Coloured Petri Nets

Modelling and Validation of Concurrent Systems

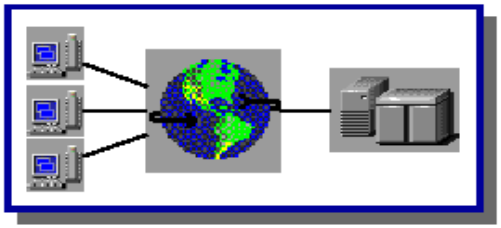
Chapter 1: Introduction to Modelling and Validation

Kurt Jensen &
Lars Michael Kristensen

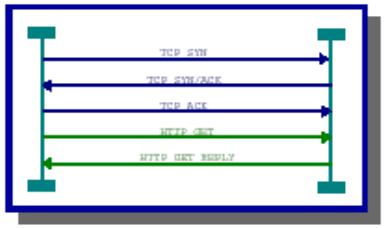
{kjensen,lmkristensen}
@daimi.au.dk

Motivation

- Many system development projects are concerned with concurrent systems:



Internet and WWW



Communication Protocols

Embedded Systems

- The behaviour of concurrent system is complex (concurrency and non-determinism):
  - The scheduling of the processes involved.
  - Messages may be lost in transmission.
  - Input received from the environment.

- Concurrent systems are challenging to design, test, and debug.

Example: NASA PathFinder

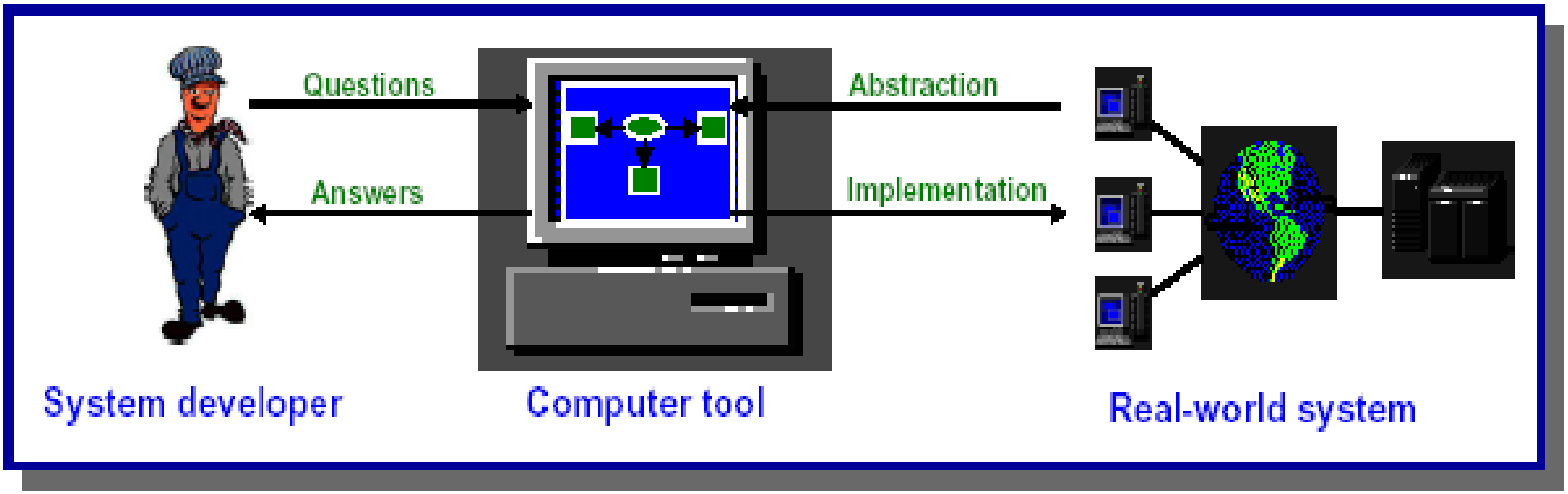
- Landed on planet Mars on July 4, 1997.
- Collection of meteorological data.

- System resets due to priority inversion.

http://research.microsoft.com/~mbj/Mars_Pathfinder/

Model-based development

- Based on the construction of executable models:



Construction and validation

- Benefits of constructing a model:
  - Insight into the design and operation of the system.
  - Completeness: Results in a more complete design.
  - Correctness: reveal errors and ambiguities in the design phase.

- Properties can be validated prior to implementation:
  - Functional properties (e.g., deadlocks, timing requirements,...).
  - Performance properties (e.g., delay, throughout, scalability,...).

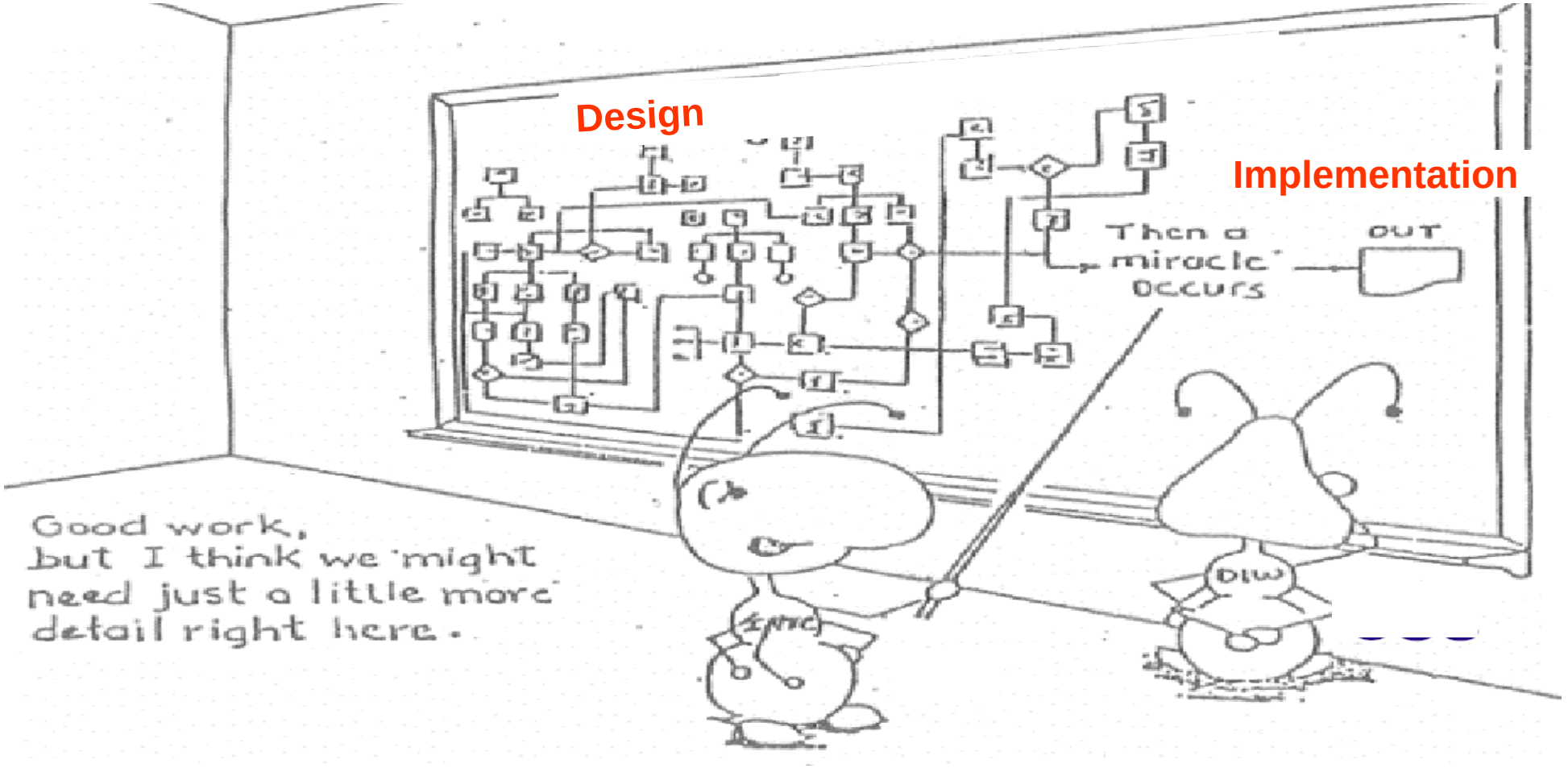
Example: IPv6 edge router discovery protocol

- Developed at Ericsson Telebit A/S.
- Modelling construction phase:

Category	Review 1	Review 2	Total
Incompleteness and ambiguity	3	6	9
Errors in the protocol	2	7	9
Simplifications	2	0	2
Additions	4	0	4
Total	11	13	24

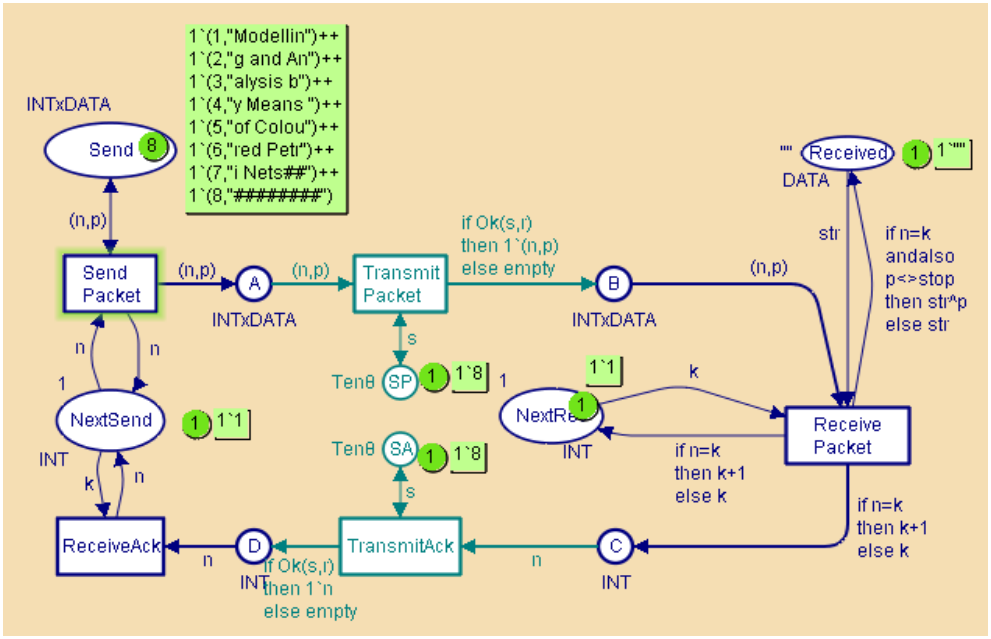
- State space analysis: 4 additional subtle errors.

From design to implementation



Coloured Petri Nets

- Graphical modelling language for concurrent systems.
- Combination of *Petri Nets* and *programming language:*



Petri Nets:

- concurrency
- control structures
- synchronisation
- communication
- resource sharing

CPN ML (Standard ML):

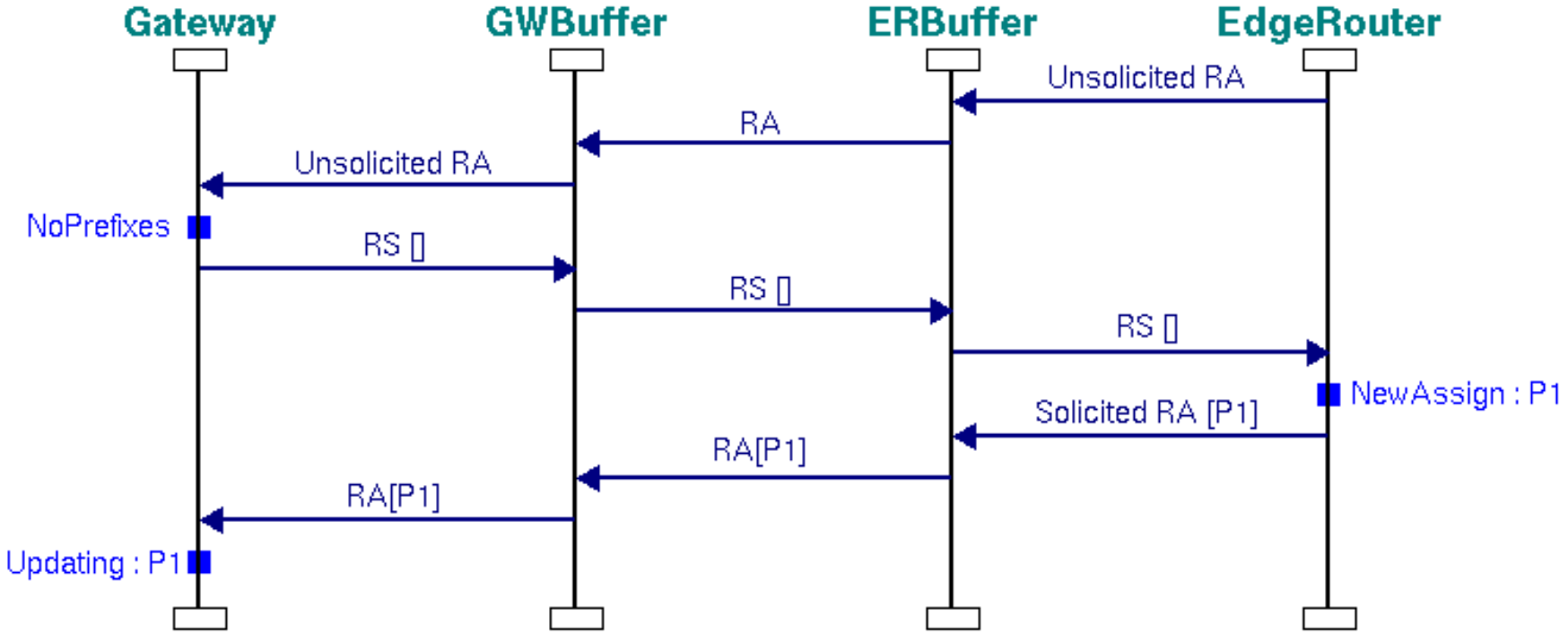
- data manipulation
- compact modelling

Modelling and validation

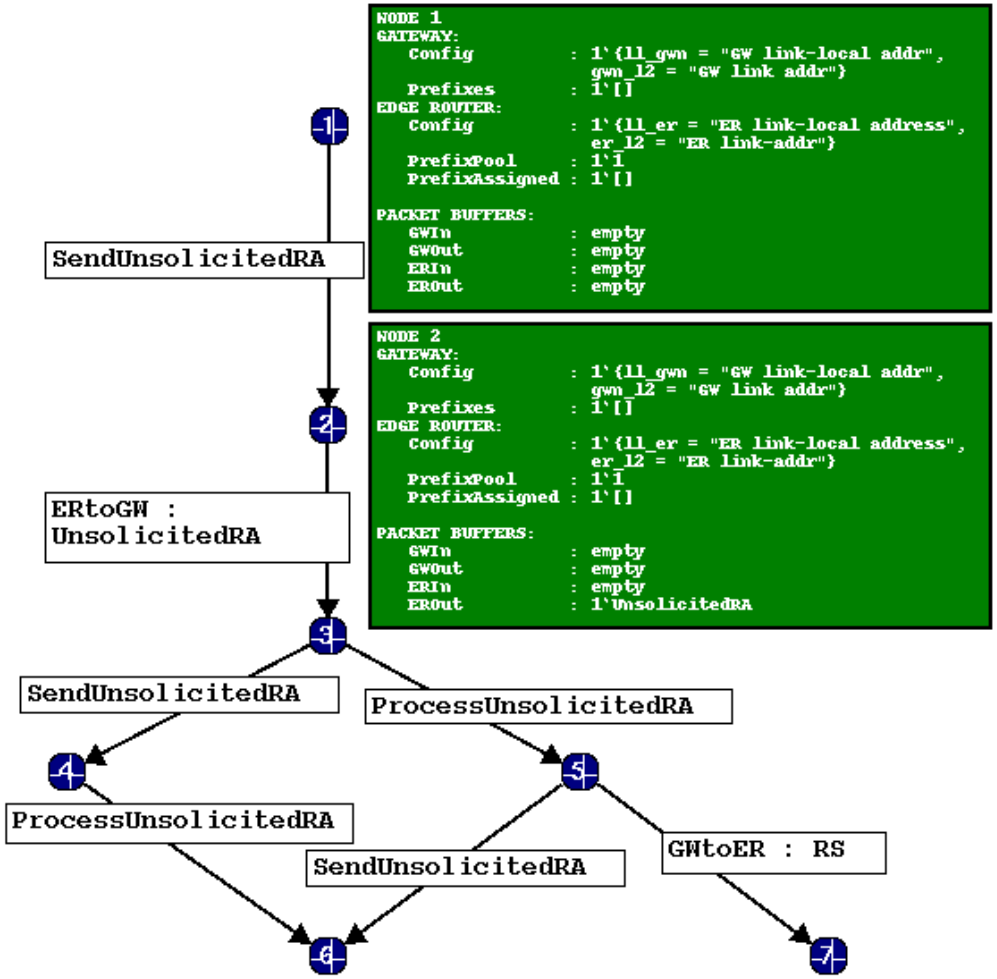
- Modelling:
  - CPN models are executable (aimed at behavioural modelling).
  - A small set of basic modelling constructs and concepts.
  - CPN models can be structured into modules.
  - CPN models can be timed.

- Validation:
  - Interactive- and automatic simulation.
  - Application domain visualisation.
  - Simulation-based performance analysis.
  - State space analysis and verification (model checking).

Visualisation



Verification by means of state spaces



Syntax and semantics

- Formal syntax and semantics:
  - Basis for simulation (execution) of the CPN models.
  - Basis for the formal verification methods (state spaces).
  - Basis for the implementation of CPN Tools.
- Not necessary for a user to know the formal definition.

- Construction and simulation of CPN models requires:
  - An understanding of the syntax and semantics of CP-nets.
  - Programming in the CPN ML language (~Standard ML).
  - Using the editing and simulation facilities of CPN Tools.
- Similar to learning a new programming language.

Application areas

Protocols and Networks

- Allocation Policies in the Fieldbus Protocol in Japan
- IEEE 802.6 Configuration Control at Telstra Research Labs
- ISDN Services at Telstra Research Laboratories
- Protocol for an Audio/Video System at Bang & Olufsen
- TCP Protocols at Hewlett-Packard
- Local Area Network at University of Las Palmas
- UPC Algorithms in ATM Networks at University of Aarhus
- BRI Protocol in ISDN Networks
- Network Management System at RC International A/S
- Interprocess Communication in Pool IDA at King's College

Software

- Mobile Phones at Nokia
- Bank Transactions & Interconnect Fabric at Hewlett-Packard
- Mutual Exclusion Algorithm at University of Aarhus
- Distributed Program Execution at University of Aarhus
- Internet Cache at the Hungarian Academy of Science
- Electronic Funds Transfer in the US
- Document Storage System at Bull AG
- ADA Program at Draper Laboratories

Control of Systems

- Security and Access Control Systems at Dalcotech A/S
- Mechatronic Systems in Cars at Peugeot-Citroën in France
- European Train Control System in Germany
- Flowmeter System at Danfoss
- Traffic Signals in Brazil
- Chemical Production in Germany
- Model Train System at University of Kiel

Hardware

- Superscalar Processor Architectures at Univ. of Newcastle
- VLSI Chip in the US
- Arbiter Cascade at Meta Software Corp.

Military Systems

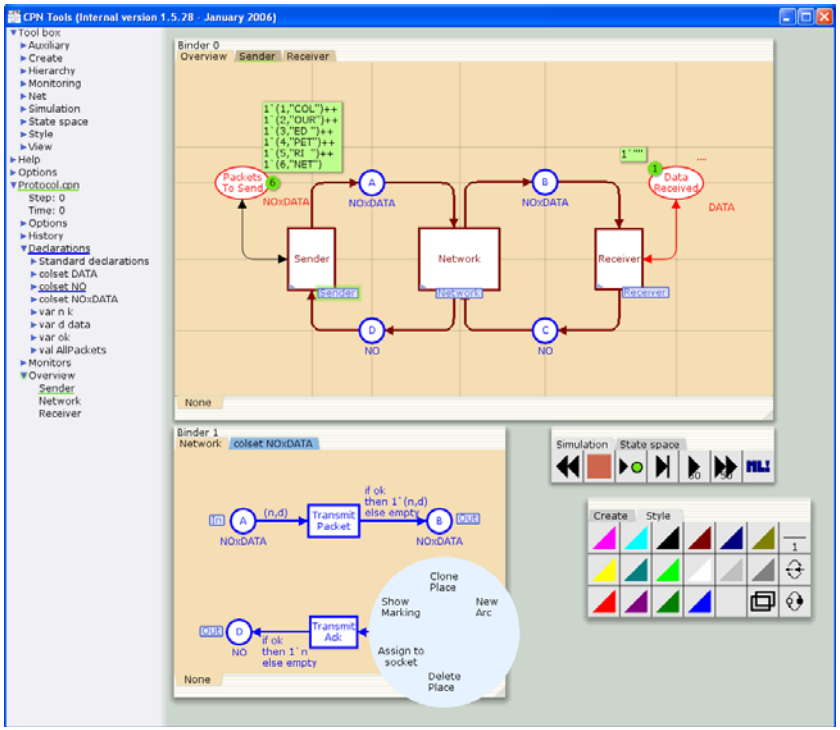
- Military Communications Gateway in Australia
- Influence Nets for the US Air Force
- Missile Simulator in Australia
- Naval Command and Control System in Canada

Other Systems

- Bank Courier Network at Shawmut National Coop.
- Nuclear Waste Management Programme in the US

Computer tools for CP-nets

- Modelling and validation are supported by CPN Tools.
- Supports:
  - Editing and syntax check.
  - Interactive- and automatic simulation.
  - State space analysis.
  - Performance analysis.
  - Application domain visualisation.
- Web pages: www.daimi.au.dk/CPNTools
- License available free of charge.



Examples of CPN Tools users

North America

- Boeing
- Hewlett-Packard
- Samsung Information Systems
- National Semiconductor Corp.
- Fujitsu Computer Products
- Honeywell Inc.
- MITRE Corp.,
- Scalable Server Division
- E.I. DuPont de Nemours Inc.
- Federal Reserve System
- Bell Canada
- Nortel Technologies, Canada

Europe

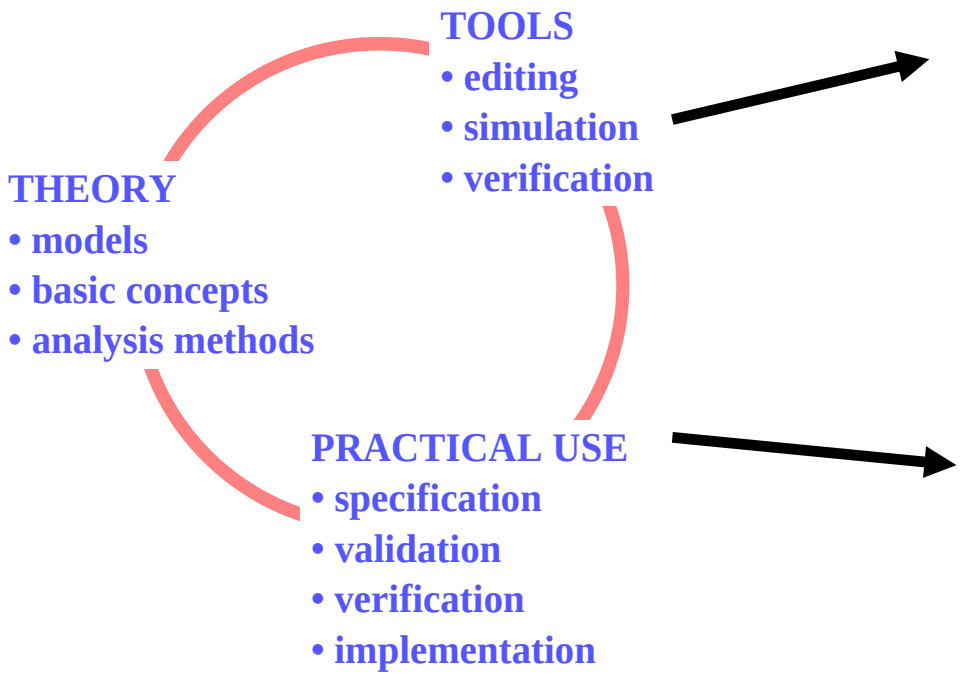
- Alcatel Austria
- Siemens Austria
- Bang & Olufsen, Denmark
- Nokia, Finland
- Alcatel Business Systems, France
- Peugeot-Citroën, France
- Dornier Satellitensysteme, Germany
- SAP AG, Germany
- Volkswagen AG, Germany
- Alcatel Telecom, Netherlands
- Rank Xerox, Netherlands
- Sydkraft Konsult, Sweden
- Central Bank of Russia
- Siemens Switzerland
- Goldman Sachs, UK

Asia

- Mitsubishi Electric Corp., Japan
- Toshiba Corp., Japan
- SHARP Corp., Japan
- Nippon Steel Corp., Japan
- Hongkong Telecom Interactive Multimedia System

Coloured Petri Nets

- **Developed by the CPN Group at the University of Aarhus.**



CPN Tools:

- 6000+ licenses
- 130+ countries

Industrial partners:

- Ericsson Telebit A/S
- Nokia Research
- Kirk Telekom
- Australian Defence

www.daimi.au.dk/CPnets