

# The ASAP Platform:

Next Generation Tool Support for State Space Analysis

*Invited tutorial*

Lars M. Kristensen  
Michael Westergaard

Department of Computer Science  
University of Aarhus  
DENMARK  
{kris,mw}@daimi.au.dk



UNIVERSITY OF AARHUS

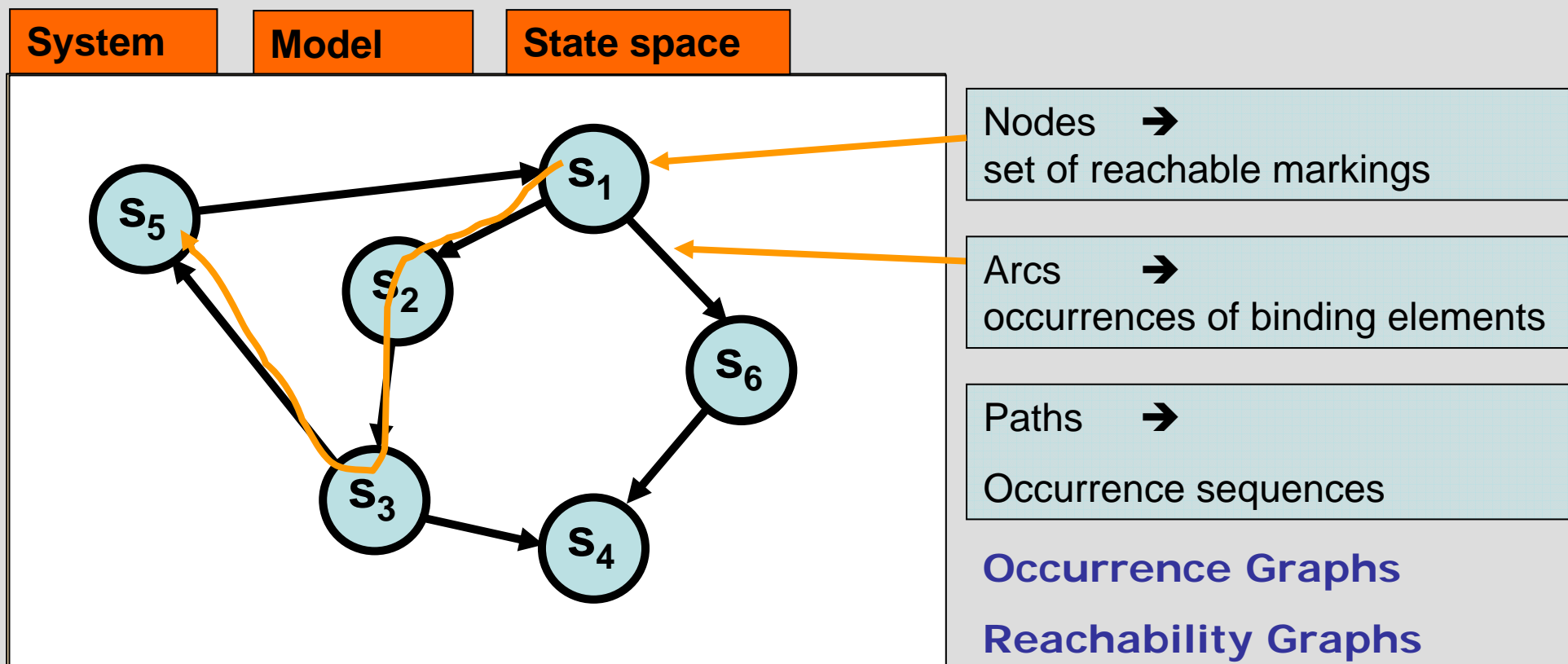
Department of Computer Science

1

CPN Workshop 2007

# State Space Analysis

- One of the main approaches to model-based **verification** of finite-state concurrent systems:



# Example

- Fra CPN bog?



# State Space Analysis

## ■ Advantages:

- Highly automatic support by computer tools.
- Rich set of behavioural properties can be analysed.
- Much of the underlying mathematics can be hidden.
- Counter examples and diagnostics information.
- Even **partial state spaces** provide a systematic and effective error-detection technique.

## ■ Disadvantages:

- Verification relative to specific system configuration.
- Inherent **state explosion problem**.

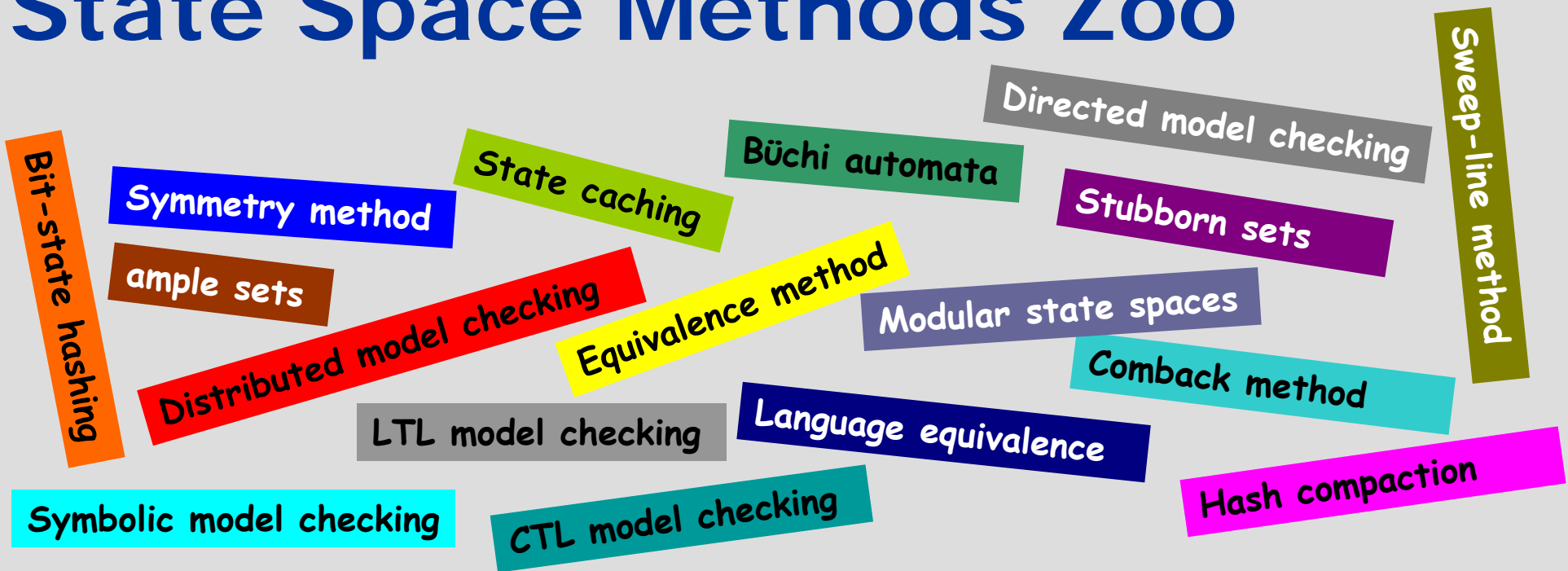
## ■ Wide range of state space methods and techniques have been developed.



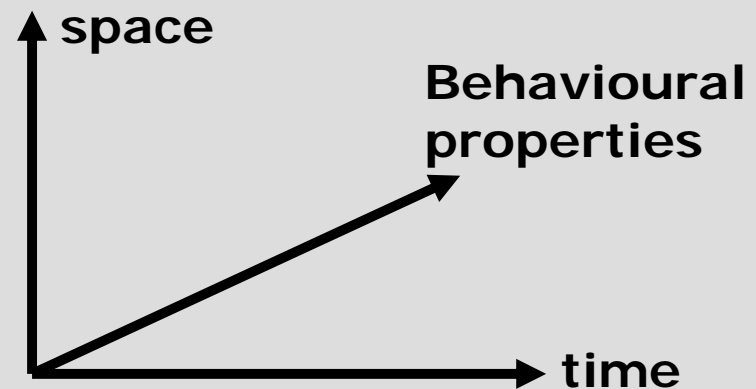
**Well, let's see if Jimmy here can help you with your state explosion problem!**



# State Space Methods Zoo



- Mostly modelling language independent.
- Typically exploits specific system characteristics.



# Computer Tools

- State space methods can now be used to validate industrial-sized practical systems.
- No state space method works well on all systems.
- Active research area: tomorrow will bring even better state space methods and techniques.
  
- A computer tool must support a wide range of state space methods.
- A computer tools must provide a platform for continuously extending the supported methods.



# Brief History of State Space Tool Support for Coloured Petri Nets

- **1G - Occurrence Graph Analyzer (OGA) [1992 - 1994]:**
  - Stand-alone tool based on loading SML images from Design/CPN.
  - Standard ML interface and implementation.
  - Supported full state spaces and simple visualisation.
- **2G - Design/CPN Occurrence Graph Tool [1994 - 2003]:**
  - Integration of OGA into Design/CPN.
  - Direct support in the graphical user interface.
  - Prototype implementations of equivalence and symmetry method, time condensed state space, and sweep-line method.
- **2.5G - CPN Tools [since 2003]:**
  - Port of Design/CPN Occurrence Graph Tool to CPN Tools.
  - Based on the faster simulation engine used in CPN Tools.
- **The software architecture made it difficult to support a collection of state space methods in a coherent manner.**



# What is ASAP?

- Next generation of computer tool support for state space analysis of CPN models.
- Developed in the ASCoVeCo research project:

**ASCoVeCo** Advanced State Space Methods and Computer Tools for Verification of Communication Protocols

**ASAP** ASCoVeCo State Space Analysis Platform

- Supported by the Danish Research Council for Technology and Production (2006 - 2009).
- Project members:
  - Lars M. Kristensen
  - Michael Westergaard
  - Sami Evangelista
  - Paul Fleischer
  - Mads K. Kjeldsen
  - Surayya Urazimbetova



# ASCoVeCo Project Objectives

- Development of new state space methods for reasoning about communication protocols.
- Algorithms and data-structures for space and time efficient implementation of state space methods.
- Design and implementation of a new state space exploration tool for Coloured Petri Nets.
- Industrial case-studies evaluating the methods and developed computer tools in practice:
  - TietoEnator, Denmark and Nokia Research, Finland.



# ASAP – Aim and Vision

- **A state space analysis tool and development platform aimed at:**
  - Research: implementation and experiments.
  - Education: user perspective and implementation perspective.
  - Industrial use: ease of use, stability, highly automatic, pragmatics methods.
- **The challenge: how to support all this in a coherent manner with a suitable user interface.**



# ASAP Fundamentals (1)

- Conducting state space analysis consists of creating and managing **verification projects**.
- A verification project consists of:
  - CPN models to be analysed.
  - Queries expressing behavioural properties.
  - Verification jobs coupling models, state space exploration methods, and queries.
  - Results of executing verification jobs.
- Eclipse Rich Client Platform provides the foundation for the user interface.

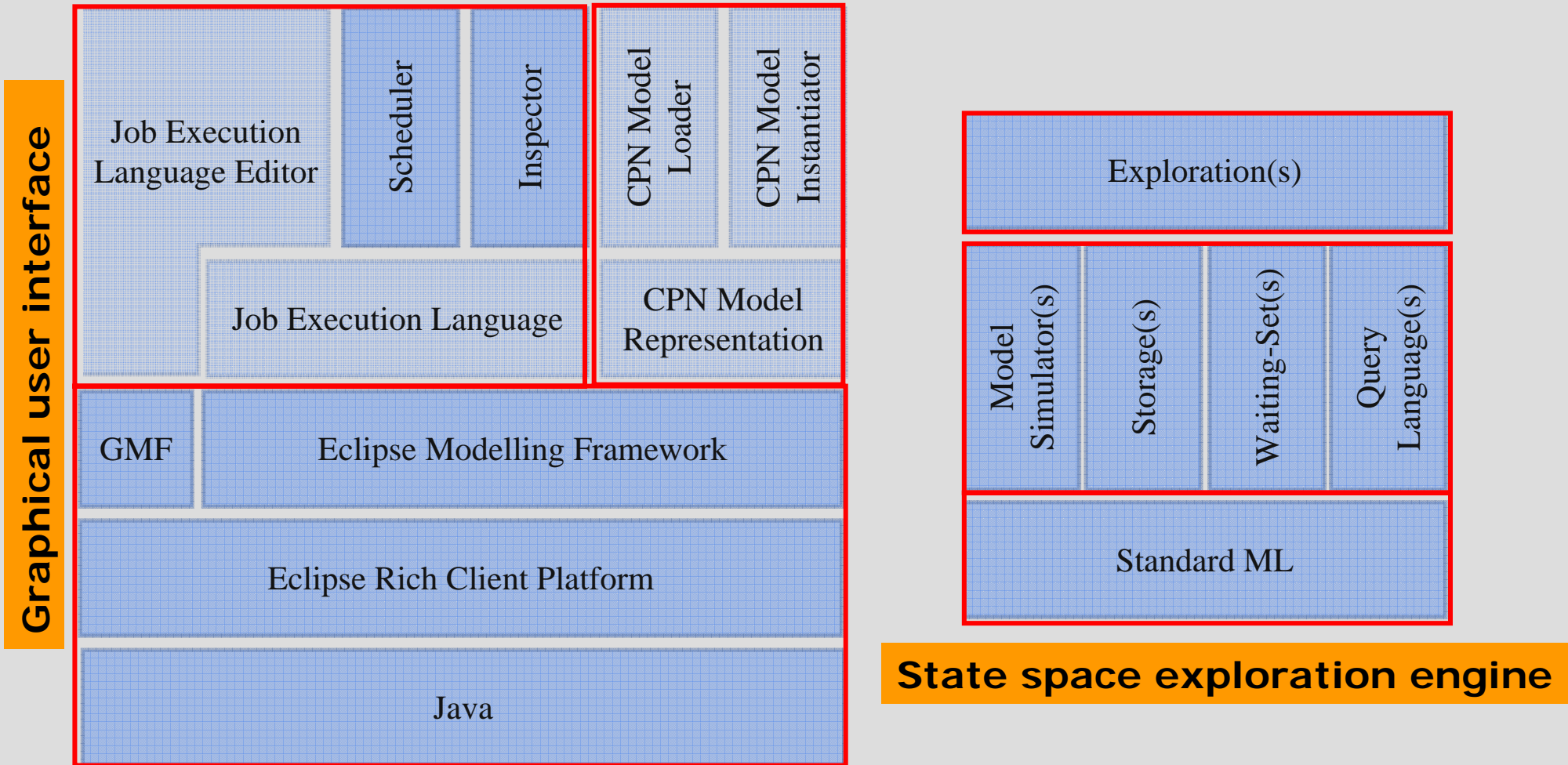


# ASAP Fundamentals (2)

- **ASAP GUI is not an integrated part of CPN Tools:**
  - CPN Tools GUI implemented in the BETA programming language.
  - Resources required to maintain and further develop GUI Framework of CPN Tools.
  - ASAP can load CPN models created with CPN Tools.
- **One common set of query languages:**
  - Separate behavioural properties and queries from the state space methods used to check them.
- **ASAP currently relies on the CPN Tools simulator:**
  - No CPN semantical gap between CPN Tools and ASAP.
  - State space methods (initially) implemented in Standard ML.
  - ASAP provides a model simulator interface to the CPN simulator.
- **Runs on Windows XP/Vista, Linux, and Mac OS X.**



# Software Architecture



# Tutorial outline

## Part A: Graphical user interface

- Demonstration of ASAP
- The Verification Job Execution Language (JEL)
- Eclipse Rich Client Platform

**10.30 – 11.00 Coffee and tea break**

## Part B: State space exploration engine

- Model simulator interface
- Test-suite and benchmarking tool
- The ComBack state space exploration method
- Outlook

