iCyPhy

(the new) iCyPhy

Industrial Cyber-Physical Systems

a SwarmLab 2.0 Center

Prabal Dutta, Edward A. Lee,
Sanjit Seshia, Alberto Sangiovanni-Vincentelli
(and any other faculty who would like to join us)

EECS, UC Berkeley

SWARMLAB UC BERKELEY

SwarmLab Retreat

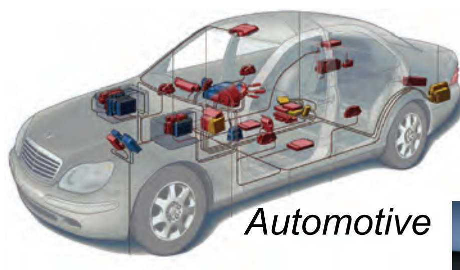
Nov. 15, 2016, Berkeley, CA

University of California at Berkeley

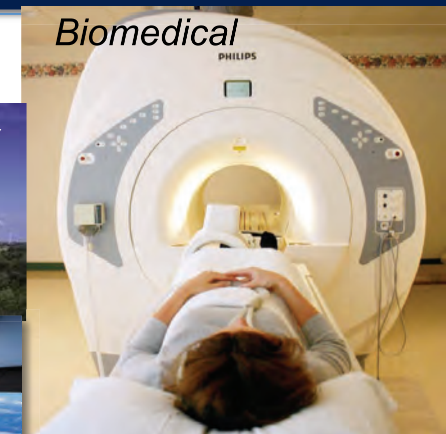
Cyber-Physical Systems
Focus on the Internet of *Important* Things

Not just information technology:

- Cyber + Physical
- Computation + Dynamics
- Security + Safety

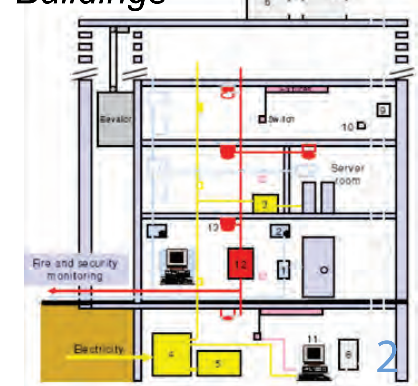


Automotive



Manufacturing

Buildings

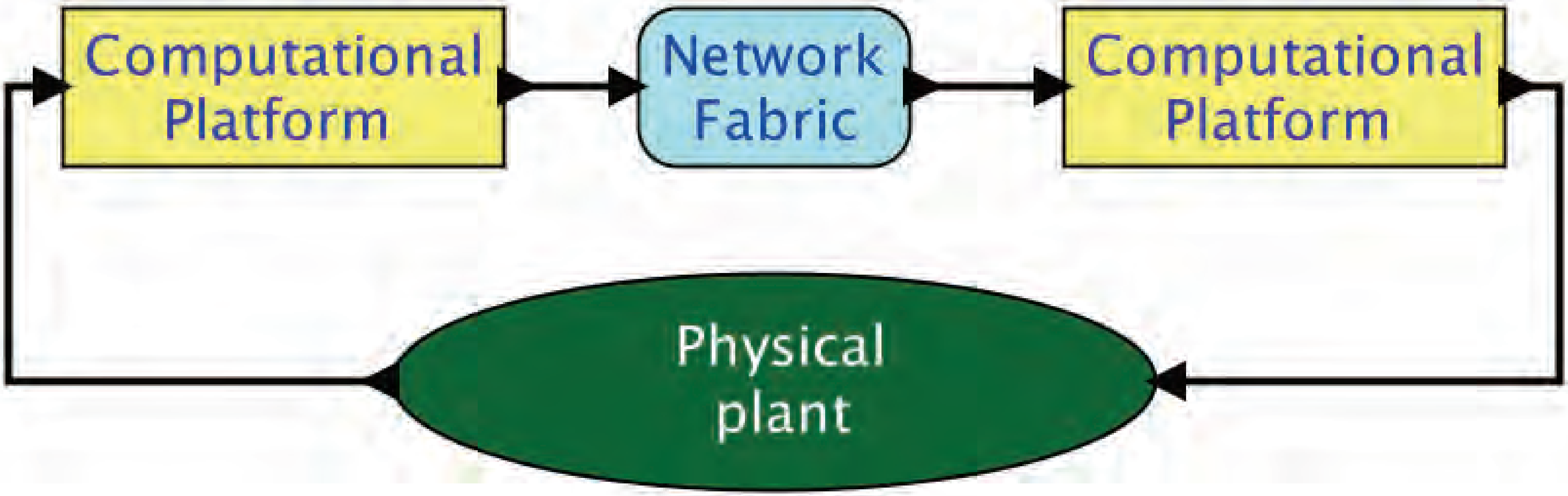


Properties:

- Highly dynamic
- Safety critical
- Uncertain environment
- Physically distributed
- Sporadic connectivity
- Resource constrained

We need engineering models and methodologies for dependable cyber-physical systems.

Schematic of a simple Cyber-Physical System



- How to design, model, and analyze such systems?
- How to achieve QoS guarantees, privacy, and security?
- How to provide safety guarantees in the face of failures?

iCyPhy
Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org




Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

iCyPhy

Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org




CapeCode
A Programming Framework for the IoT

file:/ptII/ptolemy/configs/capecode/intro.htm

File Help

(source: Wikipedia)

CapeCode, Version 0.1

The modular Internet of Things, based on Ptolemy II.

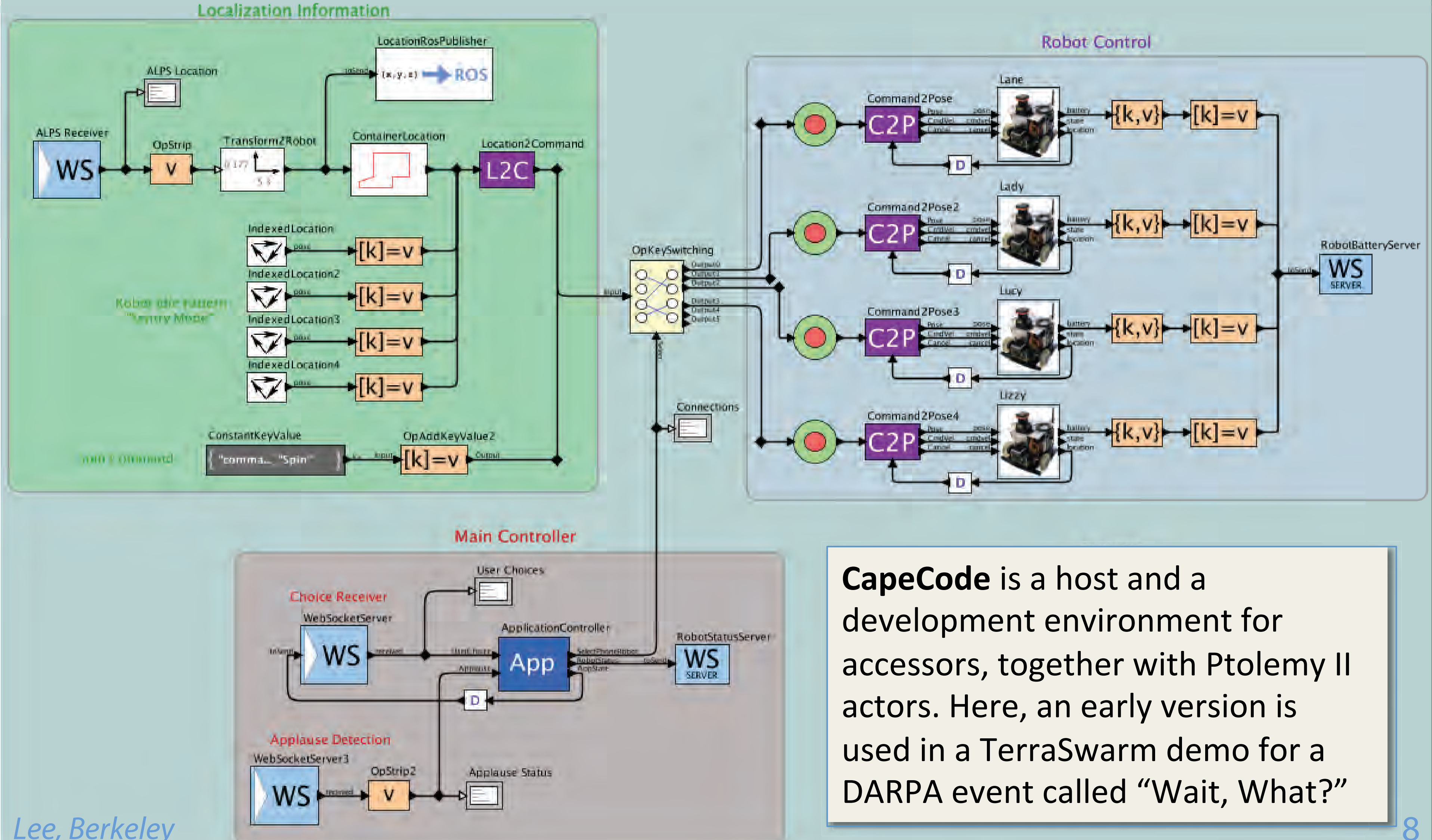
- Demos
- Documentation
- Authors
- Copyright

To create a CapeCode model, select File -> New -> Cape Code Model from the menu bar. See the Ptolemy Project web page for more information about the Ptolemy II.

CapeCode, originally developed in TerraSwarm, will be taken over by iCyPhy when TerraSwarm ends in 2017.

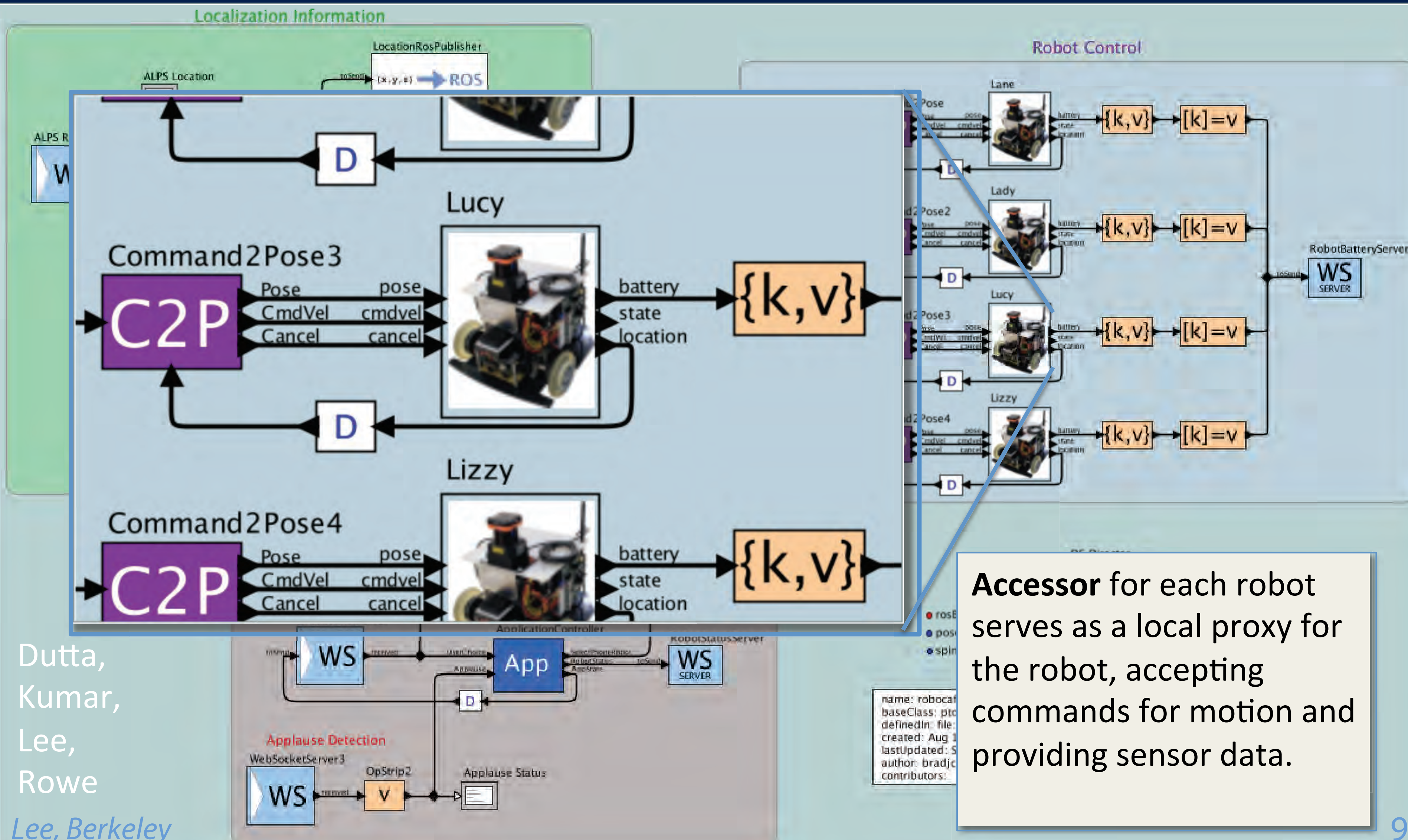
CapeCode

A Programming Framework for the IoT



CapeCode is a host and a development environment for accessors, together with Ptolemy II actors. Here, an early version is used in a TerraSwarm demo for a DARPA event called “Wait, What?”

CapeCode
A Programming Framework for the IoT

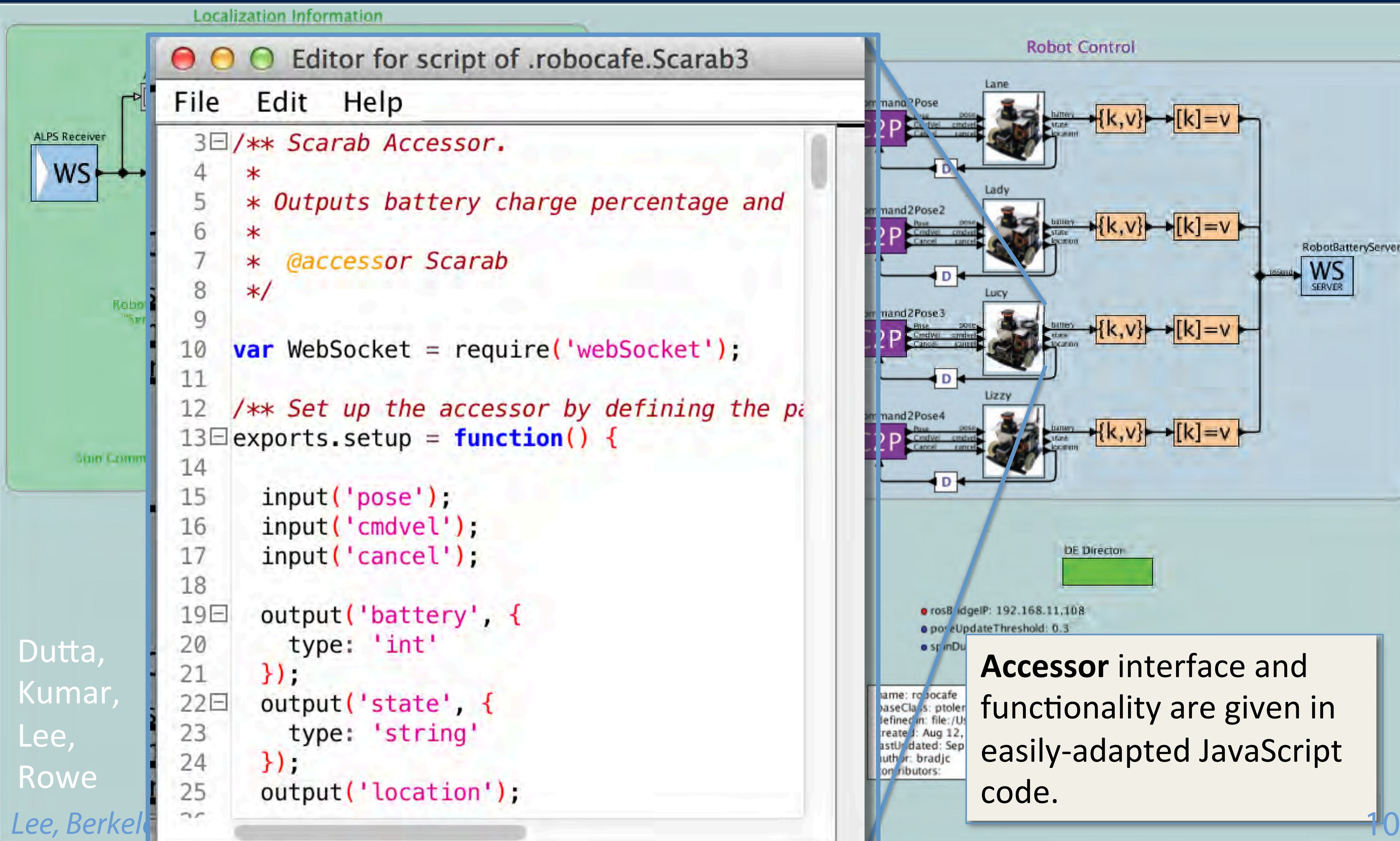


Accessor for each robot serves as a local proxy for the robot, accepting commands for motion and providing sensor data.

Dutta, Kumar, Lee, Rowe

CapeCode

A Programming Framework for the IoT

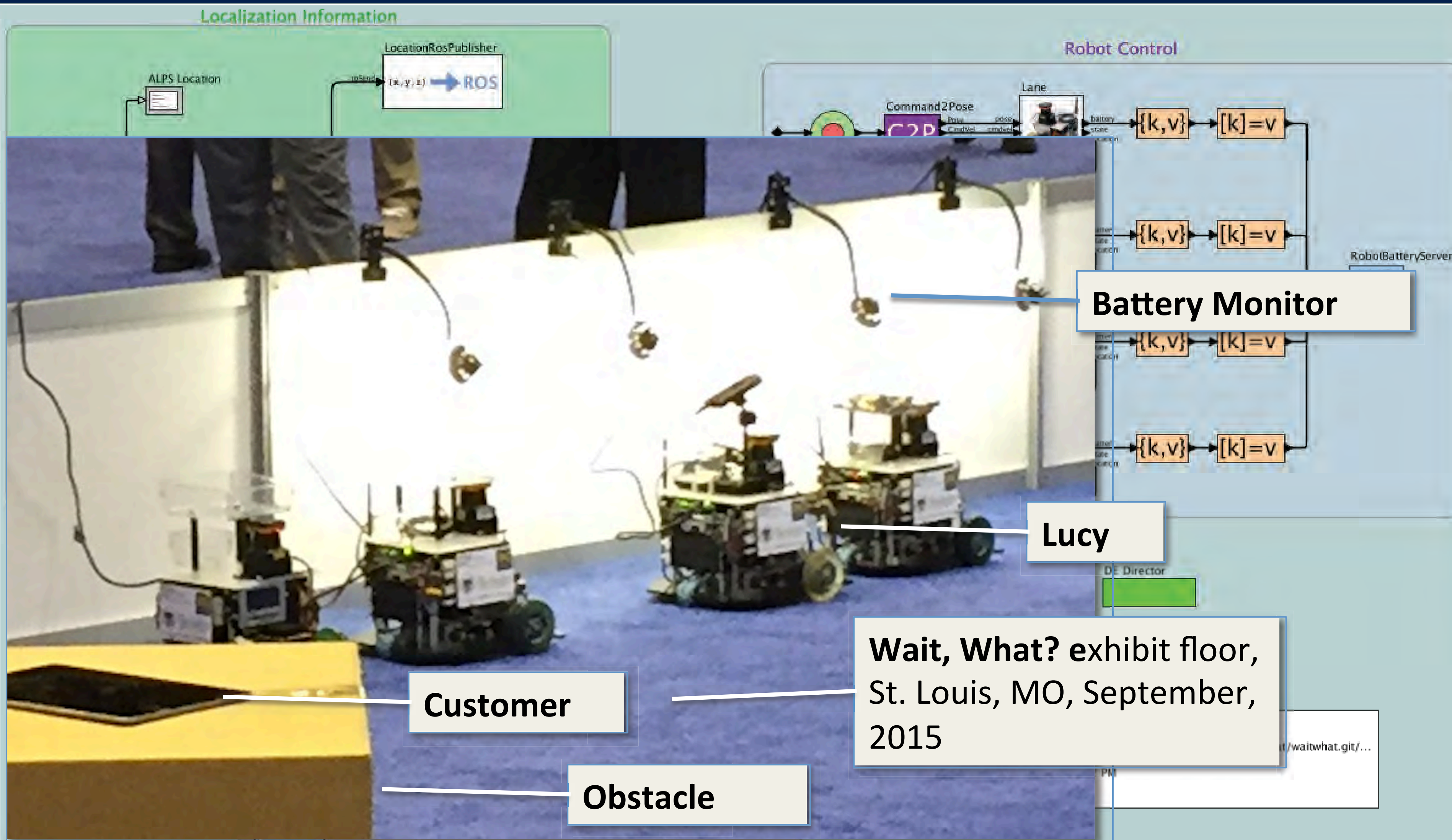


Accessor interface and functionality are given in easily-adapted JavaScript code.

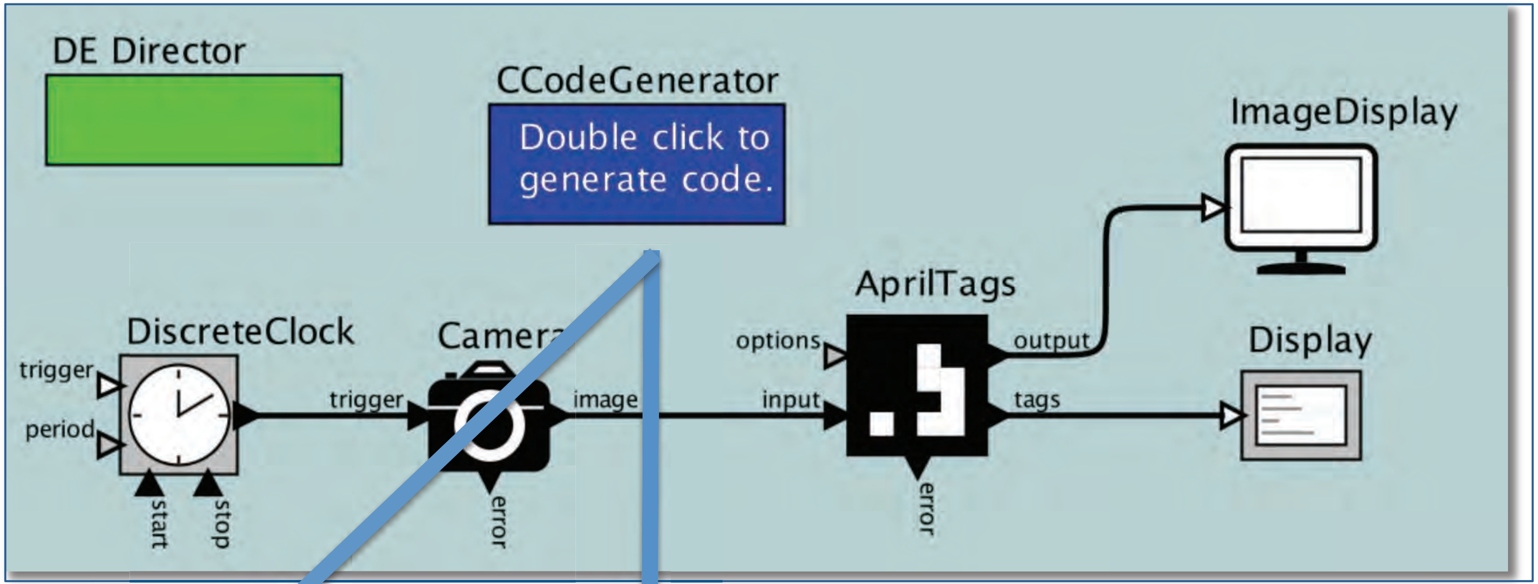
Dutta, Kumar, Lee, Rowe

CapeCode

A Programming Framework for the IoT

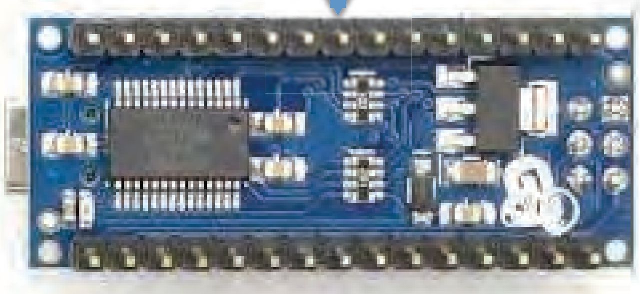


Code Generation for Deployment



C DE scheduler + Duktape + JavaScript (+ Ptides?)

Knot so Ptiny Ptarget (KPP)



Ptruly Ptiny Ptarget (PPP)

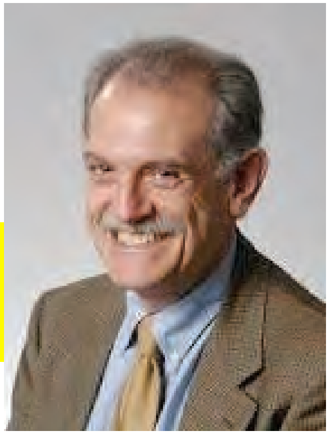
iCyPhy
Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org



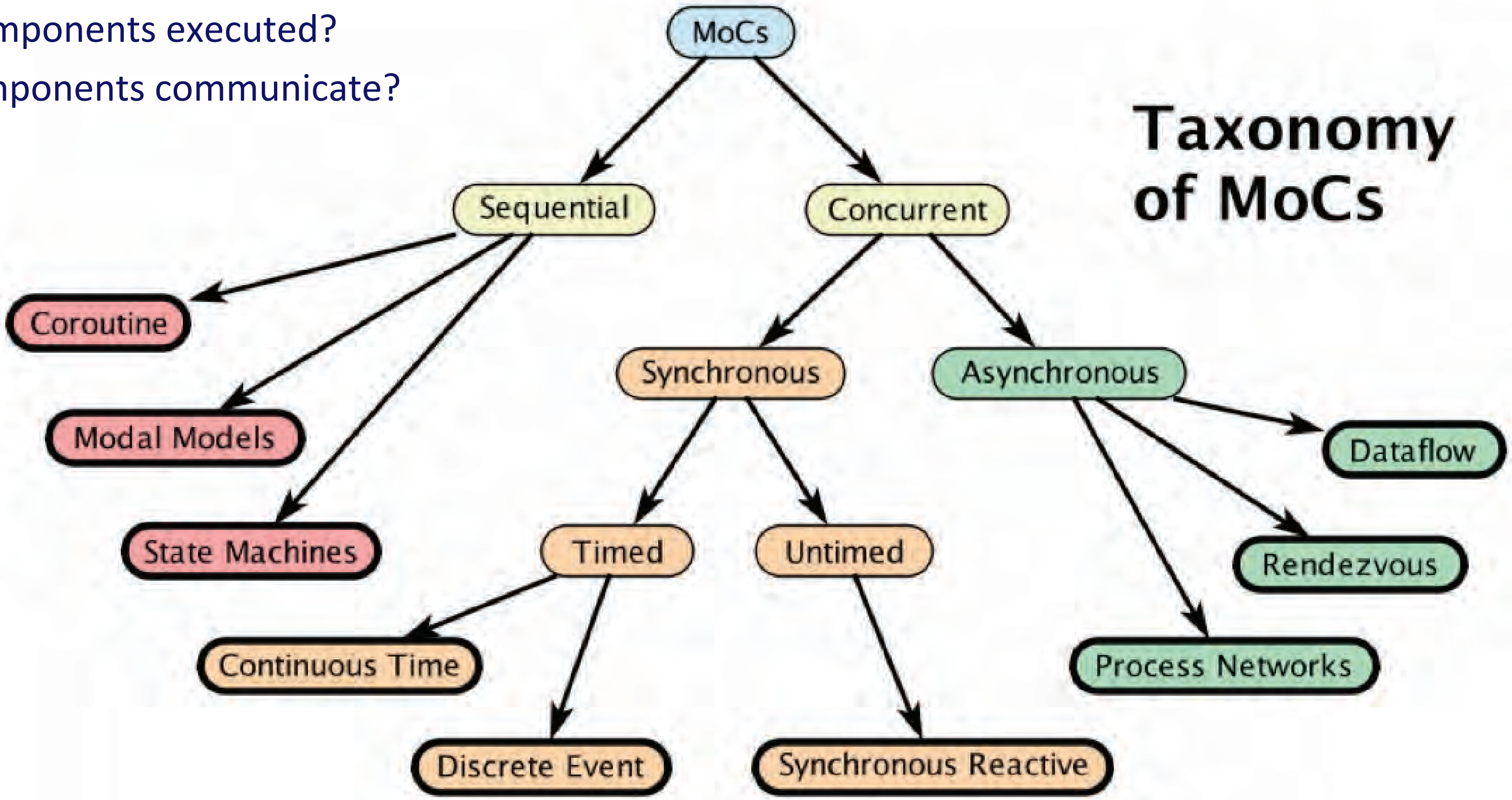



Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

Models of Computation for Complex System Dynamics

An *MoC* defines the "laws of physics" for the interaction between components in a design. It provides the rules that govern concurrent execution of the components and the communication between components. The MoC defines:

- What is a component?
- How are components executed?
- How do components communicate?



CyPhySim

http://cyphysim.org

CyPhySim is an open-source simulator for cyber-physical systems. The simulator provides a graphical editor, an XML file syntax for models, and an open API for programmatic construction of models.

CyPhySim supports the following Models of Computation:

- Discrete Event simulation
- Quantized-State Systems (QSS) simulation
- Continuous time (Runge-Kutta) simulation
- Discrete time simulation
- Modal Models
- Functional Mockup Interface (FMI)
- Algebraic loop solvers

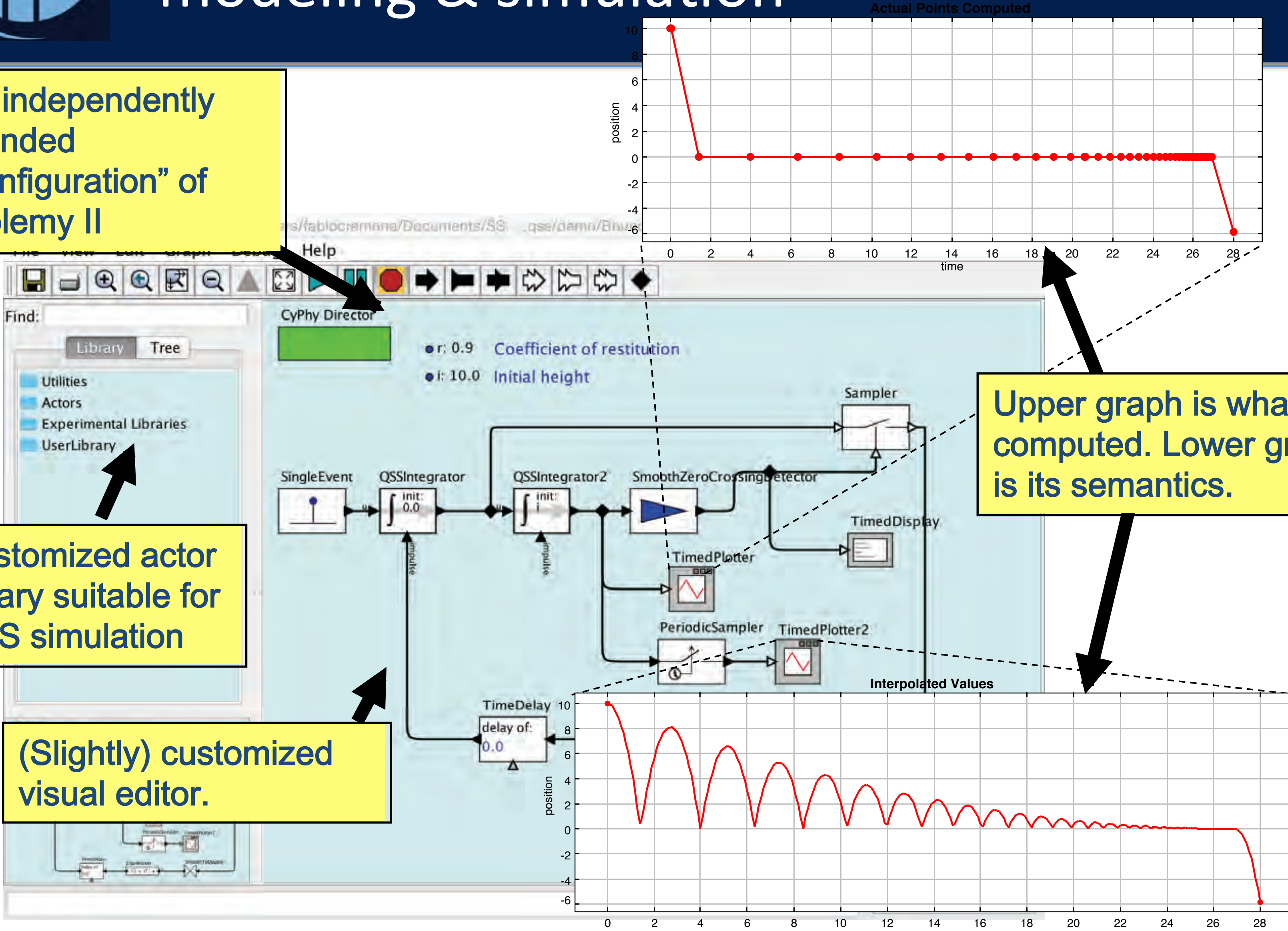
CyPhySim: Mixed discrete/continuous modeling & simulation

An independently branded "configuration" of Ptolemy II

Customized actor library suitable for CPS simulation

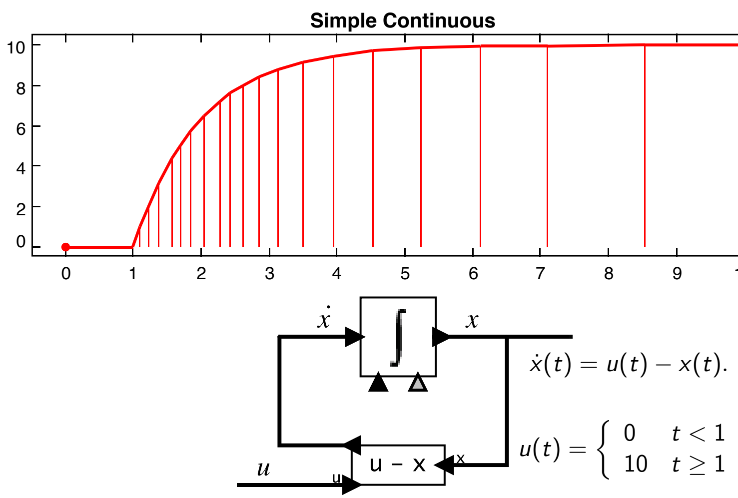
(Slightly) customized visual editor.

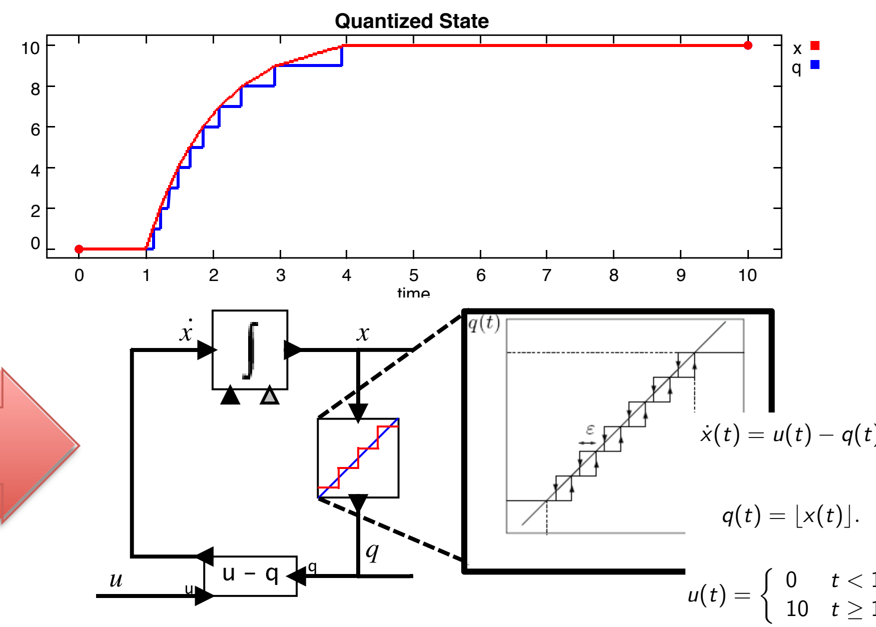
Upper graph is what is computed. Lower graph is its semantics.



Quantized-state Systems

In a classical ODE simulator, a step-size control algorithm determines sample times, and a sample value is computed at those times for all states in the model. In a QSS simulator, each state has its own sample times, and samples are processed using a DE simulation engine in time-stamp order. The sample time of each state is determined by quantizing the value of each state and producing samples only when the value changes by a pre-determined tolerance, called the quantum.





Hybrid Cosimulation: FMI

Requirements for Hybrid Cosimulation Standards*

David Broman
KTH Royal Institute of Technology & UC Berkeley

Lev Greenberg
IBM Research – Haifa, Israel

Edward A. Lee†
UC Berkeley

Michael Masin
IBM Research – Haifa, Israel

Stavros Tripakis
UC Berkeley & Aalto University

Michael Wetter
Lawrence Berkeley National Laboratory

ABSTRACT

This paper defines a suite of requirements for future hybrid cosimulation standards, and specifically provides guidance for development of a hybrid cosimulation version of the Functional Mockup Interface (FMI). A cosimulation standard defines interfaces that enable diverse simulation tools to interoperate. Specifically, one tool defines a component that forms part of a simulation model in another tool. We focus on components with inputs and outputs that are functions of time, and specifically on mixtures of discrete events and continuous time signals. This hybrid mixture is not well supported by existing cosimulation standards, and specifically not by FMI 2.0, for reasons that are explained in this paper. The paper defines a suite of test components, giving a mathematical model of an ideal behavior, plus a discussion of practical implementation considerations. The discussion includes acceptance criteria by which we can determine whether a standard supports definition of each component. In addition, we define a set of test compositions that define requirements for coordination between components, including consistent handling of timed events.

Paper circulated among FMI activists, and submitted and published in HSCC 2015.

Foundations of Cyber-Physical Systems Modeling

IEEE Access

Aug. 2014

Vol 15 No 3

Constructive Models of Discrete and Continuous Physical Phenomena

EDWARD A. LEE, (Fellow, IEEE)
Department of Electrical and Engineering Computer Sciences, University of California at Berkeley, Berkeley, CA 94720, USA
Corresponding author: E. A. Lee (eal@eecs.berkeley.edu)

This work was supported in part by the iCyPhy Research Center, through IBM, Armonk, NY, USA, and United Technologies, Hartford, CT, USA, in part by the Center for Hybrid and Embedded Software Systems, University of California at Berkeley, Berkeley, CA, USA, through the National Science Foundation, under Award 0931843 ActionWebs, in part by the Naval Research Laboratory under Grant N0013-12-1-G015, and in part by the companies, including Denso International America, Southfield, MI, USA, National Instruments Corporation, Austin, TX, USA, and Toyota, Torrance, CA, USA.

ABSTRACT This paper studies the semantics of models for discrete physical phenomena, such as rigid body collisions and switching in electronic circuits. This paper combines generalized functions (specifically the Dirac delta function), superdense time, modal models, and constructive semantics to get a rich, flexible, efficient, and rigorous approach to modeling such systems. It shows that many physical scenarios that have been problematic for modeling techniques manifest as nonconstructive models, and that constructive versions of some of the models properly reflect uncertainty in the behavior of the physical systems that plausibly arise from the principles of the underlying physics. This paper argues that these modeling difficulties are not reasonably solved by
more detailed models sim
come with a high comput
specifically to understand
in the Ptolemy II modelin

ACM Transactions on Cyber-Physical Systems,

October, 2016

Vol 1, No 1

Fundamental Limits of Cyber-Physical Systems Modeling[1]

EDWARD A. LEE, EECS Department, UC Berkeley

This paper examines the role of modeling in the engineering of cyber-physical systems. It argues that the role that models play in engineering is different from the role they play in science, and that this difference should direct us to use a different class of models, where simplicity and clarity of semantics dominate over accuracy and detail. I argue that determinism in models that are used for engineering is a valuable property and should be preserved whenever possible, regardless of whether the system being modeled is deterministic. I then identify three classes of fundamental limits on modeling, specifically chaotic behavior, the inability of computers to numerically handle a continuum, and the incompleteness of determinism. The last of these has profound consequences.

iCyPhy

Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org

Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

SST: Secure Swarm Toolkit

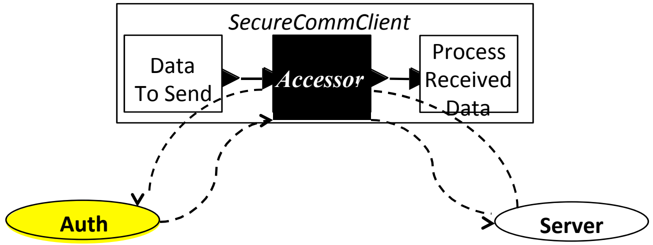
Authorization, Authentication, Security for IoT

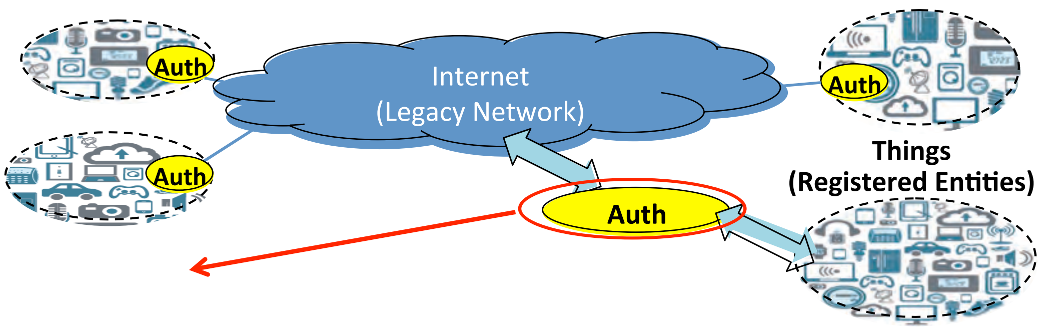
[Hokeun Kim]

Goal: Scalable, distributed, energy-sensitive network security for IoT, usable by application developers with modest security skills.

Approach:

- Open-source local authorization entity *Auth* as a gateway for authorization of the local "Things"
- Secure communication accessors for accessing local authorization service





Swarmlet streams data to/from a secure, authenticated accessor for either a client or a server.

Local Auth provides a range of security alternatives (protocols, cryptographic algorithms, key lifetimes, cached keys) by integrating techniques from existing security measures.

[1] "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities", H. Kim, A. Wasicek, B. Mehne, and E. A. Lee, FiCloud '16

SST: Secure Swarm Toolkit

Authorization, Authentication, Security for IoT

[Hokeun Kim]

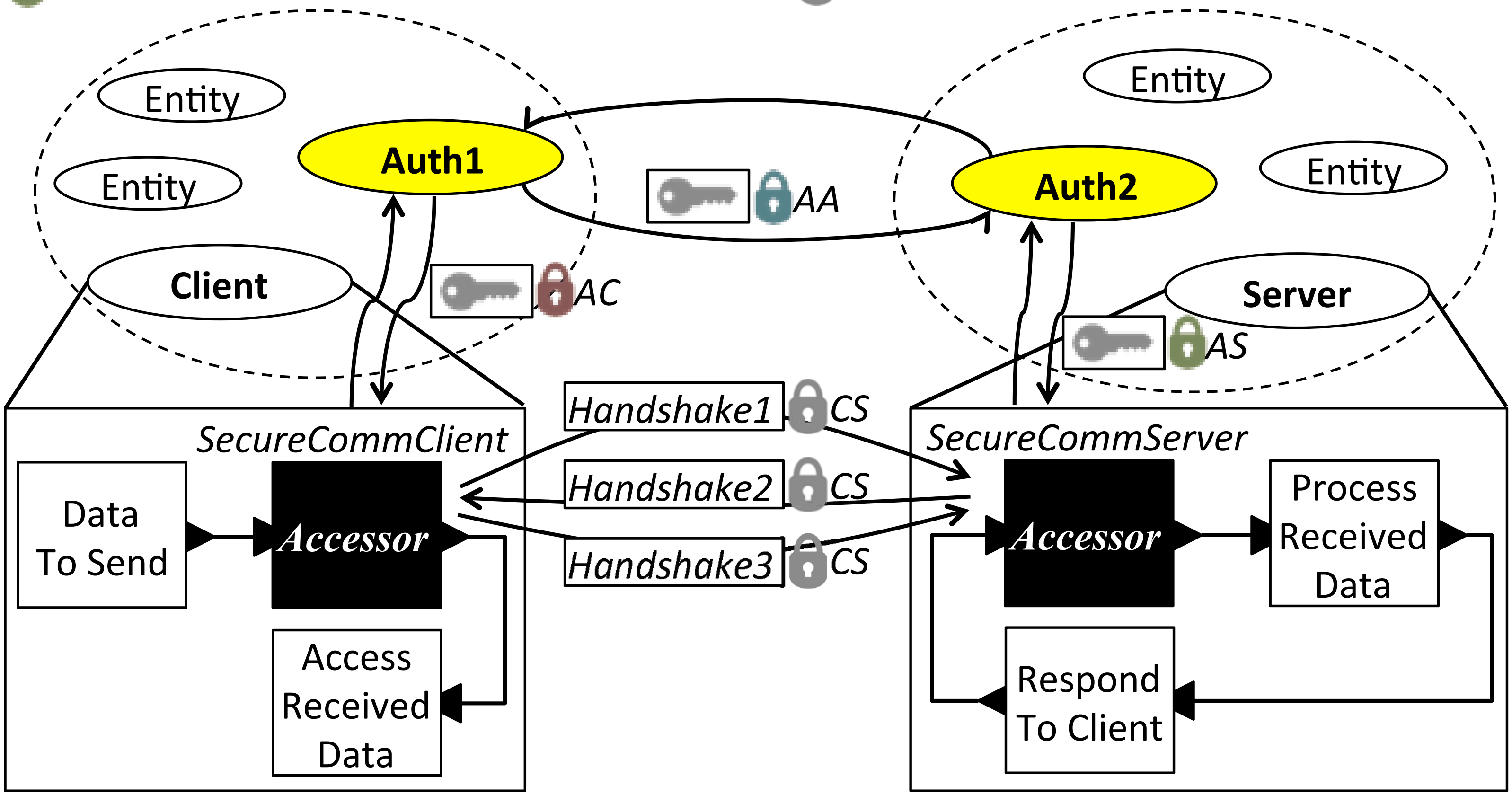
: Key for **C**lient & **S**erver

AC: Encrypted with Key for **A**uth1 & **C**lient

AA: Encrypted with Key for **A**uth1 & **A**uth2

AS: Encrypted with Key for **A**uth2 & **S**erver

CS: Encrypted with Key for **C**lient & **S**lient



iCyPhy

Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

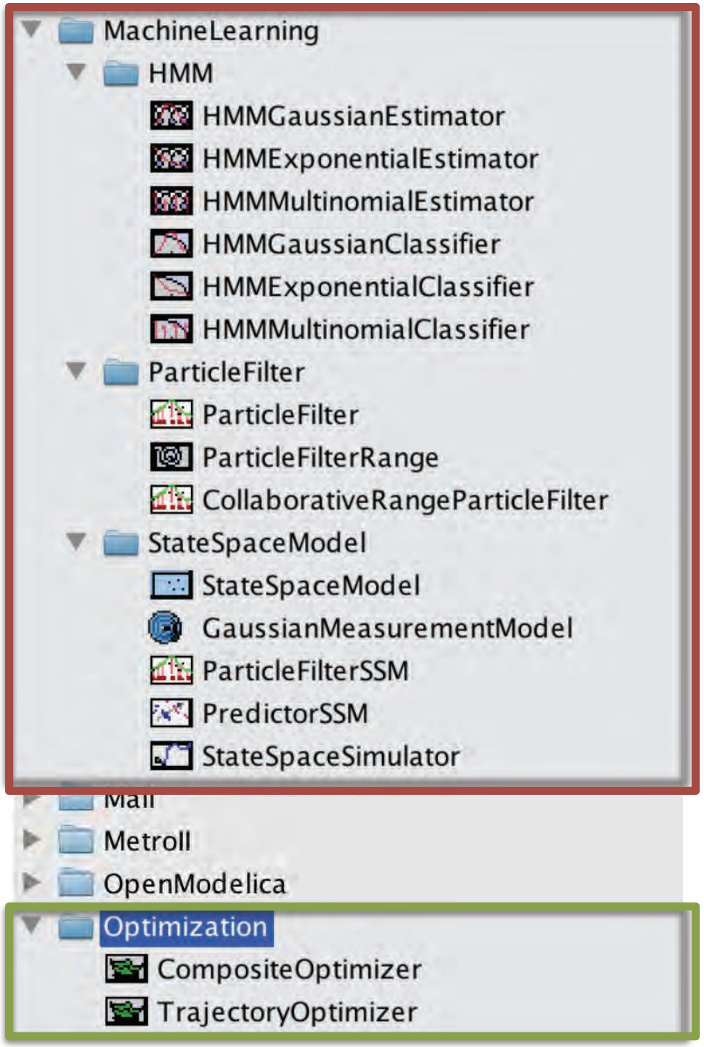
http://icyphy.org



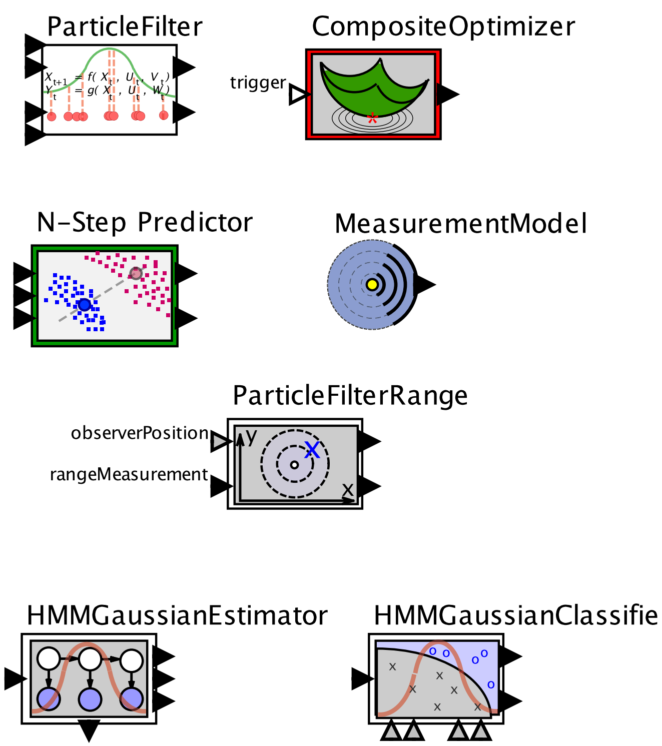

Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

PILOT: Ptolemy Learning, Inference, and Optimization Toolkit

[Akkaya]

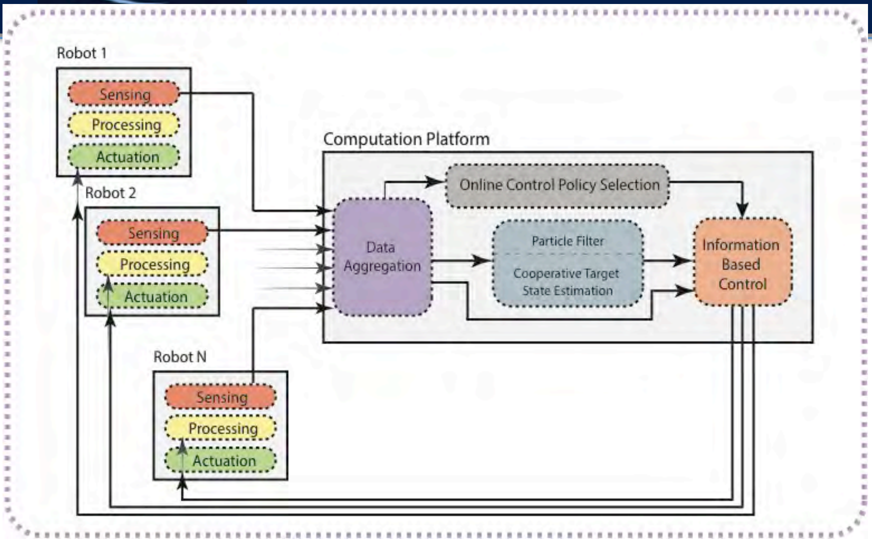


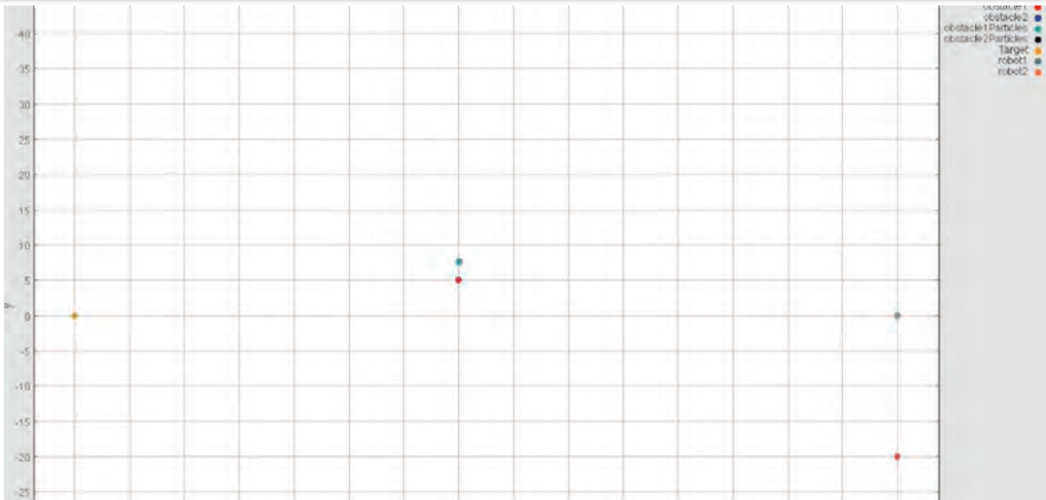
- Actor-oriented toolkit to build models on streaming data
- Bayesian Inference, state estimation, constrained optimization

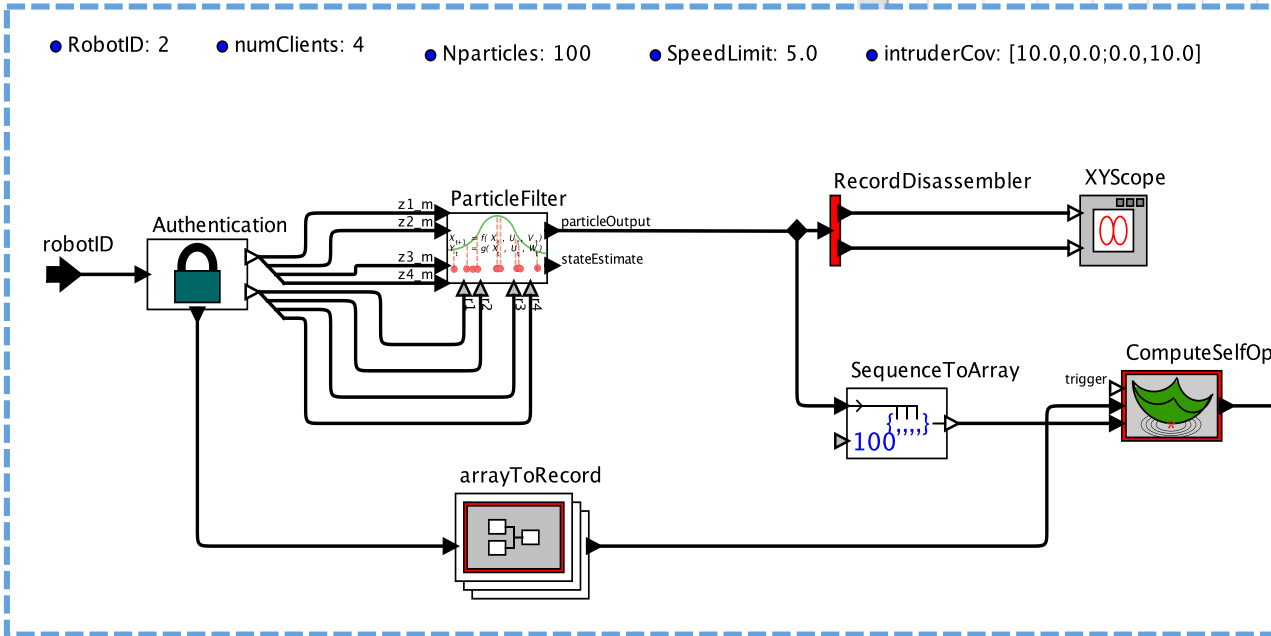


Robot Sensor Networks: Cooperative Target Localization

[Akkaya]







Akkaya, et al., "PILOT: An Actor-Oriented Learning and Optimization Toolkit for Robotic Applications," Workshop on Robotic Sensor Networks (RSN), CPS Week, Seattle, April, 2015.

Emoto et al., "Information Seeking and Model-Predictive Control of a Cooperative Robot Swarm," International Symposium on Swarm Behavior and Bio-Inspired Robotics, October 28–30, Kyoto, Japan.

iCyPhy

Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org

Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

Spatial Ontologies and Semantic Localization

[Weber]

<u>Goal:</u> Develop a Logic for Reasoning About Spatial Relationships in the Swarm, Facilitate Composition of Diverse Map Data

<u>Applications:</u> Enhance Accuracy, Security, and Privacy in Swarm Localization

Leverage ontological mapping to translate location information across maps

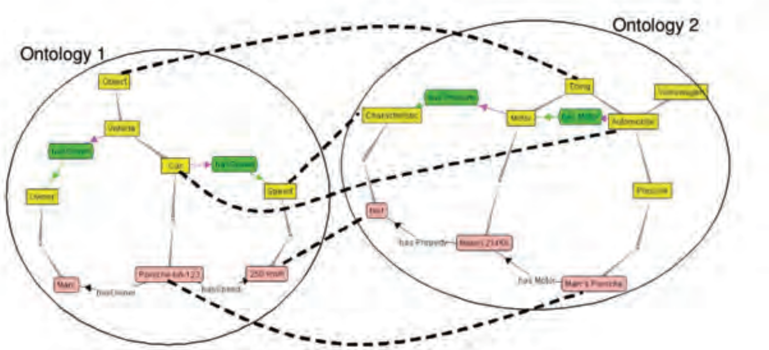
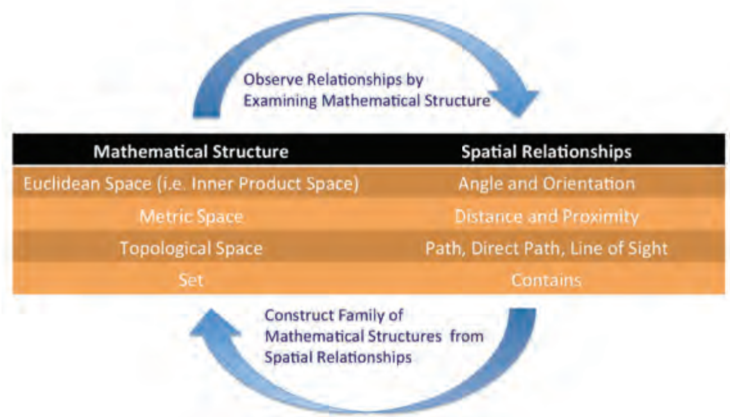


Image from S. Godugula and G. Engels, "Survey of ontology mapping techniques," *Software Quality and Assurance*, 2008.



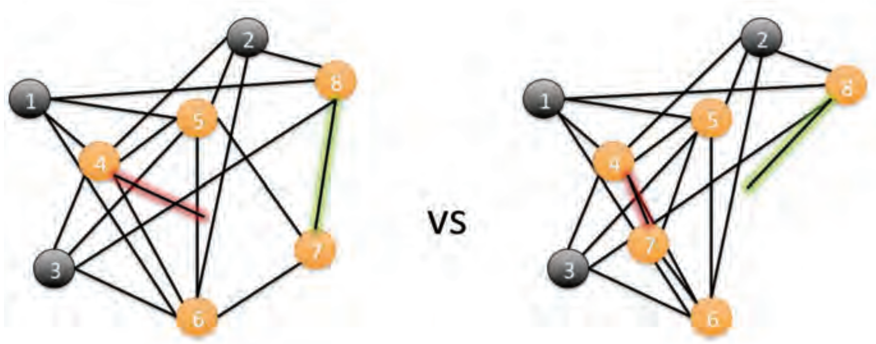
- Facilitate logical inference and verification for semantic localization
- Relate semantic localization to mathematical structures

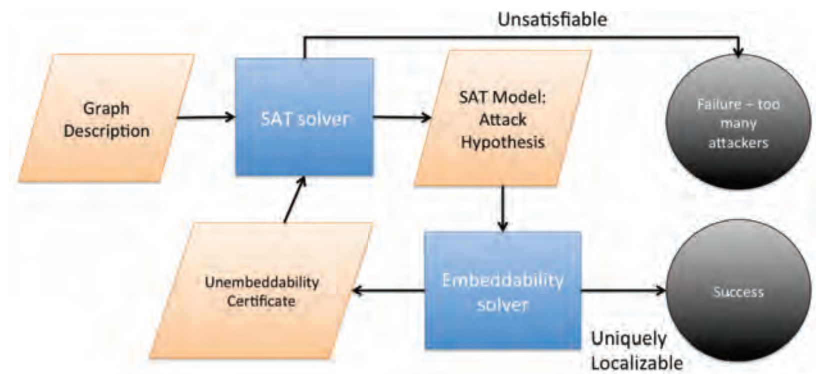
Gordian SMT: Untangling Localization Attacks in Noisy Sensor Networks

[Weber, Jin, Lederman, Shoukry, Lee, Seshia, Sangiovanni-Vincentelli]

Goal: Correctly Localize Swarm Devices with Inter-Node Distance Measurements Even in the Presence of Malicious Interference

Applications: Driverless Cars, Localization as an Authentication Mechanism, Consistency Testing for Semantic Localization





Approach:

- Detect impossible graphs with a semidefinite programming-based localization algorithm
- SAT assisted SMT solving architecture rapidly identifies maliciously corrupted edges.

"Gordian SMT: Untangling Localization Attacks in Noisy Sensor Networks", M. Weber, B. Jin, G. Lederman, Y. Shoukry, E. Lee, S Seshia, A. Sangiovanni-Vincentelli, submitted IPSN'17.

Overview Paper

Invited Paper for Sensors Journal

February, 2015
Open Access

Article

The Past, Present, and Future of Cyber-Physical Systems — A Focus on Models

Edward A. Lee

EECS Department, University of California, Berkeley, CA, USA

Version January 24, 2015 submitted to Sensors. *Typeset by LaTeX using class file mdpi.cls*

Abstract: This paper is about better engineering of cyber-physical systems (CPSs) through better models. Deterministic models have historically proved extremely useful, and arguably form the kingpin of the industrial revolution and the digital and information technology revolutions. Key deterministic models that have proved successful include differential equations, synchronous digital logic, and single-threaded imperative programs. Cyber-physical systems, however, combine these models in such a way that determinism is not preserved. Two projects show that deterministic CPS models with faithful physical realizations are possible and practical. The first project is PRET, which shows that the timing precision of synchronous digital logic can be practically made available at the software level of abstraction. The second project is Ptides, which shows that deterministic models for distributed cyber-physical systems have practical faithful realizations. These projects are existence proofs that deterministic CPS models are possible and practical.

iCyPhy

Industrial Cyber-Physical Systems Center

ICyPhy is a university-industry partnership to pursue pre-competitive research on design, modeling, and analysis techniques for cyber-physical systems, with emphasis on industrial applications. Topics:

- Hardware and software architectures
- Model-based design for CPS
- Highly dynamic networked systems
- The Internet of things (IoT)
- Safety, privacy, and security
- Synthesis and learning
- Localization and location-aware services
- Learning and optimization
- Safety-critical systems
- Human-in-the-loop systems.
- Systems-of-systems design
- Semantics of timed systems

http://icyphy.org

Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia