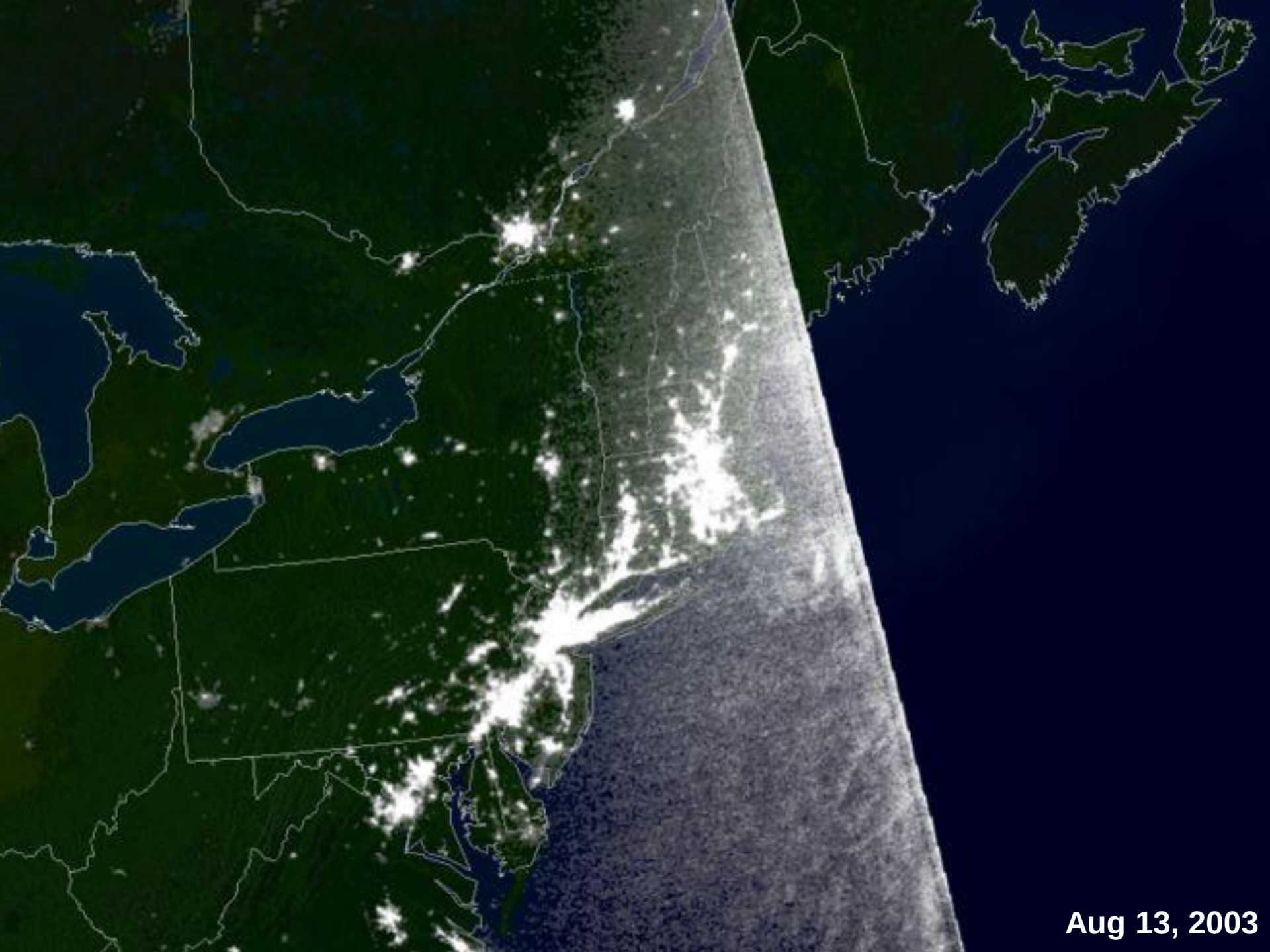

Aug 13, 2003


Aug 14, 2003

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.

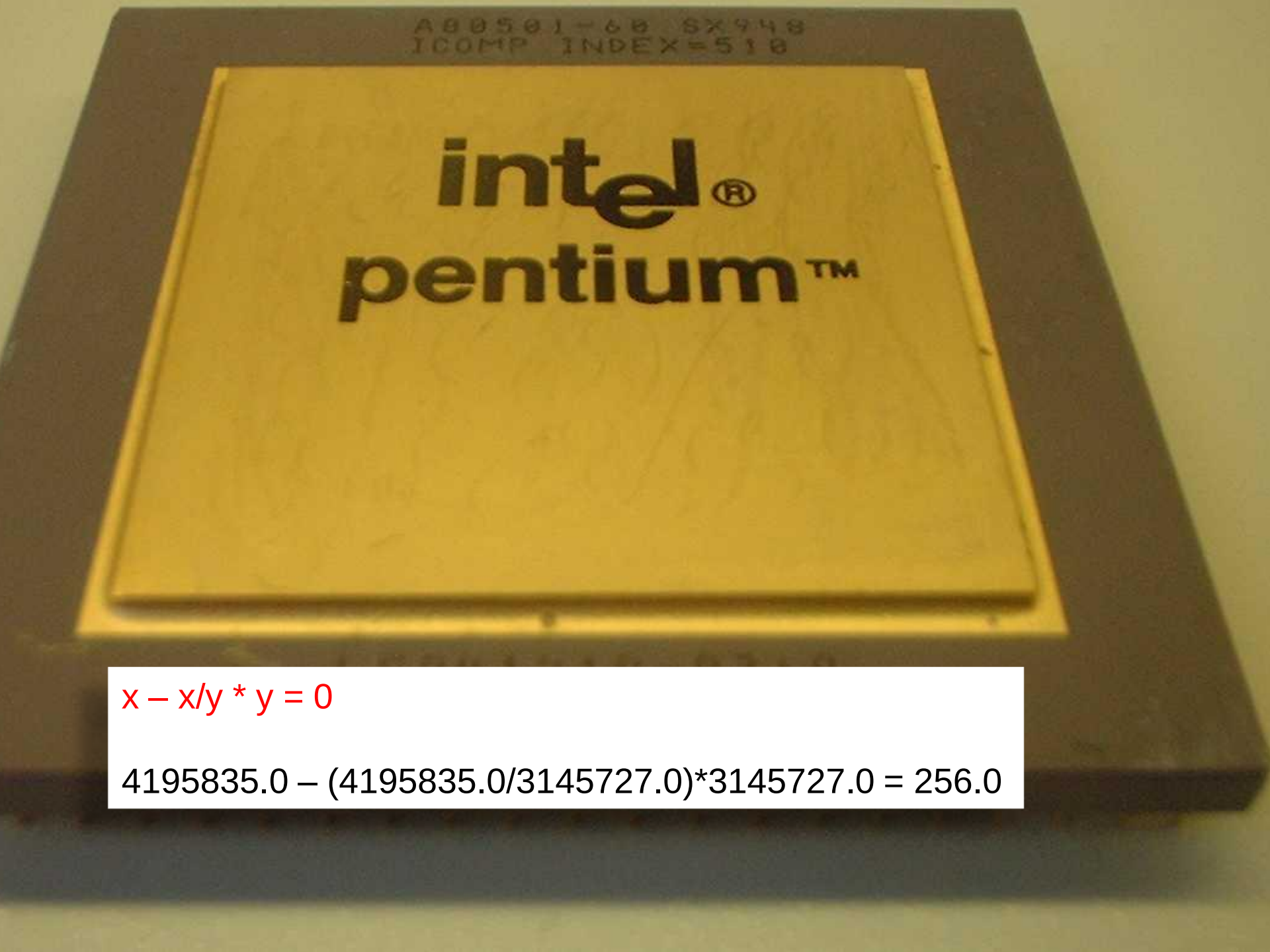
Ontario
Aug 14, 2003

```
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER

CPUID:GenuineIntel 5.2.c irql:1f  SYSVER 0xf0000565

Dll Base DateStmp - Name                 Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe         80010000 31ee6c52 - hal.dll
80001000 31ed06b4 - atapi.sys            80006000 31ec6c74 - SCSIPORT.SYS
802c6000 31ed06bf - aic78xx.sys          802cd000 31ed237c - Disk.sys
802d1000 31ec6c7a - CLASS2.SYS           8037c000 31eed0a7 - Ntfs.sys
fc698000 31ec6c7d - Floppy.SYS           fc6a8000 31ec6ca1 - Cdrom.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS           fc9c9000 31ec6c99 - Null.SYS
fc864000 31ed868b - KSecDD.SYS           fc9ca000 31ec6c78 - Beep.SYS
fc6d8000 31ec6c90 - i8042prt.sys         fc86c000 31ec6c97 - mouclass.sys
fc874000 31ec6c94 - kbdclass.sys         fc6f0000 31f50722 - VIDEOPORT.SYS
feffa000 31ec6c62 - mga_mil.sys          fc890000 31ec6c6d - vga.sys
fc708000 31ec6ccb - Msfs.SYS             fc4b0000 31ec6cc7 - Npfs.SYS
fefbc000 31eed262 - NDIS.SYS             a0000000 31f954f7 - win32k.sys
fefa4000 31f91a51 - mga.dll              fec31000 31eedd07 - Fastfat.SYS
feb8c000 31ec6e6c - TDI.SYS              feaf0000 31ed0754 - nbf.sys
feacf000 31f130a7 - tcpip.sys            feab3000 31f50a65 - netbt.sys
fc550000 31601a30 - el59x.sys            fc560000 31f8f864 - afd.sys
fc718000 31ec6e7a - netbios.sys          fc858000 31ec6c9b - Parport.sys
fc870000 31ec6c9b - Parallel.SYS         fc954000 31ec6c9d - ParVdm.SYS
fc5b0000 31ec6cb1 - Serial.SYS           fea4c000 31f5003b - rdr.sys
fea3b000 31f7a1ba - mup.sys              fe9da000 32031abe - srv.sys

Address  dword dump   Build [1381]                              - Name
fec32d84 80143e00 80143e00 80144000 ffdff000 00070b02          - KSecDD.SYS
801471c8 80144000 80144000 ffdff000 c03000b0 00000001          - ntoskrnl.exe
801471dc 80122000 f0003fe0 f030eee0 e133c4b4 e133cd40          - ntoskrnl.exe
80147304 803023f0 0000023c 00000034 00000000 00000000          - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.
```


OPEN 24 HOURS
this is the first time
start your computer. If
ese steps:
eck for viruses on your
rd drives or hard drive
make sure it is properl
n CHKDSK /F to check for
start your computer.
42 St-Port Authority Bus
Terminal Station

$x - x/y * y = 0$

$4195835.0 - (4195835.0/3145727.0)*3145727.0 = ?$

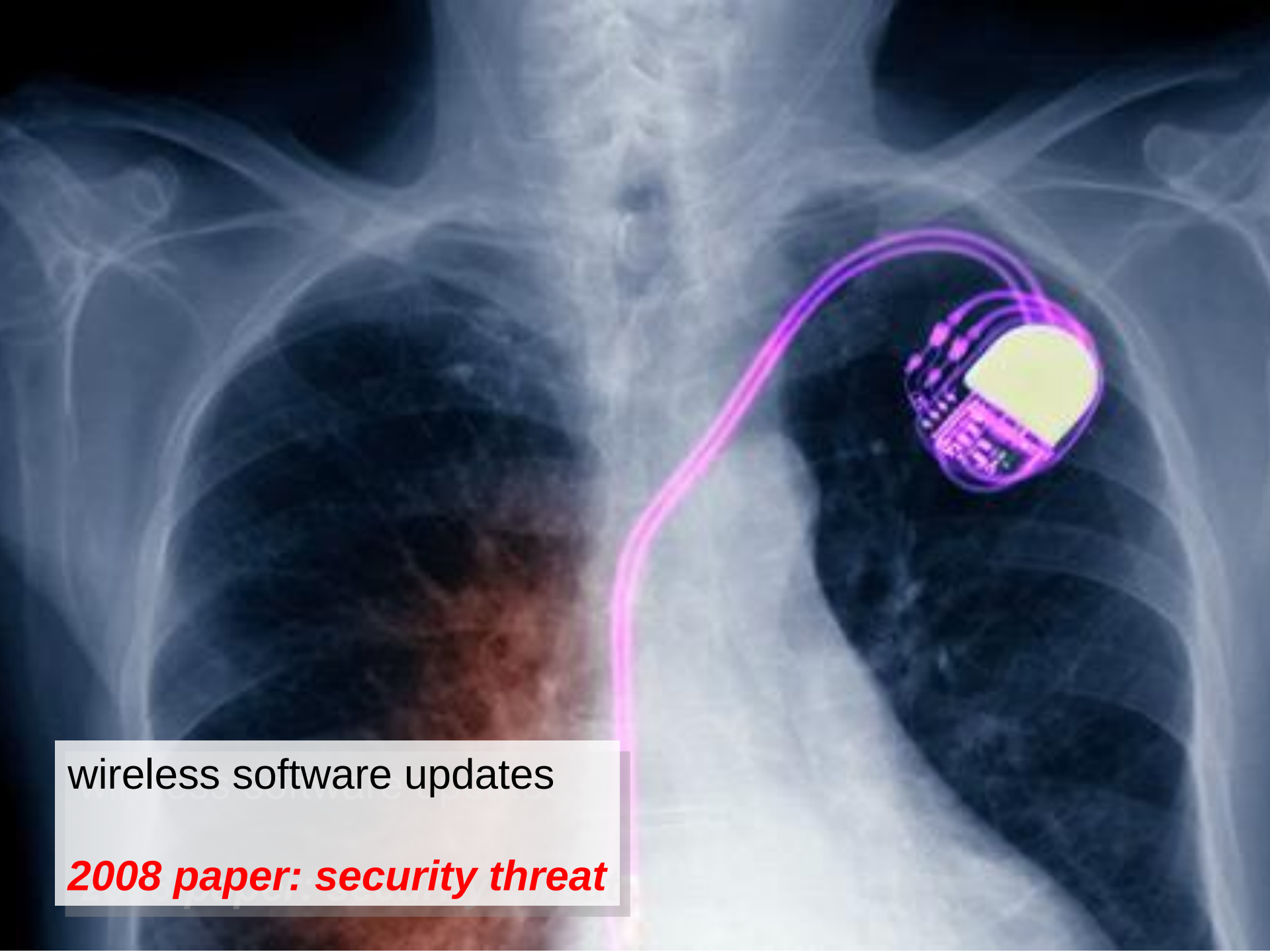


$x - x/y * y = 0$

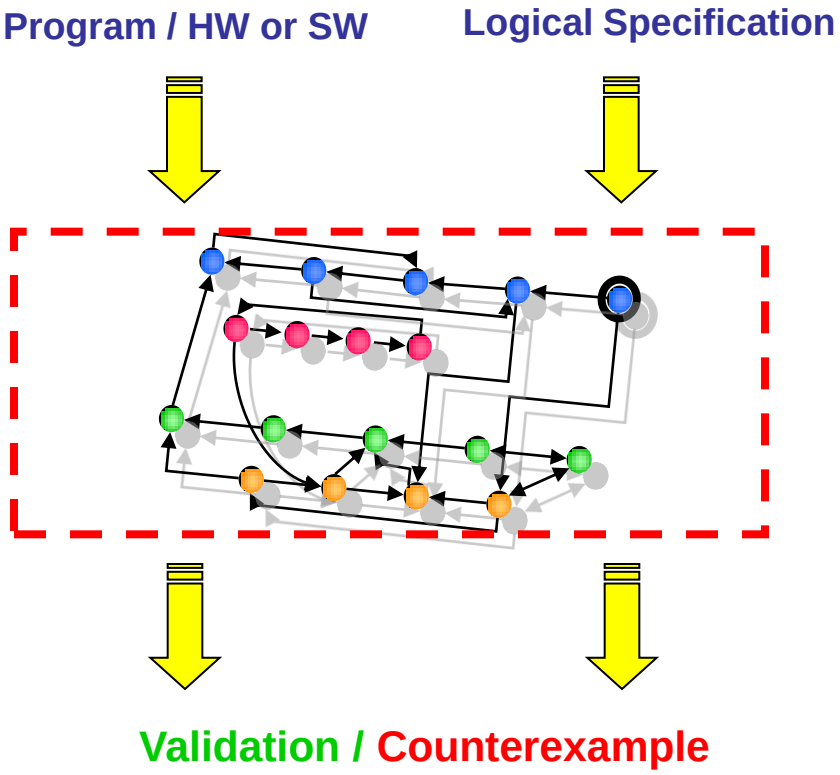
$4195835.0 - (4195835.0/3145727.0)*3145727.0 = 256.0$

Autonomous Intelligent Vehicles

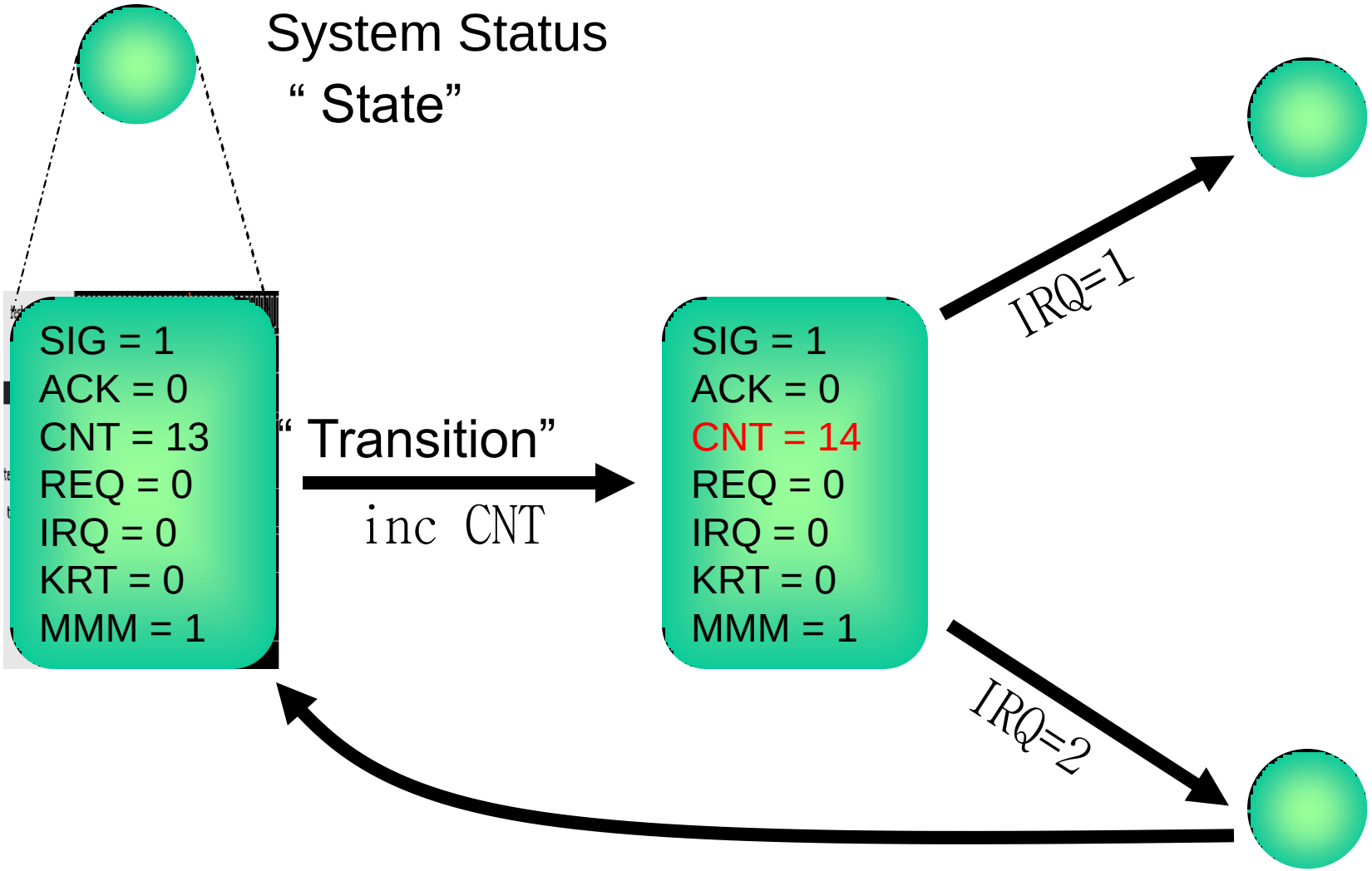
Mars Climate Orbiter 1998


wireless software updates
2008 paper: security threat

System Analysis by Model Checking

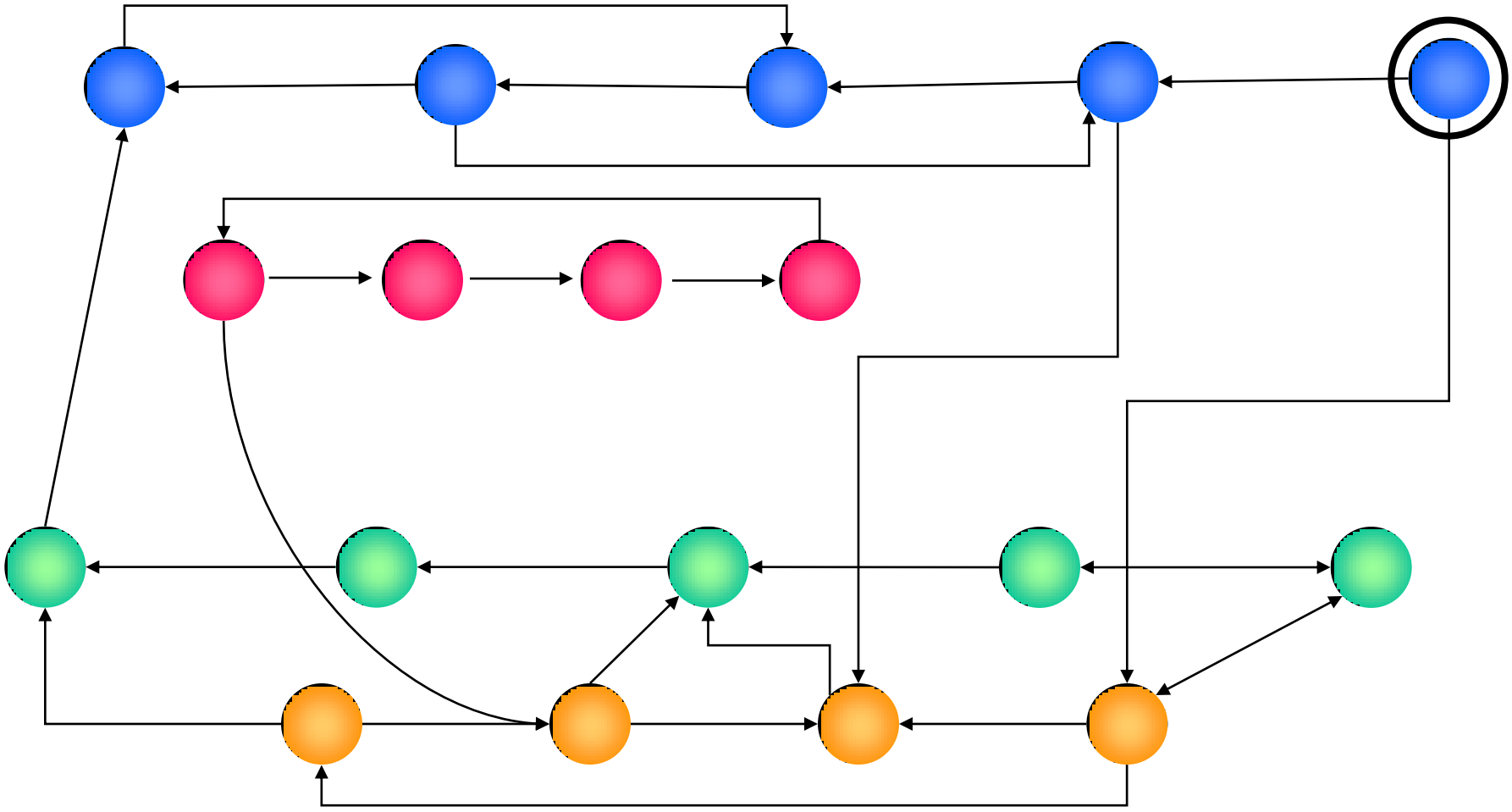


Transition Graphs



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 Che
Clarke, Emerson, Sistla

10^5 states

1990 Symbolic Model Checking
Burch, Clarke, Dill, McMillan

Hardware Industry

1992 SMV: Symbolic Model V
McMillan

10^{100} states

"Model checking is an acceptable crutch"
(Dijsktra)

1998 Bounded Model Checking using SAT
Biere, Clarke, Zhu

10^{1000} states

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

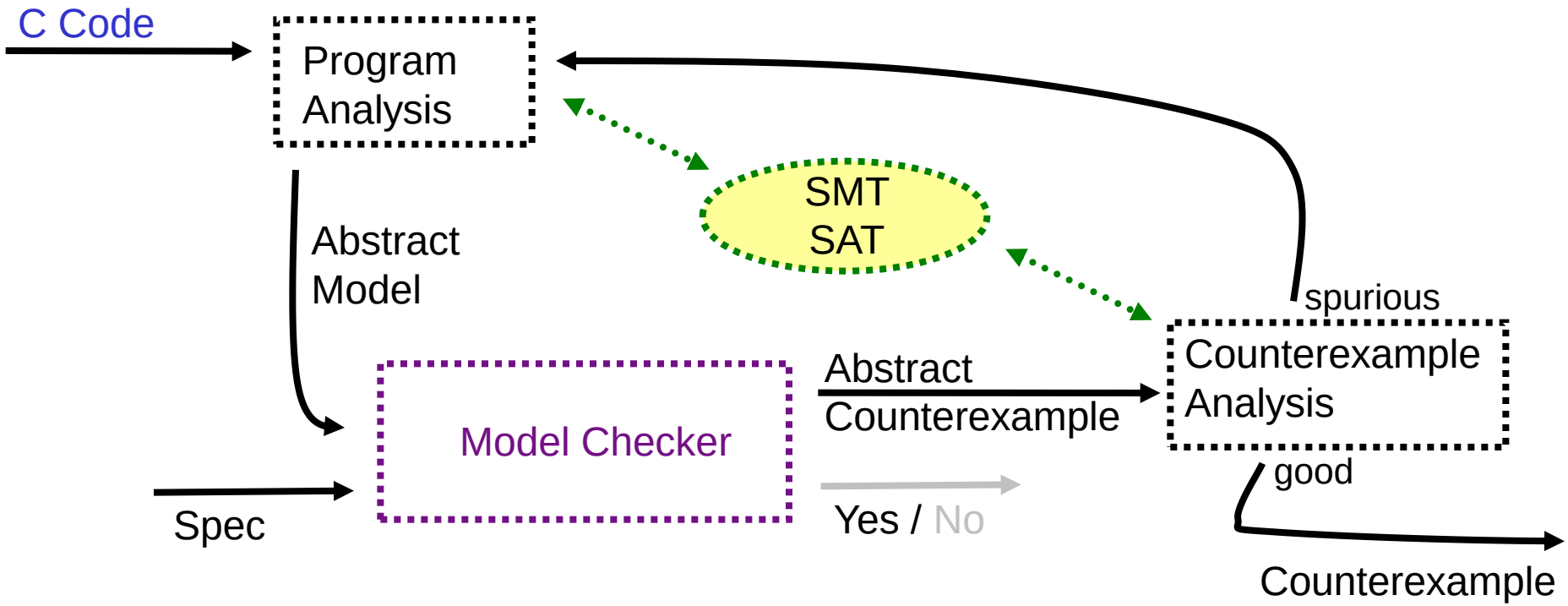
Software Industry

2000+ Software Model Chec
SLAM, BLAST, MA

infinite-state

Turing Award 2007
Emerson, Clarke, Sifakis

Software Model Checking



- 2000s: development of industrial strength C model checkers
- "… rivals theorem proving for many verification tasks" (Rushby)
- Microsoft product for Windows device driver verification

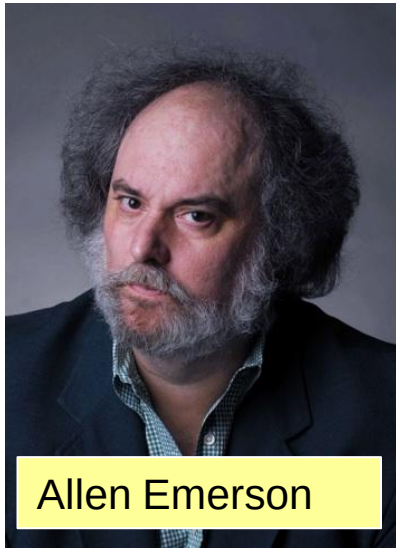
The Triumph of Model Checking

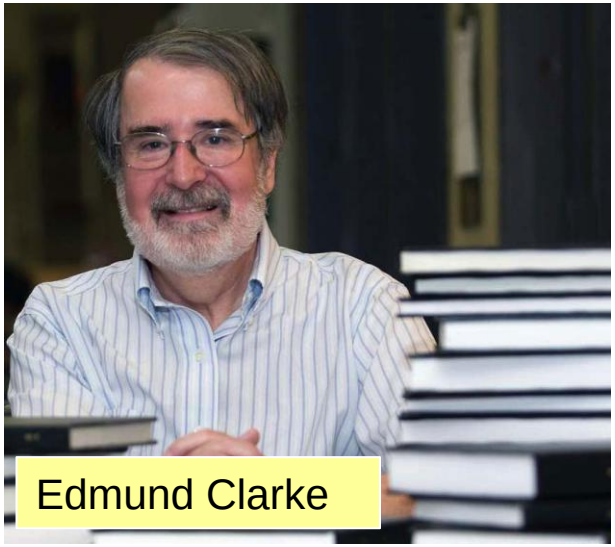
"… software verification, this has been the Holy Grail of computer science for many decades but now in some very key areas, for example, driver verification, we're building tools that do actual proofs about the software and how it works in order to guarantee the reliability." (2002)

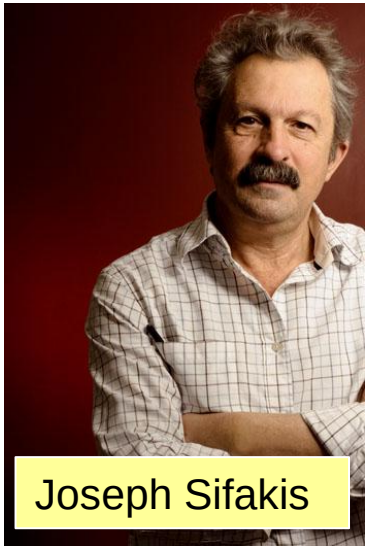
The Triumph of Model Checking

Turing Award 2007

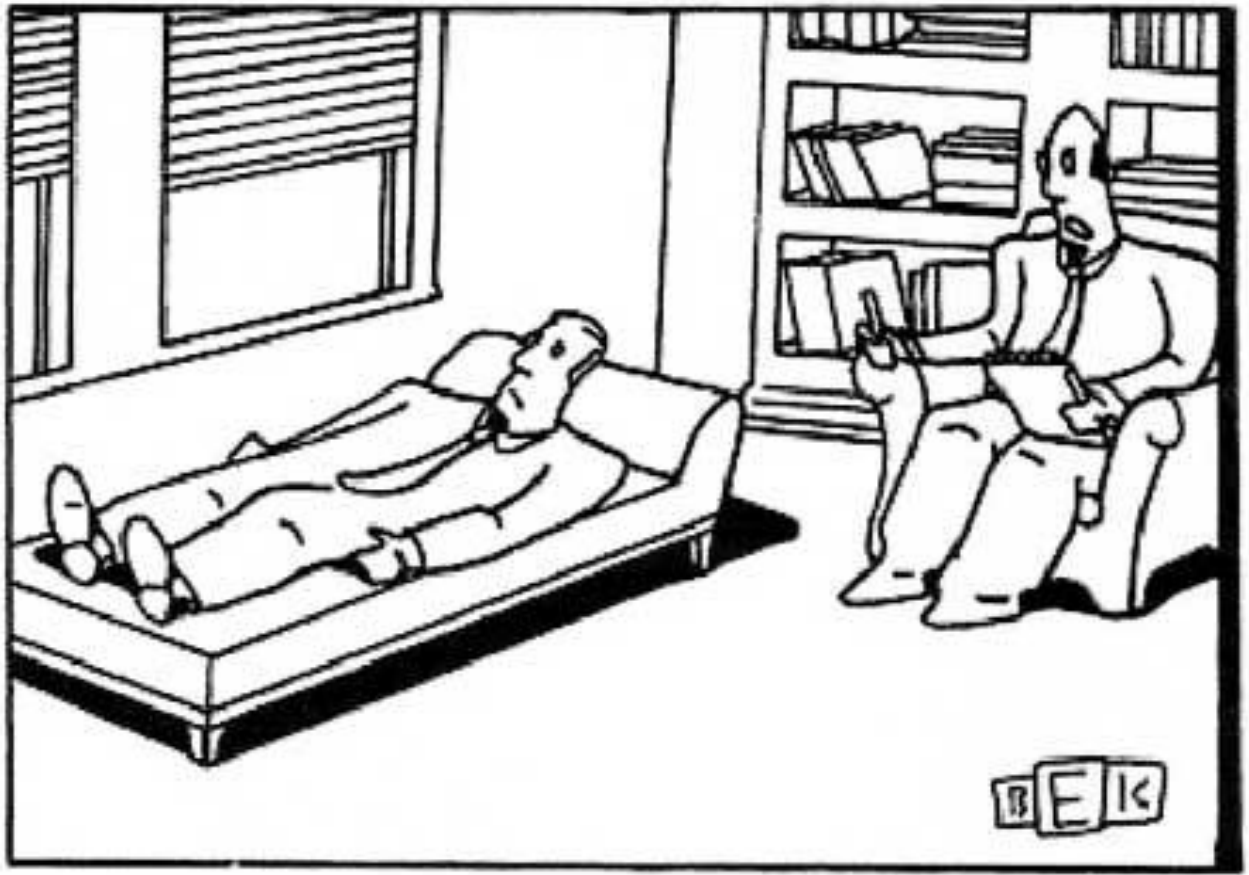
E. Clarke, A. Emerson, J. Sifakis 1981


Allen Emerson


Edmund Clarke


Joseph Sifakis

Programs Analyzing Programs



Self-Reference

Psychology

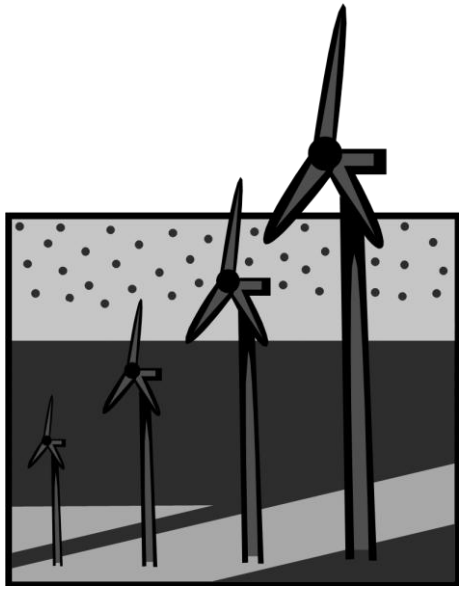
Philosophy

Logic

Computer Science

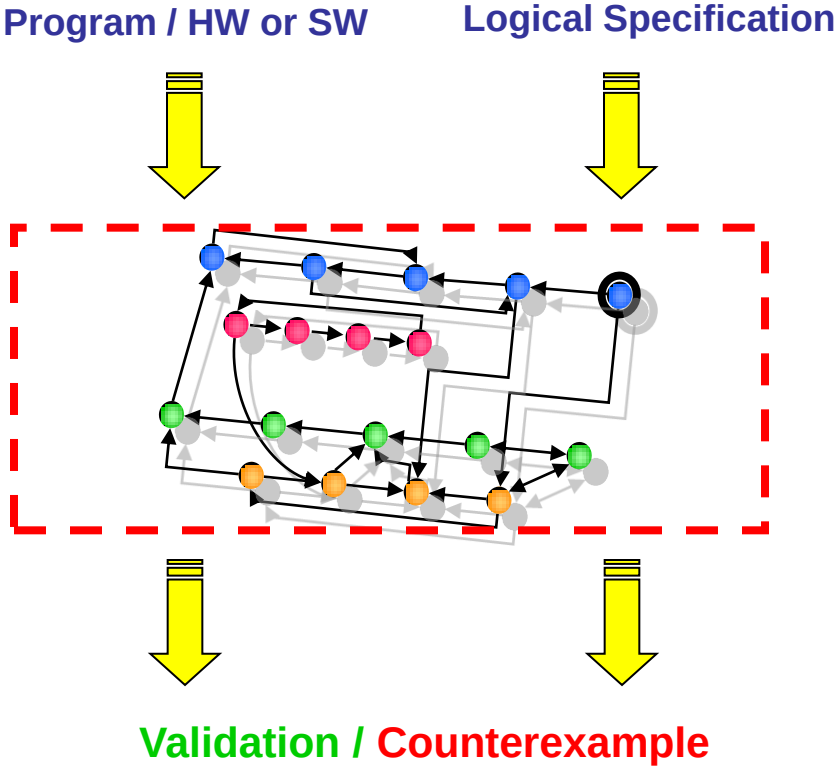
Biology

Limitations of Machine Reasoning

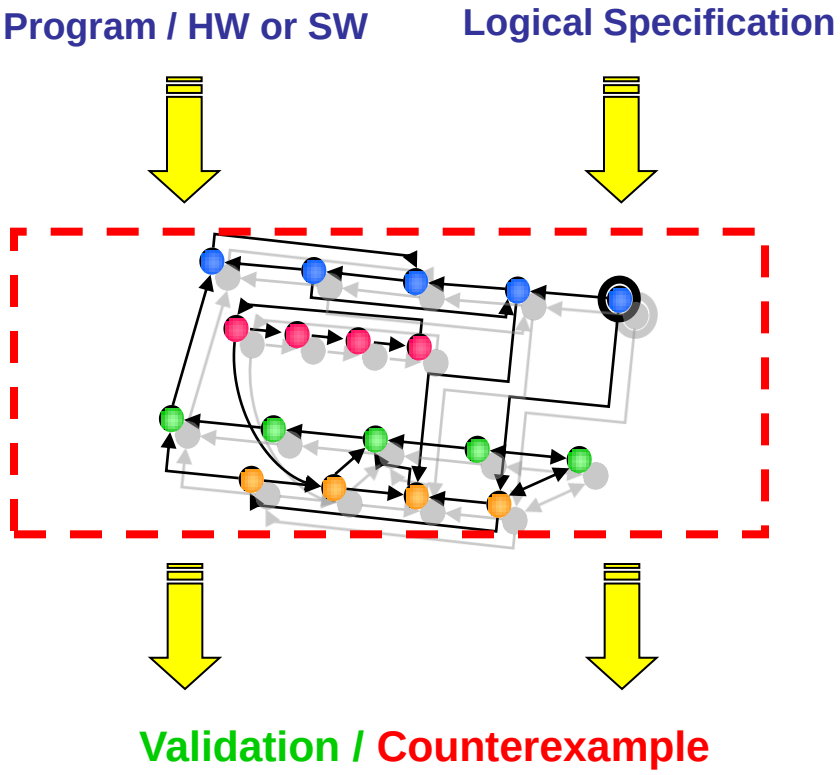


Alan Turing 1936
Program analysis by programs not possible.

System Analysis by Model Checking



System Analysis by Model Checking



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

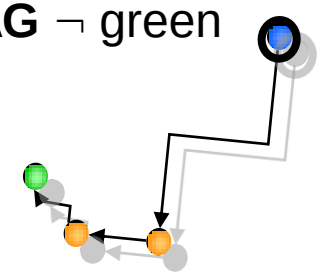
State Explosion !!!
memory, concurrency
Exponential blow-up

Validation / Counterexample
"I know a bug when I see it."

Example CTL Specifications

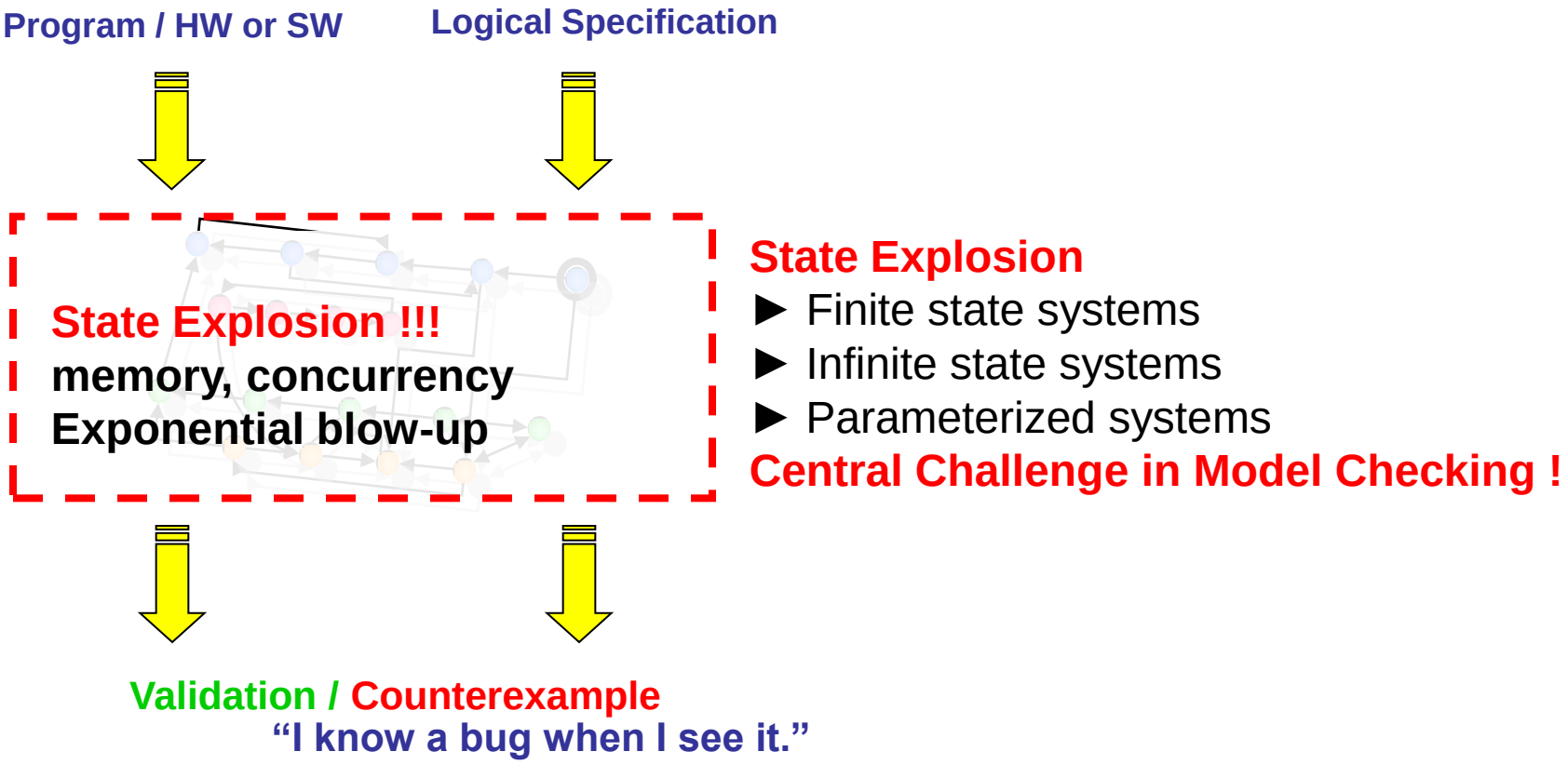
AG ψ "ψ is an invariant"
AF ψ "ψ will necessarily happen"
AGAF ψ "ψ will happen infinitely often"

Counterexample for **AG** ¬ green



Model checking
→ Reachability
→ (Nested) DFS

System Analysis by Model Checking



State Explosion

- ► Finite state systems
- ► Infinite state systems
- ► Parameterized systems

Central Challenge in Model Checking !

The Triumph of Model Checking over State Explosion

1981 Clarke / Emerson: CTL Model Checking
Sifakis / Quielle

1982 EMC: Explicit Model Che
Clarke, Emerson, Sistla

10^5 states

1990 Symbolic Model Checking
Burch, Clarke, Dill, McMillan

1992 SMV: Symbolic Model V
McMillan

10^{100} states

Conservative:
Compress Information

1998 Bounded Model Checking using SAT
Biere, Clarke, Zhu

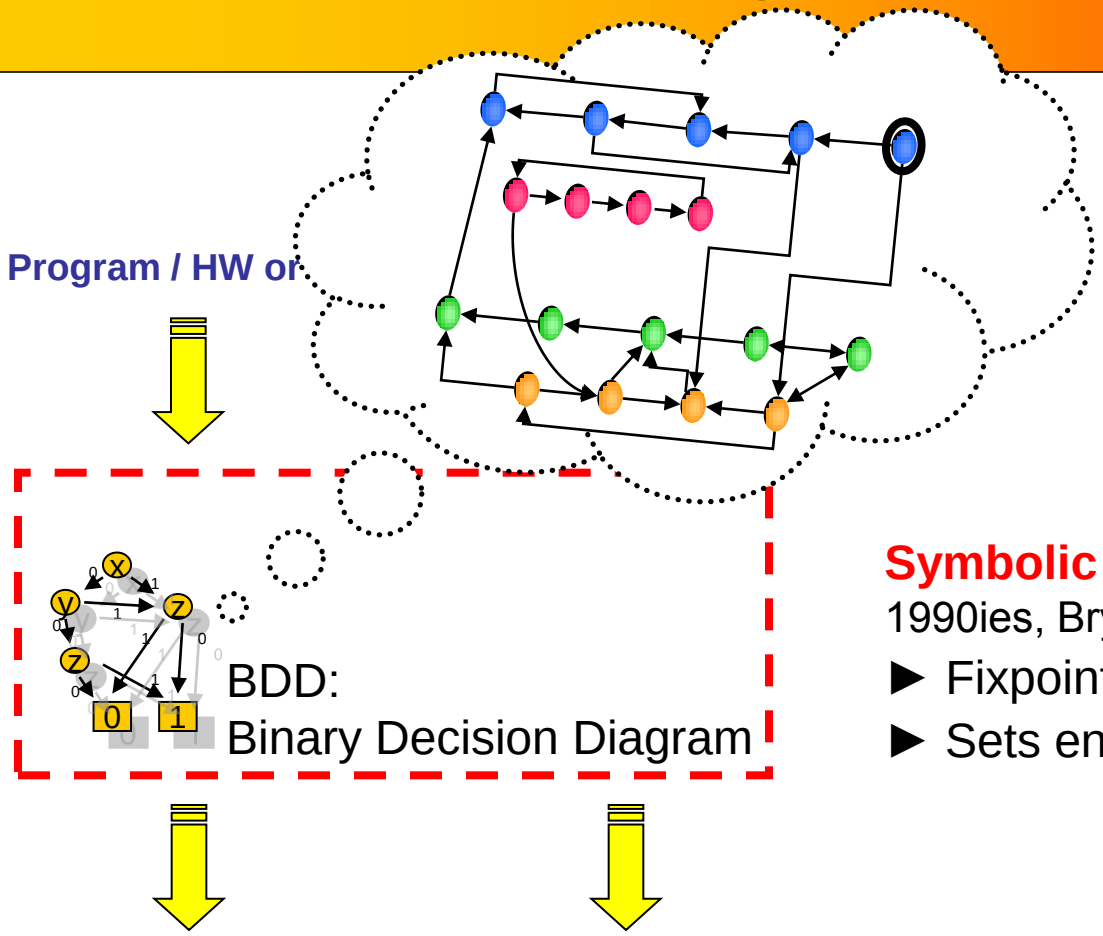
10^{1000} states

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

2000+ Software Model Chec
SLAM, BLAST, MA

infinite-state

Symbolic Model Checking

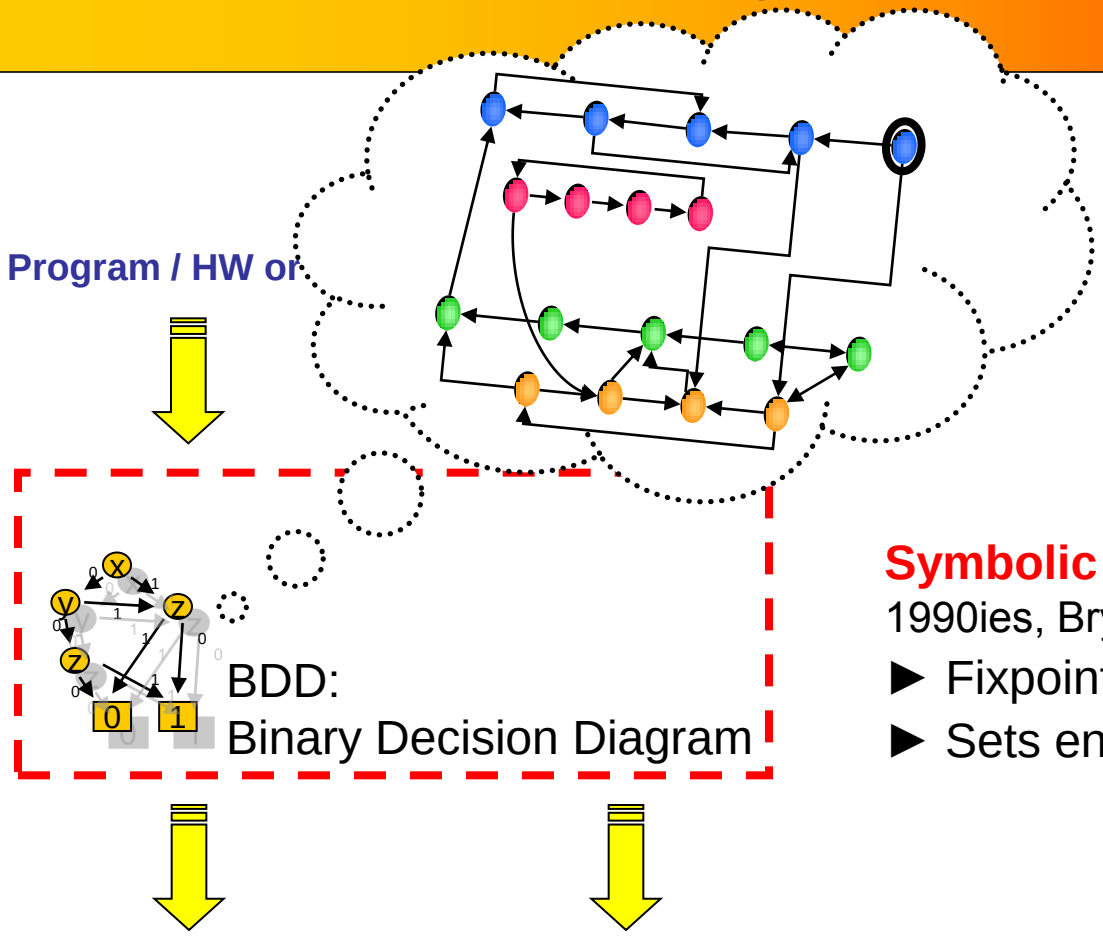


Symbolic Model Checking

1990ies, Bryant, Clarke, McMillan …

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

Symbolic Model Checking

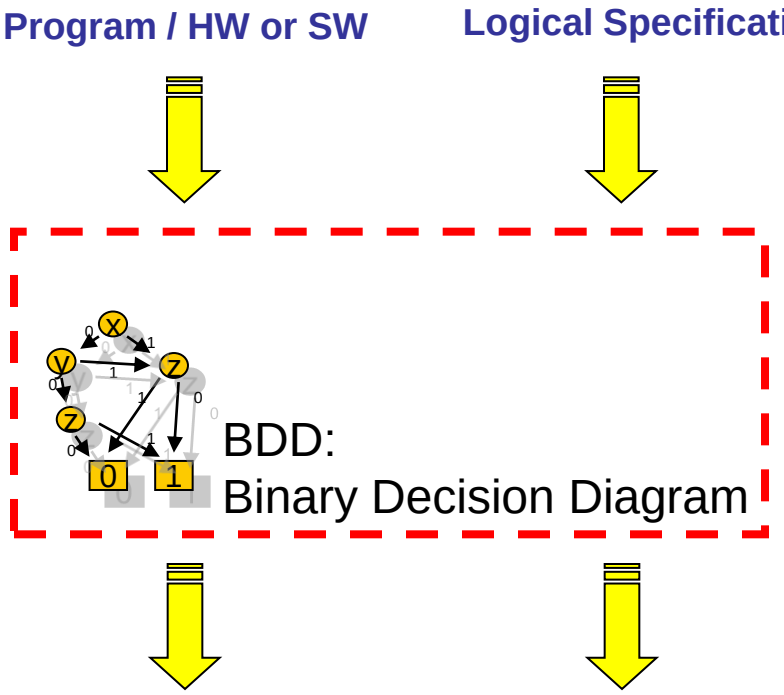


Symbolic Model Checking

1990ies, Bryant, Clarke, McMillan …

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

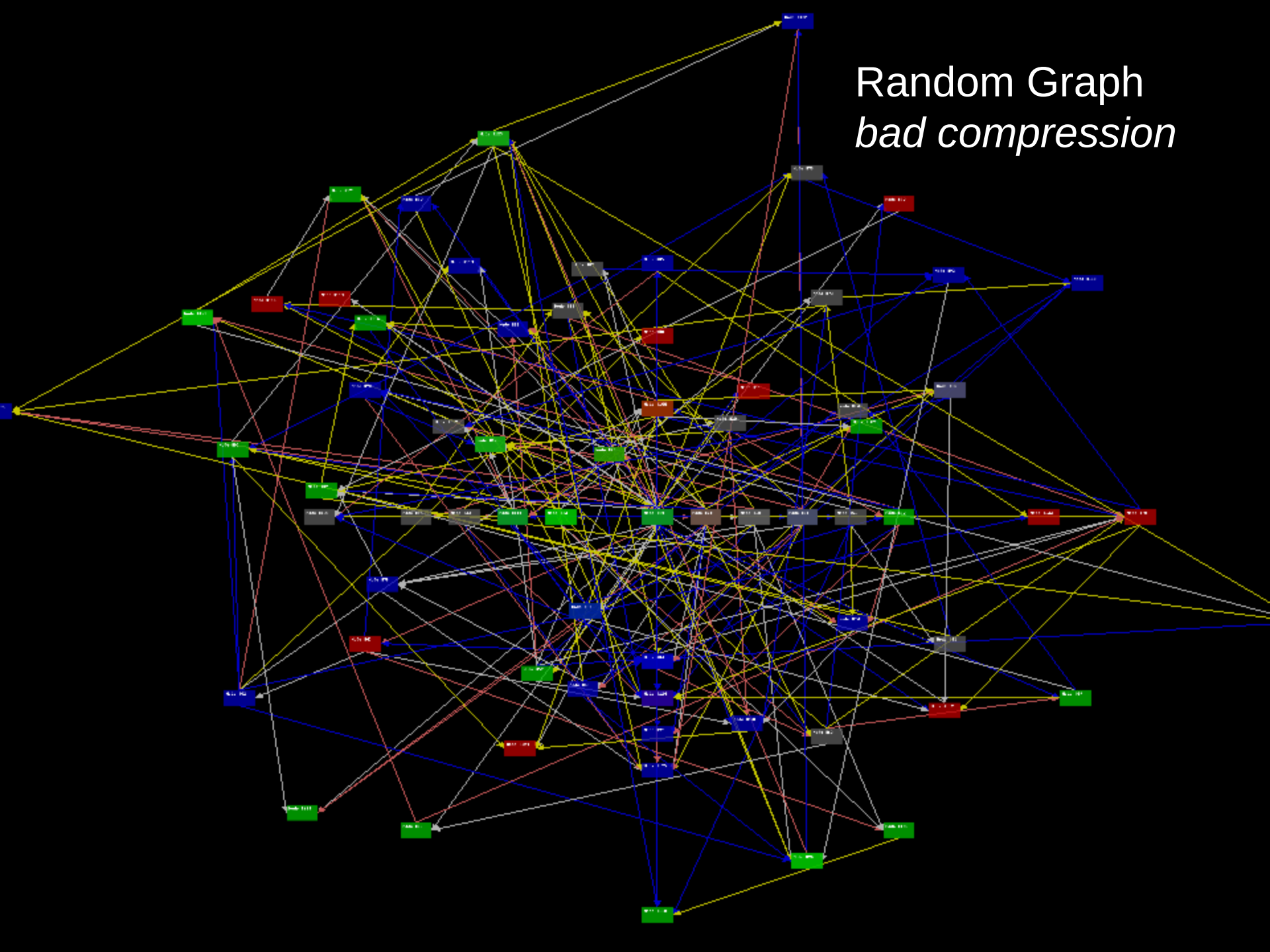
Symbolic Model Checking



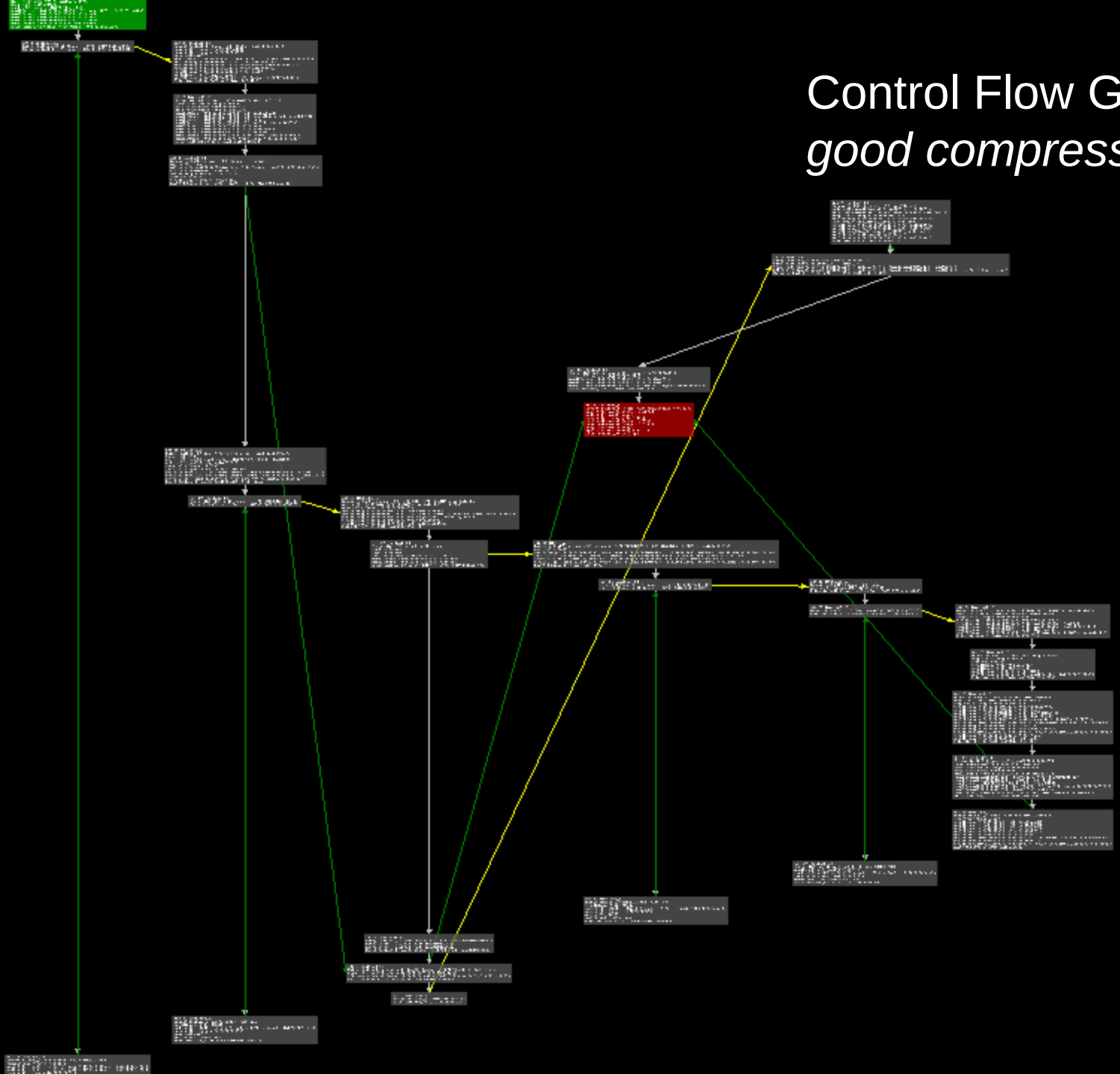
Symbolic Model Checking

1990ies, Bryant, Clarke, McMillan …

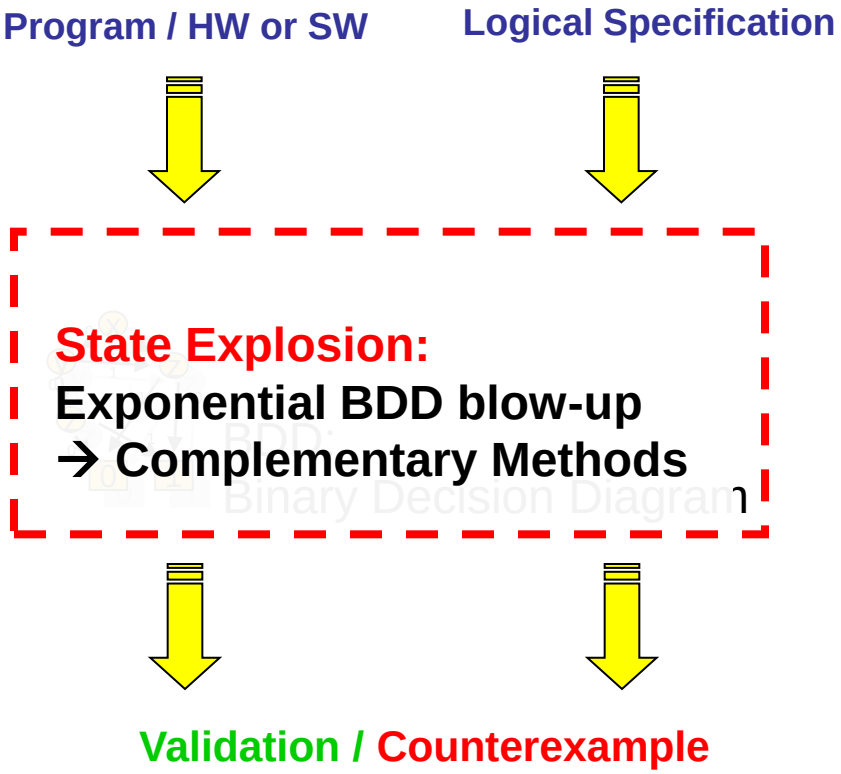
- ► Fixpoint algorithm on sets of states
- ► Sets encoded by BDDs


Random Graph
bad compression

Control Flow Graph
good compression



Symbolic Model Checking



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

1981 Clarke / Emerson: CTL Model Checking
Sifakis / Quielle

1982 EMC: Explicit Model Che
Clarke, Emerson, Sistla

10^5 states

1990 Symbolic Model Checking
Burch, Clarke, Dill, McMillan

1992 SMV: Symbolic Model V
McMillan

10^{100} states

1998 Bounded Model Checking using SAT
Biere, Clarke, Zhu

10^{1000} states

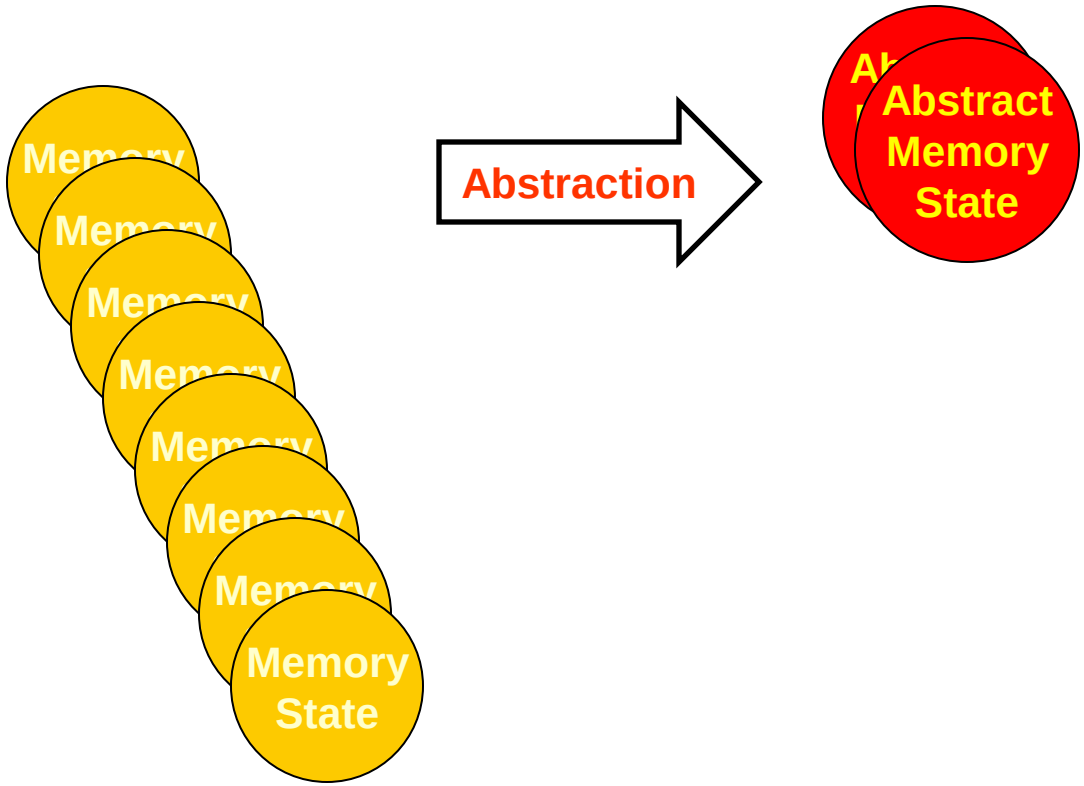
2000 Counterexample-guided Abstraction Refinement
Clarke, Grumberg, Jha, Lu, V

2000+ Software Model Chec
SLAM, BLAST, MA

infinite-state

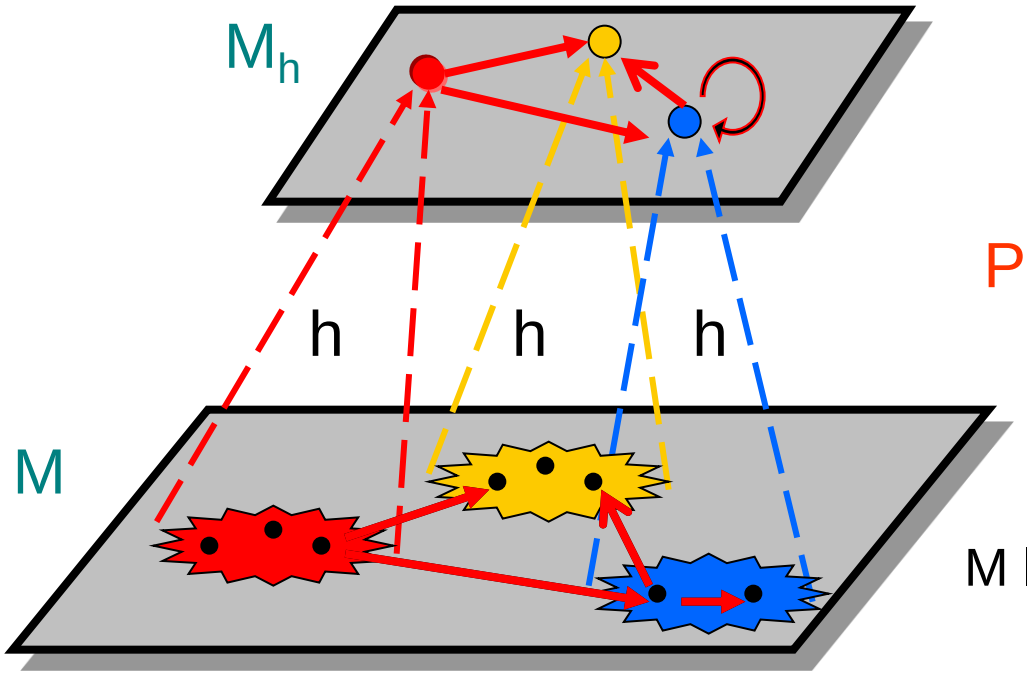
Aggressive:
Prune Information

Abstraction



Existential Abstraction

Abstraction function h maps concrete states to abstract states.



Preservation Theorem ?

M large, possibly infinite.