Temporal Logics
Linear & Branching Time Logic

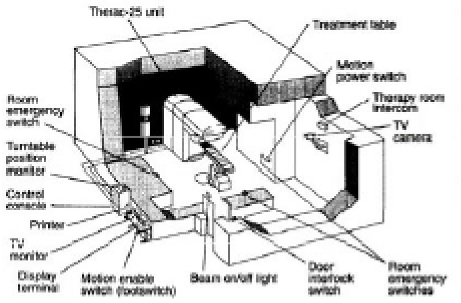
Kim Guldstrand Larsen

Overview of Course

- Temporal Logics (Linear & Branching Time)
  - Kim G Larsen
- Mobile Process Calculi
  - Hans Hüttel
- Static Analysis of Mobile Ambients
  - René Rydhof Hansen
- Process Rewrite Systems
  - Jiri Srba

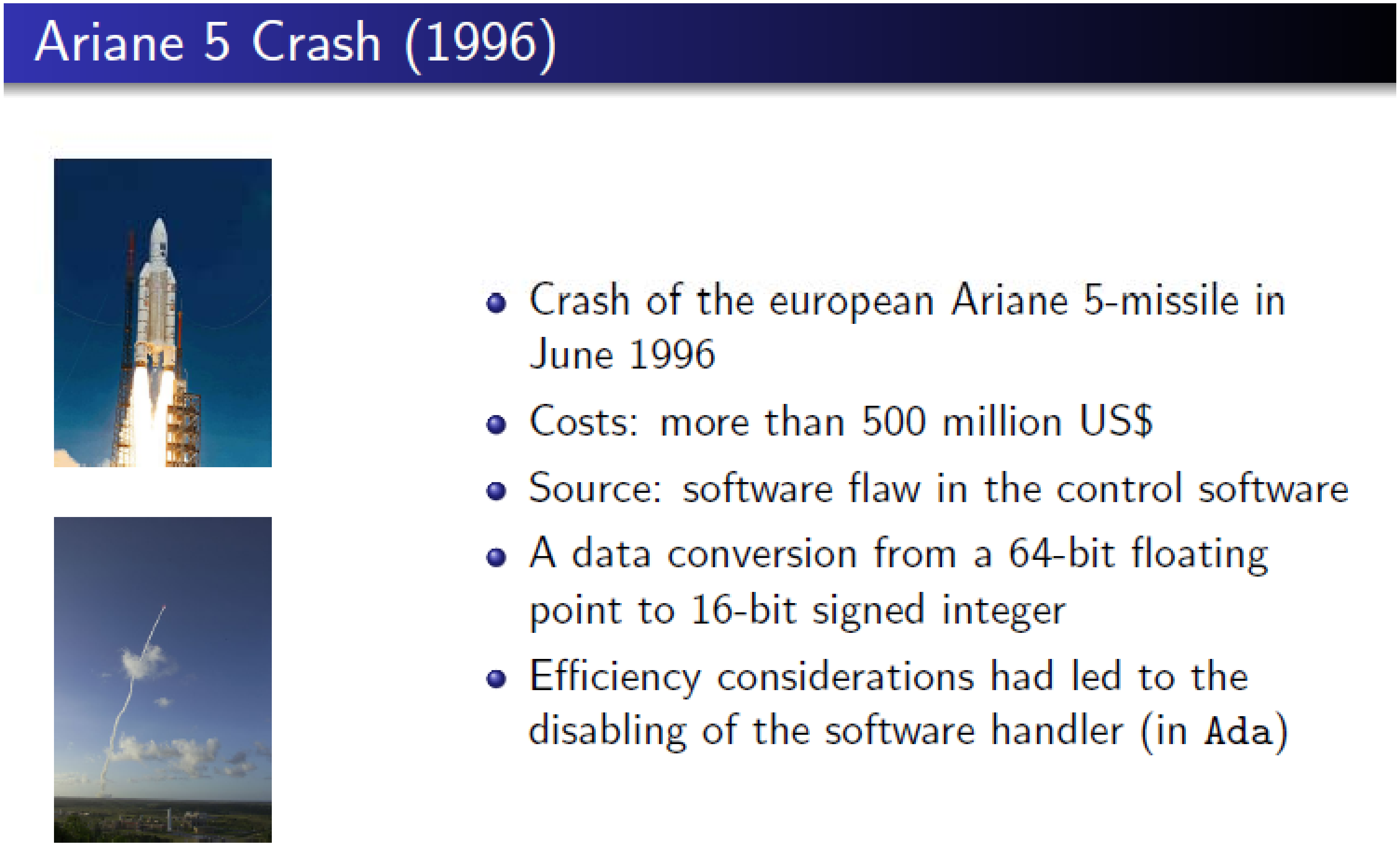
Software Errors

Therac-25 Radiation Overdosing (1985-87)



- Radiation machine for treatment of cancer patients
- At least 6 cases of overdosis in period 1985–1987 ($\approx$ 100-times dosis)
- Three cancer patients died
- Source: Design error in the control software (*race condition*)

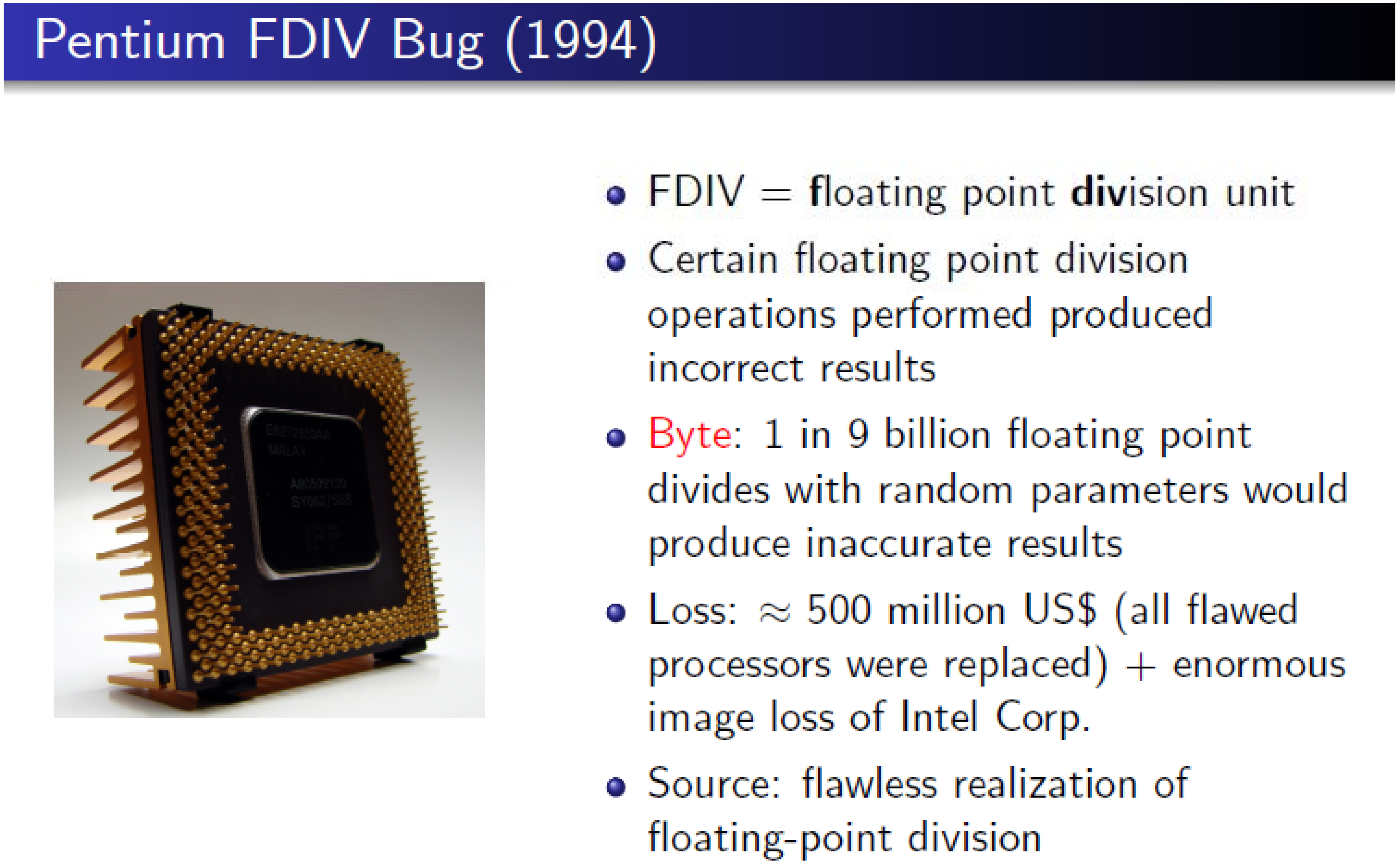
Software Errors



Ariane 5 Crash (1996)

- Crash of the european Ariane 5-missile in June 1996
- Costs: more than 500 million US$
- Source: software flaw in the control software
- A data conversion from a 64-bit floating point to 16-bit signed integer
- Efficiency considerations had led to the disabling of the software handler (in `Ada`)

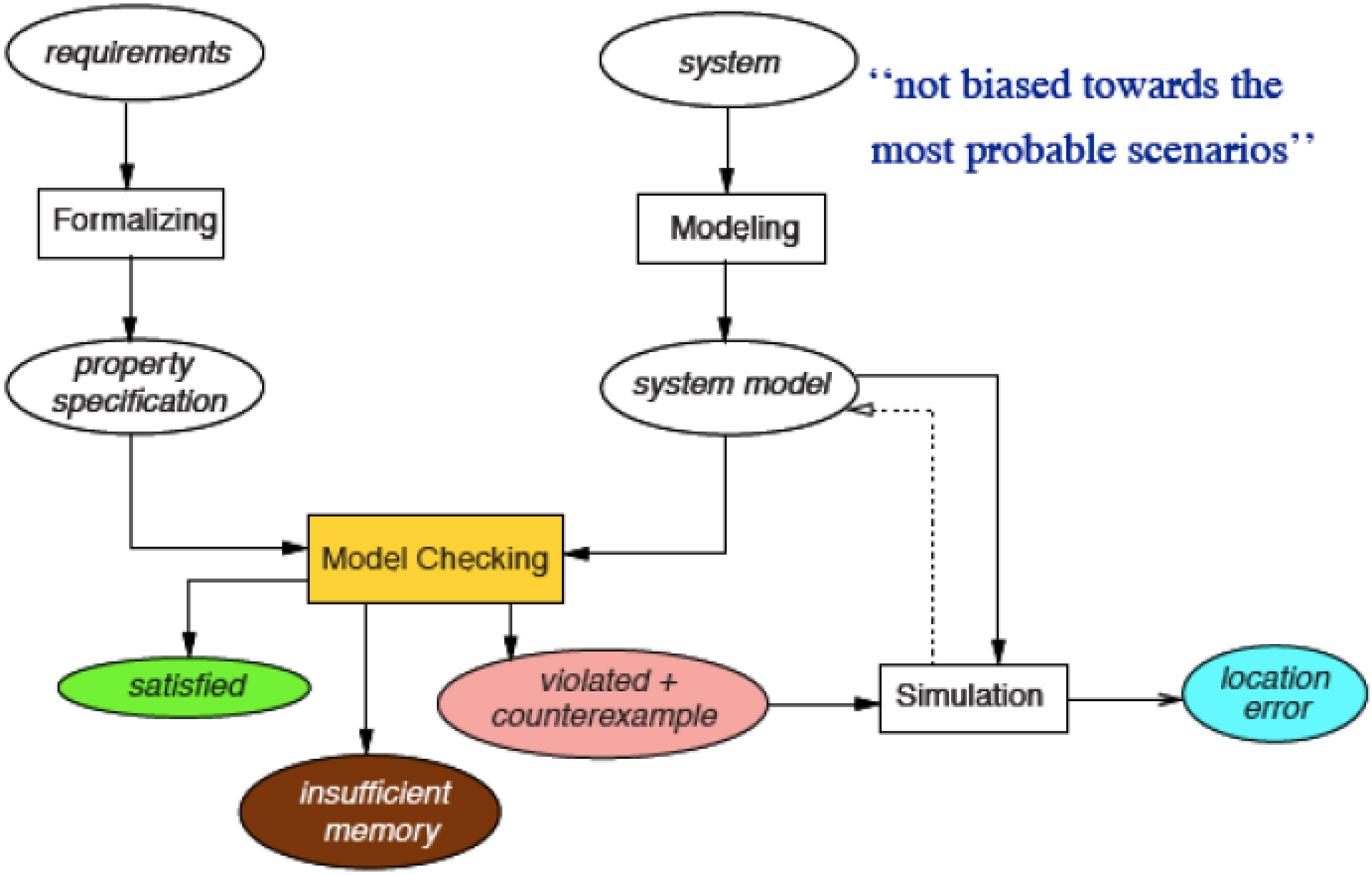
Software Errors



Pentium FDIV Bug (1994)

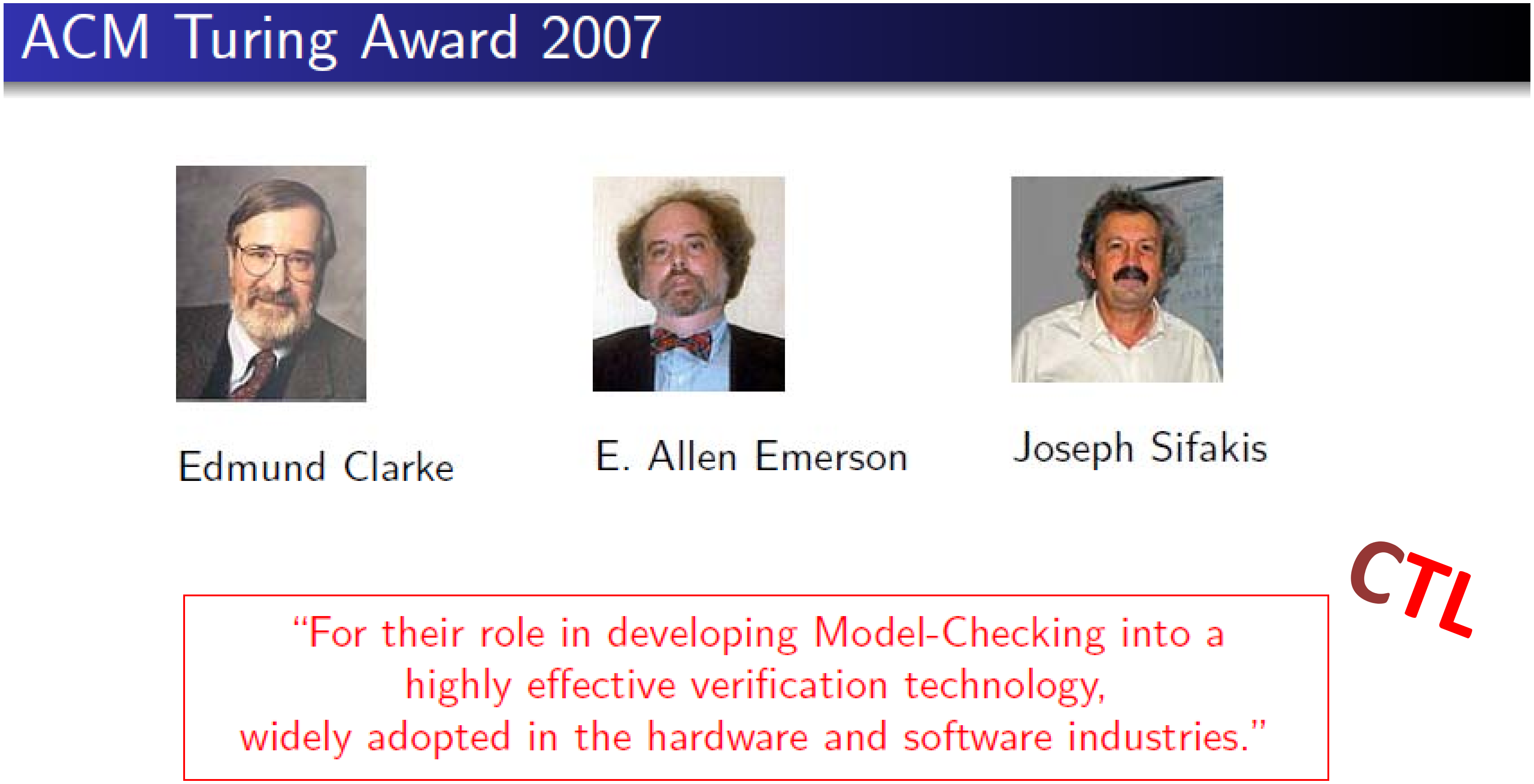
- FDIV = floating point **div**ision unit
- Certain floating point division operations performed produced incorrect results
- Byte: 1 in 9 billion floating point divides with random parameters would produce inaccurate results
- Loss: $\approx$ 500 million US$ (all flawed processors were replaced) + enormous image loss of Intel Corp.
- Source: flawless realization of floating-point division

Model Checking (overview)



''not biased towards the most probable scenarios''

Model Checking



ACM Turing Award 2007

Edmund Clarke

E. Allen Emerson

Joseph Sifakis

"For their role in developing Model-Checking into a highly effective verification technology, widely adopted in the hardware and software industries."

CTL

Some other winners: Pnueli, Milner, Hoare, Scott, Cook, Dijkstra

Model Checking

Gödel Prize 2000

Moshe Vardi

Pierre Wolper

LTL

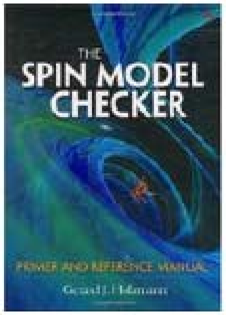
"For work on model checking with finite automata."

Some other winners: Shor, Sénizergues, Agrawal et al., . . .

Model Checking

ACM System Software Award 2001

Gerard J. Holzmann

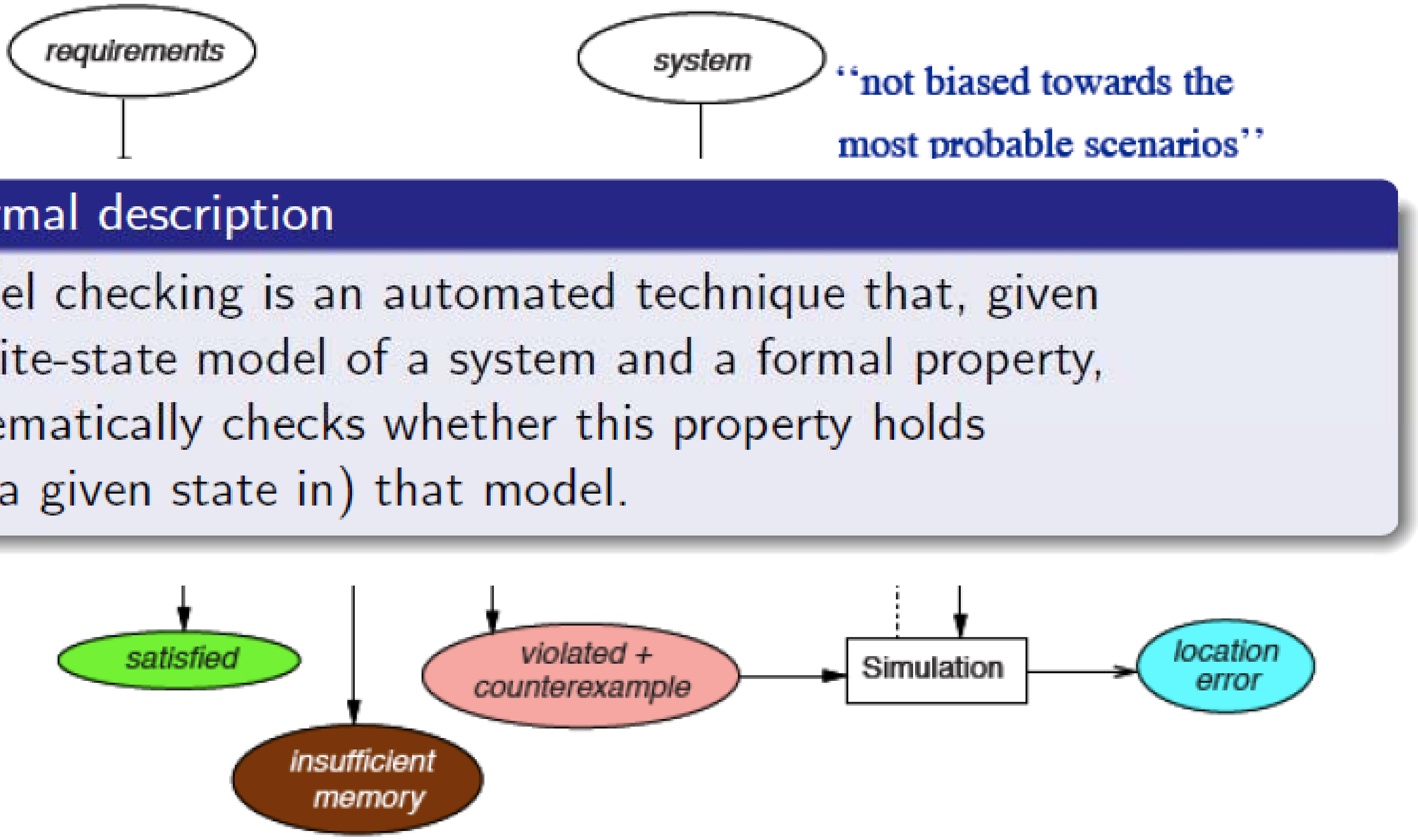


SPIN book

SPIN is a popular open-source software tool, used by thousands of people worldwide, that can be used for the formal verification of distributed software systems.

Some other winners: TeX, Postscript, UNIX, TCP/IP, Java, Smalltalk

Model Checking (overview)

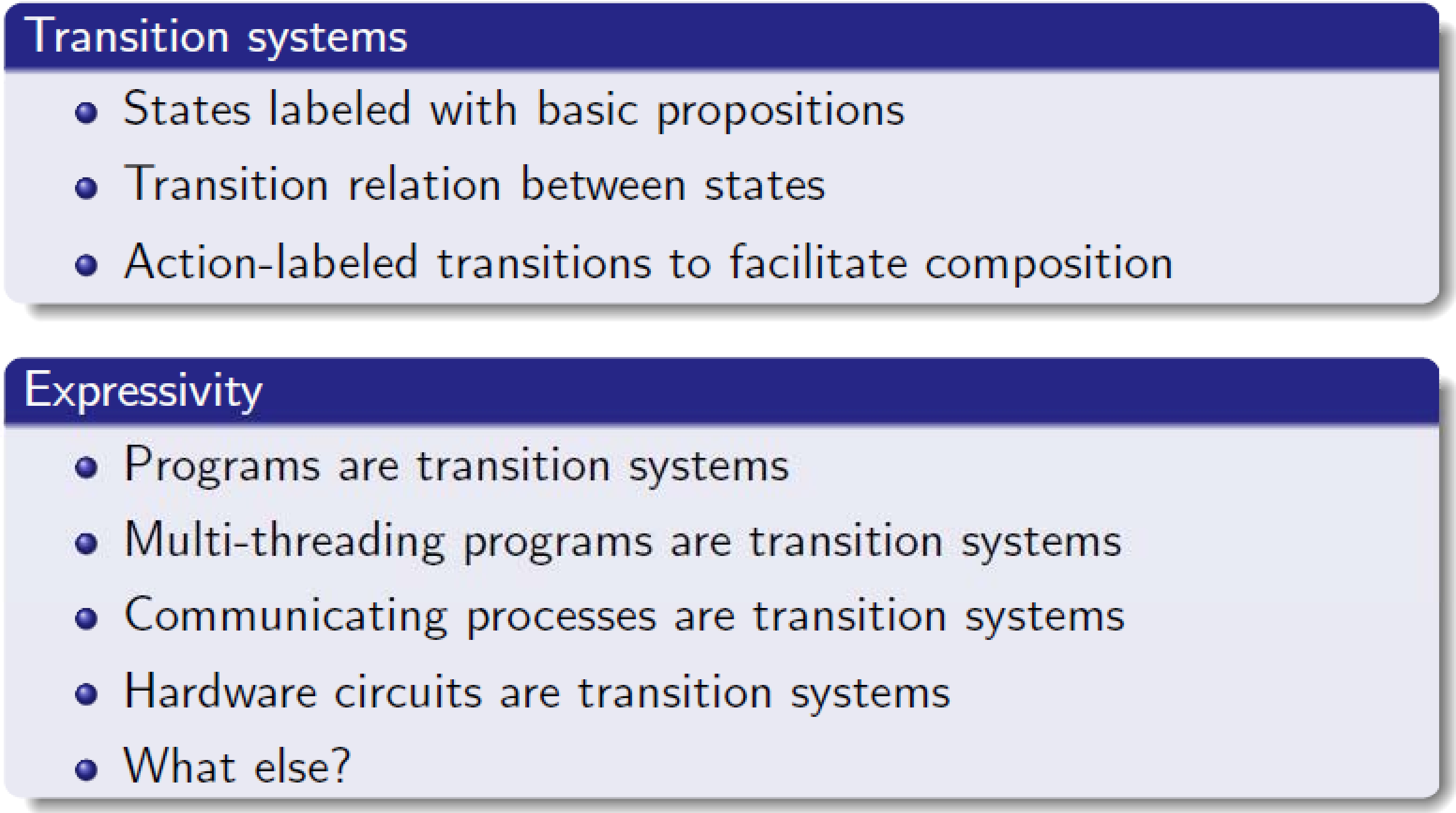


“not biased towards the most probable scenarios”

Informal description

Model checking is an automated technique that, given a finite-state model of a system and a formal property, systematically checks whether this property holds for (a given state in) that model.

What are Models?



Transition systems

- States labeled with basic propositions
- Transition relation between states
- Action-labeled transitions to facilitate composition

Expressivity

- Programs are transition systems
- Multi-threading programs are transition systems
- Communicating processes are transition systems
- Hardware circuits are transition systems
- What else?

What are Properties

Example properties

- Can the system reach a deadlock situation?
- Can two processes ever be simultaneously in a critical section?
- On termination, does a program provide the correct output?

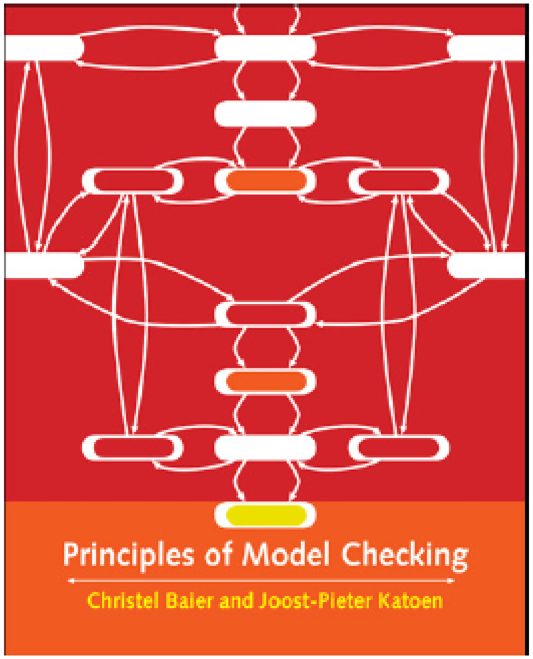
Temporal logic

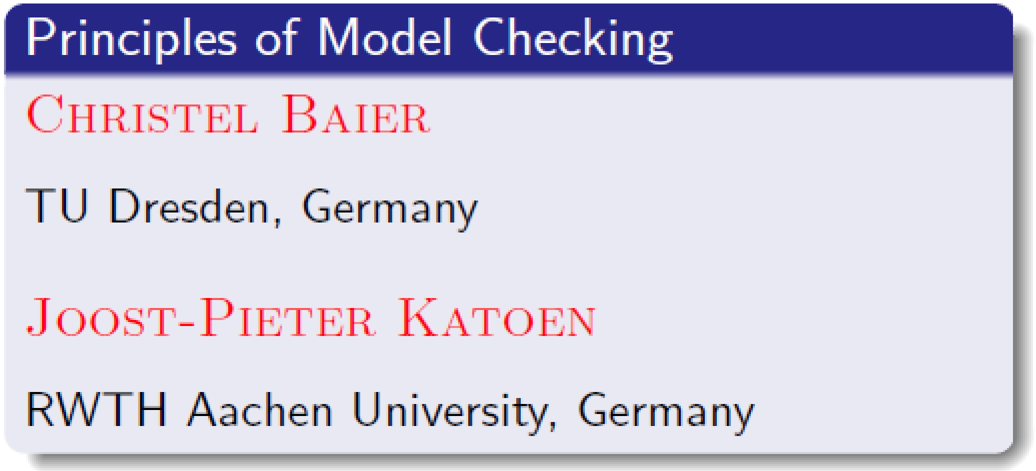
- Propositional logic
- Modal operators such as $\Box$ “always” and $\Diamond$ “eventually”
- Interpreted over state sequences (linear)
- Or over infinite trees of states (branching)

Course Topics

1. What are **properties**?
   - Safety: *something bad will never happen*
   - Liveness: *something good will eventually happen*
1. Regular Properties and **Automata**
   - Finite-state automata and regular safety
   - Büchi Automata and ω-regular properties
2. How to express properties succinctly?
   - Linear Temporal Logic (**LTL**): Syntax & Semantics
   - Expressivity & Algorithms
3. How to express properties succinctly?
   - Computational Tree Logic (**CTL**): Syntax & Semantics
   - Expressivity & Algorithms

Course Material


Principles of Model Checking
Christel Baier and Joost-Pieter Katoen



Principles of Model Checking

Christel Baier

TU Dresden, Germany

Joost-Pieter Katoen

RWTH Aachen University, Germany