Explosion

1981  Clarke / Emerson:CTL Model Checking  
       Sifakis / Quielle

1982  EMC: Explicit Model Checking  
       Clarke, Emerson, Sistla

1990  Symbolic Model Checking  
       Burch, Clarke, Dill, McMillan

1992  SMV: Symbolic Model Verifier  
       McMillan

1998  Bounded Model Checking using SAT  
       Biere, Clarke, Zhu

2000  Counterexample-guided Abstraction Refinement  
       Clarke, Grumberg, Jha, Lu, V

2000+ Software Model Checking  
       SLAM, BLAST, MAGIC, …
Symbolic Model Checking

Program / HW or SW

Logical Specification

Validation / Counterexample

Symbolic Model Checking
1990ies, Bryant, Clarke, McMillan …

► Fixpoint algorithm on sets of states
► Sets encoded by BDDs

BDD:
Binary Decision Diagram
Symbolic Model Checking

Program / HW or SW

Logical Specification

Validation / Counterexample

Symbolic Model Checking
1990ies, Bryant, Clarke, McMillan …

- Fixpoint algorithm on sets of states
- Sets encoded by BDDs

BDD: Binary Decision Diagram
Symbolic Model Checking

Program / HW or SW

Logical Specification

BDD: Binary Decision Diagram

Symbolic Model Checking
1990ies, Bryant, Clarke, McMillan …
► Fixpoint algorithm on sets of states
► Sets encoded by BDDs

Validation / Counterexample
Random Graph

bad compression
Control Flow Graph

good compression
Symbolic Model Checking

Program / HW or SW → Logical Specification

State Explosion:
Exponential BDD blow-up
→ Complementary Methods

Validation / Counterexample

Symbolic Model Checking
1990ies, Bryant, Clarke, McMillan …
- Fixpoint algorithm on sets of states
- Sets encoded by BDDs

Worst Case Complexity (HV 95-98)
- Reachability PSPACE-complete
- Formally, BDDs increase complexity
### The Triumph of Model Checking over State Explosion

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Authors/Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>1981</td>
<td>Clarke / Emerson: CTL Model Checking</td>
<td>Sifakis / Quielle</td>
</tr>
<tr>
<td>1982</td>
<td>EMC: Explicit Model Checking</td>
<td>Clarke, Emerson, Sistla</td>
</tr>
<tr>
<td>1990</td>
<td>Symbolic Model Checking</td>
<td>Burch, Clarke, Dill, McMillan</td>
</tr>
<tr>
<td>1992</td>
<td>SMV: Symbolic Model Verifier</td>
<td>McMillan</td>
</tr>
<tr>
<td>1998</td>
<td>Bounded Model Checking using SAT</td>
<td>Biere, Clarke, Zhu</td>
</tr>
<tr>
<td>2000</td>
<td>Counterexample-guided Abstraction Refinement</td>
<td>Clarke, Grumberg, Jha, Lu, V</td>
</tr>
<tr>
<td>2000+</td>
<td>Software Model Checking</td>
<td>SLAM, BLAST, MAIC</td>
</tr>
</tbody>
</table>

**Aggressive:** Prune Information
Abstraction
Existential Abstraction

Abstraction function $h$ maps concrete states to abstract states.

$M_h$

$M$

Preservation Theorem?

$M$ large, possibly infinite.