Analysis of Networked Automation Systems

Georg Frey

JPA² Group at University of Kaiserslautern: People

JPA² Group at University of Kaiserslautern: Research UnB

- Design of Distributed Automation Systems
  - Development Processes based on UML
  - Object-Oriented Automation O²A
  - Design based on IEC 61499
  - Implementation on Networked Devices
  - Object Oriented Simulation of Automation Systems (SIL, HIL)
  - Functionality Based Design using Automation Objects

- **Analysis of Networked Automation Systems**
  - **Simulation**
    - **discrete**
    - **continuous**
  - **Model Checking**
    - **timed**
    - **probabilistic**

Outline UnB

- Motivation
  - Future Directions in Control
  - Networked Automation Systems, NAS
- Analysis of NAS
  - Correctness Notions for NAS
  - Aim of the Analysis: Dependability
- Multi Model Multi Method Approach M⁴
- Introductory Example
- Analysis by Simulation
  - discrete event
  - hybrid
- Analysis by Model-Checking
  - timed
  - probabilistic
- Summary and Outlook

Motivation: Future Directions in Control

UnB

Convergence of C³-Technologies

Conclusions

… The growing synergy between communications, computation and control was noted and it is clear that evolving network technology poses major opportunities and challenges to control theory and methodologies. Questions about the convergence of C3 *technologies* (control, computing and communications) lead today to similar questions about the convergence of *disciplines …"*

[Report on the WORKSHOP ON FUTURE AND EMERGING CONTROL SYSTEMS Organized by Unit E1 Essential Technologies and Infrastructures IST Program European Commission (2000)]

Recommendations

… the Panel developed a list of five major recommendations for accelerating the impact of control.

1. Integrated Control, Computation, Communications

…

Substantially increase research aimed at the *integration* of control, computer science, communications, and networking.

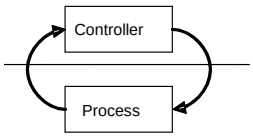
[„Future Directions in Control, Dynamics, and Systems - Control in an Information Rich World" Report of the Panel on Future Directions in Control, Dynamics, and Systems (NSF, 2002)]

2007-05-18
© Georg Frey

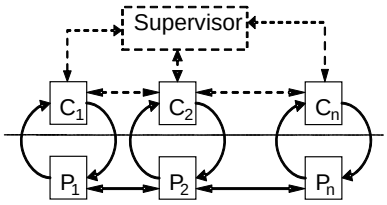
Motivation: Networked Automation System (NAS)

UnB

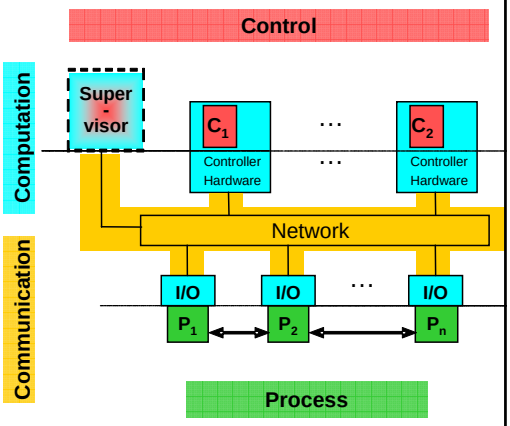
Classic closed loop



Classic distributed control



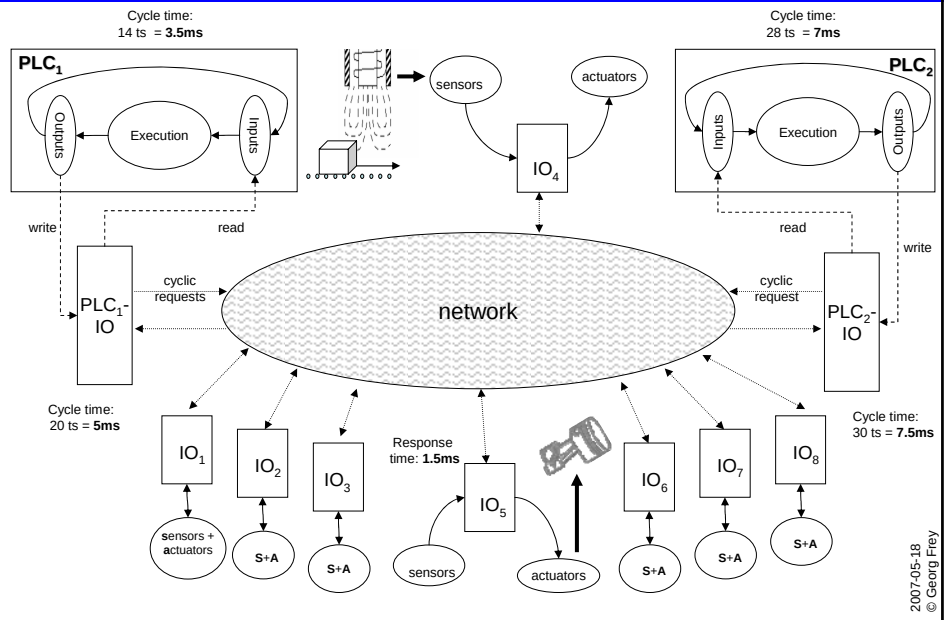
Networked Automation System



2007-05-18
© Georg Frey

Example of Networked Automation System (NAS)

UnB



Correctness Notions for NAS

UnB

- System of Hardware und Software
- Correctness Notion in the SW-Engineering Domain
  - ➢Distinction between functional and non-functional Properties
  - ➢Temporal Behavior is classified as non-functional (I?)
- Correctness Notion in the Real-Time-Computing Domain (Kopetz)
  - ➢Value-Correctness: „*Will the system respond to an input change with the correct output change*“
  - ➢Temporal Correctness: „*Will it do so within the correct time bounds*“
- Value-Correctness is the aim of many research projects in the area of logic control → In the presented work it is considered as given
- *Temporal Correctness is of special importance in NAS*
- Example: ISaGRAF Documentation (IEC 61499 Tool)

  “Delays are added in the communication interface and in the algorithms execution that must be taken into account when designing such a distributed application”.

KOPETZ, Hermann, 2003: *Time-triggered real-time computing.* Annual Reviews in Control, 27(2003), pp. 3-13

Dependability

- includes safety, reliability, quality, tolerance, robustness, availability, (security), …
- e.g.: part rejection rate, reaction on an event in a given time interval
- is influenced by: HW-failures, SW-errors, delays by HW-SW-system, failures in the network, delays by the network
- described by „value-“ and „time-based“ properties

Will the system respond to an input change with the permissible output change?

”A signal change at input A will be followed by the activation of output 5.”

Will the system do so within the permissible time bounds?

”A signal change at input A will be followed by the activation of output 5 within 50ms.”

Time based properties (related to dependability)

Will the system respond to an input change in the permissible time?

- Safety (maximum and minimum {delay} times), e.g. earliest opening of a safty clamp.
- Reliability (Probability of reacting within a given time frame)
- Quality (Distribution of values to be processed)
- Differences, distances, conservation of (original) order

Classical system verification uses hard bounds = worst case analysis

➔ often infeasible in NAS (especially if failures are considered)!

”A change in a sensor value which stays active only for a time interval (pulse) of 5 ms is detected by the controller in all cases.”

A change in a sensor value that stays active only for a time interval (pulse) of 5 ms is detected by the controller in 99% of all cases.

M⁴ Approach: Multi Model Multi Method-Approach

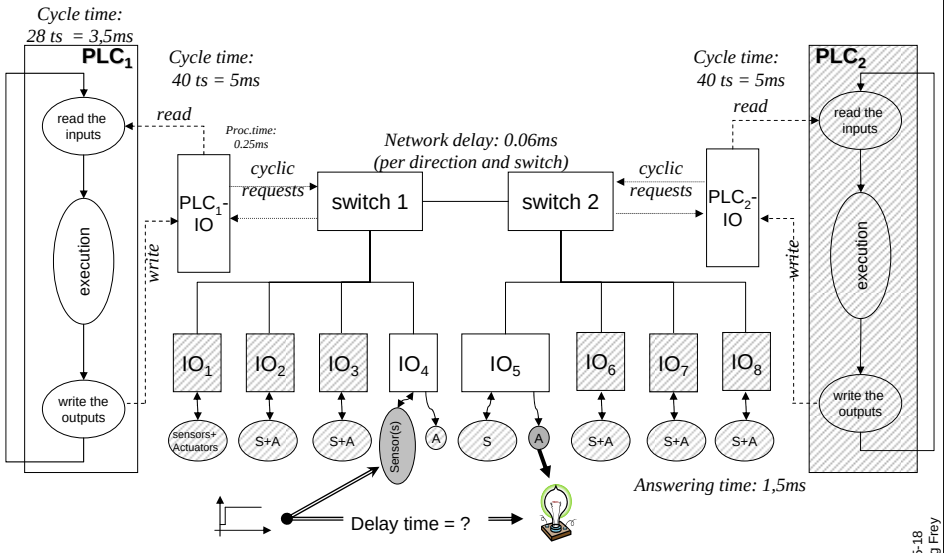
UnB

- Known Approaches (e.g. Network Calculus) deliver only extremal values
- In NAS the Distribution of Response Time is of Interest (Quality, Safety)
- Ways to Analyze the Response Times in NAS
  - ➢ Simulation
    - Only Control Part (Reaction on Input) → timed discrete event model model
      → HCTPN Simulation in CPN-Tools *(finished project, Dissertation in 2006)*
    - Closed Loop → Hybrid Model
      → Algorithms + DEs in Modelica-Language Simulation in Dymola *(running project started 2007)*
  - ➢ Formal Verification
    - Control under normal conditions → timed discrete event model
      → Timed Automata (TA) and Verification in Uppaal *(study completed)*
    - Control considering failures and distributions → probabilistic timed discrete event model
      → Discrete Time Markov Chains and Verification in PRISM using Probabilistic Model Checking, PMC *(running project, Dissertation in 2007)*

2007-05-18 © Georg Frey

Introductory Example

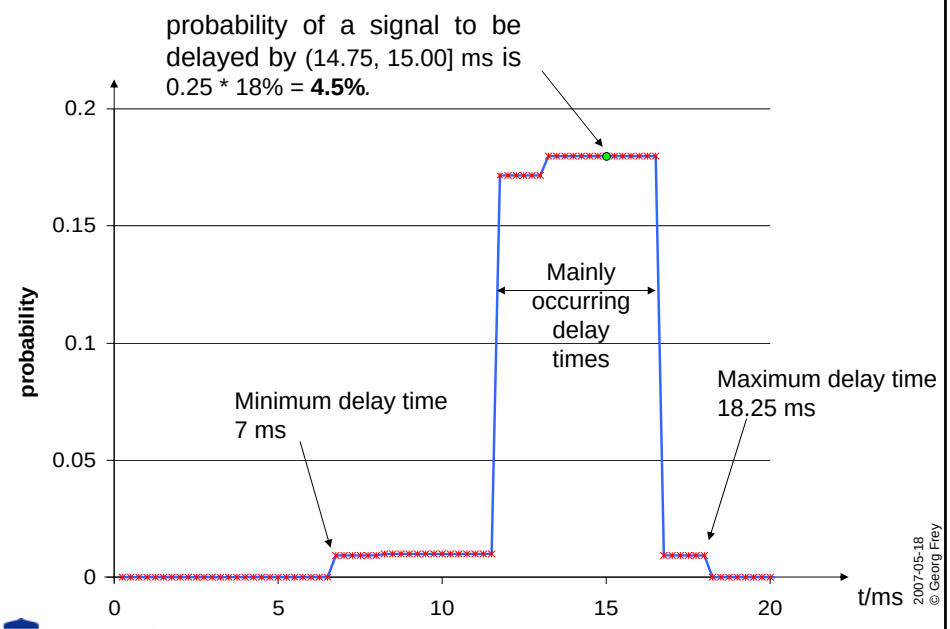
UnB



2007-05-18 © Georg Frey

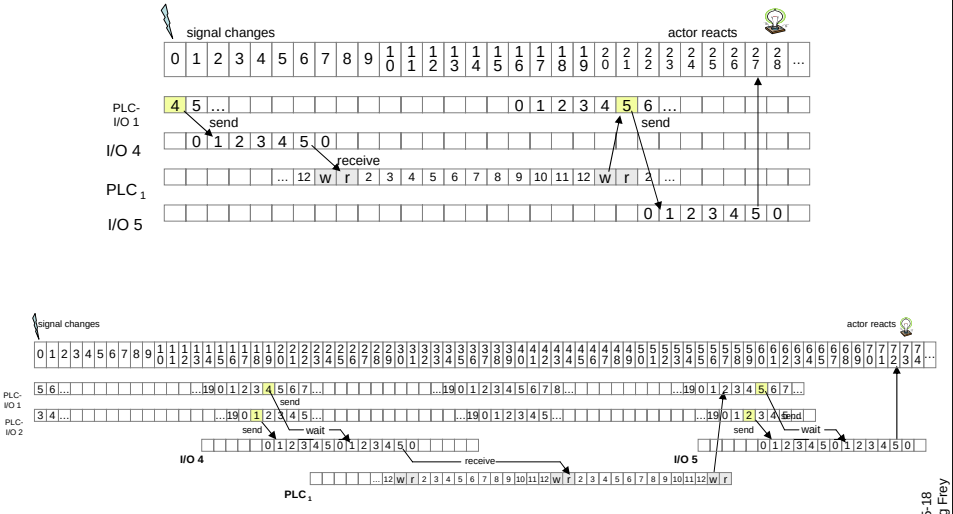
Results of Analysis by PMC

UnB



Minimum and Maximum Delay

UnB



1 time step equals 0.25 ms

Lesson learned from the Example

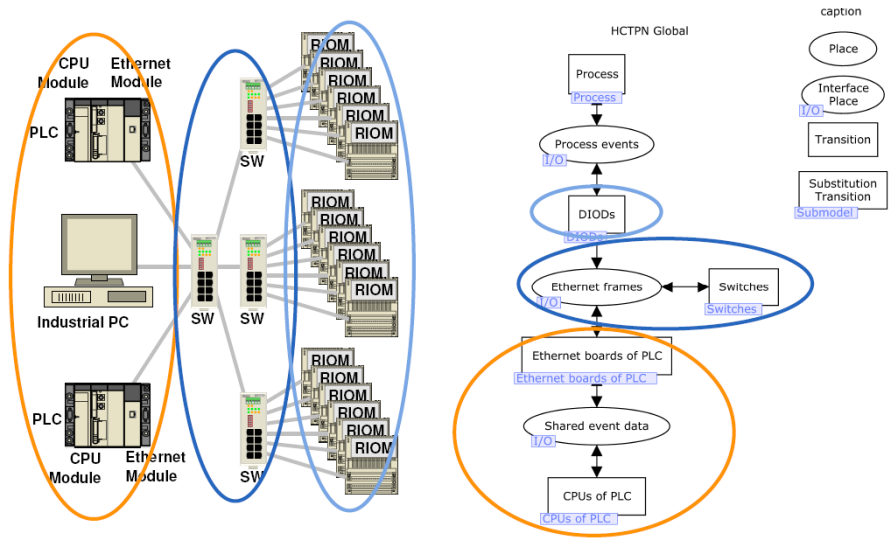
UnB

- In NAS there is an Overlay of asynchronous cyclic processes
- Response time depends on the state of the system at the time an event occurs
- Good coverage of possible states is important to get useful results
- Two approaches:
  1. Analyzing the system for a long time with stochastic input events
  2. Analyzing the system for stochastic initial states with fixed input event

2007-05-18
© Georg Frey

HCTPN Approach: System Model as Abstract Petri Net

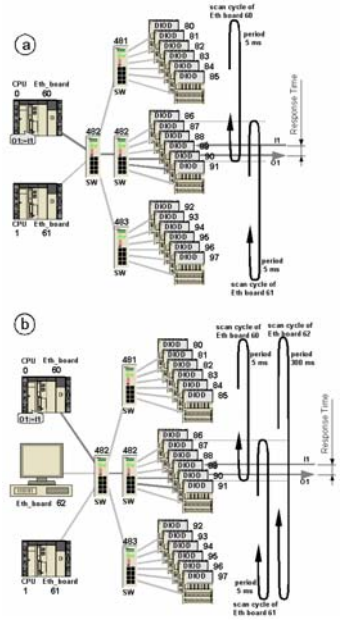
UnB

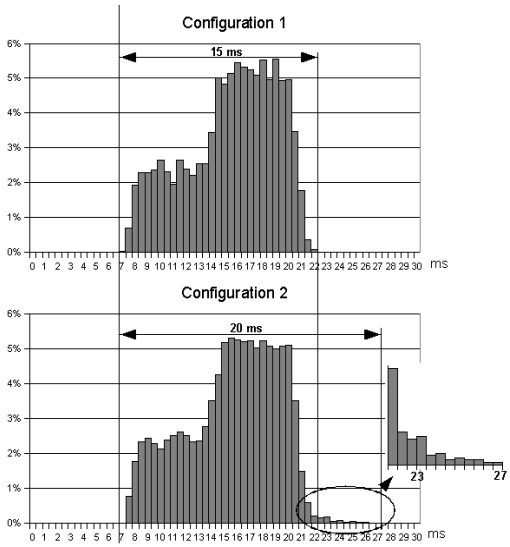


2007-05-18
© Georg Frey

HCTPN Approach: Results of Analysis for Extension of NAS

UnB





[Marsal, Denis, Faure und Frey IEEE ETFA 2006]

HCTPN Approach: Evaluation

UnB

Pros

- Approach allows detailed Modeling (e.g. TCP/IP-Stack)
- New Configurations are easy to build
- Fast Simulation of complex systems

Cons

- Abstract Model is hard to understand
- Simulation
  - Extreme Values (rare events) may be lost
  - Determination of Simulation Scenarios (Test-Cases) is critical
  - Determination of Simulation Time is critical
- Non-deterministic Behavior could hardly be modeled
- Continuous Models Cannot be integrated

Application

- Comparative Study of different Configurations (Architectures) of NAS in reasonable time

Modelica Approach: Modeling

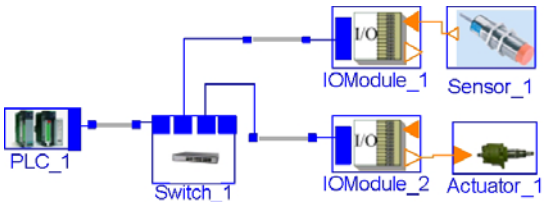
UnB

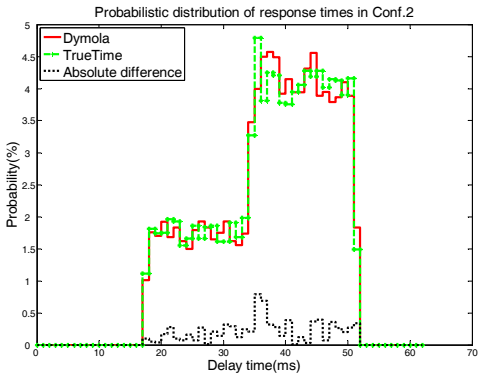
- Process Model built from continuous Modelica Blocks (DEs)
- Control part embedded into algorithm blocks including execution models
  - cyclic (PLC-Model)
  - Event-Based (embedded controllers)
- Network as algorithm models
  - Messages are represented as tokens in the model (ID number)
  - Network delays the tokens
    - Storage in Switches
    - Delay on wires
  - Content (data) of the message is kept in a database externally and read if needed

Modelica Approach: Comparative Example

UnB

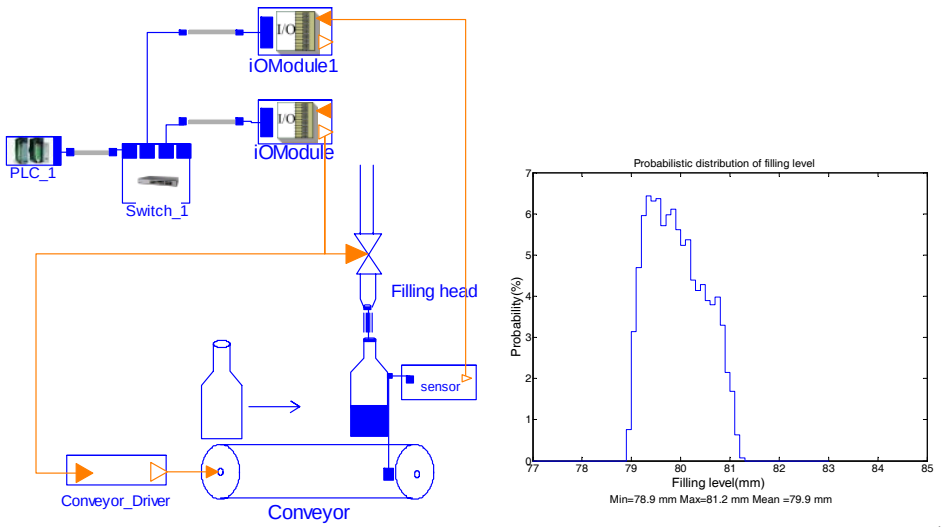
- PLC: 10ms
- PLC-I/O: 17ms
- Field-I/O: 2ms





Modelica Approach: Closed Loop Example

UnB



2007-05-18
© Georg Frey

Modelica Approach: Evaluation

UnB

Pros

- Model is block oriented (well accepted approach in automation)
- Fast modeling due to library and inheritance
- Continuous behavior can be modeled

Cons

- Problem of coverage (simulation)
- Long simulation time especially with complex discrete part
- Non-deterministic modes are hard to integrate

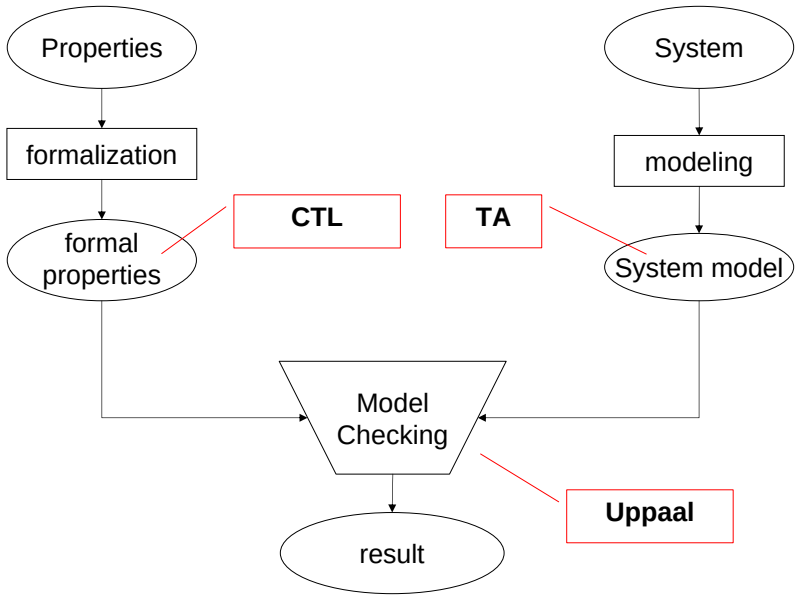
Application

- Analysis on the influence of networked systems on closed-loop behavior (NCS)

2007-05-18
© Georg Frey

TA Approach: Model Checking

UnB

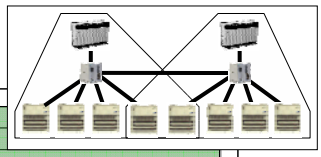


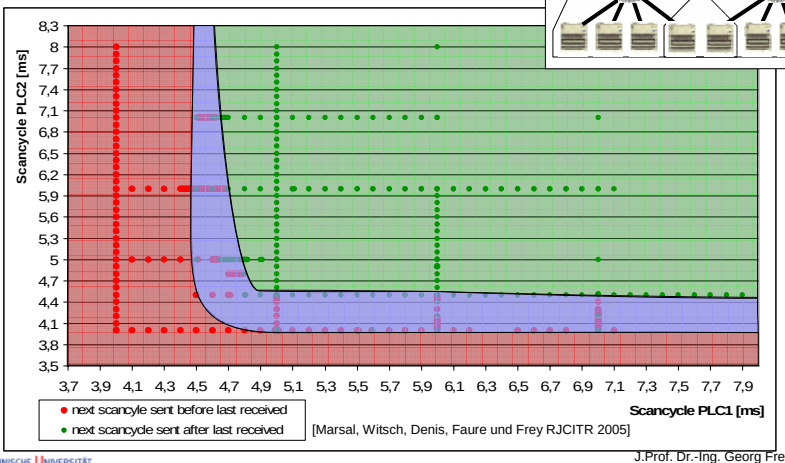
2007-05-18
© Georg Frey

TA Approach: Example

UnB

- Checking an Assumption made in the HCTPN Approach: „All Responses of the polled I/O Modules of a PLC are received before the next scan-cycle starts.“
- Test for different scan-cycles in a model with 2 PLCs





[Marsal, Witsch, Denis, Faure und Frey RJCITR 2005]

2007-05-18
© Georg Frey

TA Approach: Evaluation

UnB

Pros

- Formal Verification: All cases are covered

Cons

- Model not intuitive
- Verification is very time-consuming
- Formulation of properties is hard
- Integration of continuous dynamics is not possible
- Integration of probabilistic behavior is also not possible

Application

- Proof of special important properties (assumptions in the simulation approaches)
- Verification of reduced (conservative) Models (Reduction based on Simulation)

PMC Approach: Motivation

UnB

System immanent Reasons:

- Models of NAS often show probabilistic Behavior (Example: Network Delays)
- Exact Analysis Results (Worst-Case-Analyses) then lead to infeasible Demands on the System

Application Reasons:

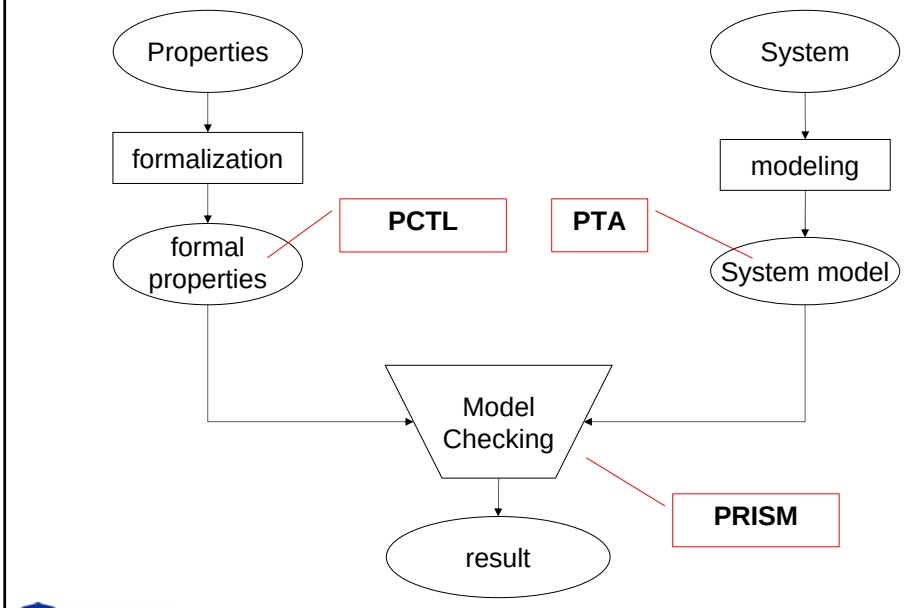
- Number of safety critical Automation Systems increases
- Modeling of Failures (stochastic) is important part of the analysis

Probabilistic Model Checking (PMC) Approach:

1. Properties with probabilistic bounds (PCTL)
2. Modeling with Probabilistic Timed Automata (PTA) and Mapping to embedded discrete-time Markov Chains (DTMC)

PMC Approach: Model Checking

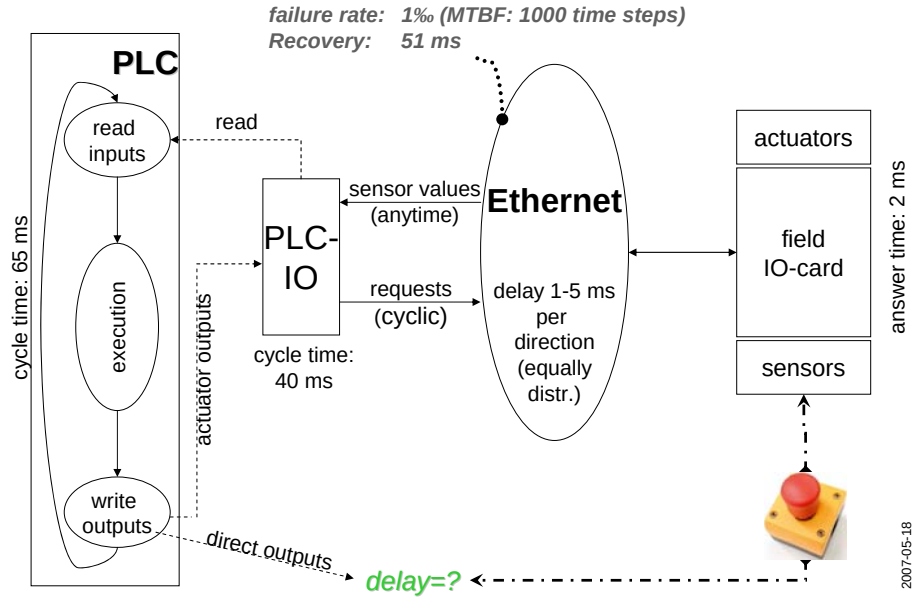
UnB



2007-05-18 © Georg Frey

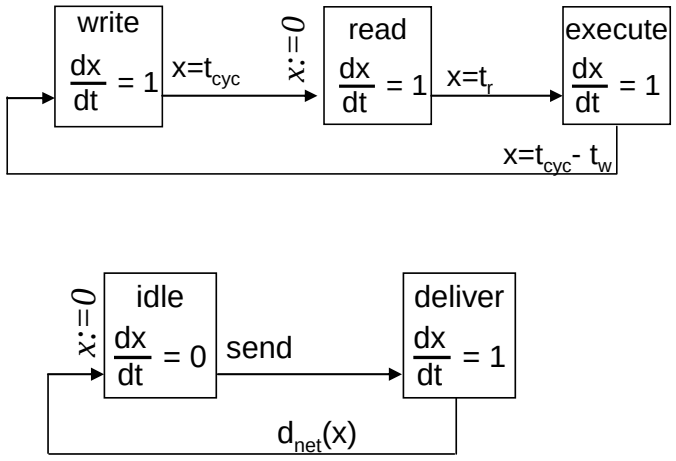
PMC Approach: Example: Reliability

UnB



2007-05-18 © Georg Frey

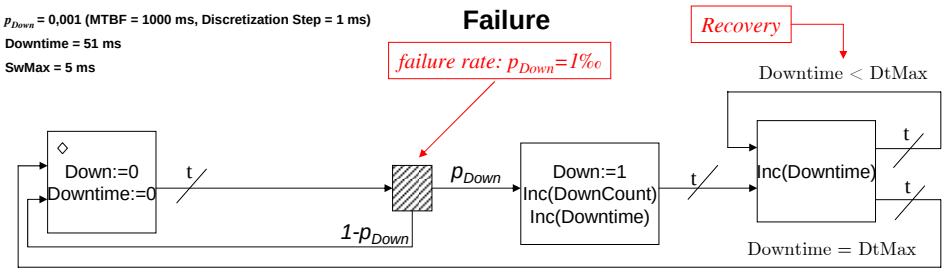
PMC Approach: Models of PLC and Network (cont. PTA) UnB



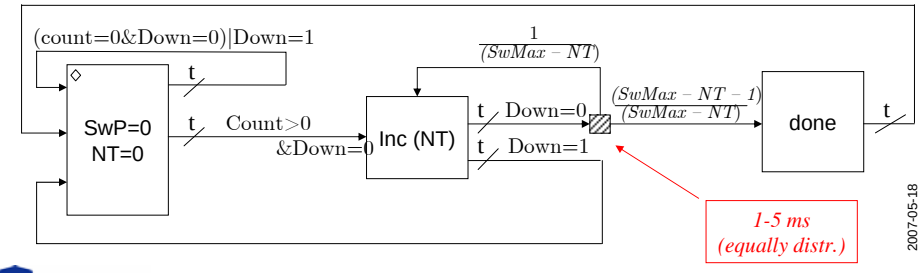
2007-05-18 © Georg Frey

PMC Approach: Models of the Network with Failure (disc. PTA) UnB

p_{Down} = 0,001 (MTBF = 1000 ms, Discretization Step = 1 ms)
Downtime = 51 ms
SwMax = 5 ms

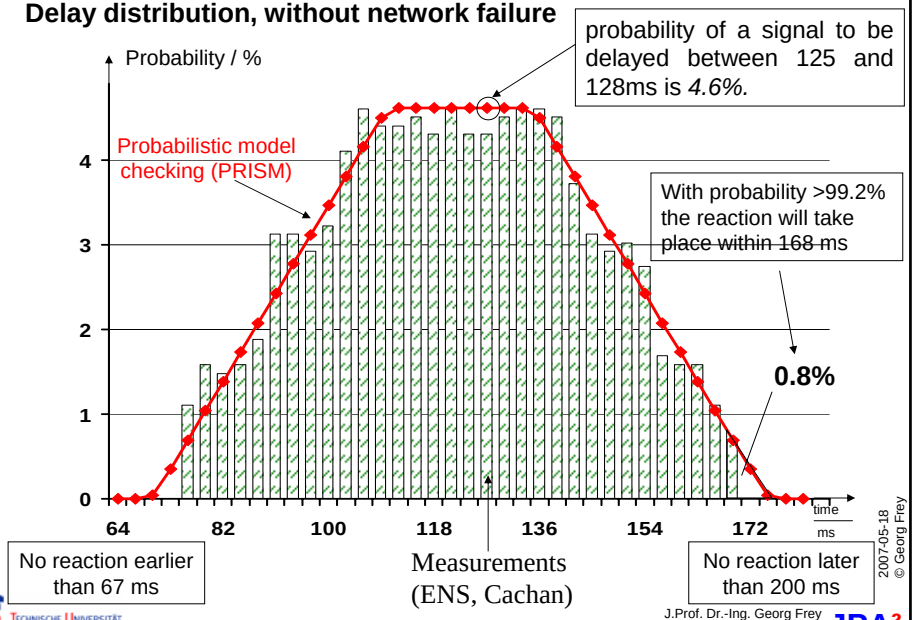


Network

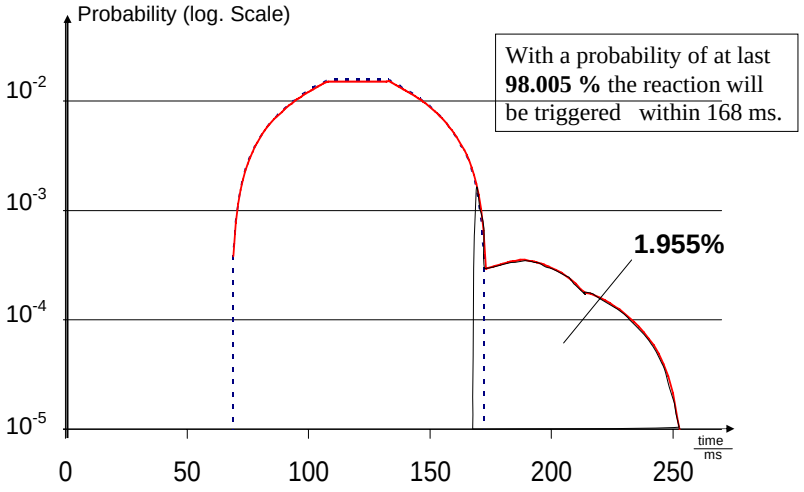


2007-05-18 © Georg Frey

Delay distribution, without network failure

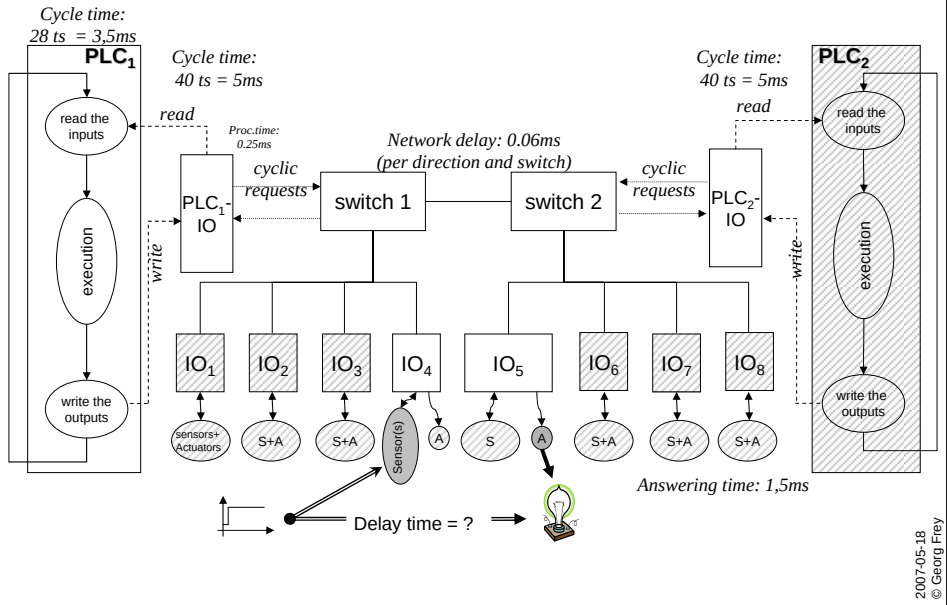


Delay distribution, considering network failures



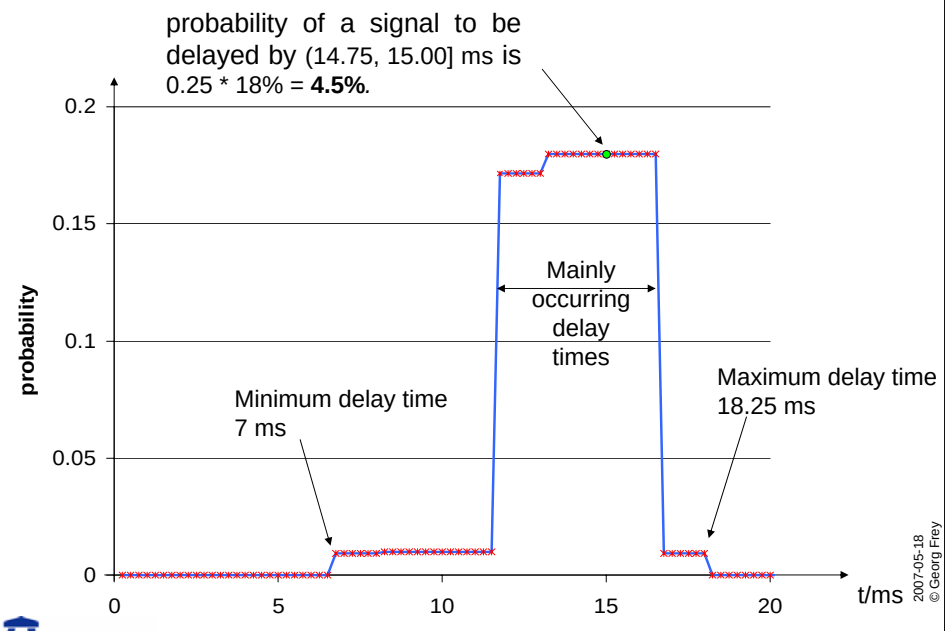
PMC Approach: Back to the Introductory Example

UnB



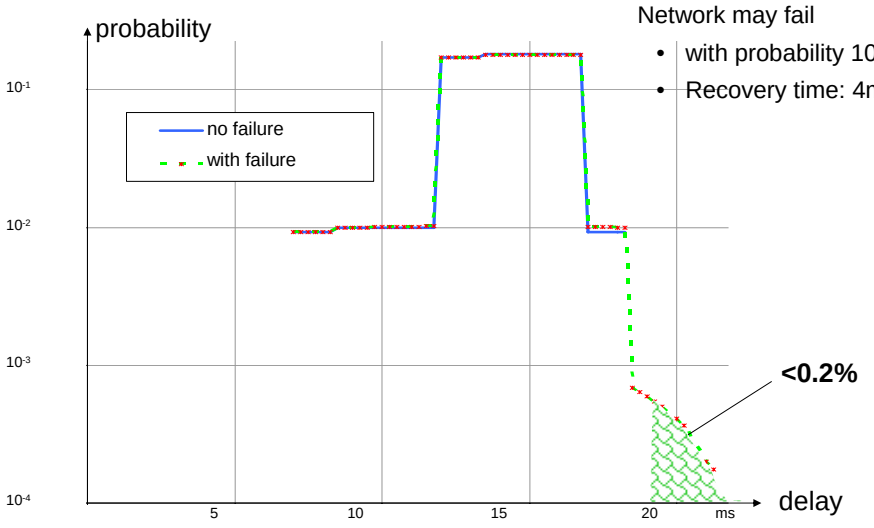
PMC Approach: Results

UnB



PMC Approach: Delay times with failures

UnB



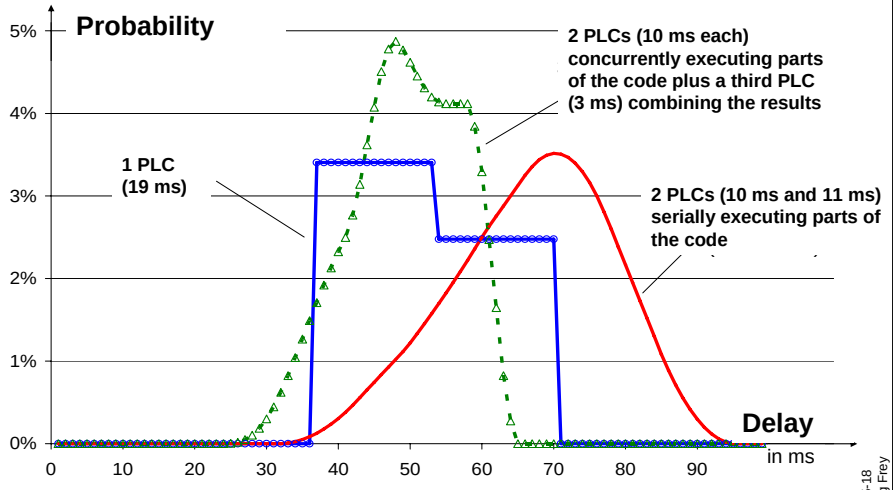
➔ **With a probability of 99.8% the delay will be less than 20ms**

2007-05-18
© Georg Frey

PMC Approach: Influence of Distributed Calculation

UnB

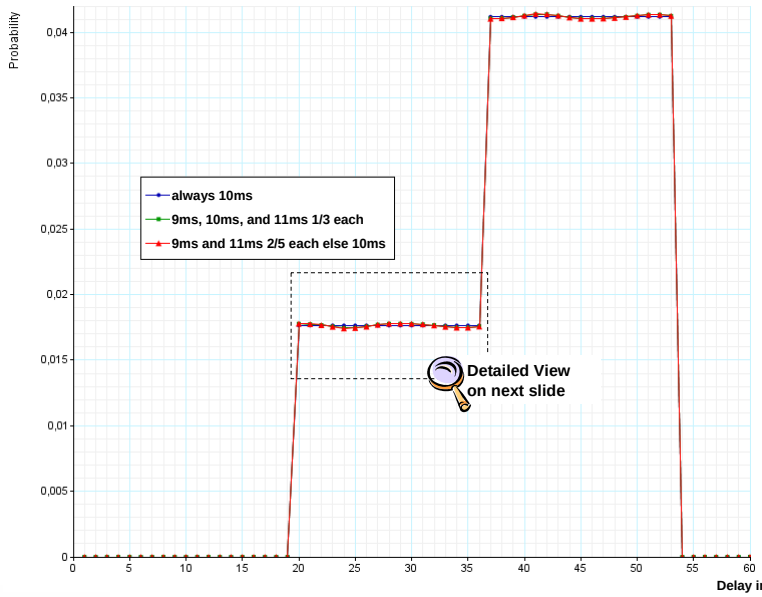
- Distributing an algorithm on several PLCs



2007-05-18
© Georg Frey

PMC Approach: Influence of Variable PLC Cycle Time

UnB

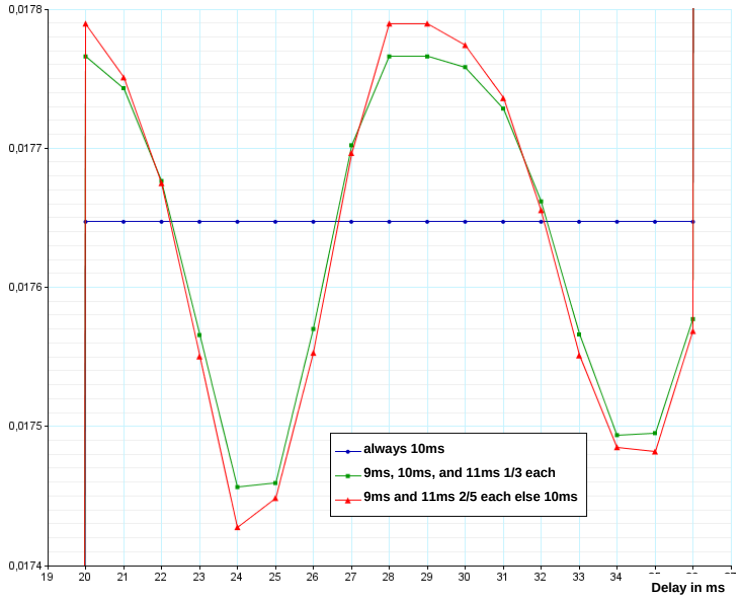


2007-05-18
© Georg Frey

PMC Approach: Influence of Variable PLC Cycle Time

UnB

Detailed View

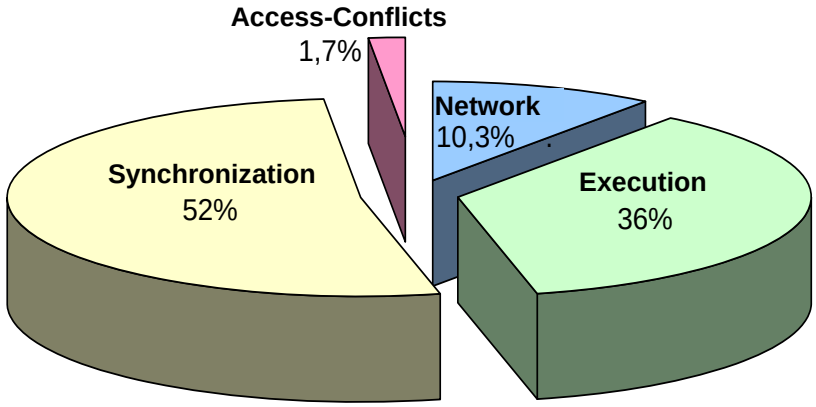


2007-05-18
© Georg Frey

PMC Approach: Evaluating different Delay Causes in NAS

UnB

- Example: 3 PLCs working in an NAS (all accessing the same I/O-board)
  - Network: Delay directly caused by the network
  - Access-Conflicts: Delays caused when several PLCs try to access the same I/O-board
  - Synchronization: Delays caused when a process has to wait for another (e.g. PLC waits for input from PLC-I/O
  - Execution: Time spent on execution of algorithms in PLCs and I/O-boards
- results are found to be similar for other configurations



2007-05-18
© Georg Frey

PMC Approach: Evaluation

UnB

Pros

- Verification Approach → Completeness
- Only approach allowing the direct modeling of probabilities
- Check of probabilistic properties is possible
- Reliability could be checked

Cons

- Complicated Modeling (Esp. Initial and Terminal conditions)
- Computationally Expensive
- Currently some problems with stability in PRISM

Application

- Proof of probabilistic Properties
- Analysis of Systems with Failures

2007-05-18
© Georg Frey

Summary

UnB

General

- Convergence of C³-Technologies Control, Computation und Communication leads to Networked Automation Systems (NAS)
- NAS pose new challenges for dependability Analysis
- Depending on the Application different methods to analyze „temporal correctness“ can be used
  - Simulation (discrete): Fast open-loop, however no completeness guarantee
  - Simulation (hybrid): Transparent, closed-loop → Application to NCS possible
  - Verification (deterministic): Only in restricted cases
  - Verification (probabilistic): Open-loop, Safety, Completeness Guarantee

Analysis Results

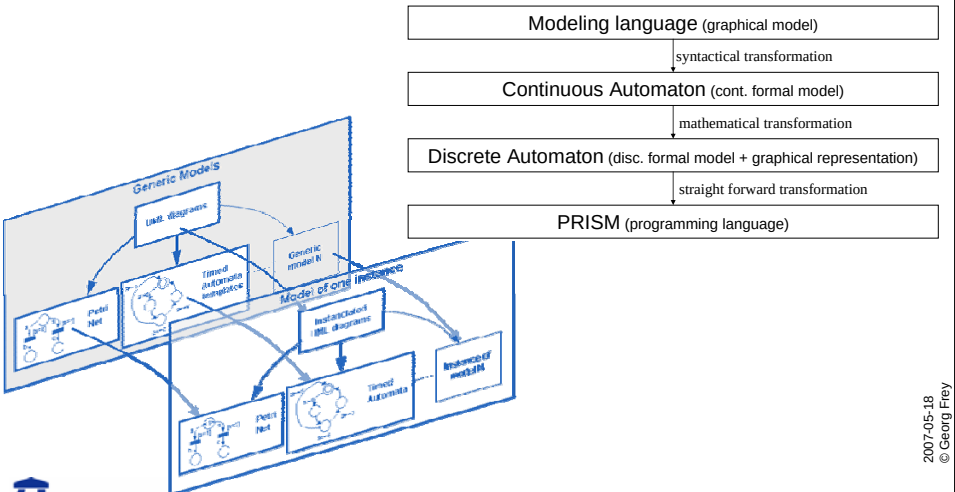
- Network delays are of minor influence in NAS (10%)
- However, network allows the structures that lead to high delays by synchronization and resource sharing (50%)
- Failures lead to extremely high response times with extremely low probability → probabilistic bounds are needed in analysis

2007-05-18
© Georg Frey

Outlook

UnB

- Consideration of complex control algorithms into analysis
- Integration of different methods in one framework
- Automated design process for PMC



2007-05-18
© Georg Frey

Thank You