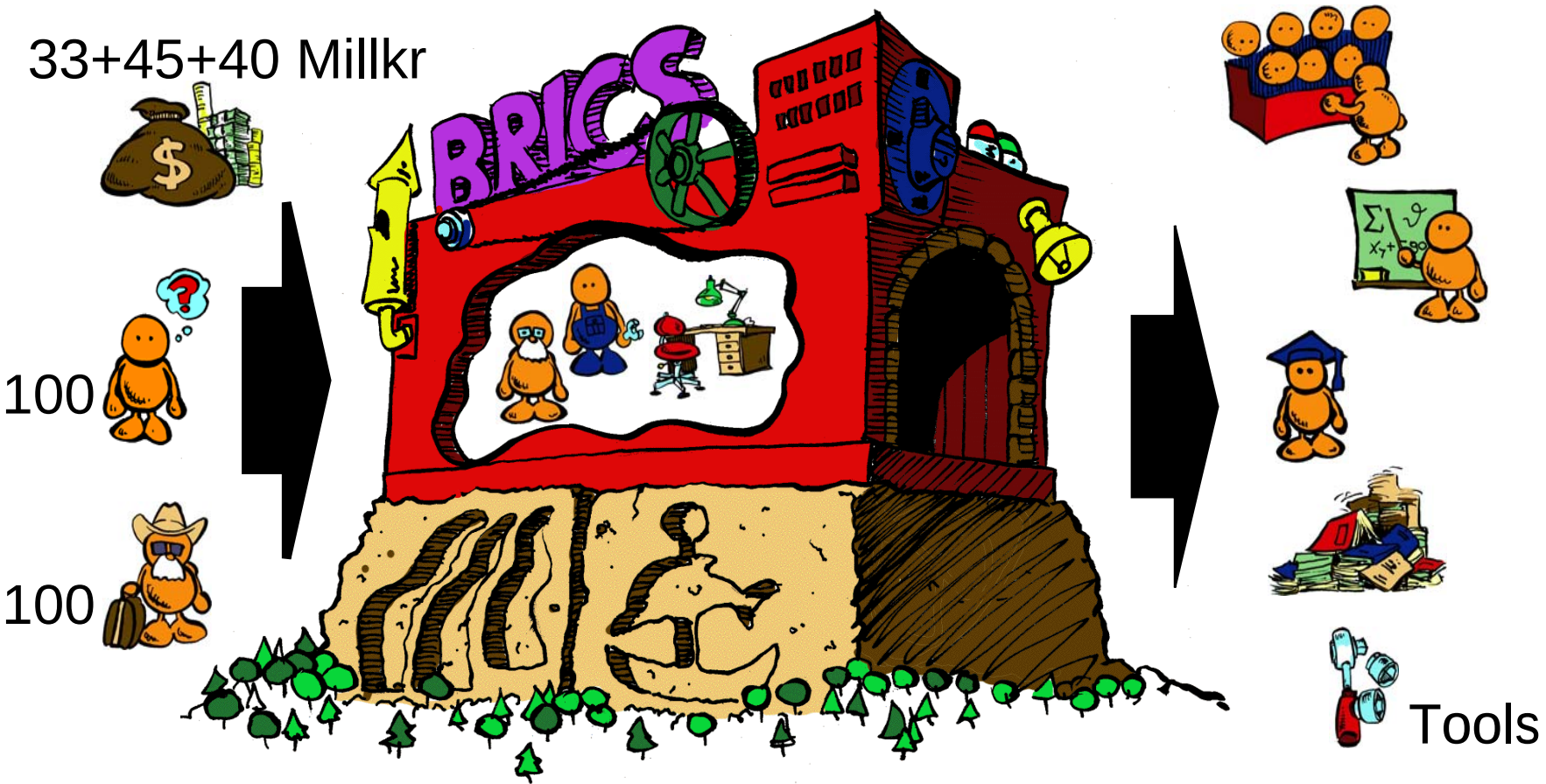
# Model Checking

Kim Guldstrand Larsen


BRICS
Basic Research
in Computer Science

# BRICS Machine

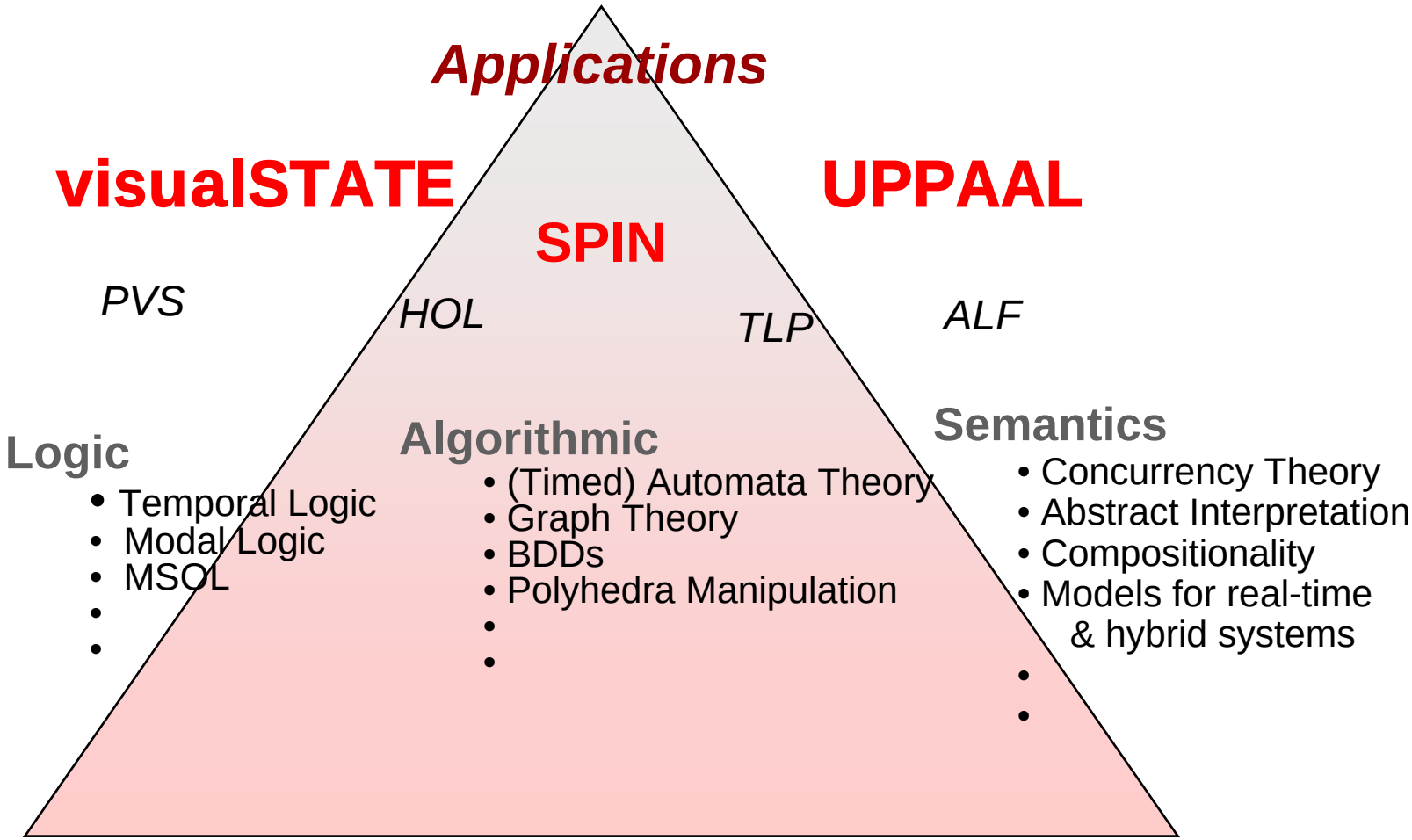
*Basic Research in Computer Science, 1993-2006*



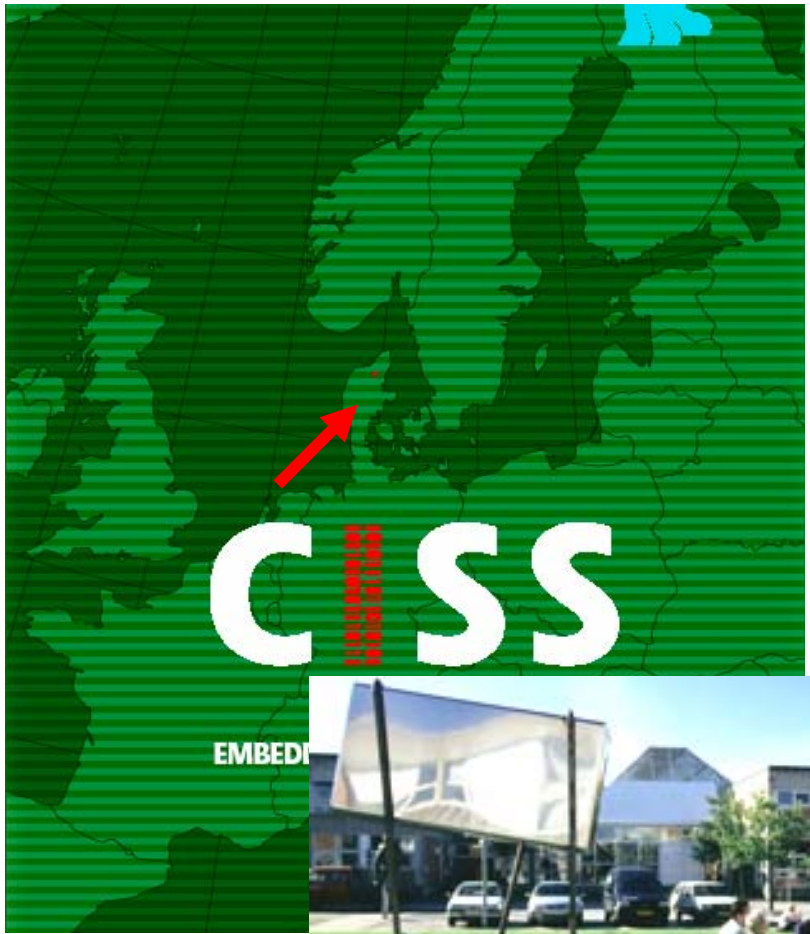

Other revelvant projects
**ARTIST, AMETIST**

BRICS
Basic Research
in Computer Science

# Tools and BRICS



# CISS: *Center for Embedded Software Systems*






**Kim Guldstrand Larsen**
kgl@cs.auc.dk
96358893

or

**CISS**
www.ciss.dk
info@ciss.dk
96357220

Aalborg Universitet
Fr. Bajersvej 7B
9220 Aalborg Ø

BRICS
Basic Research
in Computer Science

# Why CISS ?

- 80% of all software is embedded
- Demands for
  increased functionality
  with
  minimal resources
- Requires multitude of skills
  - Software construction
  - hardware platforms,
  - communication
  - testing & verification

- **Goal**:
  Give a qualitative lift to current industrial practice
  !!!!!

BRICS
Basic Research
in Computer Science

# CISS in Numbers

- Jutland-Fun IT-initiative, 2002:

  **25,5** mil. kr Ministry
  **6** mil. kr North Jutland
  **6** mil. kr Aalborg City
  **12,75** mil. kr Companies
  **12,75** mil. kr AAU

- **26** projects
- **20** CISS employees
- **25** CISS associated researcher at 3 different research groups at AAU

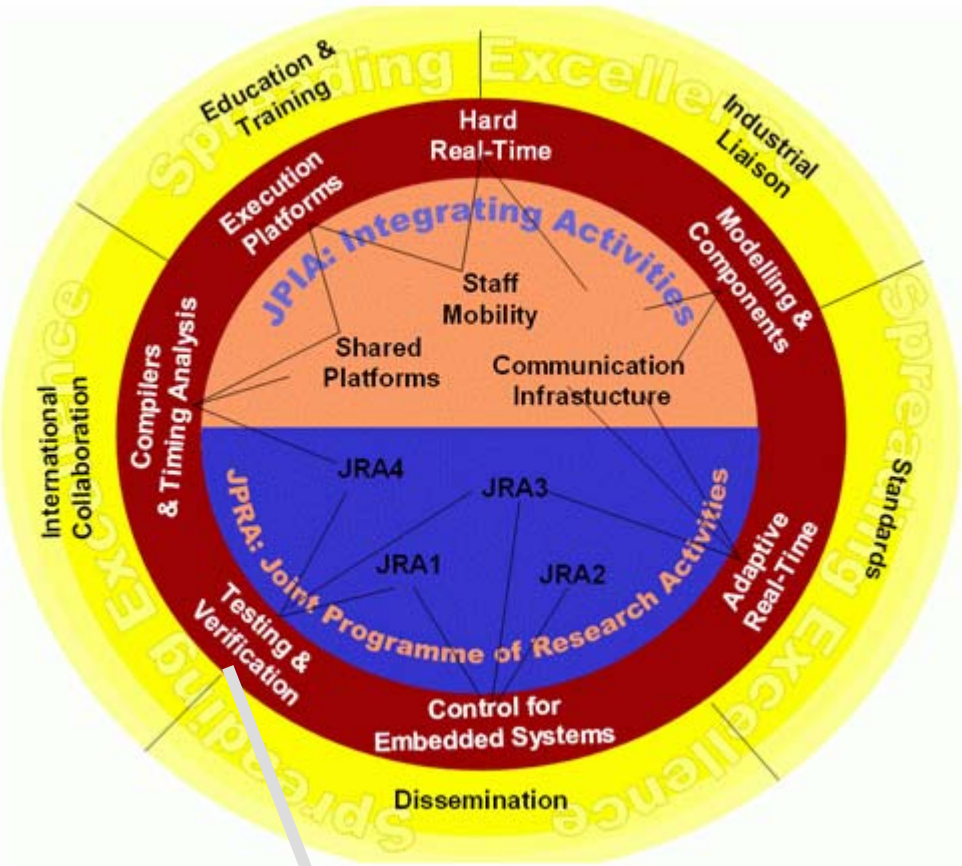
- 16 industrial PhDs

BRICS
Basic Research
in Computer Science

# ARTIST2 European Network of Excellence

6,5MEuro, 32 partners

Information Society Technologies



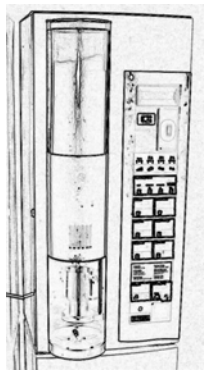

EU's 7th Framework
→
ARTEMIS Research Platform
→
Centers of Excellence

**Testing & Verification**
**CISS koordinator**

BRICS Basic Research in Computer Science

# Modelling Checking

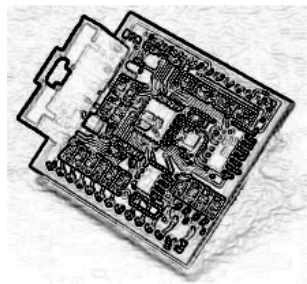
## Plant
*Continuous*



sensors

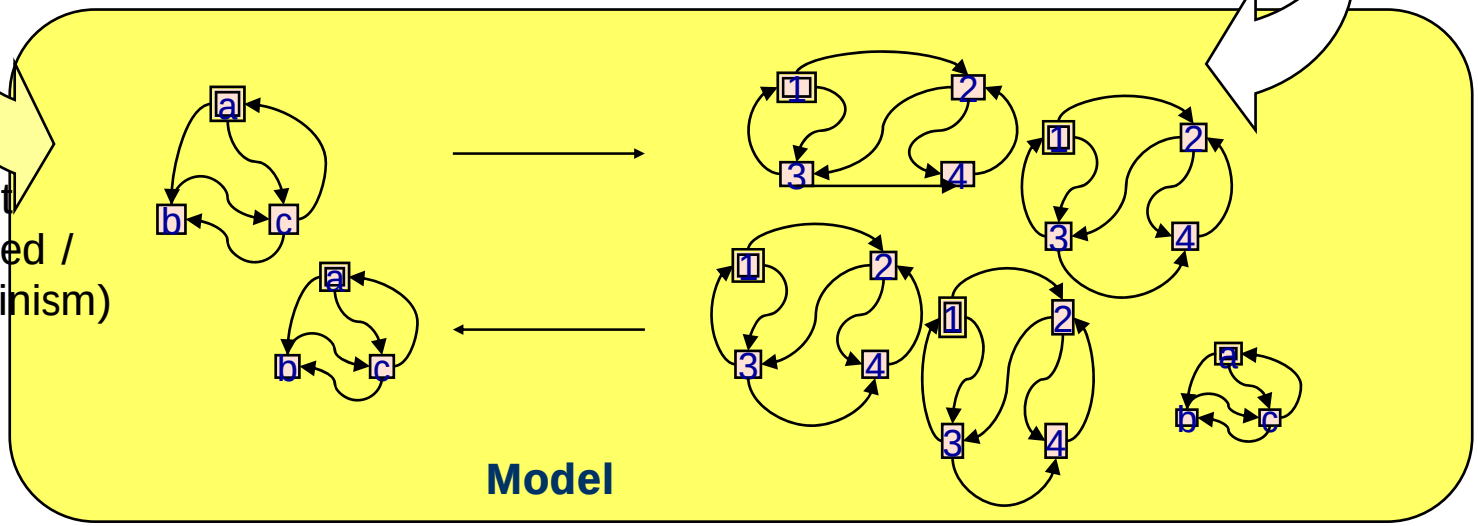
actuators

## Controller Program
*Discrete*



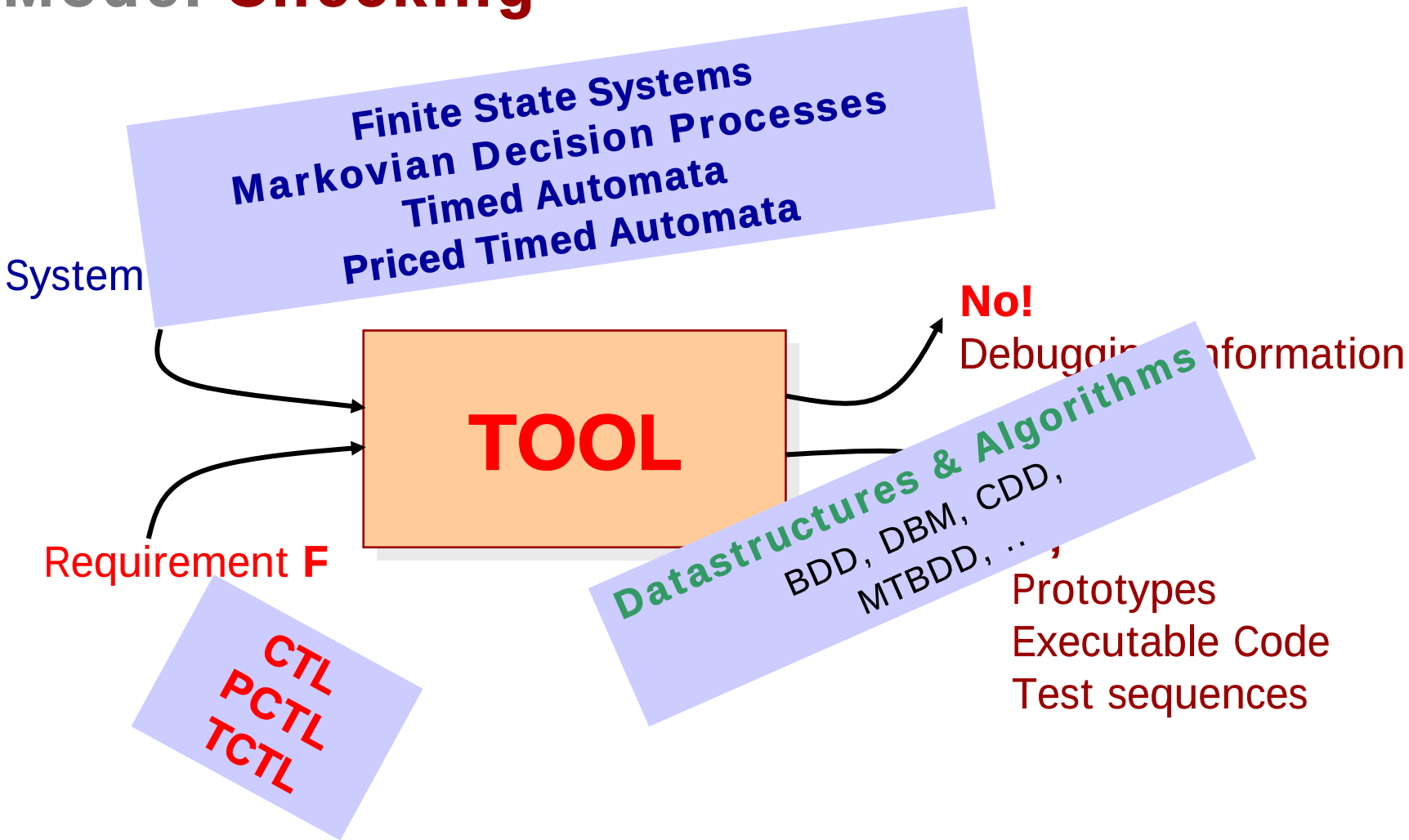
Model of tasks (automatic?)

Model of environment (user-supplied / non-determinism)




BRICS Basic Research in Computer Science

# Model Checking




**Tools:** **UPPAAL, visualSTATE, PRISM, RAPTURE**, SPIN, Statemate, Verilog, Formalcheck,...

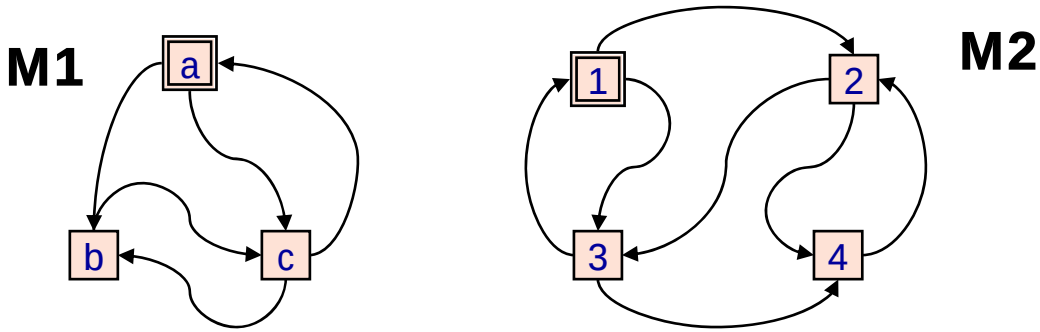
# Benfits of Model Checking

- General Verification aaproach (hardware, embedded systems, software)
- Support of partial verificiation.
- Insensitive to likelihood of error (in contrast to testing).
- Provision of diagnostic information
- Push-button technology
- Rapidly increasing interest by industry (in particular hardware and embedded systems).
- Shorten development time.
- Easily integrated in existing development cycle.
- Not too step learning curve.
- Sound and mathematical underpinning.

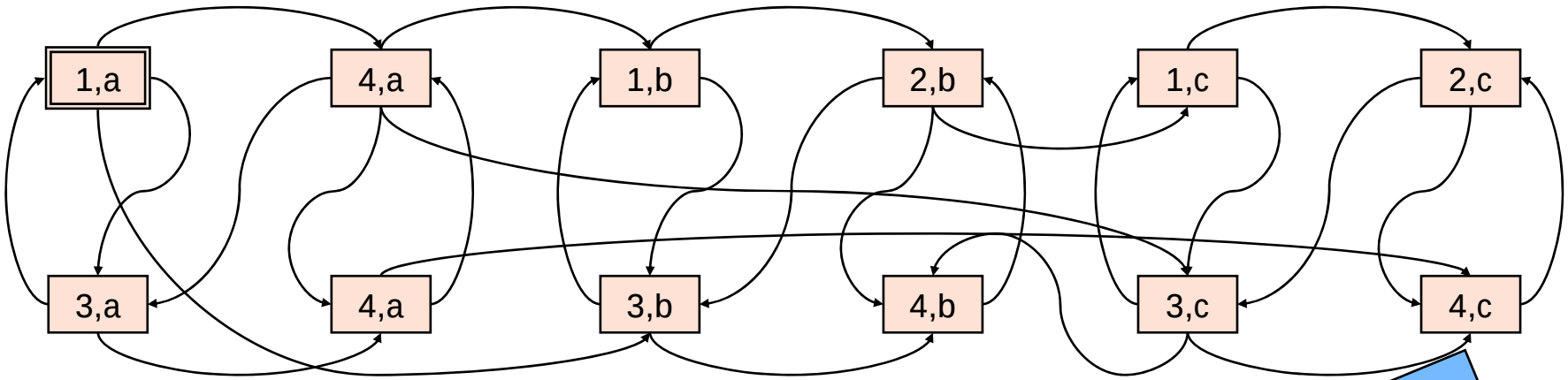
# Weaknesses of Model Checking

- Mainly appropriate to control-intensive and less to date-intensive applications.
- Limited by decidability issues.
- Verification of *system model* and not actual system.
- Only check for *stated properties.*
- Suffers from *state-explosion.*
- Requires expertice in finding appropriate abstractions and requirements.
- Model checkers may themselves have bugs.
- Verification of instances with specific parameters and no. of components.

# ‘State Explosion’ Problem




M1 x M2




**All combinations: exponential in no. of components**

**Provably theoretical intractable**

BRICS Basic Research in Computer Science

# Overview (Day 1)

- **Finite State Model Checking**
  - Kripke Structures
  - CTL: Computational Tree Logic
  - Explicit Model Checking Algorithms
- **Symbolic Model Checking**
  - Binary Decision Diagrams
  - Symbolic Model Checking of CTL
  - Compositional Backwards Reachability
- **Probabilistic Model Checking**
  - Discrete Time Markov Chains & Decision Processes
  - Probabilistic Reachability
  - Probabilistic CTL
  - Abstraction/Refinement

# Overview (Day 2)

- **Real Time Model Checking**
  - Timed Automata
  - Timed CTL
- **Symbolic Real Time Model Checking**
  - Regions and Zones
  - Symbolic Reachability Checking
  - Symbolic Liveness Checking
- **Further Optimizations**
  - Abstractions & Approximate Analyses
  - Modelling Patterns
  - ...
- **Optimal Scheduling using Model Checking**
  - Priced Timed Automata, Priced Zones
  - Optimal Reachability
  - Optimal Safety

# Reading Material

- Consult CAV'06: "25 Years of Model Checking".

- R. Bryant: *Symbolic Boolean Manipulation with Ordered Binary Decision-Diagrams.* ACM Computmg Surveys, Vol. 24, No. 3 September 1992.
- Jørgen Staunstrup, Henrik Reif Andersen, Kim G. Larsen, Henrik Leerberg, Niels Bo Theilgaard et al.: *Practical Verification of Embedded Software.* IEEE Computer May 2000.
- J.L-Nielsen, G. Behrmann, H. R. Andersn, H. Hulgaard, K. Kristoffers, K.G. Larsen: *Verification of Large State/Event Systems Using Compositionality and Dependency Analysis.* Formal Methods in System Design, 18, 5–23, 2001
- H.Hansson, B.Jonsson: *A Logic for Reasoning about Time and Reliability.* Formal Aspects of Computing (1994) 6:512-535.

# Reading Material

- G. Behrmann, A. David, K.G. Larsen: *Tutorial on UPPAAL* (see www.uppaal.com)
- J. Bengtsson, W. Yi: *Timed Automata: Semantics, Algorithsm and Tools.* (see www.uppaal.com).
- G. Behrmann, K. G. Larsen, J. I. *Rasmussen:Optimal Scheduling Using Priced Timed Automata.* ACM SIGMETRICS Performance Evaluation Review, vol. 32, nb. 4, 2005, pp. 34-40, ACM Press.

- BOOKS:
  - *Model Checking* by Ed Clarke, Orna Grumberg, Doron Peled
  - *Systems and Software Verification* by B. Berard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, P. Schnoebelen
  - *Reactive Systems: Modelling, Specification and Verification* by L. Aceto, A.Ingolfsdottir, K.G. Larsen, J.Srba
    coming soon at a book-store near you.