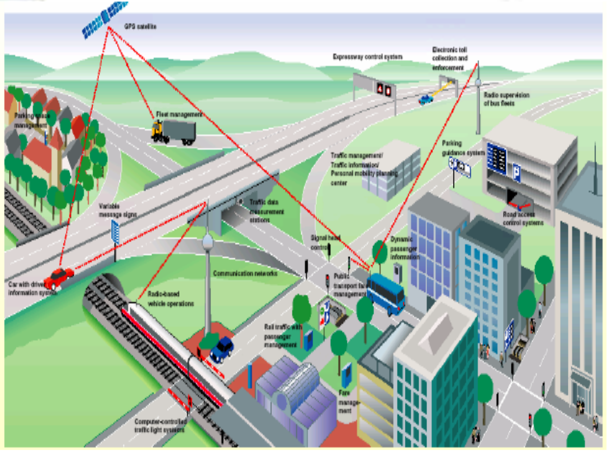
Overview of Systems, Control and Communications Research by Baras' Research Group

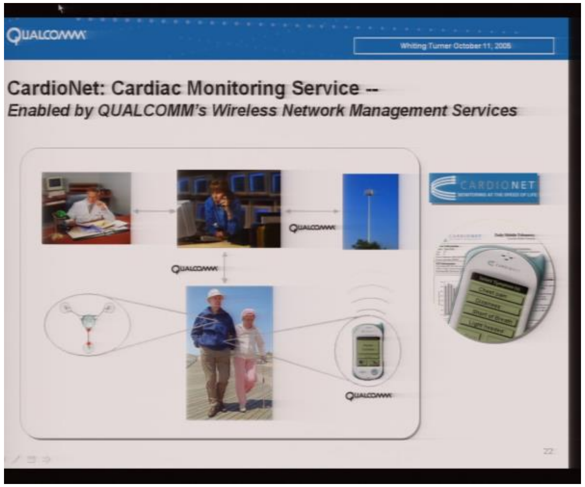
John S. Baras

**Lockheed Martin Chair,
The Institute for Systems Research and
Electrical and Computer Engineering Department,
University of Maryland College Park**

***July 8, 2016
Presentation to ECE Dept. Advisory Board
University of Maryland
College Park, Maryland***

Networked S-CPS: Ubiquitous Presence


GPS satellite
Expressway control system
Electronic toll collection and enforcement
Radio supervision of bus fleets
Parking space management
Fleet management
Traffic management/ Traffic information/ Personal mobility planning center
Parking guidance system
Variable message signs
Traffic data measurement stations
Road access control systems
Signal head control
Dynamic passenger information
Communication networks
Public transport fare management
Car with driver information system
Radio-based vehicle operations
Rail traffic with passenger management
Fare management
Computer-controlled traffic light systems



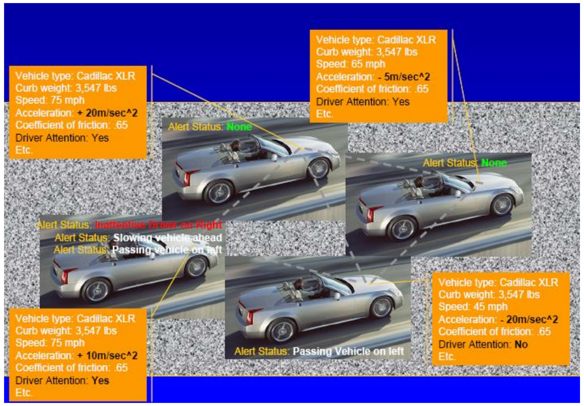
Whiting Turner October 11, 2005

CardioNet: Cardiac Monitoring Service --

Enabled by QUALCOMM's Wireless Network Management Services

22

QUALCOMM
CARDIONET
MONITORING AT THE SPEED OF LIFE
Chest pain
Dizziness
Short of Breath
Light headed



Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 75 mph
Acceleration: + 20m/sec^2
Coefficient of friction: .65
Driver Attention: Yes
Etc.

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 65 mph
Acceleration: - 5m/sec^2
Coefficient of friction: .65
Driver Attention: Yes
Etc.

Alert Status: None

Alert Status: None

Alert Status: Inattentive Driver on Right
Alert Status: Slowing vehicle ahead
Alert Status: Passing vehicle on left

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 75 mph
Acceleration: + 10m/sec^2
Coefficient of friction: .65
Driver Attention: Yes
Etc.

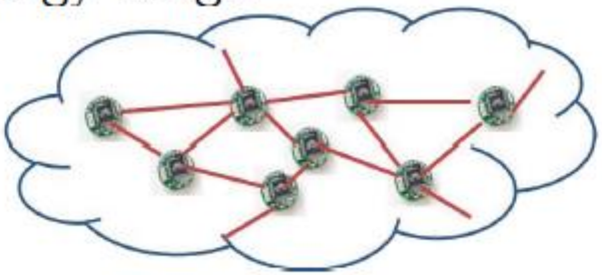
Alert Status: Passing Vehicle on left

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 45 mph
Acceleration: - 20m/sec^2
Coefficient of friction: .65
Driver Attention: No
Etc.

Sensor Networks Everywhere

Wireless Sensor Networks (WSN) for infrastructure monitoring

- Environmental systems
- Structural health
- Construction projects
- Energy usage



Bridges

Snowpack

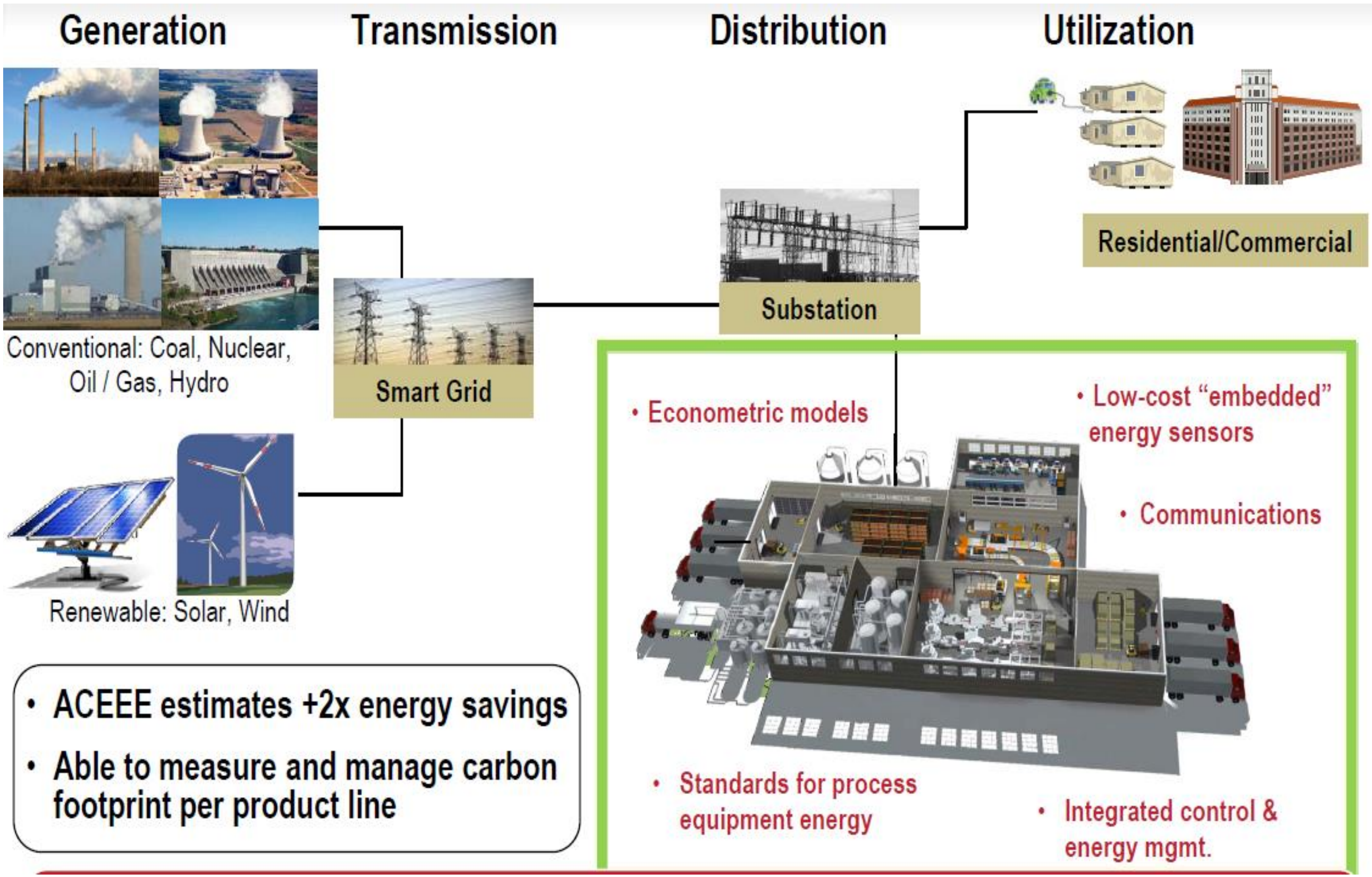
Soil liquefaction

Smart buildings

Traffic

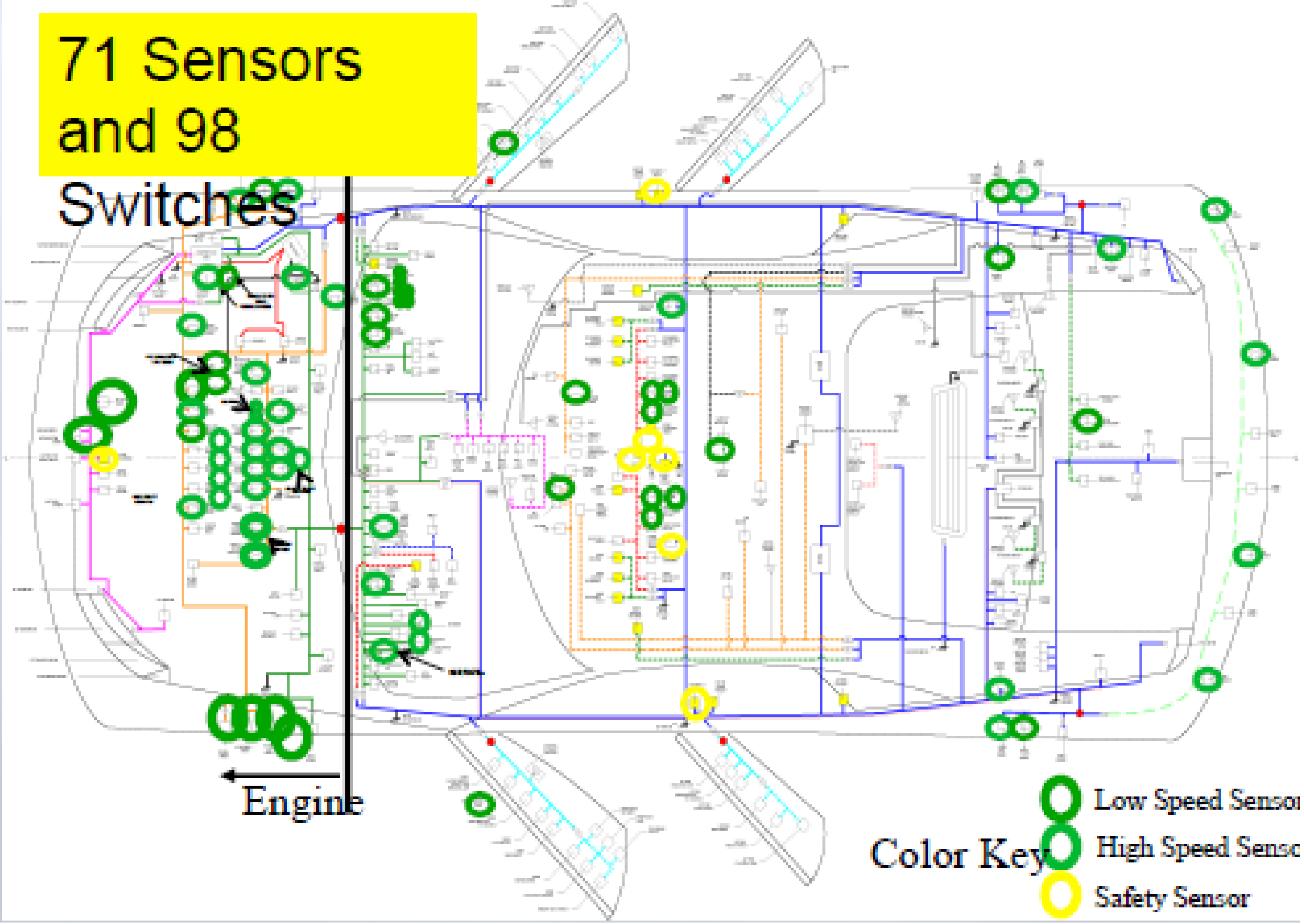
Vineyards

Smart Grids in a Network Immersed World


Generation
Transmission
Distribution
Utilization
Conventional: Coal, Nuclear, Oil / Gas, Hydro
Smart Grid
Substation
Residential/Commercial
Renewable: Solar, Wind
• Econometric models
• Low-cost "embedded" energy sensors
• Communications
• Standards for process equipment energy
• Integrated control & energy mgmt.

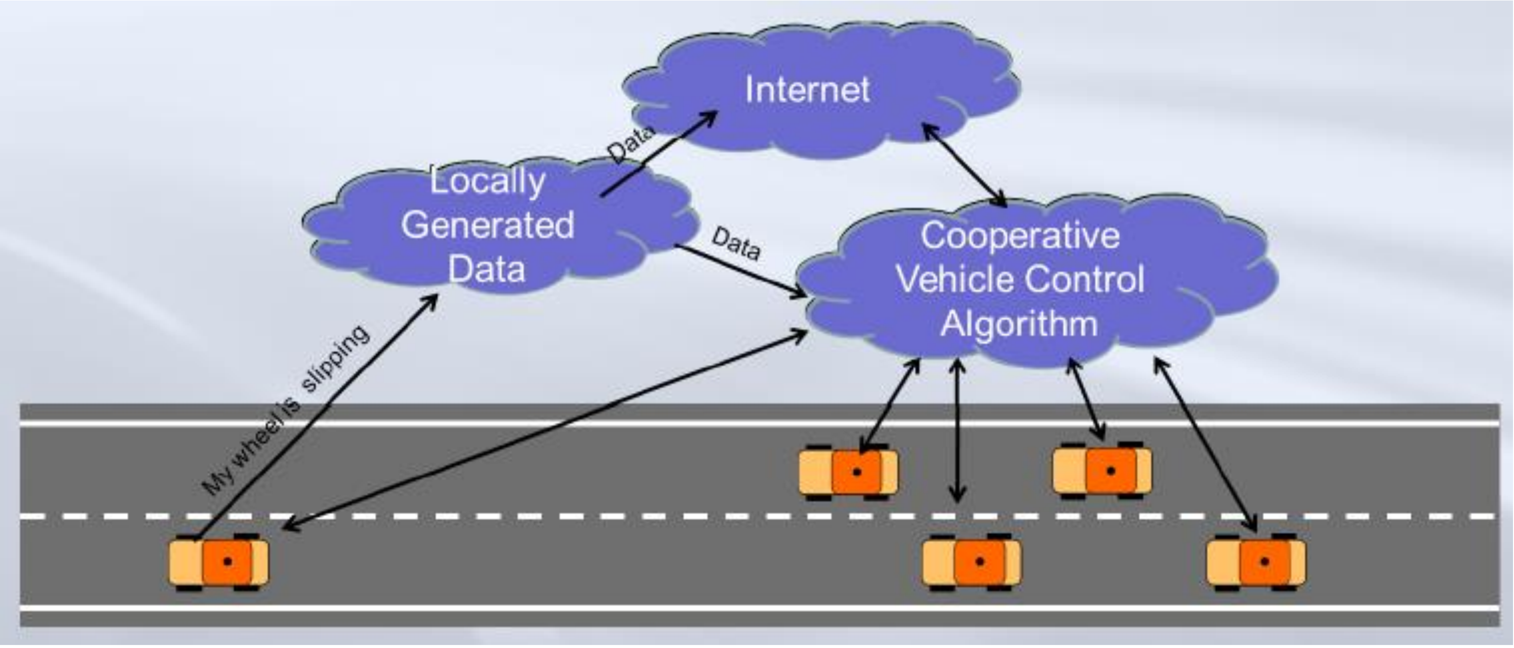
- ACEEE estimates +2x energy savings
- Able to measure and manage carbon footprint per product line

Connected Cars: Internal



Connected Cars: External

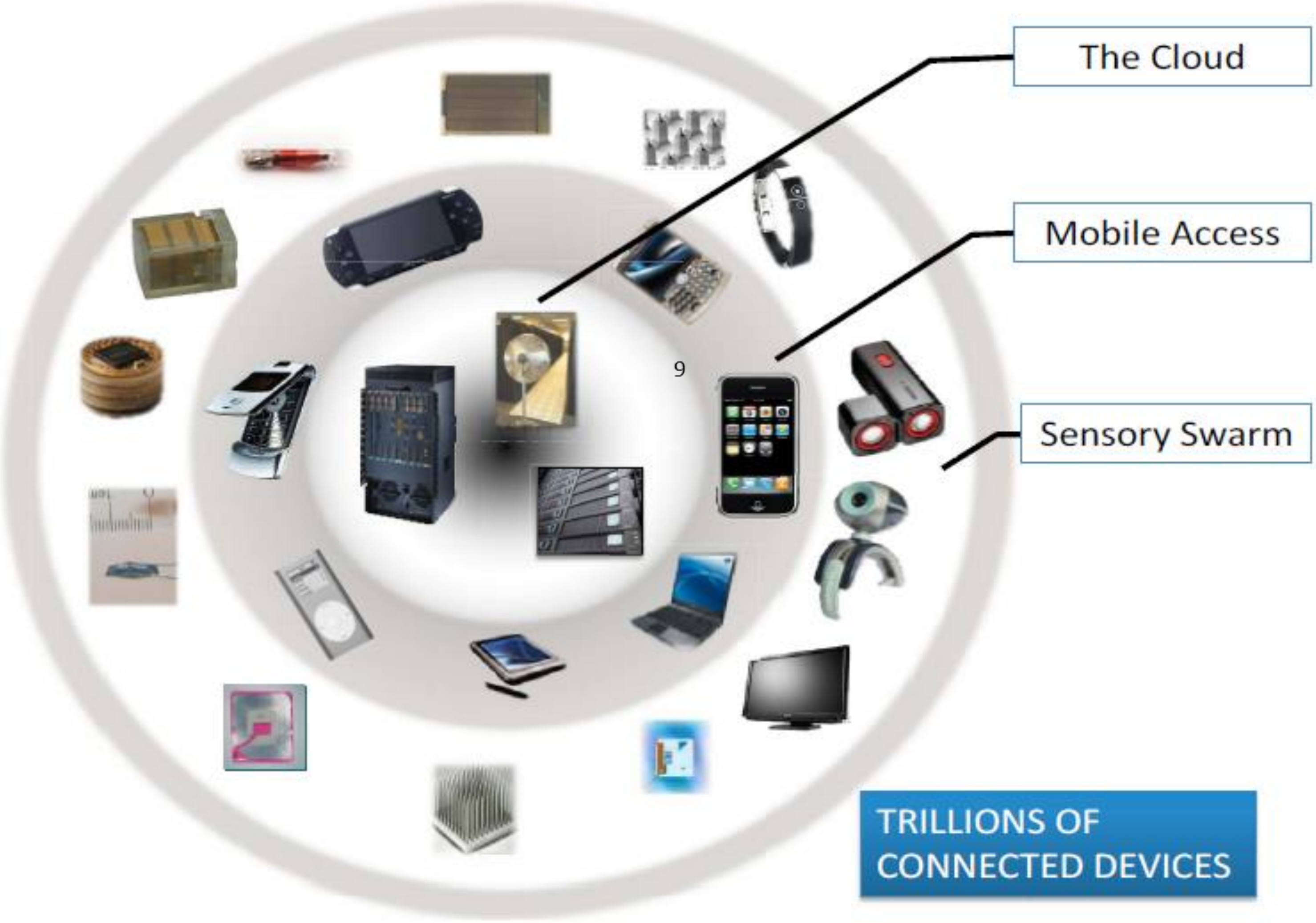
Connected Cars: Cognitive and Collaborative



Key Challenge: **Humans**

We are developing novel frameworks to include humans in this collaborative networked CPS environment

A Network Immersed World: Swarms and the Cloud



The Cloud

Mobile Access

Sensory Swarm

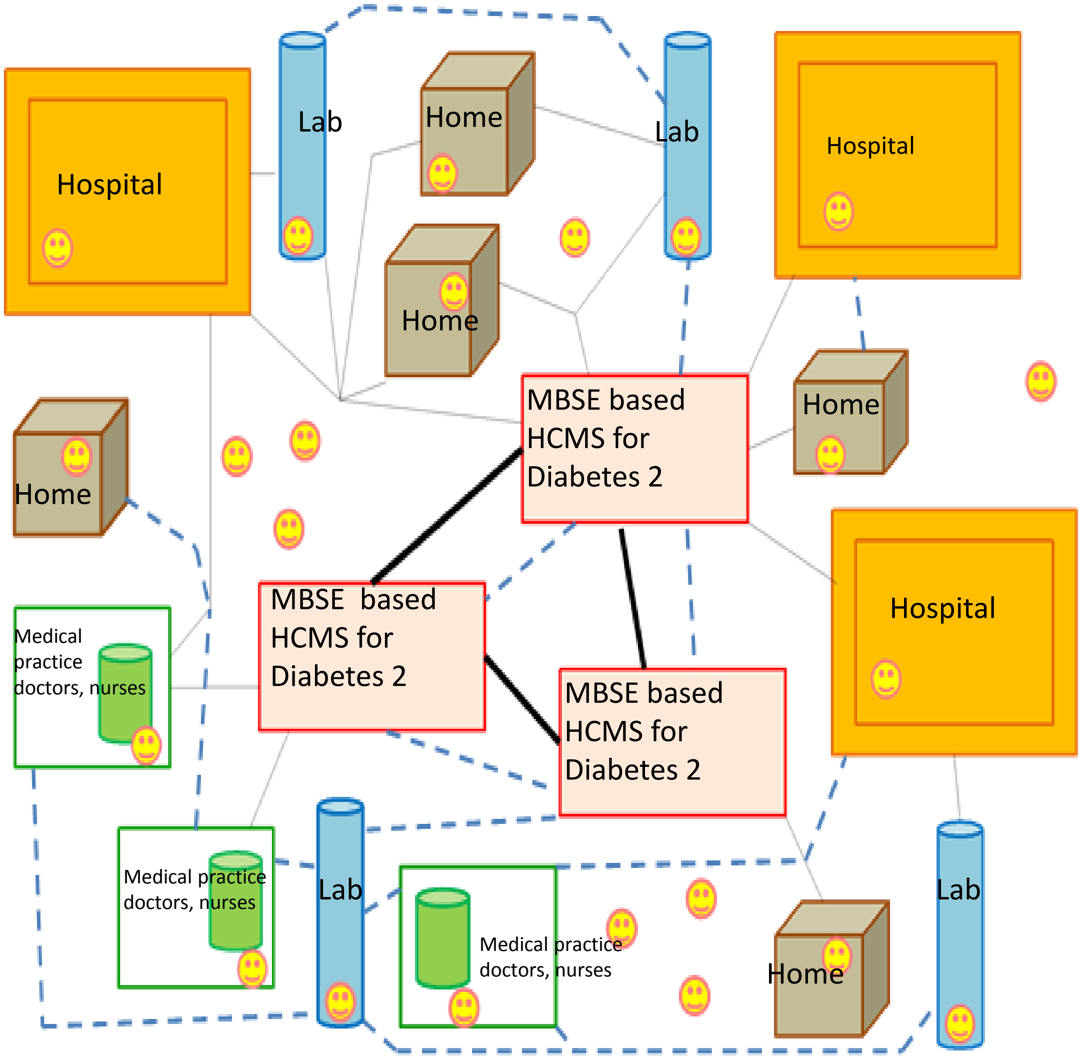
TRILLIONS OF CONNECTED DEVICES

Social Networks

- Online social network services (SNS)
  - Permeate our lives with tremendous popularity
  - Decision making via combining information from different sources
  - Benefits SNS-based applications
    - Recommender Systems
    - Online Ad targeting
- Trust relationships in SNS
  - People put different levels of trust on others in SNS
  - Important in decision making
    - People tend to accept suggestions from those they trust more

***Our work:* Semiring-Based Trust Evaluation for Information Fusion in Social Network Services**

MBSE based HCMS for Diabetes II and its functional connectivity



Hospital
Lab
Home
Lab
Hospital
Home
MBSE based HCMS for Diabetes 2
Home
Home
Medical practice doctors, nurses
MBSE based HCMS for Diabetes 2
MBSE based HCMS for Diabetes 2
Hospital
Medical practice doctors, nurses
Lab
Medical practice doctors, nurses
Home
Lab

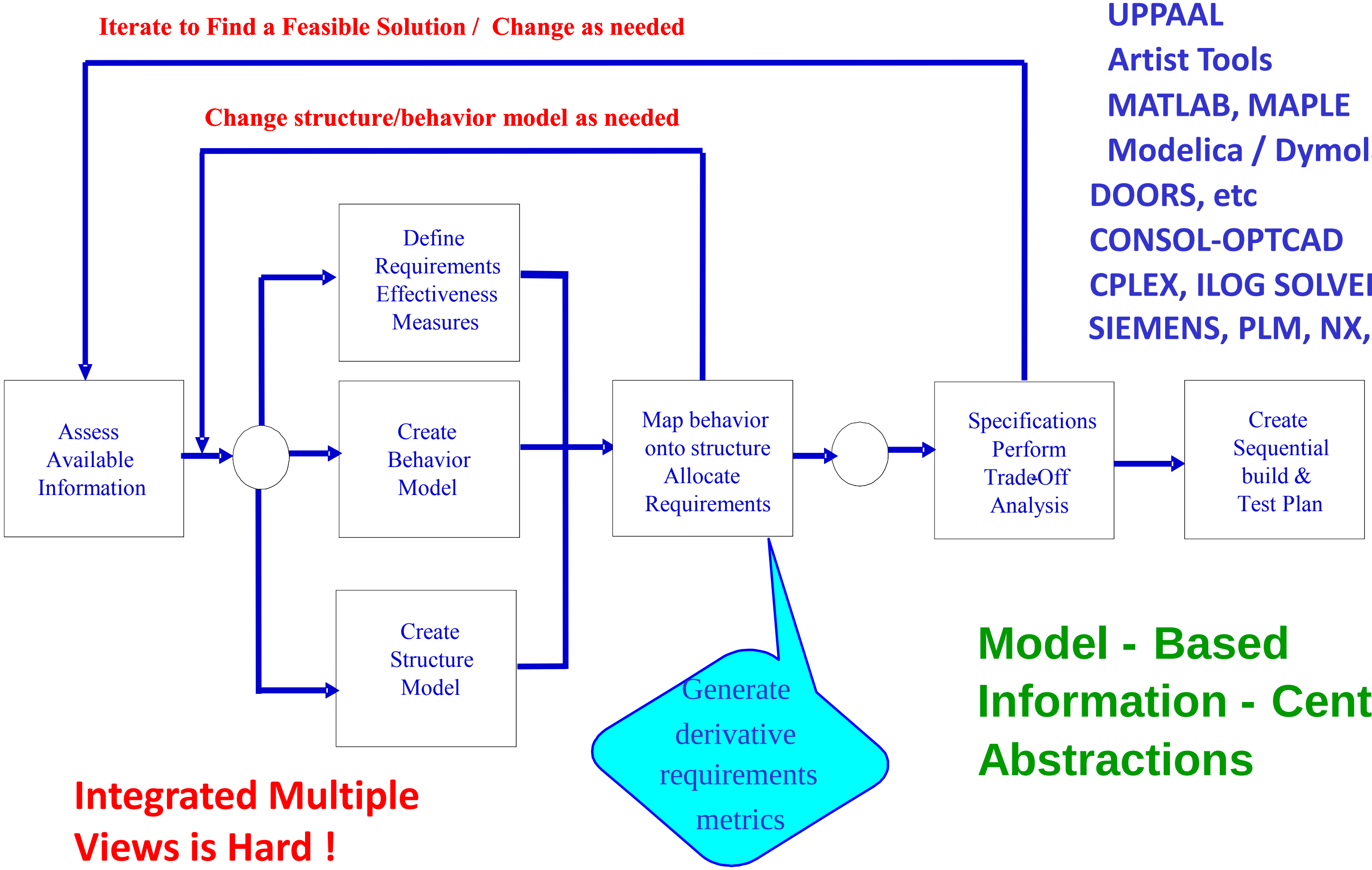
Framework for MBSE: Key Challenges Addressed

- Methodology to develop integrated modeling hubs (IMH) for CPS – multi-physics and cyber
- Methodology to link IMHs with design space exploration via multi-criteria tradeoff methods and tools
- Linkage to component databases
- Working on the last remaining challenge: requirements management
- Developed new methods and tools to handle complexity in design space exploration

MODEL-BASED SYSTEMS ENGINEERING COMPONENTS -- ARCHITECTURE

Integrated System Synthesis Tools - & Environments missing

Model- - based
UML - SysML - GME - eMFLON
Rapsody
UPPAAL
Artist Tools
MATLAB, MAPLE
Modelica / Dymola
DOORS, etc
CONSOL-OPTCAD
CPLEX, ILOG SOLVER,
SIEMENS, PLM, NX, TEAM CENTER

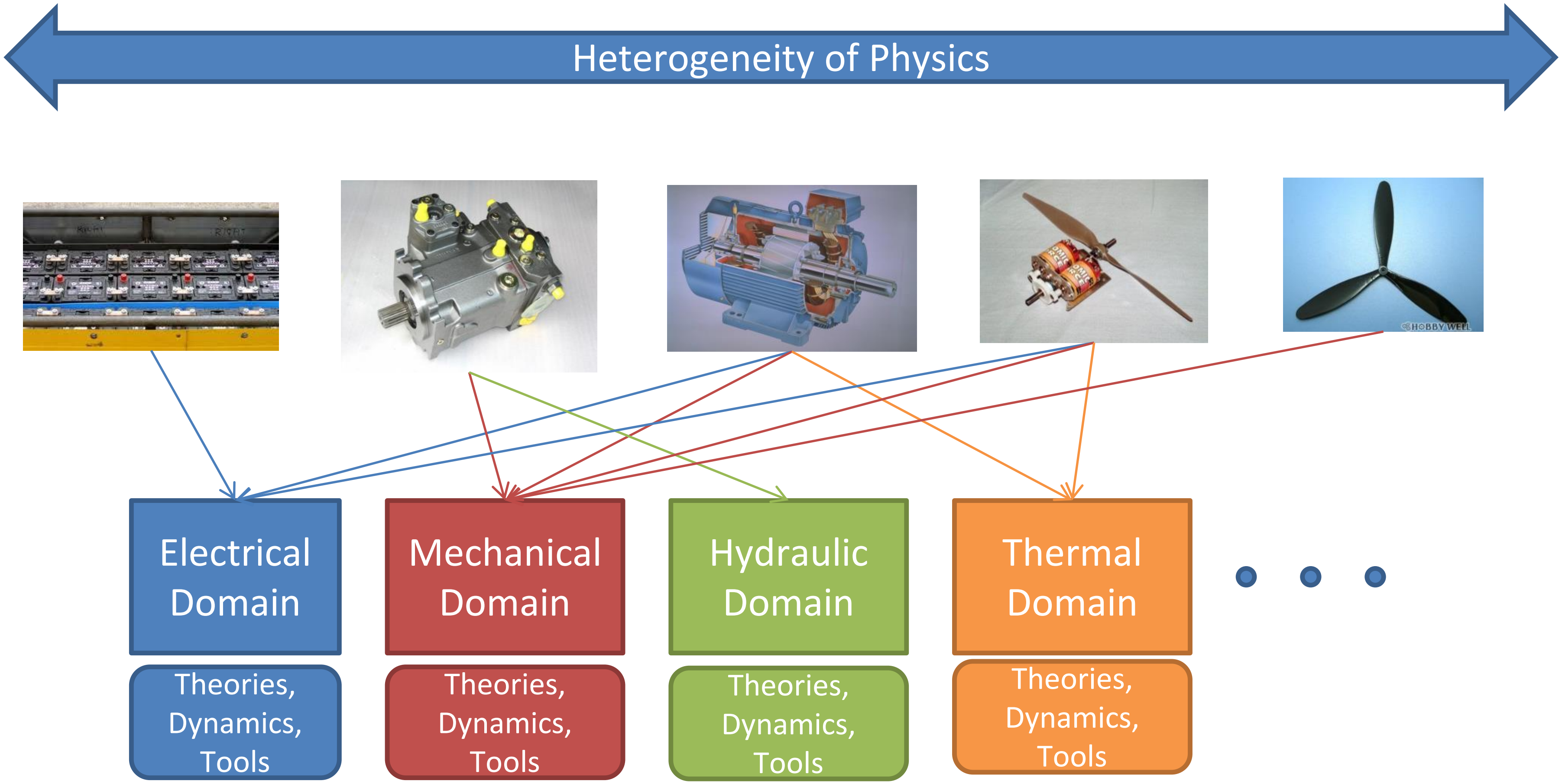


Iterate to Find a Feasible Solution / Change as needed
Change structure/behavior model as needed
Define Requirements Effectiveness Measures
Assess Available Information
Create Behavior Model
Map behavior onto structure Allocate Requirements
Specifications Perform TradeOff Analysis
Create Sequential build & Test Plan
Create Structure Model
Generate derivative requirements metrics

Model - Based Information - Centric Abstractions

Integrated Multiple Views is Hard !

Model Integration Challenge: Physics



Heterogeneity of Physics

Electrical Domain

Theories, Dynamics, Tools

Mechanical Domain

Theories, Dynamics, Tools

Hydraulic Domain

Theories, Dynamics, Tools

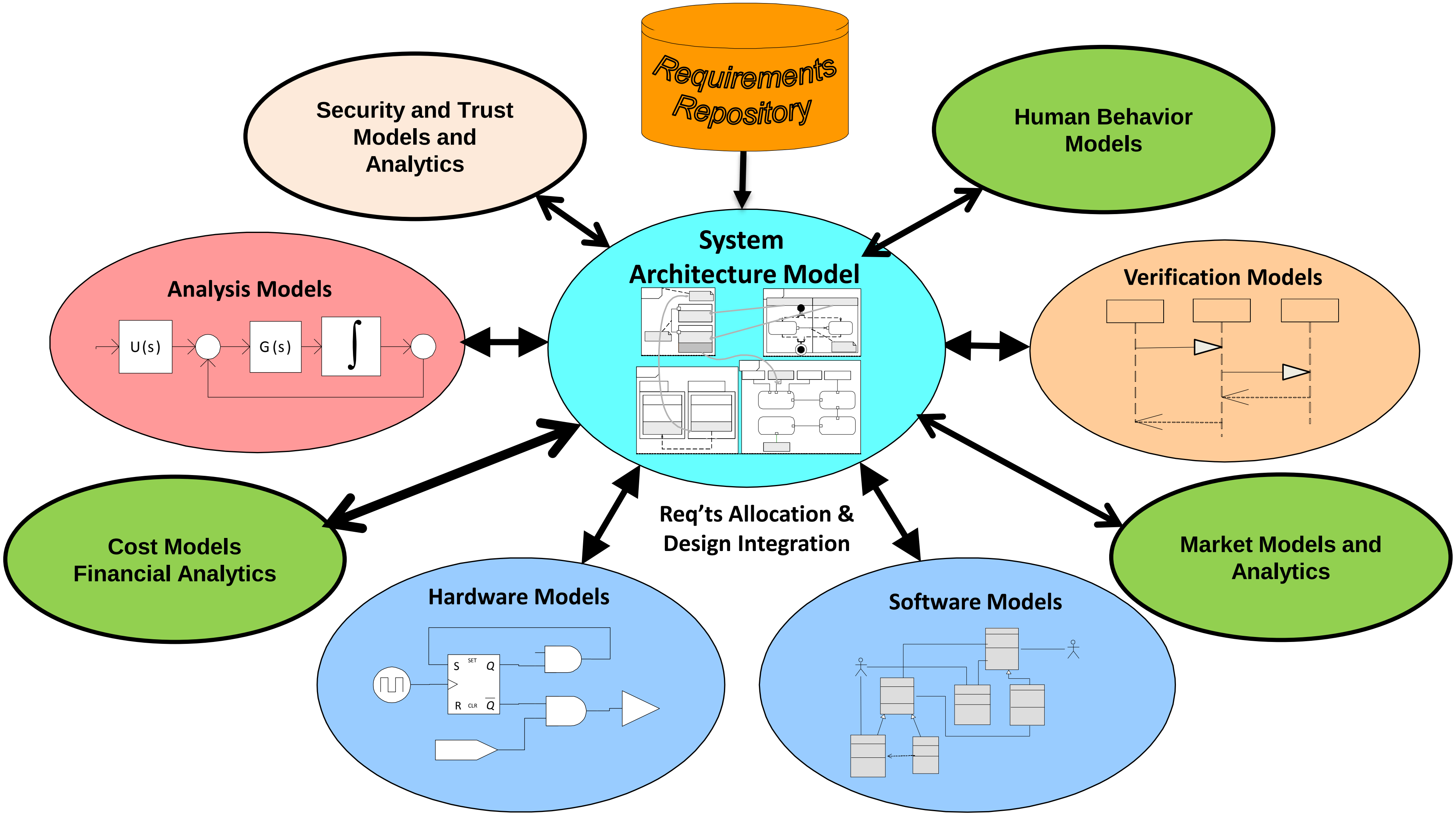
Thermal Domain

Theories, Dynamics, Tools

• • •

Physical components are involved in multiple physical interactions (multi-physics)
Challenge: How to compose multi-models for heterogeneous physical components

Using *System Architecture Model* as an Integration Framework



Requirements Repository

System Architecture Model

Security and Trust Models and Analytics

Human Behavior Models

Analysis Models

Verification Models

Cost Models Financial Analytics

Market Models and Analytics

Req'ts Allocation & Design Integration

Hardware Models

Software Models

The Institute for Systems Research

A Rigorous Framework for Model-based Systems Engineering

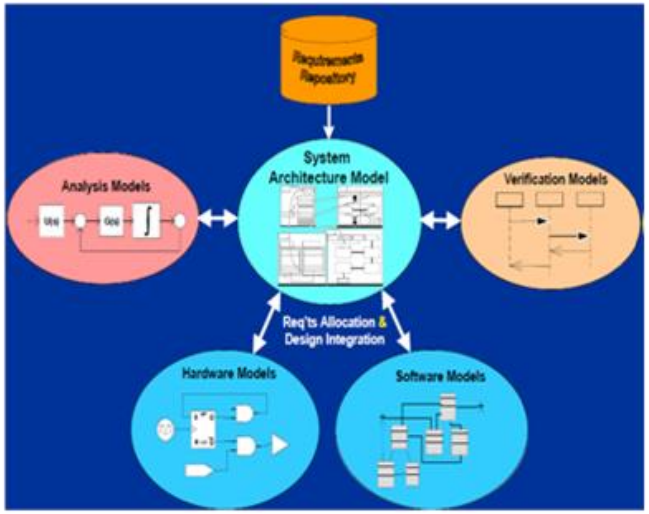
University of Maryland 1856

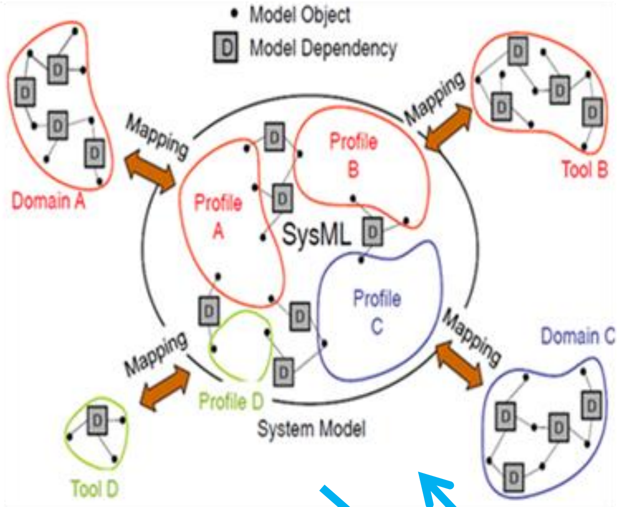
The Challenge & Need:

Develop scalable holistic methods, models and tools for enterprise level system engineering

Multi-domain Model Integration via System Architecture Model (SysML)

System Modeling Transformations





" Master System Model"

Update System Model

ILOG SOLVER, CPLEX, CONSOL-OPTCAD

Tradeoff parameters

ADD & INTEGRATE

- **Multiple domain modeling tools**
- **Tradeoff Tools (MCO & CP)**
- **Validation / Verification Tools**
- **Databases and Libraries of annotated component models from all disciplines**

DB of system components and models

BENEFITS

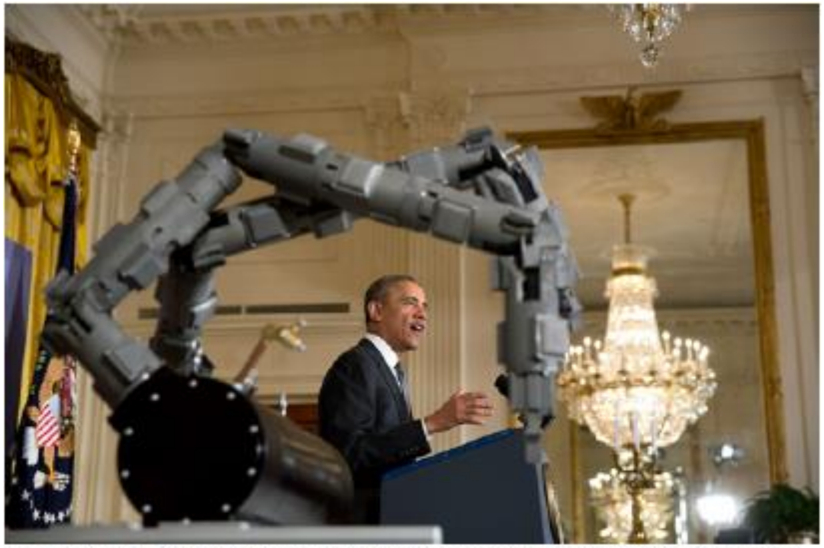
- **Broader Exploration of the design space**
- **Modularity, re-use**
- **Increased flexibility, adaptability, agility**
- **Engineering tools allowing conceptual design, leading to full product models and easy modifications**
- **Automated validation/verification**

APPLICATIONS

- **Avionics**
- **Automotive**
- **Robotics**
- **Smart Buildings**
- **Power Grid**
- **Health care**
- **Telecomm and WSN**
- **Smart PDAs**
- **Smart Manufacturing**

Digital Manufacturing Design Innovation Institute (DMDII)

- Announced February 25, 2014, 2014 by President Obama
  http://www.whitehouse.gov/the-press-office/2014/02/25/president-obama-announces-two-new-public-private-manufacturing-innovatio



President Barack Obama delivers remarks announcing two new public-private Manufacturing Innovation Institutes, and launches the first of four new Manufacturing Innovation Institute Competitions, in the East Room of the White House, Feb. 25, 2014. (Official White House Photo by Lawrence Jackson)

- Headquartered in Chicago, Illinois
- Academic-Industry-Government "Mega Project" $320M co-funding, 5 years
- **Goal**: Revitalize manufacturing along the lines described in this lecture

- "Infinite number of virtual factories and an open-source manufacturing platform"

Crowdsourcing Manufacturing

- ***Google's Project ARA***: Smartphones are composed of modules (of the owner's choice) assembled into metal frames

- ***Ubundu Edge Project***: crowdsourcing the most radical smartphone yet "Why not look for the best upcoming tech and throw it together to stay ahead of the competition?"
- ***Crowdsourcing*** the development and manufacturing of ***small unmanned aerial vehicles***

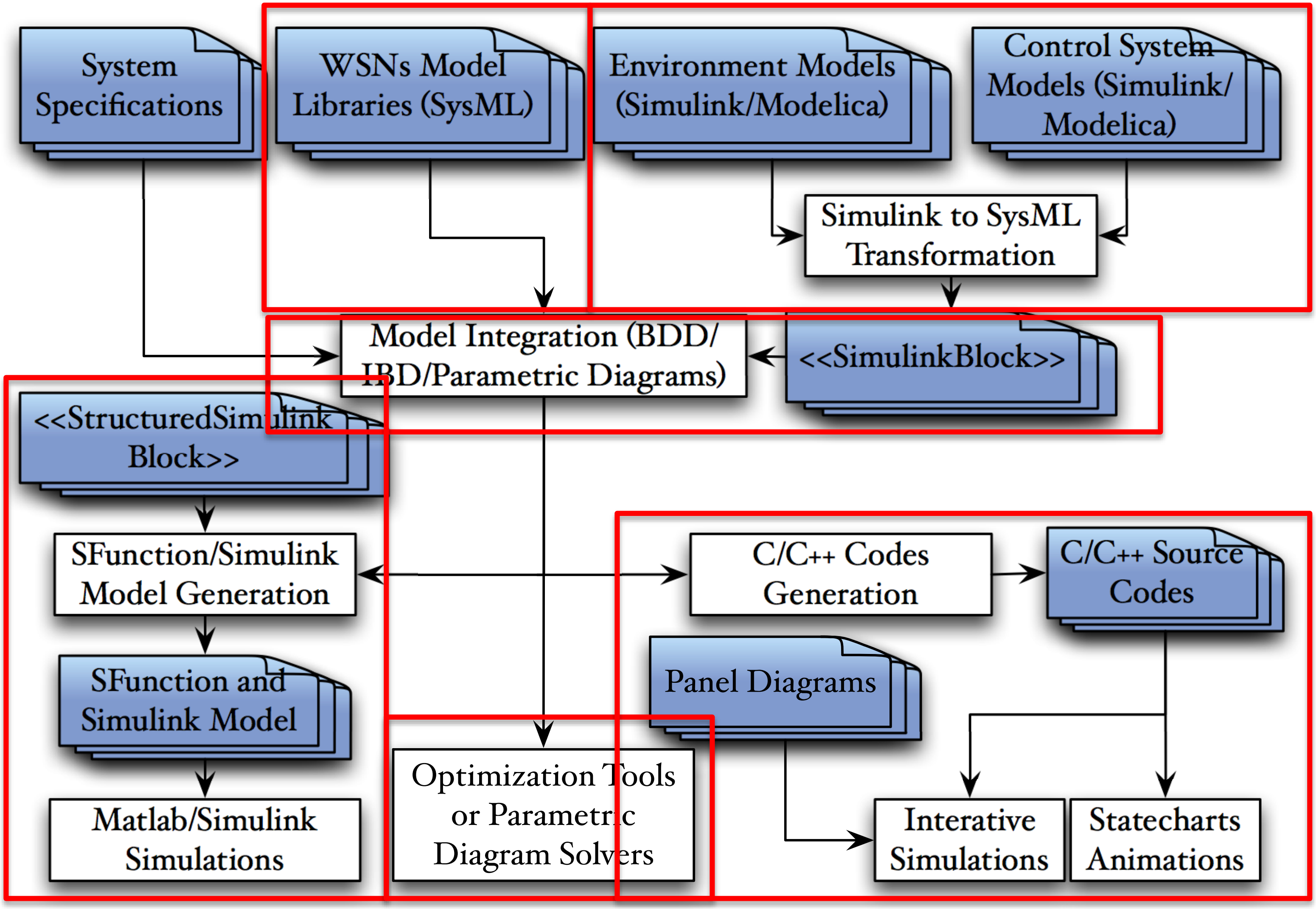
"Democratizing" Manufacturing

- **Goal**: Transforming more ordinary people to "makers" of products and services
- Helping small and medium size companies to manufacture products and services – **bridge the "gap"** from innovation, prototyping, to manufacturing

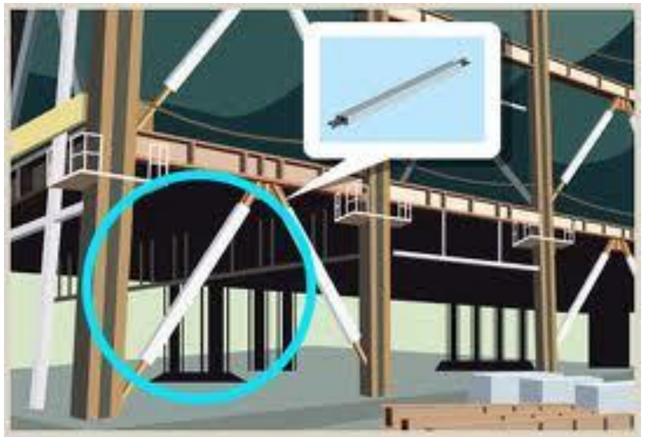
- General Electric (GE) opens manufacturing fab lab to spark ideas and participation in manufacturing through making
- Several companies have also opened up similar "open" labs: Ford etc.

- Several regional manufacturing centers (industry-university-government) are being established in various regions of USA
- "Industrial Internet" (USA) and "Industrie 4.0" (GE-EU) arrive

MBSE for Sensor Networks


System Specifications
WSNs Model Libraries (SysML)
Environment Models (Simulink/Modelica)
Control System Models (Simulink/ Modelica)
Simulink to SysML Transformation
Model Integration (BDD/ IBD/Parametric Diagrams)
<<SimulinkBlock>>
<<StructuredSimulink Block>>
SFunction/Simulink Model Generation
SFunction and Simulink Model
Matlab/Simulink Simulations
Optimization Tools or Parametric Diagram Solvers
C/C++ Codes Generation
C/C++ Source Codes
Panel Diagrams
Interative Simulations
Statecharts Animations

CPS Architecture: Buildings

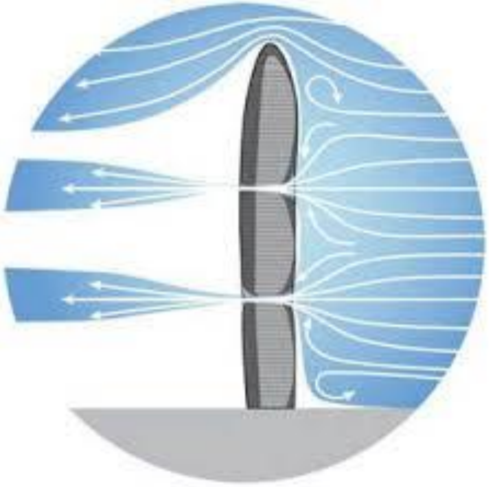


Architecture for earthquake resistance

Add computer controlled sensors, shock absorbers, material properties

CPS architecture?

Architecture for energy efficiency



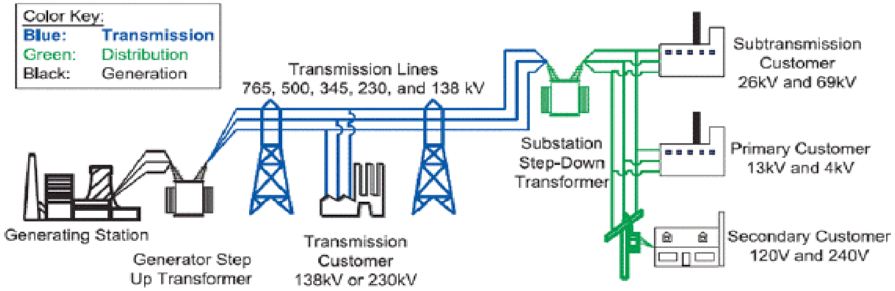
Pearl River Tower Complex, Guangzhou

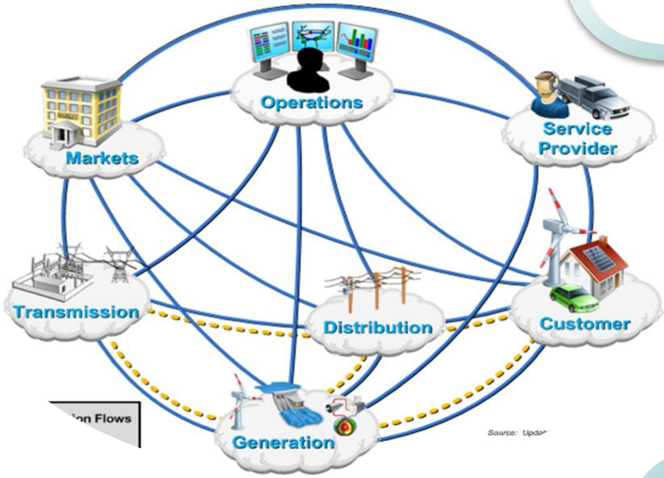
Add computer controlled sensing, HVAC, etc.

CPS architecture?

Smart Grid – Microgrids Architecture

Grid 1.0
Legacy Grid





Grid 2.0
Smart Grid

Grid 3.0
Future Grid

© 2009 Electric Power Research Institute, Inc. All rights reserved.

CPS Architecture: Materials-Geometry-Controls

The 787 Dreamliner delivers:

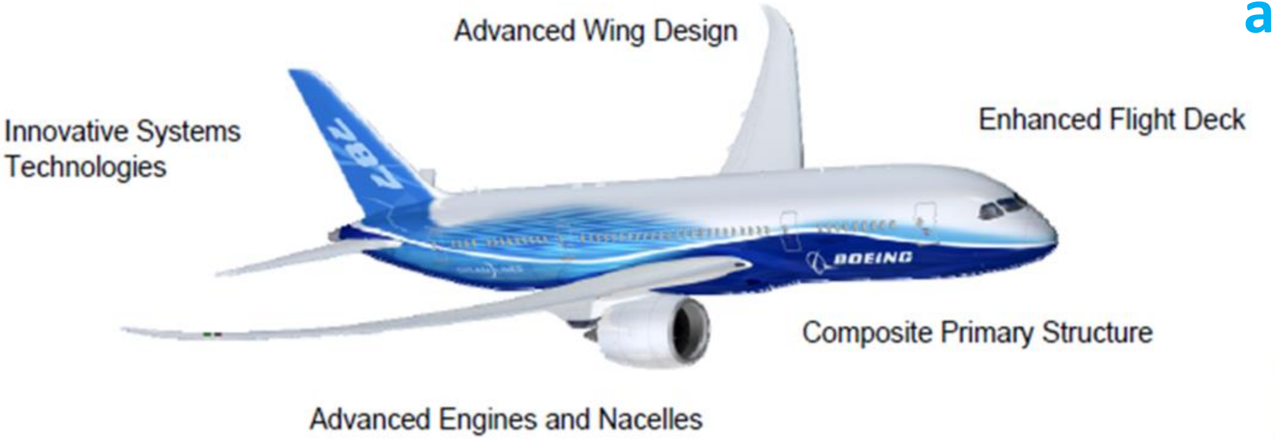
*Relative to the 767

20%* reduction in fuel and CO_2

28% below 2008 industry limits for NOx

60%* smaller noise foot print

Architecture Logics, their Representation and Integration

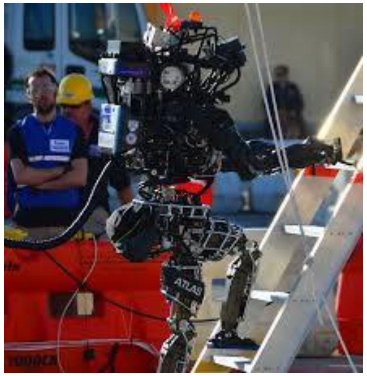

Advanced Wing Design
Innovative Systems Technologies
Enhanced Flight Deck
Composite Primary Structure
Advanced Engines and Nacelles
787
BOEING

Composite wing* – *new control algorithms

All-electric platform* – *new aircraft VMS

Smart suit* – *improve physical endurance & energy harvesting

Collaborative Autonomy



Approach: Four Pillars

The cognitive dialogue – a new architecture and formalism for cognitive systems

A dynamic attention mechanism that works through a combination of signal processing and symbolic processing of prior knowledge

The manipulation grammar and its associated *parser*

A three-layer architecture involving dynamically interacting multi-graphs and heterogeneous internal world models

Approach (cont.)

Key problems:

Robots must make sense of cluttered audio-visual environments to execute autonomously and collaboratively tasks

Find and identify objects, tools, actions, based on multi-sensory input and prior knowledge

Represent and store prior knowledge

Search scene and knowledge in an efficient and organized manner

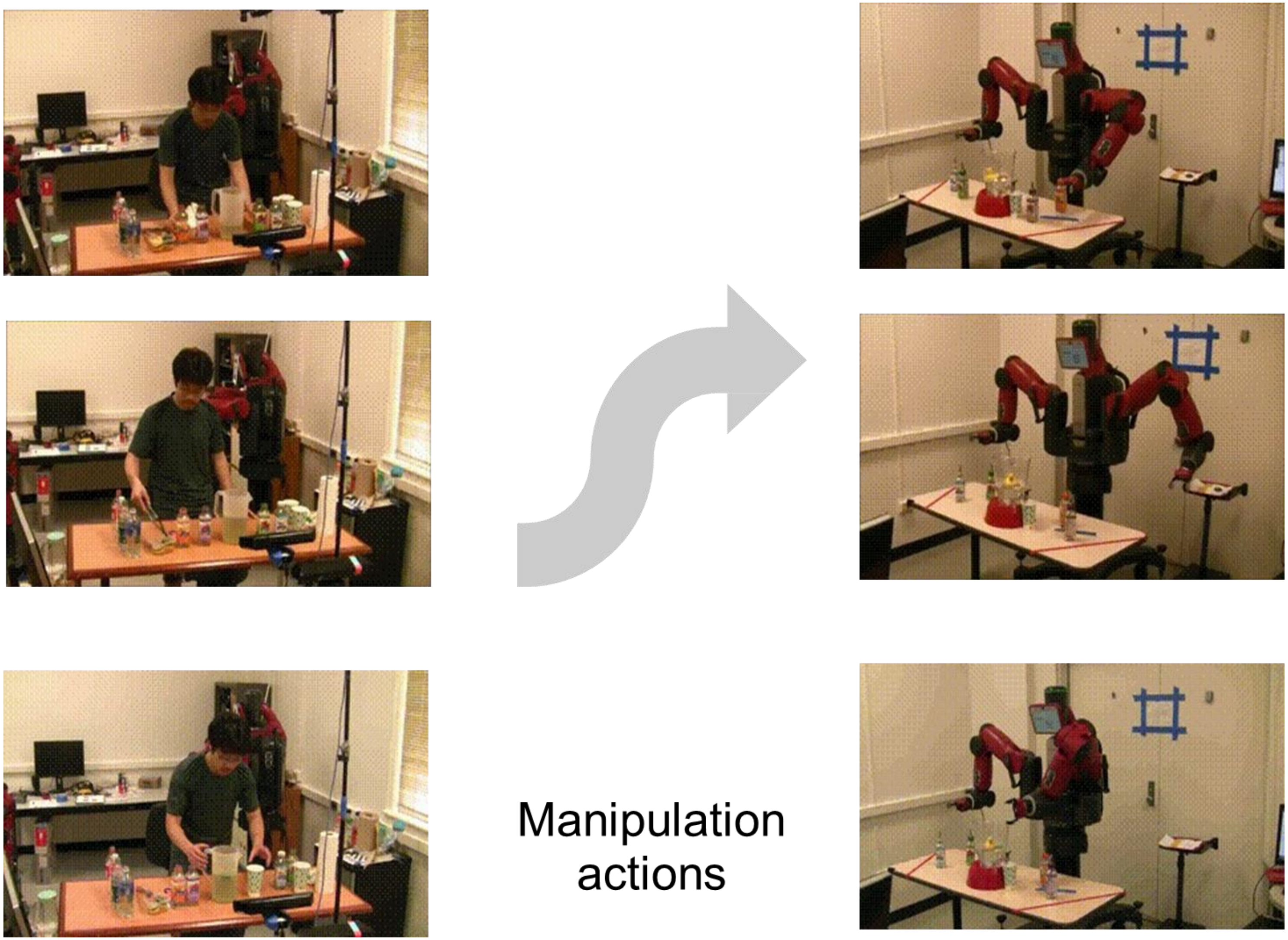
Humans utilize an elaborate attention system – need something similar, multimodal and adaptive

Need to learn, reason and communicate about objects, tools, actions

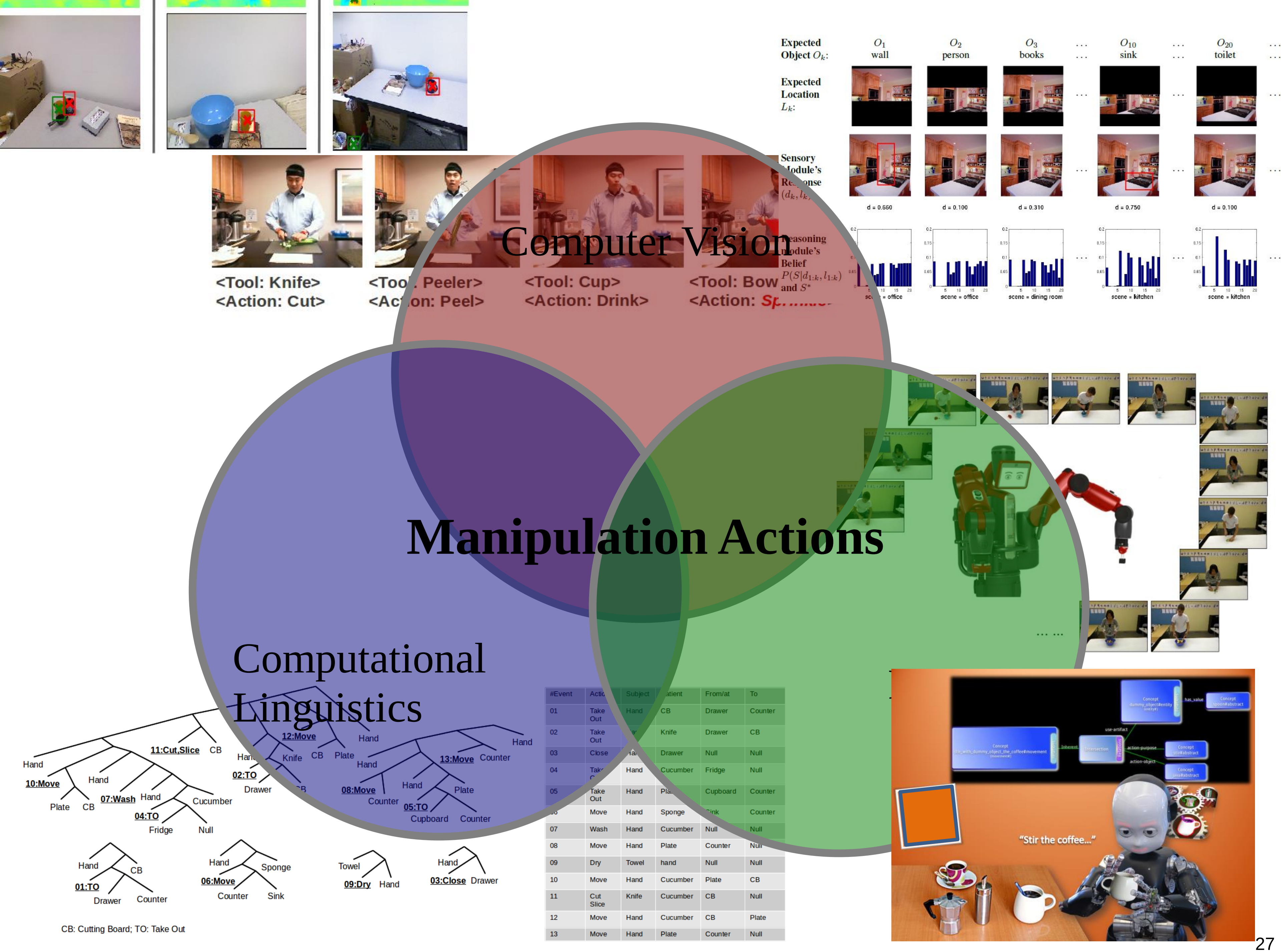
Key principle of our approach: Task-driven integration of perception, control and language

Also essential for human-robot collaboration

Focus: Manipulation Actions



Manipulation actions



Computer Vision

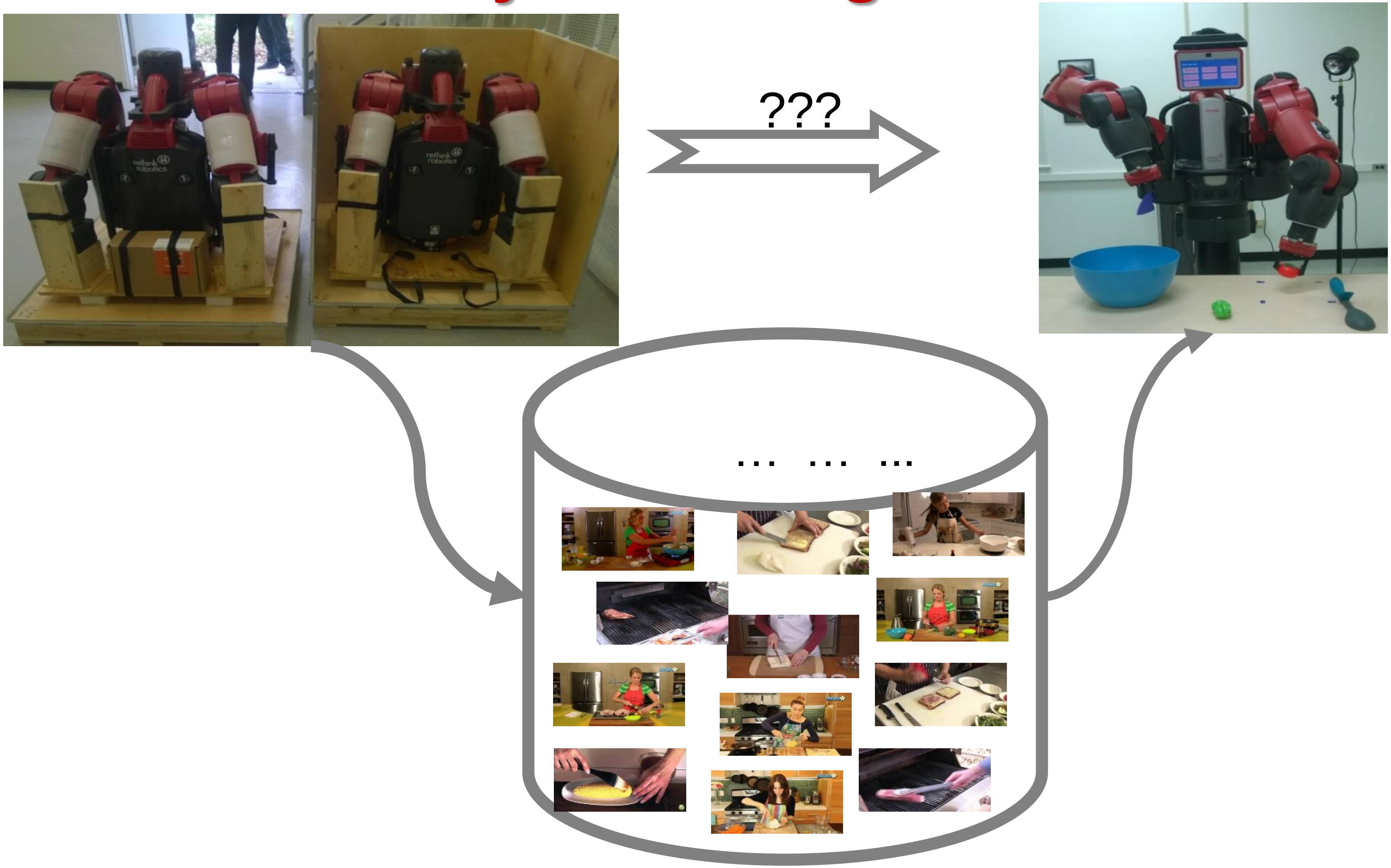
Manipulation Actions

Computational Linguistics

CB: Cutting Board; TO: Take Out

#Event	Actio	Subject	atient	From/at	To
01	Take Out	Hand	CB	Drawer	Counter
02	Take Out	Ha	Knife	Drawer	CB
03	Close	Ha	Drawer	Null	Null
04	Take O	Hand	Cucumber	Fridge	Null
05	Take Out	Hand	Pla	Cupboard	Counter
06	Move	Hand	Sponge	Sink	Counter
07	Wash	Hand	Cucumber	Null	Null
08	Move	Hand	Plate	Counter	Null
09	Dry	Towel	hand	Null	Null
10	Move	Hand	Cucumber	Plate	CB
11	Cut Slice	Knife	Cucumber	CB	Null
12	Move	Hand	Cucumber	CB	Plate
13	Move	Hand	Plate	Counter	Null

Example 2: Robot Learning Manipulation Action Plans by "Watching" on-line Videos



Example 1 : Learning Hand Movements from Markerless Demonstrations for Humanoid Tasks

- What tasks?
- How to learn tasks?
- Different situations?

Our Approach

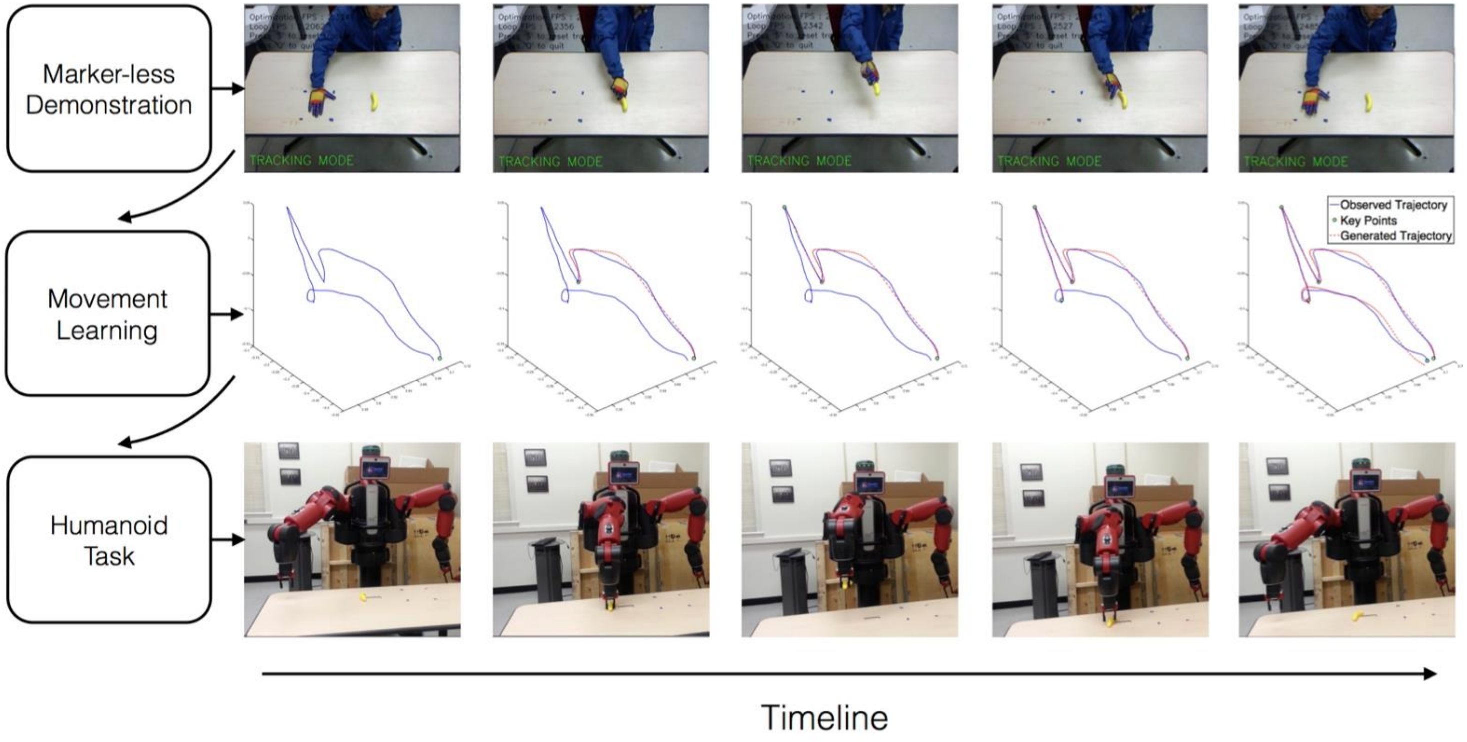
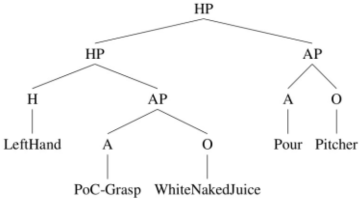


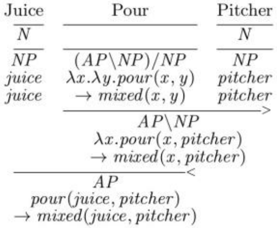
Fig. 1. Overview of learning hand movements for humanoid tasks. Placing task is an example shown here, and the drawing on hand in demonstration video is indicating hand tracker.

Robotic Execution

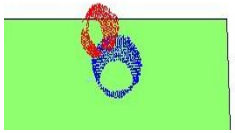
ongoing

Action Sequencing





Visual Grounding



Sensory Input

From Logic/Semantics, to Timed Automata, to Action Execution

Must link:

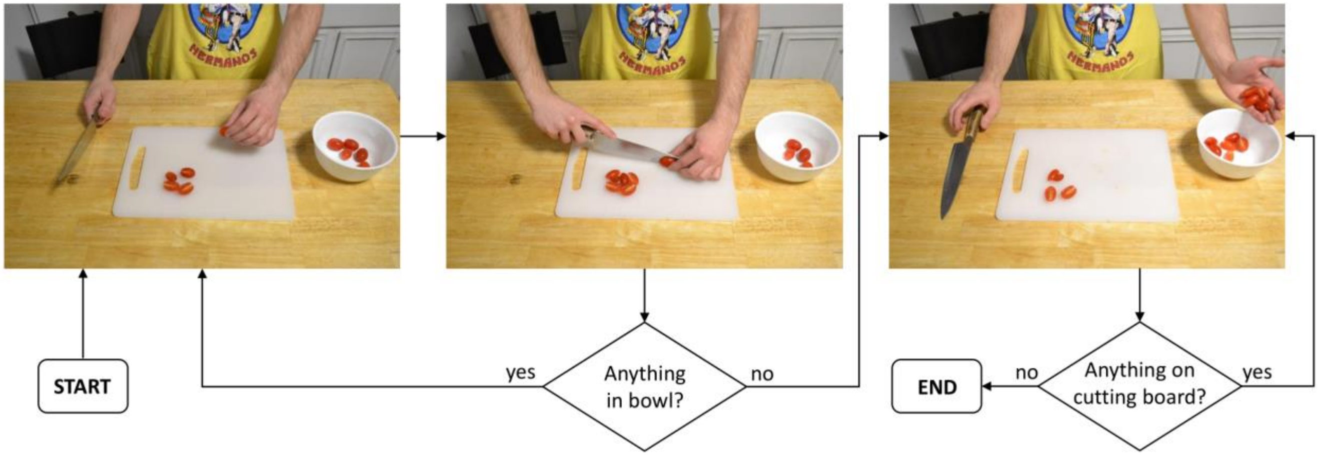
- Abstract logical/semantic description of task
- Timed automata representation of actions in a composable manner
- Taking into consideration own kinematics constraints (embodiment)

Can this be done in a principled, automatic, repeatable, verifiable manner?

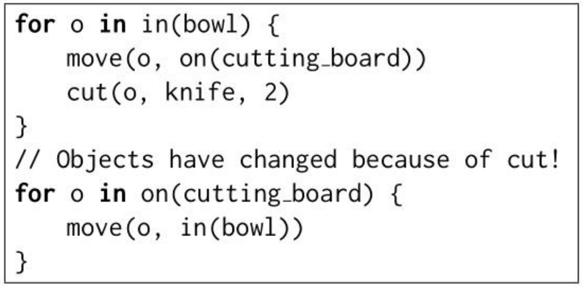
Challenges: Role and form of learning, fast execution, role of task description and performance metrics, tolerance and uncertainty models

Programming Language for Human Action

A motivating example



(a)



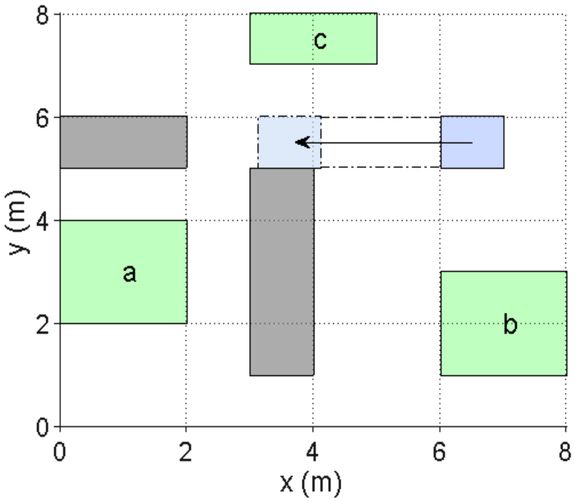
```
for o in in(bowl) {
    move(o, on(cutting_board))
    cut(o, knife, 2)
}
// Objects have changed because of cut!
for o in on(cutting_board) {
    move(o, in(bowl))
}
```

(b)

A simple action and its source code

Motion Planning with Temporal Constraints

- Q: How to generate trajectory/path based on temporal specifications such as ordering between actions, repetition of tasks, safety of the motions?
- State of art: motion planning with temporal constraints without duration, such as Linear Temporal Logic (LTL).
- We have proposed two methods for timed temporal logics, such as Metric Temporal Logic(MTL) for motion planning problem:
  - An optimization based method
  - A timed-automata based method



Always visiting area a,b,c and stay there for at least 2s. Always avoiding obstacles

Robotic Motion Planning Problem

Given: A dynamic workspace (environment),

A **time constrained task (φ)**,

A cost function.

Objective: Find the suitable control input such that the robot completes the **given task** and **minimizes** the cost function.

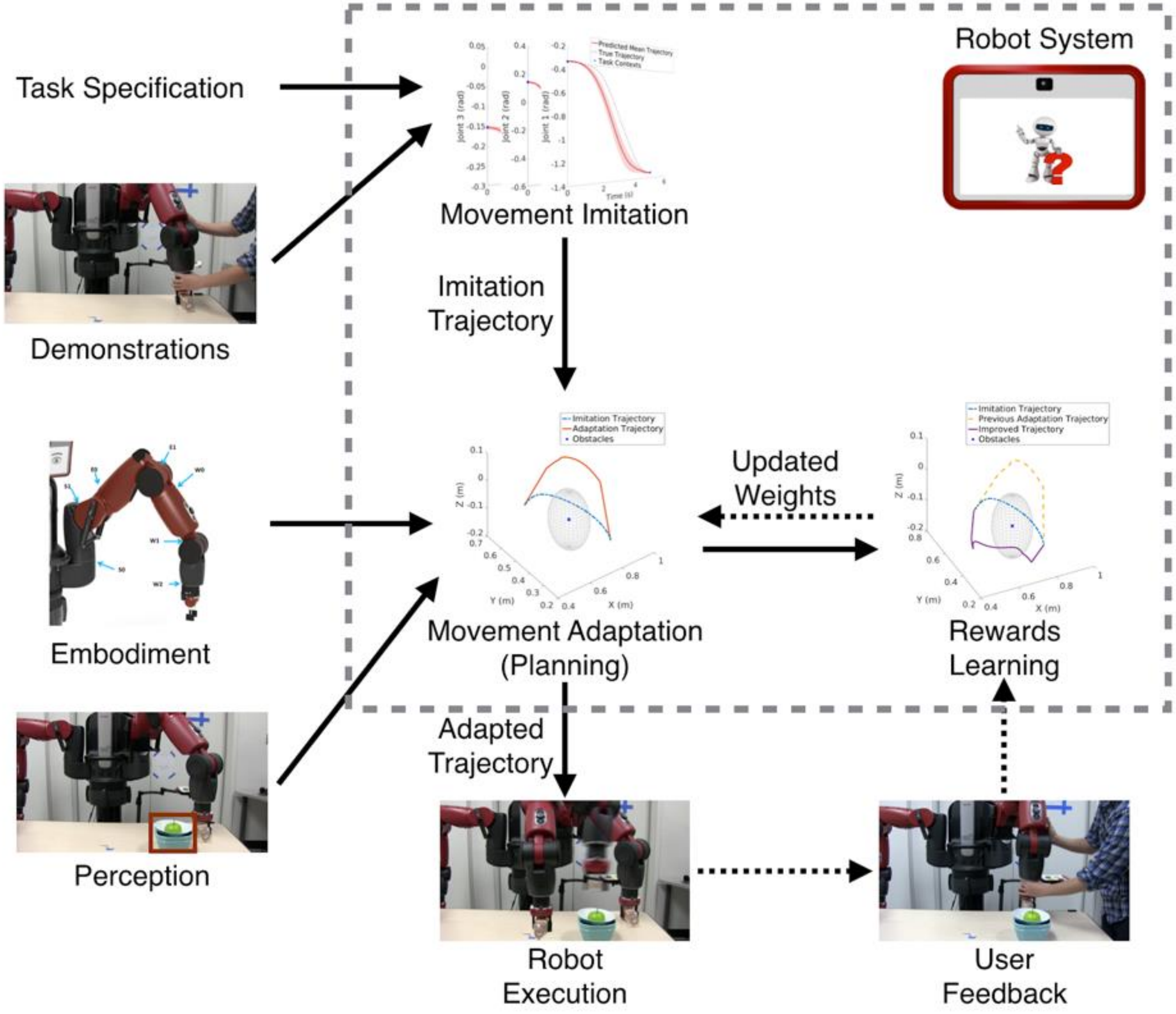
Constraints: Avoiding collisions with all **static and moving obstacles** in the workspace.

Challenges/Innovations: metric temporal logic, finite automata specs, uncertainties with mixed logical/numerical representations, automatic verification, bridge the gap between action grammars and motion planning/controls independent of learning environment and platform execution

Learning to Plan Manipulation Task Execution in New Environments

- **Learn** manipulator trajectory from demonstrations
- **Adapt** manipulator trajectory through planning with new constraints
- **Learn preferences** to adapt movement through feedback

Proposed System



Robot System

Task Specification

Demonstrations

Movement Imitation

Imitation Trajectory

Embodiment

Perception

Movement Adaptation (Planning)

Updated Weights

Rewards Learning

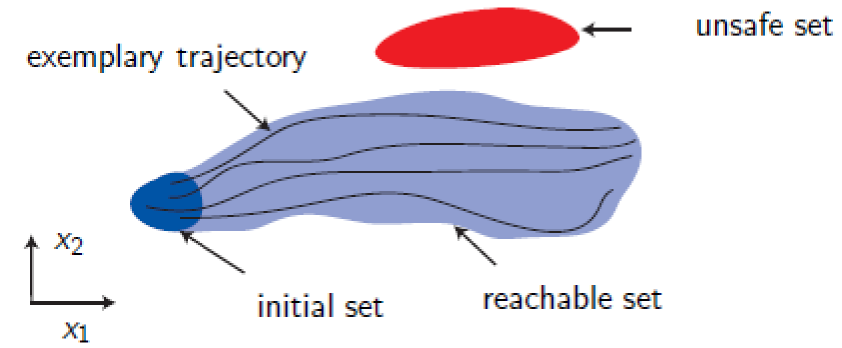
Adapted Trajectory

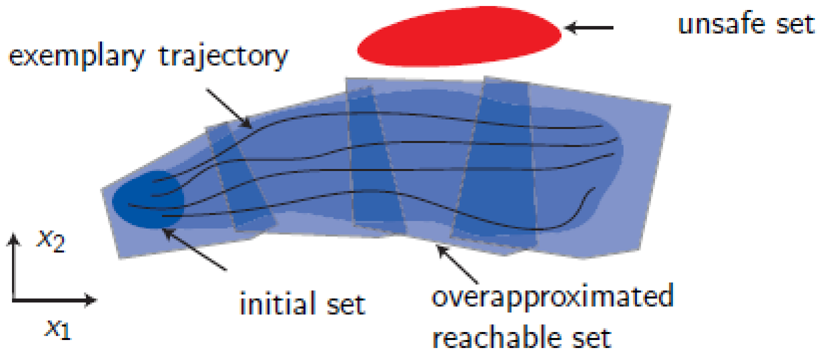
Robot Execution

User Feedback

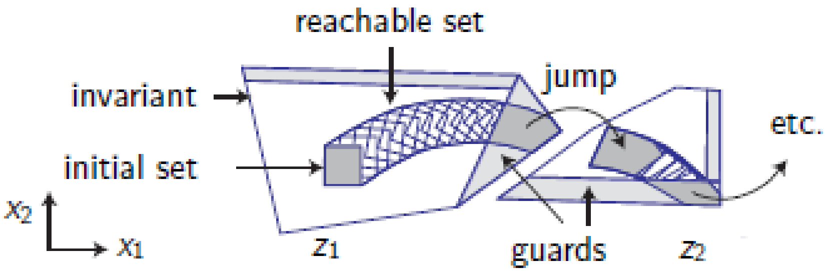
Safety & Trust in Human-Robot Teams : Integrating Logic and Set-valued Analytics

- Space-time reachability analysis (now real time)

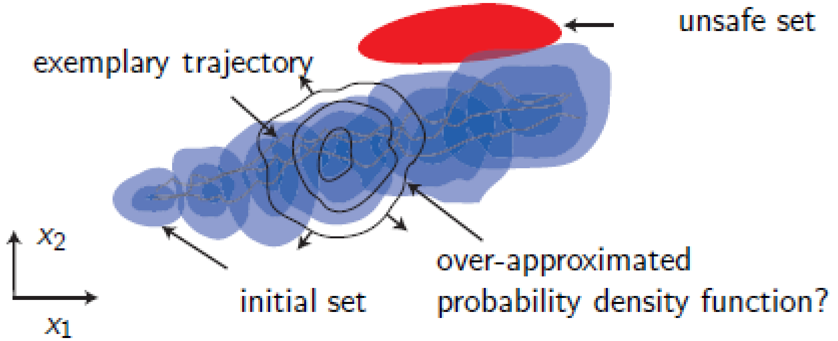




Hybrid systems



Stochastic safety systems



- Translate these to analytics: model checking, contracts, theorem proving, set valued -- Trust values? Metrics? Timed Languages?
- Roles? Role-based trust management?

Collision Avoidance via Reachable Sets

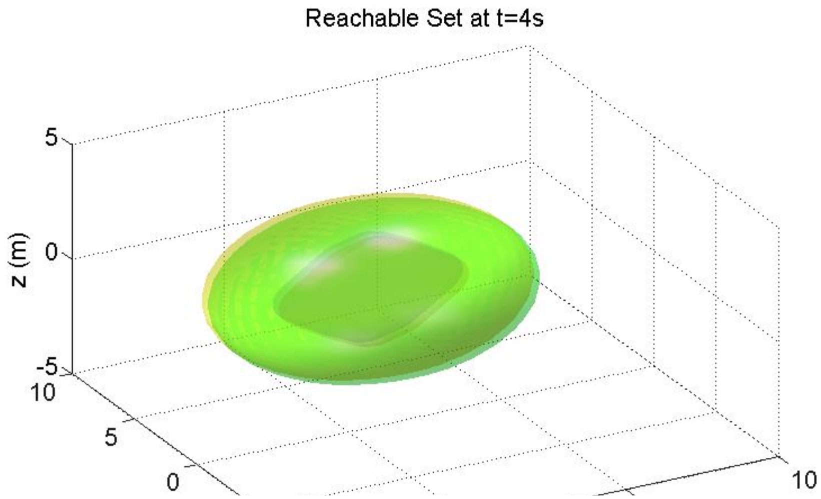
- We propose to use reachable set for collision avoidance
  - Reachable set of a dynamics is defined as set of states reachable from a bounded initial set, a control set and a disturbance set.
  - The control sets are then synthesized collaboratively so that the reachable sets of the UAVs have no intersection.
  - Existing studies in reachability literature exam the problem in a game theoretical setup such that other UAVs are treated as adversary. [I. Mitchell etc 2005] Commonly the collision avoidance is collaborative.
  - Efficient reachable set computation normally uses convex approximations such as ellipsoids [A. B. Kurzhansk 2000] and polytopes.

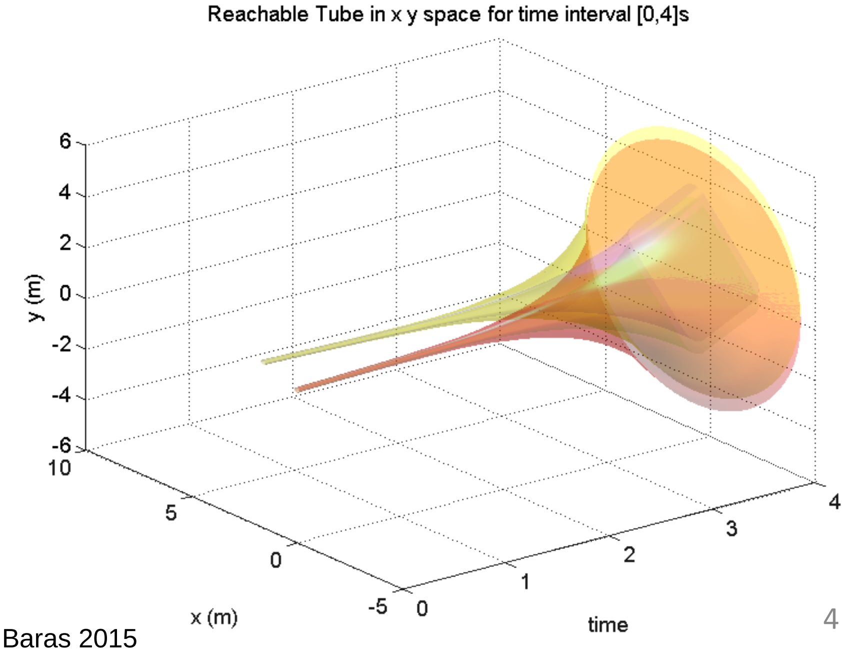
Collision Avoidance Problem

- We seek a control set design for aircraft A and B such that by using more constrained control sets than their initial ones, collision avoidance between sets are guaranteed.
- Decompose the problem to two parts
  - First we seek a tighter control constraint set for aircraft B such that the reachable set are far away from that of aircraft A but at the same time the control set of B is still large enough.
  - At the second phase we seek a safe reachable tube for aircraft A so that the reachable tube will be apart from the reachable tube of aircraft B for at least the required separation.

Initial Reachable Set and Tube

- The top plot shows the reachable set of x y z location at time of collision. The two sets are overlapping.
- The darker colored ones in the center is the inner approximation of reachable set.
- The reachable tube of x, y position only in the bottom plot shows same idea.

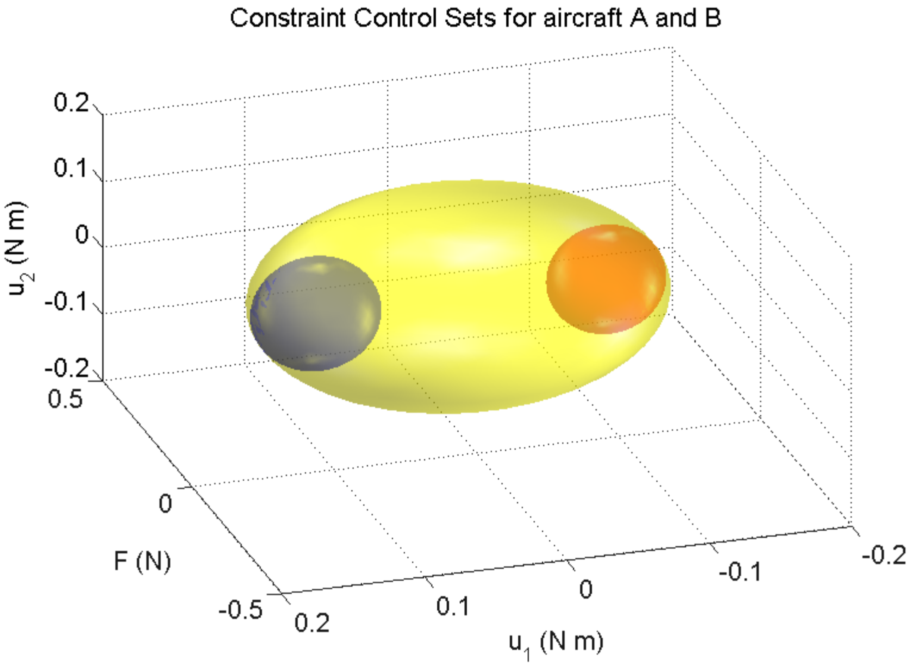


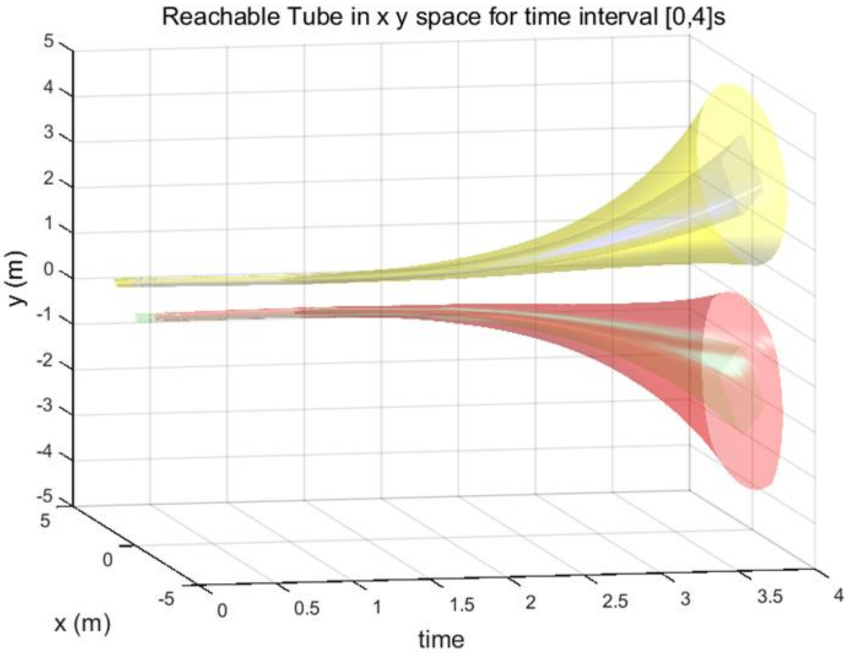


Copyright © John S. Baras 2015

Collision Avoidance Control Set Synthesis I

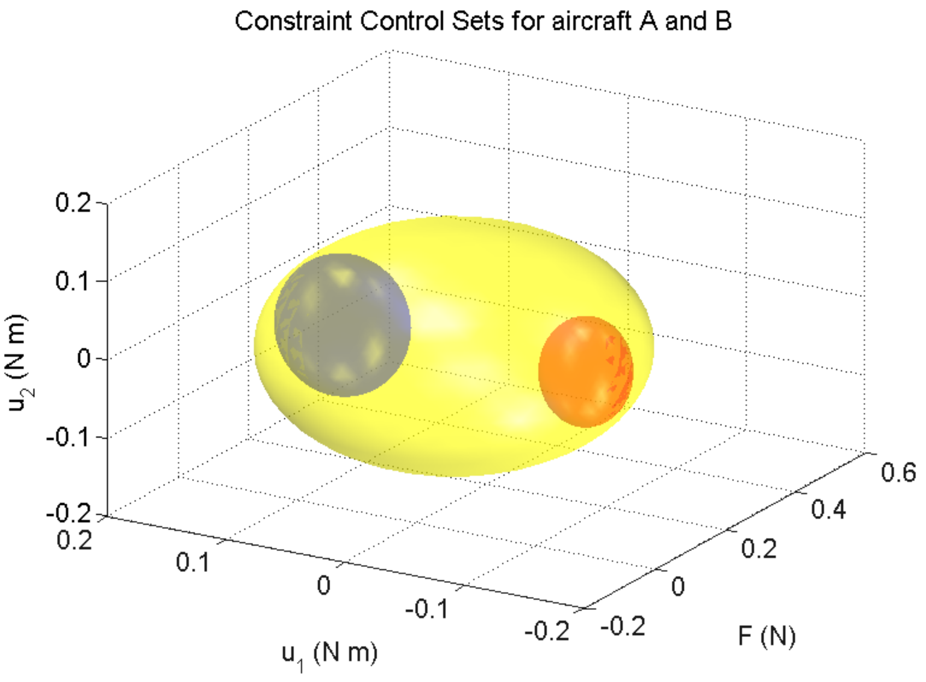
- If both UAVs have same priority, by tuning the scalarization factor, one can obtain control sets of similar size on the left.
- The reachable tube can be then visualized as the right figure.

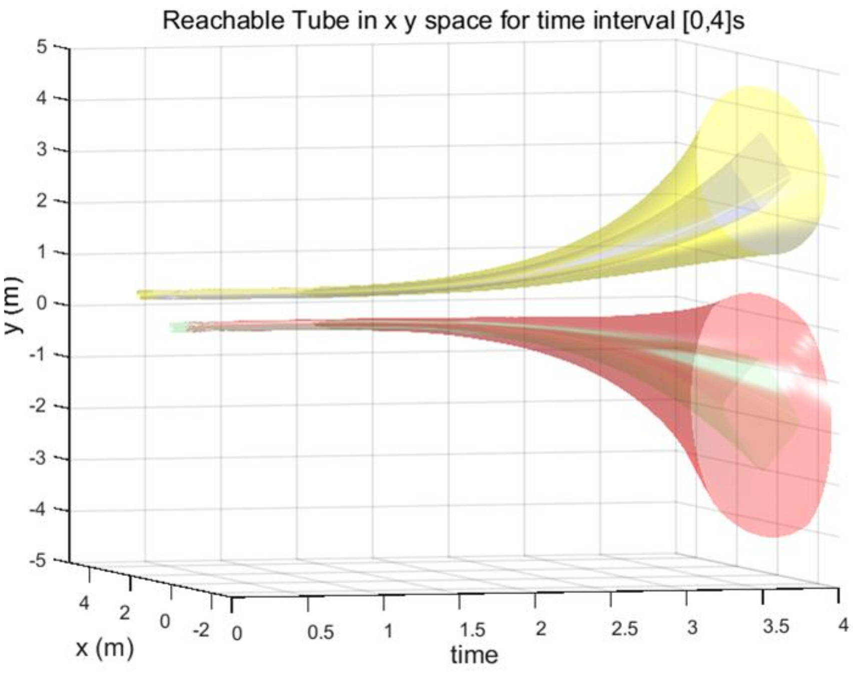

Constraint Control Sets for aircraft A and B


Reachable Tube in x y space for time interval [0,4]s

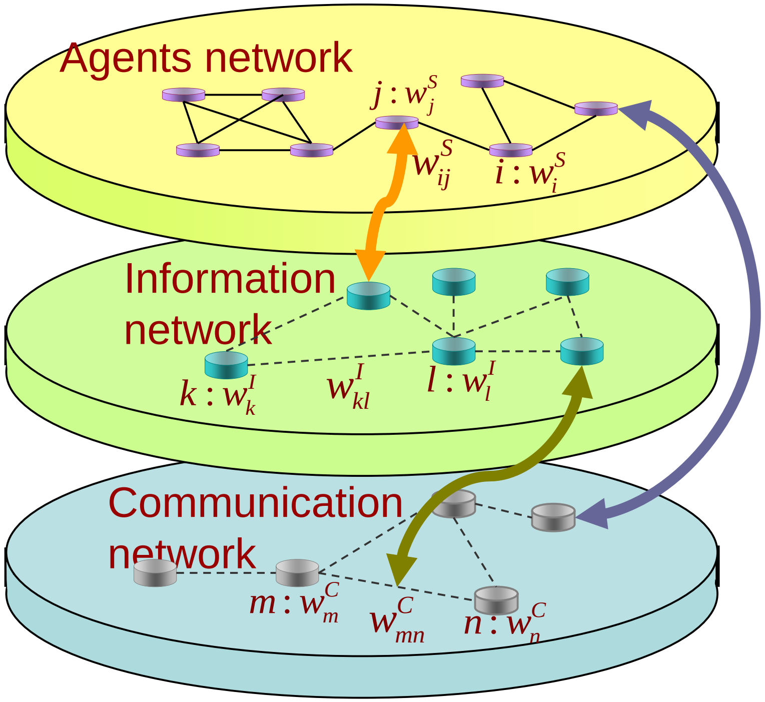
Collision Avoidance
Control Set Synthesis II

- If one of the UAVs has higher priority, it can have larger control set, so that it maintains more freedom comparing to the other one.
- The reachable tube can be then visualized as the one on the right





Multiple Interacting Dynamic Multigraphs



- Multiple Interacting Multigraphs
  - *Nodes*: agents, individuals, groups
  - Directed graphs
  - *Links*: ties, relationships
  - *Weights on links* : value, strength
  - *Weights on nodes* : importance
- **Real-life problems: Dynamic time varying graphs, relations, weights**
- **Effects of connectivity topologies**
- **Taxonomies of multigraphs involved -- performance**
  - ***Collaboration multigraph***: who collaborates with whom and when.
  - ***Communication multigraph***: who communicates with whom and when
- Need for **different probability models**
- **Future: Dynamic goal oriented planning, re-planning**

Constrained Coalitional Games

- The nodes **gain** from collaborating
- But collaboration has **costs** (e.g. **communications)**
- **Trade-off: gain from collaboration *vs* cost of collaboration**

Vector metrics involved typically

⇒ **Constrained Coalitional Games**

- **Example 1**: **Network Formation** -- Effects on Topology
- **Example 2**: **Collaborative robotics, communications**
- **Example 3**: **Web-based social networks and services**
- **Example 4**: **Groups of cancer tumor or virus cells** • • •

- **Future:**

Introduce complex behavioral models, multiple-sensory perception, Language development and efficient communications, learning from collaboration, motifs, storing and recalling patterns, multiple internal models, complexity, trust in inference and control, composite trust

SEIL
Systems Engineering & Integration Laboratory

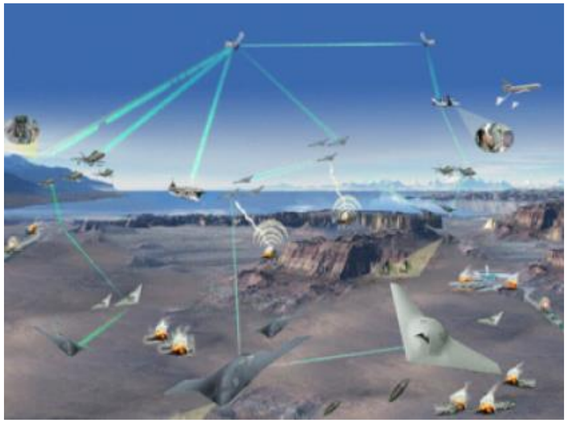
Model-Based Systems Engineering for Networked Multi-Agent Systems

The Institute for Systems Research

J. S. Baras -- baras@umd.edu

The Challenge & Need:

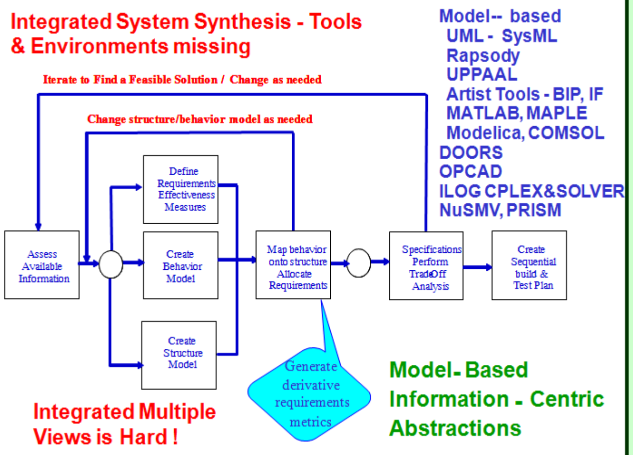
DoD Collaborative Autonomous Networked Human-Machine Systems



Heterogeneous, dynamic, multi - scale, rapid technology changes, rapid threat changes

Fig.1: MBSE process elements

Model- Based Systems Engineering



Integrated System Synthesis - Tools & Environments missing

Iterate to Find a Feasible Solution / Change as needed

Change structure/behavior model as needed

Assess Available Information

Define Requirements Effectiveness Measures

Create Behavior Model

Create Structure Model

Map behavior onto structure Allocate Requirements

Specifications Perform TradeOff Analysis

Create Sequential build & Test Plan

Generate derivative requirements metrics

Integrated Multiple Views is Hard !

Model-- based
UML - SysML
Rapsody
UPPAAL
Artist Tools - BIP, IF
MATLAB, MAPLE
Modelica, COMSOL
DOORS
OPCAD
ILOG CPLEX&SOLVER
NuSMV, PRISM

Model- Based Information - Centric Abstractions

CORE SE TOPICS

- Object Oriented modeling and beyond
- Automata, languages, design rules
- Trade-off analysis and multi-objective optimization
- Testing, validation, behaviors
- Logic programming and optimization
- Performance over time, hybrid systems
- Simulation and performance analysis

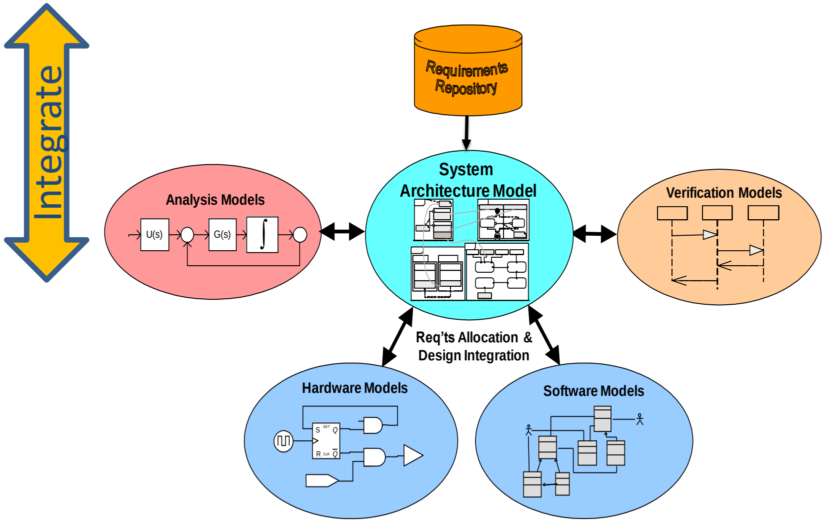


Fig. 2: Modeling and Analysis Tools Integration via **SysML** System Architecture Model

ADD & INTEGRATE

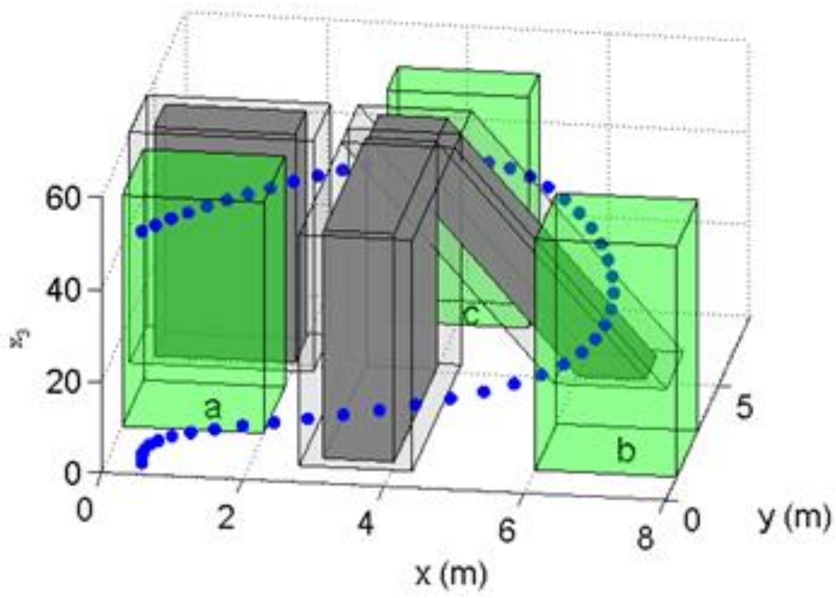
- New modeling environments
- Network models and semantics
- Reasoning, Validation and Tradeoff Tools
- Databases and Libraries of component models from all disciplines

BENEFITS

- Reduced cost and fielding time
- Modularity and re-use
- Increased agility in designing, modifying and fielding new systems

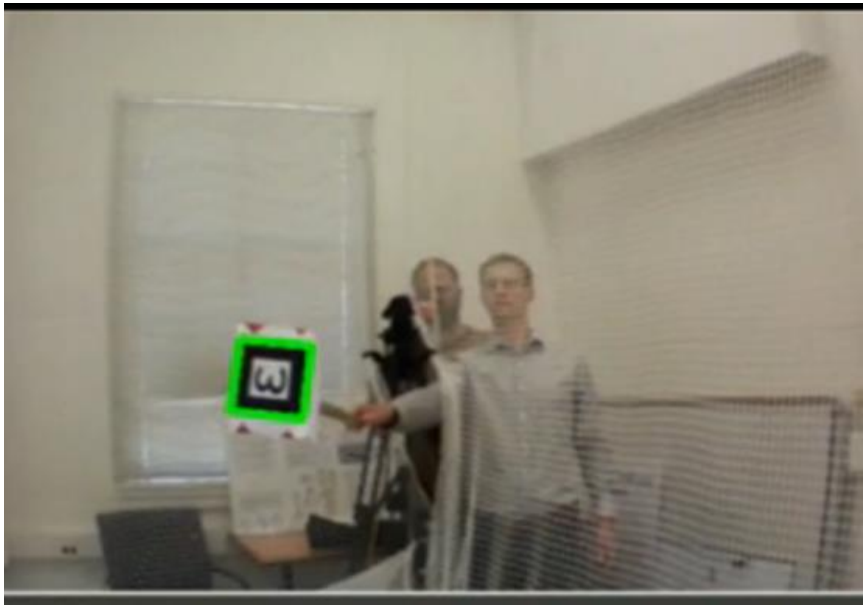
Demo 1: Synchronized Flight of Small Unmanned Aerial Systems

We follow **MBSE** (Model Based Systems Engineering) methods to create modular software



Our aircrafts use only basic onboard sensors and cameras, flying **without the aid** of motion tracking cameras that can be seen in many other experiments

Demo 2: Small Unmanned Aircraft Following a Target



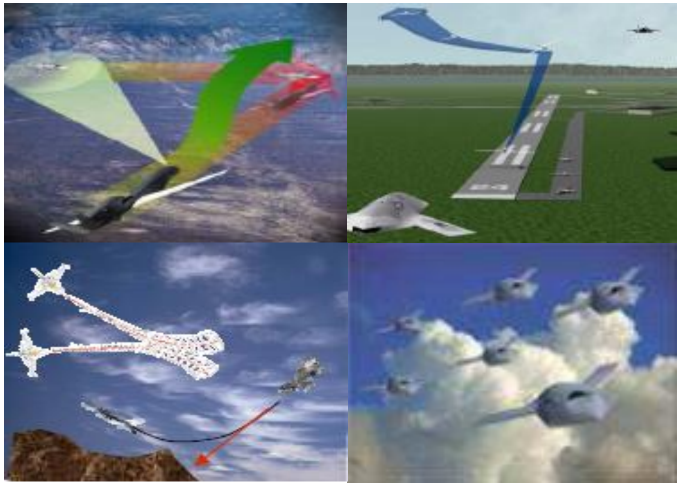
Our aircraft use a vision-based ROS package for the AR. The Drone aircraft automatically follow specific targets.

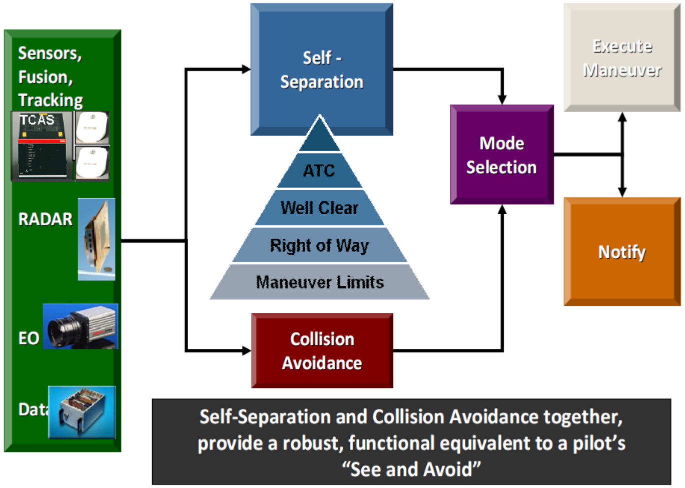
Our aircrafts use only basic onboard sensors and cameras, flying **without the aid** of motion tracking cameras that can be seen in many other experiments

Distributed Cooperative Control of UAS In Crowded Integrated Airspace with Safety

J. S. Baras -- baras@umd.edu

The Challenge & Need: Cooperative Control Sense and Avoid Technology for Autonomous UAS in Dense Environments





Sensors, Fusion, Tracking

TCAS

RADAR

EO

Data

Self - Separation

ATC

Well Clear

Right of Way

Maneuver Limits

Collision Avoidance

Mode Selection

Execute Maneuver

Notify

Self-Separation and Collision Avoidance together, provide a robust, functional equivalent to a pilot's "See and Avoid"

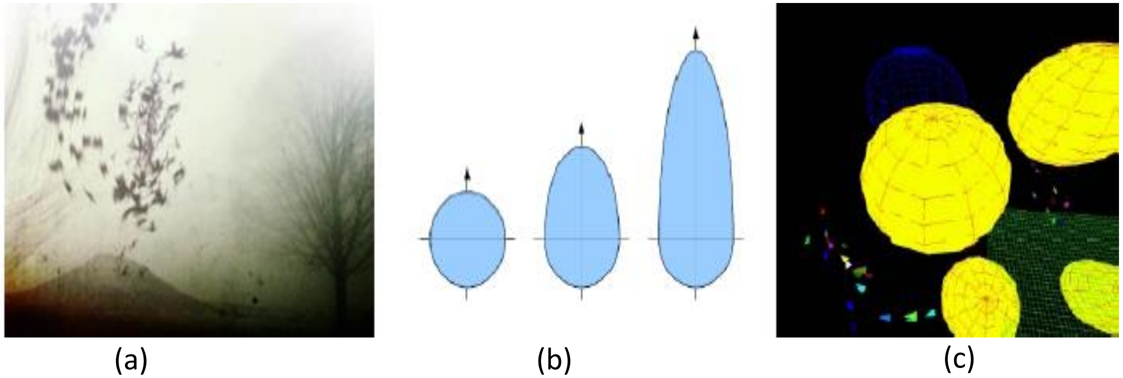


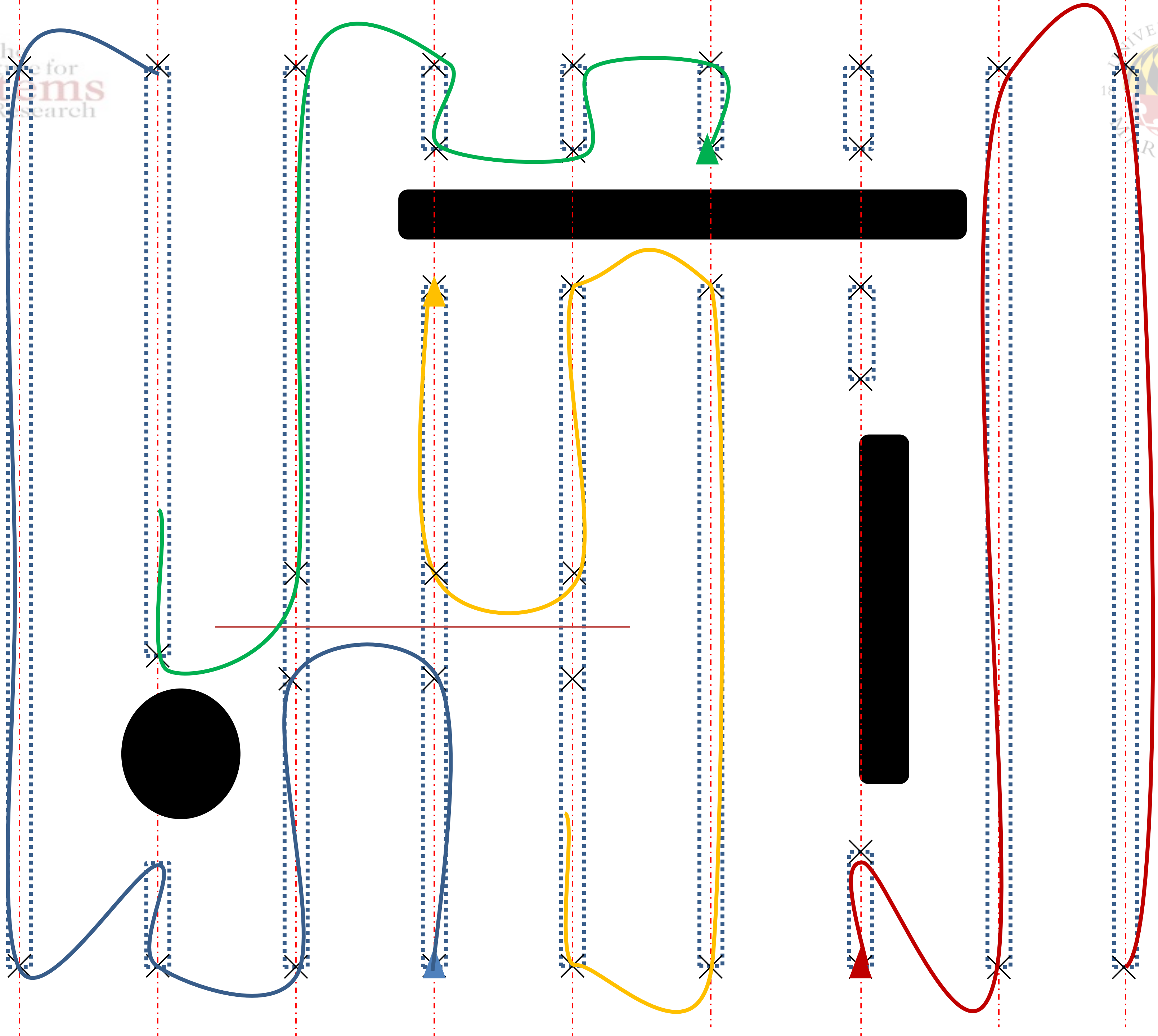
Fig.: (a) Boid animation of birds in complex environments; (b) 'bubles' of different shapes from slow to higher velocities; (c) diverse bubbles navigating obstacles to a goal

APPROACH

- Biologically inspired control (swarms, birds)
- Control theoretic analytics
- Efficient and fast computations
- Aerodynamics
- Model predictive control of hybrid automata (switched dynamical systems) including temporal logic
- Formal safety verification
- Integrated modeling, simulation, synthesis, operations tool-suite for collaborating UAS

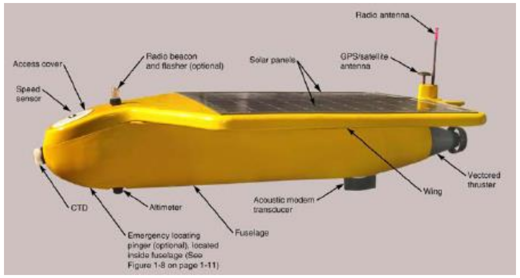
OUTCOMES / APPLICATIONS

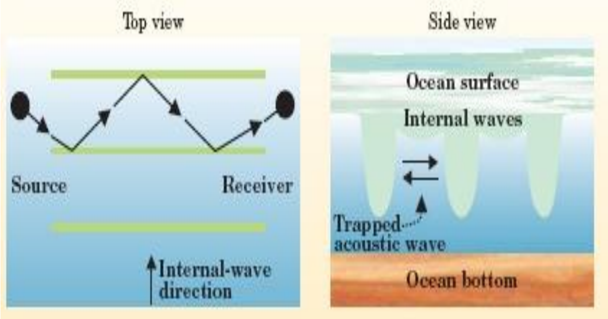
- Dynamic bubble shapes for varying safety constraints
- Guaranteed safe operation of UAS teams
- Biologically inspired high performance collaborative and safe control of UAS/UAV/UGV

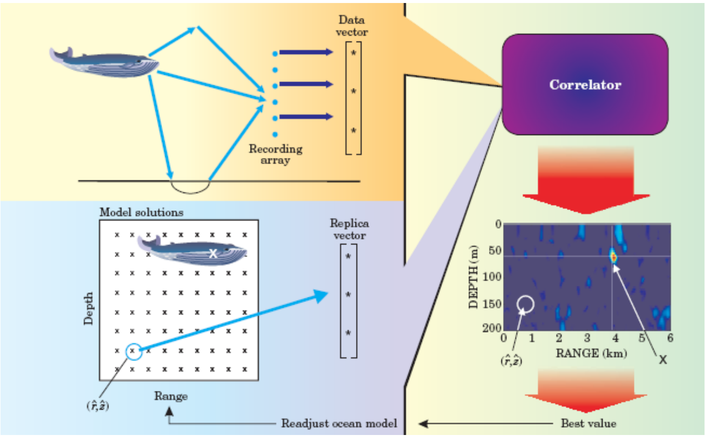


Distributed Coordination of Unmanned Underwater Vehicles (Baras)

- **Motivation**:
  - Networks of underwater vehicles for sensing, ocean mapping and exploration, surveillance
  - Cooperating heterogeneous sensing
  - Hybrid acoustic and RF communications – avoid surfacing
- **Goals**:
  - Adaptability to mission
  - New communication schemes that explore idiosyncracies of underwater channel: multiple dynamic waveguides, trapping waves, ducts, multipath. Use predictive opportunistic comms employing on-line ocean channel predictor
  - Distributed dynamic behavior-based control
- **Benefits**:
  - Dynamic insertion and removal of mission elements during execution
  - Sophisticated but energy efficient comms
  - Longer collaborative, energy efficient missions


Radio antenna
Access cover
Radio beacon and flasher (optional)
Solar panels
GPS/satellite antenna
Speed sensor
Vectored thruster
Wing
CTD
Altimeter
Acoustic modem transducer
Emergency locating pinger (optional), located inside fuselage (See Figure 1-8 on page 1-11)
Fuselage



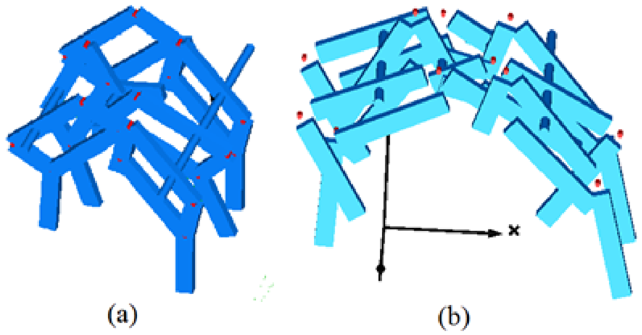


Use acoustic models to reduce comms requirements and increase efficiency

MBSE for Robotic Arms and Grippers

- Transcend areas of application: from space to micro robotics
- Include material selection in design
- Include energy sources, resilience, reliability, cost
- Include validation-verification and testing
- Use integrated SysML and Modelica environment
- Link it to tradeoff tools CPLEX and ILOG Solver
- Demonstrate reuse, traceability, change impact and management

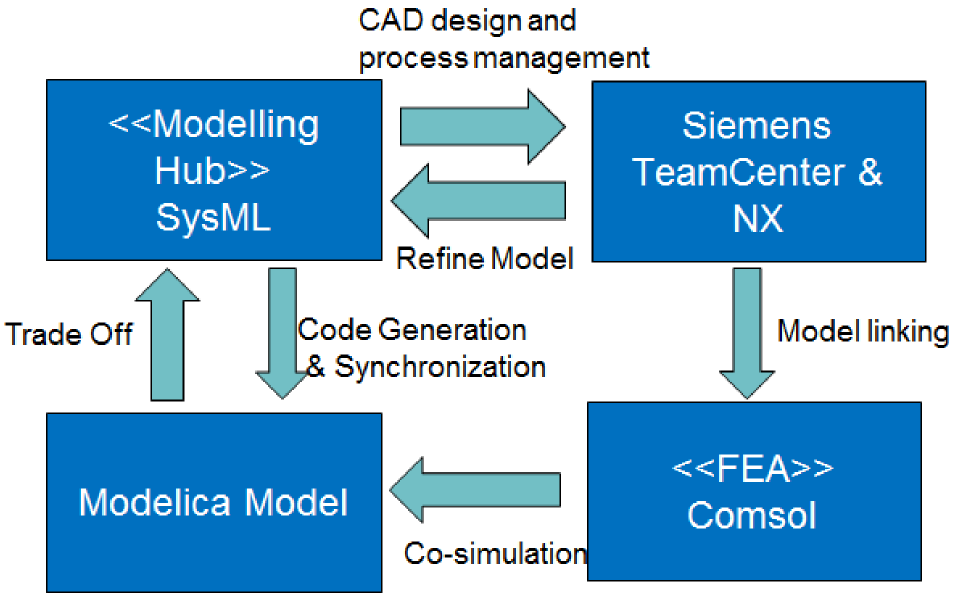
Application to Microrobotics



- Micro-robots design and manufacturing require control algorithm and physical layer (material and geometry) co-design.
- This insect-like robot is modeled in Modelica language using Differential Algebraic Equation.
- We are working on a Model-Based Systems Engineering approach to perform analysis, modeling and tradeoff for robotics and its material and control parameters.

Siemens Tools Utilization

- Design and analysis CAD model at the design phase
- Guide requirement to implementation from CAD design to physical simulation



CAD design and process management

<<Modelling Hub>> SysML

Siemens TeamCenter & NX

Refine Model

Trade Off

Code Generation & Synchronization

Model linking

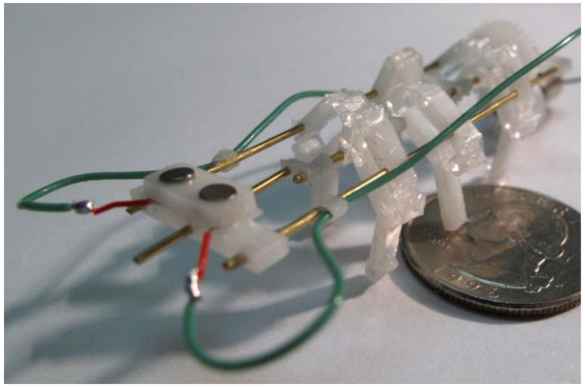
Modelica Model

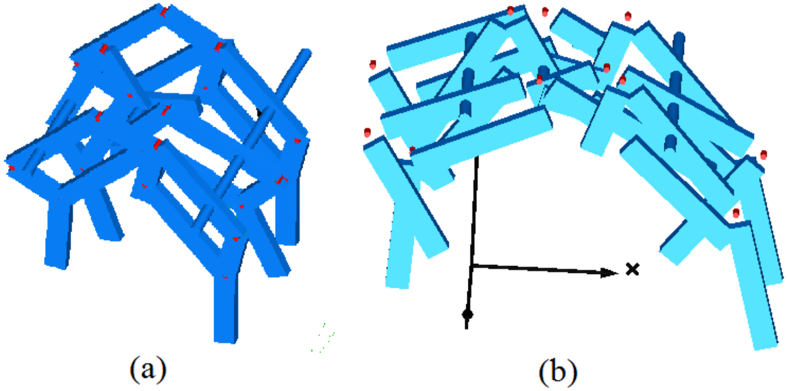
Co-simulation

<<FEA>> Comsol

Modeling

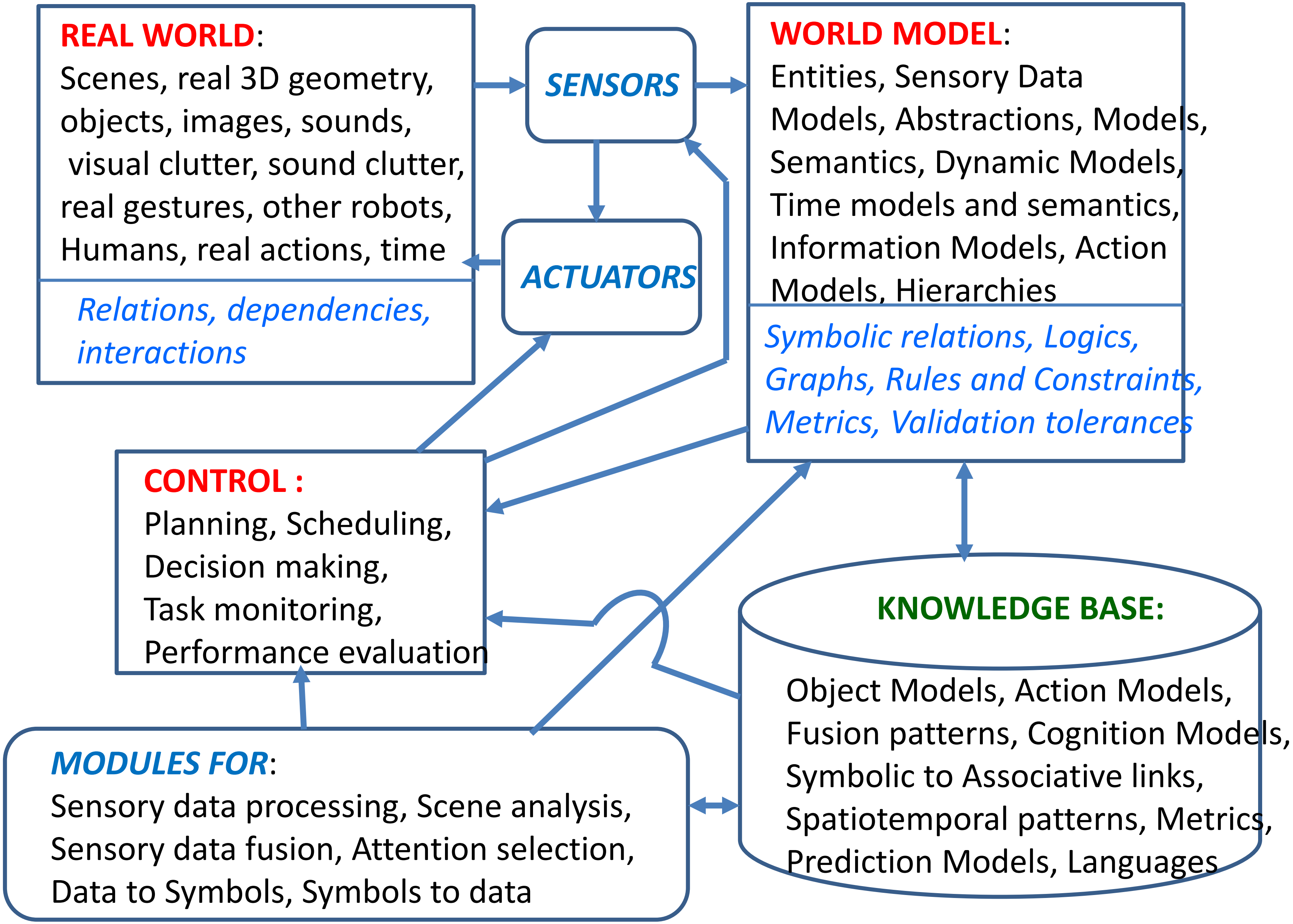
- The particular microrobots we are interested in are small insect-like robots with microfeatures, more specifically with flexible joints.





Real microrobot prototype on the left with Modelica DAE based model virtualized in Dymola on the right.
Dymola version has two distinct designs. (a) is the original design provided by D. E. Vogtmann, S. K. Gupta, and S. Bergbreiter [2012].

Sensory Perception and Cognition: Internal Models for Collaborative Autonomy



REAL WORLD:
Scenes, real 3D geometry, objects, images, sounds, visual clutter, sound clutter, real gestures, other robots, Humans, real actions, time

Relations, dependencies, interactions

SENSORS

ACTUATORS

WORLD MODEL:
Entities, Sensory Data Models, Abstractions, Models, Semantics, Dynamic Models, Time models and semantics, Information Models, Action Models, Hierarchies

Symbolic relations, Logics, Graphs, Rules and Constraints, Metrics, Validation tolerances

CONTROL :
Planning, Scheduling, Decision making, Task monitoring, Performance evaluation

KNOWLEDGE BASE:

Object Models, Action Models, Fusion patterns, Cognition Models, Symbolic to Associative links, Spatiotemporal patterns, Metrics, Prediction Models, Languages

MODULES FOR:
Sensory data processing, Scene analysis, Sensory data fusion, Attention selection, Data to Symbols, Symbols to data

CPS Architecture: Perception-Cognition and Co-Robots

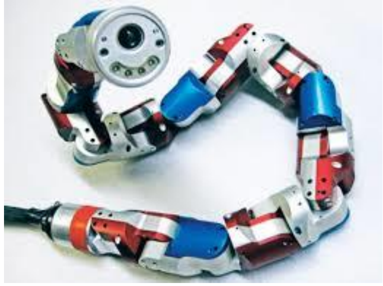
The "pressure" of "P" on "C"

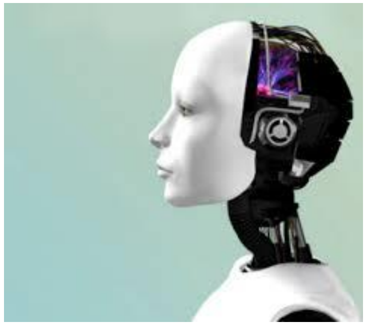
The return of analog computation?

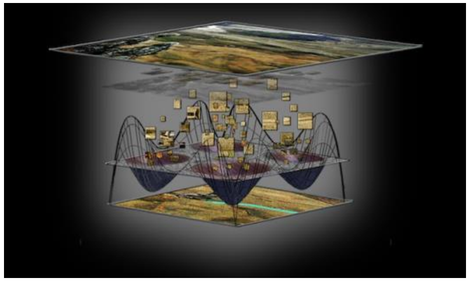
Non-von Neumann Architectures?

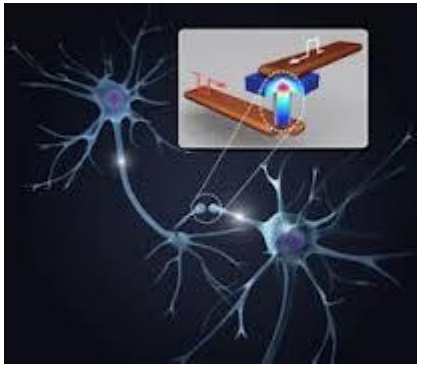
Physics of computation?

Beyond Turing?









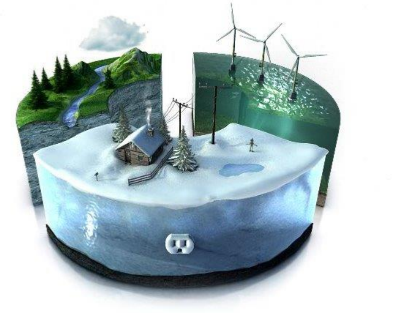
Cognition and knowledge generation from sensory perception – *communicating with humans* – *collaboration*

Not just obeying commands – *the inverse problem*

Future “Smart” Homes and Cities

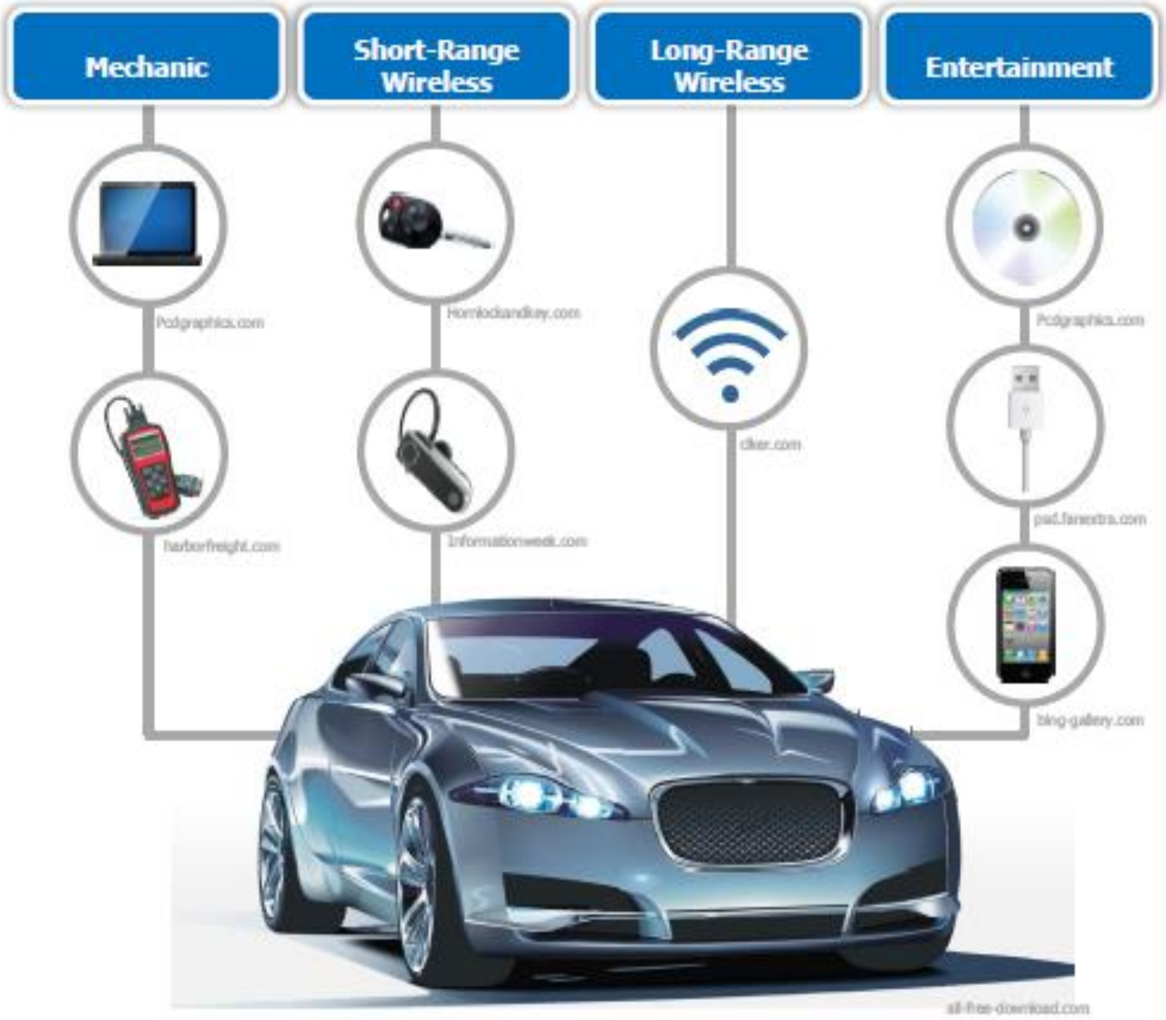
- UI for “Everything”
  - Devices with Computing Capabilities & Interfaces
- Network Communication
  - Devices Connected to Home Network

- Media: Physical to Digital
  - MP3, Netflix, Kindle eBooks, Flickr Photos
- Smart Phones
  - Universal Controller in a Smart Home



- Smart Meters & Grids
  - Demand/Response System for “Power Grid”
- Wireless Medical Devices
  - Portable & Wireless for Real-Time Monitoring

Cars are Heavily Computerized: Electronics in Cars and Vulnerabilities



<u>UW/UCSD Work:</u>

Kosher et al., IEEE Symposium on Security and Privacy, '10

- Reach CAN bus through diagnostic port

Checkoway et. al., USENIX Security, '11

- Remote attacks
- Insert virus into computer system in mechanic shop
- Bluetooth
- Telematics unit
- CD player

Physical Layer Authentication: Key Ideas and Challenges

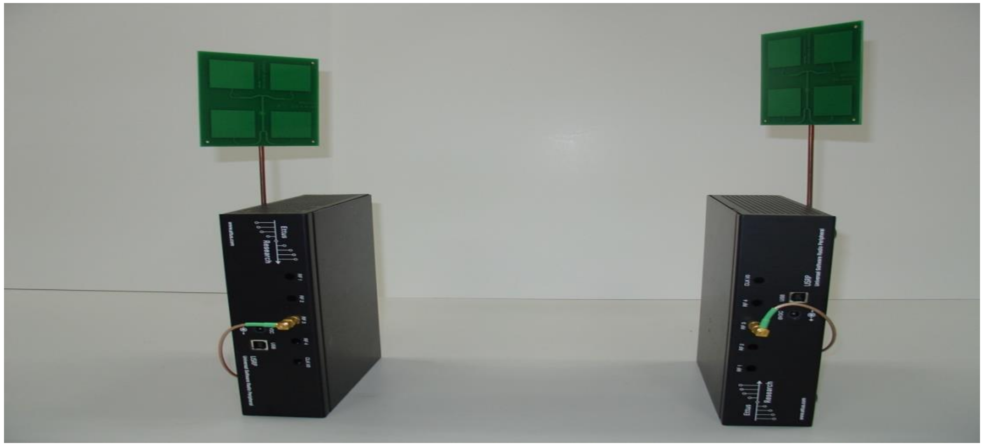
- **Exploit characteristics (a.k.a. FINGERPRINTS) of physical layer (vastly ignored todate)**
  - Waveform, RF and hardware peculiarities ⇒

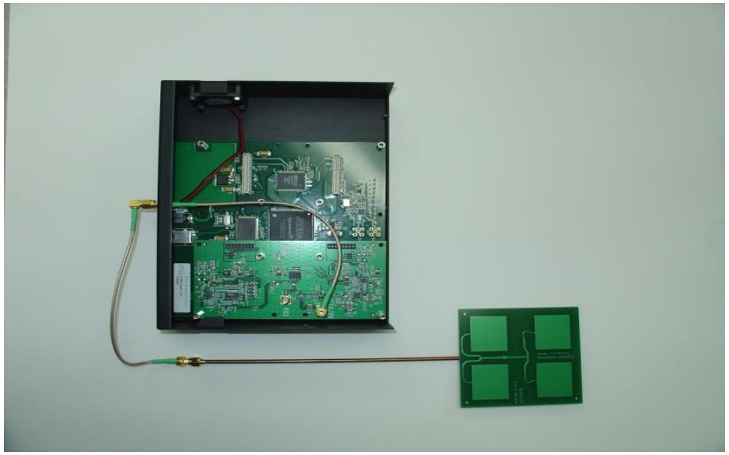
    lead to ‘unshakeable’ fingerprints
  - Embed artificial and stealthy ‘fingerprints’
  - **Authenticate the device to the network and then the user to the device** ⇒ reduces attack risk (fewer times through the net)

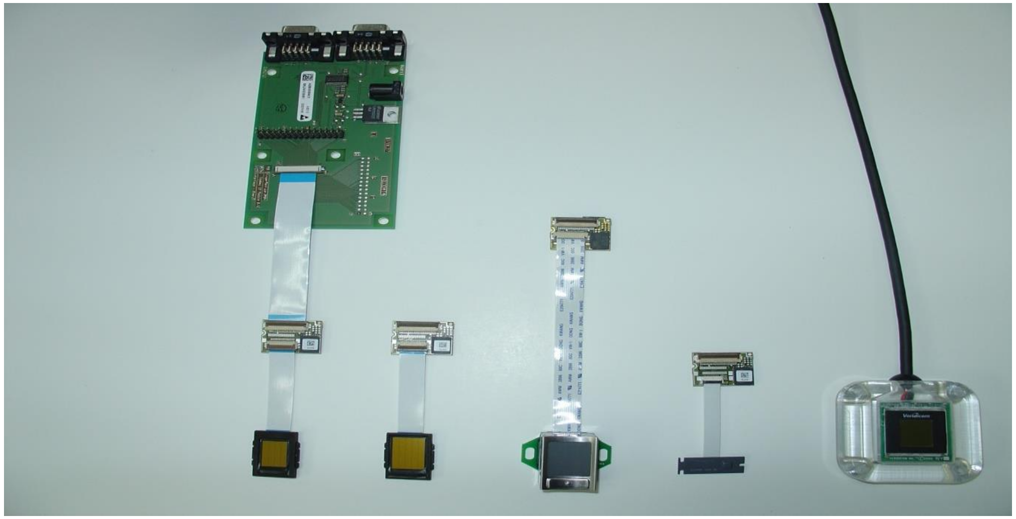
- **Distribute assurance/trust function across software and hardware (increases difficulty to attacker significantly)**
  - Trusted computing platform – architecture modifications to allow multiple sources input (including biometrics)
  - TPM – MTM chip ‘add on’ to portable devices and TCN
  - Remote software attestation

Experimental Validation

Demonstrated Very Low Power Authentication is Feasible

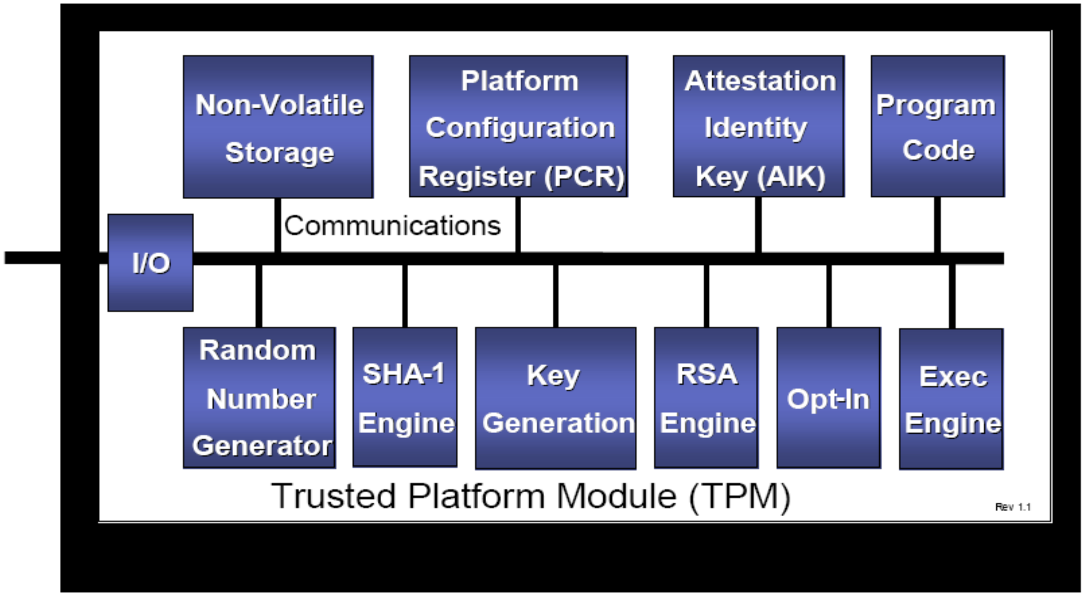






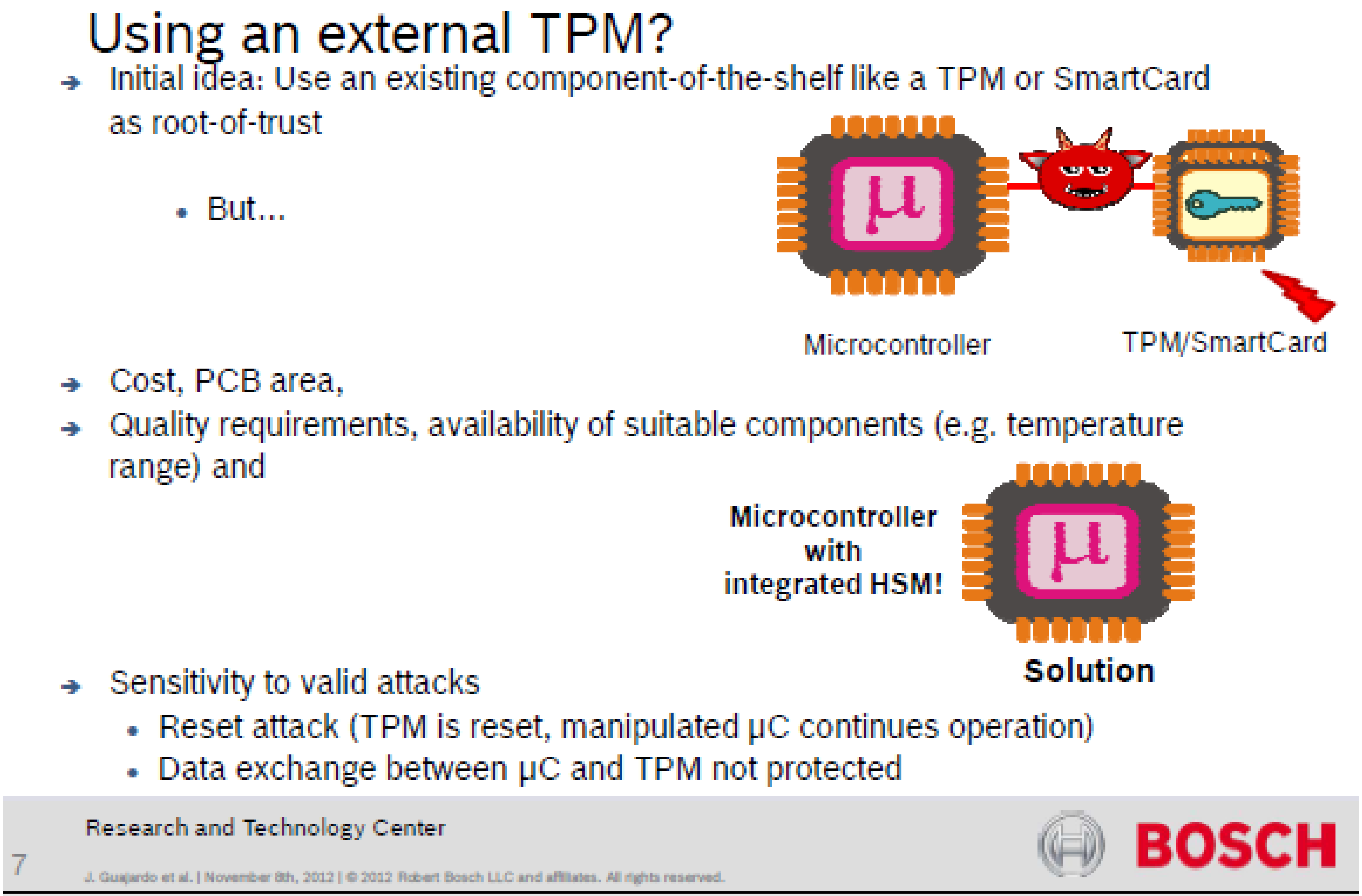
Trusted Computing

- **Trusted Platform Module technologies (TPM, MTM, TCN)**
  - A secure hardware
  - Protects the integrity and confidentiality of data with hardware support
  - Performs integrity measurements and reports them, thus attesting for the software running in the device
- **Provides a way to**
  - Understand the state of the platform,
  - Evaluate the state
  - Make a decision if the platform is appropriate for the task



Source: TCG Architecture Overview, http://www.trustedcomputinggroup.org

New Ideas: Hardware-Based Security



Using an external TPM?

- Initial idea: Use an existing component-of-the-shelf like a TPM or SmartCard as root-of-trust
    - But…

Microcontroller

TPM/SmartCard

- Cost, PCB area,
- Quality requirements, availability of suitable components (e.g. temperature range) and

Microcontroller with integrated HSM!

Solution

- Sensitivity to valid attacks
    - Reset attack (TPM is reset, manipulated µC continues operation)
    - Data exchange between µC and TPM not protected

Research and Technology Center

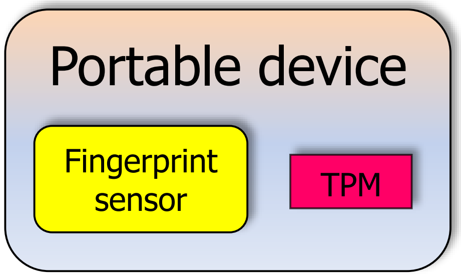
7

J. Guajardo et al. | November 8th, 2012 | © 2012 Robert Bosch LLC and affiliates. All rights reserved.

BOSCH

Security Integration on the Portable Device

- The TPM/MTM is incorporated in the device



- Biometric information
  - protected in the TPM or
  - stored in the device but encrypted with keys that are managed by the TPM
- Hardened security encourages the use of the device

- **Challenges:**

  (a) How to use informative time varying pieces of the biometric

  (b) Develop anti-spoofing techniques using the sensor signature

  (c) System integration and validation of the various fingerprints and physical layer techniques

  (d) Proof methods that security is improved – Information theoretic methods

Compositional Security and Trust in Networked Multi-Agent Systems

J. S. Baras -- baras@umd.edu

The Challenge & Need:

- Composite trust in distributed sensing and control systems (DSCS)
- Security and Trust-aware DSCS algorithms
- Universal compositional security
- Performance, security, energy, tradeoffs
- Vulnerability analysis and resilient system architectures

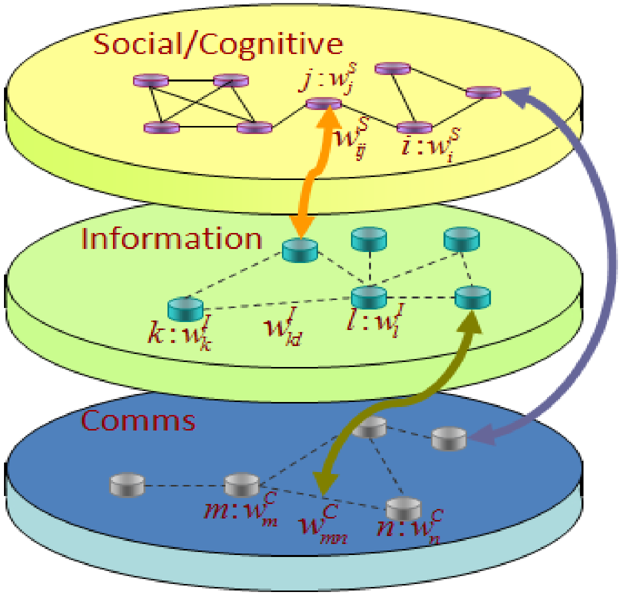


Fig.1: Social (human agent) networks supported by technological networks

APPROACH

- Security and trust aware network utility maximization
- Weighted multi-graphs
- Multiple ordered semi-rings,
- Physical layer security and authentication for universal compositional security
- Network game theory
- Distributed hybrid systems

APPLICATIONS

- Wireless communication and sensor networks
- Safety critical aircraft management systems
- Web-based social nets
- Power grid, smart grid, SCADA
- Smart buildings
- High integrity reputation and recommendation systems
- Resilience and robustness in the presence of adversaries

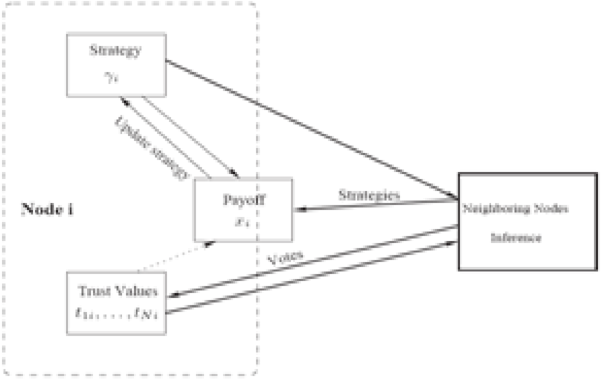


Fig. 2: Effects of trust on collaborative distributed control/operations (Baras 2005)

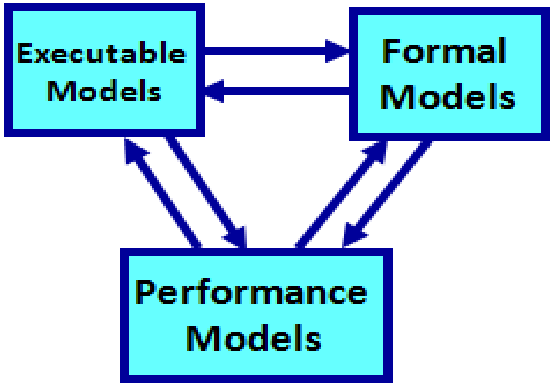
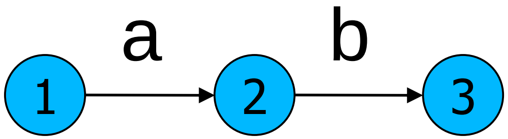


Fig. 3: Linked component-based executable, formal, performance models

Trust Semiring Properties: Partial Order

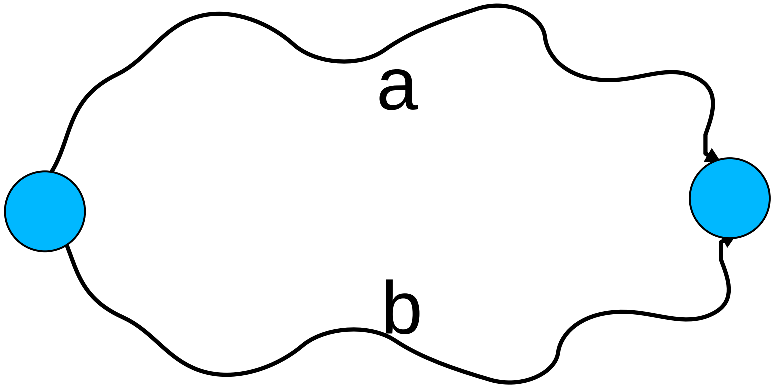
- Combined **along-a-path weight should not increase** :

$$a \otimes b \leq a, b$$



- Combined **across-paths weight should not decrease** :

$$a \oplus b \geq a, b$$



Computing Indirect Trust

- Path interpretation

$$t_{i\to j} = \bigoplus_{\text{path } p:i\to j} t^{p}_{i\to j}$$

- **Linear system interpretation**

$$t_{i\to j} = \bigoplus_{User\ k} t_{i\to k} \oplus w_{k\to j}$$

$$\vec{t}_n = W \otimes \vec{t}_{n-1} \oplus \vec{b}$$

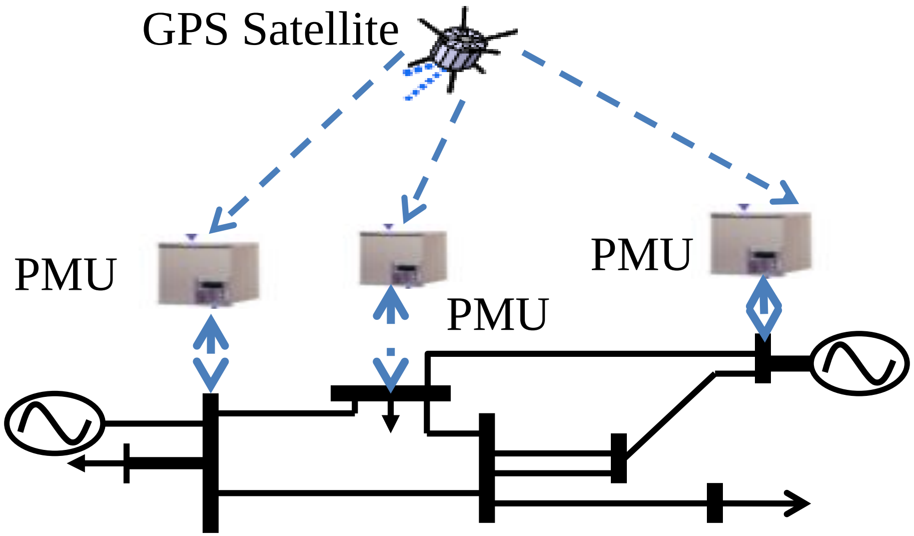
Indicator vector of pre-trusted nodes

- Treat as a **linear system**
  - We are looking for its **steady state**.

Power Grid Cyber-security

- Inter-area oscillations (modes)
  - Associated with large inter-connected power networks between clusters of generators
  - Critical in system **stability**
  - Requiring **on-line** observation and control
- Automatic estimation of modes
  - Using currents, voltages and angle differences measured by PMUs (Power Management Units) that are distributed throughout the power system

Distributed Estimation

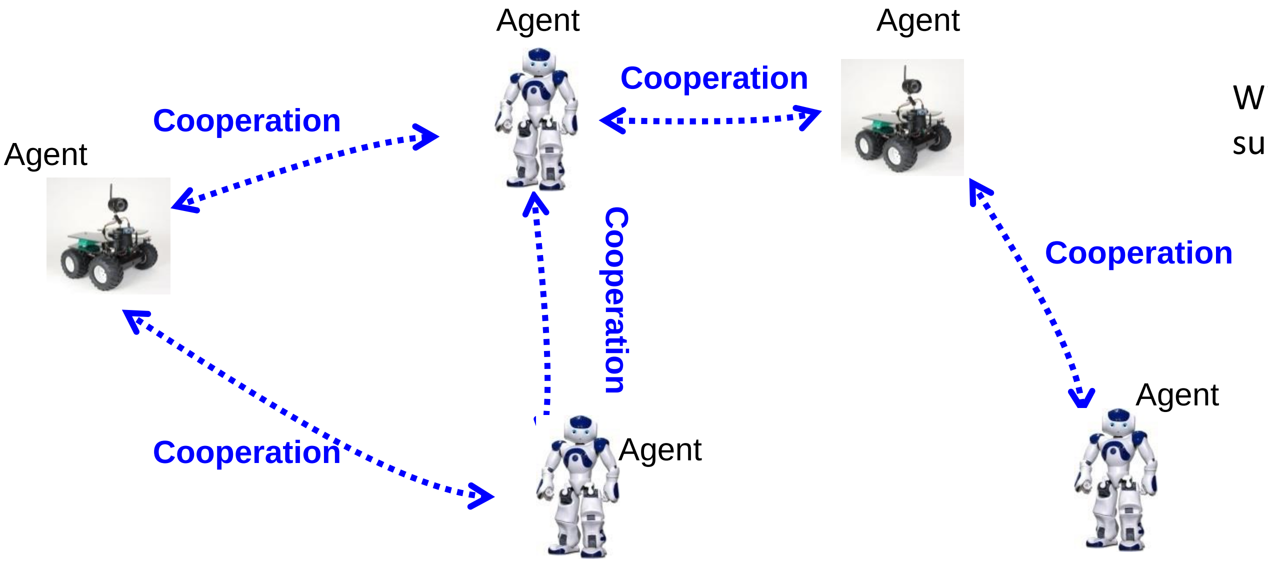


N multiple recording sites (PMUs) to measure the output signals

- To compute an accurate estimate of the state *x* (*k*), using:
  - **local measurements** $y_j(k)$;
  - information received from the PMUs in its **communication neighborhood**;
  - confidence in the information received from other PMUs provided by the **trust model**

Consensus with Adversaries

- Solve the problem via detecting adversaries in networks of low connectivity.
- We integrate a trust evaluation mechanism into our consensus algorithm, and propose a two-layer hierarchical framework.
  - Trust is established via headers (aka trusted nodes)
  - The top layer is a super-step running a **vectorized consensus algorithm**
  - The bottom layer is a sub-step executing our **parallel vectorized voting scheme**.
  - Information is exchanged between the two layers – they **collaborate**
- We demonstrate via examples solvable by our approach but not otherwise
- We also derive an upper bound on the number of adversaries that our algorithm can resist in each super-step

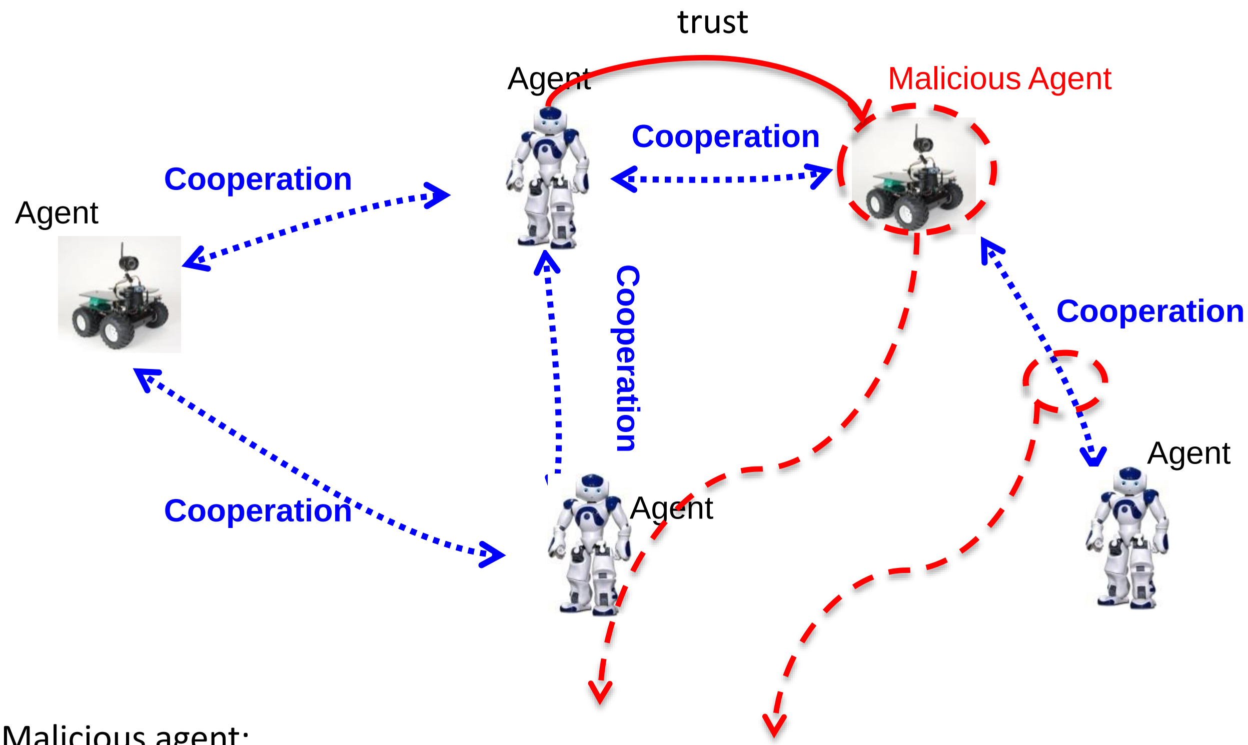


Without supervisor

- Distributed sensor fusion. Goal: all agents reach consensus on ML estimate.
- Distributed Coordination. Goal: all agents reach decision on same direction (location)

[1] Xiao, Lin, Stephen Boyd, and Sanjay Lall. "A scheme for robust distributed sensor fusion based on average consensus." Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on. IEEE, 2005.

[2] Jadbabaie, Ali, Jie Lin, and A. Stephen Morse. "Coordination of groups of mobile autonomous agents using nearest neighbor rules." Automatic Control, IEEE Transactions on 48.6 (2003): 988-1001.



Malicious agent:

- Multiparty secure computation

[4] Garay, Juan A., and Rafail Ostrovsky. "Almost-everywhere secure computation." Advances in Cryptology–EUROCRYPT 2008. Springer Berlin Heidelberg, 2008. 307-323.

- Consensus with Byzantine adversaries (System theory)

[5] Pasqualetti, Fabio, Antonio Bicchi, and Francesco Bullo. "Consensus computation in unreliable networks: A system theoretic approach." Automatic Control, IEEE Transactions on 57.1 (2012): 90-104.

Link Jam & Noise Injection:

[3] Khanafer, Ali, Behrouz Touri, and Tamer Basar. "Consensus in the presence of an adversary." 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys). 2012.

Problem Formulation (cont.)

- Without considering failures, for certain nodes, the consensus problem in distributed control can be solved by simply iteratively calculating weighted averages of nodes’ neighboring states.
  - Network of agents modeled by directed graph $G(k) = (V;E(k))$

    V denotes the set of nodes and $E(k)$ the set of edges at time k

    $N_i(k) = \{j \mid e_{ij}(k)$ Î $E(k), j$ ¹ $i\}$ set of neighbor nodes of i

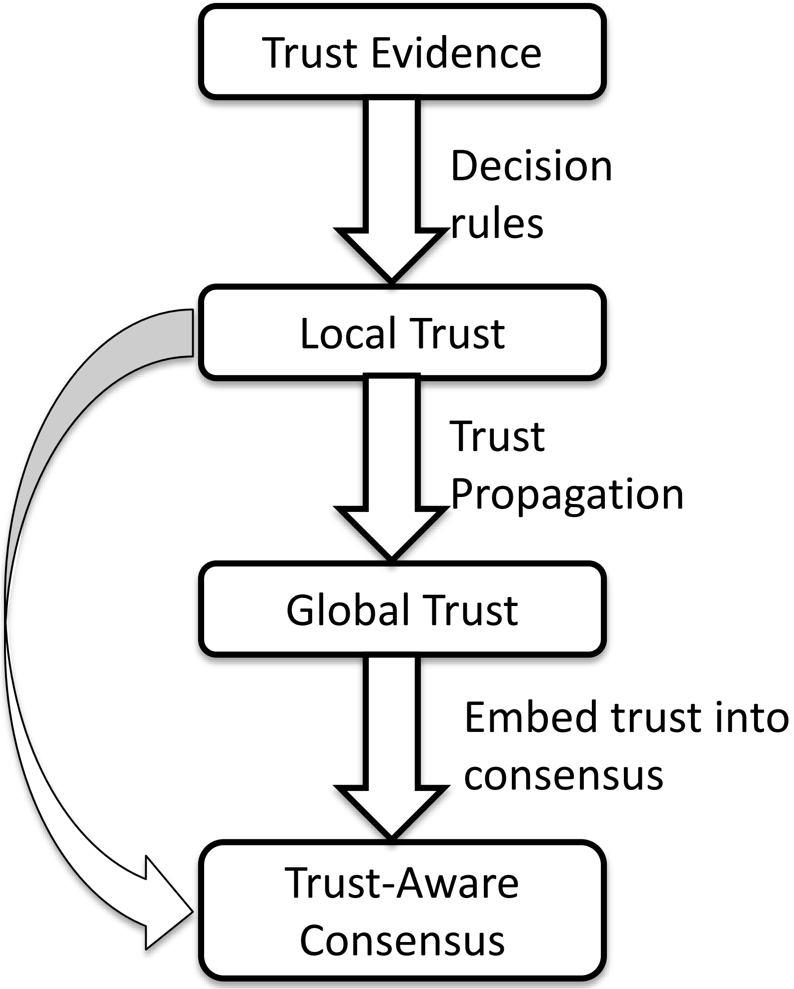
    “can hear from at time k”. $N_i^+(k) = N_i(k) \cup \{i\}$
  - Nodes’ states (decisions, beliefs, opinions, etc.) evolve in time according to the dynamics:

$$x_i(k) = \sum_{j \in N_i(k)} w_{ij}(k) x_j(k-1) + w_{ii}(k) x_i(k-1)$$

$X(k) = \{x_1(k), x_2(k), \ldots, x_N(k)\}^T$ N-dimensional vector of nodes’ states at time k.

$W(k)$ is the updating matrix (weight matrix) at time k, rows sum to 1.

Trust-Aware Consensus



Trust Evidence

Decision rules

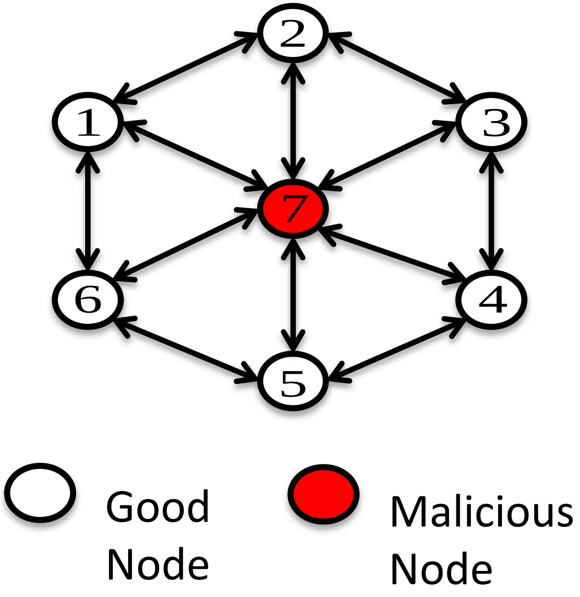
Local Trust

Trust Propagation

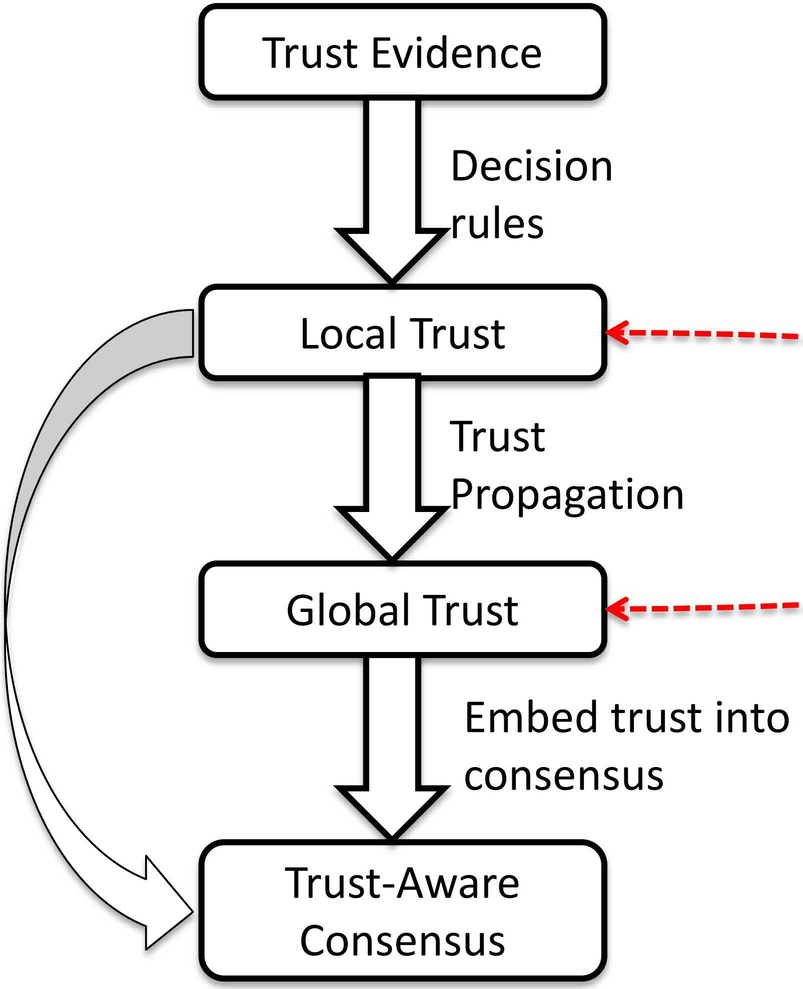
Global Trust

Embed trust into consensus

Trust-Aware Consensus



Trust-Aware Consensus

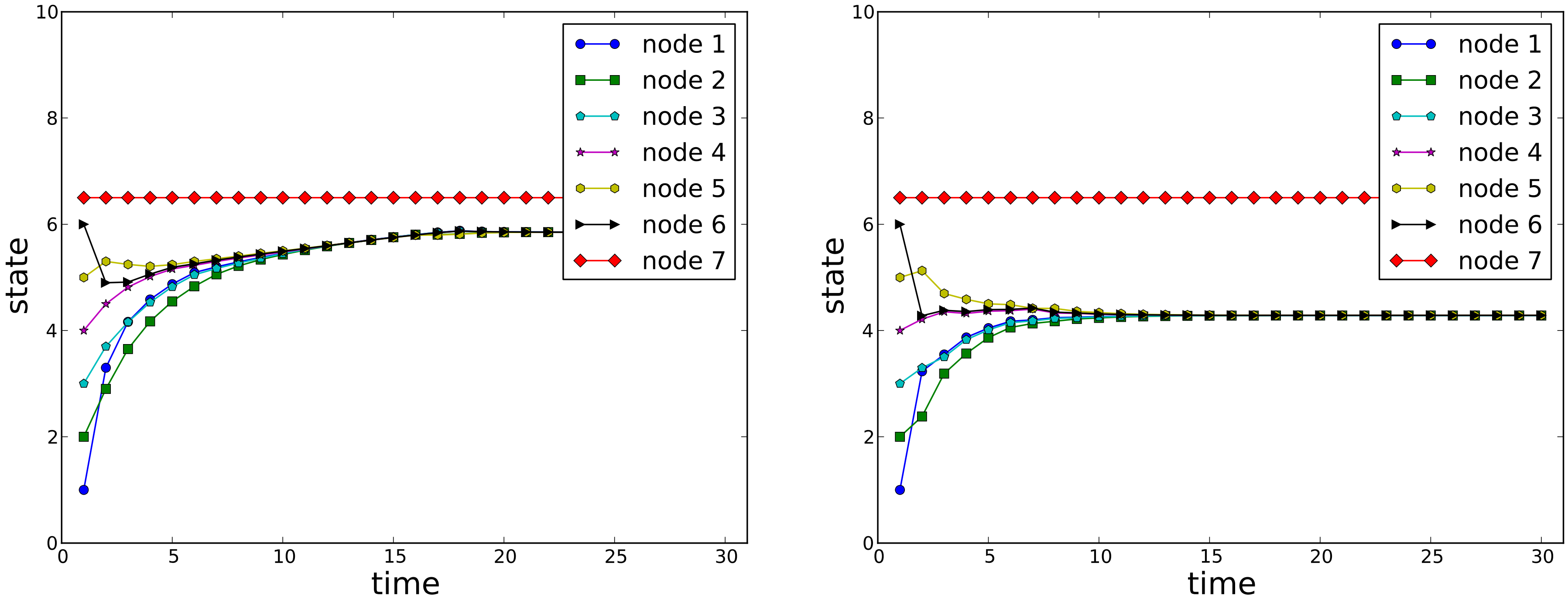


$$x_i(k) = \frac{1}{A_i(k)} \sum_{j \in N_i} t_{ij}(k) x_j(k-1)$$

$$A_i(k) = \sum_{j \in N_i} t_{ij}(k)$$

$t_{ij}(k)$ is “equilibrium” global trust values

Simulations



Adversary outputs constant message. Figure on the left has no trust propagation. Figure on the right has trust propagation.

Joint Content Delivery and Wireless Network Optimization

Existing System Design

Different metrics/utilities:

- Ads: number of views (= ad payout).
- Videos: time spent.
- General: user satisfaction.

Social Network

Predict “rewards”.

“Big Data”: various ML models.

Slow in training, fast in computing.

Asynchronous, centralized.

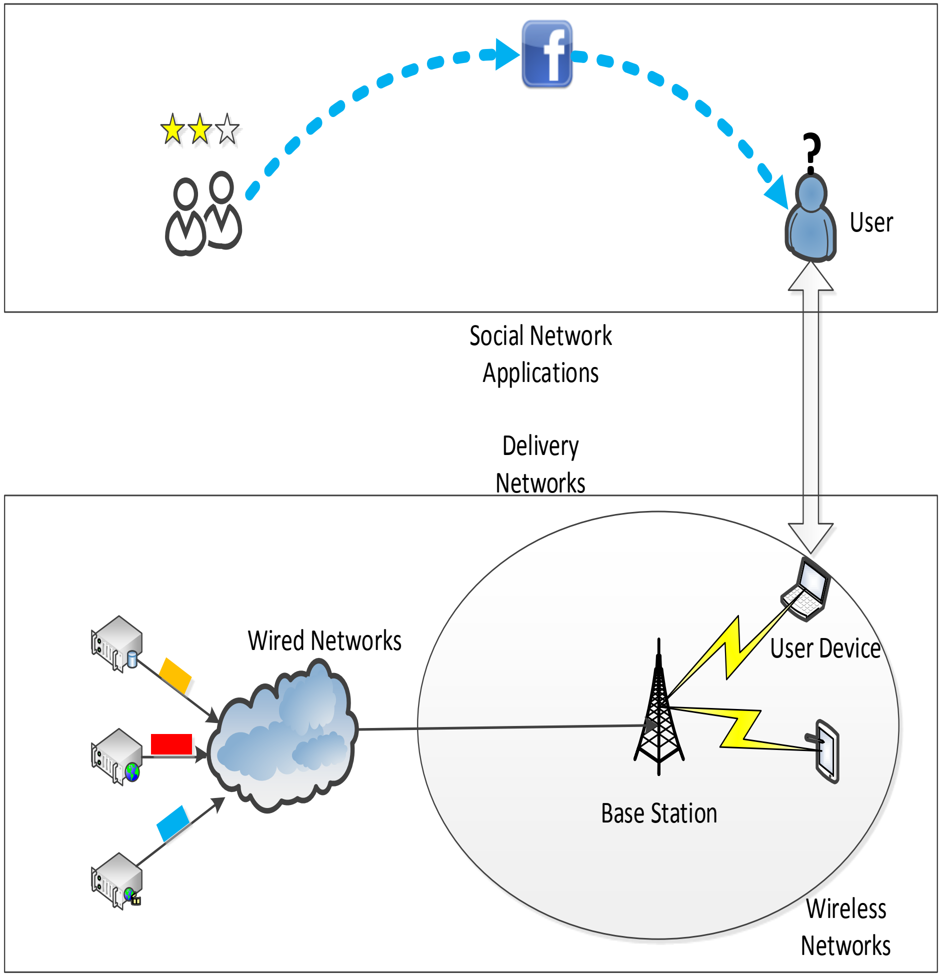
Wireless Network

Schedule resource for delivery.

Randomness of channel.

Time-variant.

Synchronized, distributed.



Three Scenarios/Problems

- Single base station, time-invariant reward.
  - Basic problem.
  - Establish foundation framework.
- Multiple base stations, time-invariant reward.
  - Many system configurations.
- Single base station, time-variant reward.
  - Time-variance specifically due to social dynamics.

Comparison

	Traditional	Joint Optimal
What to deliver?	Social optimal	Joint optimal
How to deliver?	Unicast	Multicast
Fragmentation?	Packet	Content package

Simulation Results – Overall System Rewards

Significant joint optimization gain.

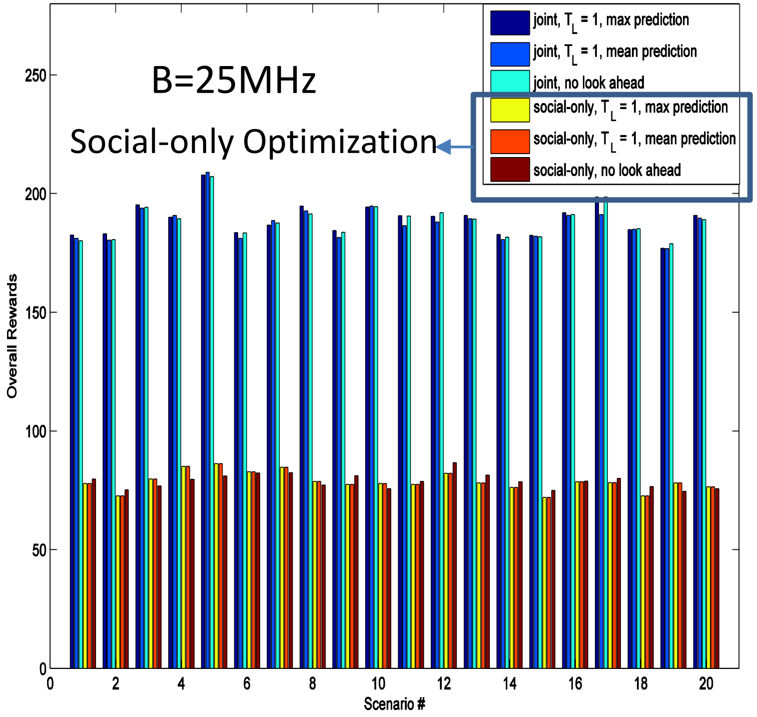
Myopic scheduling is sufficiently good.

No significant improvement for look-ahead.

Number of contents

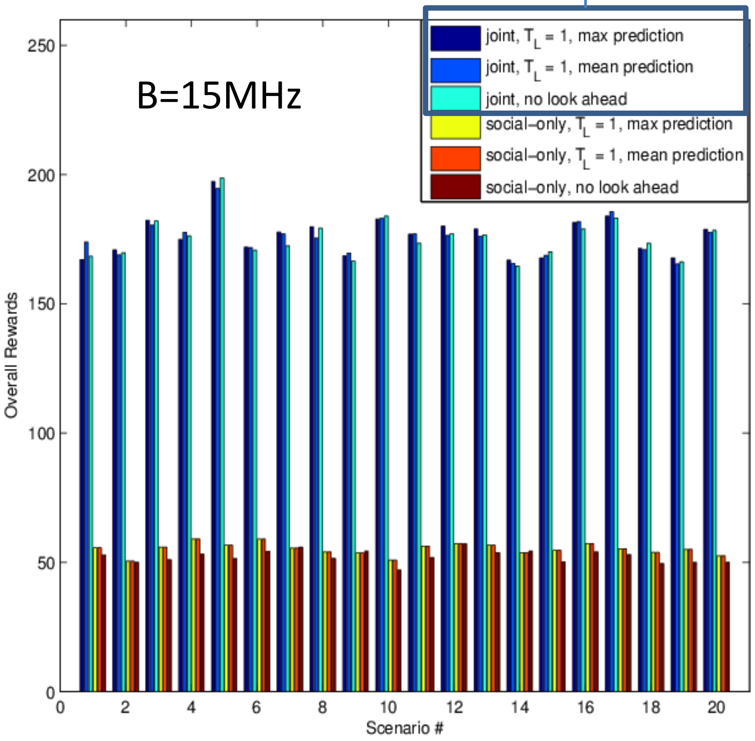
M=30, N=20

Number of users


B=25MHz

Social-only Optimization

Joint Optimization


B=15MHz

Thank you!

baras@isr.umd.edu

301-405-6606

http://www.isr.umd.edu/~baras

Questions?