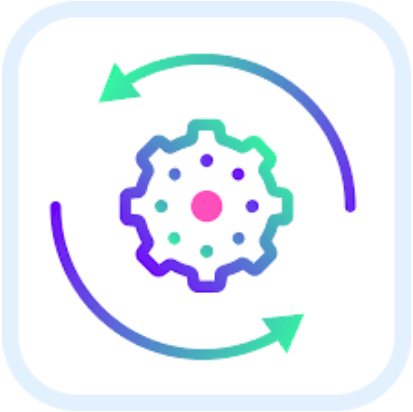


Framework for closed-loop formal verification of distributed automation software with plant model generator from event logs

Midhun Xavier*, Sandeep Patil*, Valeriy Vyatkin*†

*Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden

†Department of Electrical Engineering and Automation, Aalto University, Espoo, Finland

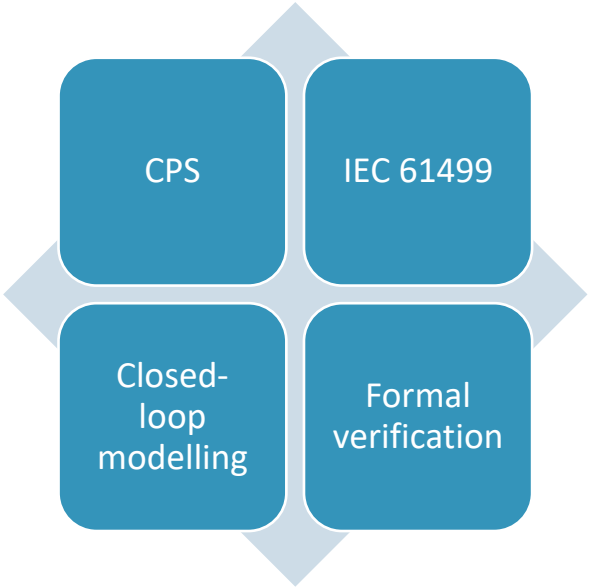
LULEÅ UNIVERSITY OF TECHNOLOGY

Contents

- Introduction
- CPS modelling and verification using tool chain
- Plant model generation from event logs
- Conclusion
- Future work

LULEÅ UNIVERSITY OF TECHNOLOGY

Introduction



LULEÅ UNIVERSITY OF TECHNOLOGY

Introduction - CPS modelling with IEC 61499

Cyber-physical systems is quite popular in industry world.

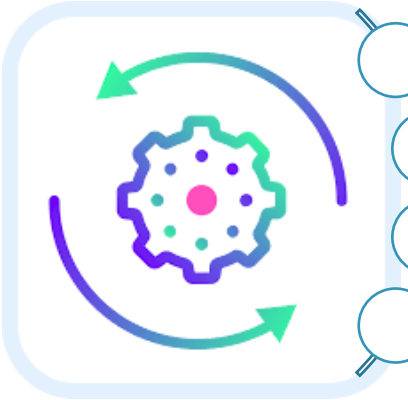
The IEC 61499 architecture is a powerful mechanism for engineering such systems.

The IEC 61499 provides a graphical engineering interface and supports programming in terms of state machines.

It has been proven also an efficient way of modelling CPS in automation.

LULEÅ UNIVERSITY OF TECHNOLOGY

Introduction - Formal verification of closed-loop systems



- Cyber-physical systems pose a significant challenge for their efficient verification and validation.
- Formal verification (FV) which proves or disproves the correctness of algorithms.
- FV can be used to verify the correctness and safety of these automation systems.
- Closed-loop modelling has been proposed for the most comprehensive verification.

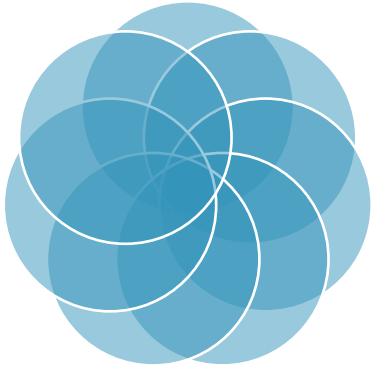
LULEÅ UNIVERSITY OF TECHNOLOGY

Part 1 - CPS modelling and verification using Tool chain

Description of Framework

Modelling of non-determinism in SMV

Discrete state modelling approach

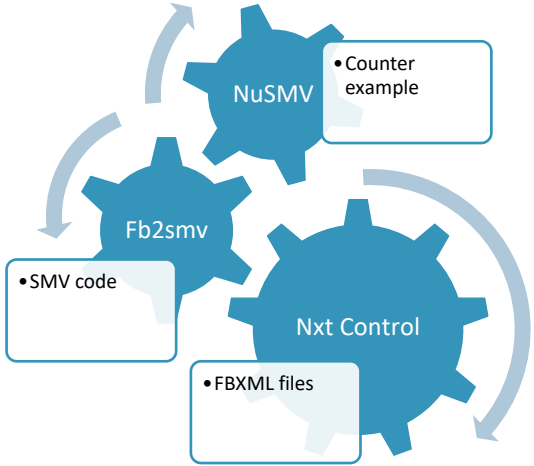


Tool chain

FB2SMV tool

Simulation model

Case study – Drilling station



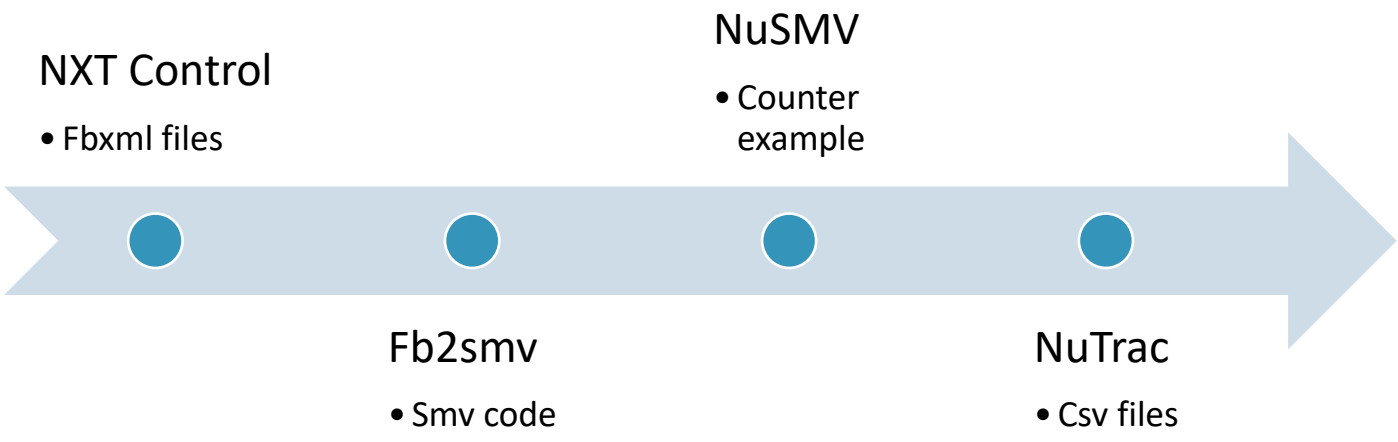
LULEÅ UNIVERSITY OF TECHNOLOGY

Description of Framework

- CPS (in IEC 61499 standard) → modelling language (SMV code)
- Fb2smv tool - IEC 61499 Function Blocks → SMV code
- Simulation model of the plant may result complex model for verification
- Integration of simplified model of the plant with model of the controller
- Introduction of notation in IEC 61499 for discrete state modelling
- Tool chain – Design, simulation and verification

LULEÅ UNIVERSITY OF TECHNOLOGY

Tool Chain



Tool chain for formal verifcation of CPSs in IEC 61499 standard

LULEÅ UNIVERSITY OF TECHNOLOGY

fb2smv tool

Generates SMV models of FB systems in IEC 61499

Fb2smv input

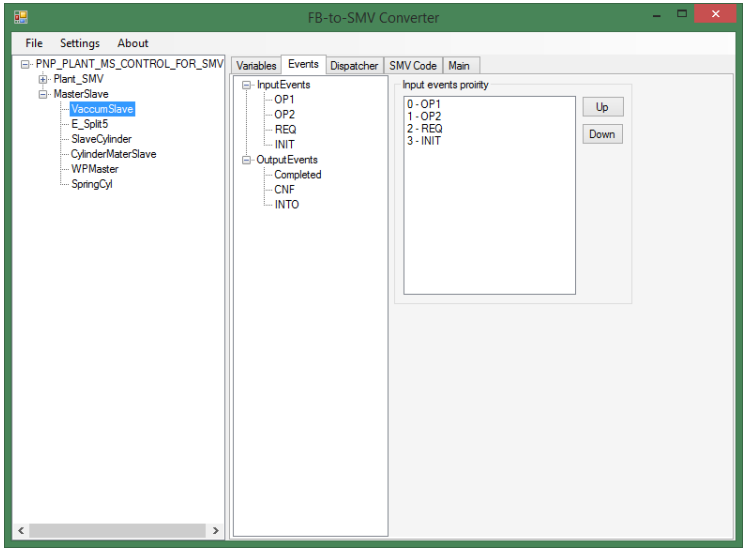
- IEC 61499 FB expressed in XML format

Fb2smv output

- Generates smv code with help of ASM semantics

Features of fb2smv

- Converts basic and composite FBs
- Limiting boundaries of variable
- Decides input event priority
- The proposed NDT notation added to the tool



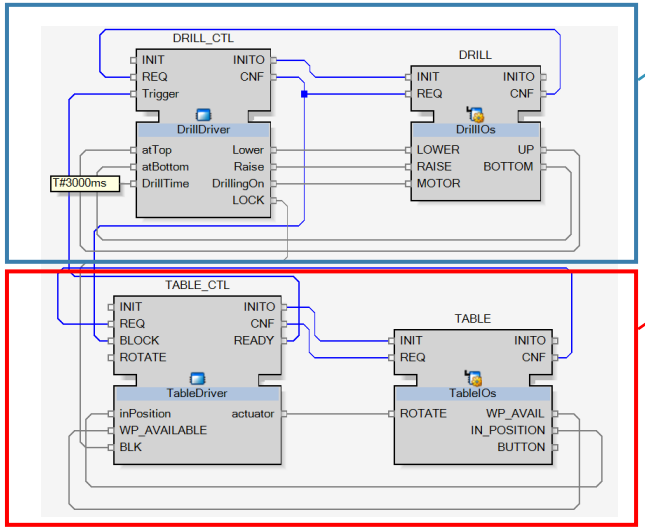
fb2smv converter window

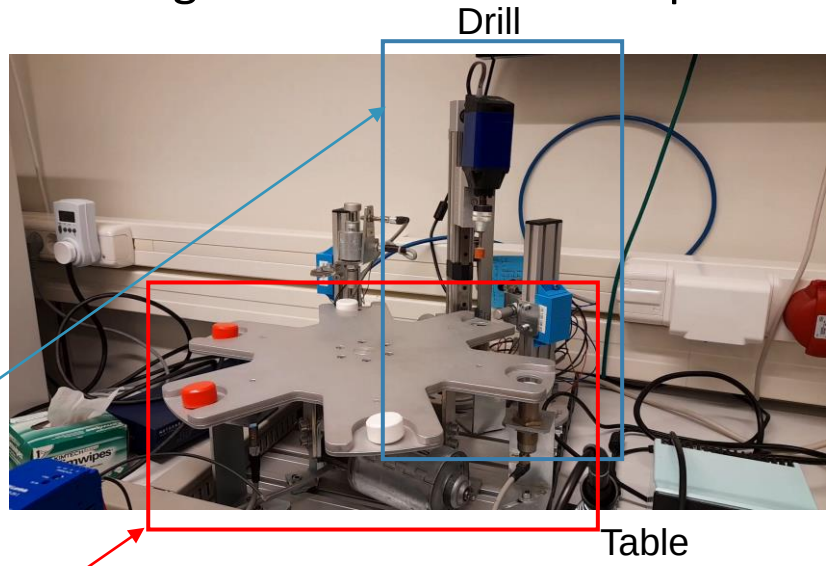
LULEÅ UNIVERSITY OF TECHNOLOGY

Case study: Drilling Station composed from Intelligent Mechatronic Components

The Industry 4.0 vision is to compose production systems from autonomous assets

Quick verification and validation is the key to agility





LULEÅ UNIVERSITY OF TECHNOLOGY

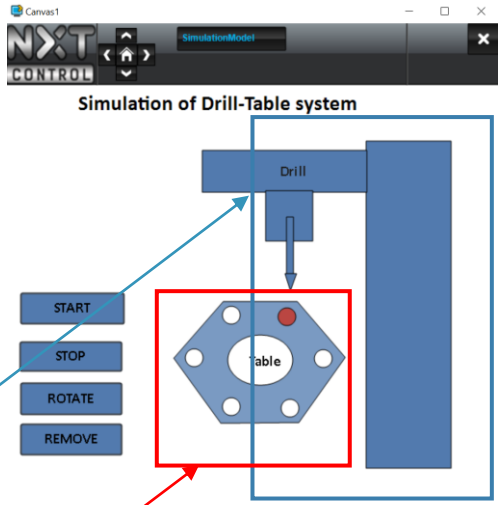
Simulation model

Controllers are connected exactly same way as in the real configuration

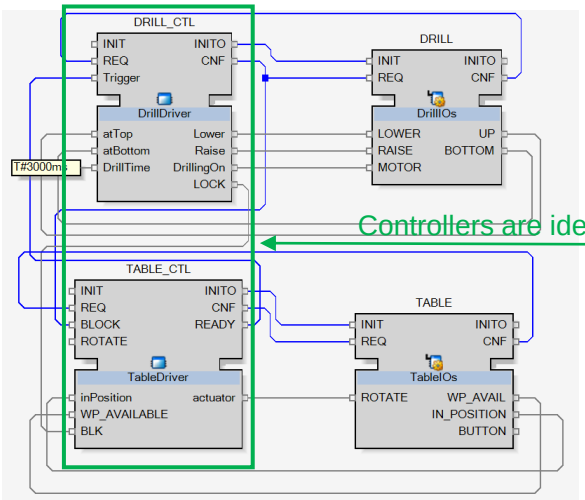
Simulation function blocks substitute interfaces to real IOs

Simulation can help finding many bugs in the controller integration

However, there are some intermittent errors which do not appear in simulation but occur in real system operation

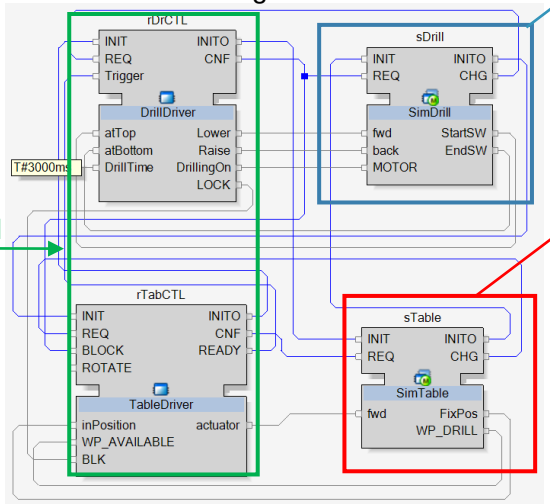


Deployment to PLC configuration



Controllers are identical

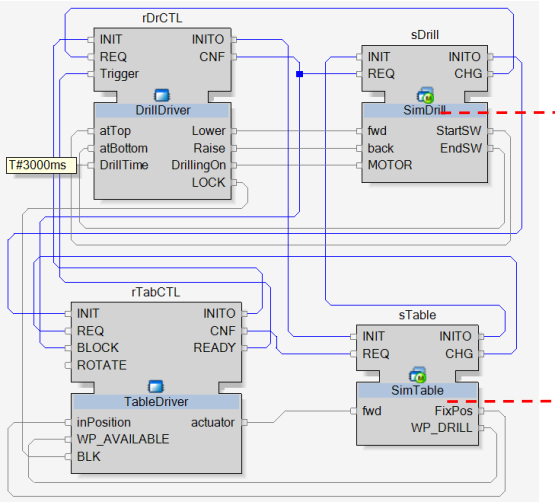
Simulation configuration



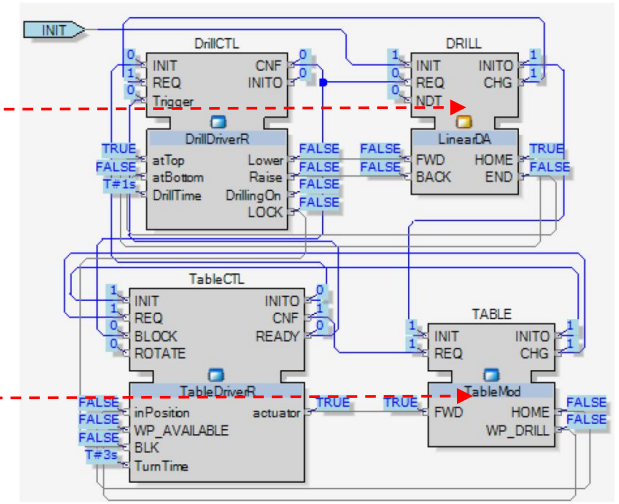
LULEÅ UNIVERSITY OF TECHNOLOGY

Idea: Methodology to reduce simulation configuration to discrete model, but with non-determinism

Simulation configuration



Discrete-state configuration



Substitute simulation models with discrete-state models

Make small modifications to controllers if they use timers

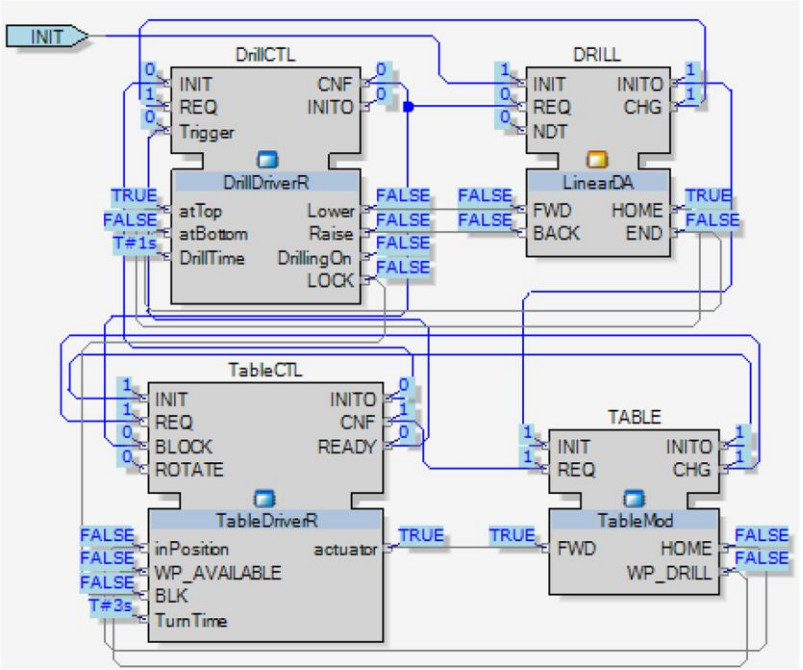
LULEÅ UNIVERSITY OF TECHNOLOGY

Discrete-state modelling approach

Discrete state model created based on simulation model

Here, FBs simulating the drill and table are substituted by their analogs operation in discrete domain

It can be translated into SMV model using fb2smv without much complexity increase



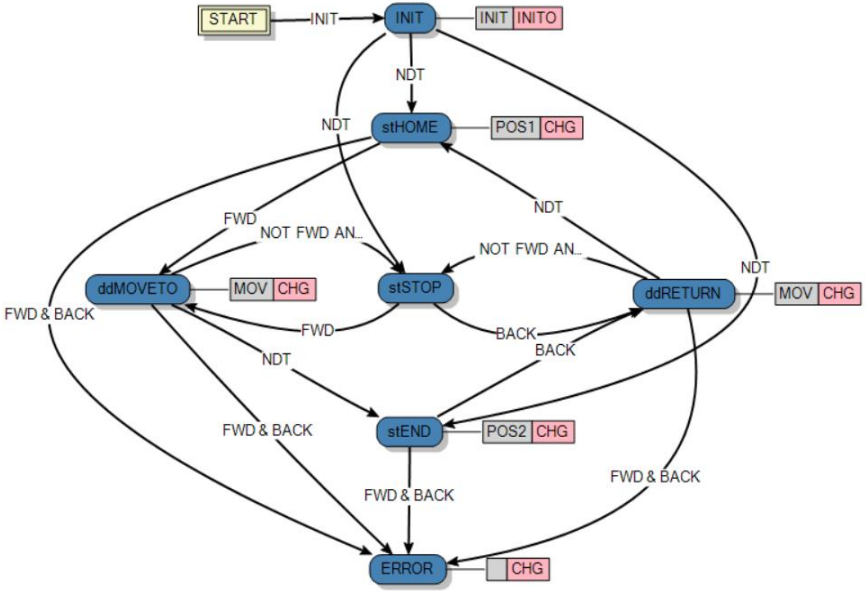
Discrete state FB model of drilling station

LULEÅ UNIVERSITY OF TECHNOLOGY

Discrete-state modelling approach

Notation for plant modelling

- Introduction of motion states i.e ddMOVETO and ddRETURN
- Transition from one motion to another via NDT signal
- Error state implementation
  - Whenever FWD and BACK is TRUE simultaneously plant will go to an ERROR state



Discrete state linear motion process model with NDT

LULEÅ UNIVERSITY OF TECHNOLOGY

Discrete-state modelling approach

Non-deterministic transition in controllers

- Formal modelling of timers is computationally hard
- Delay can be substituted by NDT signal

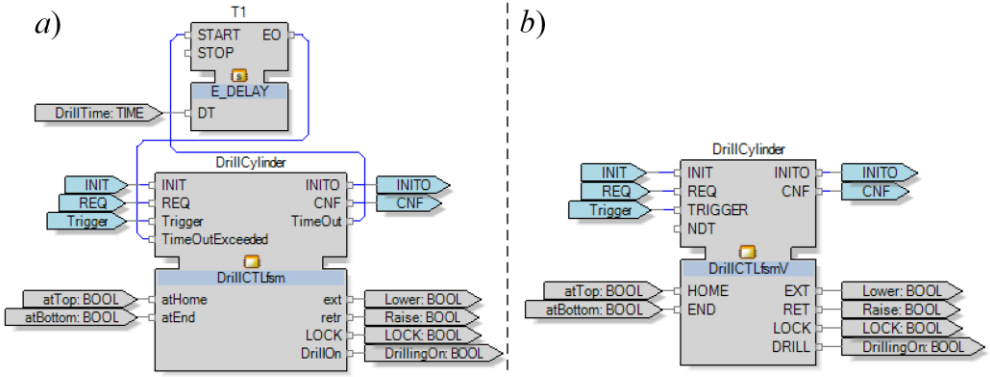


Figure. a) The real drill controller with external timeout. b) The interface of modified drill Controller with non- deterministic transition input.

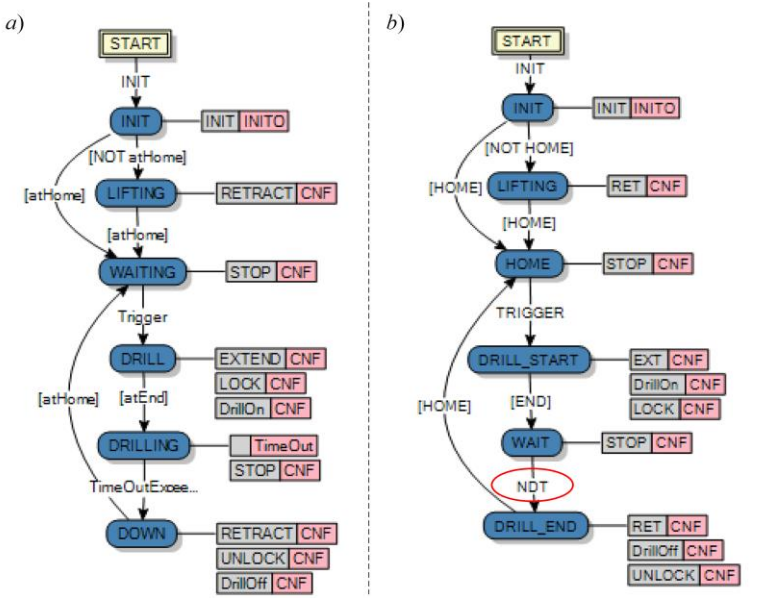


Figure. a) The ECC of the real drill controller; b) The ECC of the modified drill controller with NDT modelling the time delay.

LULEÅ UNIVERSITY OF TECHNOLOGY

Discrete-state modelling approach

Modelling of non-determinism in SMV		
Decleration	Initialization	Next transition
•VAR NDT:= boolean;	•init(NDT):= { TRUE, FALSE };	•next(NDT):={ TRUE, FALSE }; •or •next(NDT):= case •Condition: { TRUE, FALSE }; •TRUE : NDT; •Esac;

LULEÅ UNIVERSITY OF TECHNOLOGY

Results and Analysis

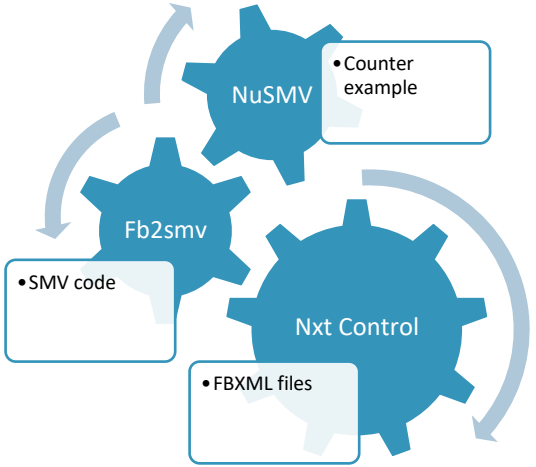
- Following specification are verified,

❑ -- specification G !(DRILL_TABLE_CFB3_inst.DrillCTL_RET = TRUE &

DRILL_TABLE_CFB3_inst.ActuatorGen_EO = TRUE)

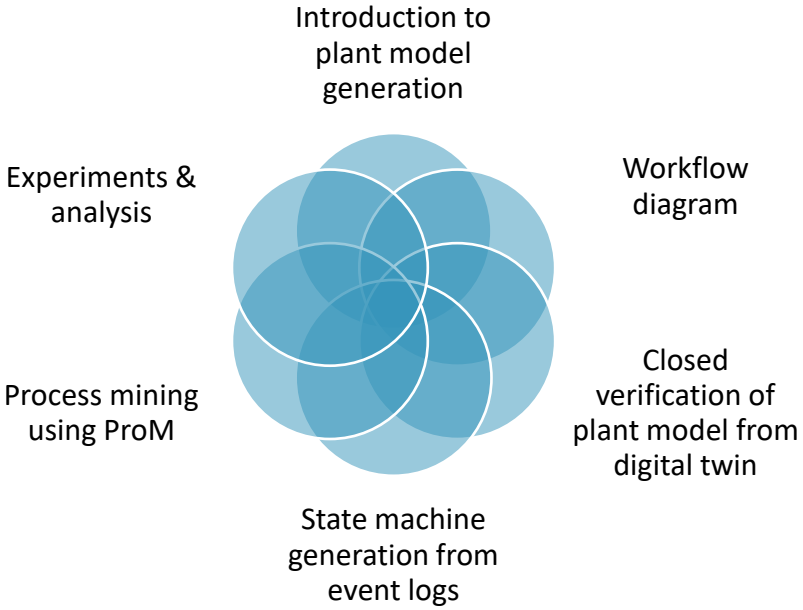
The counterexample generation for the specification took 26000 seconds to complete

❑ -- specification G !(DRILL_TABLE_CFB3_inst.DRILL.Q_smv = ERROR_ecc)



LULEÅ UNIVERSITY OF TECHNOLOGY

Part 2 – Plant model generation from event logs



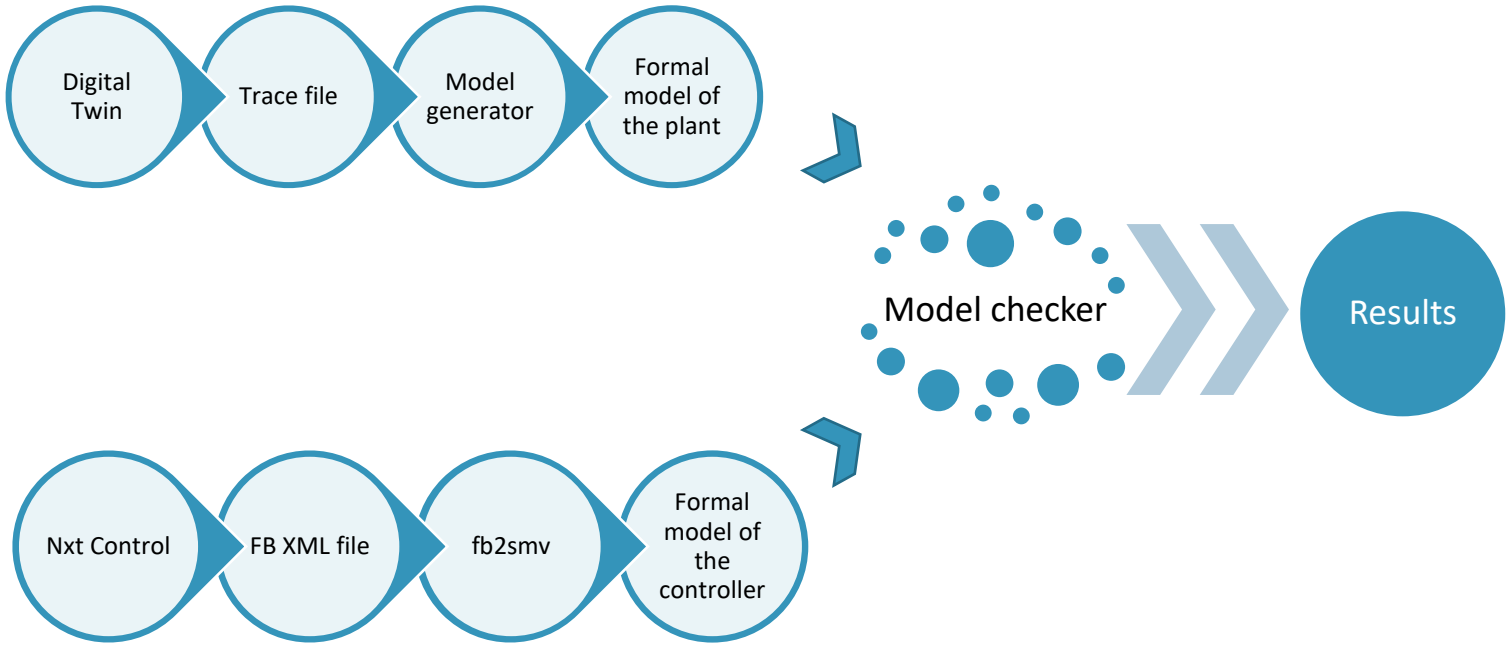
LULEÅ UNIVERSITY OF TECHNOLOGY

Introduction to plant model generation

- It would be great if it was possible to generate formal models automatically.
- How to generate the plant model automatically?
- Simulation models are widely used for manufacturing systems, and it can be used for recording event logs.
- Process mining can be used for constructing process models from event log.
- Explores an approach to automatically generate plant models of control systems from event log of digital twin.

LULEÅ UNIVERSITY OF TECHNOLOGY

Proposed solution



LULEÅ UNIVERSITY OF TECHNOLOGY

Experiment 1

EnAS is a laboratory scale assembly system.

Simulation model of EnAS developed using visual components.

Major components in the simulation model are the main plant, AGV and IRB

Controller created in nxtSTUDIO is connected to the Plant in visual components via OPC UA communication protocol

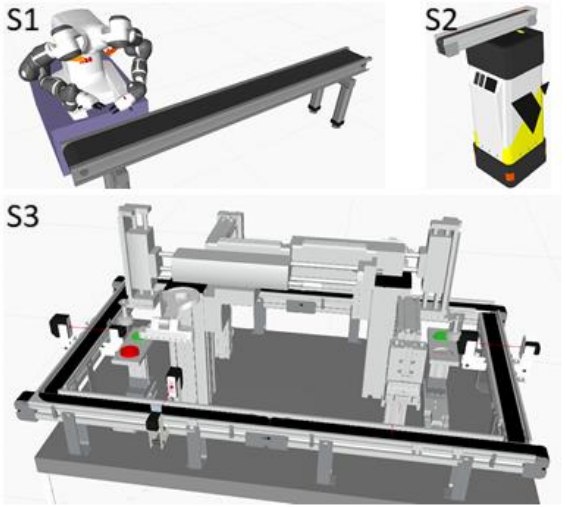


Figure . S1) Isolated IRB-subsystem of plant, S2) Isolated AGV-subsystem of the plant, S3) Main section of the plant

LULEÅ UNIVERSITY OF TECHNOLOGY

Closed loop verification of plant model from digital twin

Trace generation from digital twin

- In Visual Components whenever an action occurs, it records the event to trace file.
- Each event consists of timestamp, component and action.

Model generation from event log

- Model generator algorithm creates basic structure of smv code structure.
- It declares and initializes each component's variables and finally transitions of each variable is identified.

Embedding the plant model into SMV code structure provided by the fb2smv tool

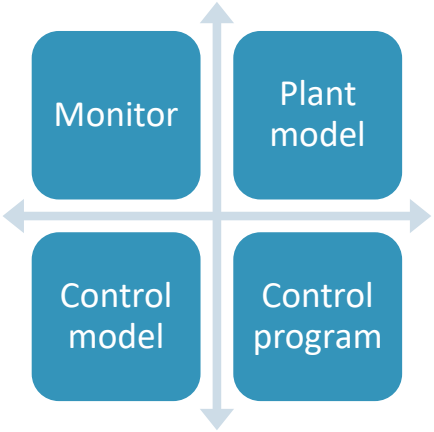
- Receiving control signals from controller to plant
- Insert the logic of plant model
- Passing sensor values to controller

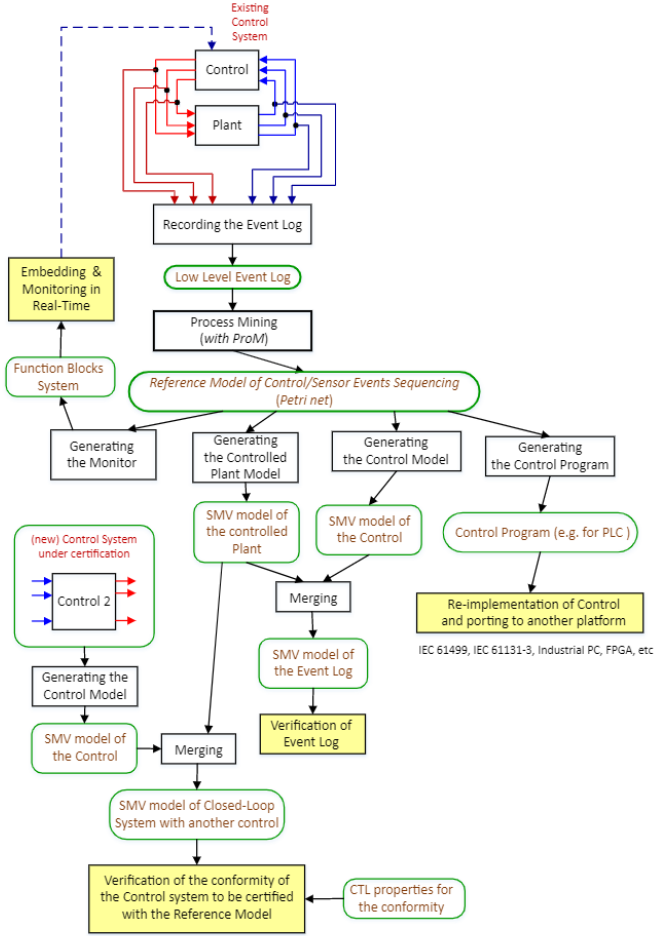
Updated SMV code is given for verification purpose.

LULEÅ UNIVERSITY OF TECHNOLOGY

Workflow diagram

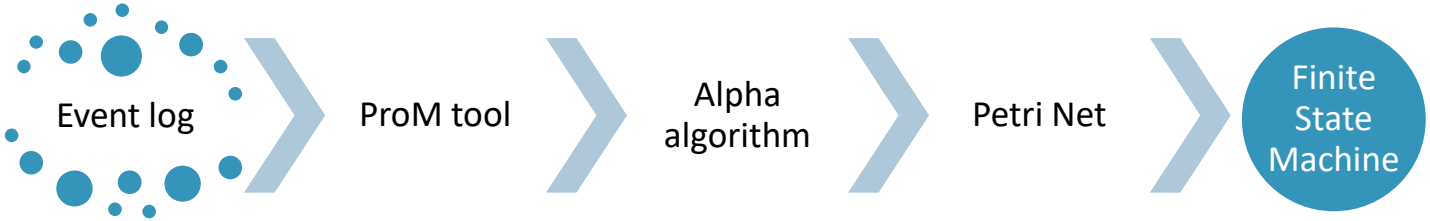
Expected outcomes





LULEÅ UNIVERSITY OF TECHNOLOGY

State machine generation from event logs



LULEÅ UNIVERSITY OF TECHNOLOGY

State machine generation from event logs

LULEÅ UNIVERSITY OF TECHNOLOGY

Experiment 2

Two-cylinder system.

Simulation model of system is developed using Nxt control's HMI.

Major components in the simulation model are the Vertical cylinder and Horizontal cylinder

Event log is recorded via OPC UA Communication protocol

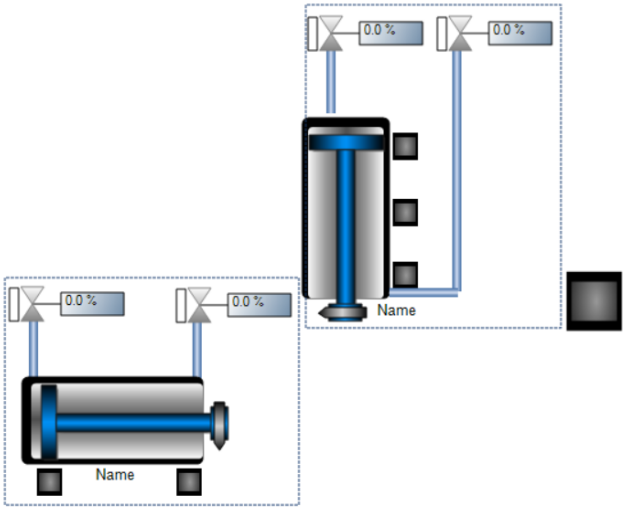


Figure. HMI representation of two-cylinder system

LULEÅ UNIVERSITY OF TECHNOLOGY

Event log

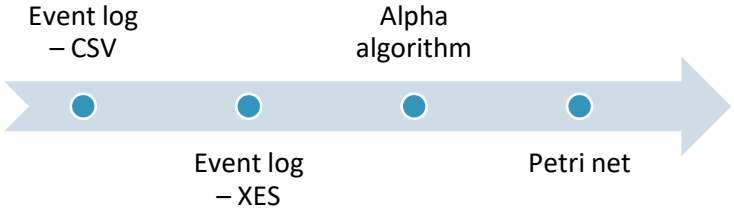
```
ProcessId,Timestamp,Component,Action
S-M
1001,2021-08-20 11:02:01.097932,VERTICALCYLINDER,VCEXT=TRUE
1001,2021-08-20 11:02:02.984882,VERTICALCYLINDER,VCPOSITION=MID
1001,2021-08-20 11:02:06.865219,VERTICALCYLINDER,VCEXT=FALSE
S-M-S
1002,2021-08-20 11:02:01.097932,VERTICALCYLINDER,VCEXT=TRUE
1002,2021-08-20 11:02:02.984882,VERTICALCYLINDER,VCPOSITION=MID
1002,2021-08-20 11:02:06.865219,VERTICALCYLINDER,VCEXT=FALSE
1002,2021-08-20 11:02:06.864222,VERTICALCYLINDER,VCRETR=TRUE
1002,2021-08-20 11:02:10.467188,VERTICALCYLINDER,VCPOSITION=START
1002,2021-08-20 11:02:10.465197,VERTICALCYLINDER,VCRETR=FALSE
```

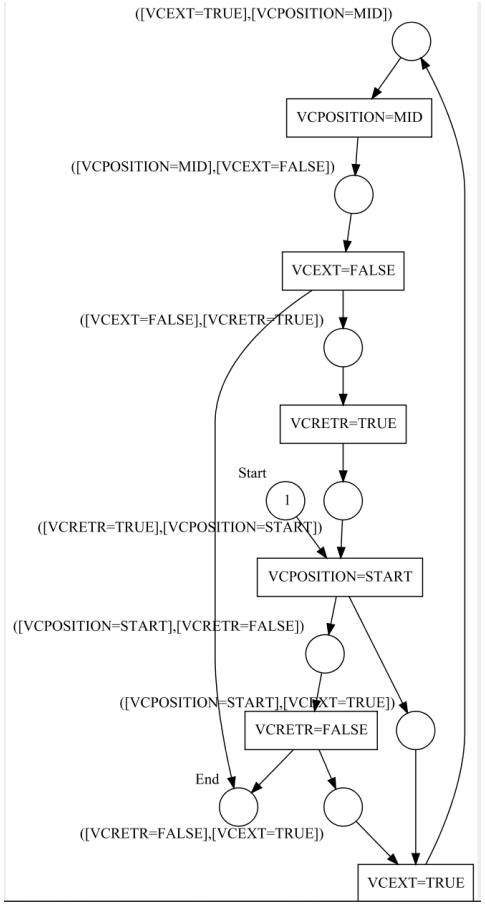
LULEÅ UNIVERSITY OF TECHNOLOGY

Process mining using ProM

Process mining helps to extract process models from event logs

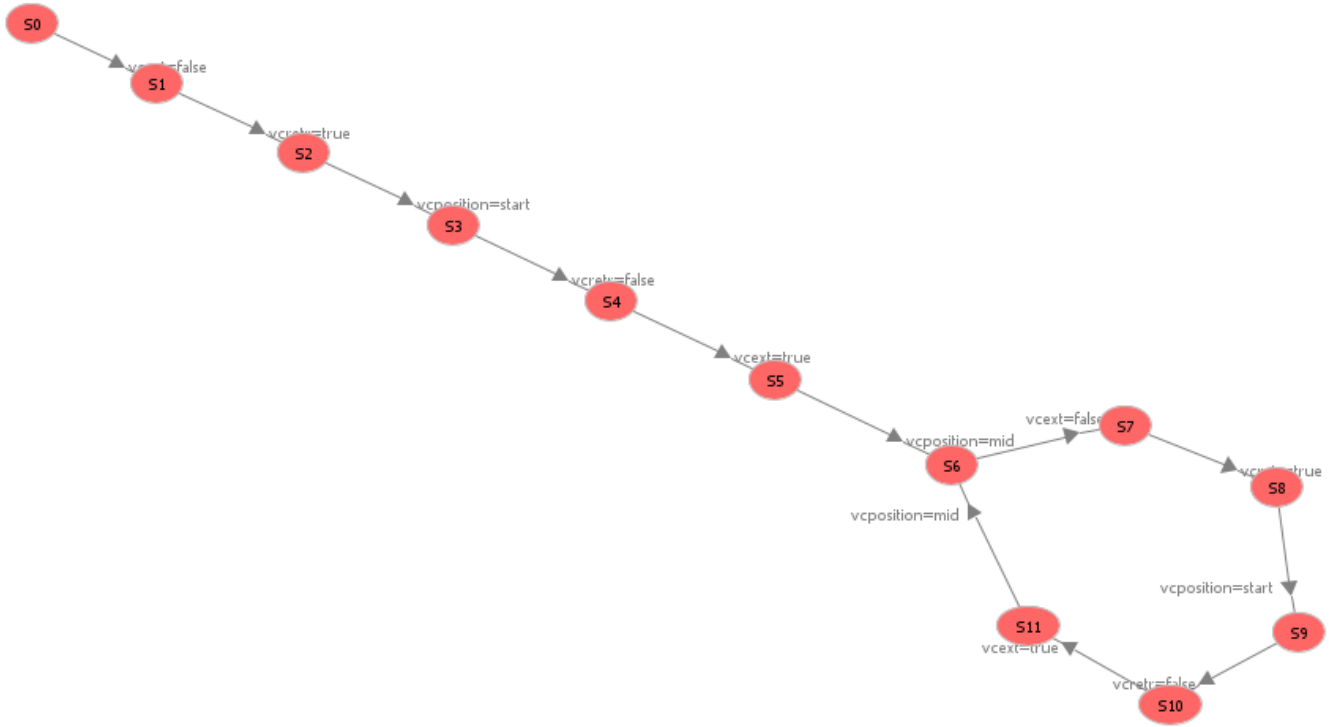
Alpha algorithm is used to develop models in the form of Petri nets





LULEÅ UNIVERSITY OF TECHNOLOGY

Reachability Graph



Conclusion and future plan

- Implemented monitor and plant model from recoreded event log
- The tool chain helps to verify and evaluate the generated plant model
- Continous development and evaluation of DCS
- Accurate implementation of formal model is done with the help of fb2smv and NDT

- Identification of timing problems due to different time scales of controller and plant
- Tool chain identifies all possible errors and automatically fixes them
- Ensuring the digital twin records all possible traces in the plant
- The developed plant model generation method should be applied to another system to see if it works correctly

LULEÅ UNIVERSITY OF TECHNOLOGY

Thank you

LULEÅ
UNIVERSITY
OF TECHNOLOGY