EUROSIM 2016

Generation of Formal Plant Models Based on Simulation Environments

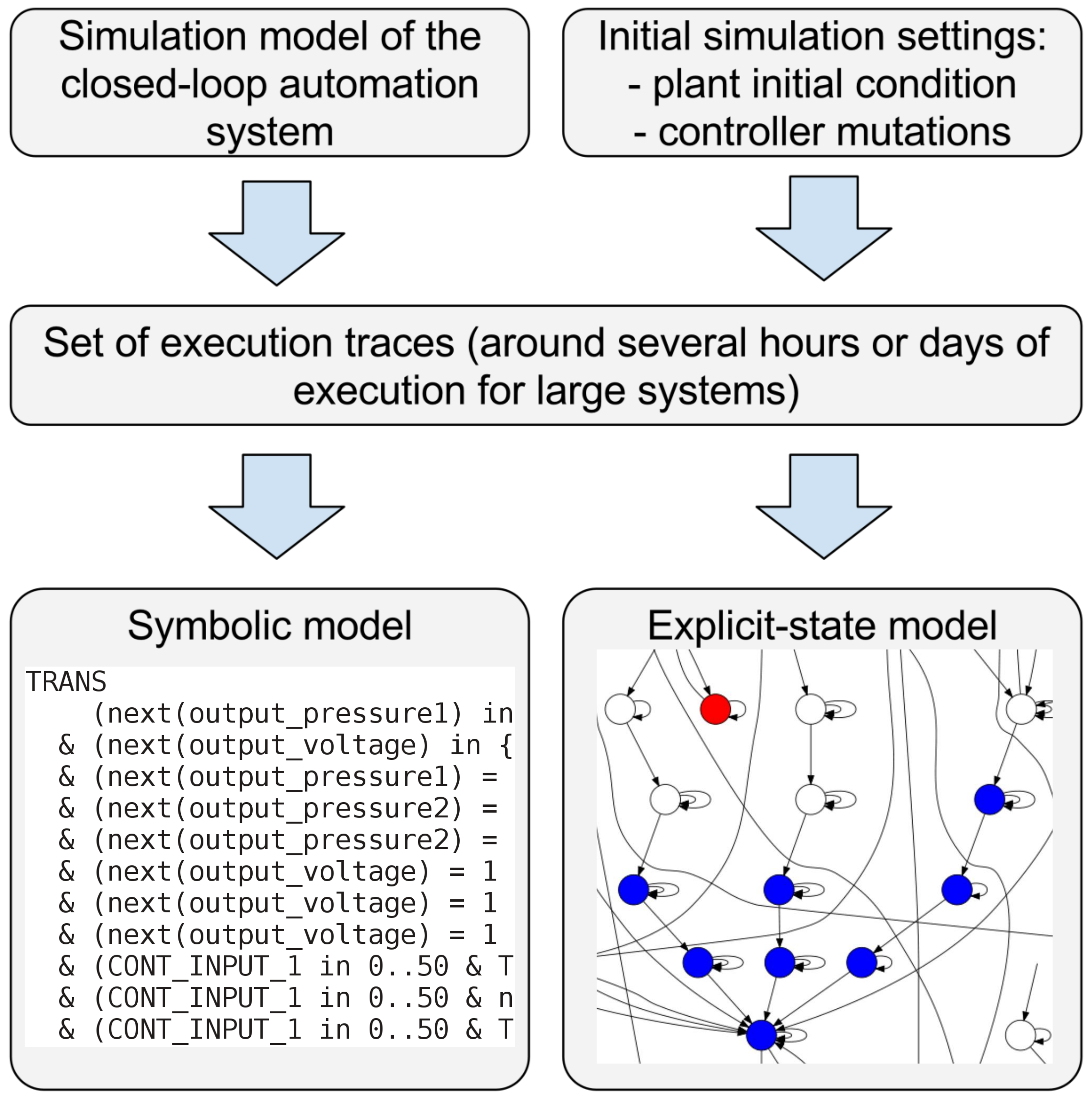
Igor Buzhinsky[1, 2] (igor.buzhinskii@aalto.fi), Andrei Sandru[2], Antti Pakonen[3], Daniil Chivilikhin[1, 2],
Vladimir Ulyantsev[1], Anatoly Shalyto[1], Valeriy Vyatkin[2, 4]

[1]ITMO University [2]Aalto University [3]VTT Technical Research Centre of Finland Ltd. [4]Luleå University of Technology

Introduction & Motivation

- **Closed-loop model checking** is a formal verification technique to ensure safety and reliability of automation systems
- Requires a **formal, discrete-state plant model** in addition to the model of the controller
- How to construct the model of the plant automatically?
- If a simulation model is available, the formal model can be created based on **execution traces**

Overview of the approach



Simulation model of the closed-loop automation system

Initial simulation settings:
- plant initial condition
- controller mutations

Set of execution traces (around several hours or days of execution for large systems)

Symbolic model

```
TRANS
    (next(output_pressure1) in
  & (next(output_voltage) in {
  & (next(output_pressure1) =
  & (next(output_pressure2) =
  & (next(output_pressure2) =
  & (next(output_voltage) = 1
  & (next(output_voltage) = 1
  & (next(output_voltage) = 1
  & (CONT_INPUT_1 in 0..50 & T
  & (CONT_INPUT_1 in 0..50 & n
  & (CONT_INPUT_1 in 0..50 & T
```

Explicit-state model

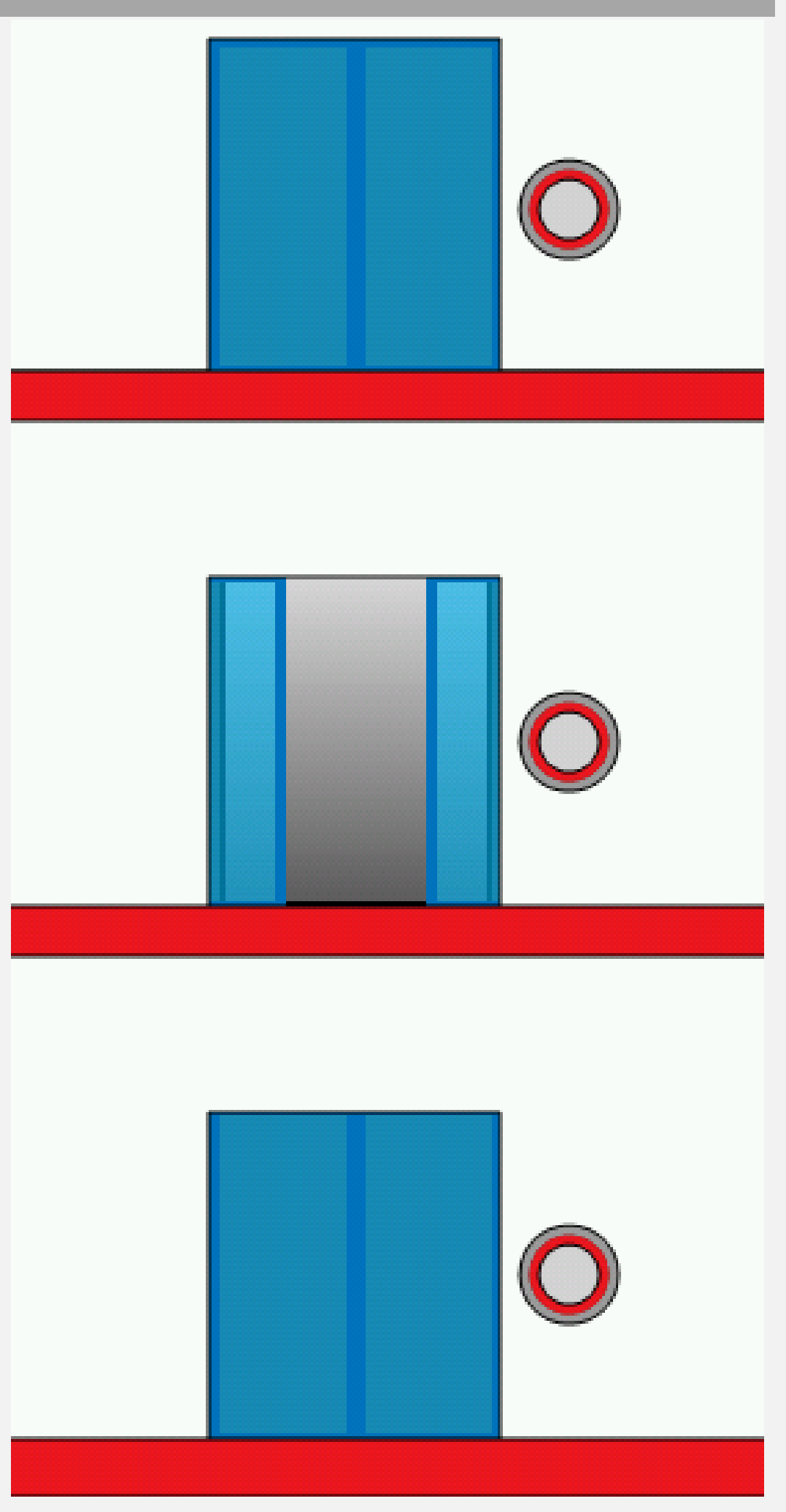
Overall scheme of the proposed approach

Highlights

- Explicit consideration of plant models **increases the volume of temporal properties** of the system under verification which can be properly checked
- The **complexity** of the simulation model can be **drastically reduced**, which allows to apply formal verification to large systems
- While explicit-state plant models are **graphical** and thus **easy for comprehension**, symbolic (constraint-based) models are **quicker to verify** by symbolic verifiers such as NuSMV and nuXmv
- Limited support of linear temporal logic (LTL) properties as an additional source of specification for plant model generation

Simple example: elevator simulation model in NxtStudio

- NxtStudio is an IDE for IEC 61499-compliant function block (FB) applications
- The Elevator model is an example of a simple automation system, yet required to be reliable
- Trace recording with the help of the CSVWRITER FB
- How to record traces? Manual scenarios; random input (button pressing) sequences
- Preliminary investigations on ensuring plant model coverage



Real-world example: nuclear power plant simulation model in Apros

- Apros is a simulation environment to model continuous combustion and nuclear plants, including their controllers
- A generic **nuclear power plant** (NPP) simulation model was provided by Fortum Power and Heat Oy
- Generated formal plant models were verified in NuSMV in closed loop with controller models obtained using a tool provided by VTT Technical Research Centre of Finland Ltd.

Simulation NPP model

Process networks
- Primary circuit
- Pressure vessel
- Emergency system
- Steam generators
- Etc.

Automation networks
- Reactor control
- Plant and turbine power control
- Reactor and turbine trip
- Protection networks
- Etc.

Structure of the simulation NPP model

References

[1] Buzhinsky I. and Vyatkin V. (2016) *Plant Model Inference for Closed-Loop Verification of Control Systems: Initial Explorations*. 2016 IEEE International Conference on Industrial Informatics (INDIN 2016), Poitiers, France, July 18–21, 2016, pp. 736–739

Acknowledgments

- Supported by the SAUNA project, funded by the Finnish Nuclear Waste Management Fund (VYR) as a part of research program SAFIR2018
- Supported by the Ministry of Education and Science of the Russian Federation, project RFMEFI58716X0032

The 9th Eurosim Congress on Modelling and Simulation
12–16 September 2016, Oulu, Finland

ITMO UNIVERSITY

Aalto University
School of Electrical Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY