# Formal Methods for Cyber-Physical Systems, at Work

**Ichiro Hasuo**
National Institute of Informatics & SOKENDAI
Research Director, ERATO MMSD Project, JST

# Outline

* Quality assurance of **cyber-physical systems**
    * **Formal methods at work**,
      coping with uncertainties
* Introducing the ERATO MMSD project
* Tech showcase:
  "formal methods that are **down-scalable**"
    * Monitoring
    * Search-based testing
* Applications, "**power of math**"

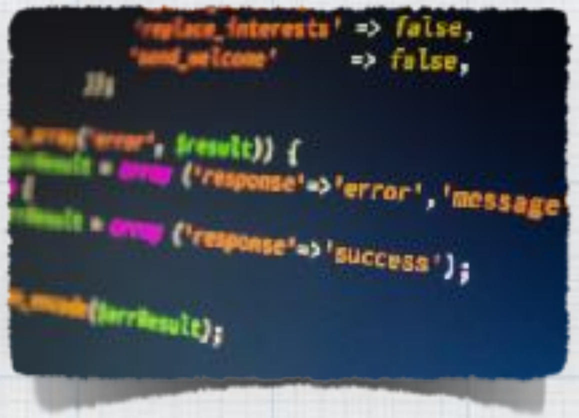
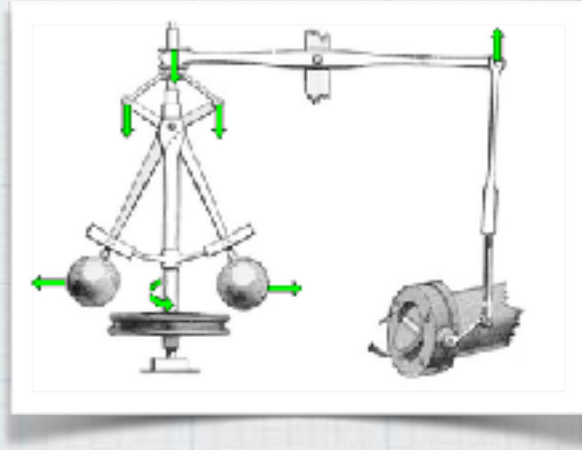
# Cyber-Physical Systems：
# Control Theory and Formal Methods/Software Science

- Cyber-Physical System (CPS)
  - “A mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users” (Wikipedia)
  - Physical plant (continuous)

    +

    Digital control (discrete)
  - In US: NSF Key Area of Research (2006-)



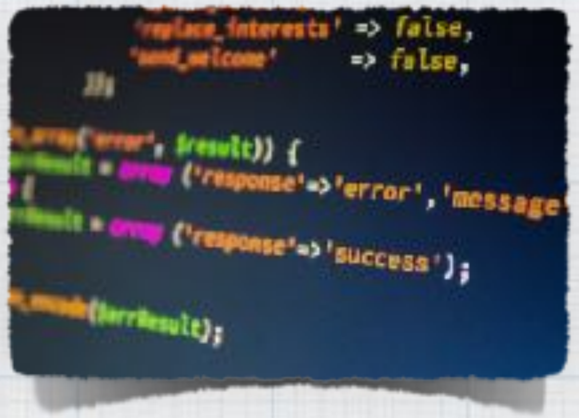



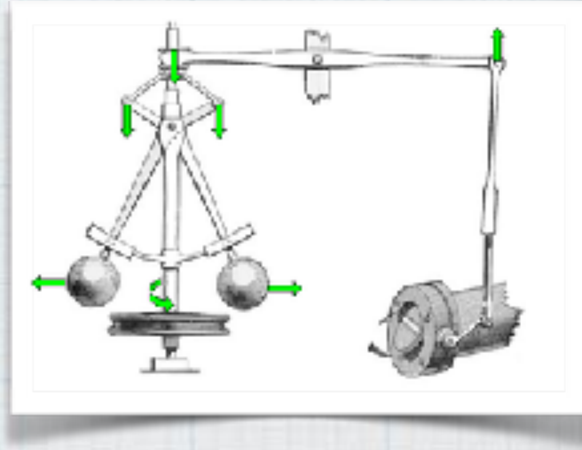
# Cyber-Physical Systems：
# Control Theory and Formal Methods/Software Science

- Formal methods:
  Logical proofs for “correctness” of (discrete) programs
  - Model checking
    (SPIN, NuSMV, Uppaal, PRISM, …) [Pnueli, Clarke, Emerson, Sifakis, …]
  - Theorem Proving
    (Coq, Agda, …) [Milner, Coquand, Leroy, Voevodsky, …]

- Control Theory:
  Analysis of continuous dynamics
  - Stability, Lyapunov function, …

- Their similarity is widely recognized
  - e.g. HSCC, one of the main conferences of annual CPS Week



# CPS Research, So Far (the V&V Aspect)

CPS
(esp. hybrid systems)

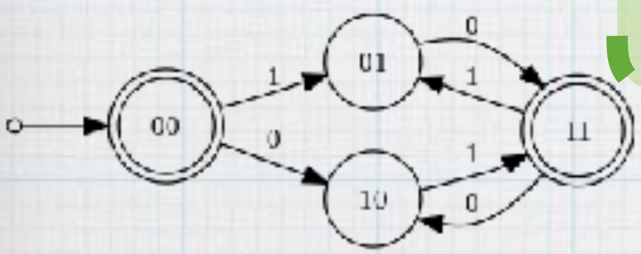
Analysis

Formal Methods

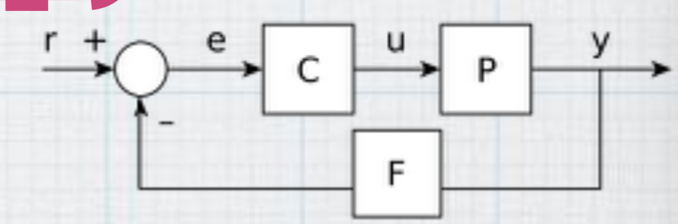
Collaboration

Control Theory

$\Box(p \Rightarrow \Diamond q)$

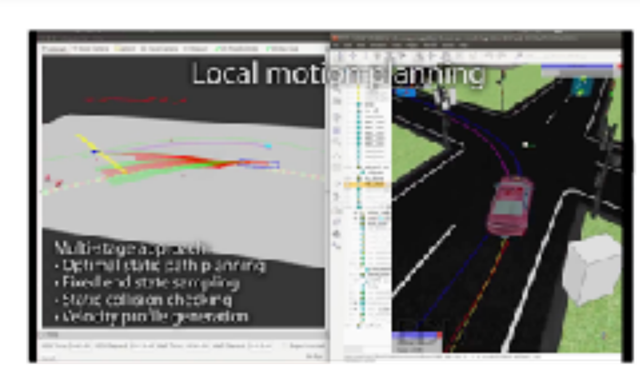



$x' = f(x, u)$




* Problem: practical applicability. Why?
  * Scalability
  * Uncertainties.
    Physical environments, black-box models, statistical AI/ML, …

# On ERATO MMSD




- JST ERATO Project, 2016/10-2022/03
  https://group-mmm.org/eratommsd

- Our goal:
  formal methods for cyber-physical systems (CPS)
  - Extend formal methods, from software to CPS
  - Safety, reliability, V&V (Verification & Validation).
    "Check if a system behaves as expected"
  - Emphasizing industry collaboration, also for scientific inspirations
  - Automated driving as a strategic target domain.
    Collaboration with U Waterloo:
    www.autonomoose.net

- Our team:
  - 28 researchers, > 20 students (as of 2019/09)
  - International and scientifically diverse

# Our Organization

ERATO MMSD

**International** and **multi-disciplinary**. "**creative chaos**"

**Kyoto U IS Site:**
**Advanced Deductive Verification**
**Leader:**
Kohei Suenaga

**Kyoto U RIMS Site:**
**Categorical Infrastructure**
**Leader:**
Masahito Hasegawa

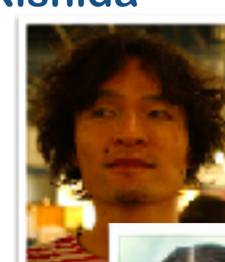
**Kyushu U Site:**
**Optimization for CPS V&V**
**Leader:**
Hayato Waki

**Osaka U Site:**
**Control Theory for CPS**
**Leader:**
Toshimitsu Ushio

**Group 0 @ NII:**
**Metatheoretical Integration**
**Leader:** Shin-ya Katsumata

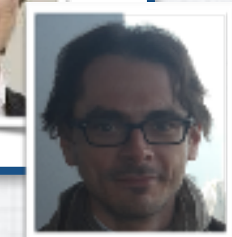
**Topics:**
Programming Languages, Formal Semantics, Categorical Models, Mathematical Logic, ...

**Group 1 @ NII:**
**Heterogeneous Formal Methods**
**Leader:** Ichiro Hasuo
**Subleader:** Masako Kishida



**Topics:**
Automata Theory, Control Theory, Formal Verification, Proof Assistants, Automated Deduction, Runtime Verification

**Group 3 @ NII:**
**Formal Methods and Intelligence**
**Leader:** Fuyuki Ishikawa
**Subleader:** Paolo Arcaini



**Topics:**
Software Engineering, Formal Modeling, Testing, Safe & Explainable AI

**Group 2 @ U Waterloo:**
**Formal Methods in Industry**
**Leader:** Krzysztof Czarnecki

**Topics:**
Automated Driving, Software Engineering, Machine Learning

# Members

2019.6, Tokyo NII Site

ERATO 蓮尾メタ数理システムデザインプロジェクト
ERATO Metamathematics for Systems Design Project
国立情報学研究所 & 科学技術振興機構 National Institute of Informatics & Japan Science and Technology Agency

G0 G1 G3

## Group Leaders, Assoc. Prof's


Shin-ya Katsumata


Ichiro Hasuo


Masako Kishida


Etienne Andre


Fuyuki Ishikawa


Paolo Arcaini

## Assistant Prof's (and similar)


Jeremy Dubut

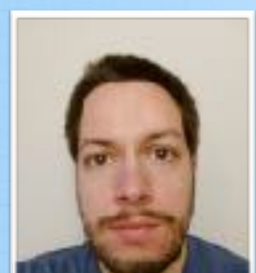

Taro Sekiyama


Akihisa Yamada


Ahmet Cetinkaya


Tsutomu Kobayashi

## Post-docs (and similar)


David Sprunger


Clovis Eberhart


Kenta Cho


Sasinee Pruekprasert


Toru Takisaka


Chao Huang


Xiaoyi Zhang

## Grad Students, RAs


Satoshi Kura


Yuichi Komorida

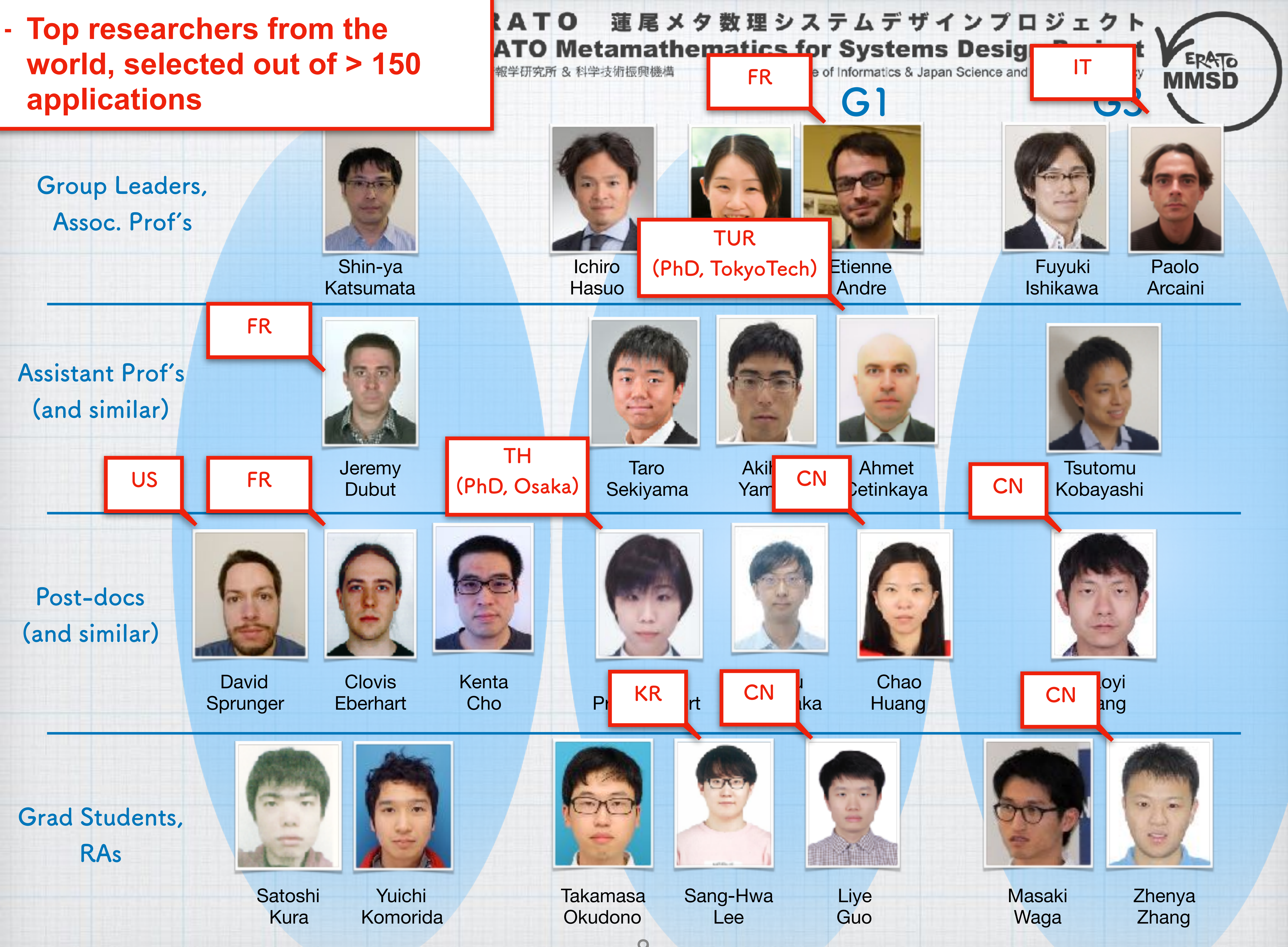

Takamasa Okudono


Sang-Hwa Lee


Liye Guo

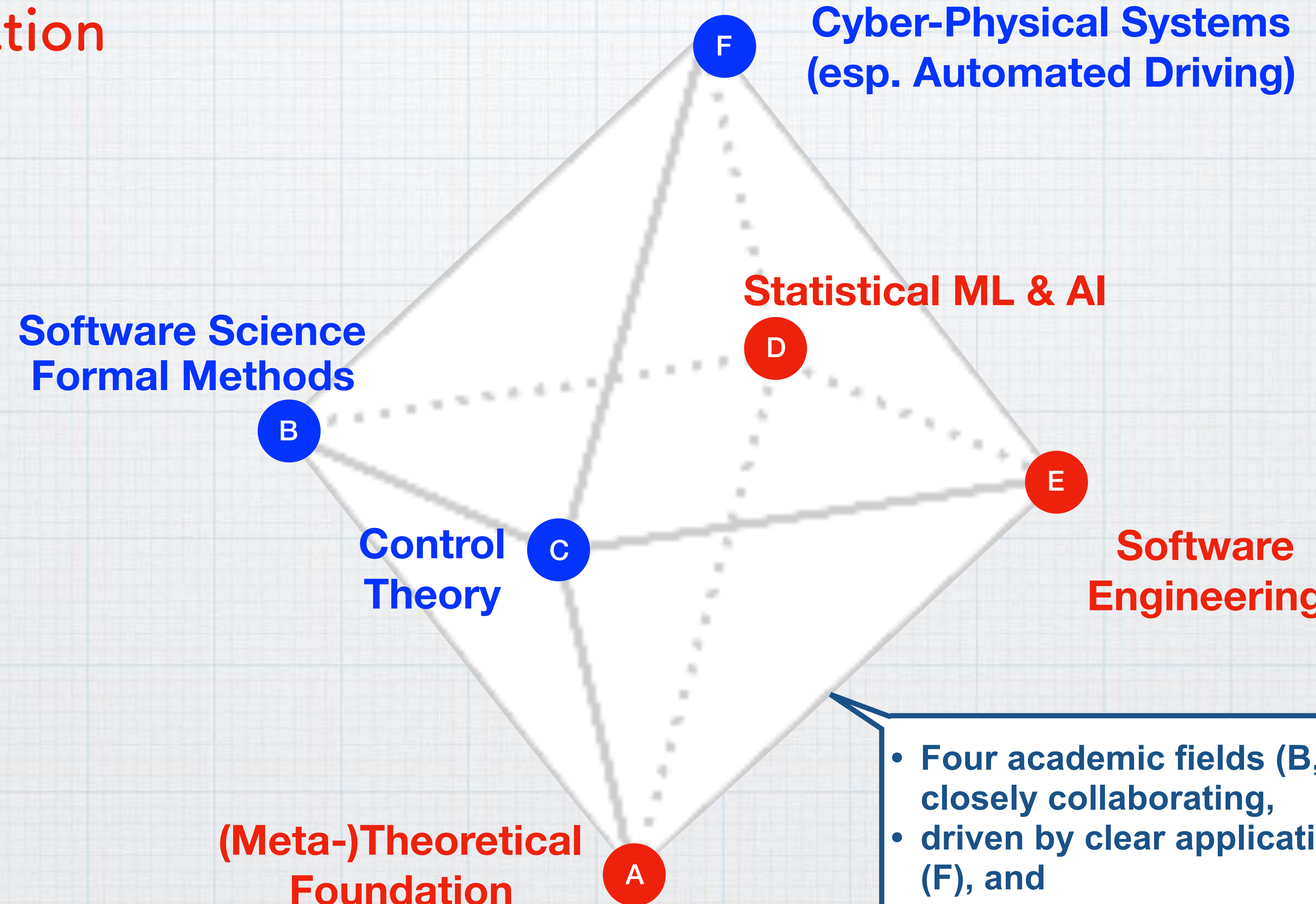

Masaki Waga


Zhenya Zhang



- Top researchers from the world, selected out of > 150 applications
RATO 蓮尾メタ数理システムデザインプロジェクト
ATO Metamathematics for Systems Design Project
報学研究所 & 科学技術振興機構
e of Informatics & Japan Science and
ERATO MMSD
G1
G3
FR
IT
TUR (PhD, TokyoTech)
FR
TH (PhD, Osaka)
US
FR
CN
CN
KR
CN
CN
Group Leaders, Assoc. Prof's
Shin-ya Katsumata
Ichiro Hasuo
Etienne Andre
Fuyuki Ishikawa
Paolo Arcaini
Assistant Prof's (and similar)
Jeremy Dubut
Taro Sekiyama
Ahmet Cetinkaya
Tsutomu Kobayashi
Post-docs (and similar)
David Sprunger
Clovis Eberhart
Kenta Cho
Chao Huang
Grad Students, RAs
Satoshi Kura
Yuichi Komorida
Takamasa Okudono
Sang-Hwa Lee
Liye Guo
Masaki Waga
Zhenya Zhang

# Interdisciplinary Efforts towards CPS: Six Scientific Fields


- Four academic fields (B,C,D,E) closely collaborating,
- driven by clear application goals (F), and
- backed up by mathematical foundation (A)

# Academic Achievements

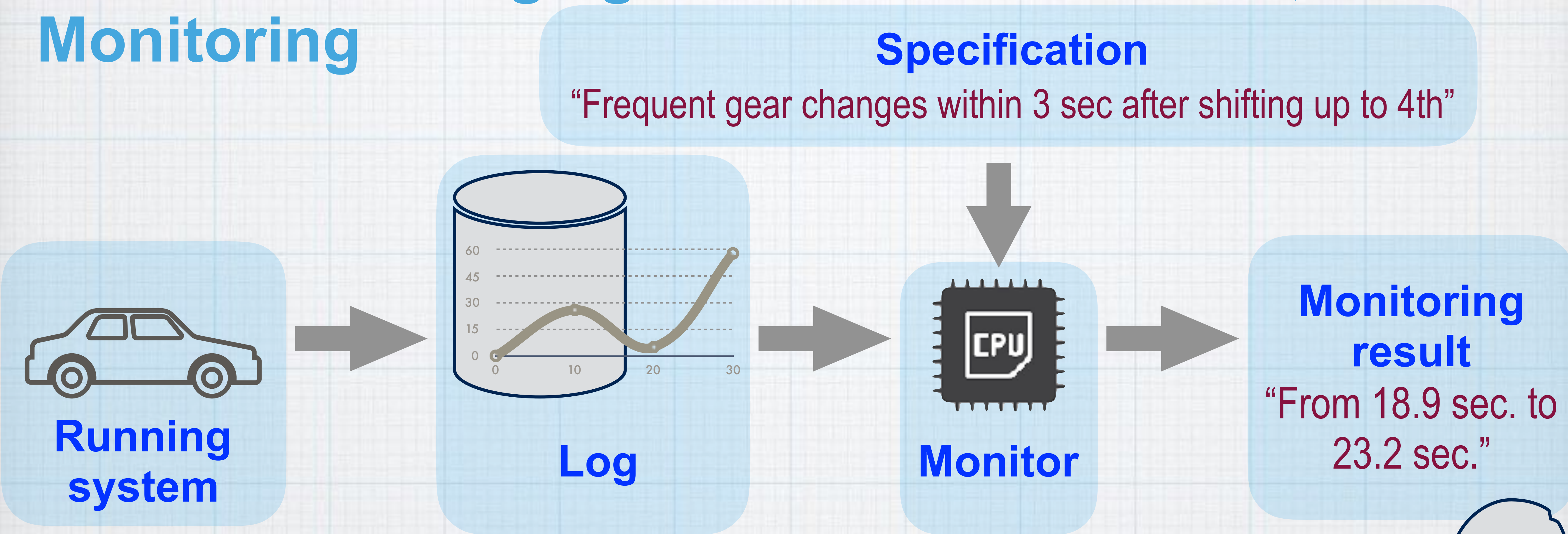
* International visibility:
  * CORE rank A* (top 4%, LICS, CAV, POPL, …):
    > 10 papers
  * CORE rank A (top 5~18%, ATVA, TACAS, GECCO, ICECCS, …):
    > 20 papers
  * Best paper awards：

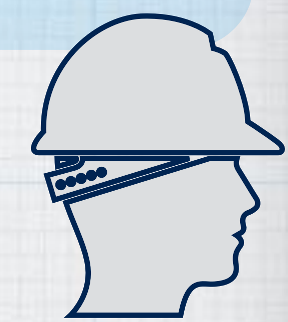
    ICECCS’18, FoSSaCS’19 (CORE rank A), FORMATS’19
  * At LICS’19 (CORE rank A*):
    **6 out of 60 accepted papers** were coauthored by us

# Outline

* Quality assurance of **cyber-physical systems**
  * **Formal methods at work**,
    coping with uncertainties
* Introducing the ERATO MMSD project
* Tech showcase:
  "formal methods that are **down-scalable**"
  * Monitoring
  * Search-based testing
* Applications, "**power of math**"

# Pattern Matching against Timed Automata, Monitoring



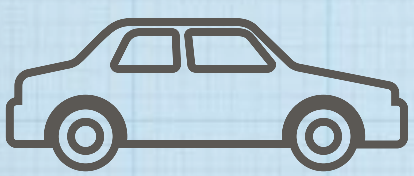



- Runtime verification, monitoring
- Not straightforward, esp. when specs involve timing constraints
  - Speed requirements (GBs of log per second)
  - Computing resource (embedded)
  - …
- Industry needs
- Technically: theory of **(parametrized) timed automata**

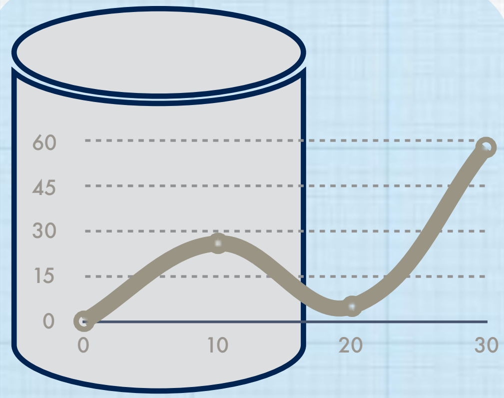
# Pattern Matching against Timed Automata, Monitoring

**Specification**

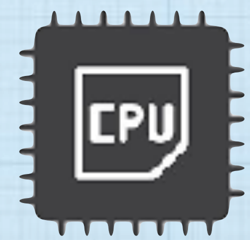
"Frequent gear changes within 3 sec after shifting up to 4th"



**Running system**



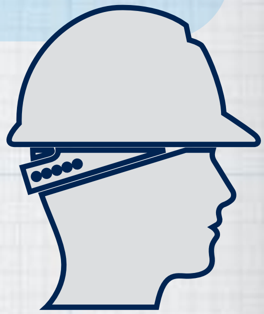

**Log**




**Monitor**

**Monitoring result**

"From 18.9 sec. to 23.2 sec."

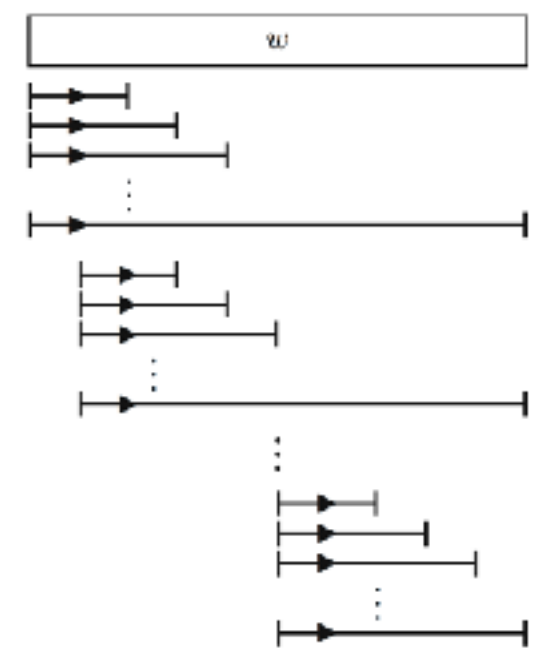


- Use cases
  - "Here is 1 PB of log, and I want to extract its relevant parts"
  - "Raise an alert if this specific type of anomaly occurs"

# Monitoring: Problem Formulations

- Given: a log, discrete time w = abaaacb…bbc
  a spec φ "no occurrence of c for 6 steps after b"
  Answer: all subsequences of w that satisfy φ

Nontrivial due to temporal causality




- Given: a log, continuous time w = (a, 0.12) (b, 1.28) …
  a spec φ "no occurrence of c for 6 seconds after b"
  Answer: all subsequences of w that satisfy φ
  [Ulus, CAV'17] [Waga+, FORMATS'17]

**Infinitely many such subsequences (starting at t=1? t = 1.01? t = 1.001? …)**
**➜ Efficient representation & computation by zones**

- Given: a log, continuous time w = (a, 0.12) (b, 1.28) …
  a parametrized spec φ(p)
  "no occurrence of c for p seconds after b" "b occurs with a period of p seconds"
  Answer: all the pairs of (p, (a subseq. of w that satisfies φ)))
  [Andre+, ICECCS'18] [Waga+, NFM'19] [Waga+, CAV'19]

**In industry, fixing a spec is a big challenge.**
**Parameters ➜ flexibility in specs**

# Monitoring: Our Achievements

- Given: a log, discrete time w = abaaacb…bbc
  a spec φ "no occurrence of c for 6 steps after b"
  Answer: all subsequences of w that satisfy φ

**Efficient algorithm from theory of timed automata. Processes ~ 1M events/ second (laptop).**

**[Waga+, FORMATS'17]**
https://github.com/maswag/monaa

**Also implemented on Renesas RH850**

- Given: a log, continuous time w = (a, 0.12) (b, 1.28) …
  a spec φ "no occurrence of c for 6 seconds after b"
  Answer: all subsequences of w that satisfy φ
  [Ulus, CAV'17] [Waga+, FORMATS'17]

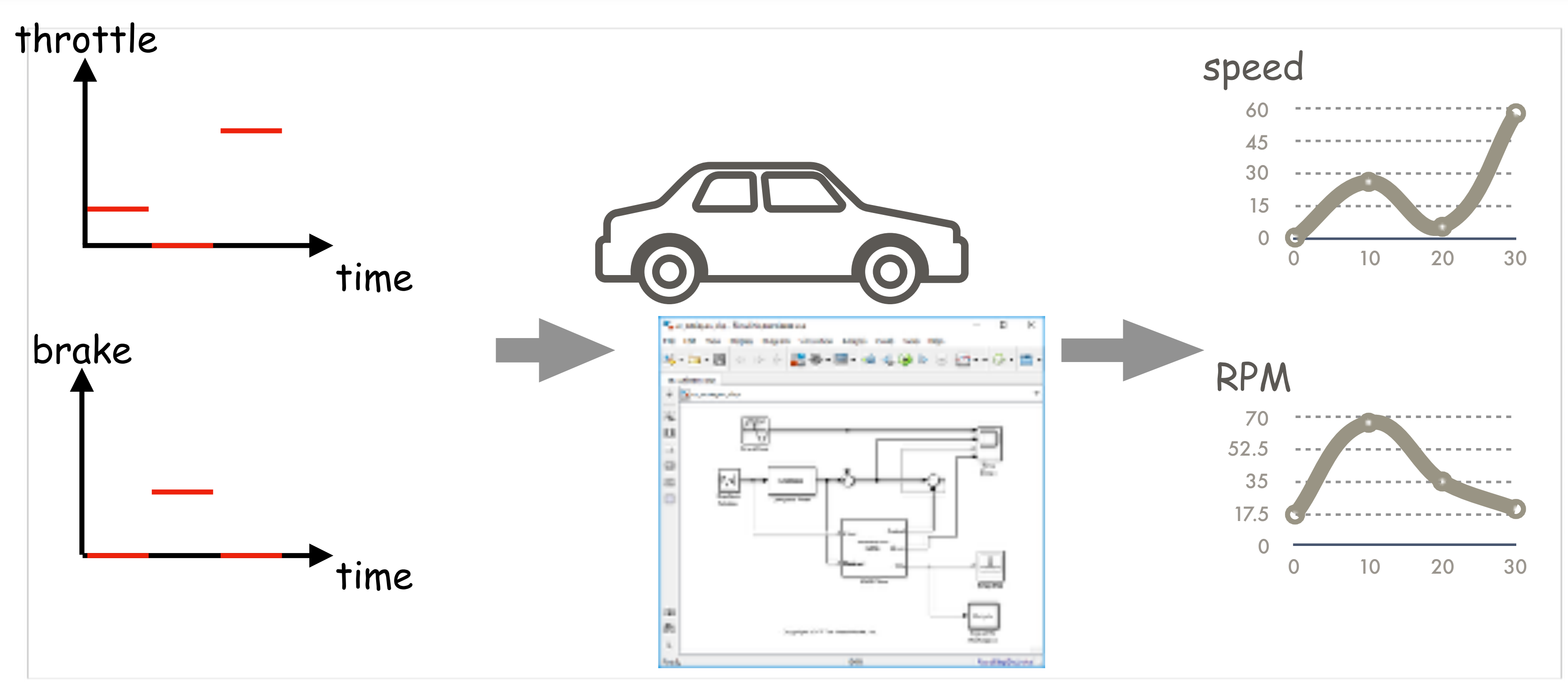
**Efficient algorithm using parametrized timed automata. Processes ~ 10K events/second (laptop). [Waga+, NFM'19]**
https://github.com/maswag/symon

- Given: a log, continuous time w = (a, 0.12) (b, 1.28) …
  a parametrized spec φ(p)
  "no occurrence of c for p seconds after b" "b occurs with a period of p seconds"
  Answer: all the pairs of (p, (a subseq. of w that satisfies φ)))
  [Andre+, ICECCS'18] [Waga+, NFM'19] [Waga+, CAV'19] …

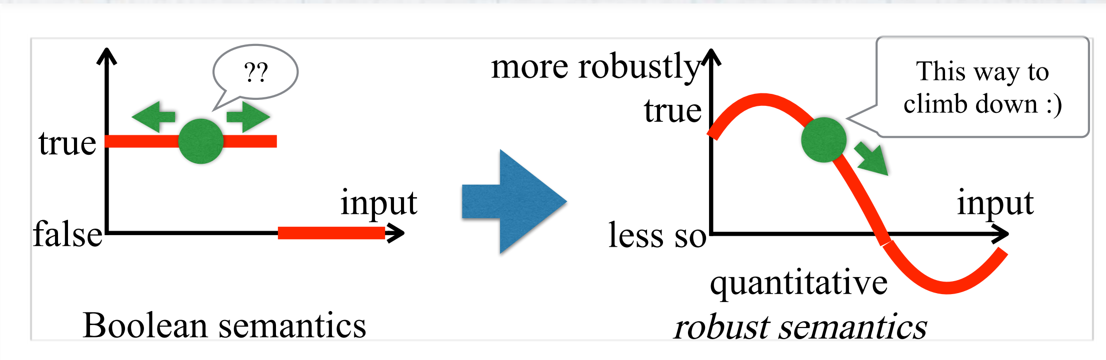
# Search-Based Testing by Reinforcement Learning

[Zhang+, EMSOFT'18] [Zhang+, CAV'19] [Fainekos & Pappas, TCS'09]

* Black-box, search-based testing. Actively search for erroneous input by:
  * Try an input signal
  * Observe the system's behavior
  * Choose the next input that is likely to be erroneous



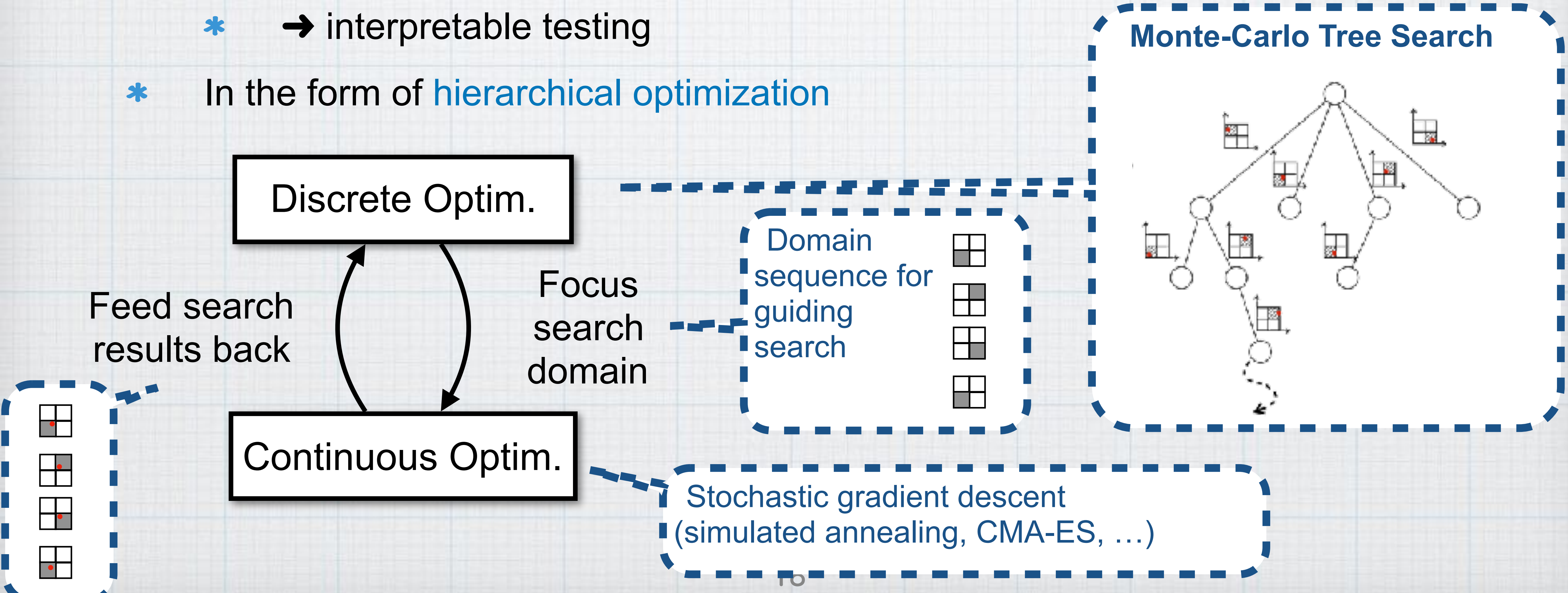

* [Fainekos & Pappas, TCS'09]
  A reinforcement learning problem, by moving
  * from the Boolean semantics (erroneous or not)
  * to quantitative "robust semantics" (how far from being erroneous)



# Search-Based Testing by Reinforcement Learning

[Akazaki & Hasuo, CAV'15]
[Zhang, Ernst, Sedwards, Arcaini & Hasuo, EMSOFT'18]
[Zhang, Hasuo & Arcaini, CAV'19] …

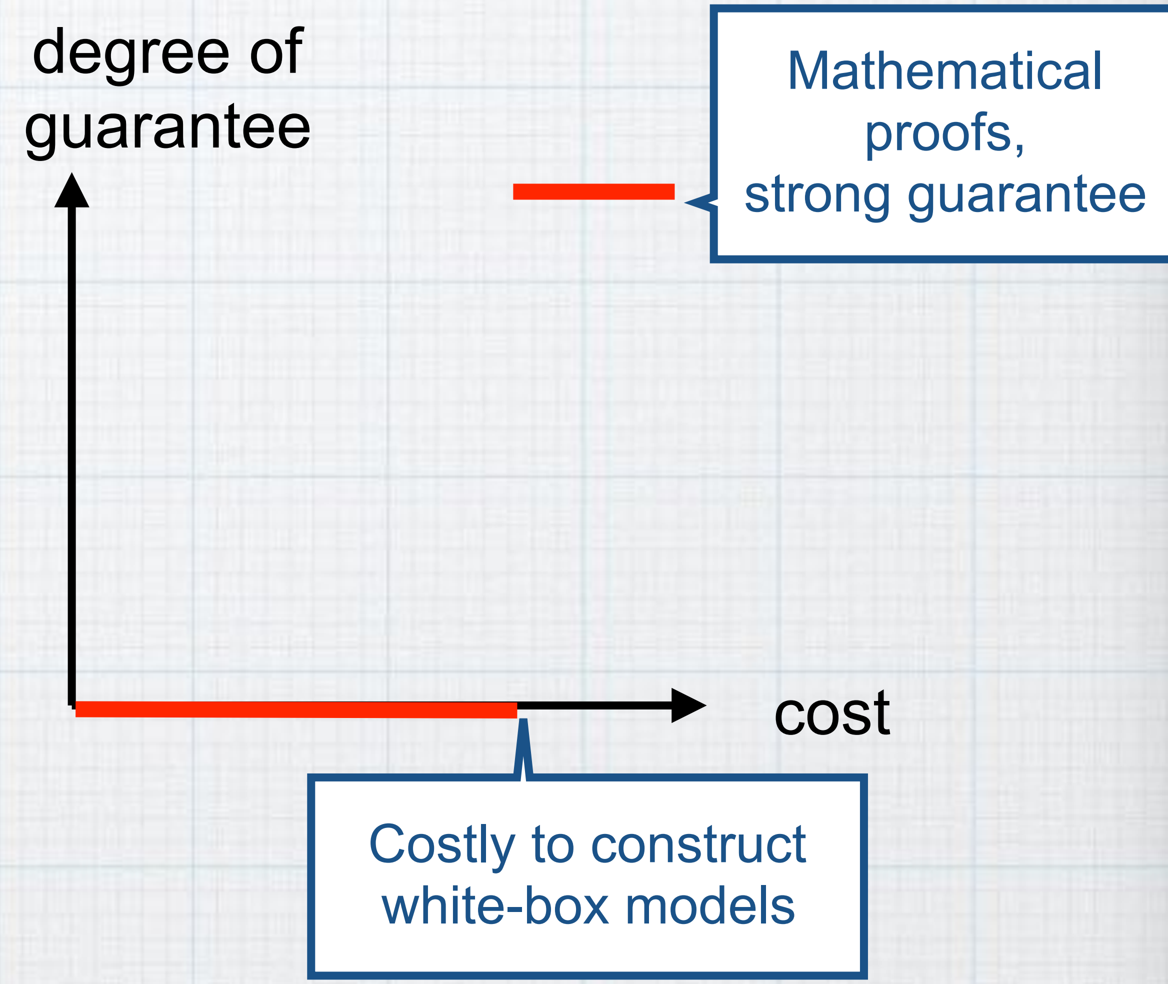
- Survey: [Kapinski+, IEEE Control Syst. '16]
  J. Kapinski, J. V. Deshmukh, X. Jin, H. Ito, and K. Butts, "Simulation-based approaches for verification of embedded control systems: An overview of traditional and advanced modeling, testing, and verification techniques," IEEE Control Syst., vol. 36, no. 6, pp. 45–64, Dec. 2016.
- Our Contribution In [Zhang+, EMSOFT'18] [Zhang+, CAV'19]
  - Exploit discrete structures in stochastic gradient descent
    - ➜ efficient and extensive search
    - ➜ interpretable testing
  - In the form of hierarchical optimization



# Towards Formal Methods That Are Down-Scalable

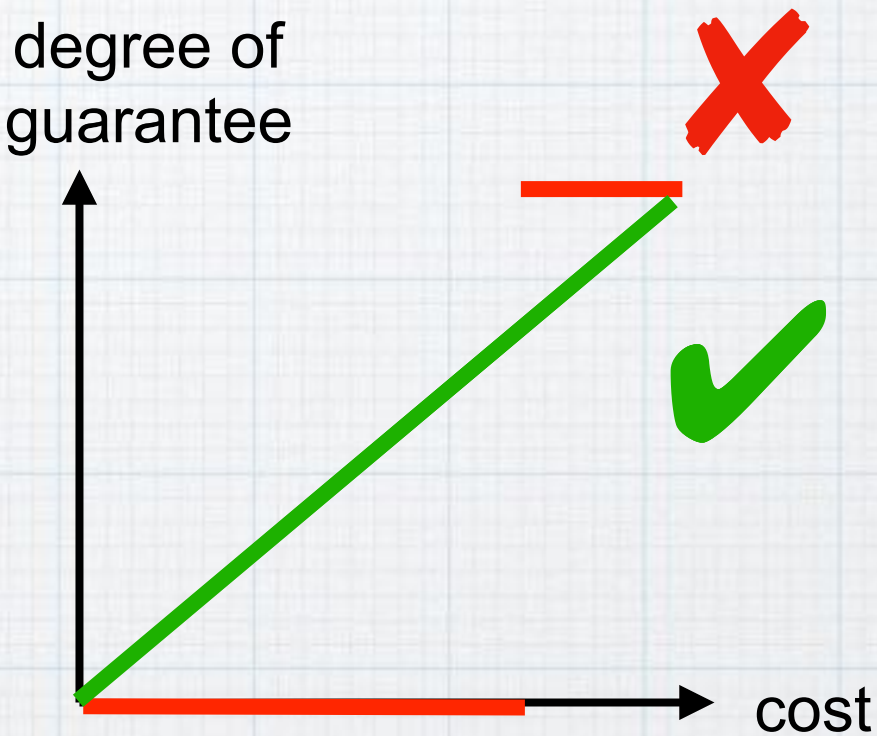
* Many FM methods are not down-scalable
  * They demand white-box models
  * ➜ huge cost before non-zero benefit

* Example applications to CPS:
  airplanes (Airbus), space (NASA), …
  * Failure is so expensive
    ➜ worth verification effots
  * Still takes decades
  * Integrating continuous dynamics is hard
    ➜ They focus on software



# Towards Formal Methods That Are Down-Scalable

- Real-world applications (esp. automotive domain), need down-scalability
  - Even if we can only afford half the cost,
  - degree of guarantee does not become zero, but half
- Our efforts at ERATO MMSD
  - Combine testing and formal verification. Search-based testing, monitoring
  - Contract-based verification ➜ formal safety architecture (contract-based verification, see reserve slides)



# Outline

* Quality assurance of **cyber-physical systems**
    * **Formal methods at work**,
      coping with uncertainties
* Introducing the ERATO MMSD project
* Tech showcase:
  "formal methods that are **down-scalable**"
    * Monitoring
    * Search-based testing
* Applications, "**power of math**"

# Industry Collaboration

- Mainly **automotive**, but not exclusively
  - Production systems
  - AI startups
- Inspiring **scientific research**, too
  - New problems
  - Solve a problem
    ➜ generalize the solution
    ➜ **scientific novelty**
- A lot of **industry needs**
  - Methods applicable off-the-shelf
    (monitoring, search-based testing)
  - High demand for formal verification
  - "What is an expected level of quality assurance?"

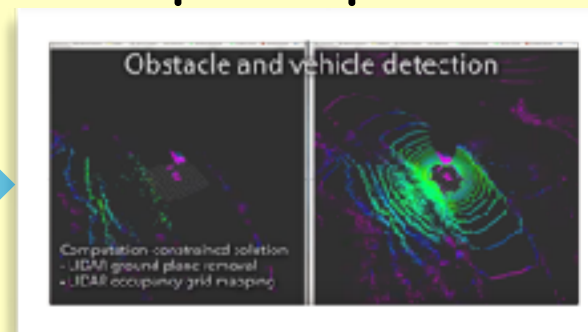
# Collaboration with U Waterloo

test tool

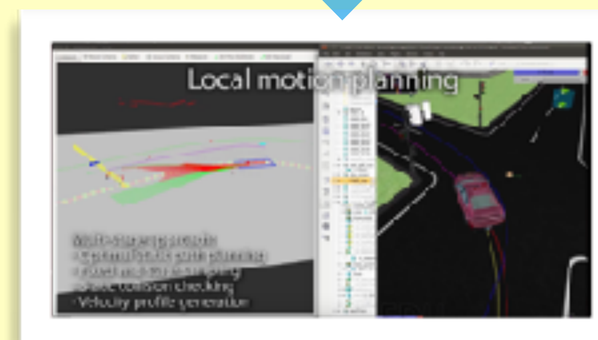
env. input

(road shape,
pedestrians,
other cars, …)

perception




object recognition




behavior planning
path planning


local planning
path tracking

ego car's
position & status

Our goal: comprehensive software stack with perception units, controllers, simulators, and <u>testing tools</u>
(cf. ROS, robot operating system)
- serving academic users
- used as (part of) prototype products
- testbed for technical components

Simulation environment

ERATO　蓮尾メタ数理システムデザインプロジェクト

ERATO Metamathematics for Systems Design Project

国立情報学研究所 & 科学技術振興機構　National Institute of Informatics & Japan Science and Technology Agency

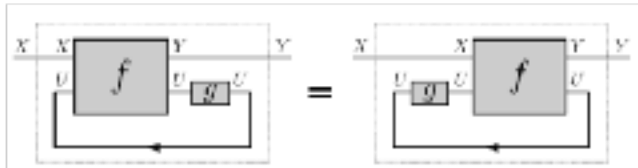
ERATO

MMSD

logic, algebra, category theory, …

Traced monoidal categories

$$\mathrm{Tr}^{U}_{X,Y} : \mathbf{C}(X \otimes U, Y \otimes U) \to \mathbf{C}(X, Y)$$




[Sprunger & Katsumata, LICS'19]

## Abstract Technique

$$T[\_]$$

$$A \quad ::= \quad \mathtt{true} \mid \mathtt{false} \mid A_1 \wedge A_2 \mid \neg A \mid a_1 < a_2 \mid \forall x \in {}^*\mathbb{N}.\, A \mid \forall x \in {}^*\mathbb{R}.\, A$$

$$\begin{tikzcd} FX \arrow[r, dashed, "F\mathsf{beh}_c"] & FZ \\ X \arrow[u, "c"] \arrow[r, dashed, "\mathsf{beh}_c"'] & Z \arrow[u, "\mathrm{final}"'] \end{tikzcd} \qquad \begin{tikzcd} FX \arrow[r, "Ff"] & FY \\ X \arrow[u, "c"] \arrow[r, "f"'] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u, "d"'] \end{tikzcd}$$

system behavior simulation

Identify "mathematical essense"

Choose parameter $e_1$

Choose parameter $e_2$

## Existing Technique

$$T_1 = T[e_1]$$

## Novel Technique

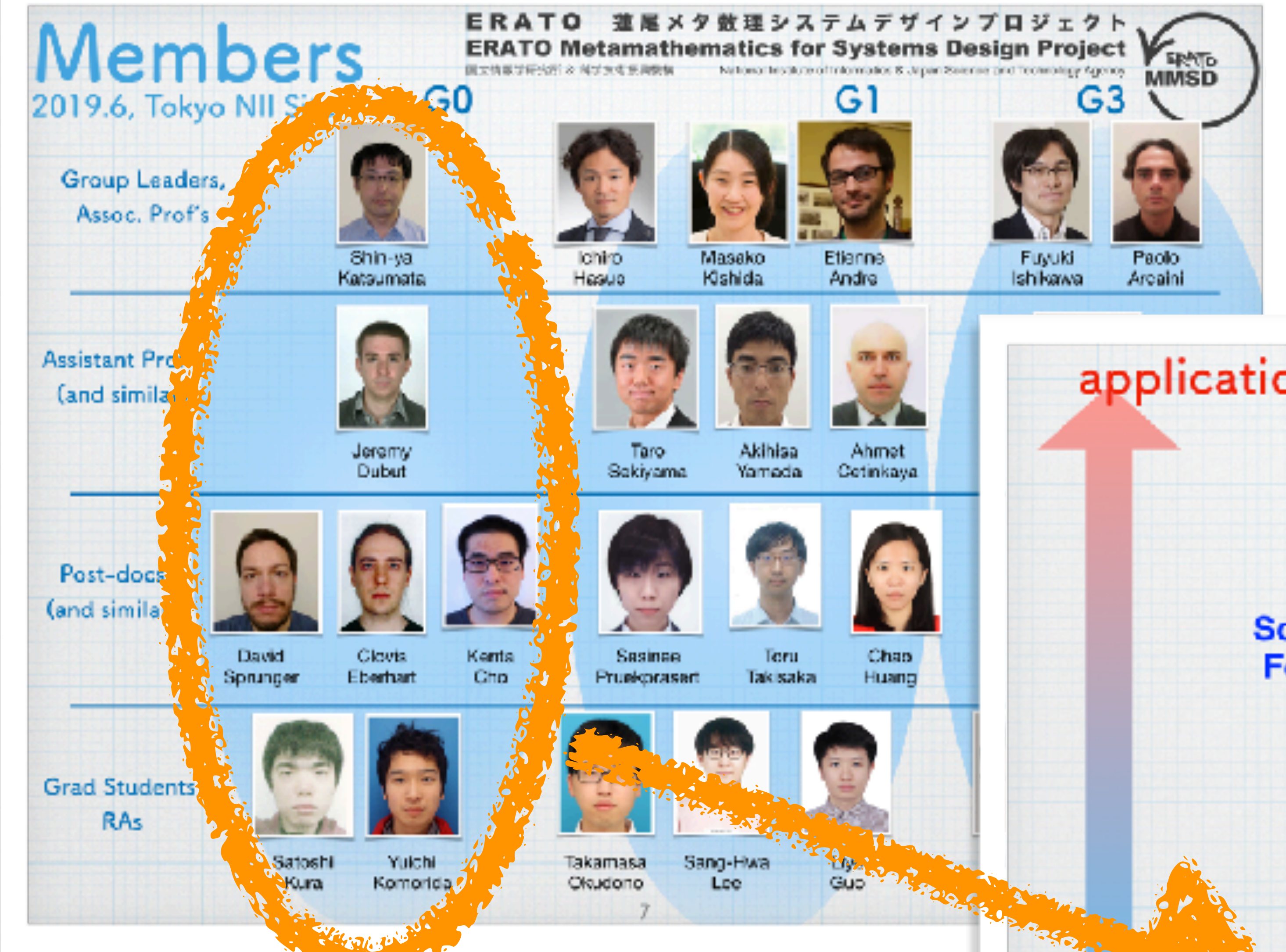
$$T[e_2]$$

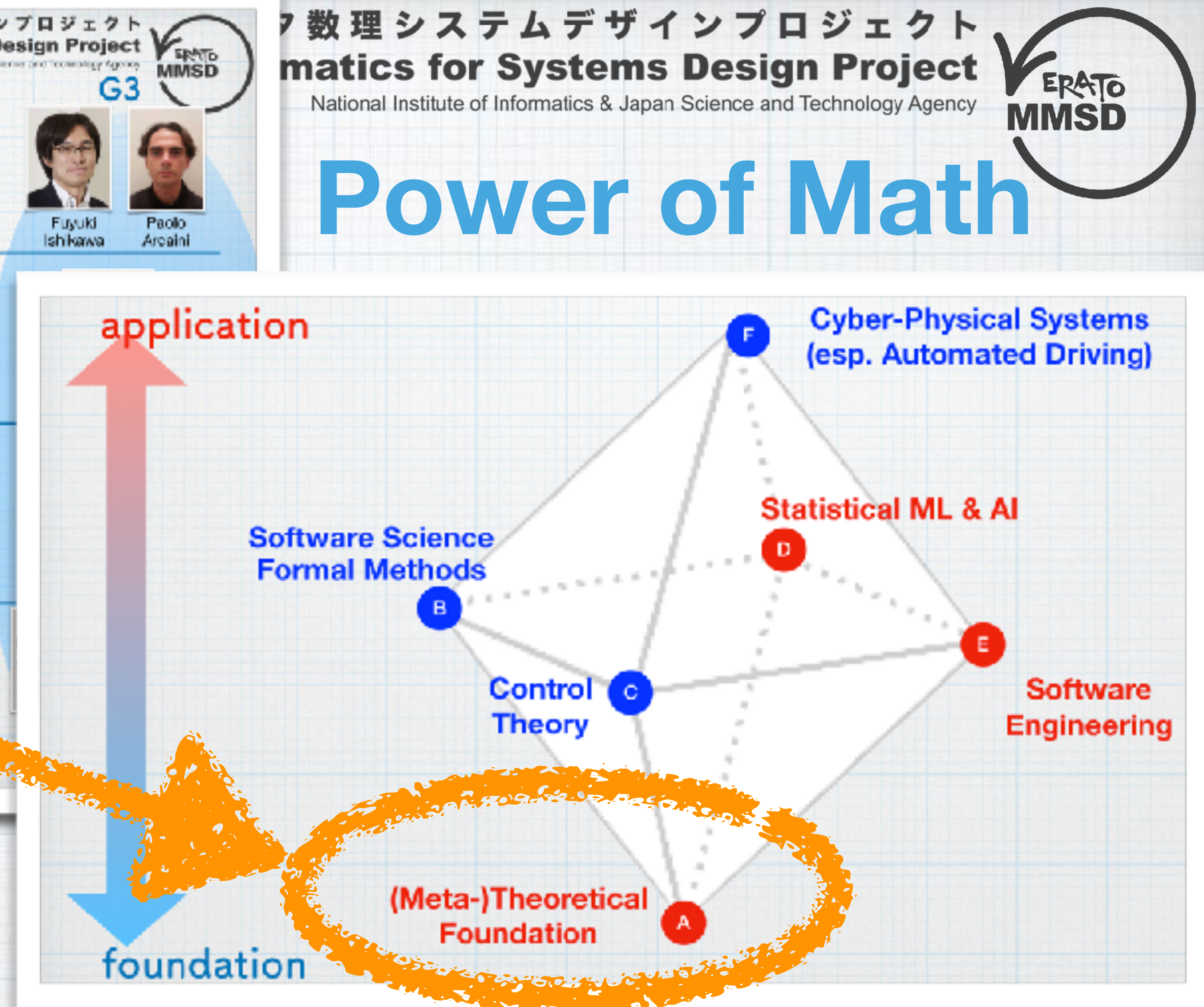
knot invariants, QFTs, semantics of recursion, …

Reachability in Automata

back-propagation algorithm for recurrent neural networks

**Result that stemmed from "deep learning reading group" at ERATO MMSD**




- Contribution of "**theoreticians and listeners**" have been remarkable, direct and indirect
  - "Metatheoretical transfer"
  - Interpreters between disciplines
  - Great "reserve forces"

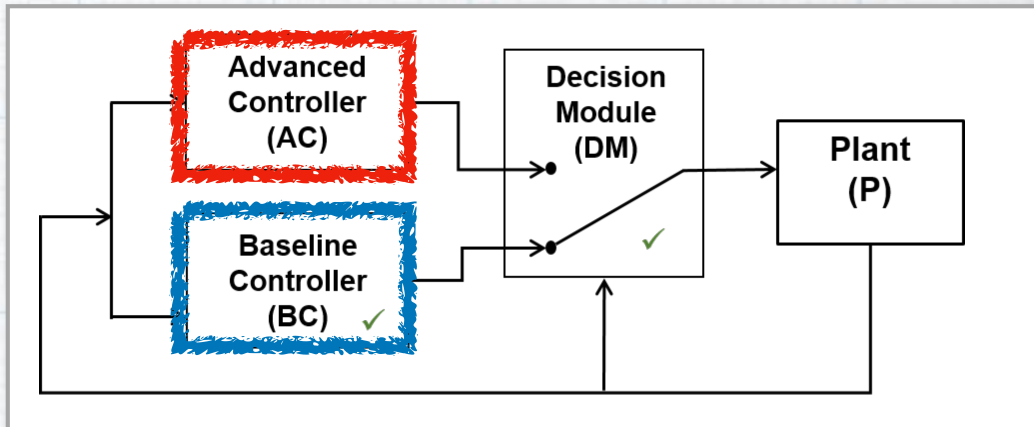
# Conclusions

* Quality assurance of **cyber-physical systems**
  * **Formal methods at work**,
    coping with uncertainties
* Introducing the ERATO MMSD project
* Tech showcase:
  "formal methods that are **down-scalable**"
  * Monitoring
  * Search-based testing
* Applications, "**power of math**"

Thanks for your attention!
https://group-mmm.org/eratommsd

# Reserve Slides

# Formal Safety Architecture

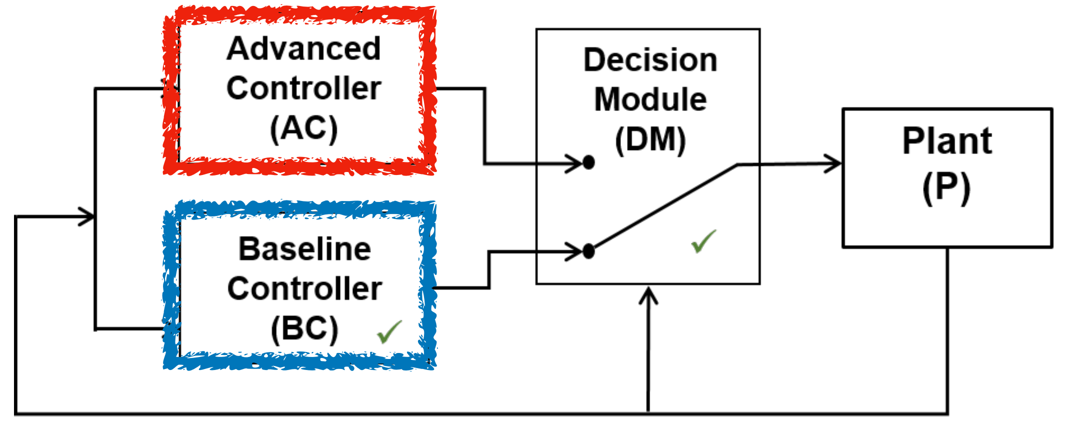


Phan et al., ACSD'17

* Example: simplex architecture (right)
  * AC is
    complex, performance-oriented, black-box
  * BC is
    simple, safety-oriented, (hopefully) white-box
* Idea: we can verify the whole system
  even if AC is a black-box!
  * Enough to show:
    safety of BC, and correctness of DM
  * We impose certain contracts on AC
* Related
  * FM4AI (ML/AI components as AC)
  * Monitoring (checking contracts on AC)
* One promising way to
  make formal verification down-scalable
  * Weaker contracts on AC
    ➜ weaker safety guarantee (but hopefully non-zero)

# Formal Safety Architecture

* **At ERATO MMSD:**
  **we formalize, verify and refine safety architectures**




Phan et al., ACSD’17

* **Event-B: a formal modeling language**
  **[Abrial, “The Event-B Book”, 2010 CUP] [Kobayashi+, ICFEM’18]**
  **Based on state transition systems.**
  **A tool Rodin supports:**
  * **Safety proofs**
  * **Incremental modeling by refinements**
    * **Flexibility in choosing model fidelity ➜ down-scaling**
    * **From (our) general model to (industry partner’s) individual model**