Quality Assurance of Cyber-Physical Systems

Mathematical Metatheory, Machine Learning and Automated Driving

物理情報システム研究の新地平

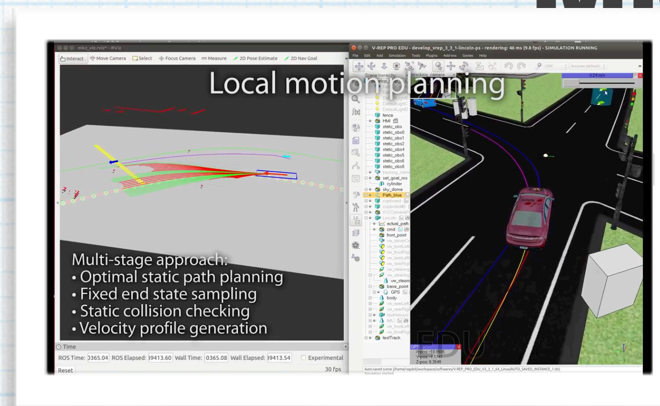
自動運転や機械学習をも包括する数学的基盤

Slides available:
bit.ly/2SdJpIY

Ichiro Hasuo　蓮尾 一郎

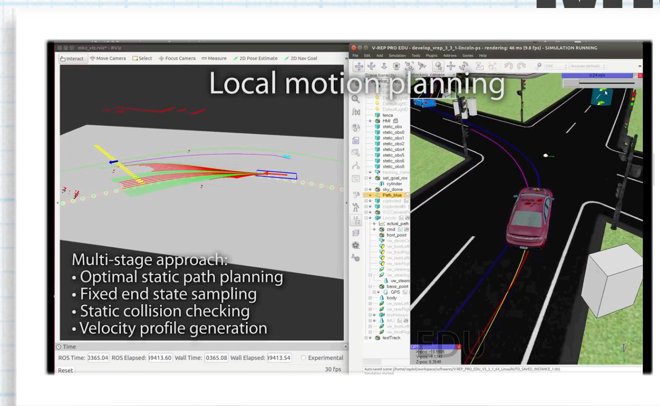
National Institute of Informatics, SOKENDAI
ERATO HASUO Metamathematics for Systems Design Project

On ERATO MMSD



- JST ERATO Project, 2016/10-2022/03
- 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"
  - Automated driving as a strategic target domain.
    Collaboration with U Waterloo: www.autonomoose.net
- Our principle: broaden the realm of CPS research
  - Theory:
    abstract mathematical metatheory
    ➜ scale out to diverse applications
  - Practice: real-world systems (not only toy examples)

On ERATO MMSD



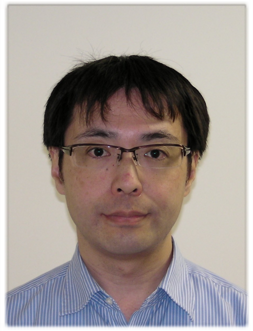
* JST ERATO Project, 2016/10-2022/03
* Our goal:
  formal methods for cyber-physical systems (CPS)
  * Extend formal methods, from software to CPS
  * Safety, reliability, V&V (Verification & Validation).
    "Check if a system behaves as expected"
  * Automated driving as a strategic target domain.
    Collaboration with U Waterloo: www.autonomoose.net
* Our principle: broaden the realm of CPS research
  * Theory:
    abstract mathematical metatheory
    ➜ scale out to diverse applications
  * Practice: real-world systems (not only toy examples)

Our Organization

International and multi-disciplinary. “creative chaos”

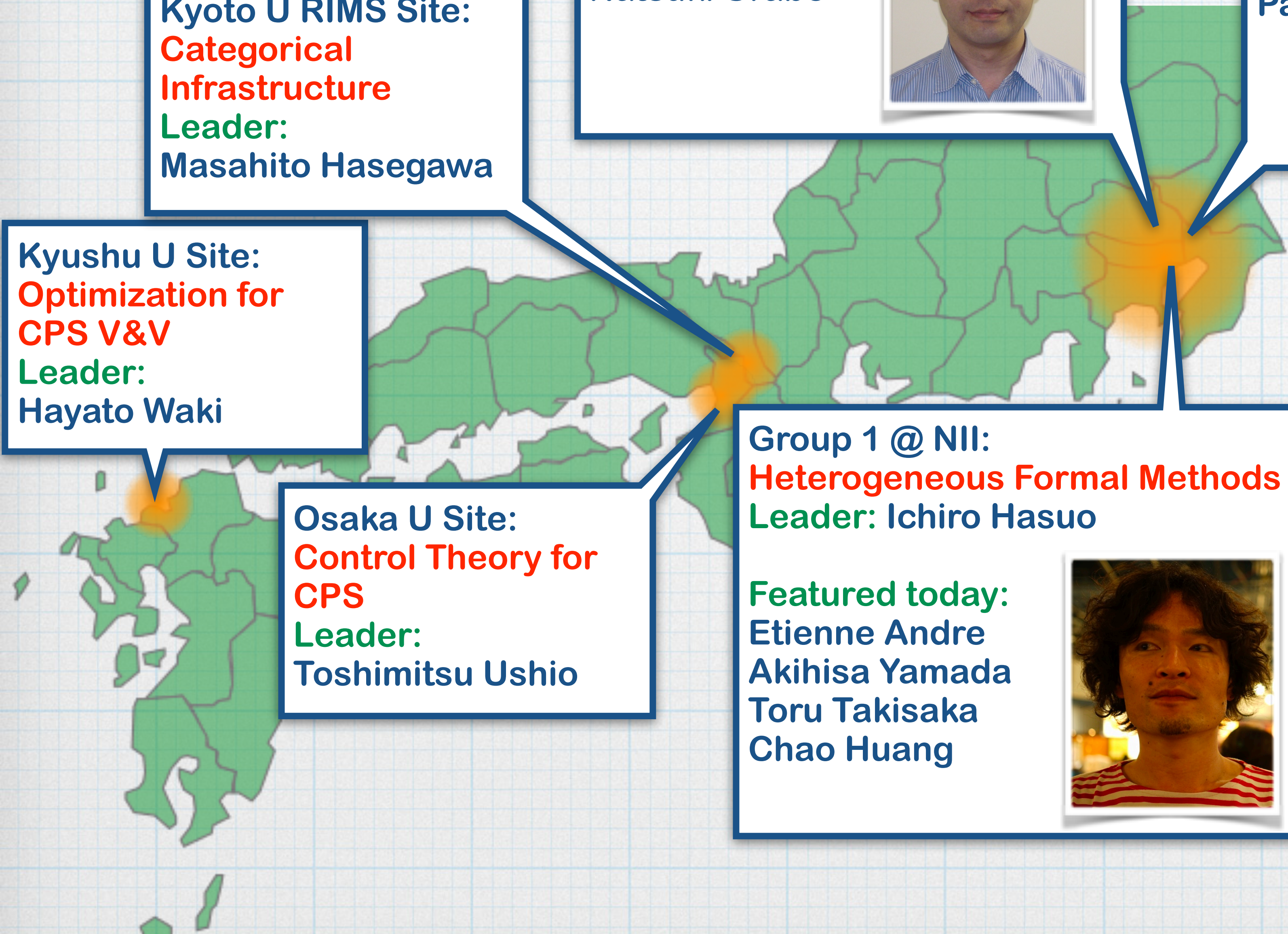
Group 0 @ NII:
Metatheoretical Integration
Leader: Shin-ya Katsumata

Featured today:
Kenta Cho
Clovis Eberhart
Natsuki Urabe



Group 3 @ NII:
Formal Methods and Intelligence
Leader: Fuyuki Ishikawa

Featured today:
Masaki Waga
Paolo Arcaini



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 1 @ NII:
Heterogeneous Formal Methods
Leader: Ichiro Hasuo

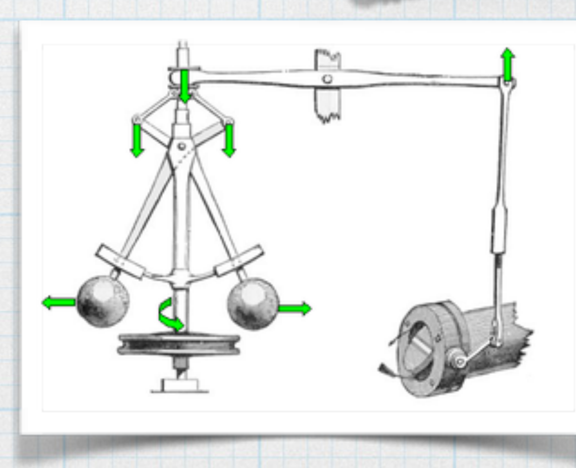
Featured today:
Etienne Andre
Akihisa Yamada
Toru Takisaka
Chao Huang

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

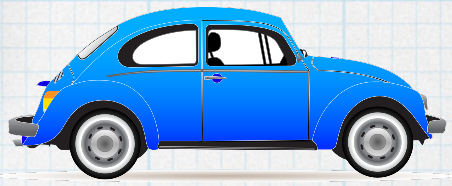
Cyber-Physical Systems : Control Theory and Formal Methods/Software Science

- 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-)
- Formal methods: Logical proofs for "correctness" of (discrete) programs
  - Model checking [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
  - Toru Takisaka's talk on martingale synthesis for probabilistic programs (later)



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



CPS
(esp. hybrid systems)

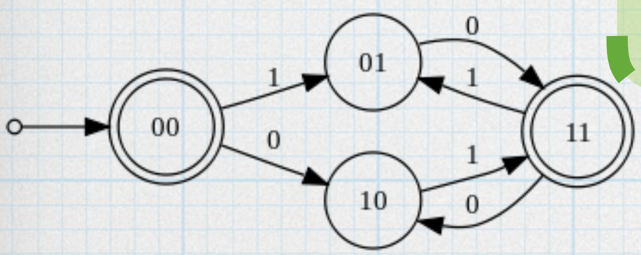
Analysis

Formal Methods

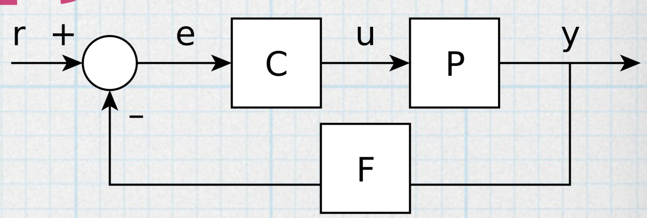
Collaboration

Control Theory

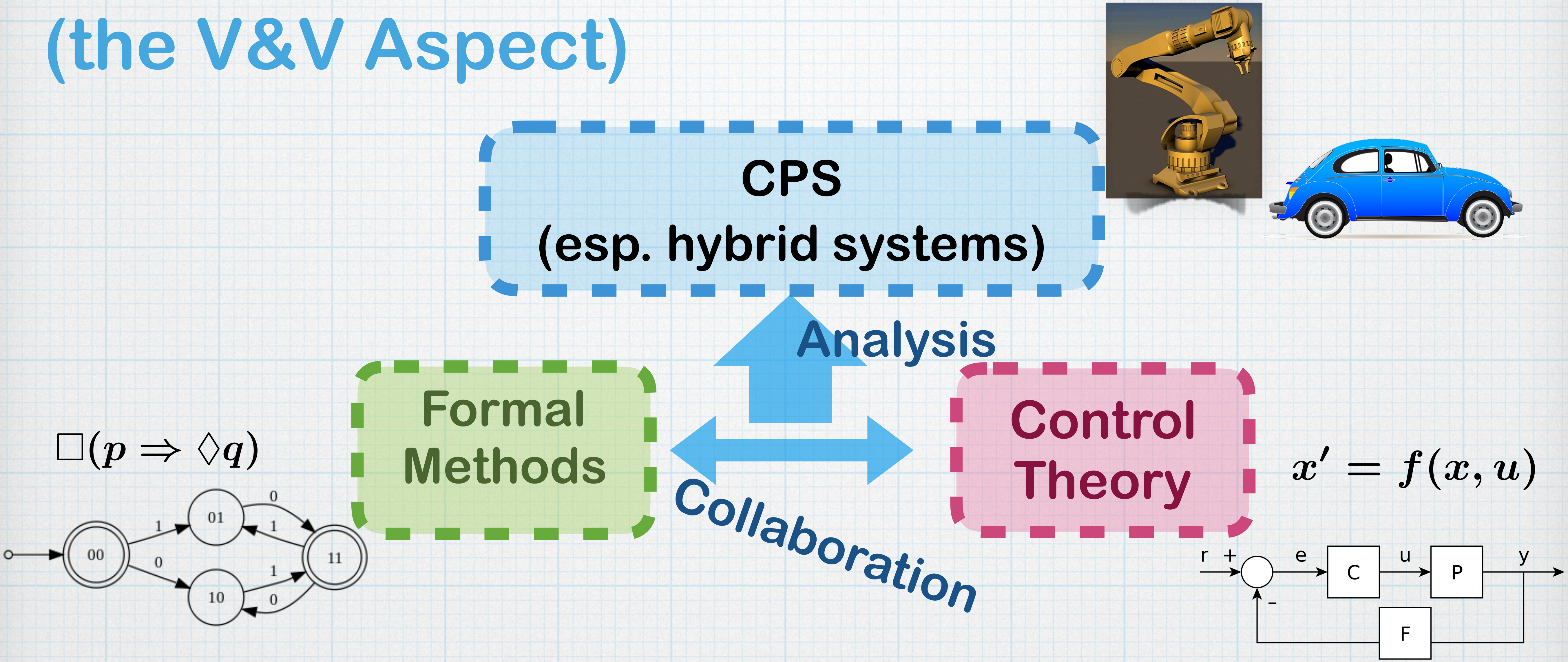
$\Box(p \Rightarrow \Diamond q)$



$x' = f(x, u)$

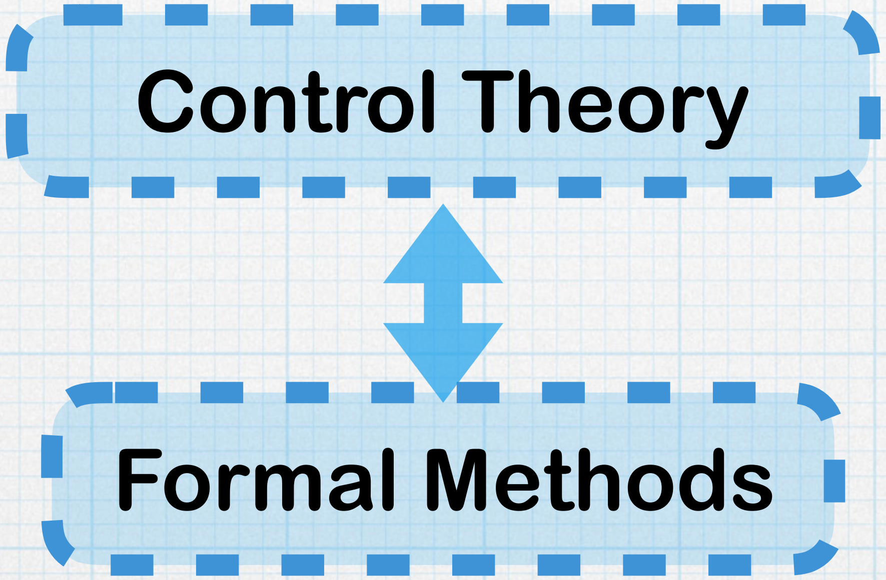


CPS Research, So Far (the V&V Aspect)

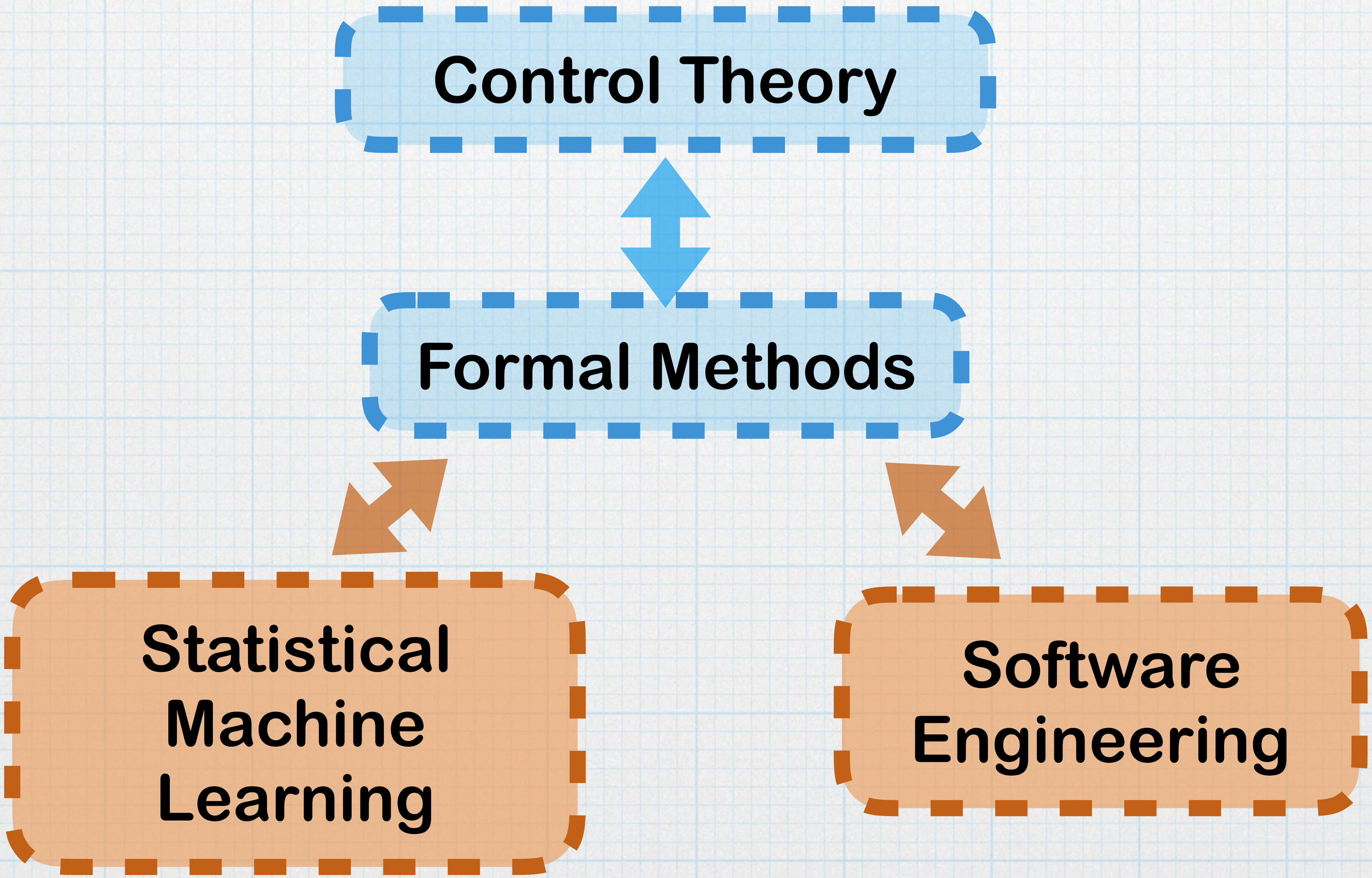


- Problem: scalability, esp. for real-world CPSs
  - Require complete understanding of a white-box model
  - Insist on being absolutely sound and correct
  - Little tolerance to uncertainty and noise
    ➜ don't get along with statistical machine learning

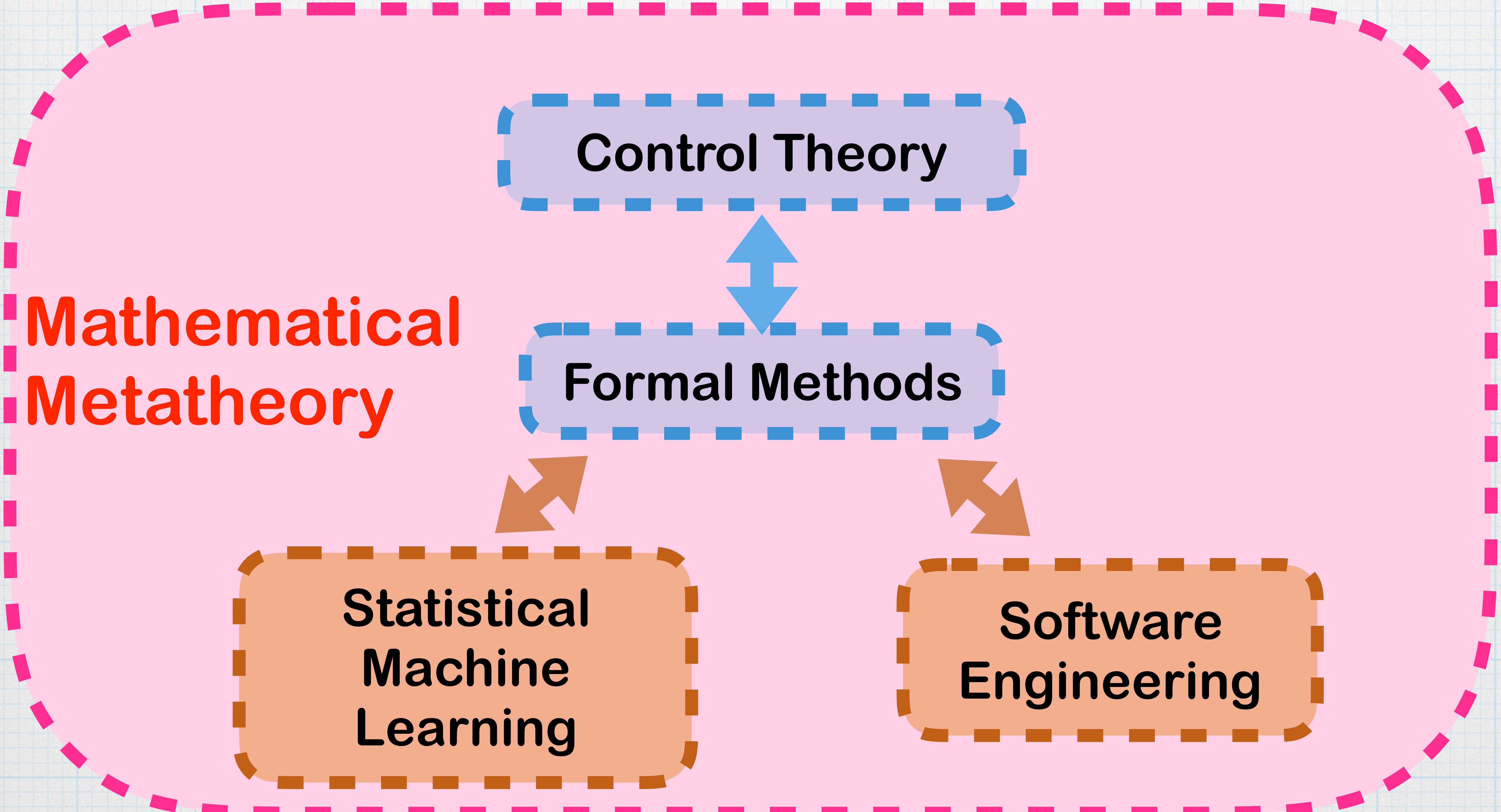
CPS Research: Our Comprehensive Approach



CPS Research: Our Comprehensive Approach



CPS Research: Our Comprehensive Approach



Bidirectional Collaboration with Statistical Machine Learning

* Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
* Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box

Bidirectional Collaboration with Statistical Machine Learning

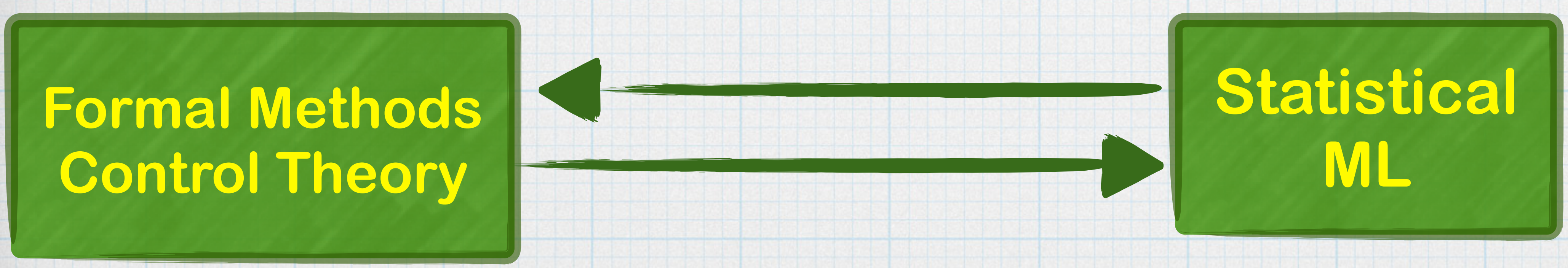
* Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
* Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box

Formal Methods Control Theory

Statistical ML

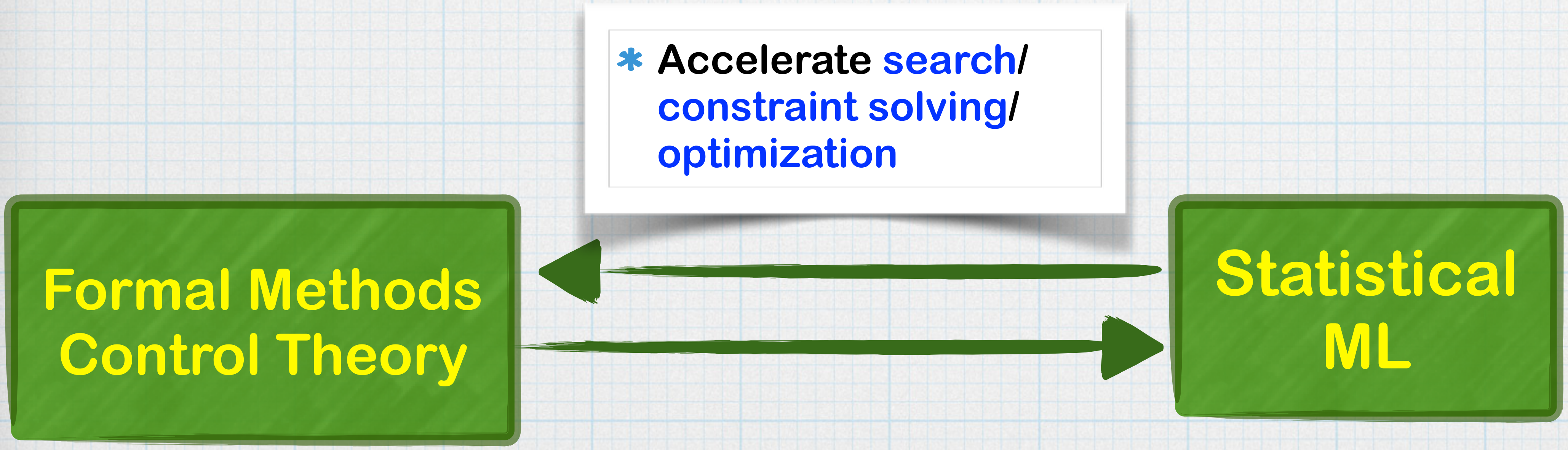
Bidirectional Collaboration with Statistical Machine Learning

* Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
* Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box



Bidirectional Collaboration with Statistical Machine Learning

Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box



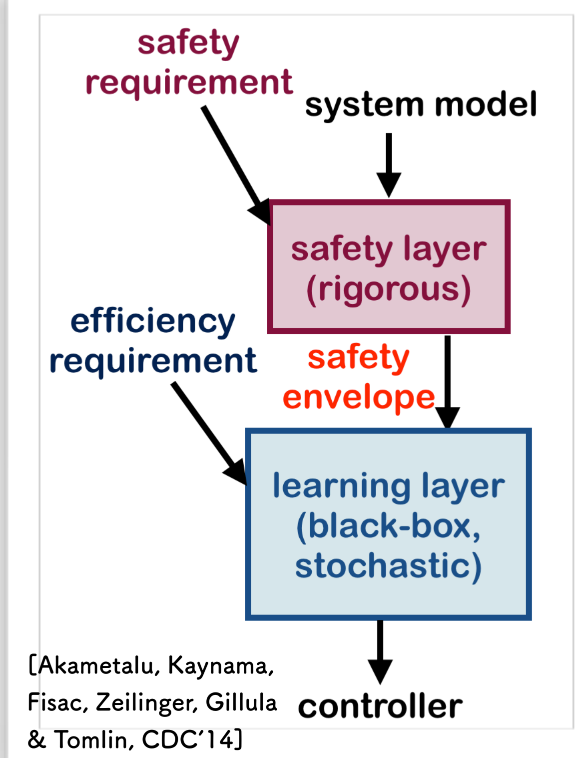
Bidirectional Collaboration with Statistical Machine Learning

Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box

* Accelerate search/ constraint solving/ optimization

Formal Methods Control Theory ⇄ **Statistical ML**

* Acknowledge that ML components are unreliable
* Wrap them with "safety envelopes,"
* within which ML optimizes



Key: system-level architecture for collaboration between logic and ML. Separation of concerns

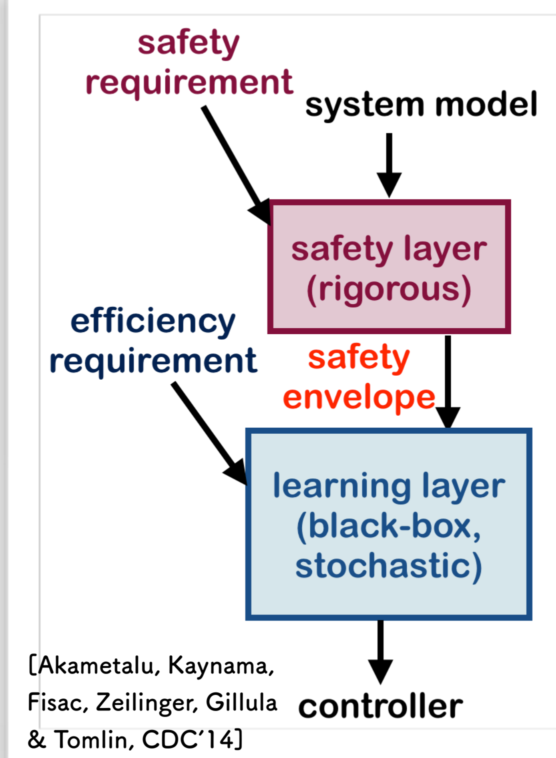
Bidirectional Collaboration with Statistical Machine Learning

Statistical ML	Inductive (learn from data)	Uncertainty (data is noisy)	(Typically) Black Box
Formal Methods, Control Th.	Deductive (Infer from absolute axioms)	Mathematical & Logical Rigor	White Box

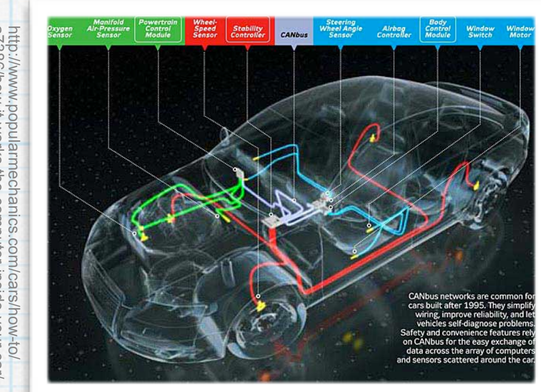
- Accelerate search/ constraint solving/ optimization

Formal Methods Control Theory ⇄ Statistical ML

- Acknowledge that ML components are unreliable
- Wrap them with "safety envelopes,"
- within which ML optimizes



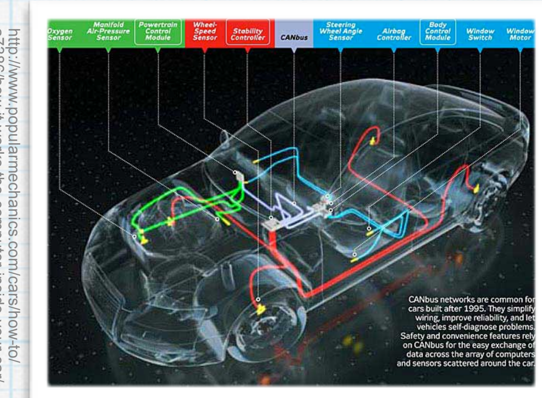
Software Engineering and Empirical Application of Formal Methods and Control Theory



http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/

- Challenges in industrial application
  - Scalability: real systems are complex
  - Need complete white-box models
    - Unrealistic. Components from suppliers, neural nets, …
  - Industry practitioners need not appreciate rigorous proofs
    - How do we check axioms (= environmental assumptions)?

Software Engineering and Empirical Application of Formal Methods and Control Theory

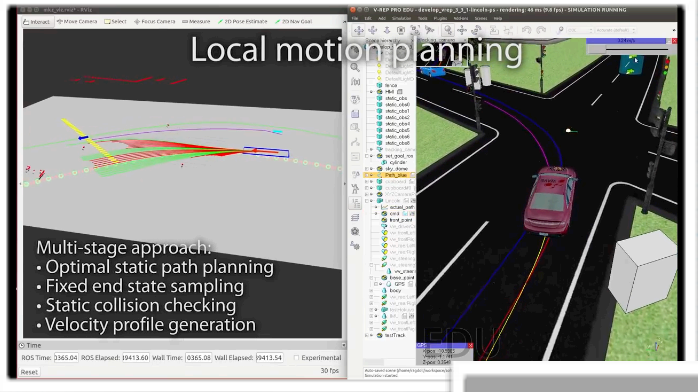


http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/

- Challenges in industrial application
  - Scalability: real systems are complex
  - Need complete white-box models
    - Unrealistic. Components from suppliers, neural nets, …
  - Industry practitioners need not appreciate rigorous proofs
    - How do we check axioms (= environmental assumptions)?

- ➜ We focus on supporting empirical quality assurance methods (i.e. testing)
  - What software engineering has been doing for years
  - Testing, runtime verification, …
  - Ample use of deductive techniques from formal methods
    - Examples: from specifications to score functions, optimize test cases, …
    - Talks by Etienne Andre, Masaki Waga, Paolo Arcaini

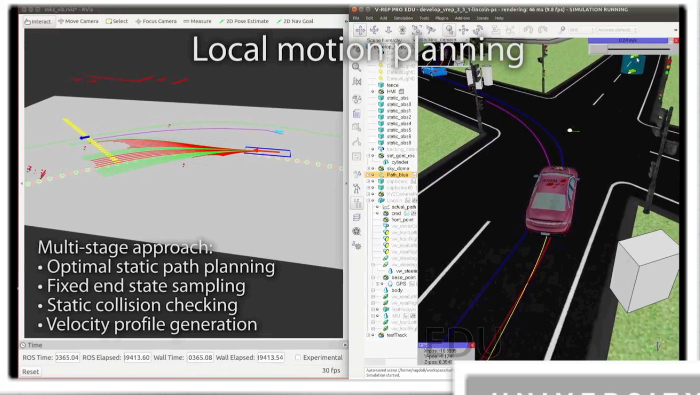
Exit Strategy (in Application)



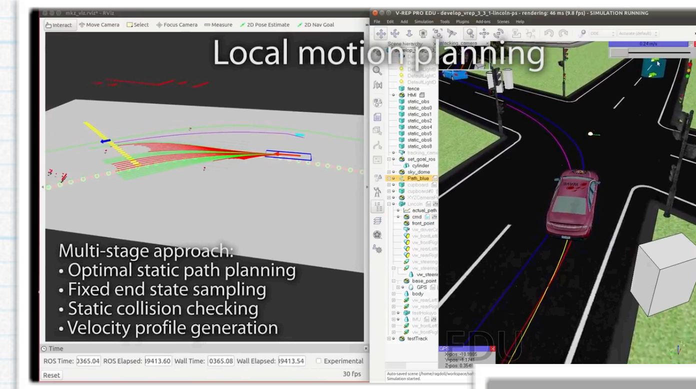
- Outlets
  - Industry collaboration: a few companies
  - Automated Driving Vehicle Project "Autonomoose" (U Waterloo). (Mostly) nonproprietary software stack for automated driving

Exit Strategy (in Application)

* <u>Outlets</u>
    * Industry collaboration: a few companies
    * Automated Driving Vehicle Project "Autonomoose" (U Waterloo). (Mostly) nonproprietary software stack for automated driving

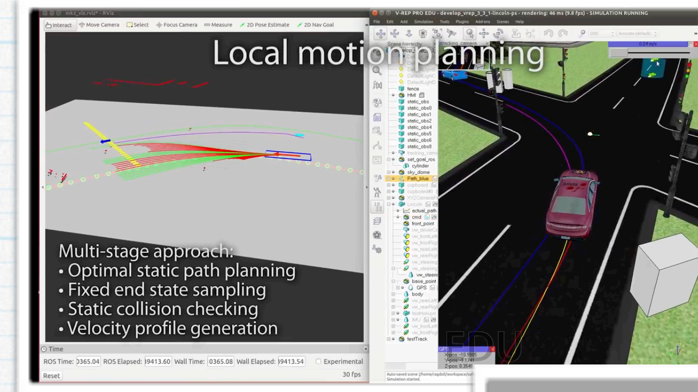


Exit Strategy (in Application)



- **Outlets**
  - Industry collaboration: a few companies
  - Automated Driving Vehicle Project "Autonomoose" (U Waterloo). (Mostly) nonproprietary software stack for automated driving
- **Goal 1**: our advanced quality assurance techniques, put to real use
  - Safety is rarely a competition area
  - ➜ we aim at standards (ISO 26262, SOTIF, …)

Exit Strategy (in Application)



* Outlets
  * Industry collaboration: a few companies
  * Automated Driving Vehicle Project "Autonomoose" (U Waterloo). (Mostly) nonproprietary software stack for automated driving

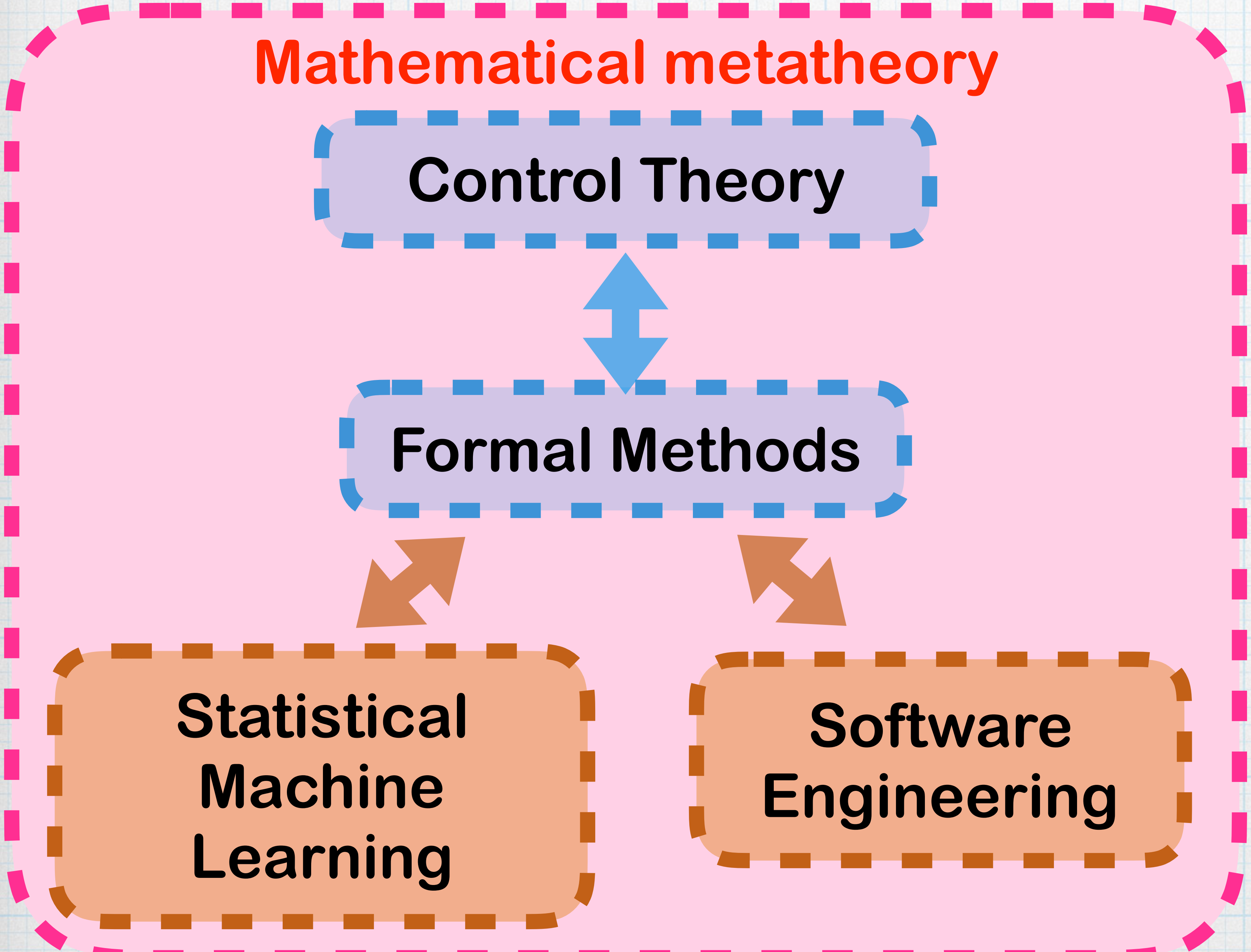
* Goal 1: our advanced quality assurance techniques, put to real use
  * Safety is rarely a competition area
  * ➜ we aim at standards (ISO 26262, SOTIF, …)

* Goal 2: offer software platform for developing, verifying and validating automated driving software
  * For industry and academia
  * Perception ➜ Object Recognition ➜ Path Planning ➜ Path Tracing, + Simulation + Testing, V&V
  * Improvement of each component + Interface between components, DSL (domain specific language)

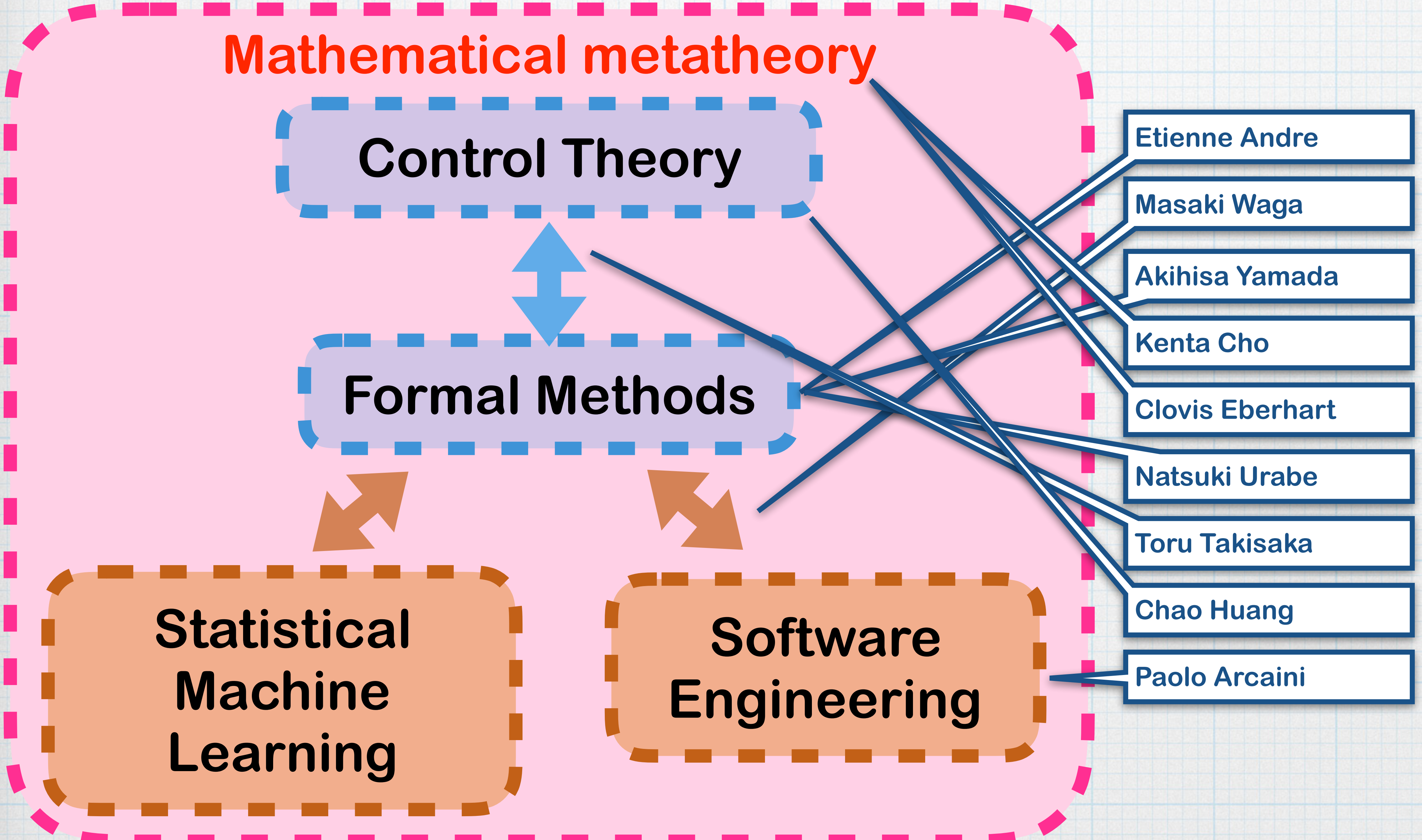
    ➜ the whole framework
  * Our unique strength: advanced V&V techniques + their theoretical foundation + programming language theory

Strategic contribution areas

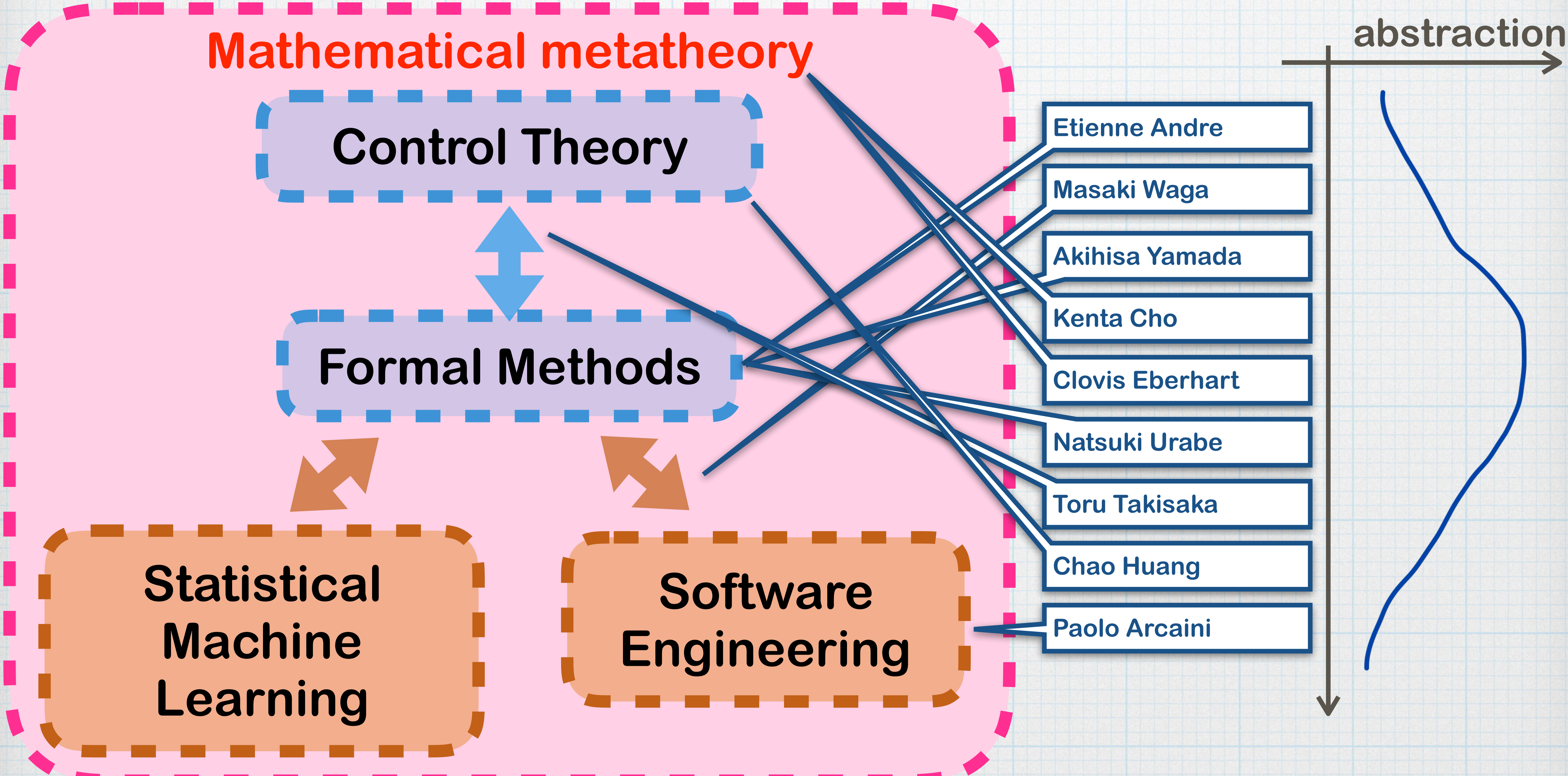
CPS Research: Our Comprehensive Approach



CPS Research: Our Comprehensive Approach



CPS Research: Our Comprehensive Approach



CPS Research: Our Comprehensive Approach