Model-Based Design of Connected and Autonomous Vehicles

Akshay Rajhans, PhD

Senior Research Scientist
Advanced Research and Technology Office
MathWorks
https://arajhans.github.io

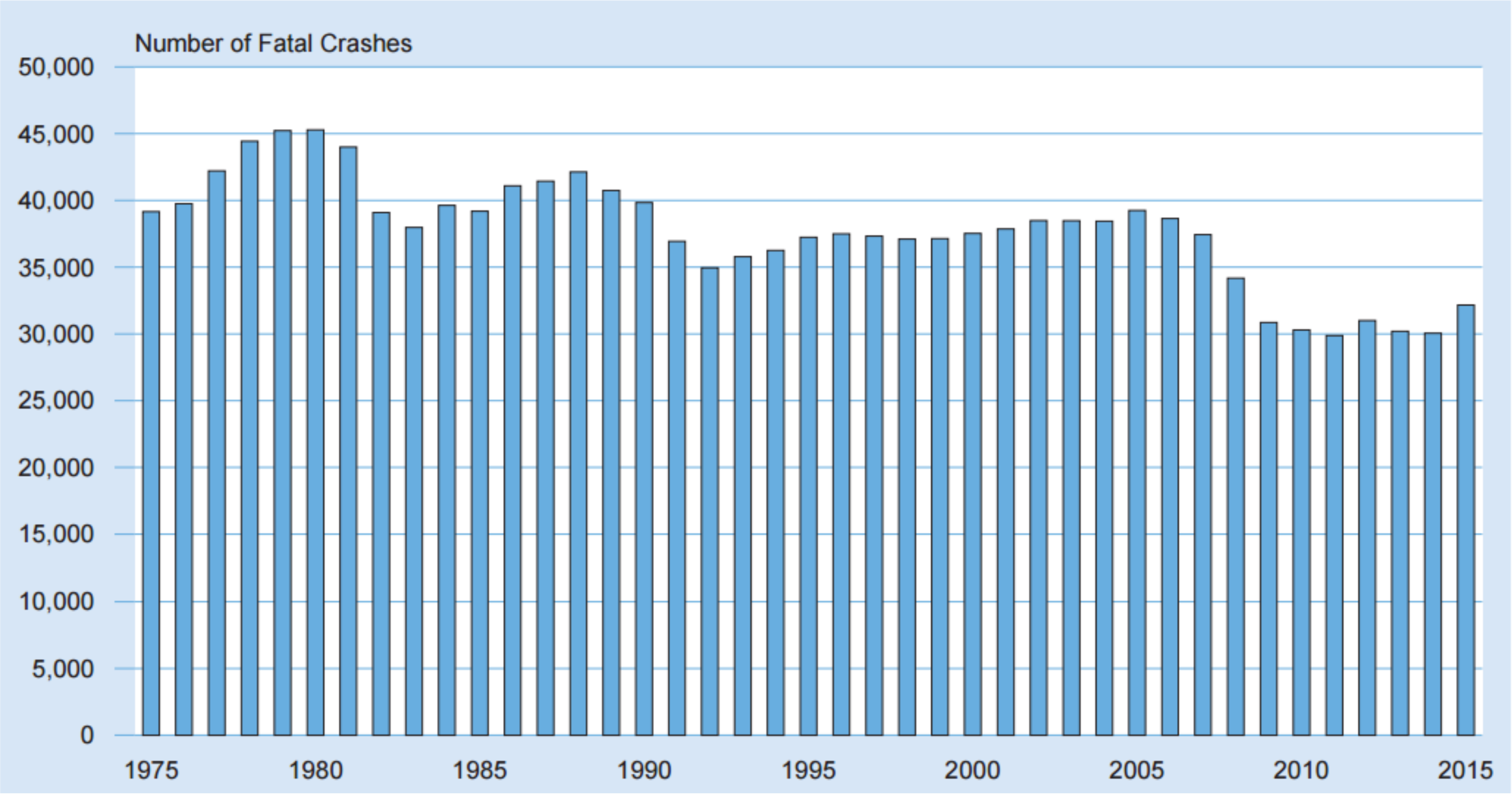
2nd IEEE Summer School on Connected and Autonomous Vehicles
May 19, 2017

How do we design safe and reliable cyber-physical systems ?

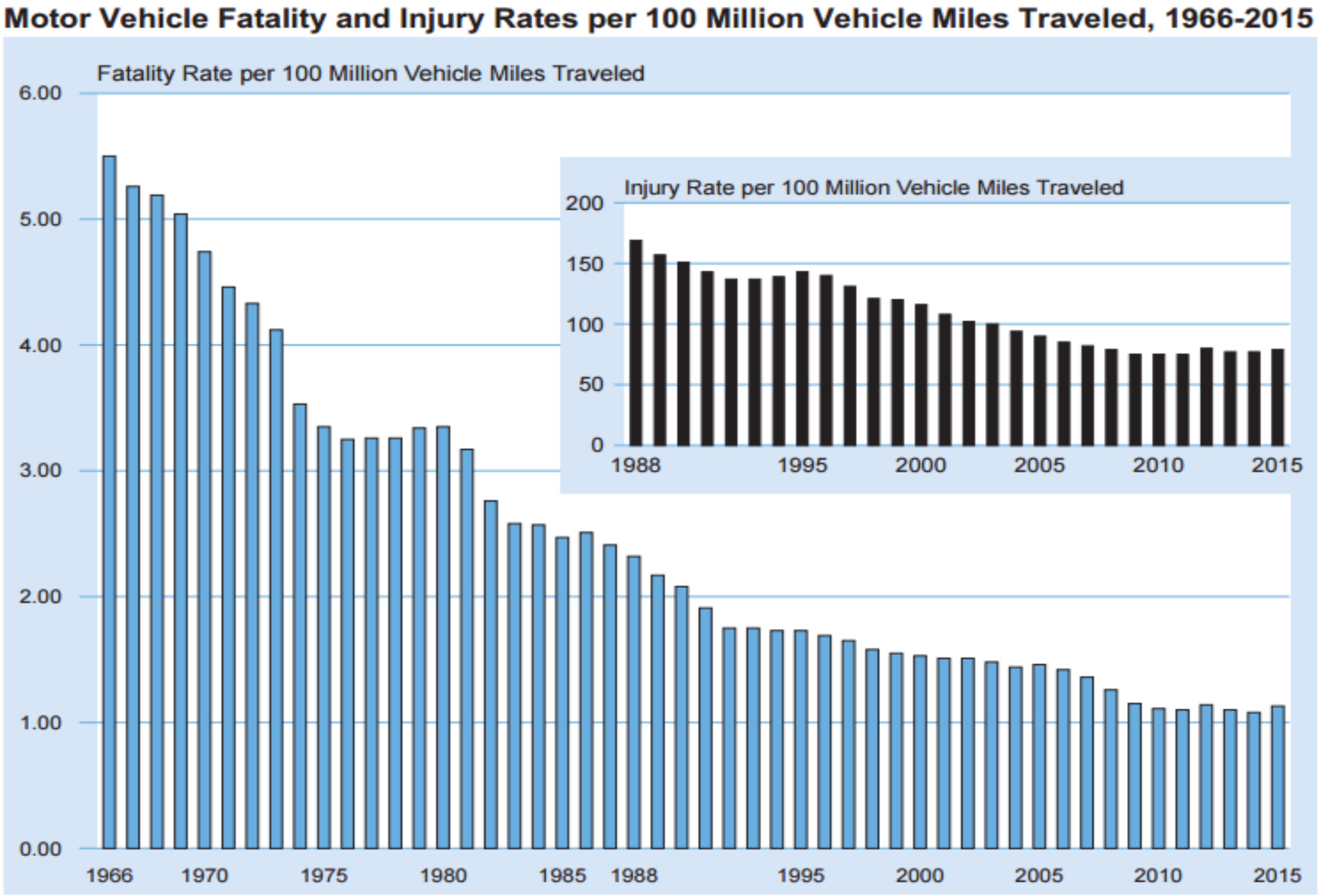
Model-based design (MBD)

- Analyze and understand the requirements specification
- Develop computational model(s) of the system
  - Check the model against the real system
    - ``are you are building the right thing?'' (validation)
  - Check the model against specifications
    - ``are you building it right?'' (verification)
- Build a prototype
  - test the prototype in the actual working environment
- Production

Fatal Crashes, 1975-2015



https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384



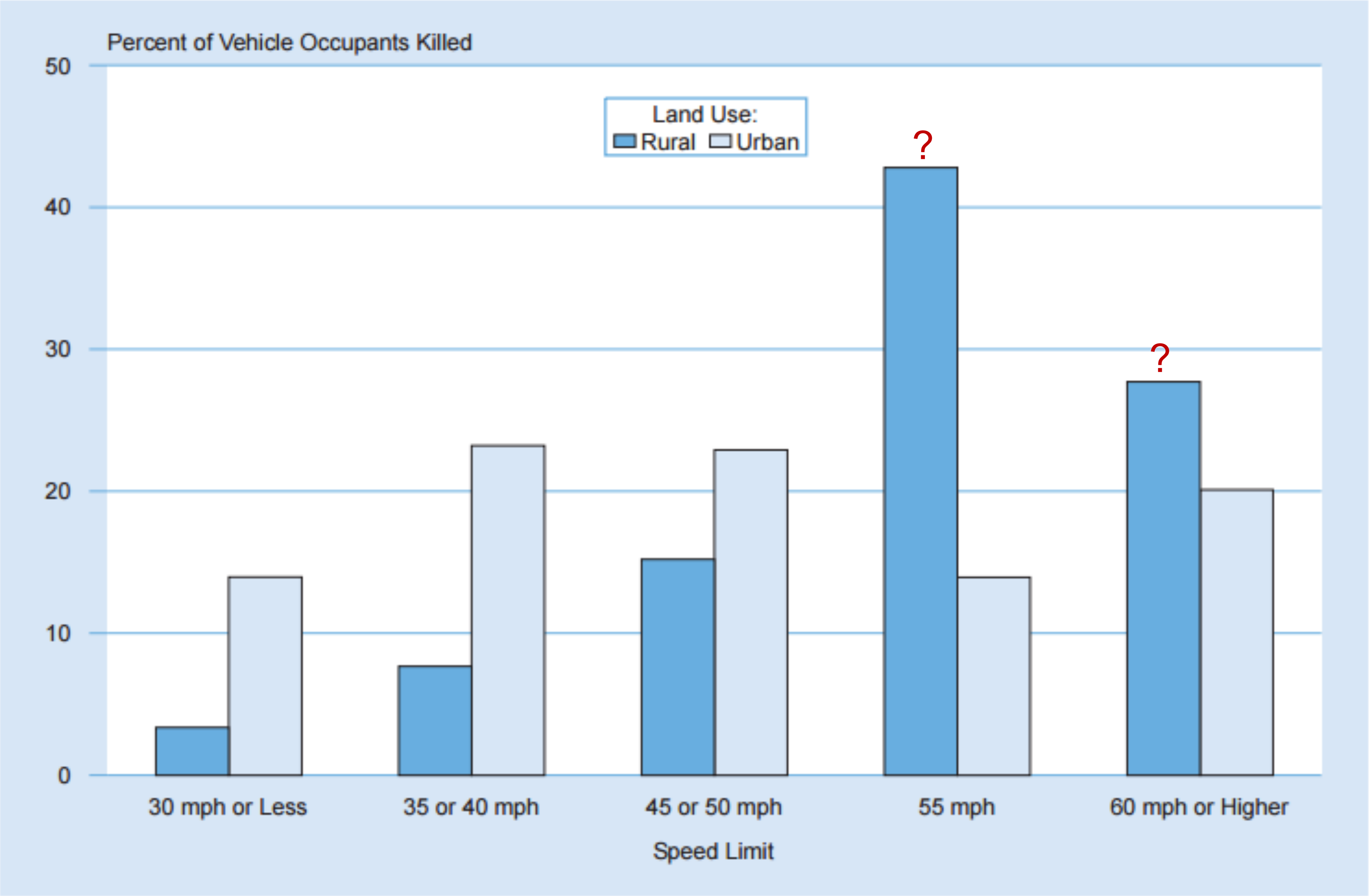
https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

Vehicles Involved in Fatal Crashes by Speed Limit and Land Use

Speed Limit	Land Use						Total	
	Rural		Urban		Unknown			
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
30 mph or less	707	15.8	3,033	67.9	725	16.2	**4,465**	**100.0**
35 or 40 mph	1,707	20.6	5,523	66.5	1,071	12.9	**8,301**	**100.0**
45 or 50 mph	3,506	35.9	5,374	55.0	890	9.1	**9,770**	**100.0**
55 mph	9,743	74.8	2,928	22.5	351	2.7	**13,022**	**100.0**
60 mph or higher	6,600	60.0	4,152	37.7	254	2.3	**11,006**	**100.0**
No Statutory Limit	113	33.6	177	52.7	46	13.7	**336**	**100.0**
Unknown	629	31.1	1,187	58.7	207	10.2	**2,023**	**100.0**
Total	**23,005**	**47.0**	**22,374**	**45.7**	**3,544**	**7.2**	**48,923**	**100.0**

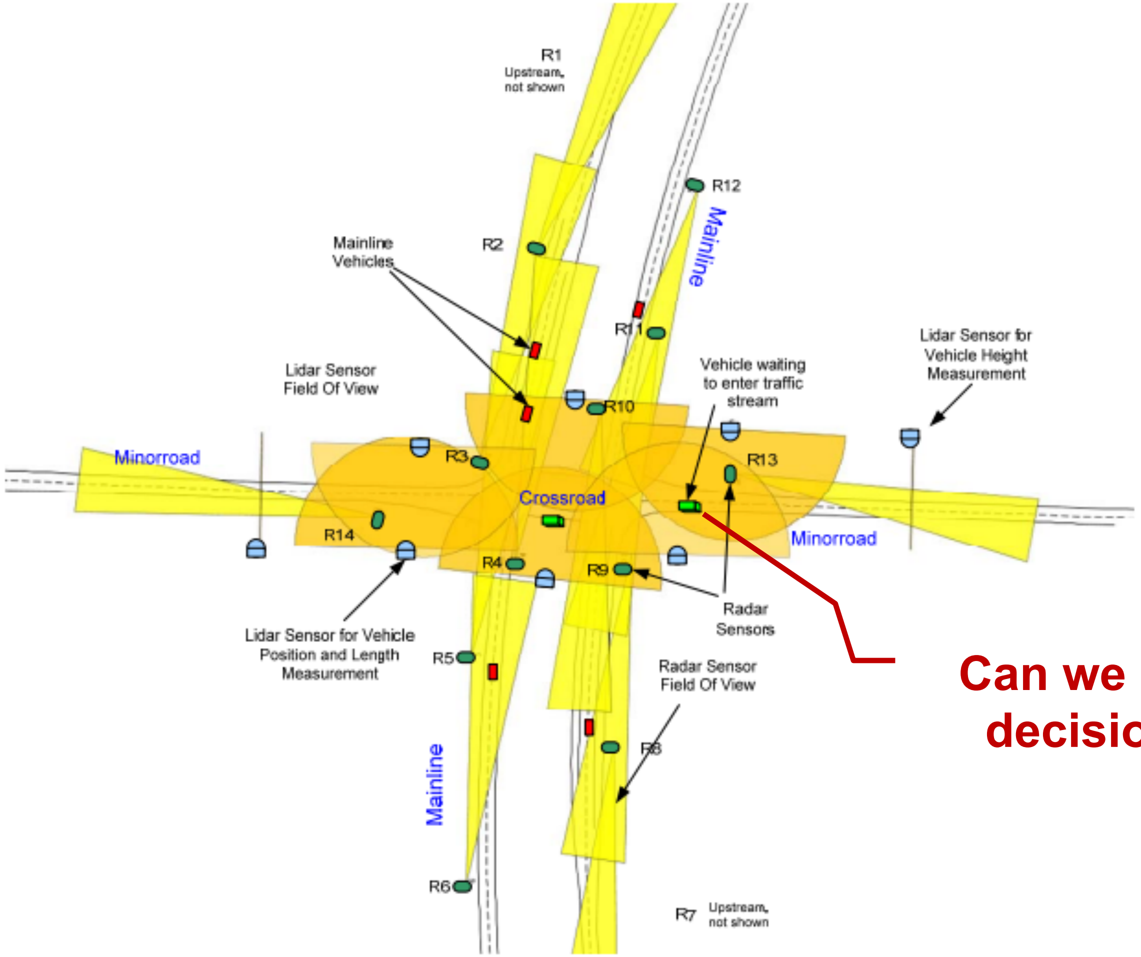
https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

Percent of Vehicle Occupants Killed, by Speed Limit and Land Use



https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

Cooperative Intersection Collision Avoidance System: Stop-Sign Assist (CICAS-SSA)



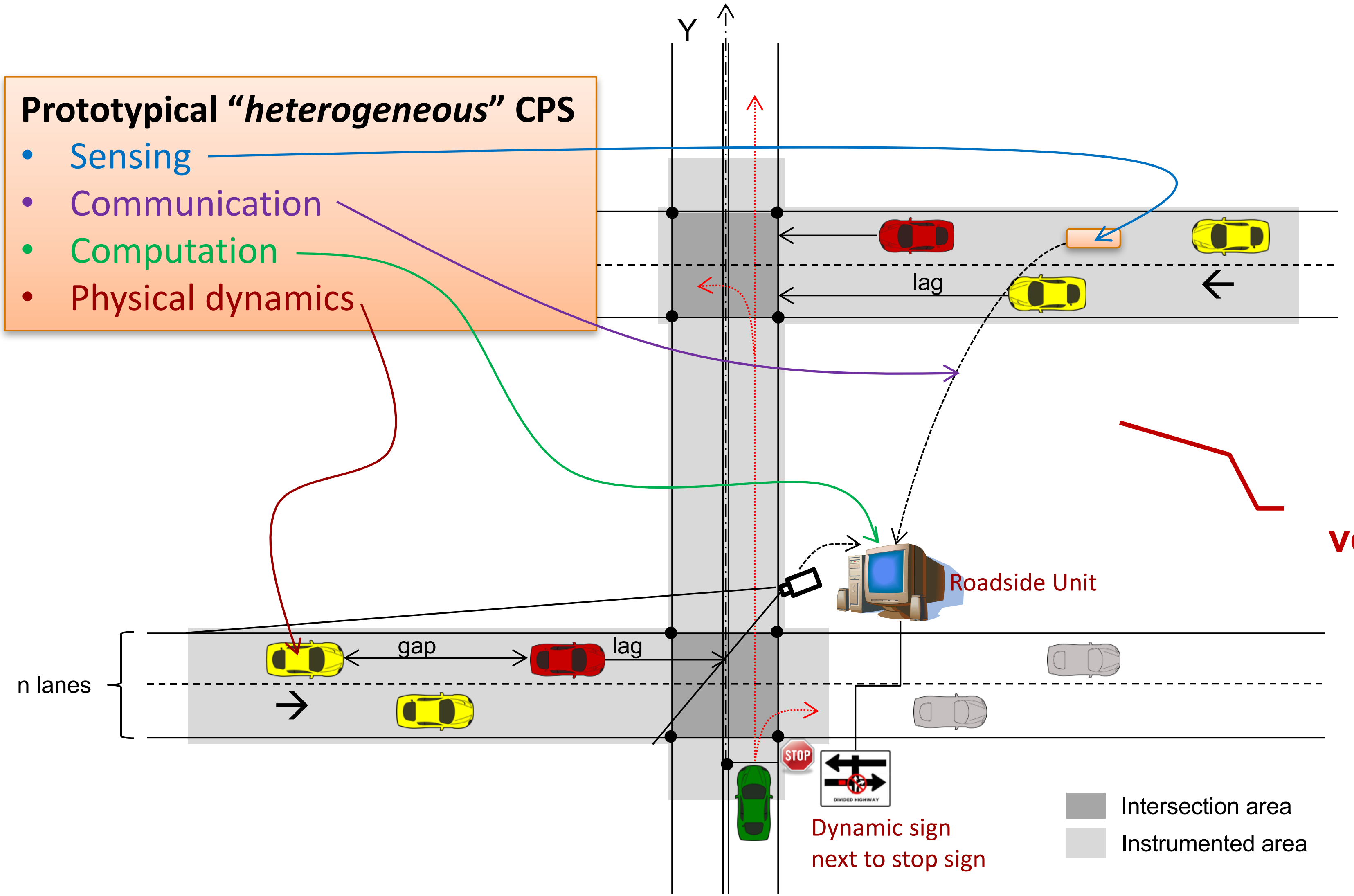
Can we assist in the decision making?

Figure 1: Plan view of a typical instrumented rural four lane expressway intersection. Sensors are radar (yellow triangles indicate field of view and) scanning lidar (orange semicircles); all data is sent from sensor processors to the main central processor.

http://www.dot.state.mn.us/guidestar/2006_2010/cicas/CICAS-SSA%20Report%202.pdf

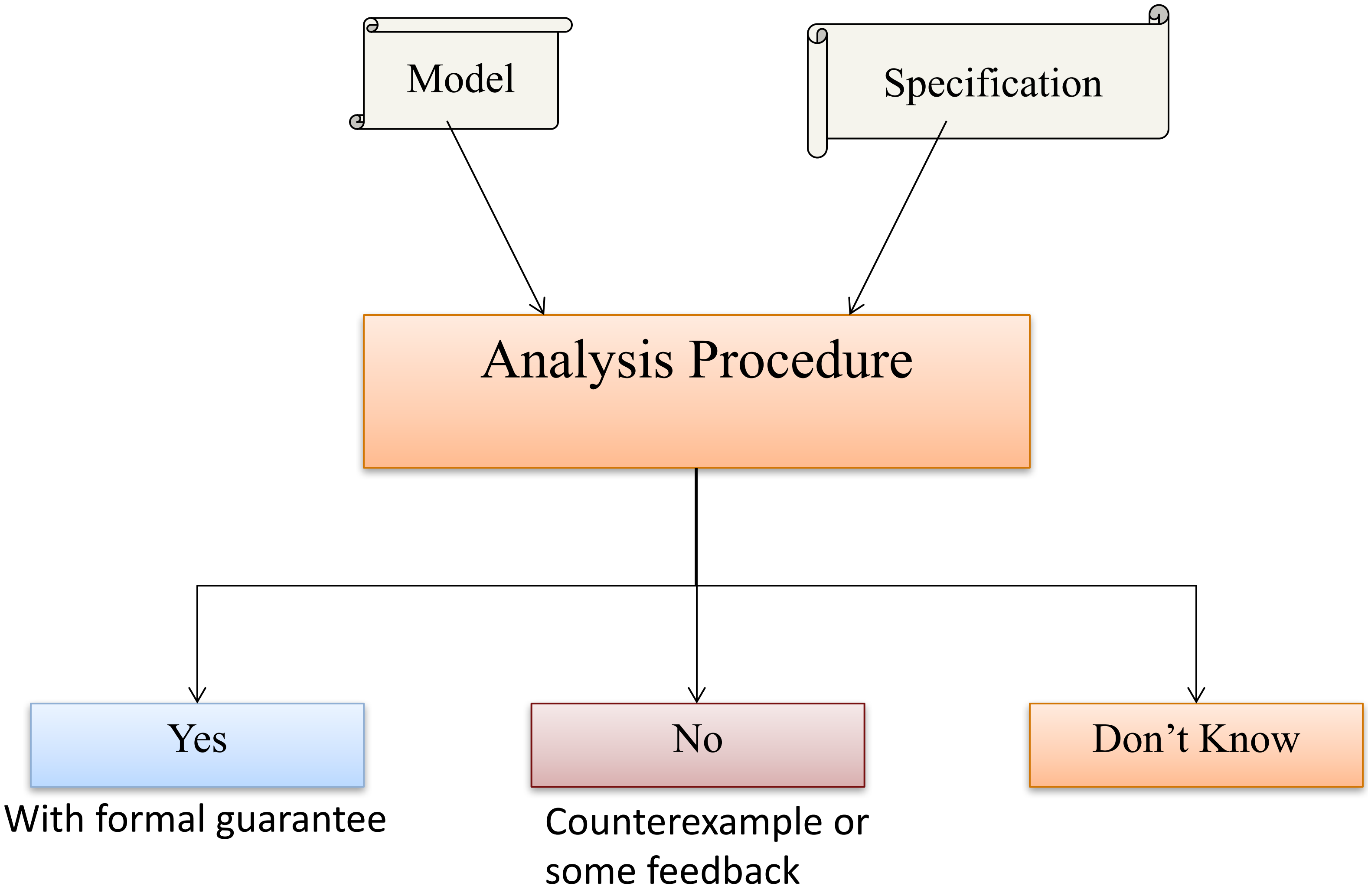
CICAS-SSA Schematic

Prototypical "*heterogeneous*" CPS
- Sensing
- Communication
- Computation
- Physical dynamics

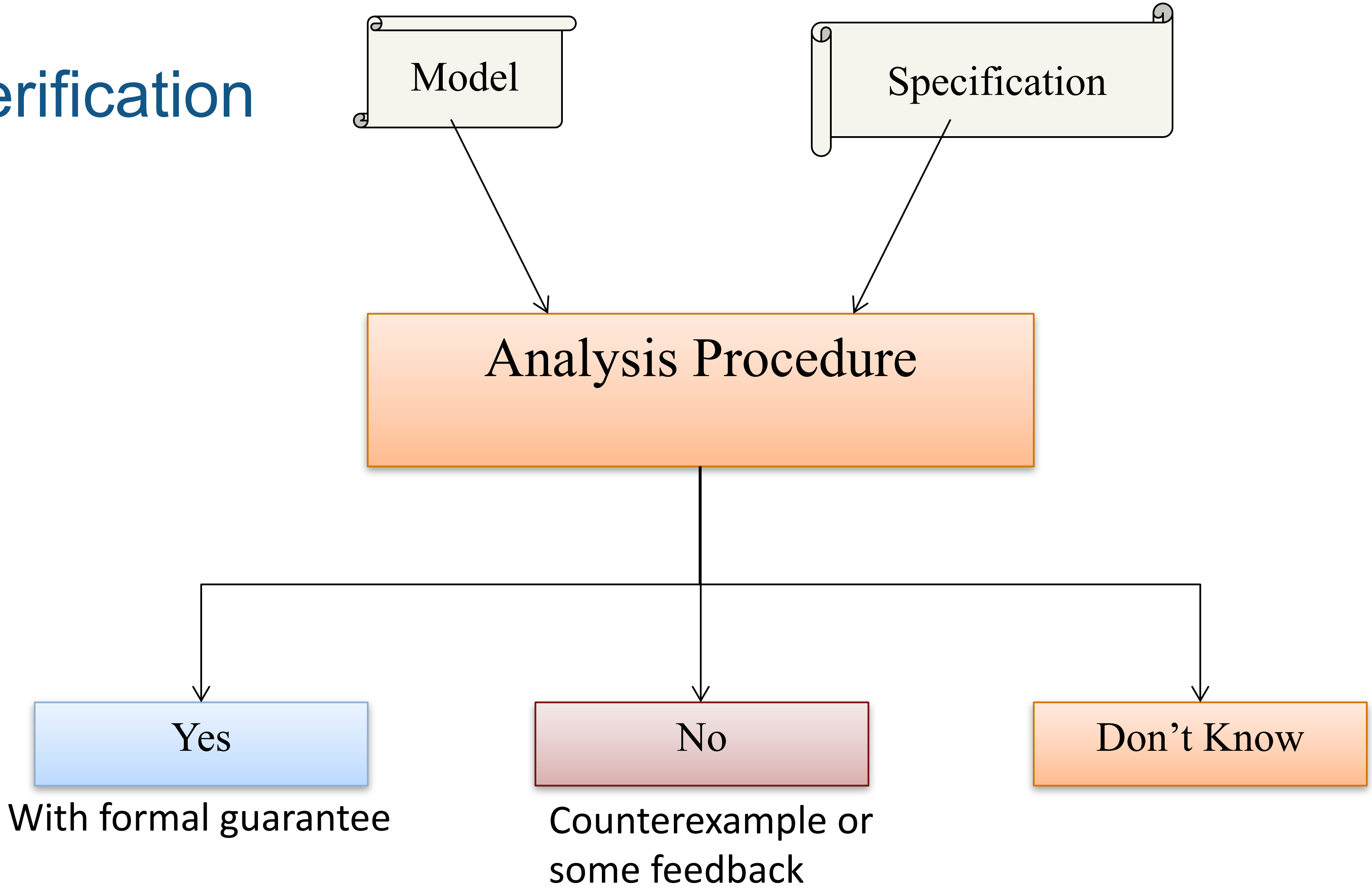


Can we formally verify such a system?

Formal Verification



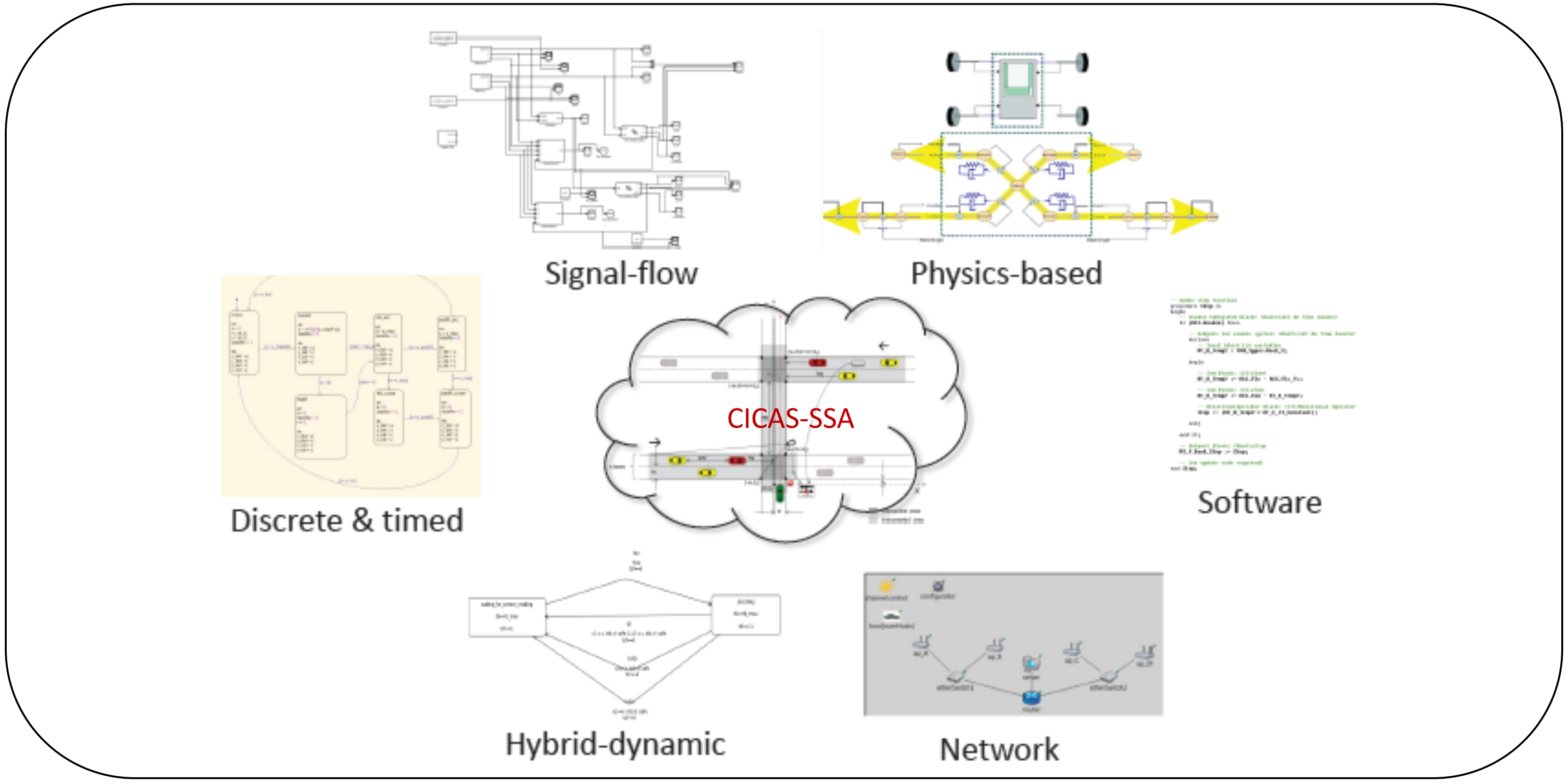
Formal Verification



There is no system model!

But there are models…

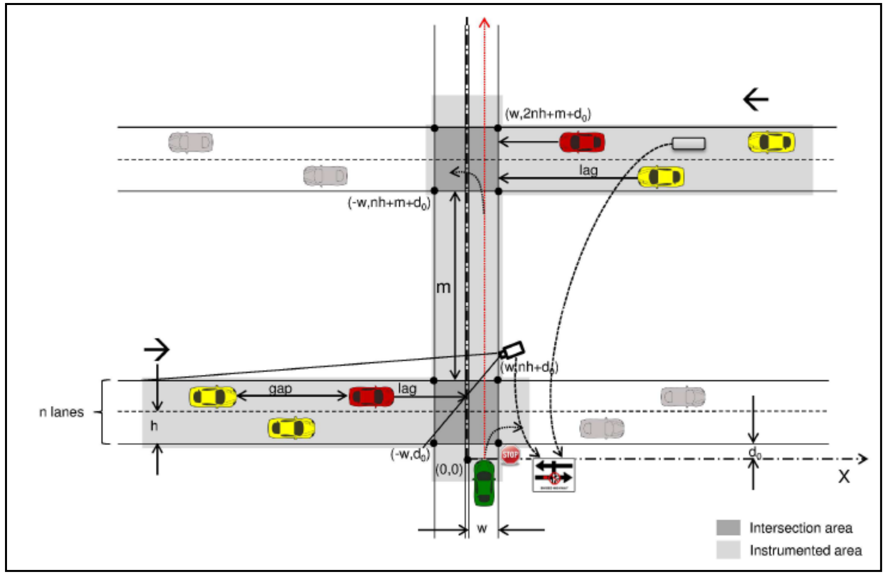
Heterogeneity in modeling formalisms and analysis techniques

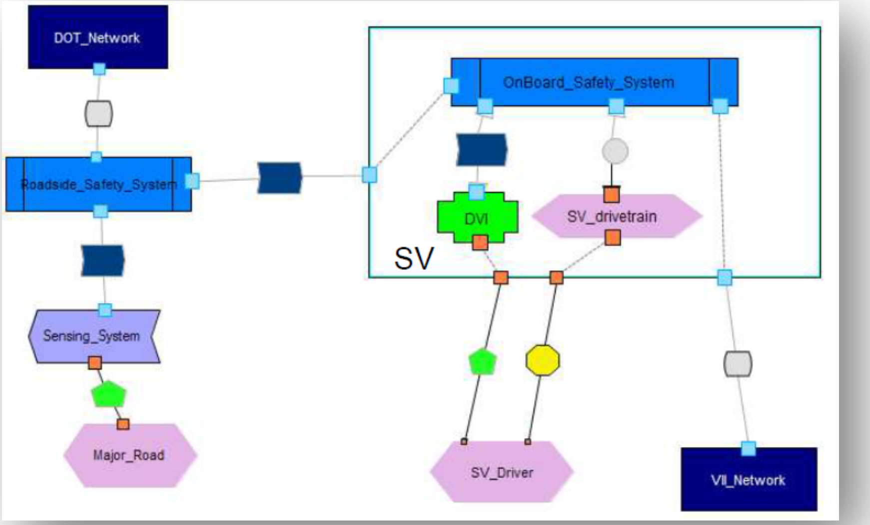


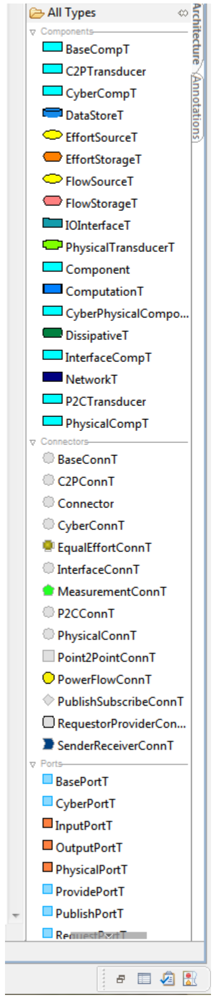
- *Different formalisms suited for different aspects of system design*
- Each model represents *some* design aspect well
- Models make *interdependent assumptions*
- *Tools work only with their formalisms*

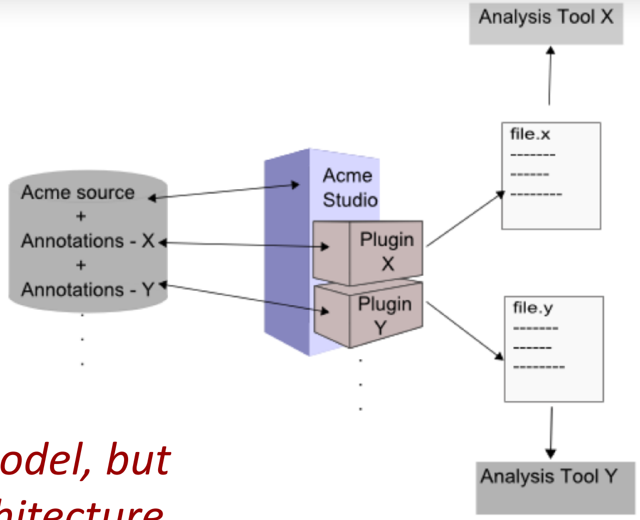
How do we ensure correctness of the system?

Cyber-Physical System Architecture

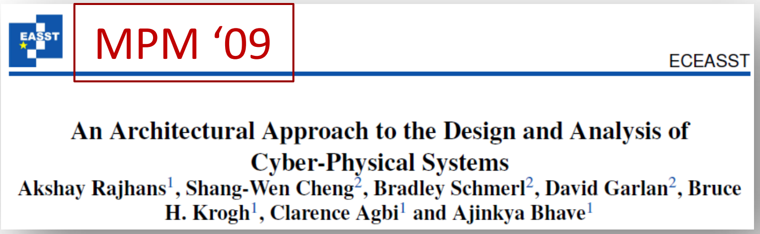








CPS architectural style palette in AcmeStudio


MPM '09

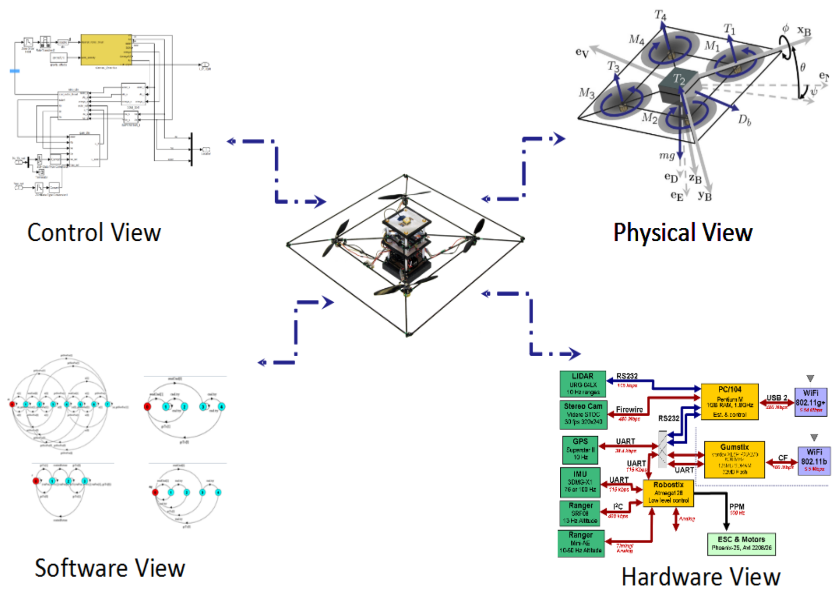
ECEASST

An Architectural Approach to the Design and Analysis of Cyber-Physical Systems

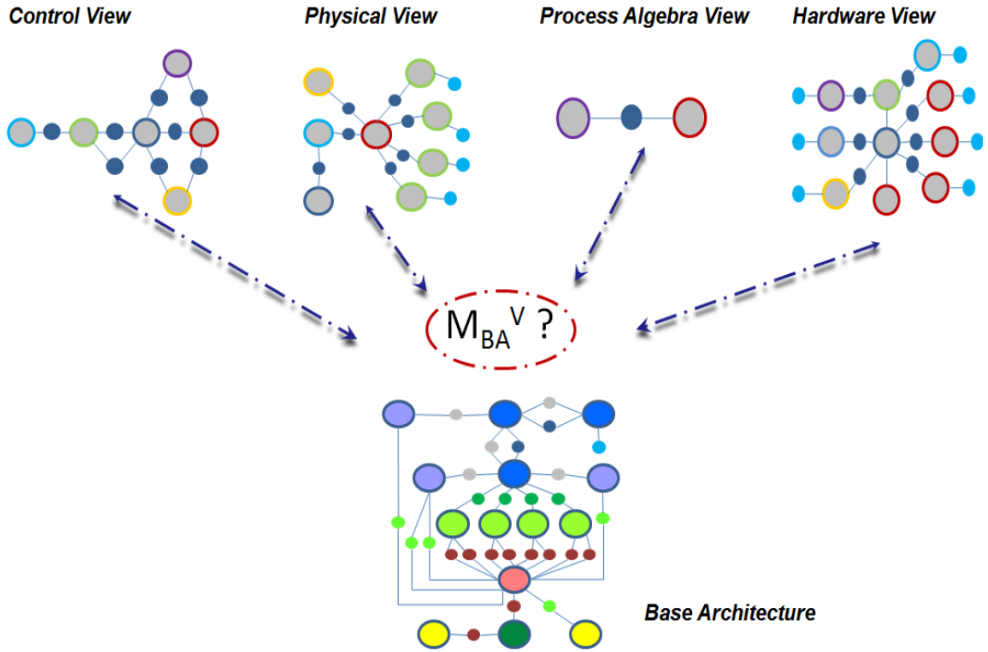
Akshay Rajhans[1], Shang-Wen Cheng[2], Bradley Schmerl[2], David Garlan[2], Bruce H. Krogh[1], Clarence Agbi[1] and Ajinkya Bhave[1]

There is no system model, but there is a system architecture

Architectural views



Models as architectural views



Structural consistency using graph morphisms

Augmenting Software Architectures with Physical Components

Ajinkya Bhave[1], David Garlan[2], Bruce H. Krogh[1], Akshay Rajhans[1], Bradley Schmerl[2]

[1]Dept. of Electrical and Computer Engineering
[2]School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3890 USA
email: {ajinkya@ | garlan@cs.| krogh@ece.| arajhans@ece.| schmerl@cs.}cmu.edu

ERTS² '10

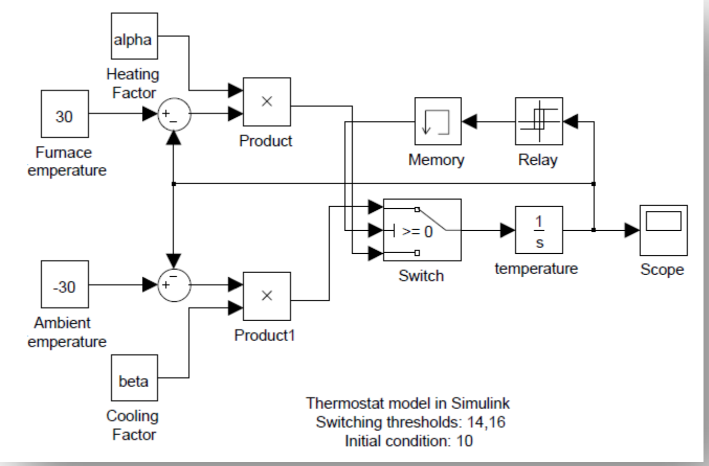
View Consistency in Architectures for Cyber-Physical Systems

ICCPS '11

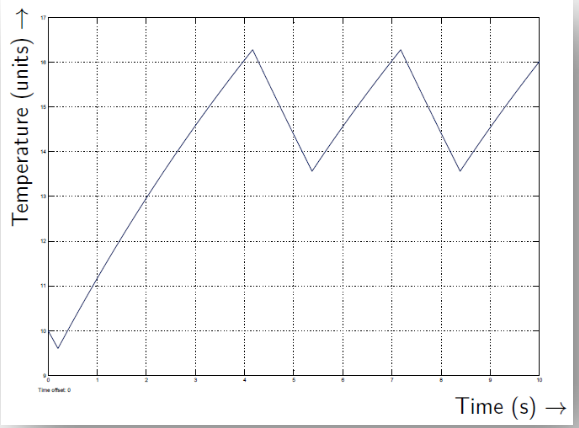
Ajinkya Bhave, Bruce H. Krogh   David Garlan, Bradley Schmerl

"Model structure vs system structure"
Analysis: Consistency, completeness

Semantic domains of models and specifications



Model M

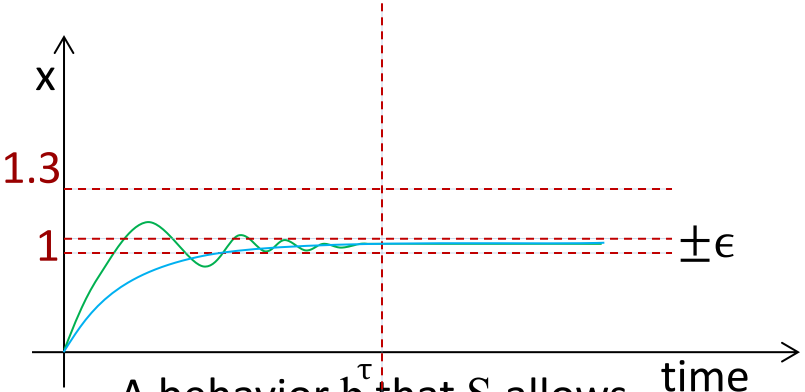


A behavior b that M exhibits

1) “overshoot is no more than 1.3 units and settling time is less than τ”

2) $\square(x < 1.3) \land \diamond_{\tau} (x \in [1 \pm \epsilon])$

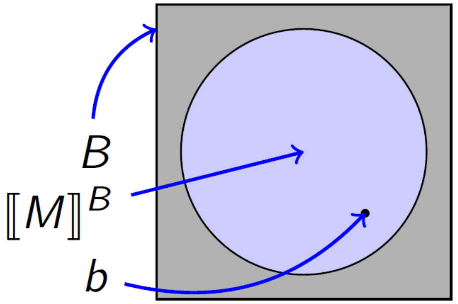
Specification S



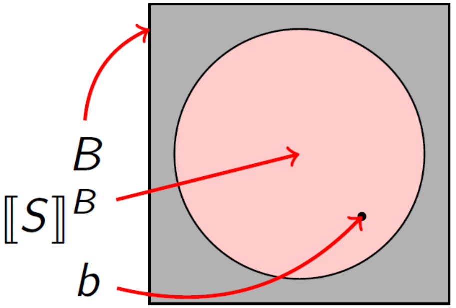
A behavior b that S allows

$$M \models^{B} S$$

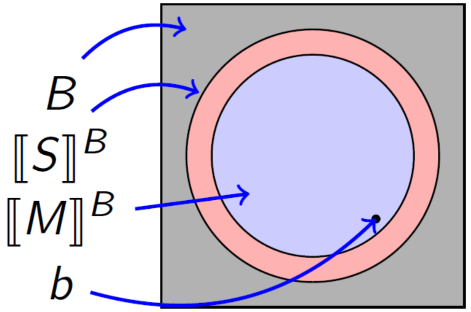
$$[\![M]\!]^{B} \subseteq [\![S]\!]^{B}$$



$[\![M]\!]^{B}$: “semantic interpretation” of M in a behavior domain B



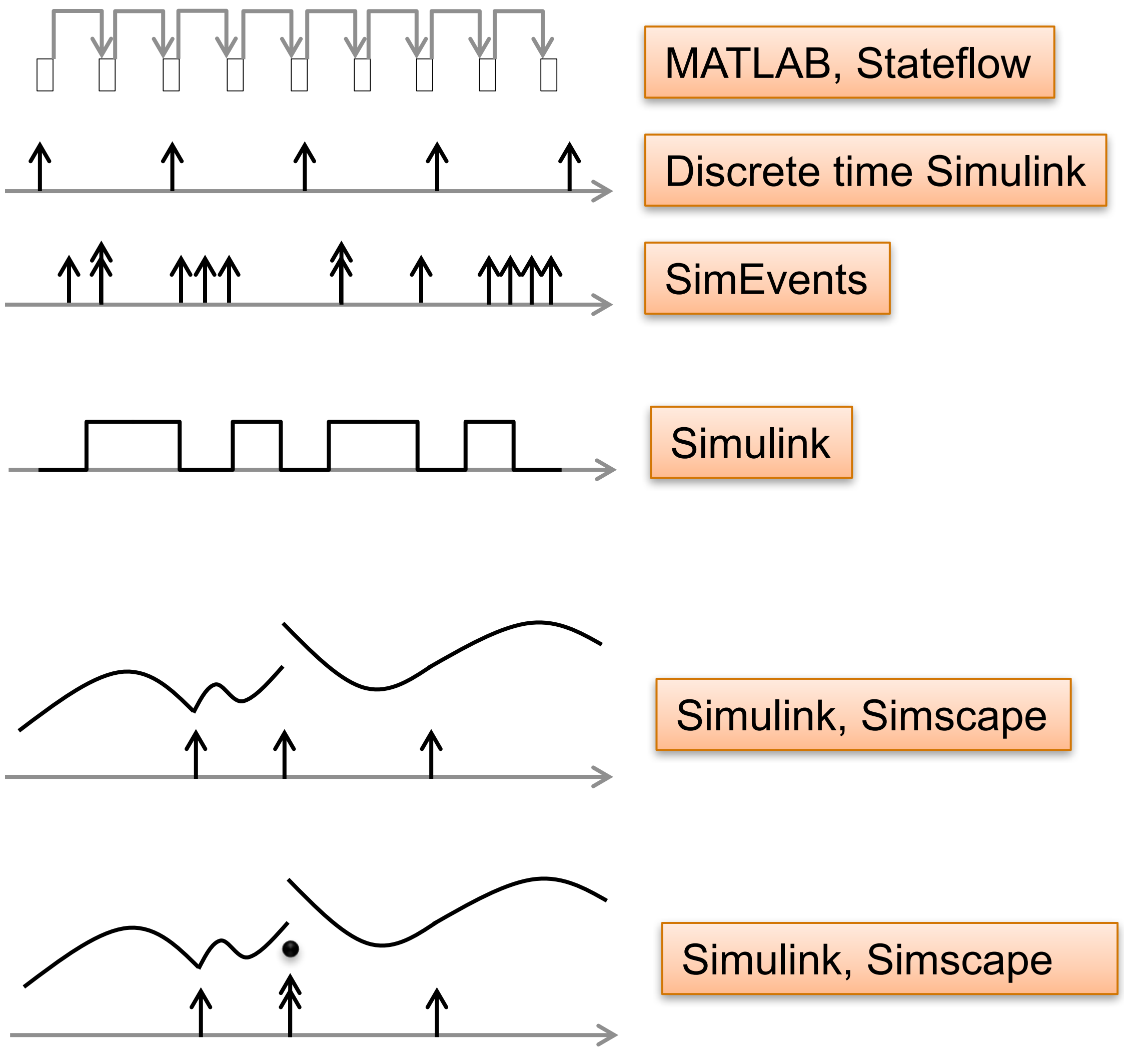
$[\![S]\!]^{B}$: “semantic interpretation” of S in B



Behavior domains B precisely defined in behavior formalisms B (e.g., *discrete traces, continuous trajectories, hybrid traces*)

The semantic domain of a dynamic system

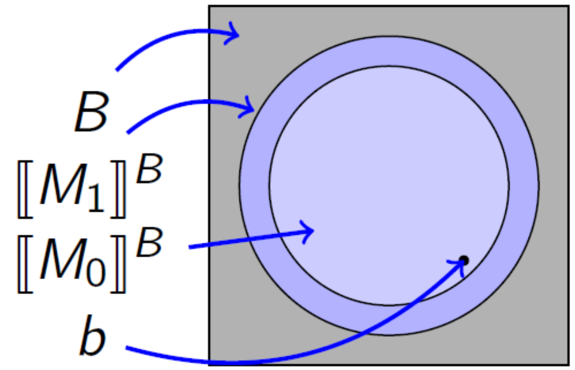
- Points, [ ]
  - On **N**
  - On **R** x **N**
- Intervals, [⟩ (⟨ ⟩, ⟨])
  - On **R**
- Hybrid point/interval
  - On **R**
  - On **R** x **N**



Abstraction and Implication

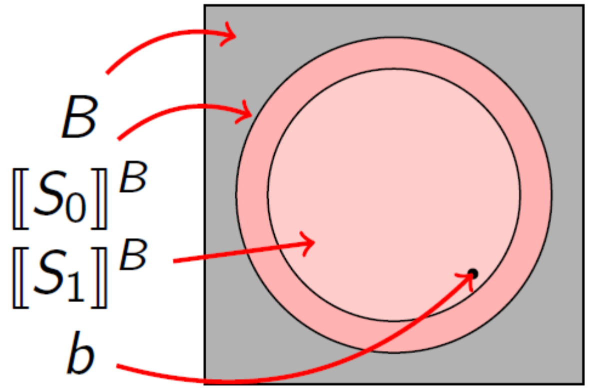
- Model M_1 abstracts M_0 in B, written $M_0 \sqsubseteq^B M_1$

  if $[\![M_0]\!]^B \subseteq [\![M_1]\!]^B$



- Specification S_1 implies S_0 in B, written $S_1 \Rightarrow^B S_0$

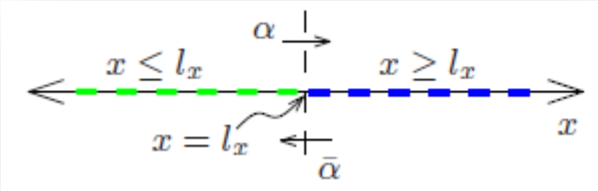
  if $[\![S_1]\!]^B \subseteq [\![S_0]\!]^B$

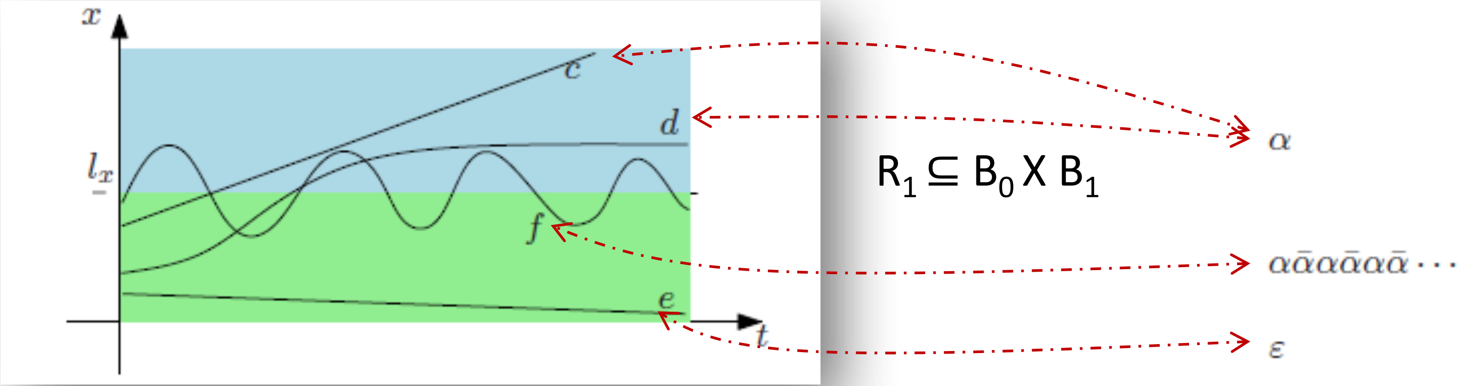


Mappings between semantic domains via behavior relations

- *Approach:* Create “behavior relations” between domains

Example





B_0 : 1-d continuous trajectories in x

$B_1 = \{\alpha, \bar{\alpha}\}^* \cup \{\alpha, \bar{\alpha}\}^\omega$

Given $R_1 \subseteq B_0 \times B_1$
set-based inverse map
R_1^{-1}(‘α’)={c,d,…}

Heterogeneous Abstraction and Implication

- Heterogeneous extensions of behavior-set inclusions

Heterogeneous Abstraction

$M_0 \sqsubseteq^{R_1} M_1$, if

A $\quad [\![M_0]\!]^{B_0} \subseteq R_1^{-1}([\![M_1]\!]^{B_1})$.

Heterogeneous Specification Implication

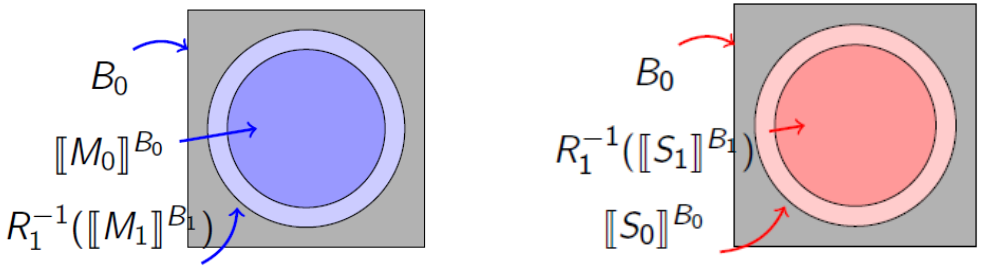
$S_1 \Rightarrow^{R_1} S_0$, if

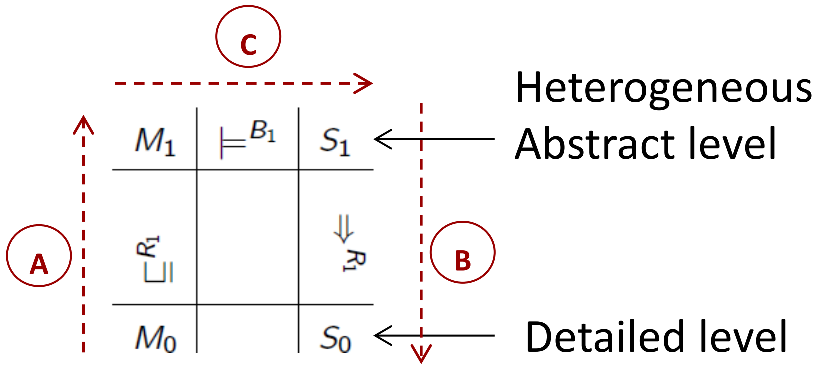
B $\quad R_1^{-1}([\![S_1]\!]^{B_1}) \subseteq [\![S_0]\!]^{B_0}$.

Heterogeneous Verification

If $M_0 \sqsubseteq^{R_1} M_1$, $M_1 \models^{B_1} S_1$ and $S_1 \Rightarrow^{R_1} S_0$, then $M_0 \models^{B_0} S_0$. C

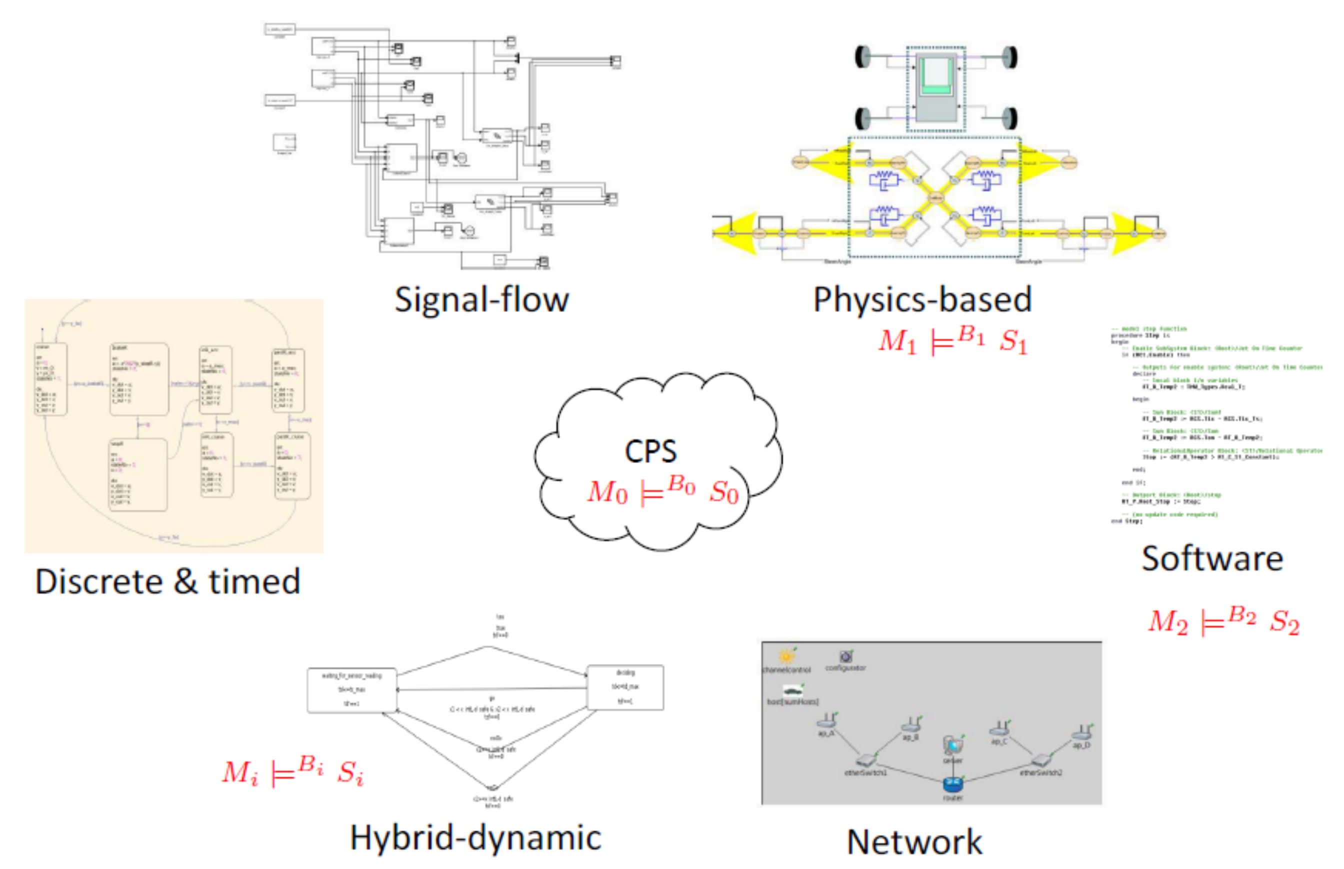
(in words)





(pictorially)

Multi-model Verification Problem



How do we use $M_1 \models^{B_1} S_1, \ldots, M_n \models^{B_n} S_n$ to infer $M_0 \models^{B_0} S_0$?

Multi-model conjunctive and disjunctive heterogeneous verification

Conjunctive specification implication

Given behavior relations $R_i \subseteq B_0 \times B_i$, a set of specifications $S_1, \ldots S_n$ *conjunctively imply* S_0 if $\bigcap_i R_i^{-1}([\![S_i]\!]^{B_i}) \subseteq [\![S_0]\!]^{B_0}$.

Model coverage (disjunctive abstraction)

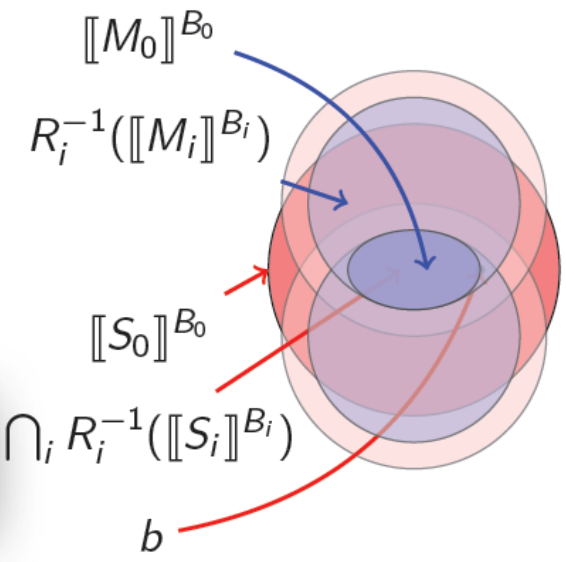
Given behavior relations $R_i \subseteq B_0 \times B_i$, a set of models $M_1, \ldots M_n$ *cover* M_0 if $[\![M_0]\!]^{B_0} \subseteq \bigcup_i R_i^{-1}([\![M_i]\!]^{B_i})$.

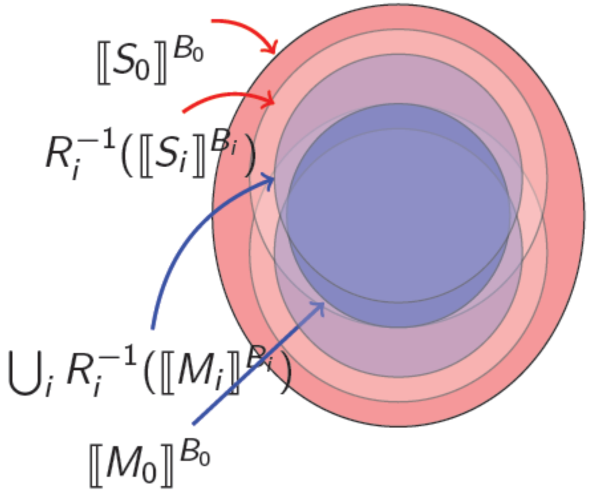
Typical use case

- Each model captures a different aspect
- Specs pertain to only the relevant one

Typical use case

- Each model captures a different subset of behaviors, e.g., a specific nondeterministic choice





Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

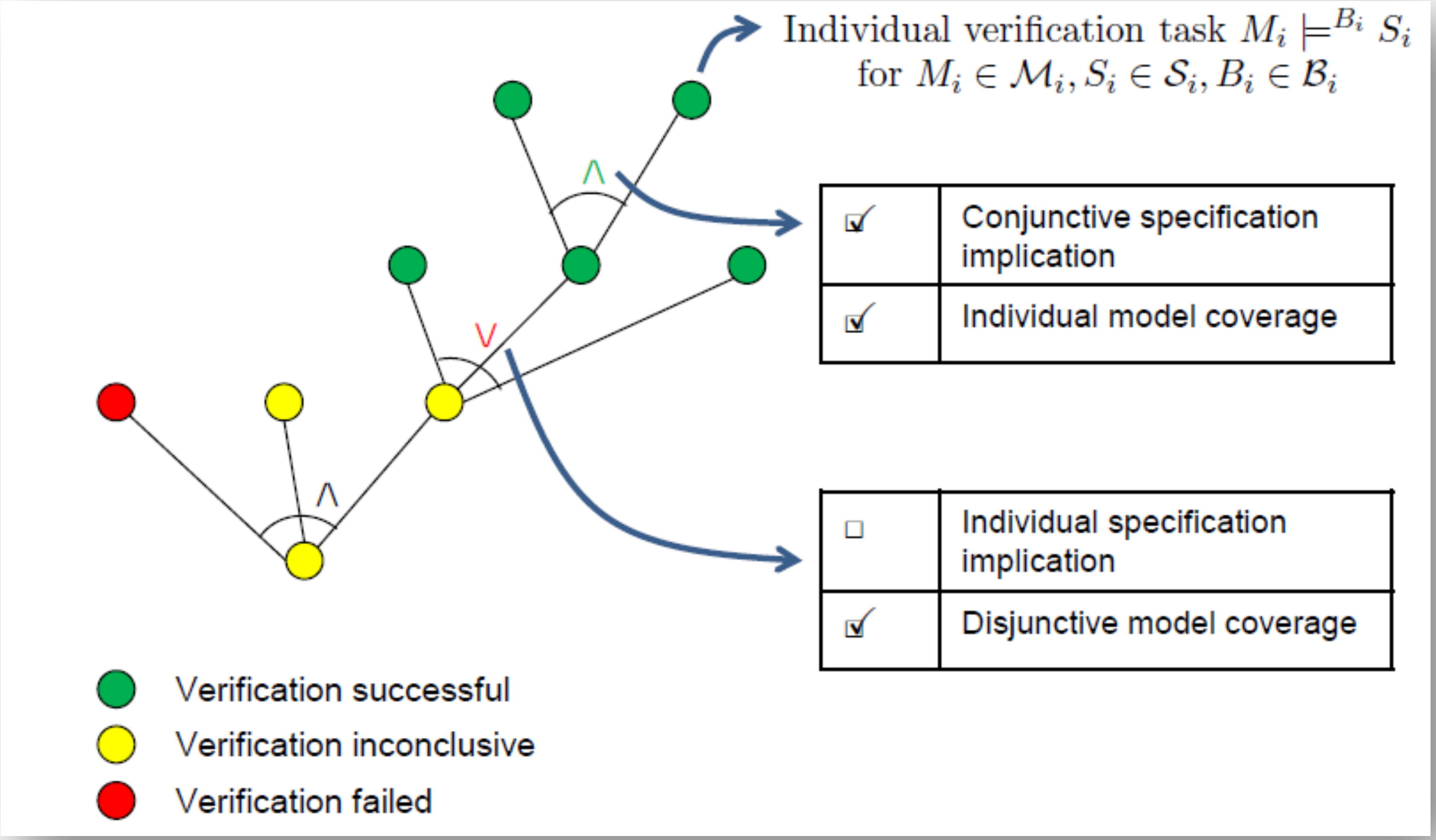
HSCC '12

Akshay Rajhans
arajhans@ece.cmu.edu

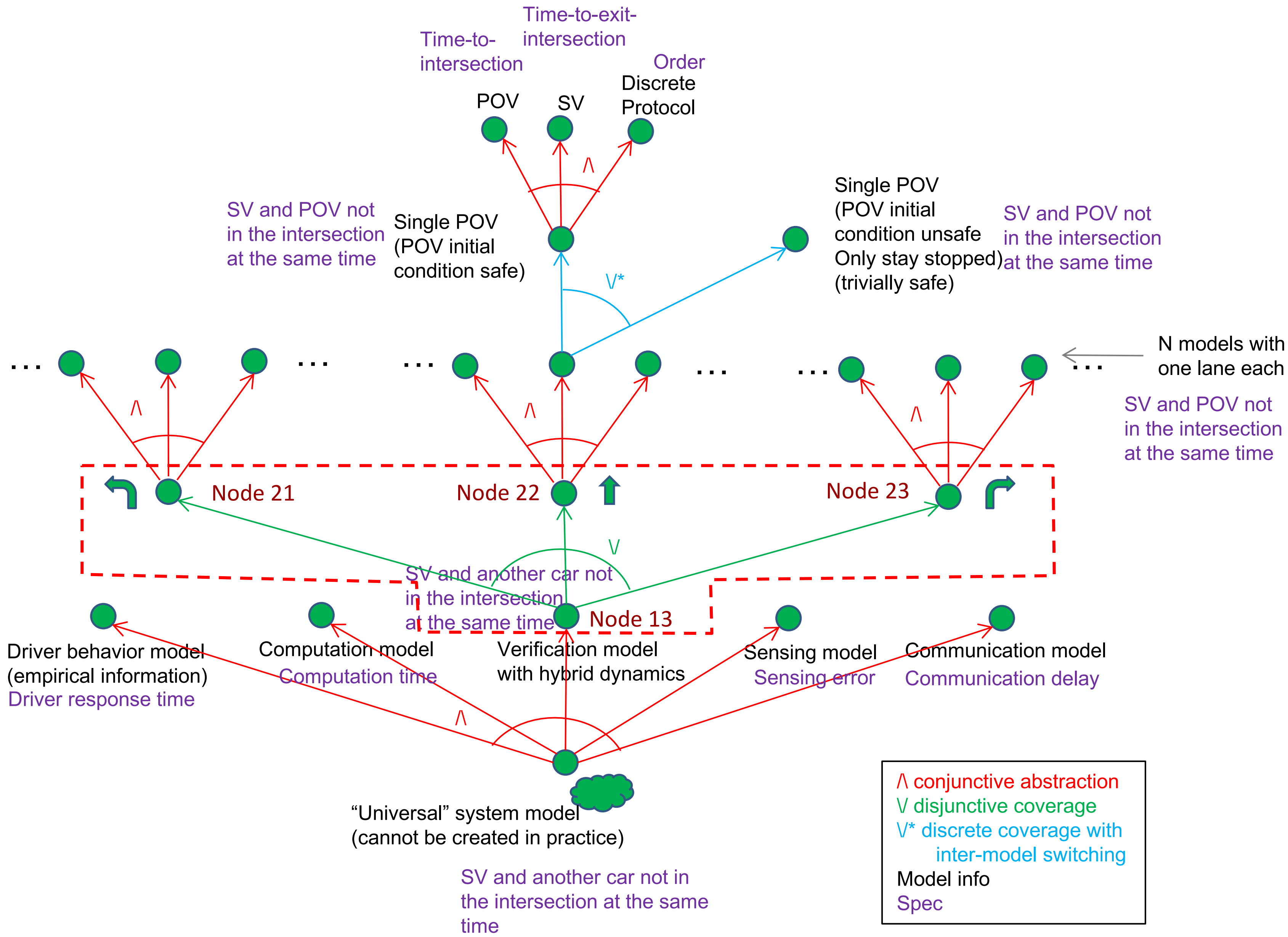
Bruce H. Krogh
krogh@ece.cmu.edu

Hierarchical Verification

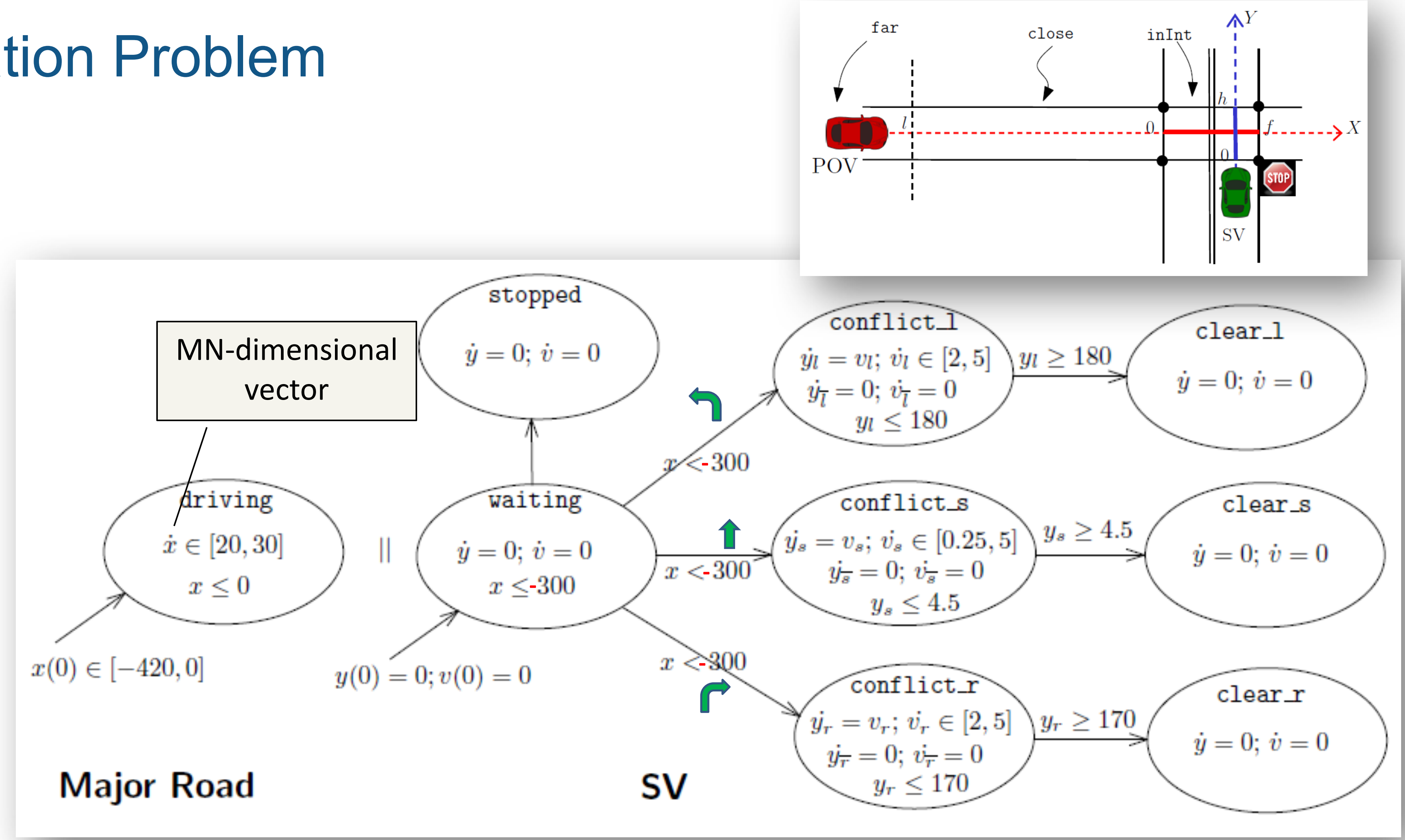
Conjunctive and disjunctive verification constructs can be nested arbitrarily



Heterogeneous Verification of CICAS



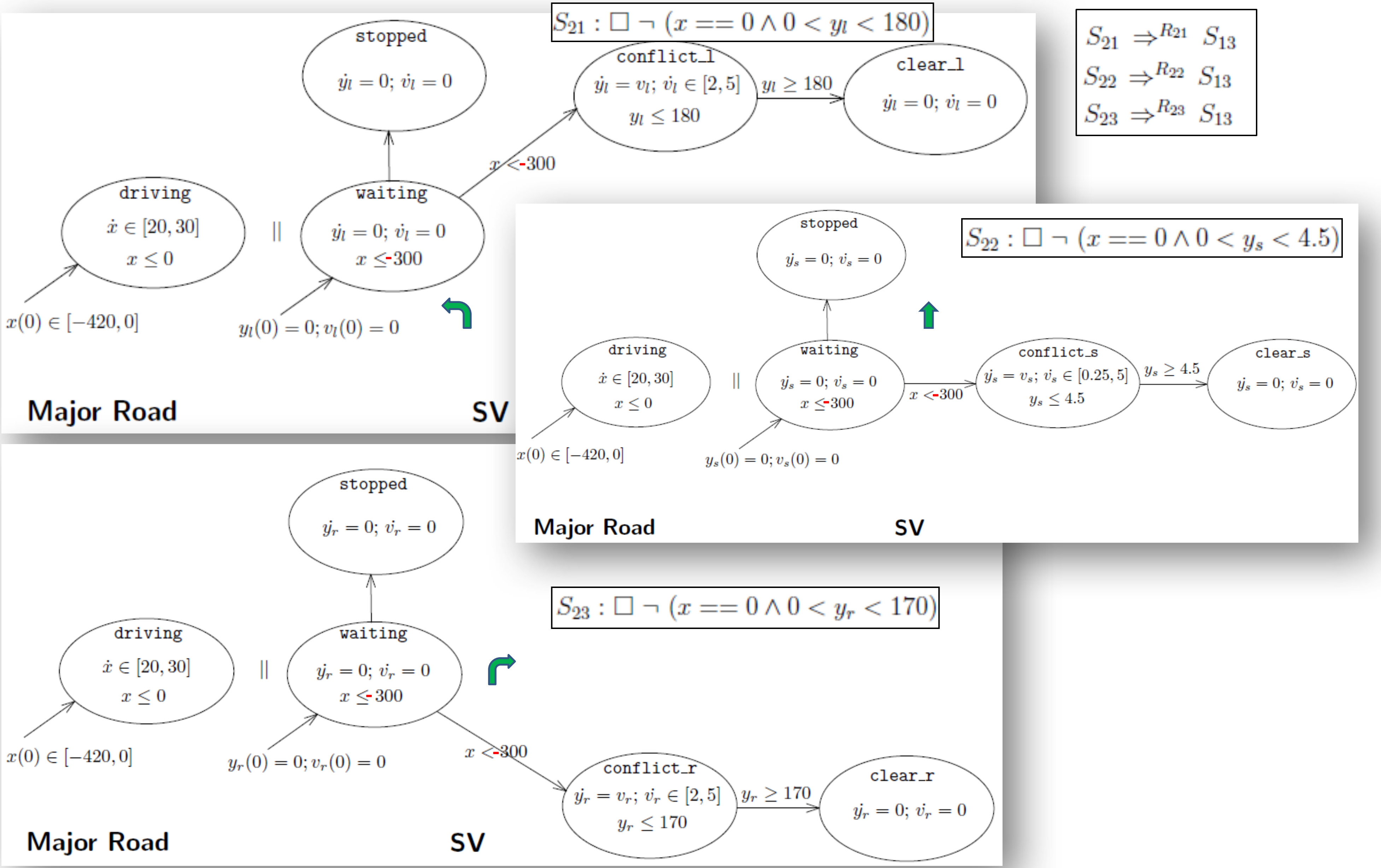
Verification Problem



Verification objective: "SV and another car are never in the intersection at the same time"

$$\square \neg ((x == 0 \wedge 0 < y_s < 4.5) \vee (x == 0 \wedge 0 < y_r < 170)) \vee (x == 0 \wedge 0 < y_l < 180))$$

Disjunctive Heterogeneous Verification

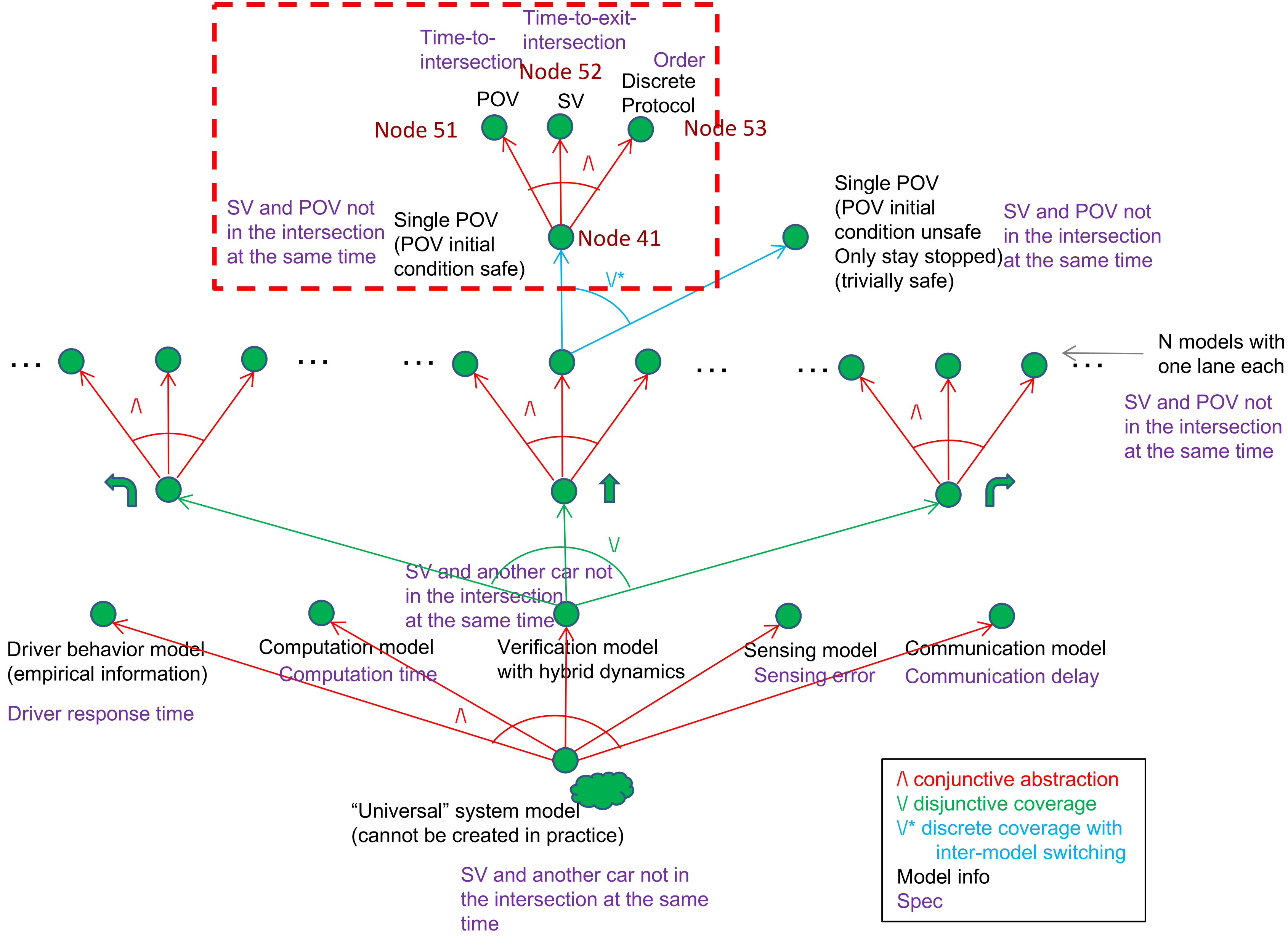


$S_{21} \Rightarrow^{R_{21}} S_{13}$

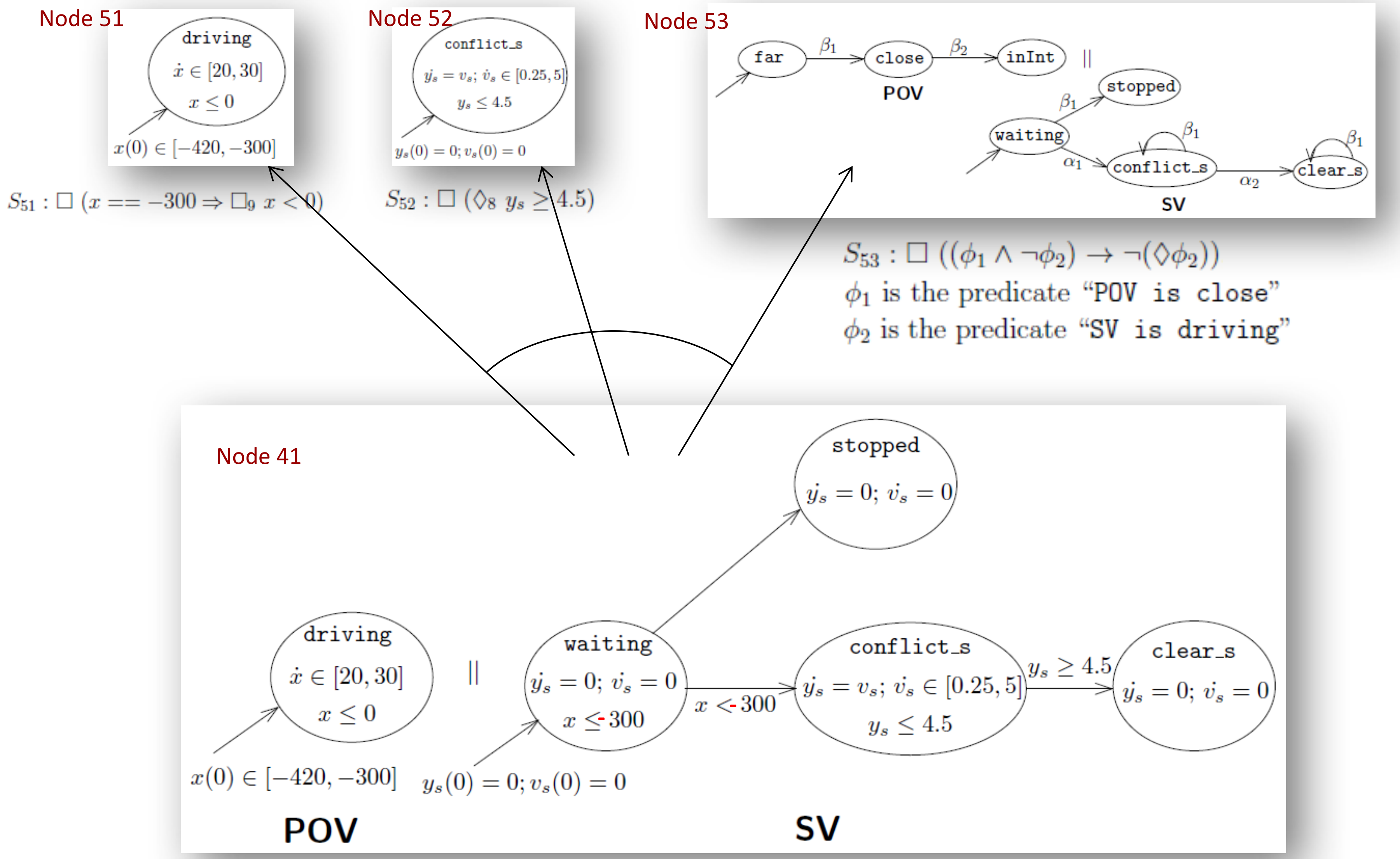
$S_{22} \Rightarrow^{R_{22}} S_{13}$

$S_{23} \Rightarrow^{R_{23}} S_{13}$

Heterogeneous verification of CICAS-SSA

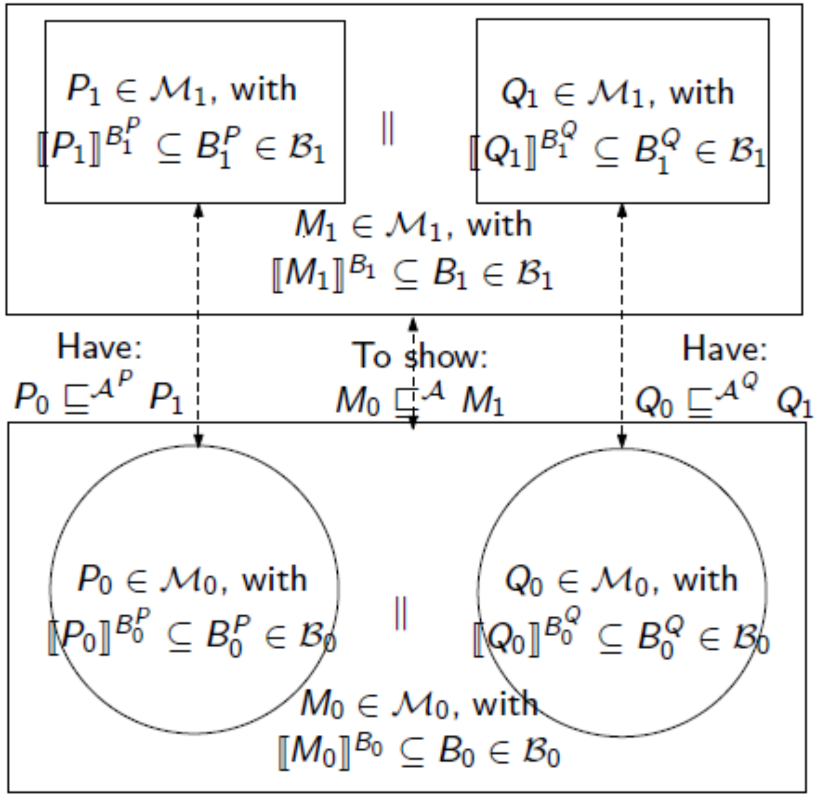


Conjunctive Heterogeneous Verification



$S_{41} : \Box\ \neg\ (x == 0 \wedge 0 < y_s < 4.5)$

Leveraging Compositionality for Heterogeneous Abstraction



Schematic

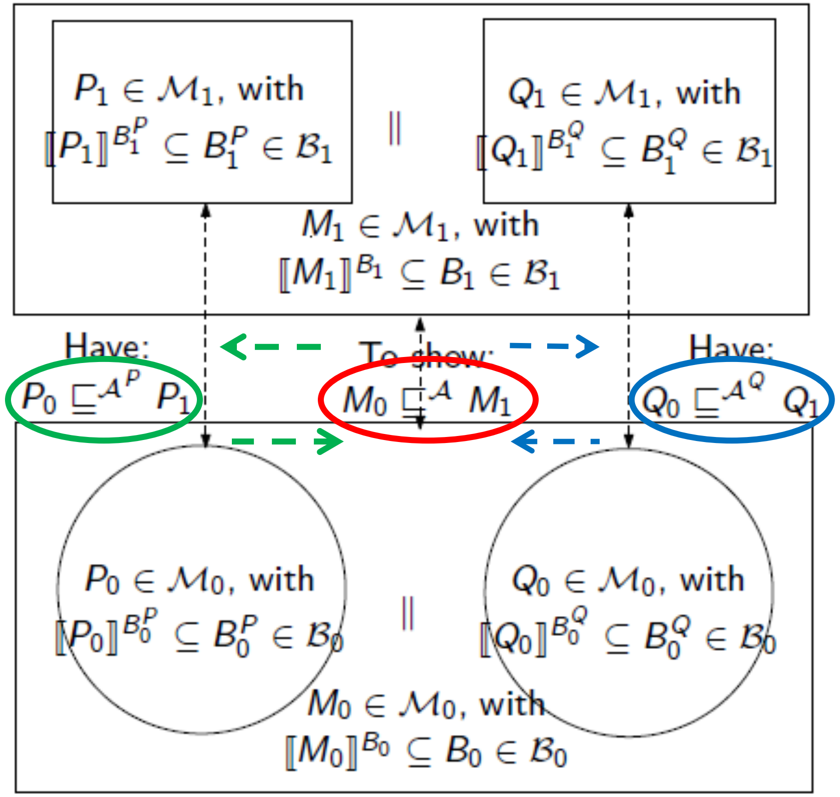
Objective: Conclude heterogeneous abstraction of the composition by establishing that of the components

Rationale: Component's local semantics defined in a behavior domain of smaller dimension

Need

- Behavior abstraction functions $\mathcal{A}$: behavior relations that are also functions
- Mappings between local/global behavior domains of the same type
- Mappings between local/global abstraction functions

Compositionality Conditions



"Models as composition of components"
Analysis: Compositional Abstraction

Centralized Development

Start with $\mathcal{A}$, *localize* to get $\mathcal{A}^{\mathcal{P}}$, $\mathcal{A}^{\mathcal{Q}}$

If localizations of $\mathcal{A}$ are $\mathcal{A}^{\mathcal{P}}$ and $\mathcal{A}^{\mathcal{Q}}$, then compositional heterogeneous abstraction via $\mathcal{A}$ holds

Decentralized Development

Start with $\mathcal{A}^{\mathcal{P}}$, $\mathcal{A}^{\mathcal{Q}}$, *globalize* to get $\mathcal{A}$

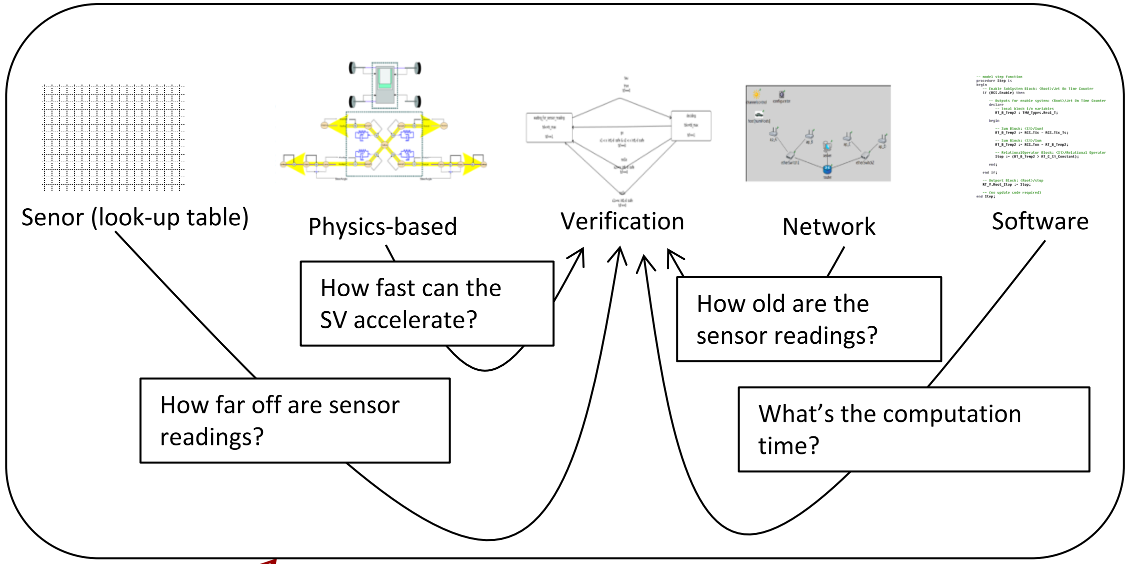
If globalizations of $\mathcal{A}^{\mathcal{P}}$, $\mathcal{A}^{\mathcal{Q}}$ are consistent (call it $\mathcal{A}$), then compositional heterogeneous abstraction via $\mathcal{A}$ holds

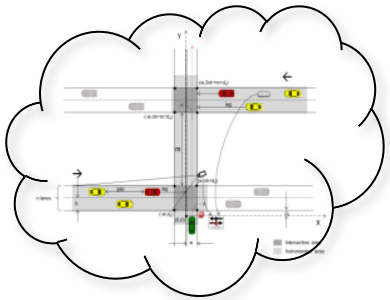

Compositional Heterogeneous Abstraction

HSCC '13

Akshay Rajhans   Bruce H. Krogh

Semantic Assumptions as Parameter Constraints





Dependencies that cut across modeling formalisms can be captured as parameter constraints

CDC '11

Using Parameters in Architectural Views to Support Heterogeneous Design and Verification

Akshay Rajhans†, Ajinkya Bhave†, Sarah Loos‡, Bruce H. Krogh†, André Platzer‡, David Garlan‡

Problem

- *Semantic interdependencies* across formalisms
- *Consistency*

Challenge

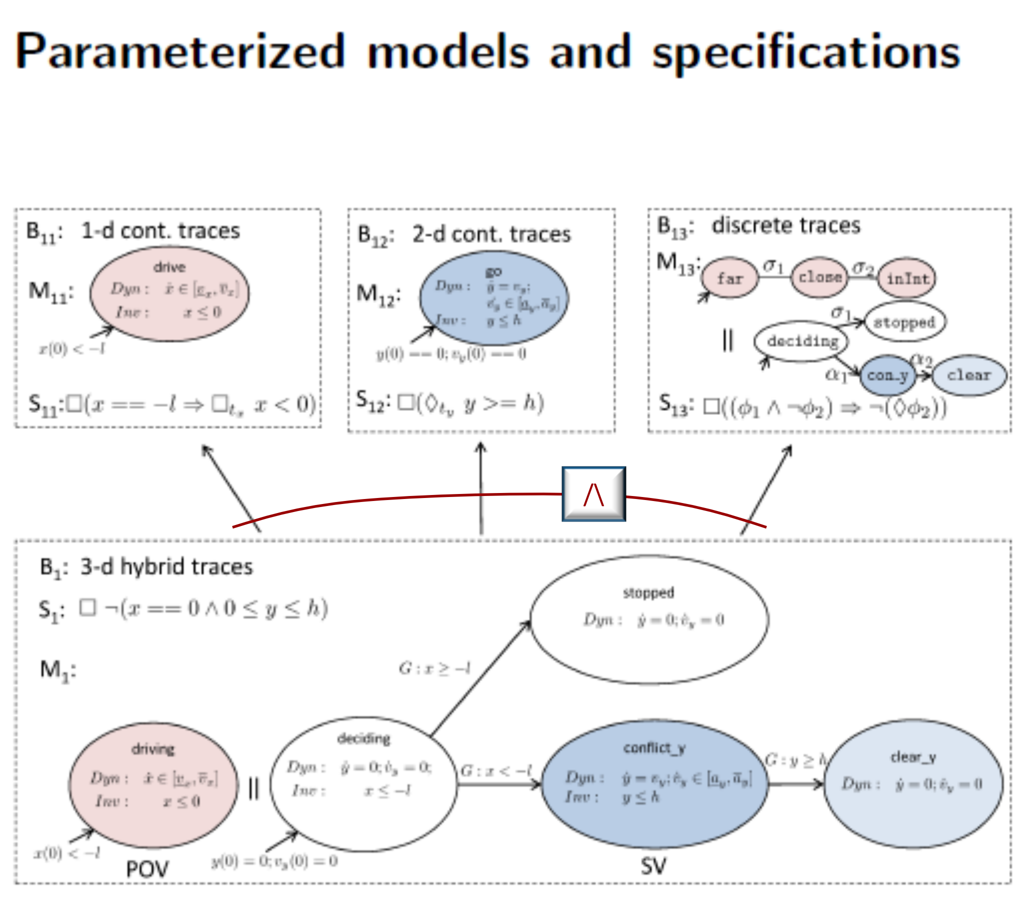
- *Formal representation* that is *universal* to all modeling formalisms

Approach

- interdependencies as an *auxiliary constraint on parameters*
- Find *effective constraint* on given model/spec. parameters (existential quantification)
- Use *SMT solvers* or *theorem provers* to prove consistency

Ensures semantic (parameter) consistency using external SMT solvers or provers

Parametric Verification of CICAS



Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

HSCC '12

Akshay Rajhans
arajhans@ece.cmu.edu

Bruce H. Krogh
krogh@ece.cmu.edu

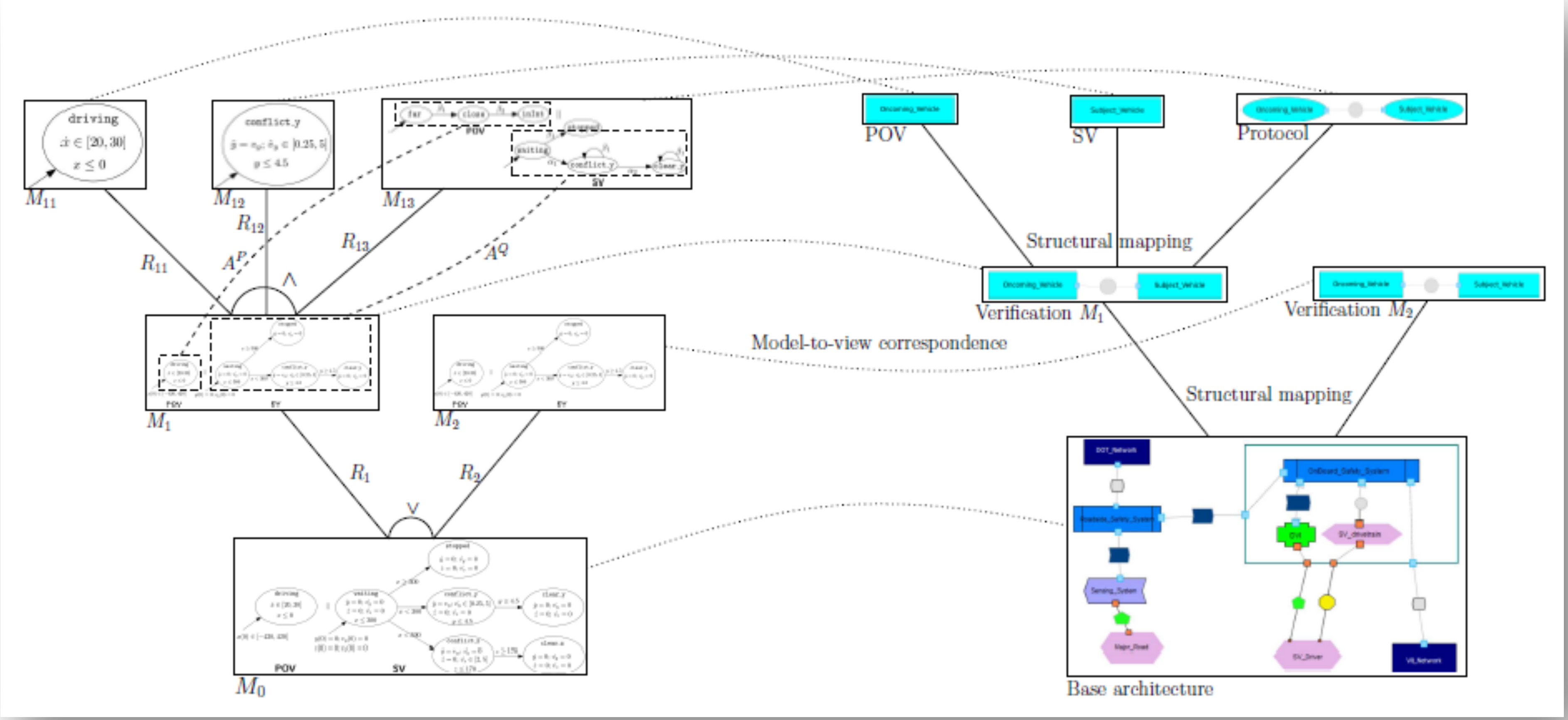
1. *Explicitly identify model parameters* e.g. *speed limits, intersection geometry, minimum acceleration,* and *spec. parameters*, e.g., *POV min. time-to-intersection, SV max. time-to-clear-intersection*

2. *Model interdependencies as an auxiliary constraint* e.g., those dictated by *speed limits, newton's laws* and *intersection geometry* on *time-to-intersection*, …

3. *Project global constraints and interdependencies (aux. constraint) onto local sets of parameters*

Proved semantic consistency in theorem prover KeYmaera

Semantic and Structural Hierarchies



Semantic side ***Structural side***

TAC '14
(CPS Special Issue)

Supporting Heterogeneity in
Cyber-Physical Systems Architectures

Akshay Rajhans†, Ajinkya Bhave†, Ivan Ruchkin‡, Bruce H. Krogh†*, David Garlan‡, André Platzer‡ and Bradley Schmerl‡

Summary

Cyber-Physical Systems present a major paradigm shift with systems that are

- Adaptive, Autonomous, Connected, and Collaborative

Model-based design critical for safe and efficient design process

- Open-ness and heterogeneity pose research challenges

Contributions for supporting heterogeneity in MBD of CPS

- *Architectural modeling:* high-level structural representation [MPM '09]
- *Model structures as architectural views* for comparing structure [ERTS '10]
- Semantic mappings using *behavior relations* enable *(compositional) heterogeneous verification* [HSCC '12, HSCC '13]
- *Constraint consistency* for consistent simplifying assumptions [CDC '11, HSCC '12]

Many challenges still remain

References*

MPM '09

ECEASST

An Architectural Approach to the Design and Analysis of Cyber-Physical Systems

Akshay Rajhans[1], Shang-Wen Cheng[2], Bradley Schmerl[2], David Garlan[2], Bruce H. Krogh[1], Clarence Agbi[1] and Ajinkya Bhave[1]

ERTS² '10

Augmenting Software Architectures with Physical Components

Ajinkya Bhave[1], David Garlan[2], Bruce H. Krogh[1], Akshay Rajhans[1], Bradley Schmerl[2]

[1]Dept. of Electrical and Computer Engineering
[2]School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3890 USA
email: {ajinkya@ | garlan@cs.| krogh@ece.| arajhans@ece.| schmerl@cs.}cmu.edu

ICCPS '11

View Consistency in Architectures for Cyber-Physical Systems

Ajinkya Bhave, Bruce H. Krogh   David Garlan, Bradley Schmerl

CDC '11

Using Parameters in Architectural Views to Support Heterogeneous Design and Verification

Akshay Rajhans†, Ajinkya Bhave†, Sarah Loos‡, Bruce H. Krogh†, André Platzer‡, David Garlan‡

HSCC '12

Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

Akshay Rajhans, arajhans@ece.cmu.edu   Bruce H. Krogh, krogh@ece.cmu.edu

HSCC '13

Compositional Heterogeneous Abstraction

Akshay Rajhans   Bruce H. Krogh

TAC:CPS '13 (submitted)

Supporting Heterogeneity in Cyber-Physical Systems Architectures

Akshay Rajhans†, Ajinkya Bhave†, Ivan Ruchkin‡, Bruce H. Krogh†*, David Garlan‡, André Platzer‡ and Bradley Schmerl‡

*Other work available at https://arajhans.github.io

MathWorks®

Accelerating the pace of engineering and science