New Automotive Project with Toyota

Bruce H. Krogh

CMACS PI Review Meeting

Oct. 29, 2010

- Overview of new NSF project
- Automotive systems application
- Opportunities for CMACS

CPS:MEDIUM:GOALI: CPS Architectures for Multi-Model Verification of Embedded Control Systems

3-year NSF Project

CMU PIs: David Garlan, Bruce H. Krogh, Andre Platzer

Toyota PIs: Ken Butts, Prashant Ramachandra

CPS:MEDIUM:GOALI:
CPS Architectures for Multi-Model Verification
# of Emb[illegible] Systems

Cyber-Physical Systems

CMU PIs: David [illegible], Andre Platzer

Toyota PIs: Ken Butts, Prashant Ramachandra

CPS:MEDIUM:GOALI:
CPS Architectures for Multi-Model Verification
# of Emb l Systems

Medium Project

CMU PIs: David Ga ogh, Andre Platzer

Toyota PIs: Ken Butts, Prashant Ramachandra

CPS:MEDIUM:GOALI:
CPS Architectures for Multi-Model Verification of Embedded Control Systems

Grant Opportunities for Academic Liaisons to Industry

CM　　　　　　　　　　　　　　*Platzer*

Toyota　　　　　　　　　　　　*machandra*

CPS:MEDIUM:GOALI:

CPS Architectures for Multi-Model Verification of Embedded Control Systems

3-year NSF Project

CMU PIs: David Garlan, Bruce H. Krogh, Andre Platzer

Toyota PIs: Ken Butts, Prashant Ramachandra

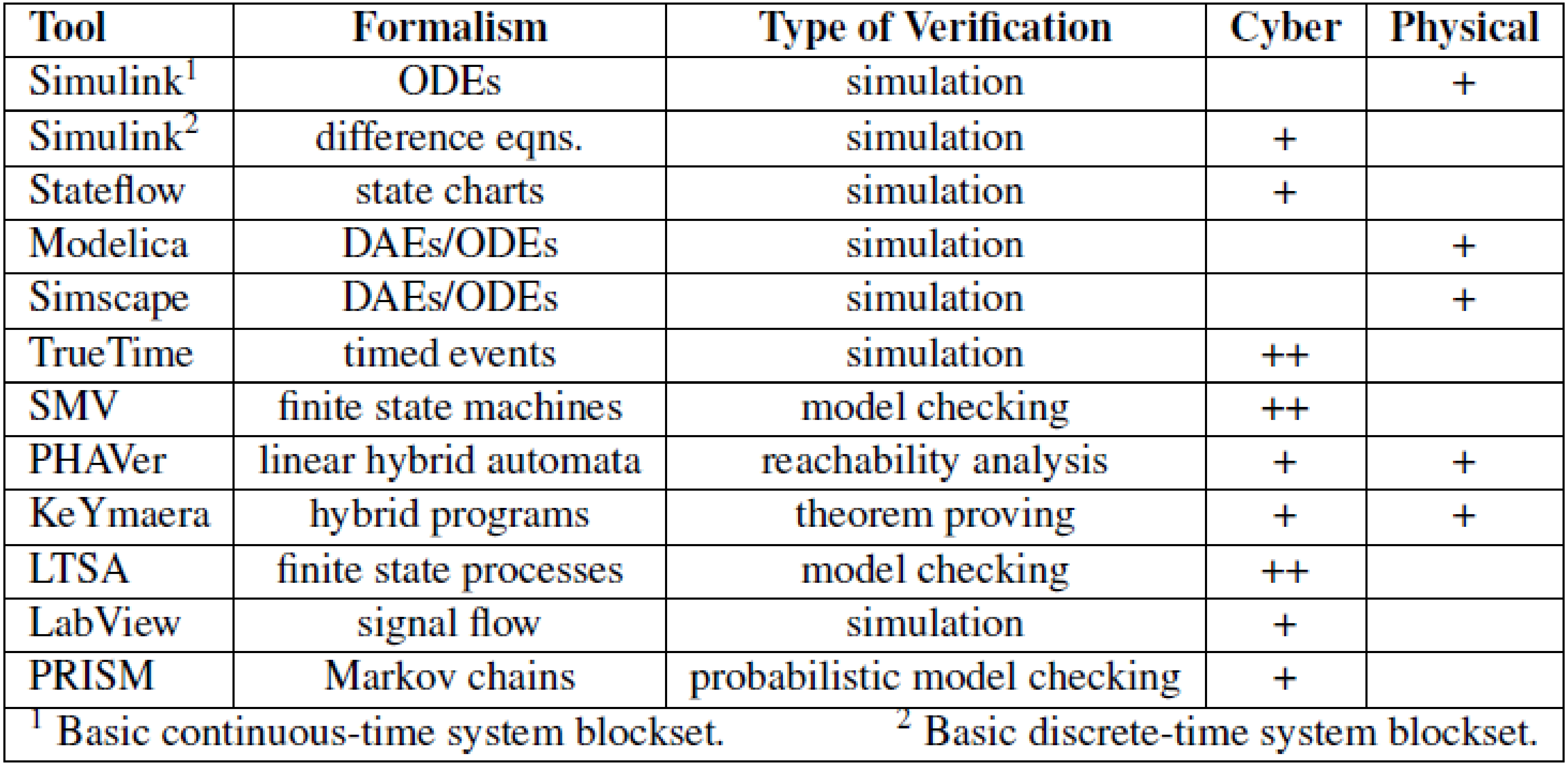
Motivation

- Developing complex cyber-physical systems requires analyses of multiple models **using different formalisms and tools.**

Motivation

- Developing complex cyber-physical systems requires analyses of multiple models using different formalisms and tools.
- How can we:
  - guarantee models are consistent with each other?
  - infer system-level properties from heterogeneous analyses of heterogeneous models?

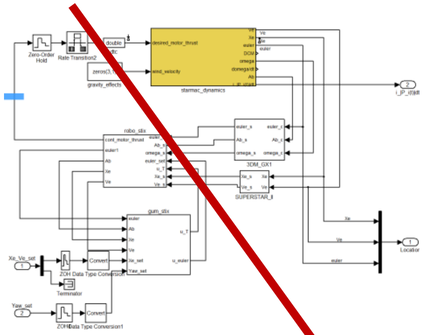
Tools and Formalisms Used in Embedded Control System Development



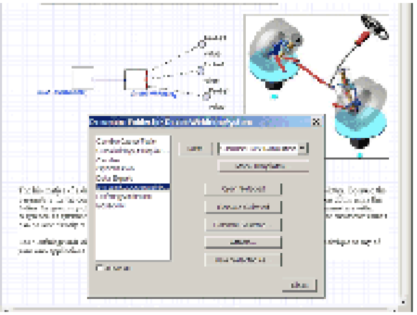
Tool	Formalism	Type of Verification	Cyber	Physical
Simulink[1]	ODEs	simulation		+
Simulink[2]	difference eqns.	simulation	+	
Stateflow	state charts	simulation	+	
Modelica	DAEs/ODEs	simulation		+
Simscape	DAEs/ODEs	simulation		+
TrueTime	timed events	simulation	++	
SMV	finite state machines	model checking	++	
PHAVer	linear hybrid automata	reachability analysis	+	+
KeYmaera	hybrid programs	theorem proving	+	+
LTSA	finite state processes	model checking	++	
LabView	signal flow	simulation	+	
PRISM	Markov chains	probabilistic model checking	+	

[1] Basic continuous-time system blockset. [2] Basic discrete-time system blockset.

Multiple Views of a CPS



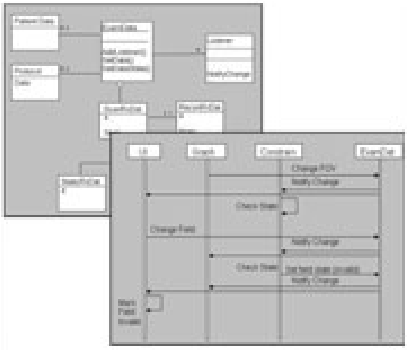
Control View



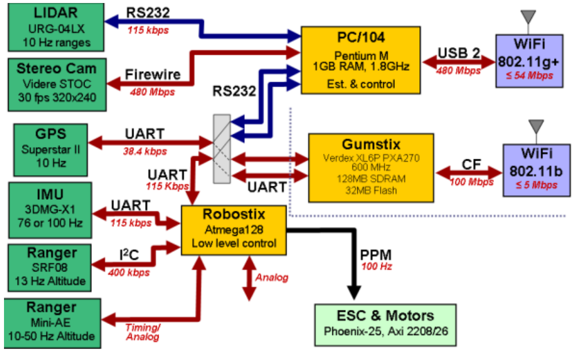
Physical View

physical

cyber

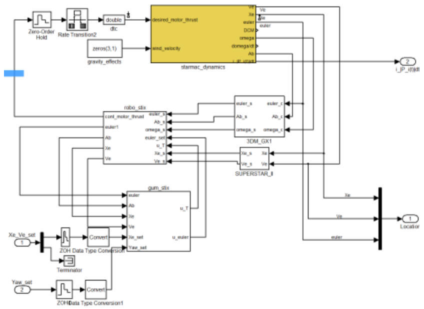


Software View

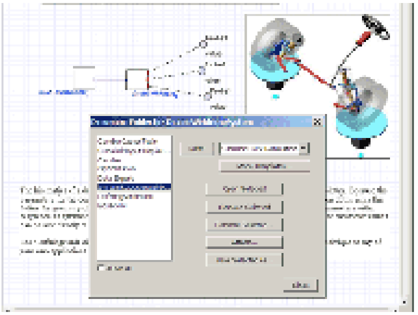


Hardware View

Is there a unifying representation?

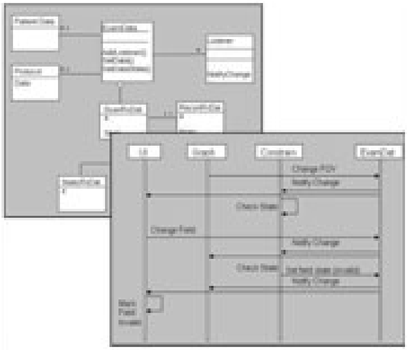


Control View

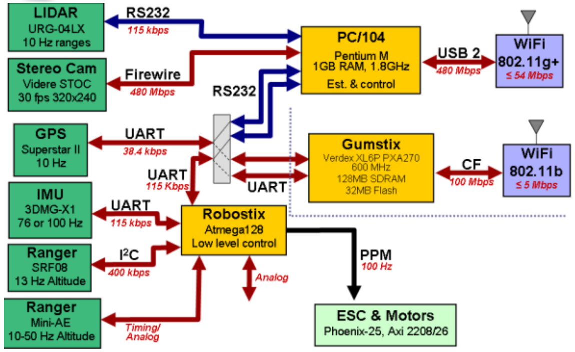


Physical View

?



Software View



Hardware View

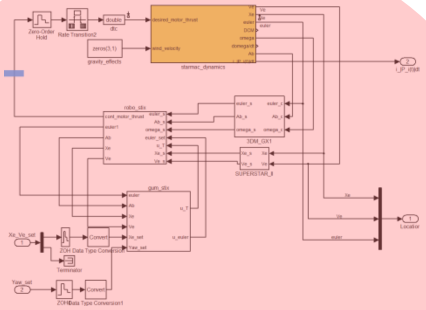
Multi-Domain Modeling/Analysis
Approach 1: Universal Modeling Language

Goal: Create a language that encompasses *everything* that needs to be modeled

E.g.:

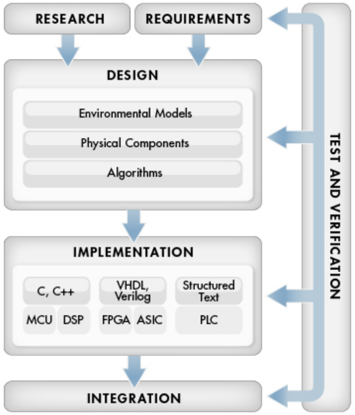
- UML/SysML (actually multiple views)
- MATLAB Simulink+Toolboxes

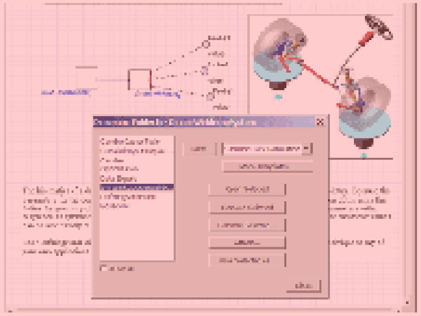
Universal Model Vision



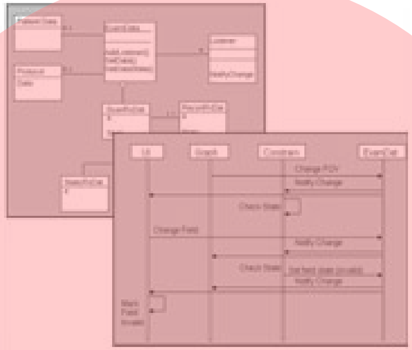
Control View

Model-Based Design*

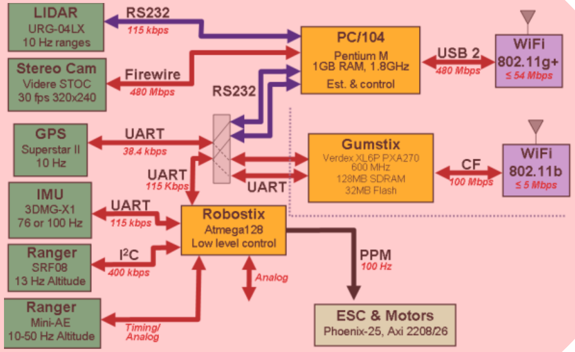




Physical View



Software View



Hardware View

* http://www.mathworks.com/model-based-design/

Problems with Universal Models

- Comprehensive models representing *everything* are intractable
- Separation of concerns supports multi-disciplinary development
- Analysis tools operate on specific types of models, not universal models

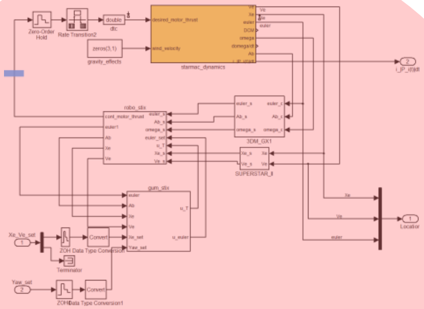
Multi-Domain Modeling/Analysis Approach 2: Model Translation

Goal: Automatically translate models from one formalism into another formalism

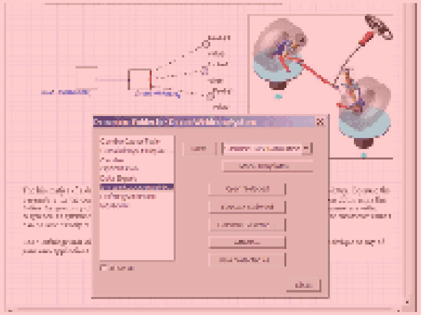
E.g.:

- ARIES (Automatic Integration of Reusable Embedded Software)
  http://kabru.eecs.umich.edu/bin/view/Main/AIRES
- HSIF (Hybrid Systems Interchange Format)
  http://ptolemy.eecs.berkeley.edu/projects/mobies/

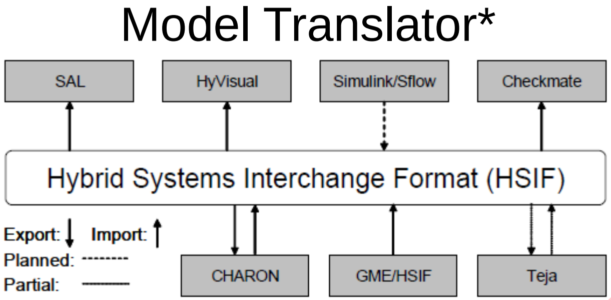
Model Translation Vision

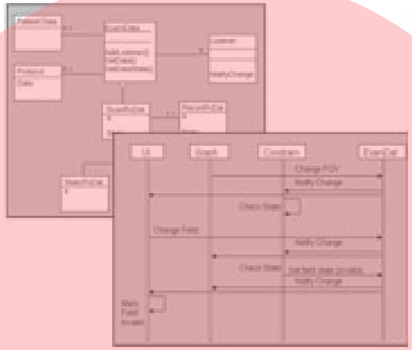


Control View

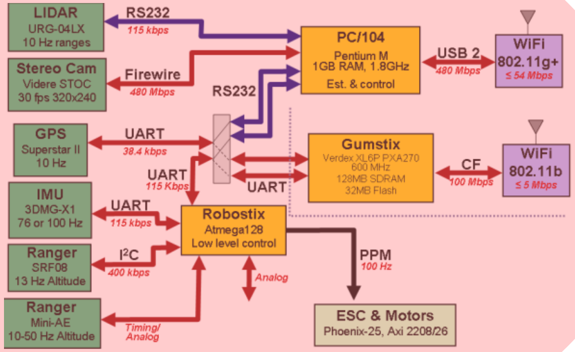


Physical View





Software View



Hardware View

* J. Sprinkle, Generative components for hybrid systems tools, Journal of Object Technology, Mar-Apr 2003.

Problems with Model Translation

- Tool-specific translation isn’t scalable
- Universal translation requires a universal modeling language (Approach 1)
- Modeling languages and tools evolve continually

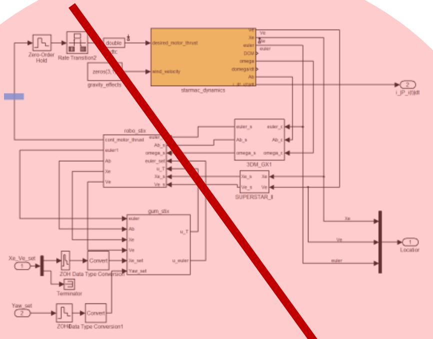
Multi-Domain Modeling/Analysis Proposal: Architectural Approach

Goal: Unify heterogeneous models through *light-weight* representations of their structure and semantics using architecture description languages (ADLs).

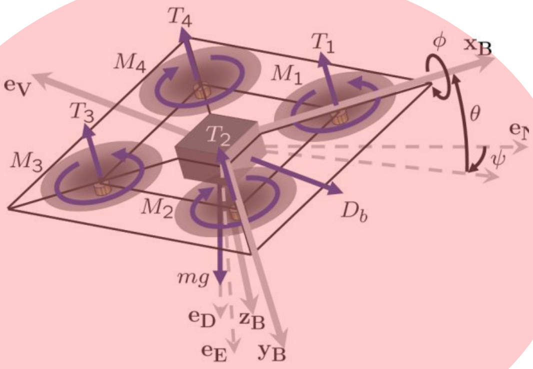
Current ADLs

- UML/SysML
- AADL

Architectural Approach



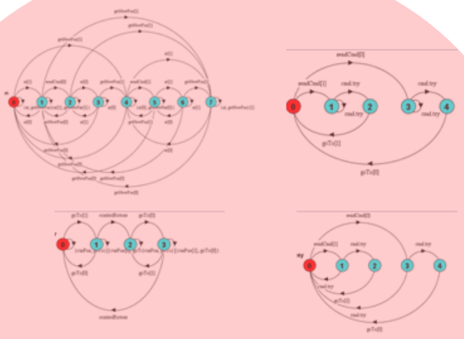
Control View



Physical View

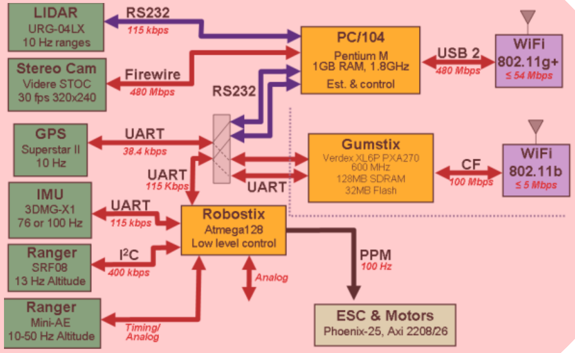
physical

cyber



Software View

Current ADLs

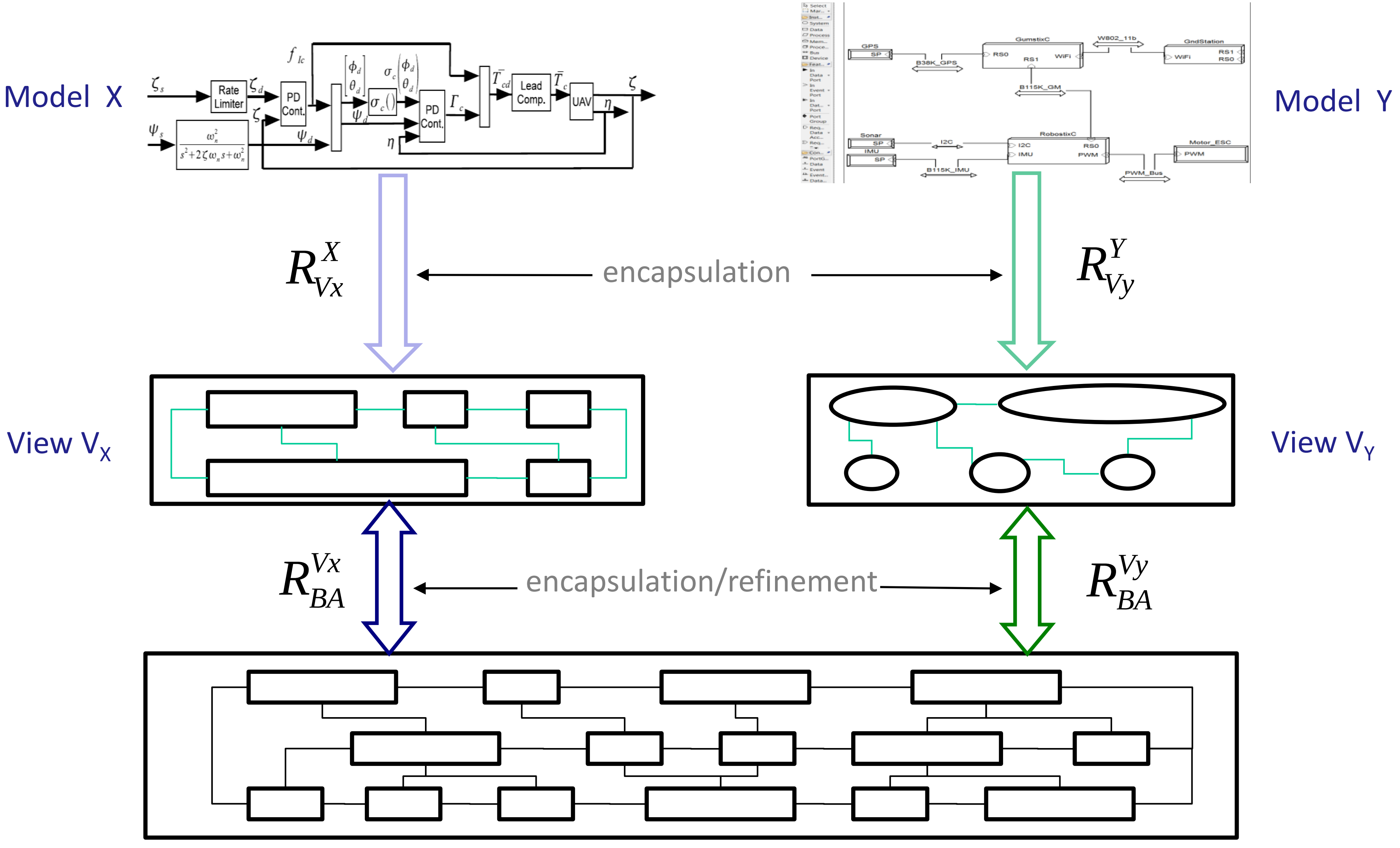


Hardware View

Proposal: CPS Architectural Style

- **A unifying framework to:**
  - Detect structural inconsistencies between models
  - Detect semantic inconsistencies in modeling assumptions
  - Infer system-level properties
  - Evaluate design trade-offs across cyber-physical boundary

Models as Architectural Views



Model X

Model Y

R^{X}_{Vx}

encapsulation

R^{Y}_{Vy}

View V_X

View V_Y

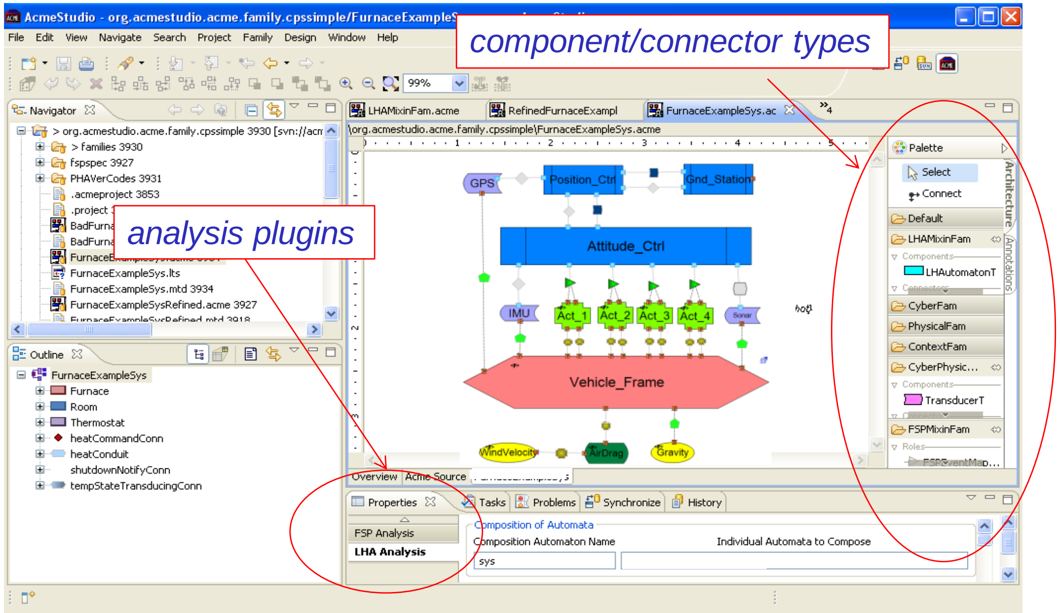
R^{Vx}_{BA}

encapsulation/refinement

R^{Vy}_{BA}

Base CPS Architecture

Architecture Tool: AcmeStudio



component/connector types

analysis plugins

- Extensible framework for architecture design and analysis
- The CPS style has been created as a stand-alone AcmeStudio family
- Analysis tools will be developed as AcmeStudio plugins

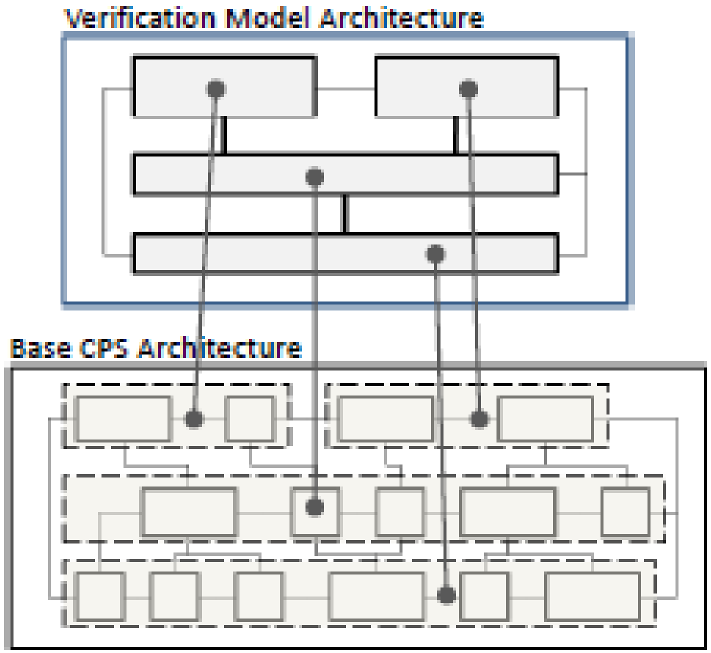
Heterogeneous Verification

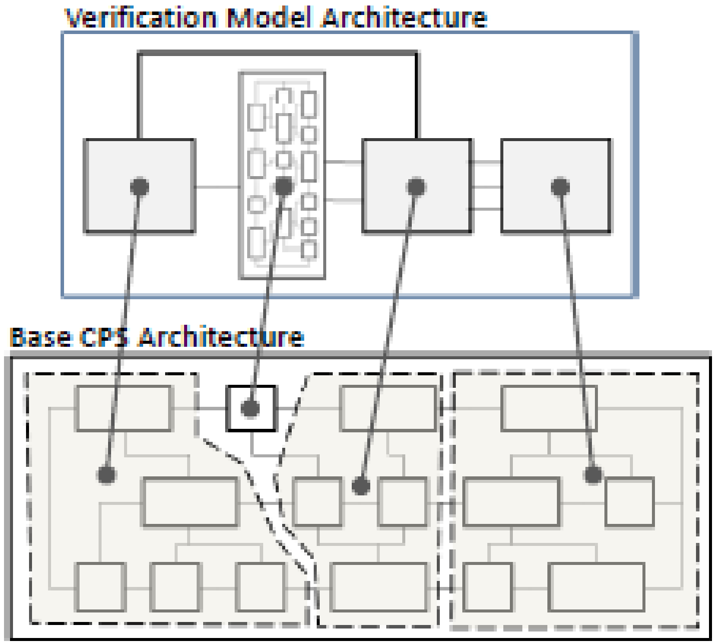
- **Annotate architectures with**
  - system-level specifications/requirements
  - assumptions underlying models/views
  - guarantees provided by model-based analyses
- **Develop algorithms for**
  - consistency analysis for specifications & assumptions
  - integration of model-based verification results
  - coverage via heterogeneous verification activities

Building on Previous work

- **Model-based design**
  - leverage existing models, tools, methods at the system level (rather than replace them)
- **Architecture**
  - build on extensive research in ADLs for cyber systems
- **Formal methods**
  - develop rigorous (sound, complete) logic for integrating knowledge from heterogeneous sources

Abstraction and Refinement





- How are verification assumptions/results related to each other?
- What can be inferred about system-level requirements?

GOAL: System-Level Logic for Heterogeneous Verification

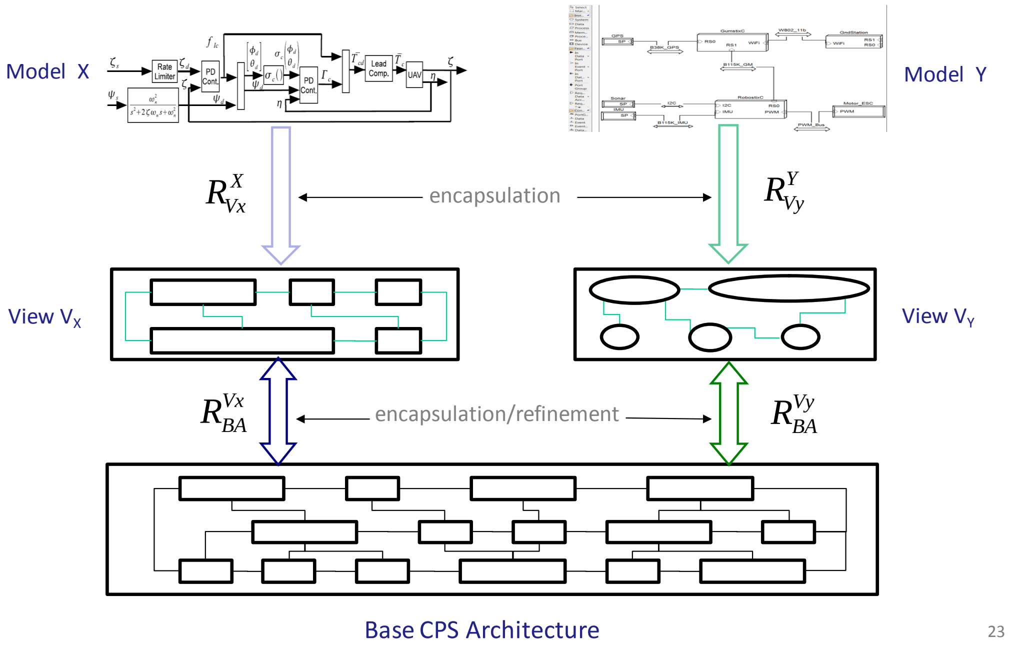
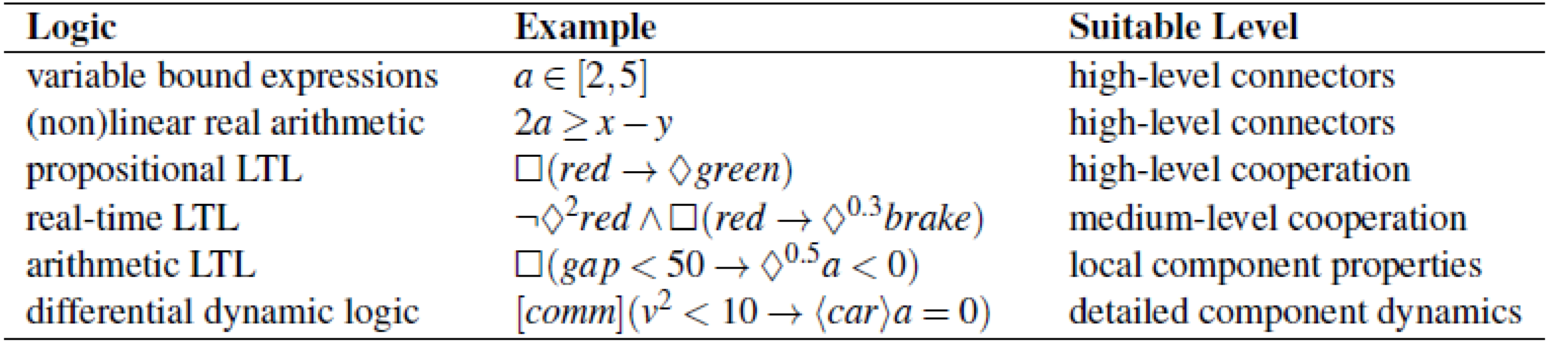


Table 2: Range of possible choices for the logic of properties at different architectural levels

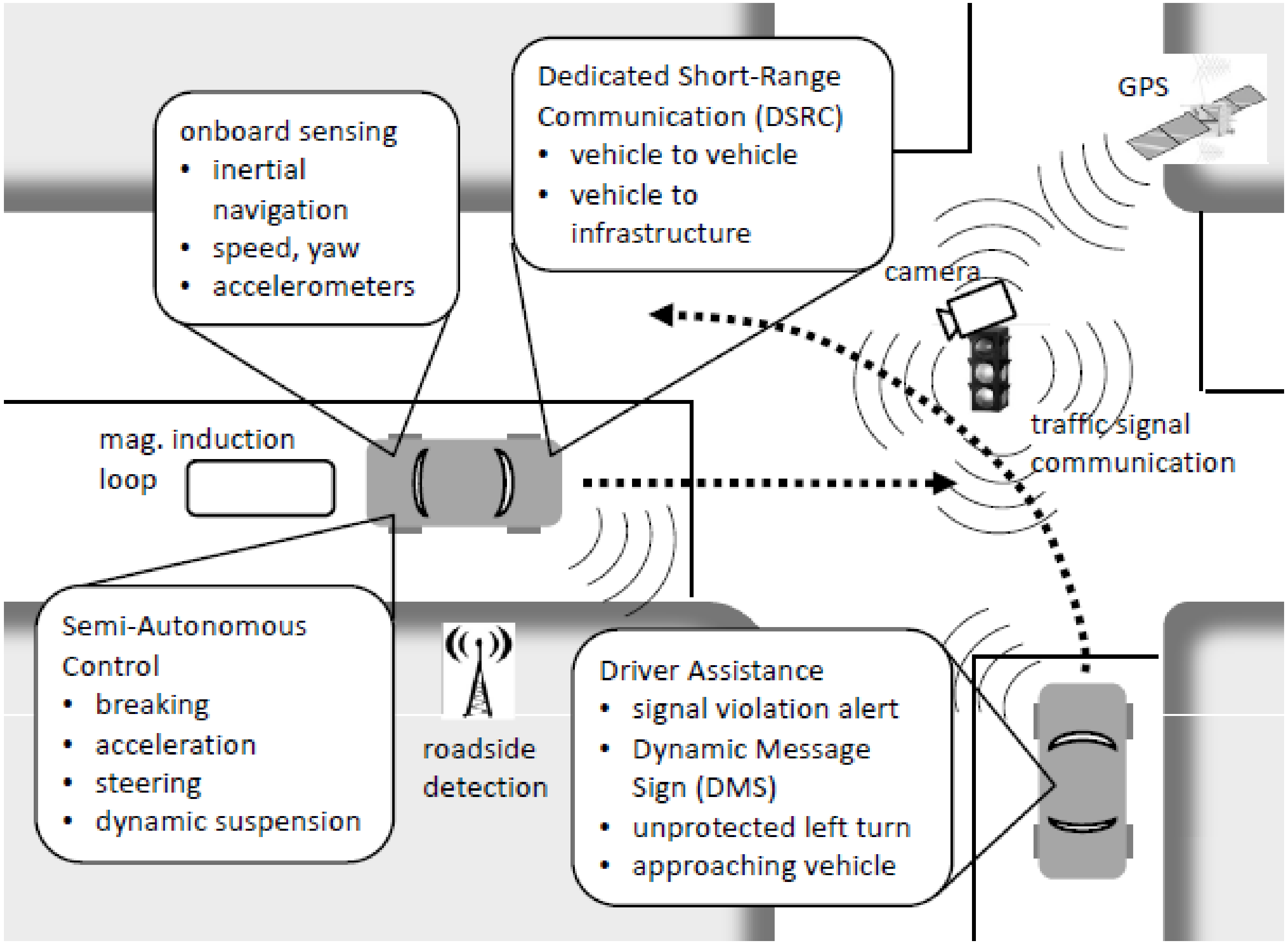


Logic	Example	Suitable Level
variable bound expressions	$a \in [2,5]$	high-level connectors
(non)linear real arithmetic	$2a \geq x - y$	high-level connectors
propositional LTL	$\Box(red \rightarrow \Diamond green)$	high-level cooperation
real-time LTL	$\neg\Diamond^2 red \wedge \Box(red \rightarrow \Diamond^{0.3} brake)$	medium-level cooperation
arithmetic LTL	$\Box(gap < 50 \rightarrow \Diamond^{0.5} a < 0)$	local component properties
differential dynamic logic	$[comm](v^2 < 10 \rightarrow \langle car \rangle a = 0)$	detailed component dynamics

GOALI: Collaboration with Toyota Technical Center-Ann Arbor

- **Toyota Project Management**
  - Ken Butts, Power Train Control Dept.
  - long-time champion of formal methods for automotive control system development
- **Target application: CICAS**
  - cooperative intersection collision avoidance system
  - public-domain models from government project
  - internal Toyota research on active braking

CICAS Scenario



onboard sensing

- inertial navigation
- speed, yaw
- accelerometers

Dedicated Short-Range Communication (DSRC)

- vehicle to vehicle
- vehicle to infrastructure

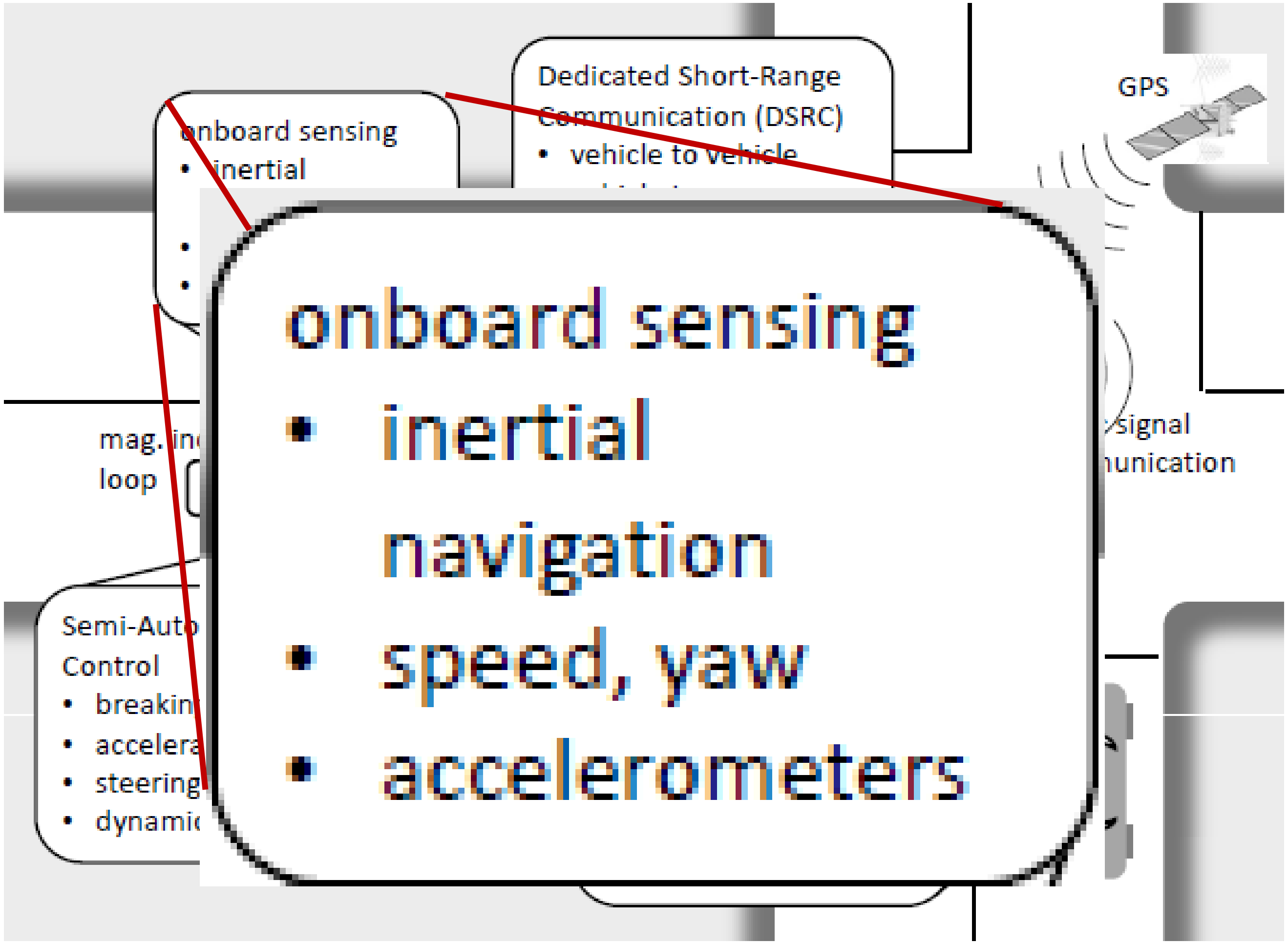
Semi-Autonomous Control

- breaking
- acceleration
- steering
- dynamic suspension

Driver Assistance

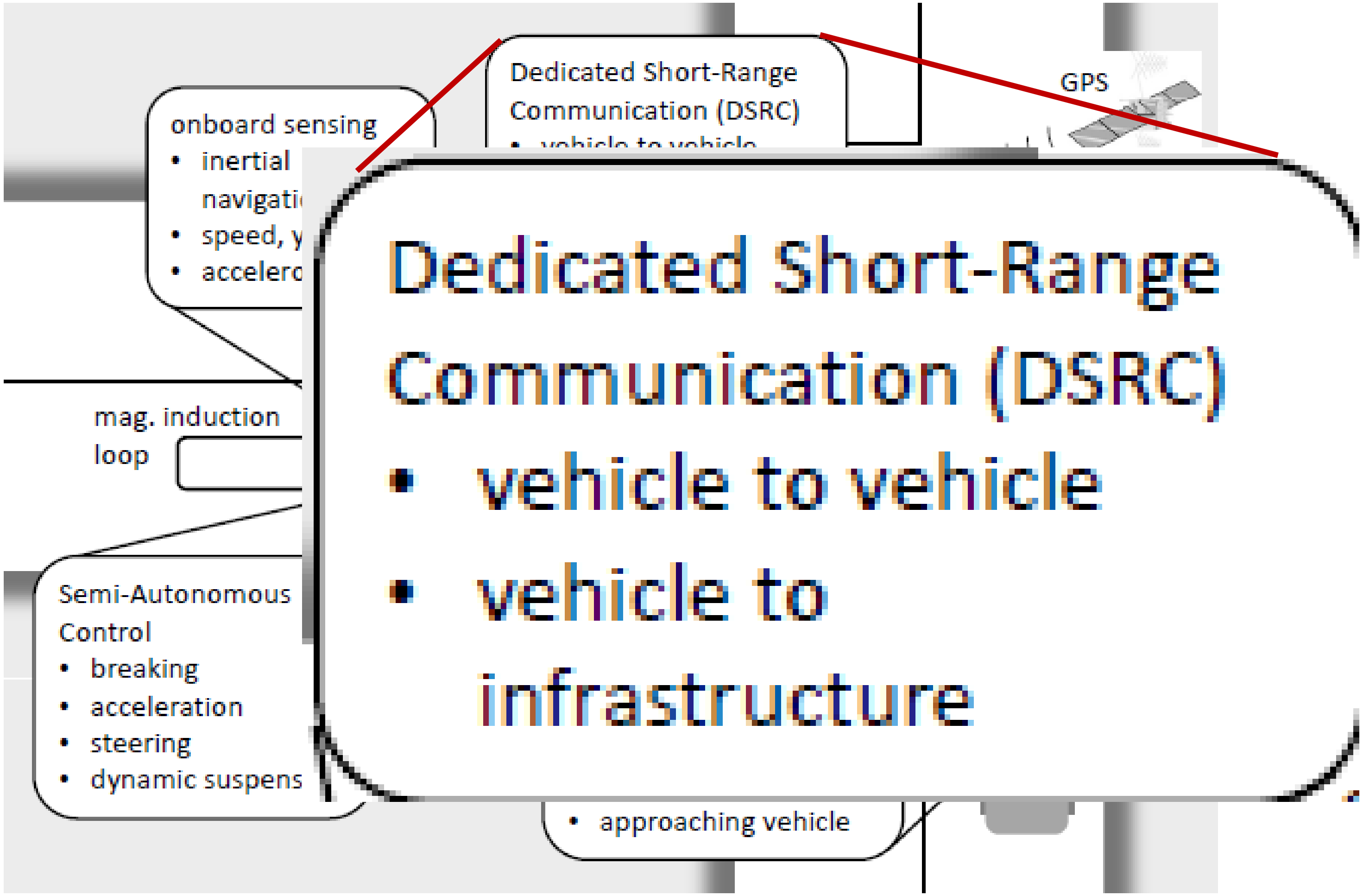
- signal violation alert
- Dynamic Message Sign (DMS)
- unprotected left turn
- approaching vehicle

CICAS Scenario



onboard sensing
- inertial navigation
- speed, yaw
- accelerometers

CICAS Scenario



onboard sensing
- inertial navigati
- speed, y
- accelero

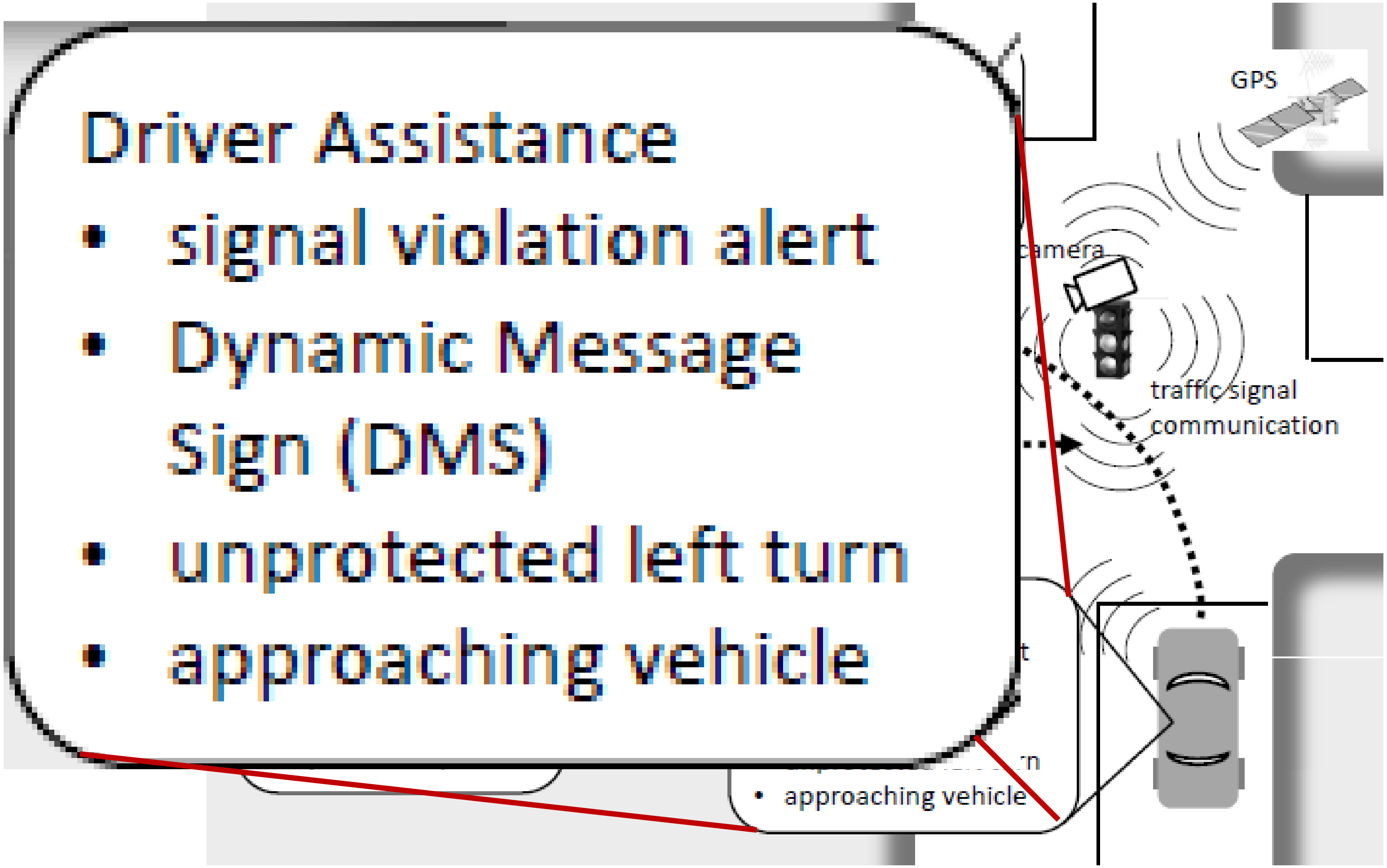
Dedicated Short-Range Communication (DSRC)
- vehicle to vehicle

Semi-Autonomous Control
- breaking
- acceleration
- steering
- dynamic suspens

- approaching vehicle

Dedicated Short-Range Communication (DSRC)
- vehicle to vehicle
- vehicle to infrastructure

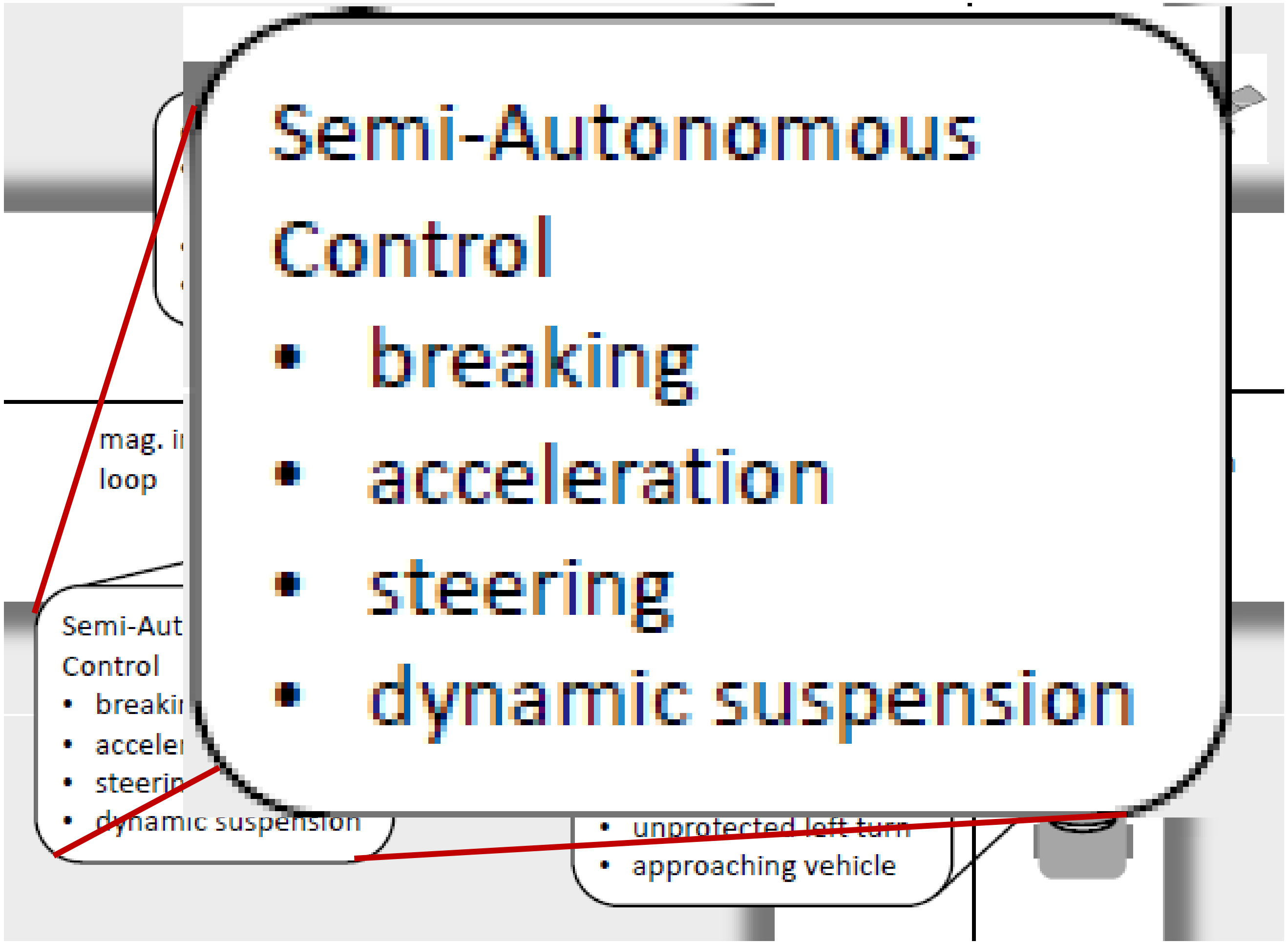
CICAS Scenario



Driver Assistance

- signal violation alert
- Dynamic Message Sign (DMS)
- unprotected left turn
- approaching vehicle

CICAS Scenario



Semi-Autonomous Control
- breaking
- acceleration
- steering
- dynamic suspension

Automotive Safety: Social Impact

At the inquest into the world's first road traffic death in 1896, the coroner was reported to have said "this must never happen again". More than a century later, 1.2 million people are killed on roads every year and up to 50 million more are injured.

www.who.int/features/2004/road_safety/en/

One in every 50 deaths worldwide is associated with road accidents ... traffic crashes are second only to childhood infections and AIDS as a killer of people between the ages of 5 and 30. ... By 2020, traffic deaths are expected to increase by 80 percent as hundreds of millions of cars are added to the roads.

www.dui.com/dui-library/fatalities-accidents/statistics/traffic-deaths

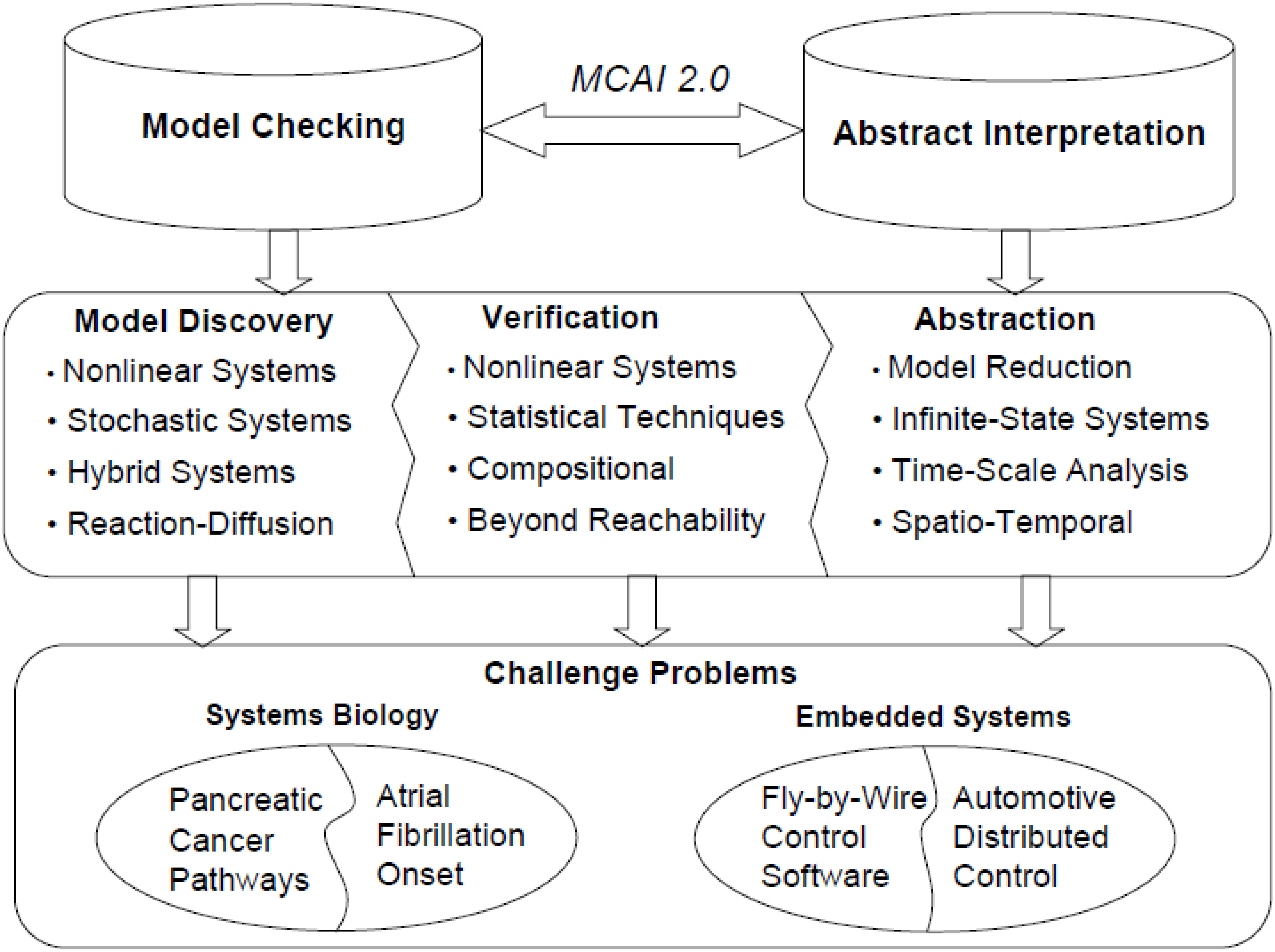
CICAS-Intersection Collisions

Intersection collisions account for 21.5% of traffic fatalities and 44.8% of traffic injuries in the US.

http://safety.fhwa.dot.gov/intersection/resources/fhwasa10005/brief_2.cfm

- **Technologies being developed**
  - driver situational awareness
    - e.g., advanced warning on traffic light states
  - infrastructure countermeasures
    - e.g., adaptive traffic light timing
  - vehicle countermeasures
    - e.g., active breaking

Opportunities for CMACS



CMACS Opportunities

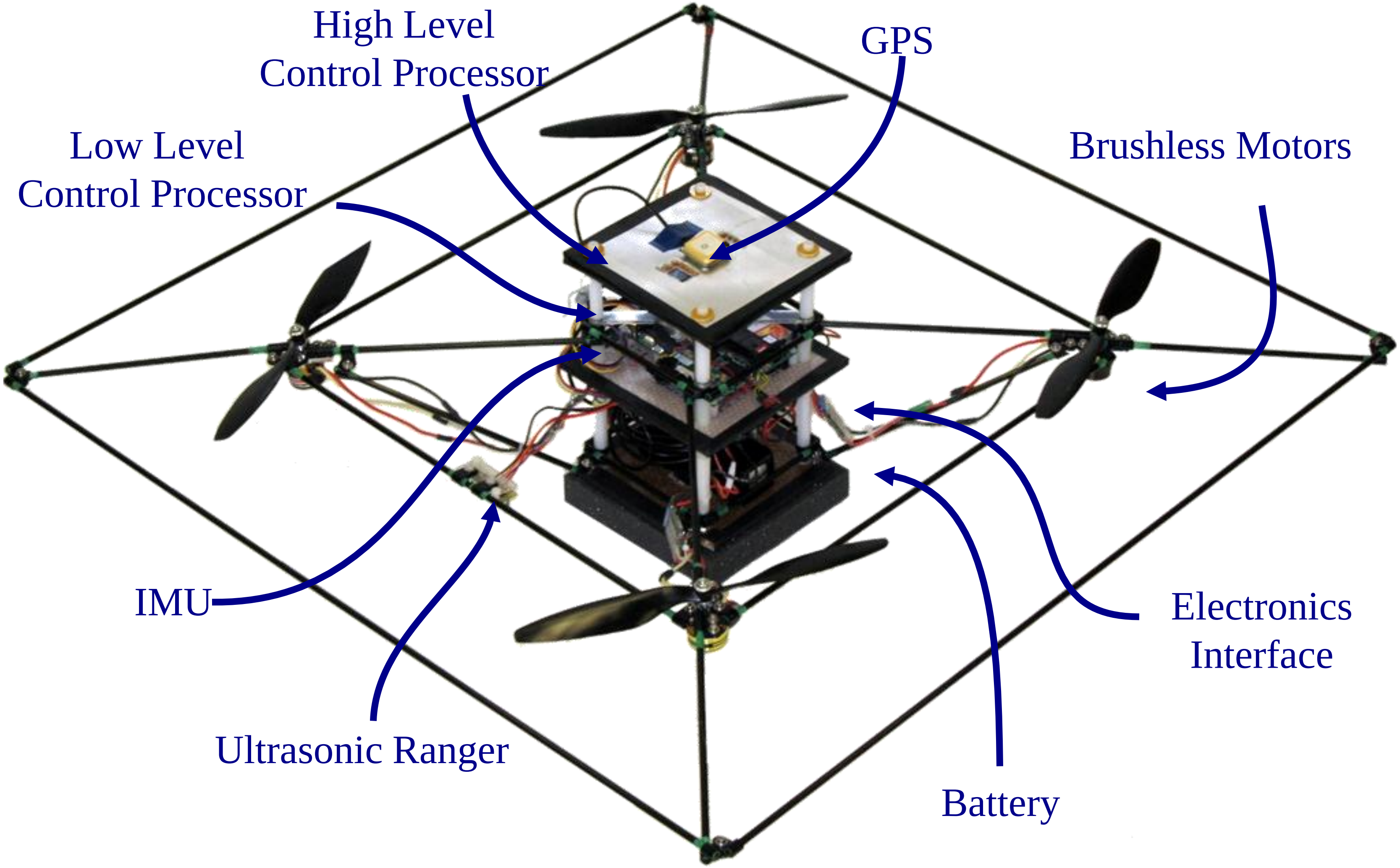
"We are also planning a significant effort in Open-Source Tool Development and in the formation of a Testbed Repository. ... [this] will lead to new, open-source verification tools, as well as new models of ... embedded systems, which will be disseminated for public use."

Next Steps for CMACS-Toyota

- Matthias Althoff will work with Toyota to develop relevant models
- Matthias Althoff and Sarah Loos will apply some of their work on verifying properties of vehicle control policies
- We’ll help anyone interested to develop examples

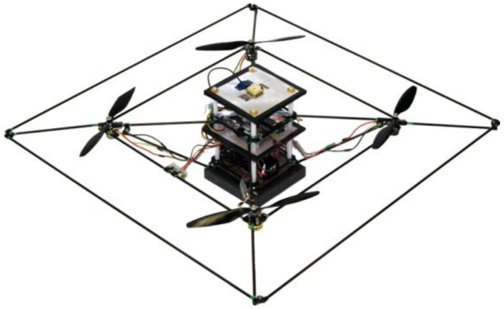
Auto/Aero Panel Discussion

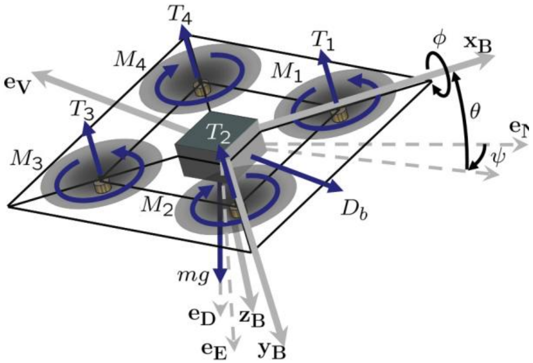
A Cyber-Physical System (CPS): STARMAC Quadrotor*



*http://hybrid.eecs.berkeley.edu/starmac/

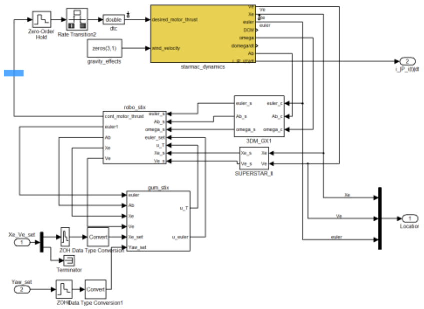
Multiple Views of a CPS



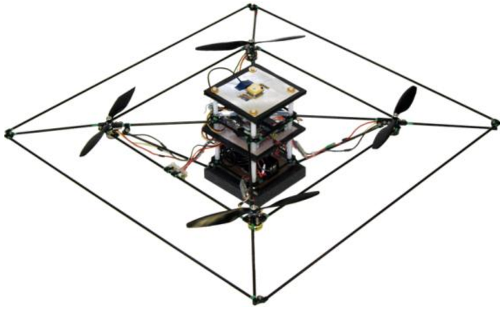


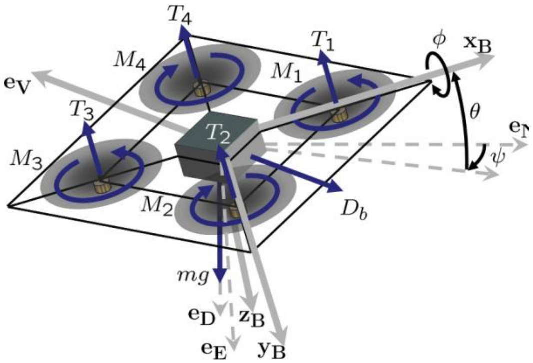
Physical View

Multiple Views of a CPS



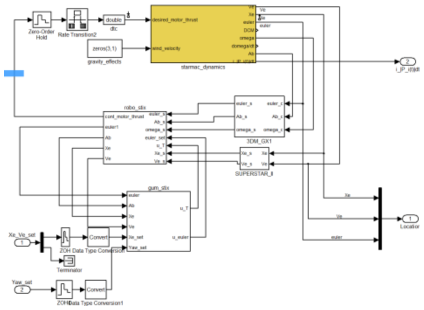
Control View



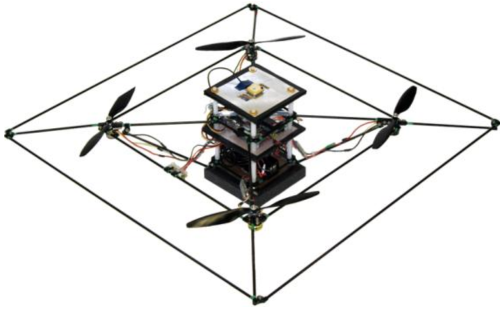


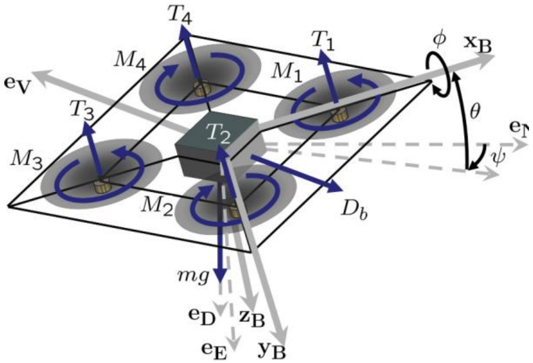
Physical View

Multiple Views of a CPS

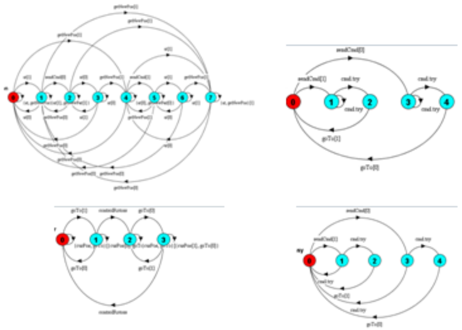


Control View



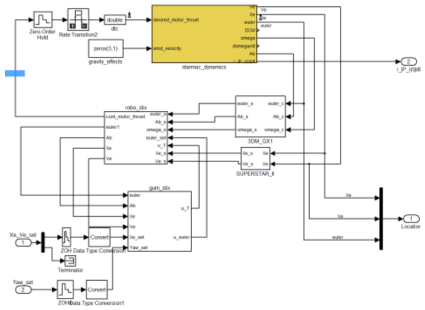


Physical View

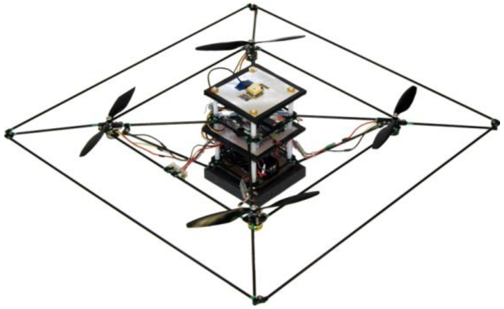


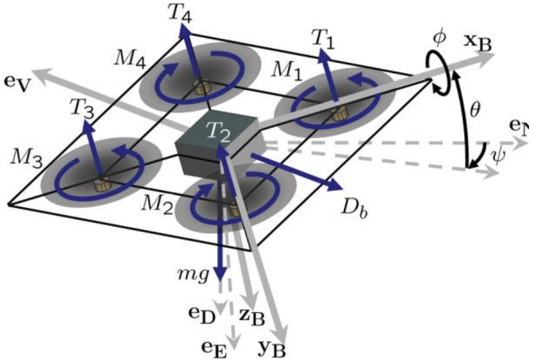
Software View

Multiple Views of a CPS

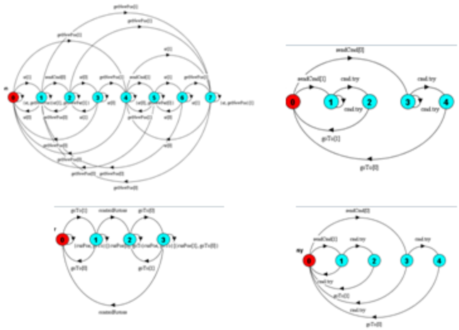


Control View

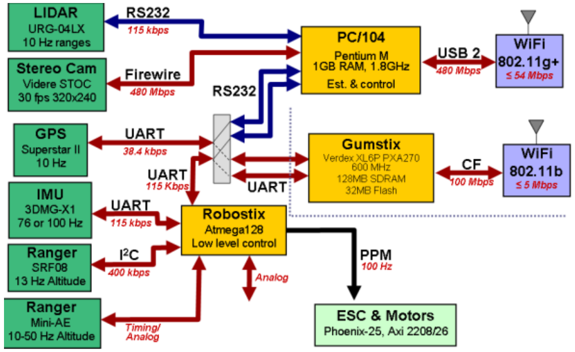




Physical View



Software View



Hardware View

Project Plans

- **Research heterogeneous verification**
  - architectural concepts and tools
  - methods for multi-tool verification (e.g., assume-guarantee)
  - system-level logic
- **Collaboration with Toyota**
  - develop case studies
  - tool development
  - regular meetings & exchanges
- **Education & Outreach**
  - course modules on cyber-physical systems
  - senior/MS course on CPS architectures
  - year three industrial seminars