Lab Introduction

FY2023

石井 大輔 / Daisuke ISHII

情報科学系 / School of Information Science

次世代デジタル社会基盤研究領域 / Next-gen digital infrastructure area

dsksh@jaist.ac.jp, https://www.dsksh.com

Overview of Ishii lab

- Work on both theoretical aspects and implementations/ experimentations on software
- Software engineering/science for cyber-physical systems (CPS)
  - Modeling language for CPS
  - Model checking and testing methods for CPS
  - Etc.
- The current number of students is small
- Feel free to contact me (dsksh@jaist.ac.jp) and visit the lab!

物理情報系 / Cyber-physical systems (CPS)

- Computer systems that is tightly integrated with physical environment
  - Input: sensors; Output: actuators
  - Hybrid system of discrete and continuous behaviors
  - Example: automobiles, airplanes, robots, houses, medical devices, power plants, etc.

- Inter-disciplinary area
  - Programming languages, software engineering, numerical simulation, control theory, optimization, etc.

Image courtesy of NSF.

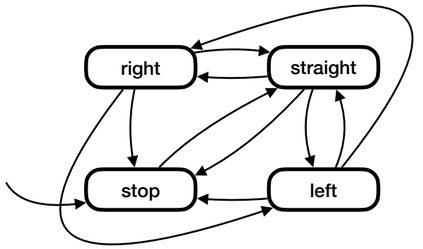
Modeling CPS

- Describe two components
  - Physical system (plant): Continuous system
    - E.g. mathematical equations
  - Cyber system (controller): Discrete system
    - E.g. state transition systems

$$x'(t) = u(t) \cos \theta(t)$$

$$y'(t) = u(t) \sin \theta(t)$$

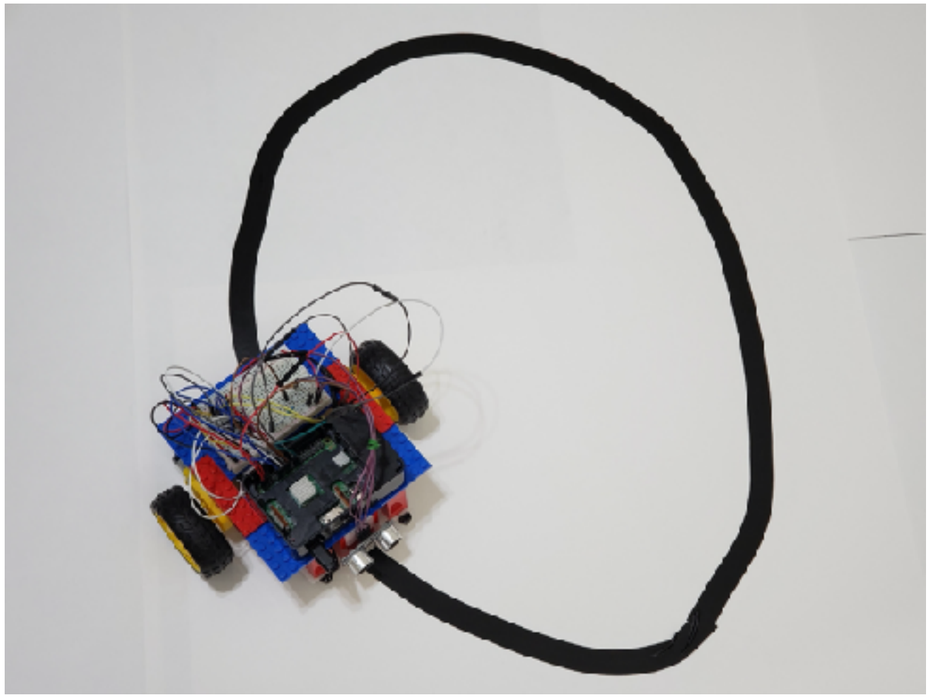
$$\theta'(t) = w(t)$$



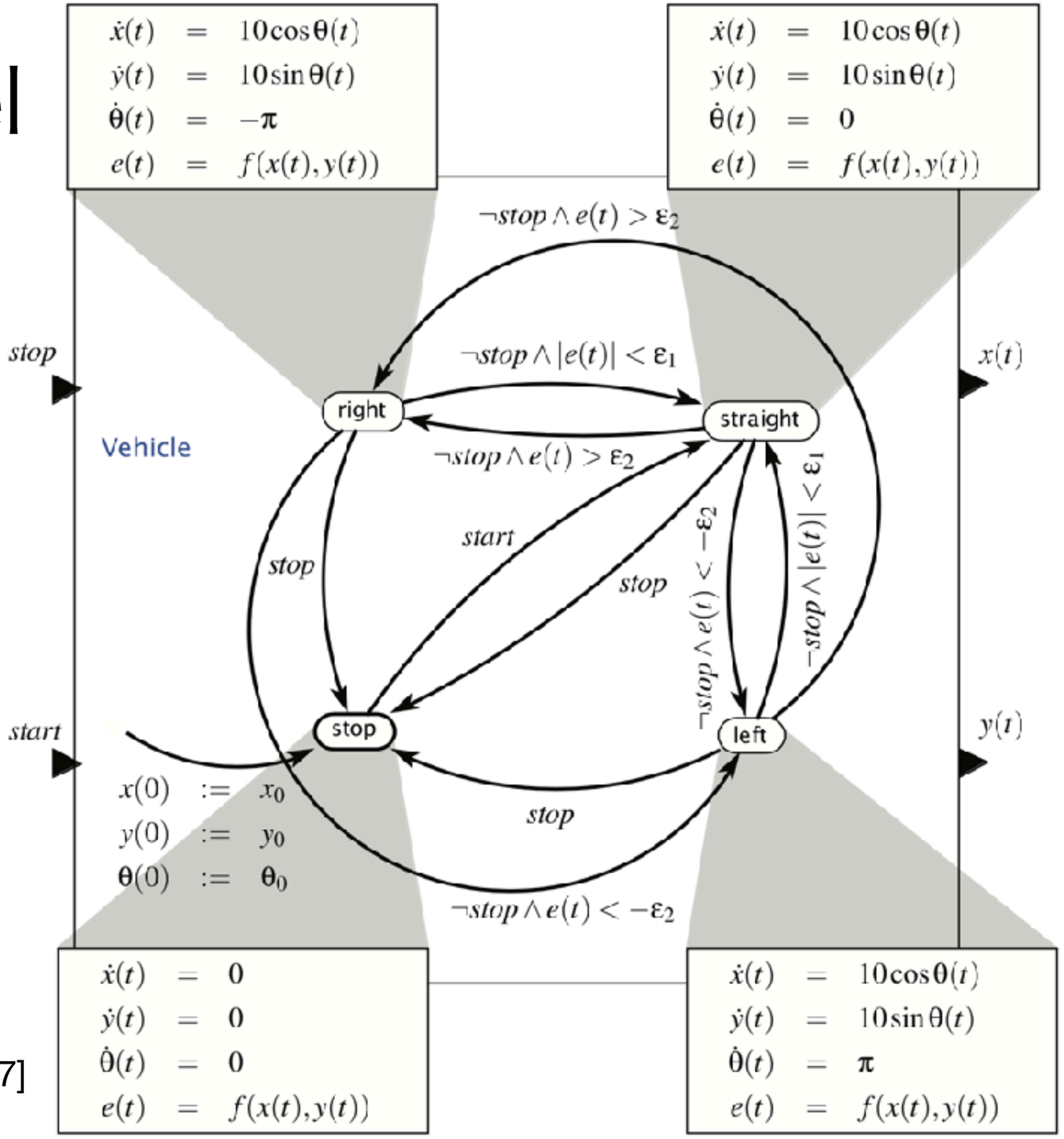
- CPS modeling languages
  - Provide syntax for describing both continuous and discrete behaviors
  - Example
    - MATLAB/Simulink/Stateflow (graphical)
    - HydLa [Ueda, Ishii+], Acumen [Taha+], Lustre [Caspi+] (textual)

Example CPS model

- Line tracer



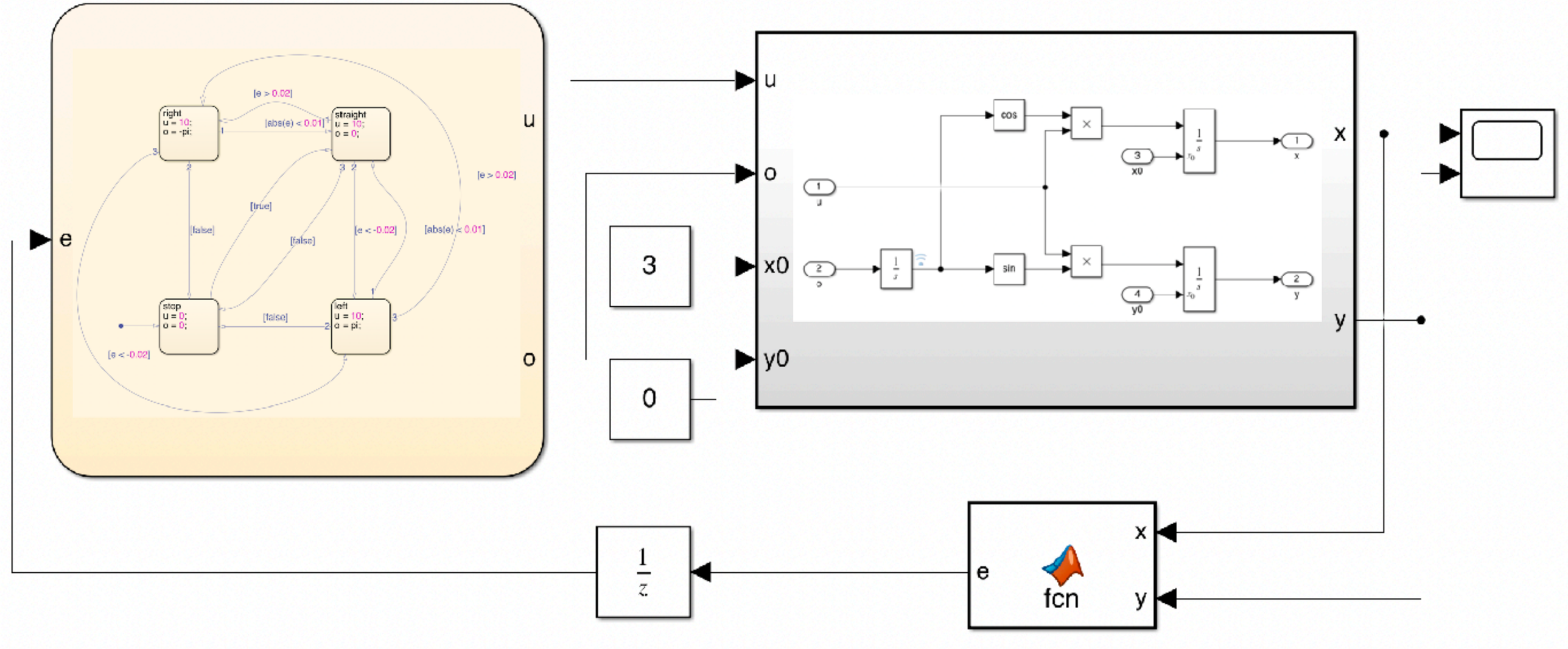
https://automaticaddison.com/how-to-make-a-line-following-robot-using-raspberry-pi/



[Lee&Seshia, 2017]

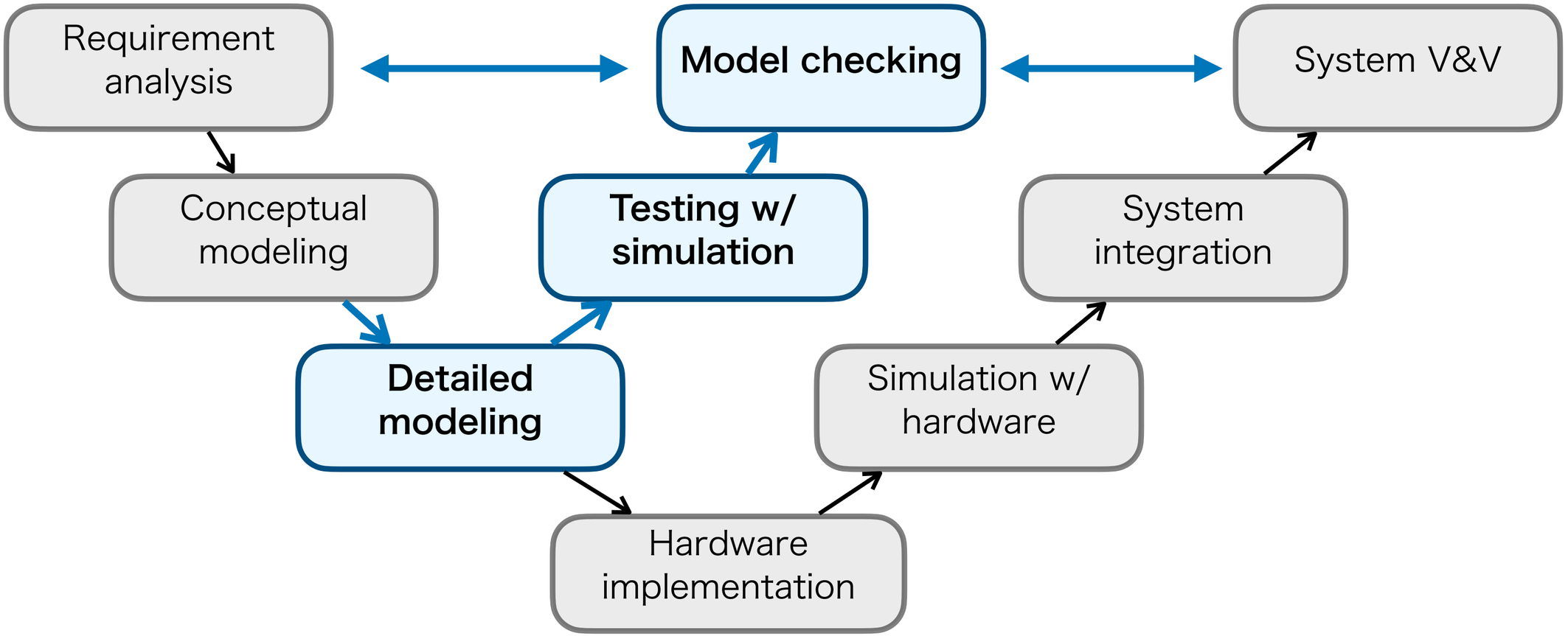
Example CPS model (line tracer)

- Model described with Simulink/Stateflow



モデル検査の対象 / Model checking target

- We aim at the verification of CPS models

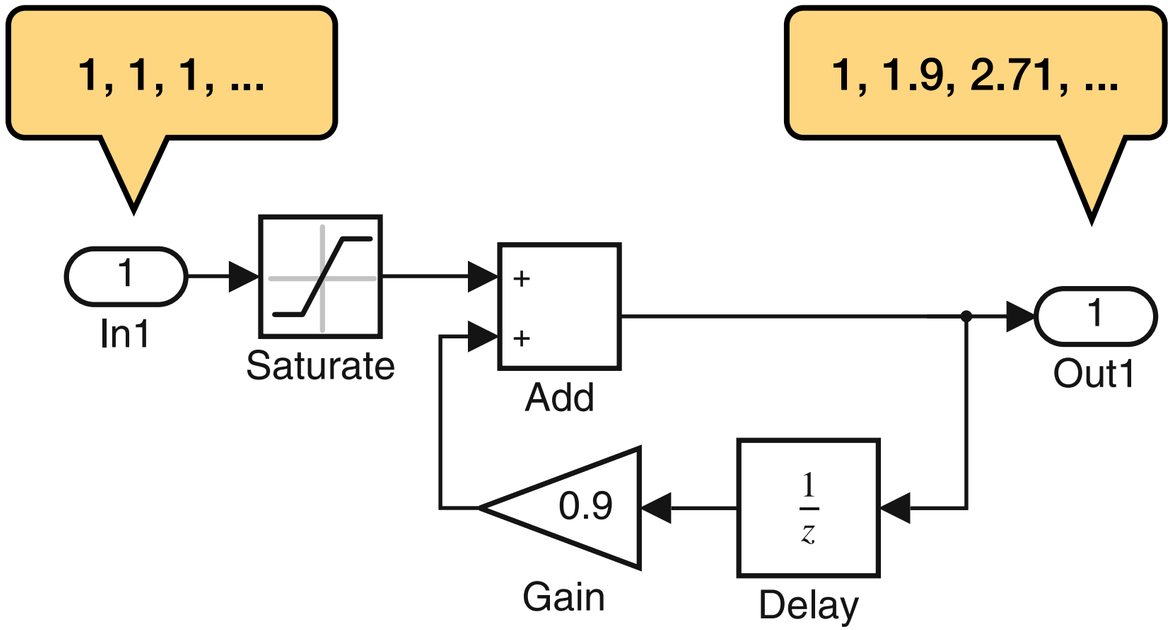


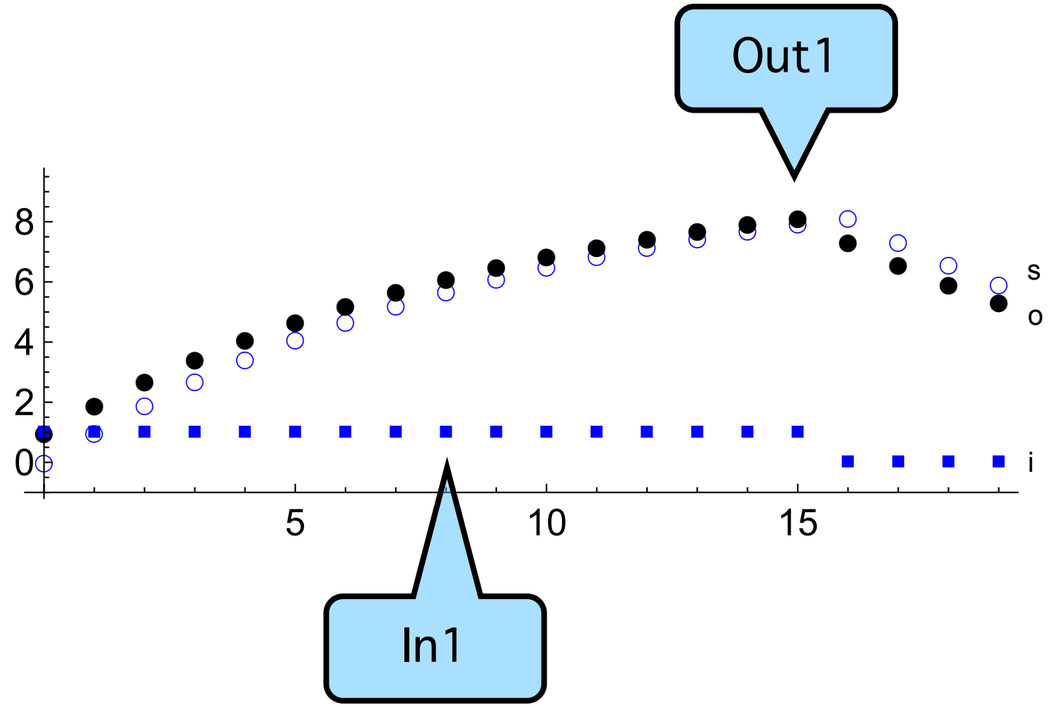
Overview

- Issues in the modeling/simulation/verification of cyber-physical systems (CPS)
  - Autonomy and scaling (in size and complexity) of systems
  - Approximations made in modeling (abstraction) and simulation (numerical errors)
  - Computational difficulty in verification
  - etc.
- Objective: Enable to model CPS appropriately and to verify their useful properties

(Discrete-time) Simulink models

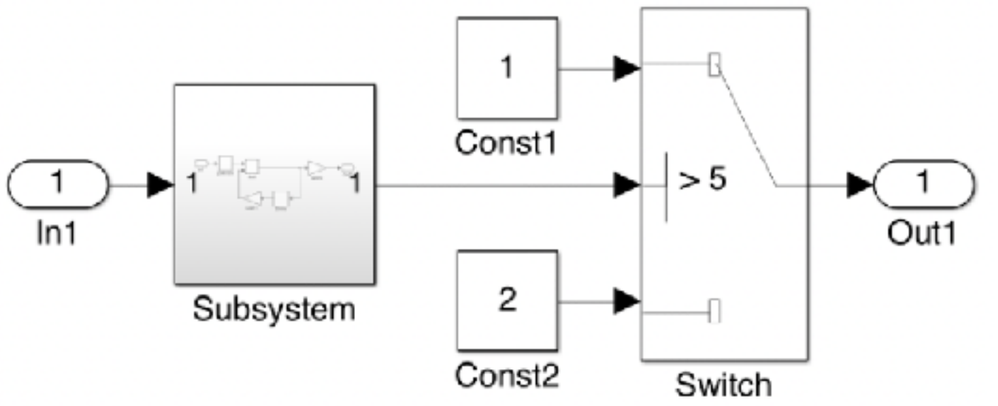
- Diagrams describing computation on signals

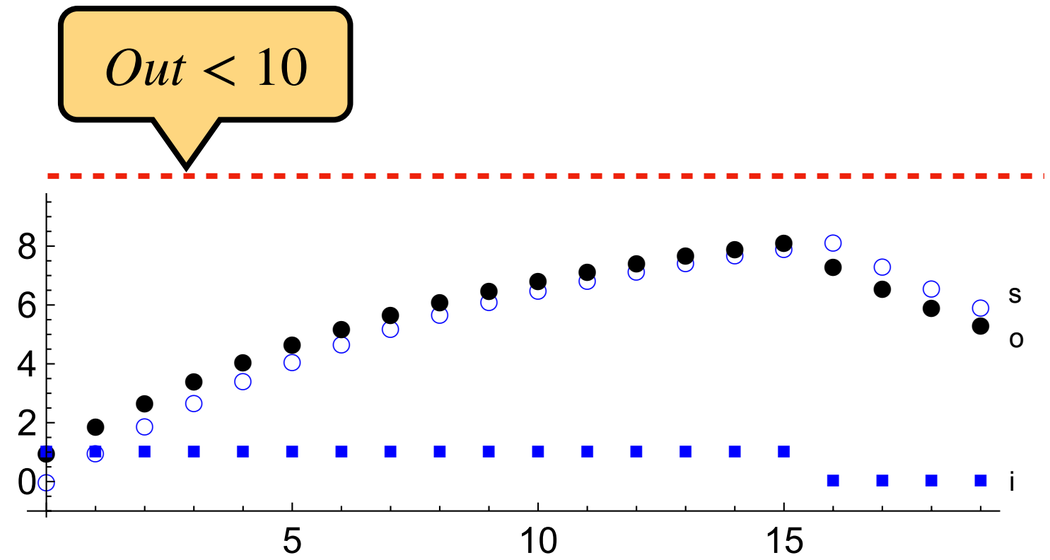




Safety properties

- Properties stating that "something bad never happens"
  - Example: "always $Out < 10$"
  - Example: "when $Out = 2$, Freq(In) > 1000[Hz]"



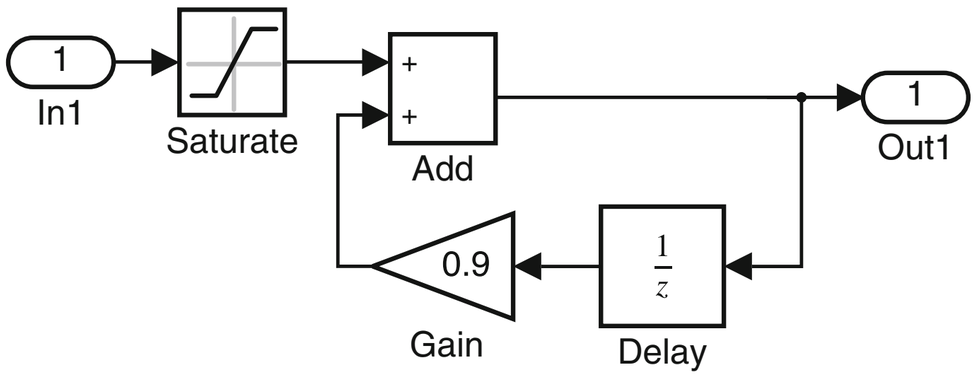


Simulink encoding example

- Description of a model content and a property in a logic formula (SMT-LIB)

$I(s_0) \iff s_0 = 0$

$T(s, s', i, o) \iff \exists lv, \ldots$
$\wedge\, o = lv + 0.9 s_0 \wedge s1 = o$




```
(define-fun init ((s@0 Real)) Bool
  (= s@0 0)
)
(define-fun trans ((c Int)
  (s@0 Real) (s@1 Real) (a Real) (o Real))
  Bool
  (let ((lv (saturate 1 (- 1) i)))
    (and (= o (+ lv (* 0.9 s@0)))
         (= s@1 o) )

 ;; Invariant instrumentation.
 (<= o 10)
 ) )
...
```

$o \leq 10$

Silver bullet: SMT solvers

- Tool for checking satisfiability modulo theories
  - Input: predicate logic formulas
  - Based on efficient search algorithms
  - E.g. Z3, https://github.com/Z3Prover/z3
  - E.g. CVC5, https://cvc5.github.io/

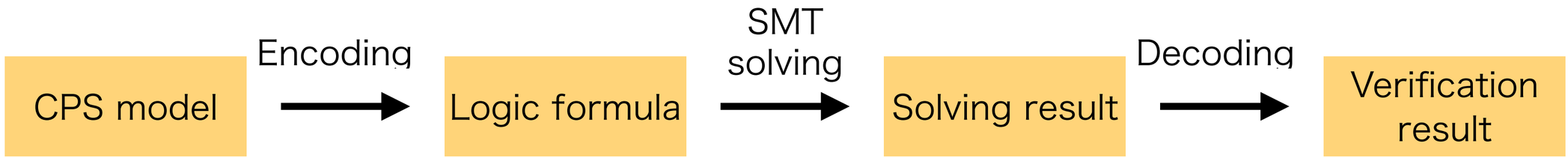
- Example theories
  - Integer/real arithmetic
  - Equality and functions
  - Bit vectors
  - Differential equations

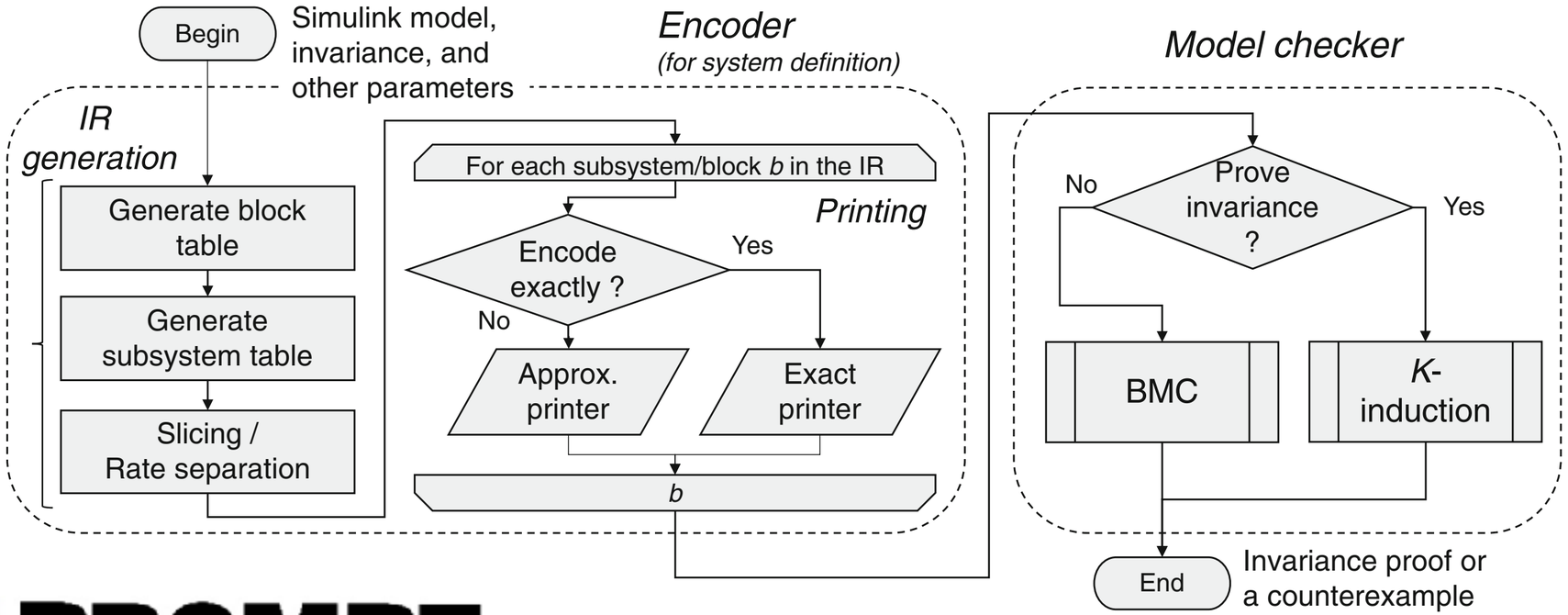
$x = 2y + 1 \ \wedge \ (x > y \ \Rightarrow \ z = y / x)$

x, y: integer variables
z: real variables

Solution: Satisfiable
$x = 3$, $y = 1$, $z = 0.333...$

Example: SMT-based model checking of Simulink models





PROMPT
Performable RatiOnalized Model Perfectionalization Tool

https://www.gaio.co.jp/products/prompt-2/

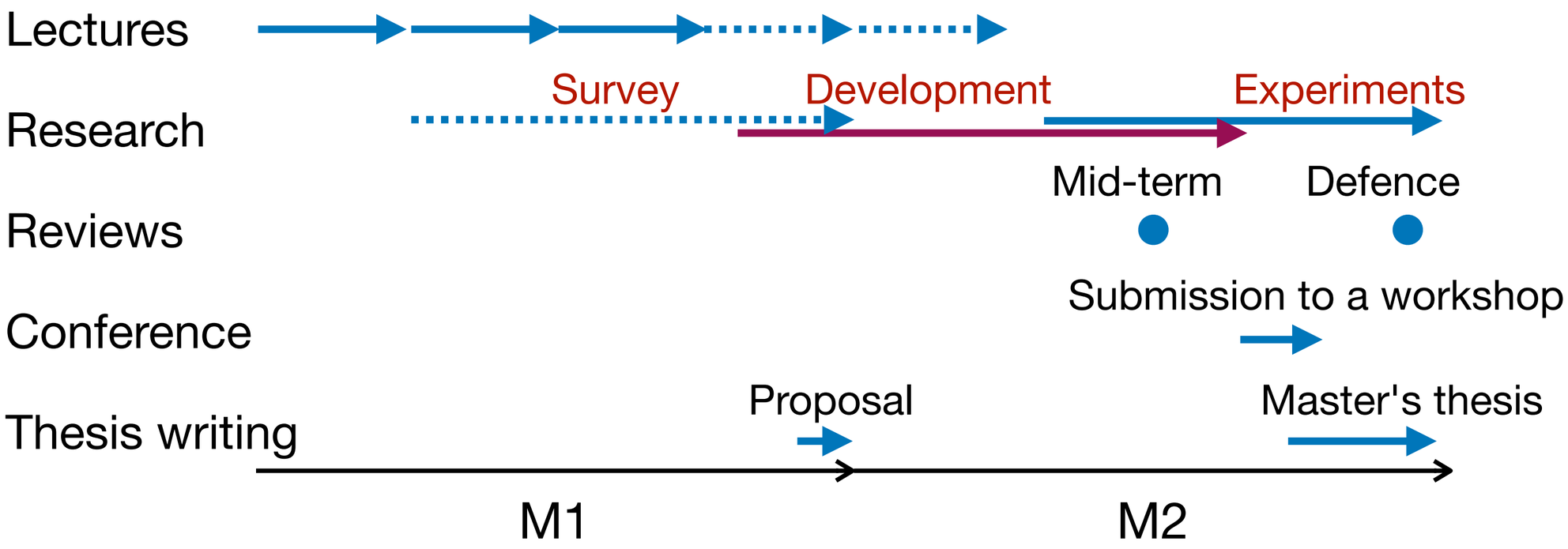
D. Ishii, T. Tomita, T. Aoki, T.Q. Ngô, T.B.N. Do, H. Takai:
SMT-Based Model Checking of Industrial Simulink Models,
ICFEM, LNCS 13478, pp. 156-172, 2022.

Model checking applications

- Model-based testing
  - Use models as a test oracle
- Test generation
  - Boundary test objectives
  - E.g. Search for an input signal that can enable a Switch block
- Coverage testing
  - Check whether every block is activated at lease once in a test execution
- Safety verification
  - Instrument a failure detection circuit and check whether it is activated

Example Studying Schedule at JAIST

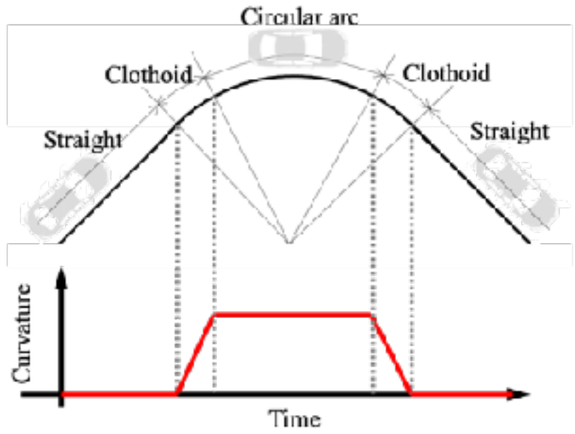
- 1st year: Focus on the lectures
- 2nd year: Mainly work on the research at the lab



研究プロジェクト / Research project

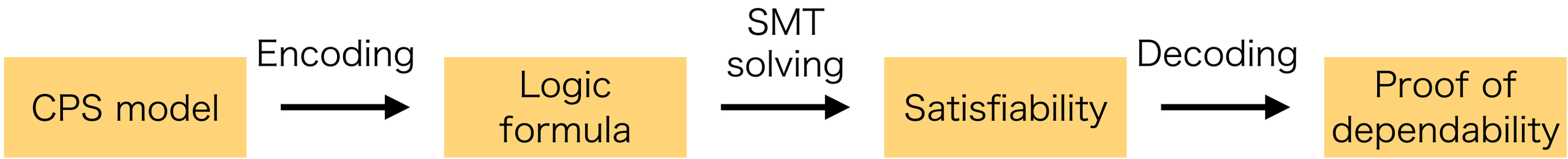
- Application development

Robot arm controller



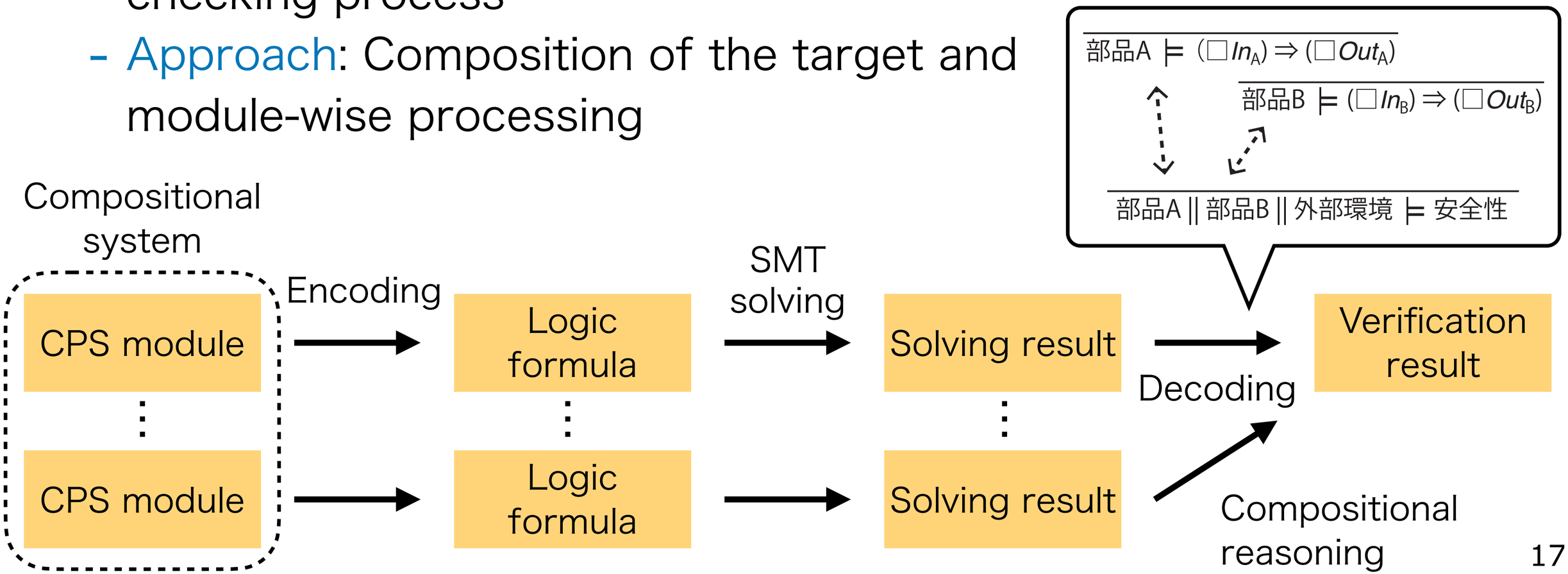
Driver-assistance system

- Development of an SMT-solver-based MC method



Example master's research (1)

- Compositional checking of models
  - Issue: Scalability issue of the model checking process
  - Approach: Composition of the target and module-wise processing

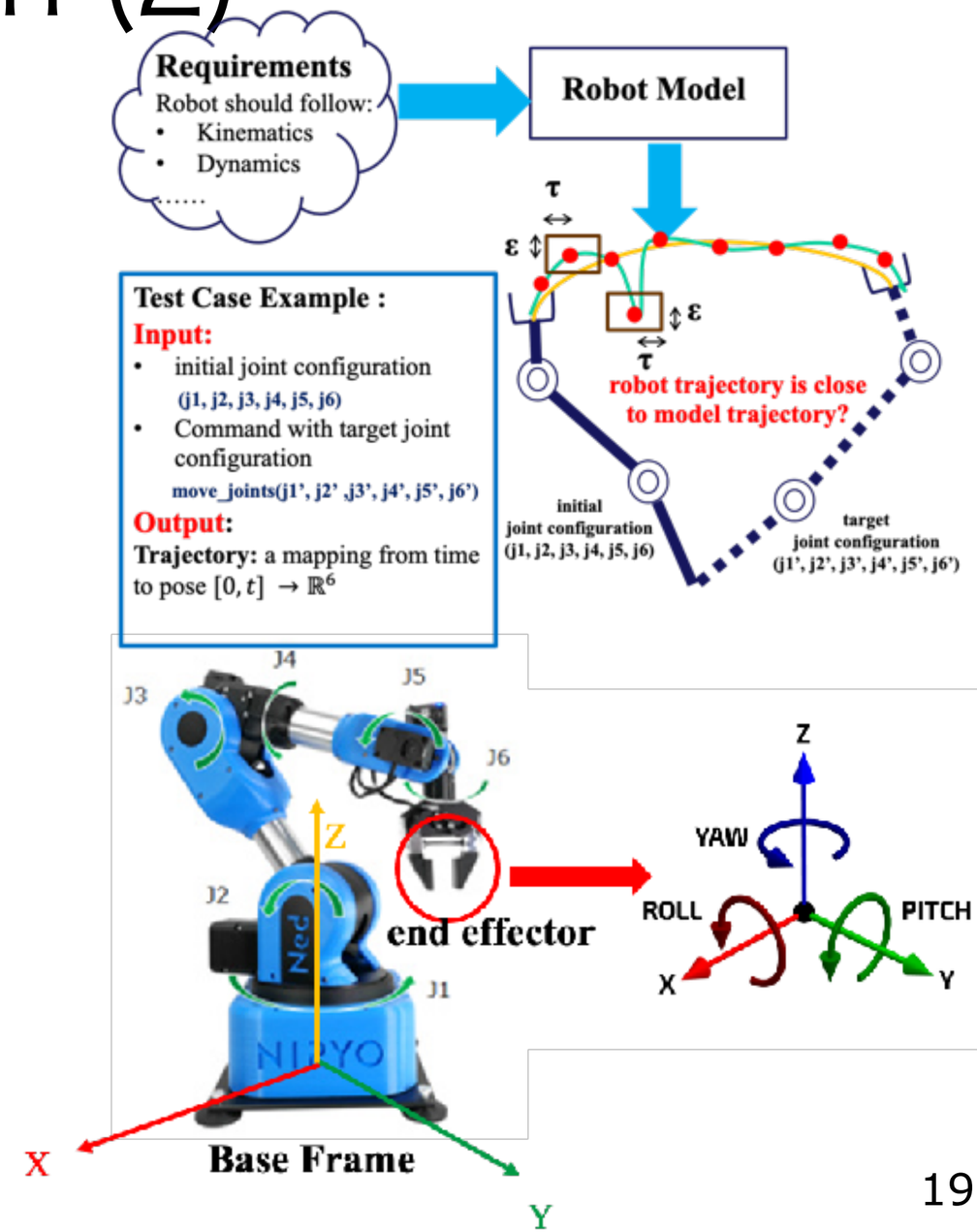


Example master's research (1)

- Research items
  - Survey
    - On MC methods/tools (e.g. Kind2, SMT solvers)
    - On compositional MC methods
  - Theoretical development
    - Design of a new MC method
    - Proof of the correctness of the method
  - Software implementation
    - Extension of an existing tool
  - Experiments
    - Collect motivating examples
    - Evaluation of the method

Example master's research (2)

- Test method for a robot arm
  - Issue: Gap between the model and the implementation in the robot development
    - ✳ E.g. gap w.r.t time and poses
  - Approach:
    Application of the model-based testing (MBT) method



Example master's research (2)

- Research items
  - Survey
    - Robotics basics, ROS
    - Model-based testing methods
  - Theoretical development
    - Modeling of kinematic and dynamical aspects of the target robot
    - Design of a conformance checking method
  - Software implementation
    - Conformance checking module for the ROS framework (w/ Python)
  - Experiments
    - Case study on the robot/model conformance
    - Evaluation of the proposed method

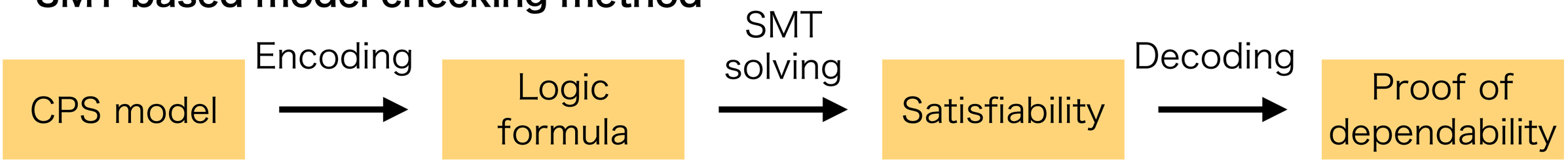
学生募集 / Call for new lab members

- 現在の研究プロジェクト
  / Current projects

Robot arm controller

Driver-assistance system

SMT-based model checking method



- その他のテーマでも / Or, other themes
  - 例: 機械学習系の検証 / E.g. verification of ML systems