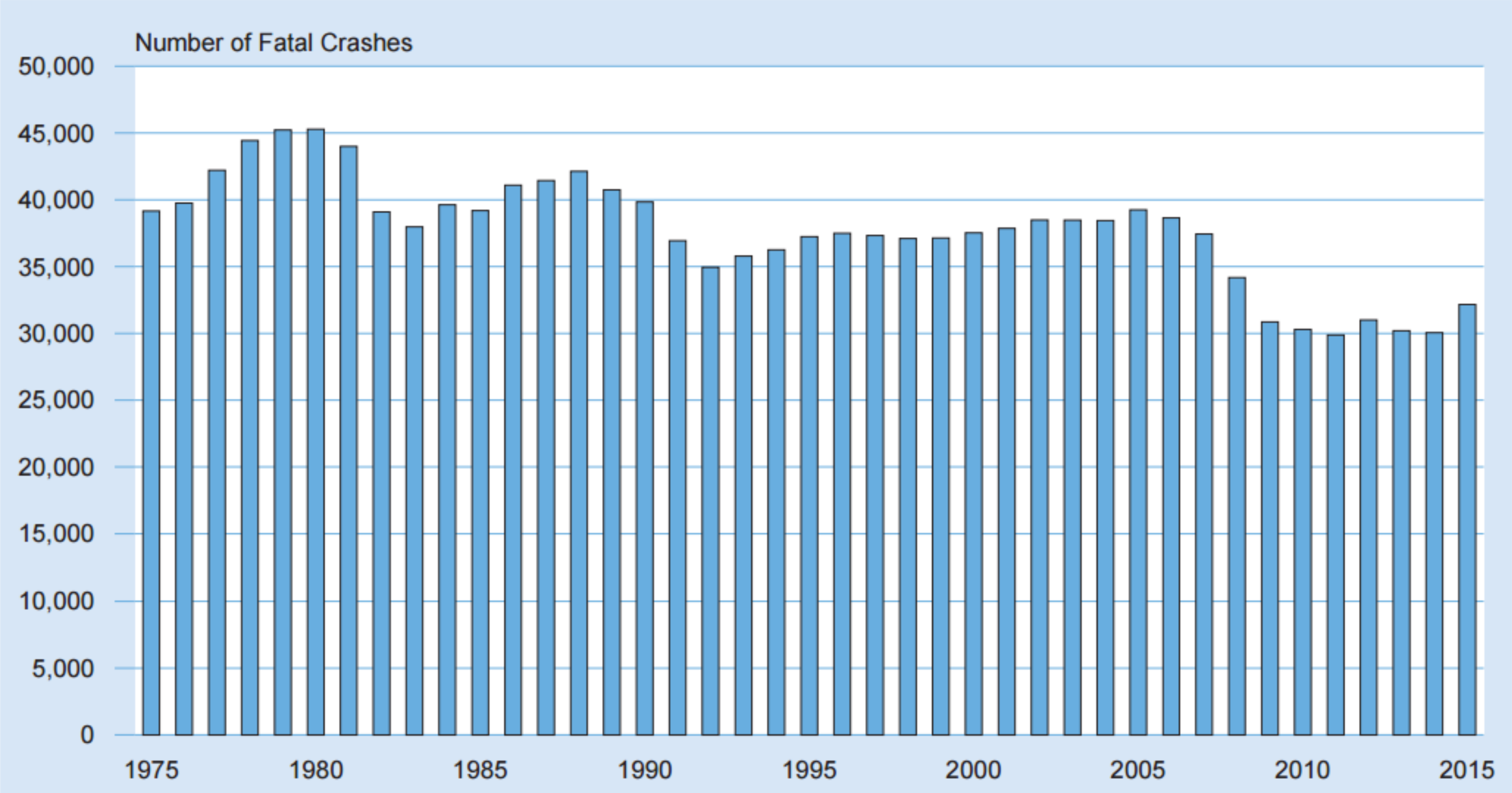
Model-Based Design Challenges for Cyber-Physical Systems

Akshay Rajhans, PhD

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

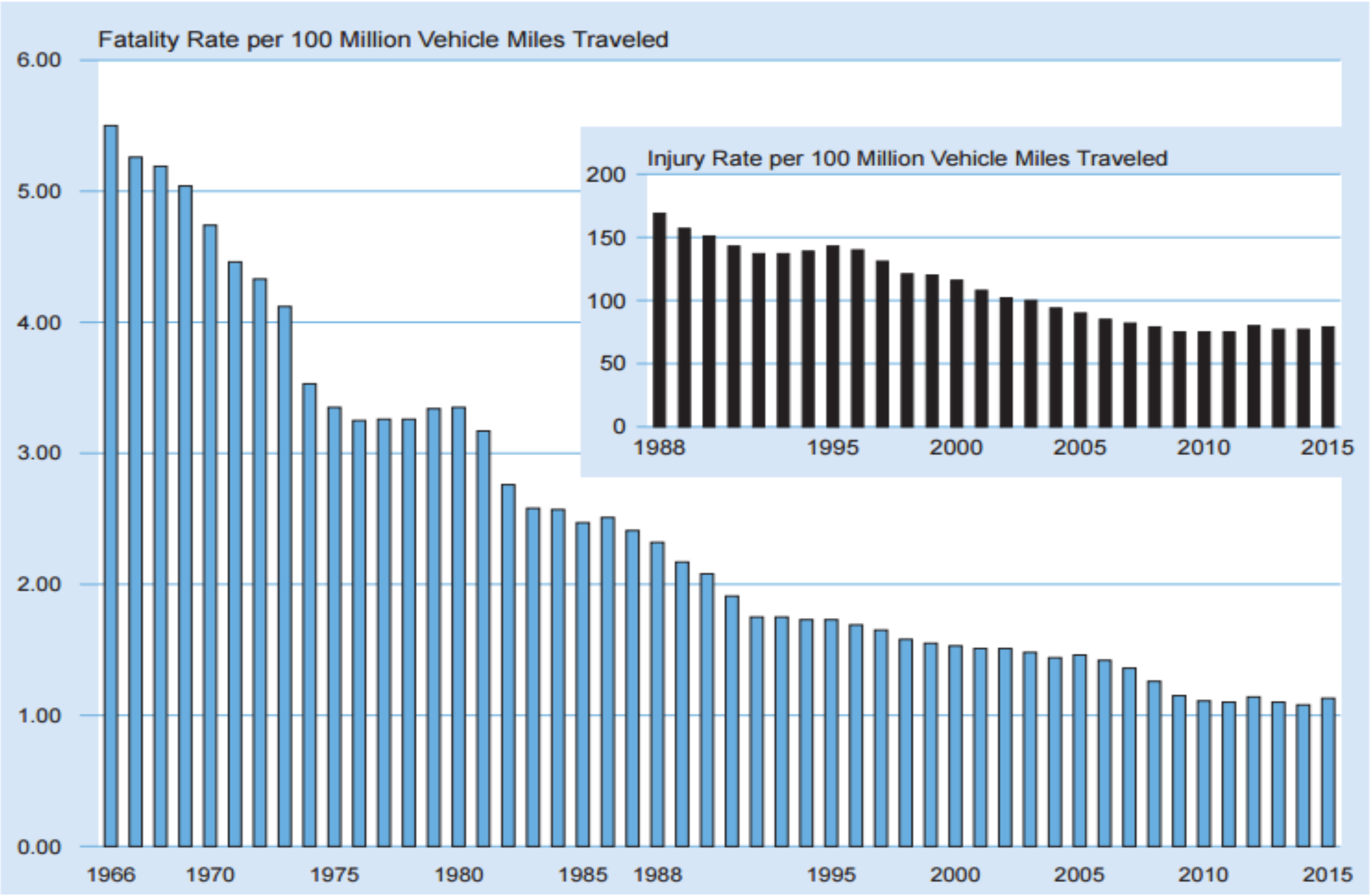
ExCAPE PI Meeting, University of Pennsylvania
May 5, 2017

Fatal Crashes, 1975-2015



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

Motor Vehicle Fatality and Injury Rates per 100 Million Vehicle Miles Traveled, 1966-2015



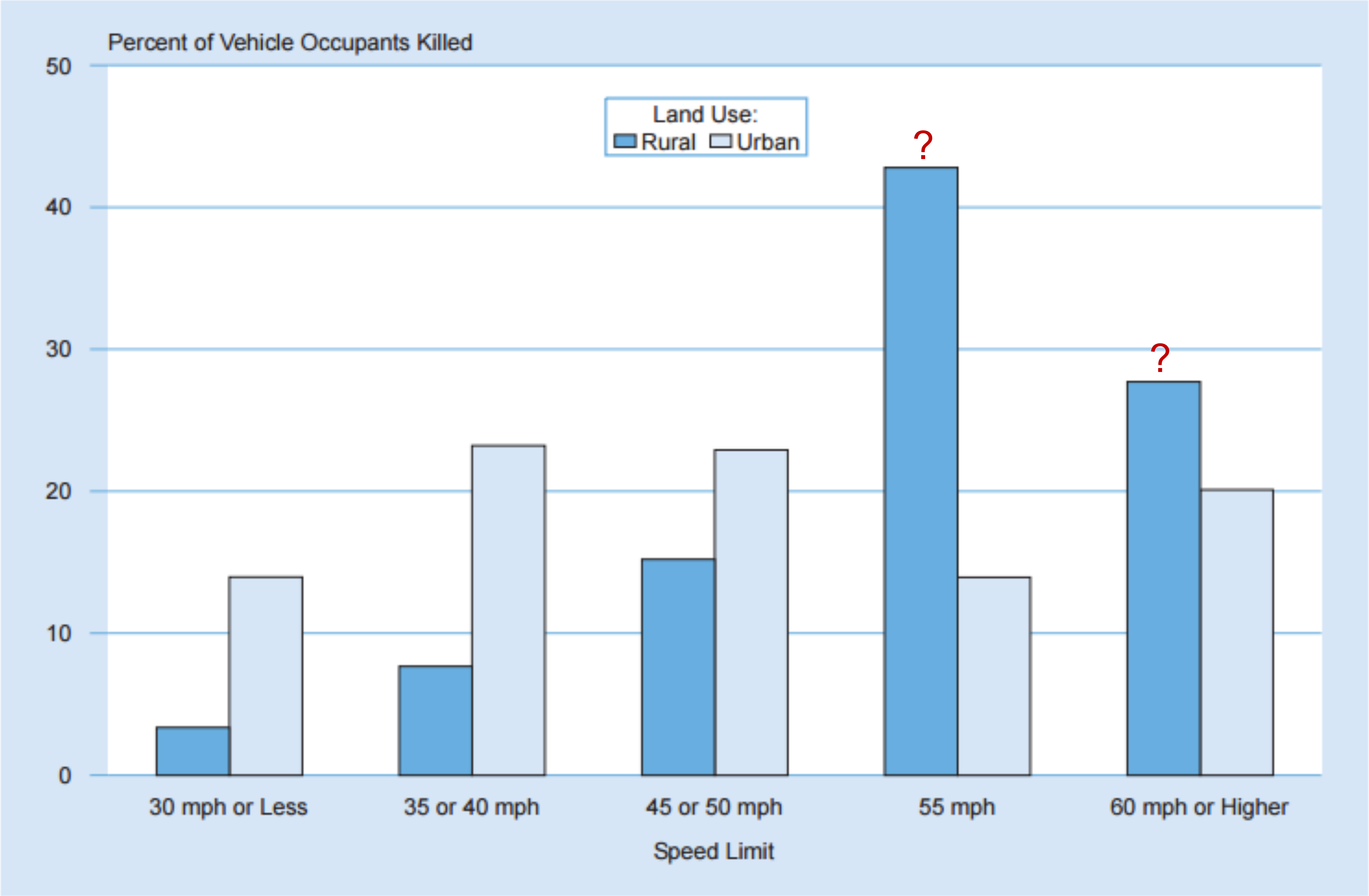
https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

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**

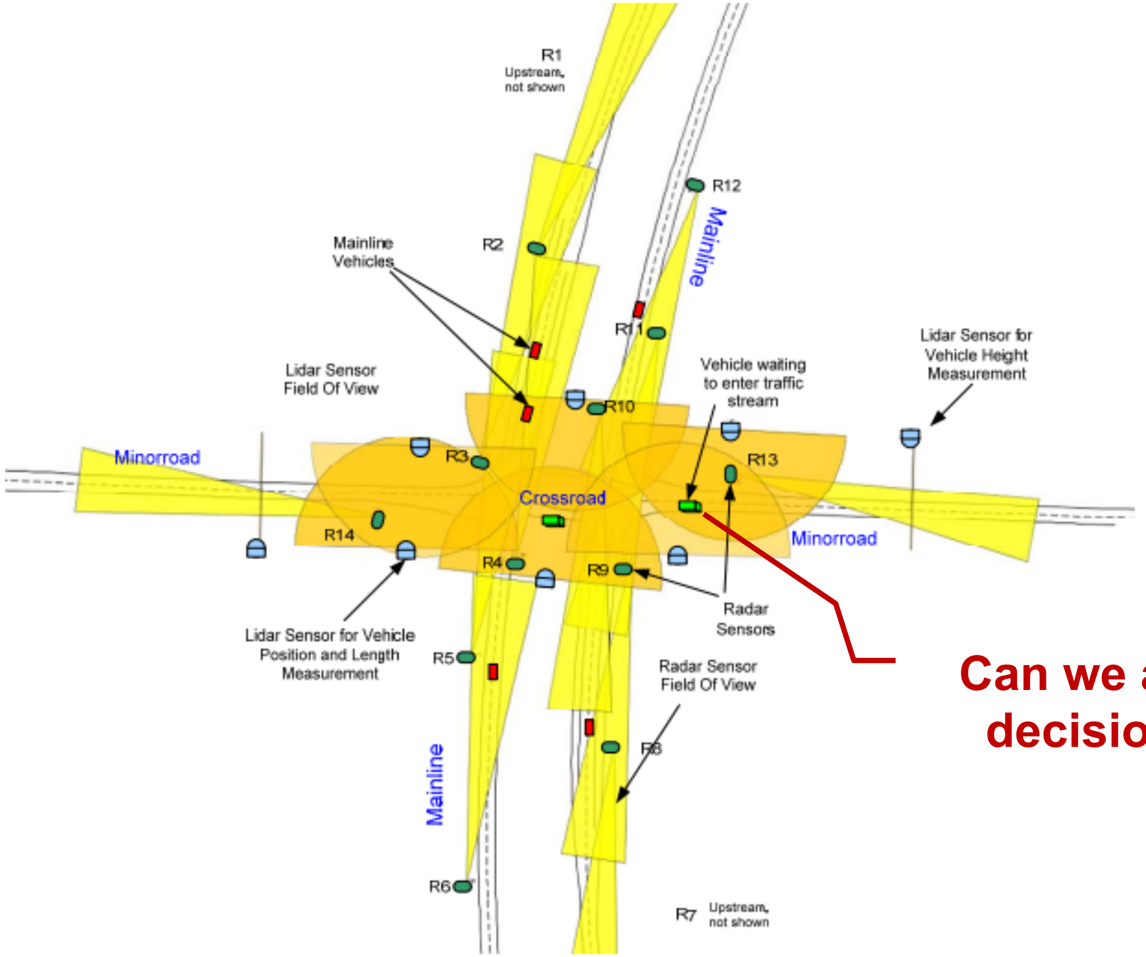
https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

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)



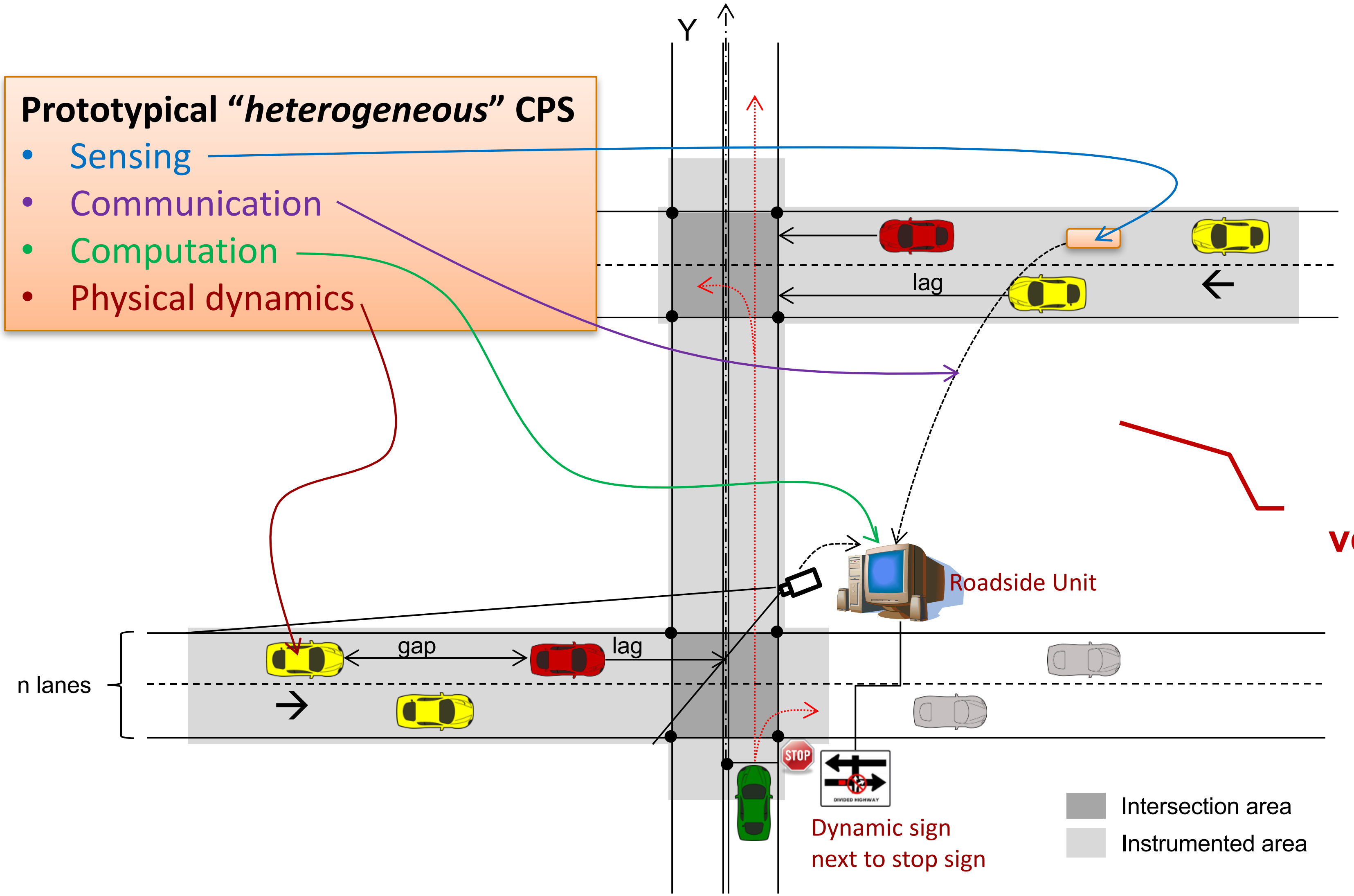
Can we assist in the decision making?

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

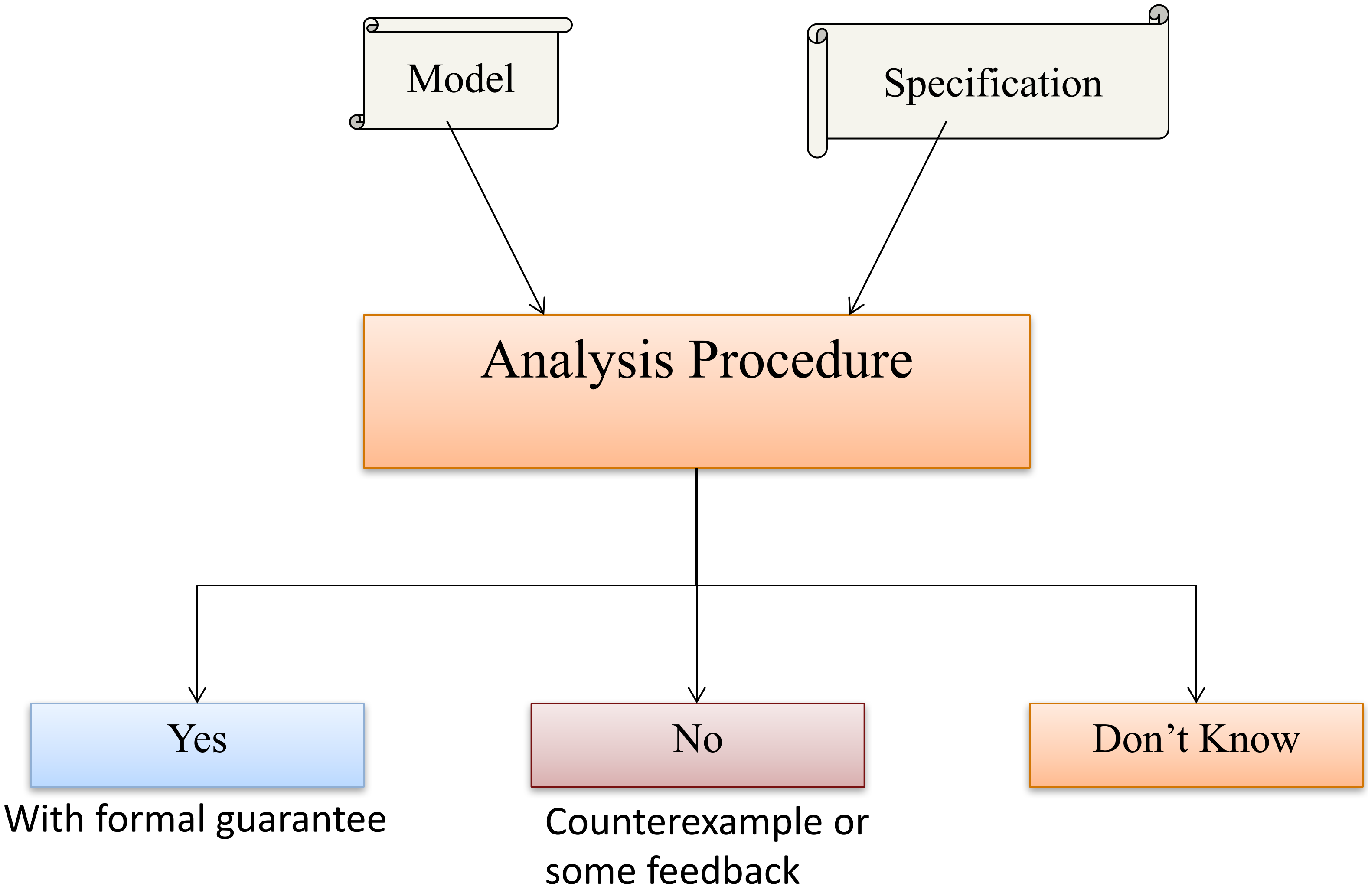
CICAS-SSA Schematic

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

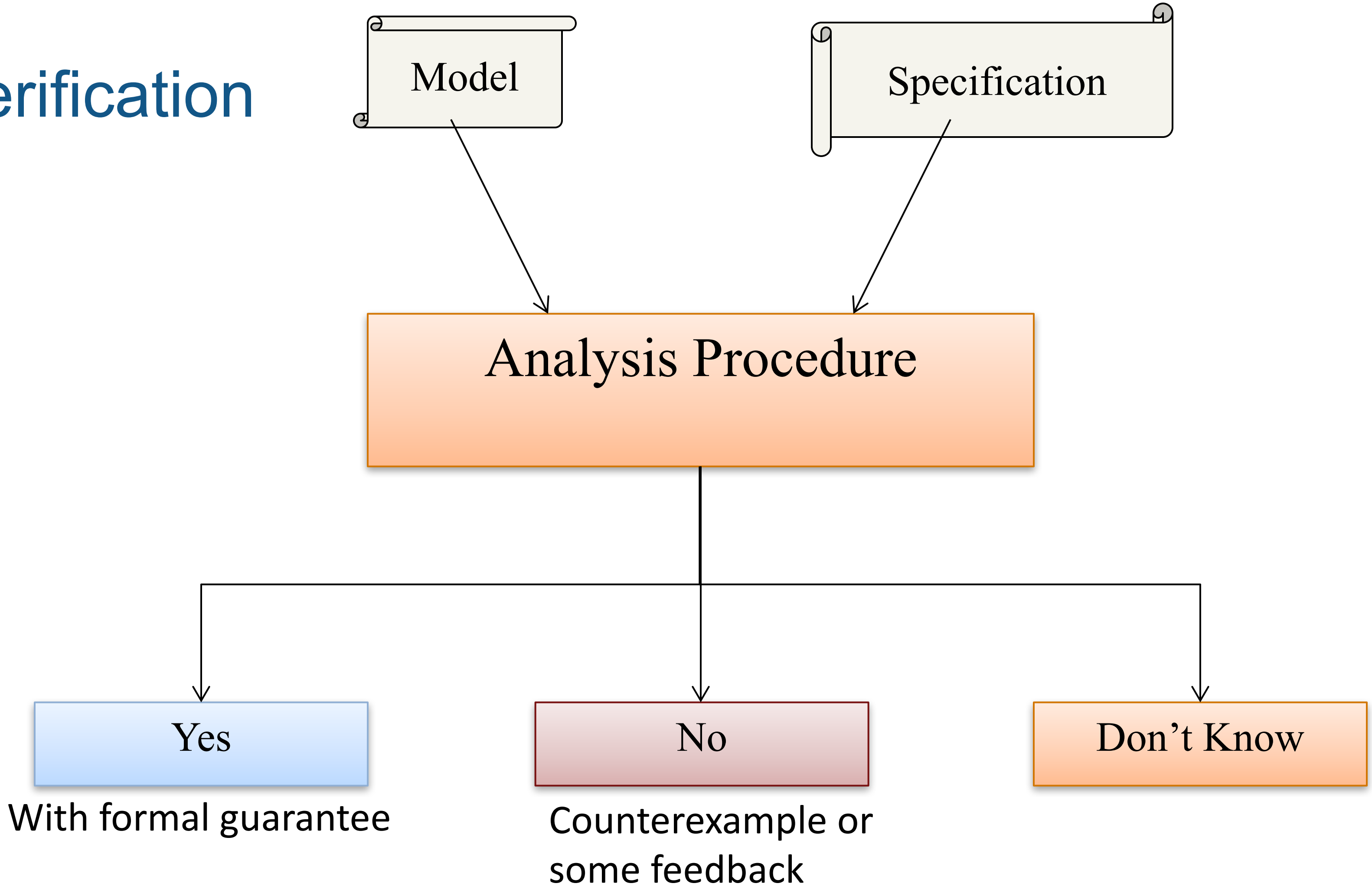


Can we formally verify such a system?

Formal Verification



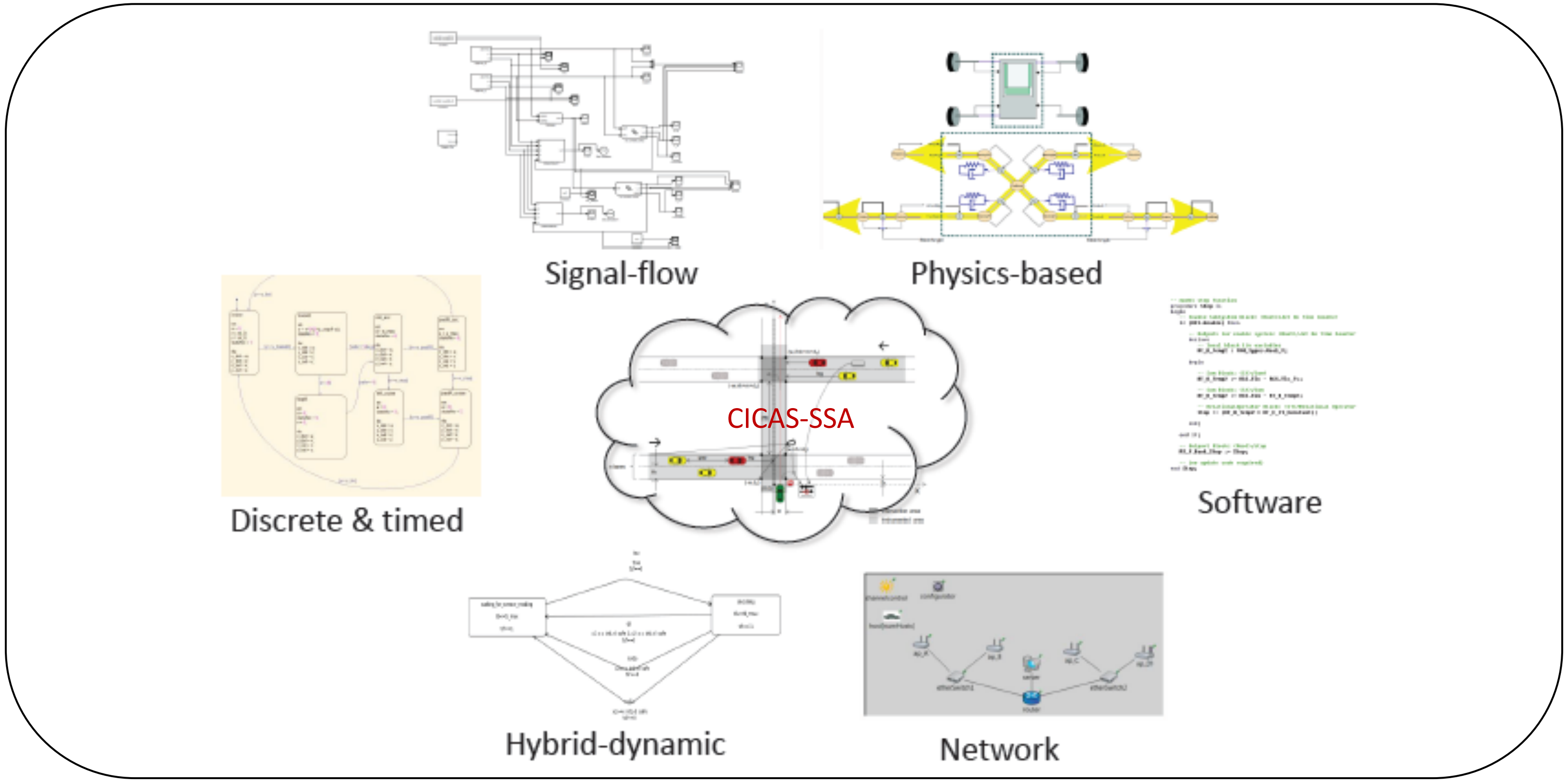
Formal Verification



There is no system model!

But there are models…

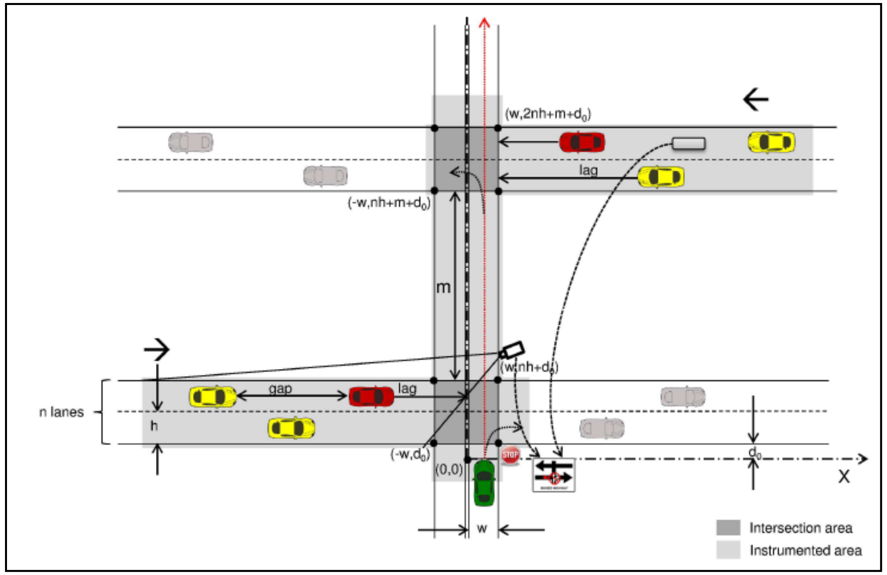
Heterogeneity in modeling formalisms and analysis techniques

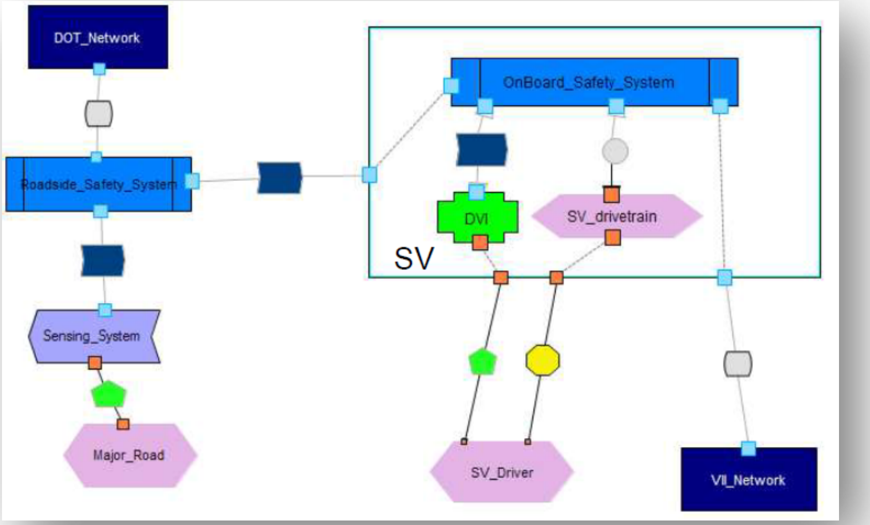


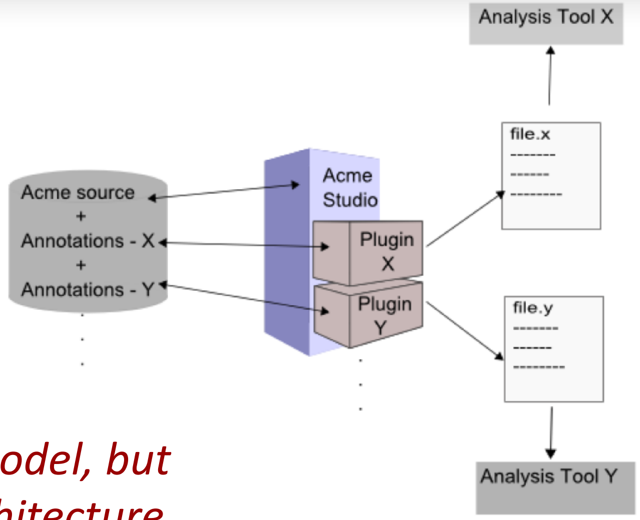
- *Different formalisms suited for different aspects of system design*
- Each model represents *some* design aspect well
- Models make *interdependent assumptions*
- *Tools work only with their formalisms*

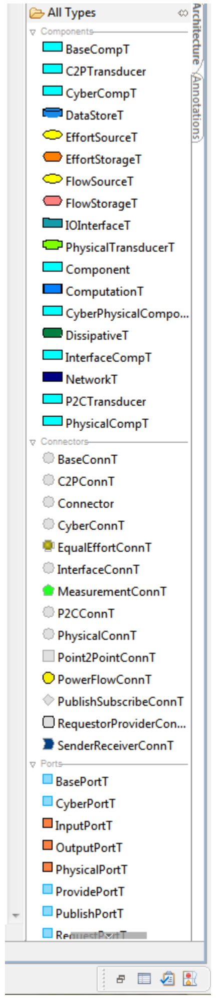
How do we ensure correctness of the system?

Cyber-Physical System Architecture









CPS architectural style palette in AcmeStudio

MPM '09

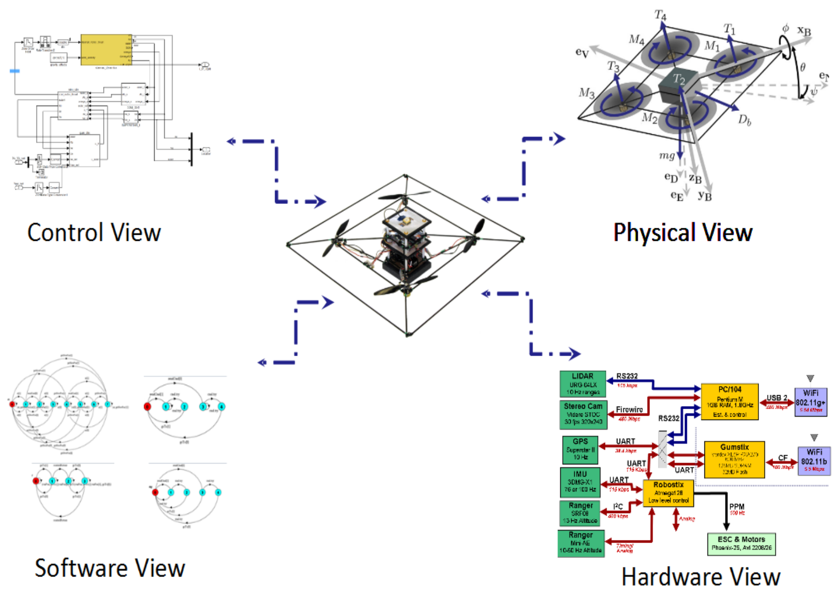
ECEASST

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

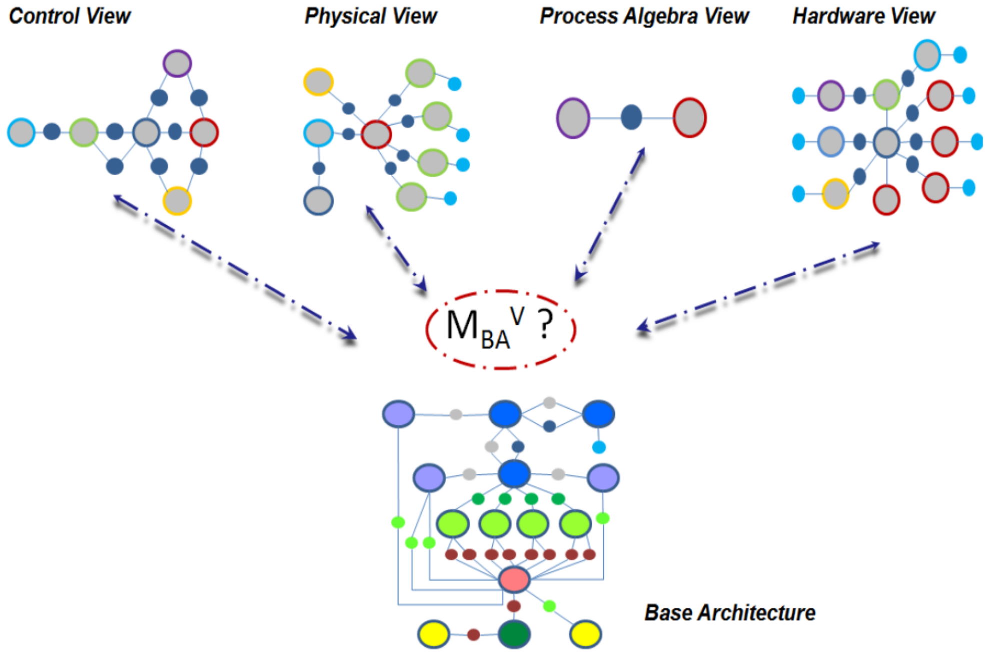
Akshay Rajhans[1], Shang-Wen Cheng[2], Bradley Schmerl[2], David Garlan[2], Bruce H. Krogh[1], Clarence Agbi[1] and Ajinkya Bhave[1]

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

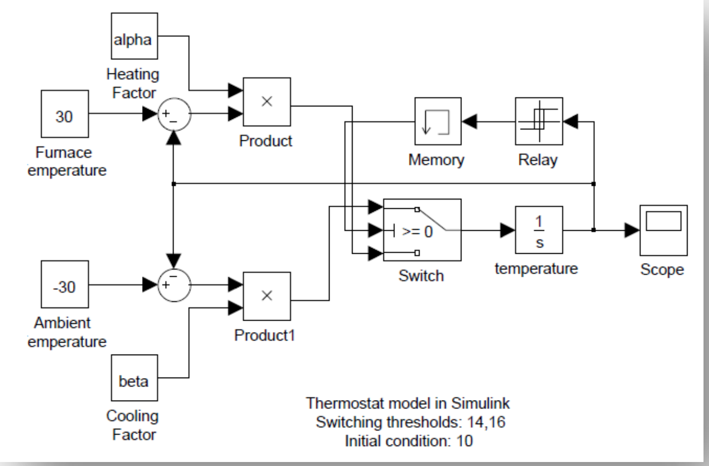
ICCPS '11

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

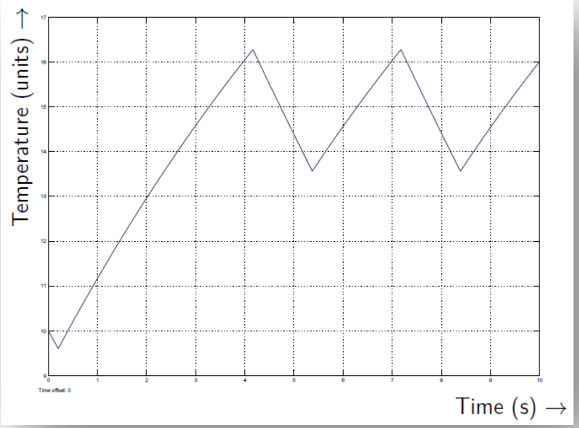
"Model structure vs system structure"

Analysis: Consistency, completeness

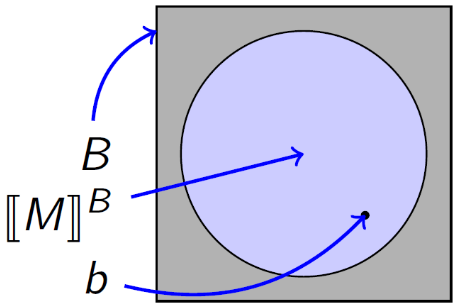
Semantic domains of models and specifications



Model M



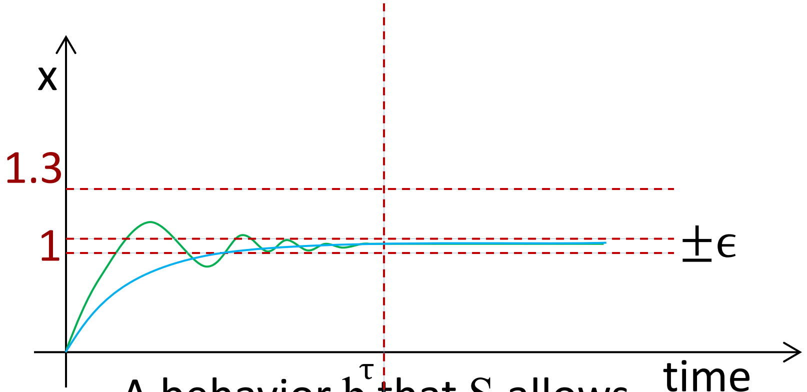
A behavior b that M exhibits



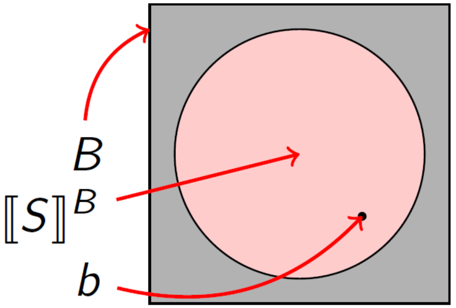
$[\![M]\!]^B$: "semantic interpretation" of M in a behavior domain B

> 1) "overshoot is no more than 1.3 units and settling time is less than τ"
>
> 2) $\square(x < 1.3) \wedge \diamond_\tau (x \in [1 \pm \epsilon])$

Specification S

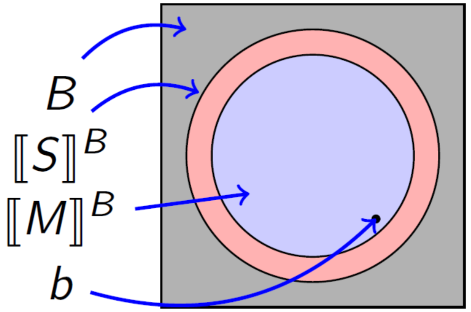


A behavior b that S allows



$[\![S]\!]^B$: "semantic interpretation" of S in B

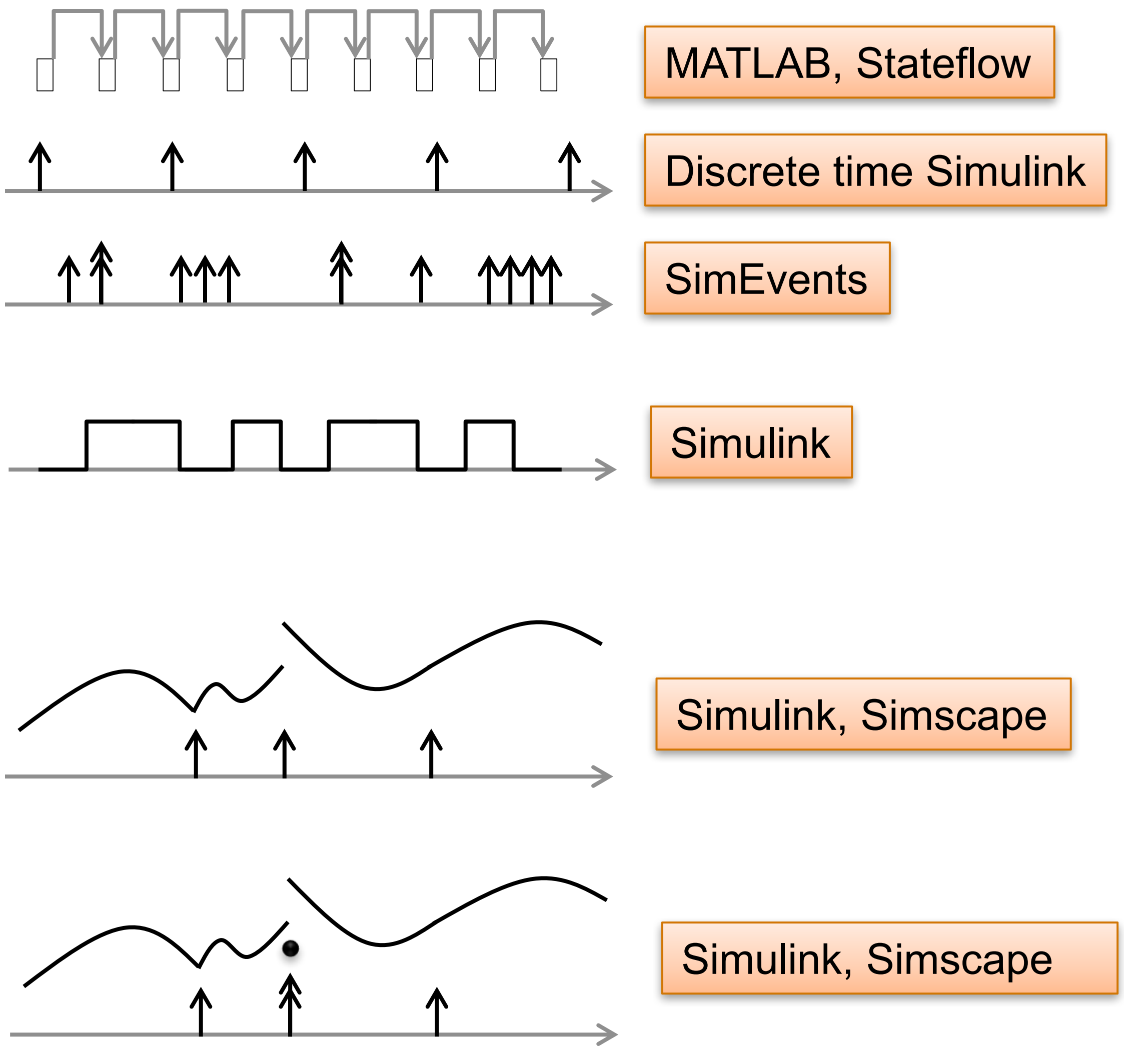
$$M \models^B S \qquad\qquad [\![M]\!]^B \subseteq [\![S]\!]^B$$



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

The semantic domain of a dynamic system

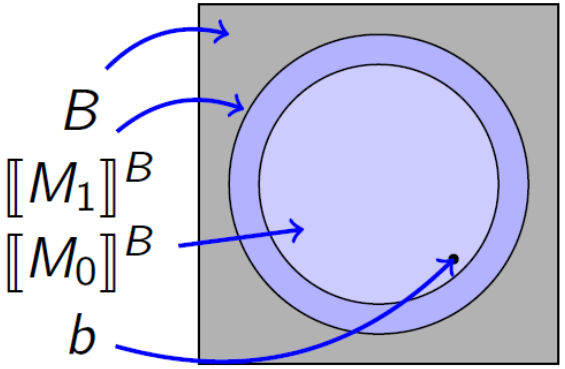
- Points, [ ]
  - On **N**
  - On **R** x **N**
- Intervals, [〉 (〈 〉, 〈])
  - On **R**
- Hybrid point/interval
  - On **R**
  - On **R** x **N**



Abstraction and Implication

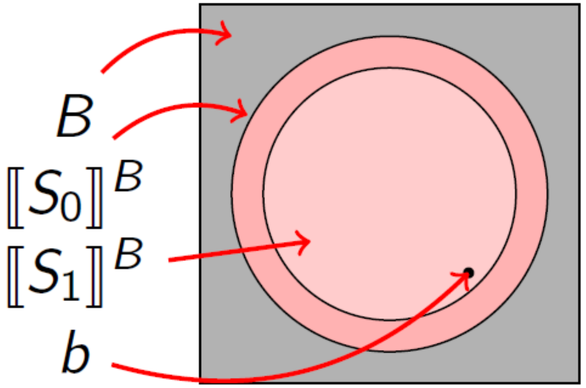
- Model M_1 abstracts M_0 in B, written $M_0 \sqsubseteq^B M_1$

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



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

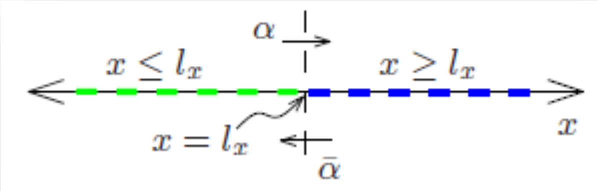
  if $[\![S_1]\!]^B \subseteq [\![S_0]\!]^B$

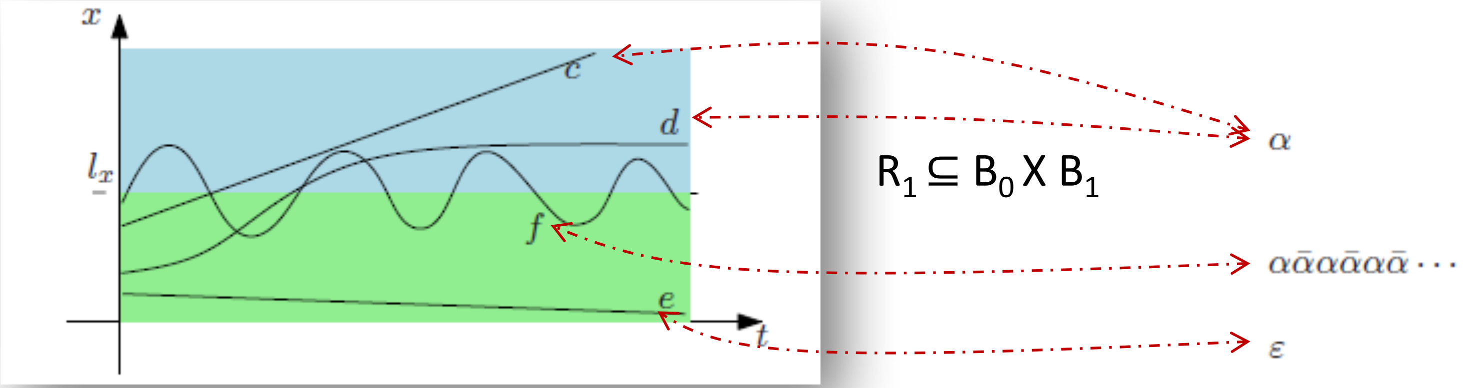


Mappings between semantic domains via behavior relations

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

Heterogeneous Specification Implication

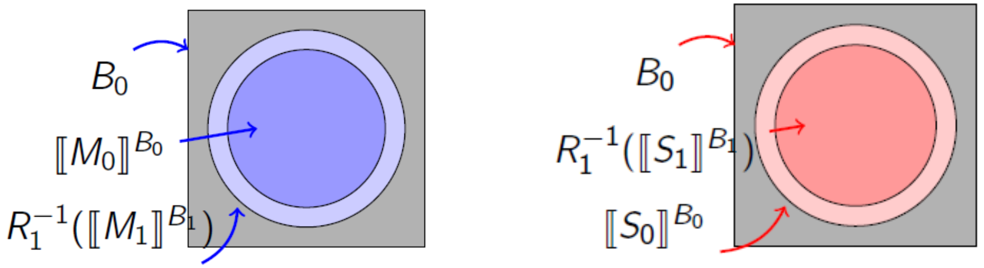
$S_1 \Rightarrow^{R_1} S_0$, if

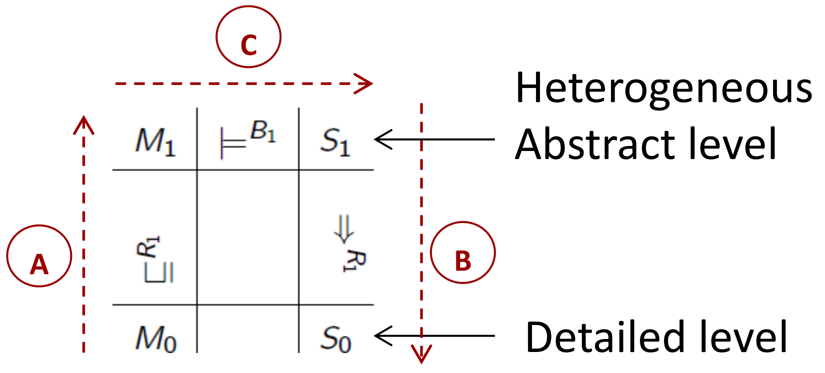
(B) $$R_1^{-1}([\![S_1]\!]^{B_1}) \subseteq [\![S_0]\!]^{B_0}.$$

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)

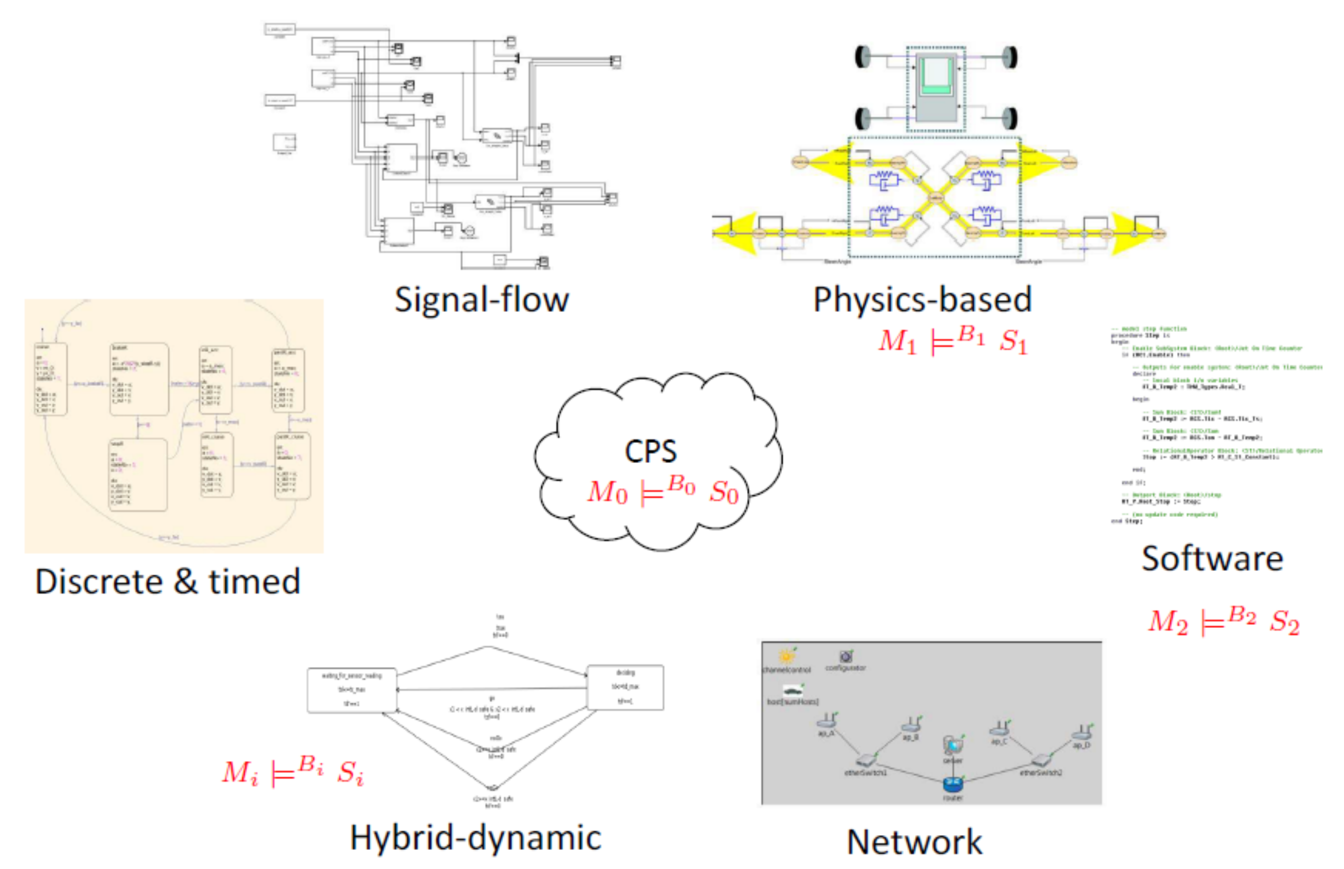
(in words)





(pictorially)

Multi-model Verification Problem

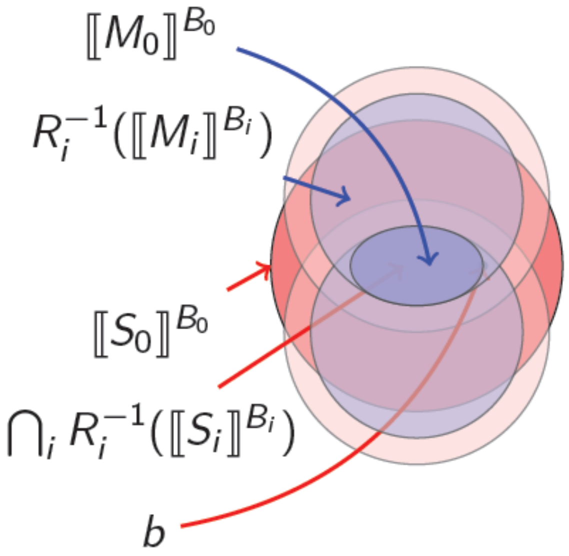


How do we use $M_1 \models^{B_1} S_1, \ldots, M_n \models^{B_n} S_n$ to infer $M_0 \models^{B_0} S_0$?

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 $\bigcap_i R_i^{-1}([\![S_i]\!]^{B_i}) \subseteq [\![S_0]\!]^{B_0}$.

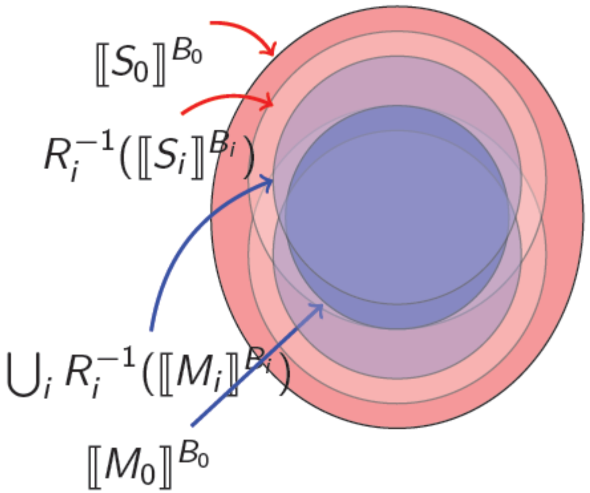


Typical use case

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

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 $[\![M_0]\!]^{B_0} \subseteq \bigcup_i R_i^{-1}([\![M_i]\!]^{B_i})$.

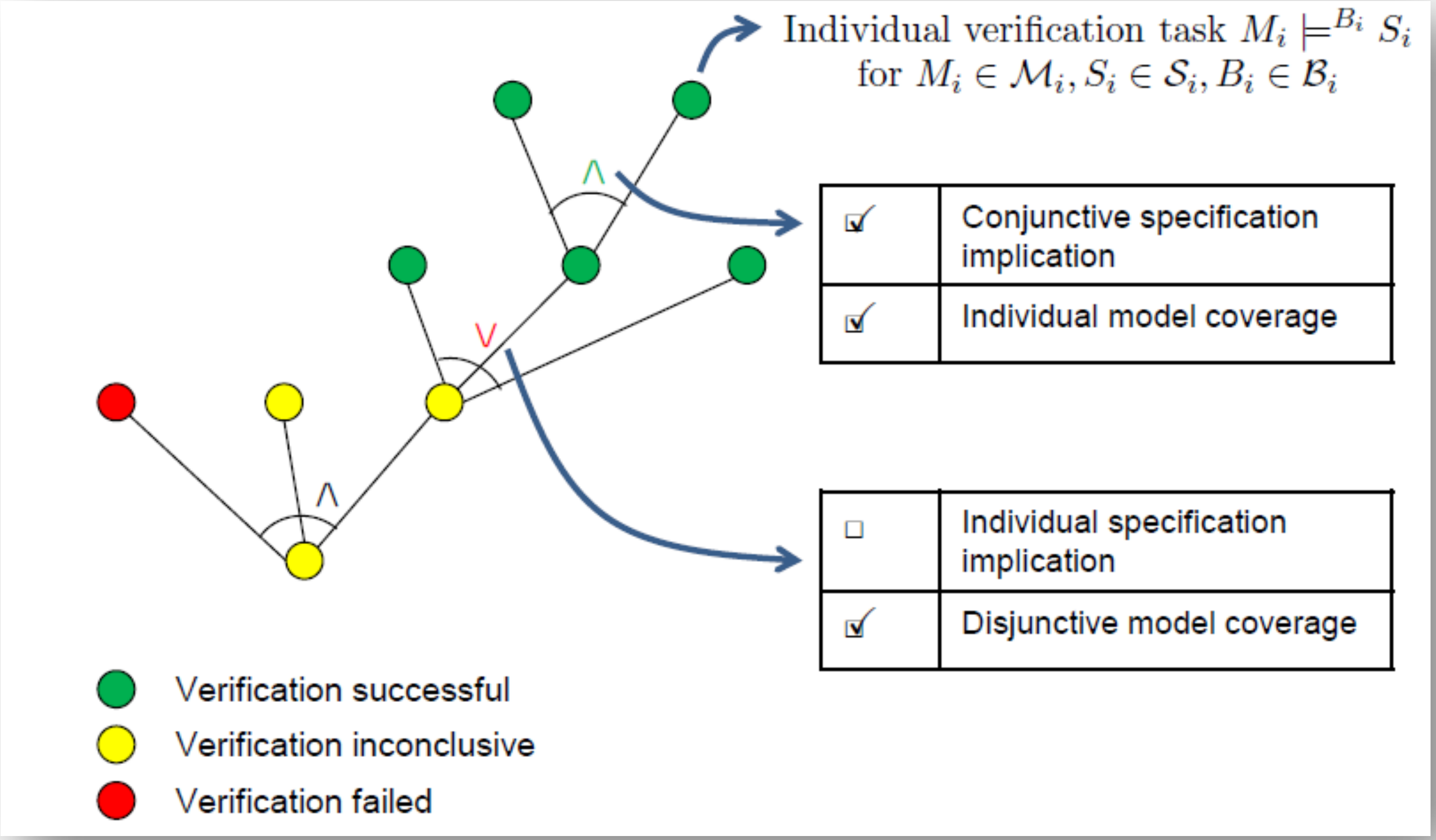


Typical use case

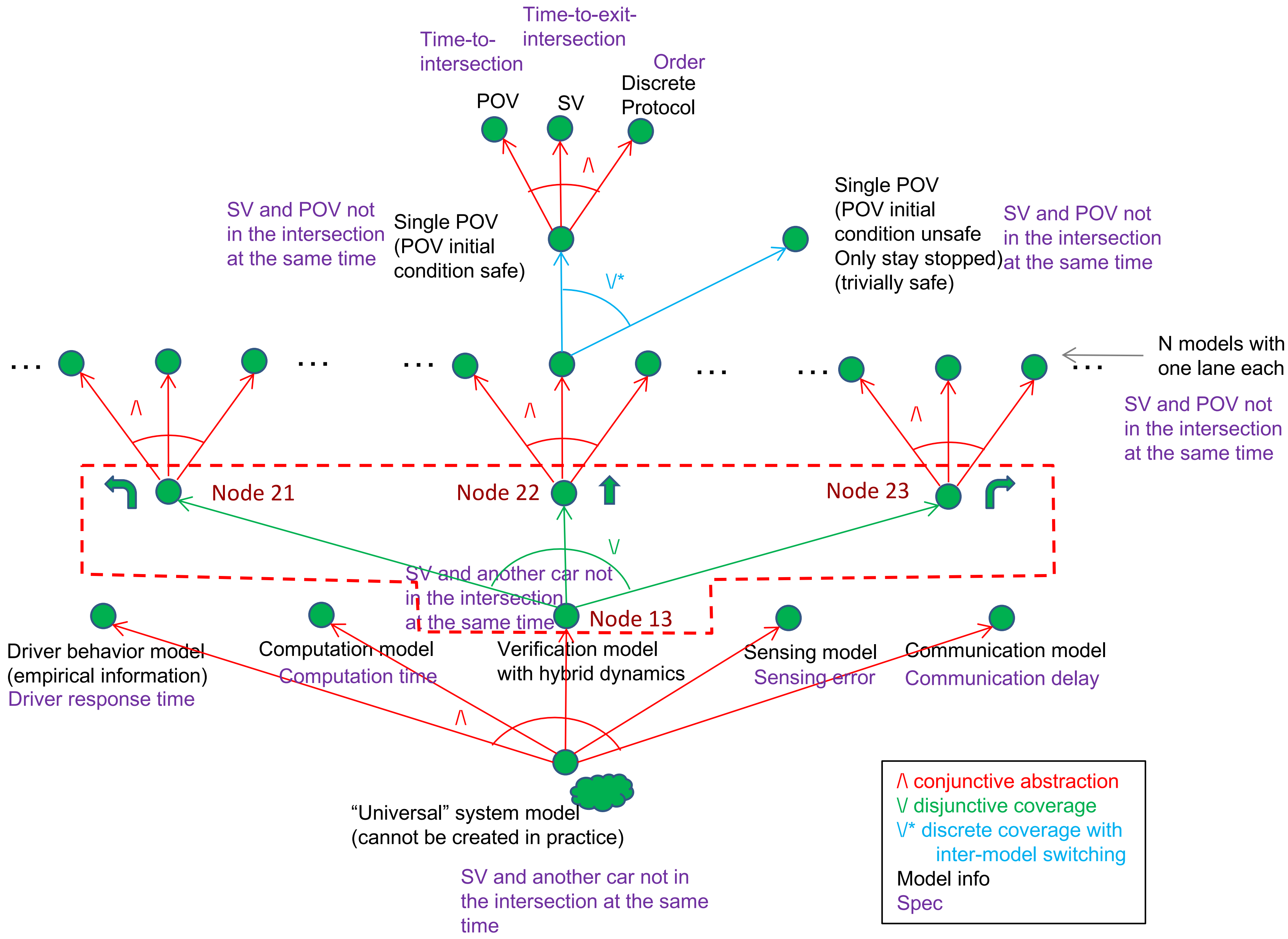
- Each model captures a different subset of behaviors, e.g., a specific nondeterministic choice

Hierarchical Verification

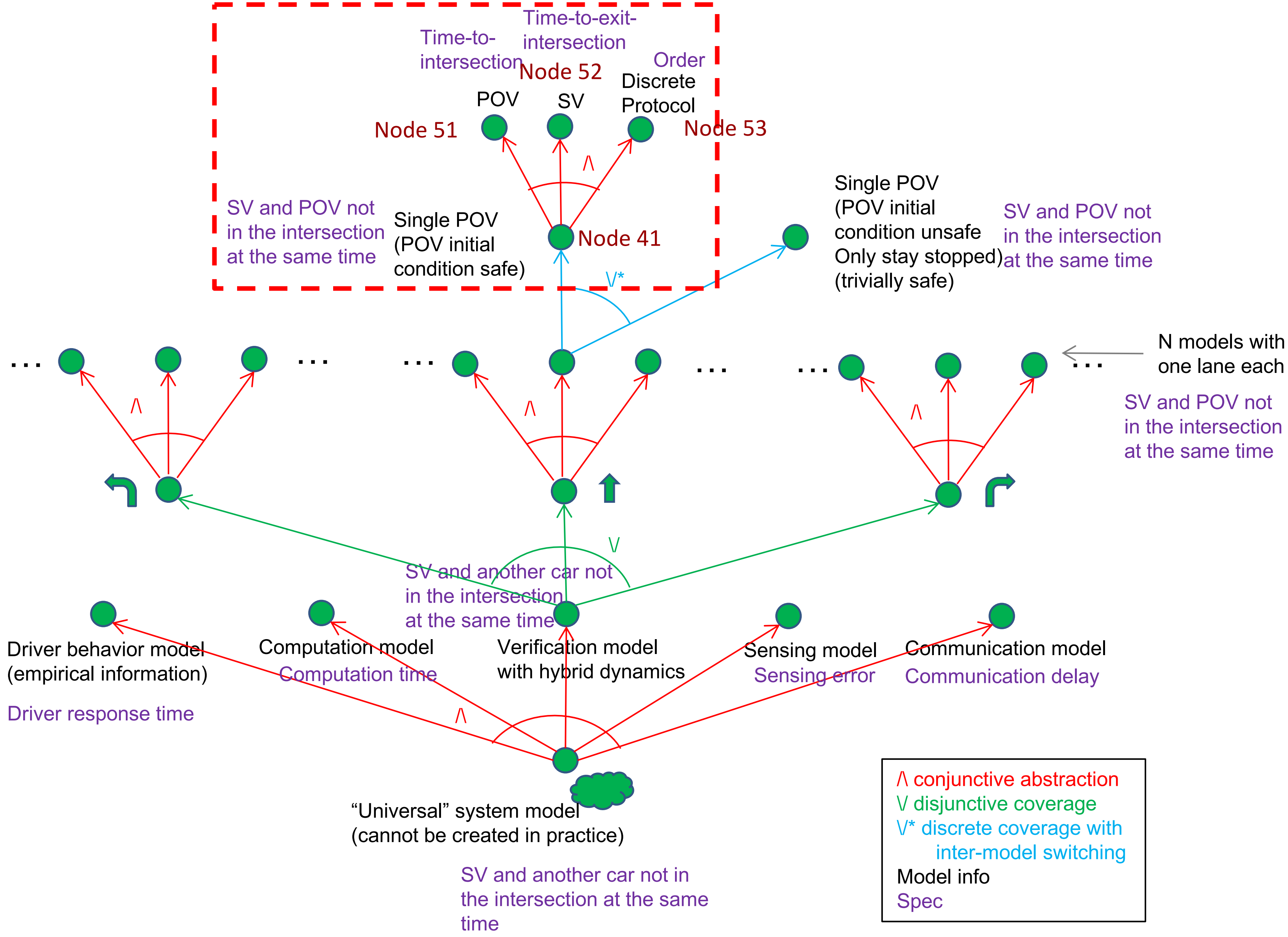
Conjunctive and disjunctive verification constructs can be nested arbitrarily



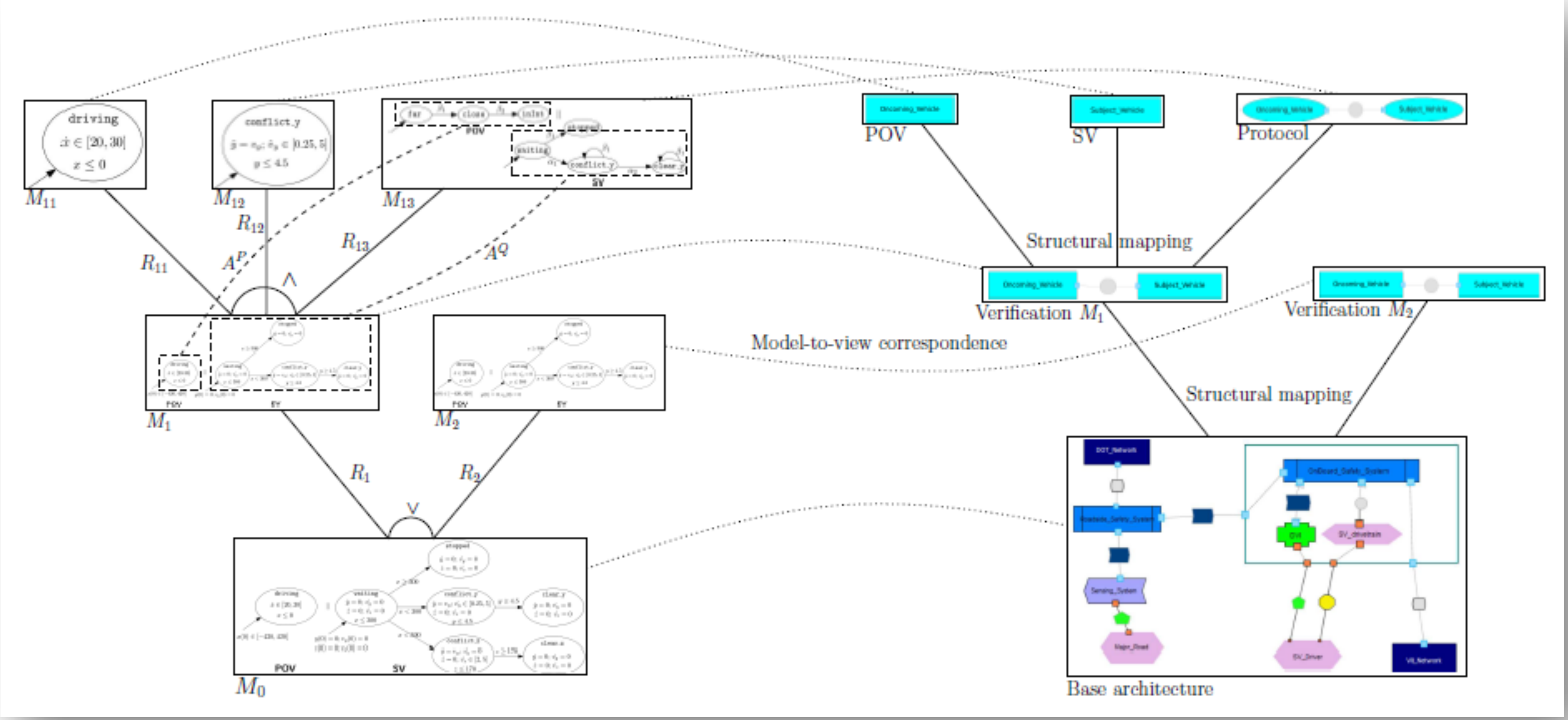
Het. Verification of CICAS



Heterogeneous verification of CICAS-SSA



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‡

References

- A. Rajhans, "*Multi-Model Heterogeneous Verification of Cyber-Physical Systems*," PhD Thesis, Carnegie Mellon University, 2013.

- A. Rajhans, A. Bhave, I. Ruchkin, B. Krogh, D. Garlan, A. Platzer and B. Schmerl, "*Supporting Heterogeneity in Cyber-Physical System Architectures*", IEEE Transactions on Automatic Control's Special Issue on Control of Cyber-Physical Systems, Vol. 59, Issue 12, pages 3178-3193.
- A. Rajhans and B. H. Krogh, "*Compositional Heterogeneous Abstraction*," 16th International Conference on Hybrid Systems: Computation and Control, 2013.
- A. Rajhans and B. H. Krogh, "*Heterogeneous Verification of Cyber-Physical Systems Using Behavior Relations*," 15th International Conference on Hybrid Systems: Computation and Control, 2012.
- A. Rajhans, A. Bhave, S. Loos, B. H. Krogh, A. Platzer and D. Garlan, "*Using Parameters in Architectural Views to Support Heterogeneous Design and Verification*," 50th IEEE Conference on Decision and Control, 2011.
- A. Bhave, D. Garlan, B. Krogh, A. Rajhans and B. Schmerl, "*Augmenting Software Architectures with Physical Components*," Embedded Real Time Software and Systems (ERTS^2), 2010. '
- A. Rajhans, S.-W. Cheng, B. Schmerl, D. Garlan, B. H. Krogh, C. Agbi and A. Bhave, "*An Architectural Approach to the Design and Analysis of Cyber-Physical Systems*," Third International Workshop on Multi-Paradigm Modeling (MPM), 2009.

Preprints available at https://arajhans.github.io

MathWorks®

Accelerating the pace of engineering and science