Addressing heterogeneity in model-based development of cyber-physical systems

Akshay Rajhans

ECE PhD candidate, Carnegie Mellon University

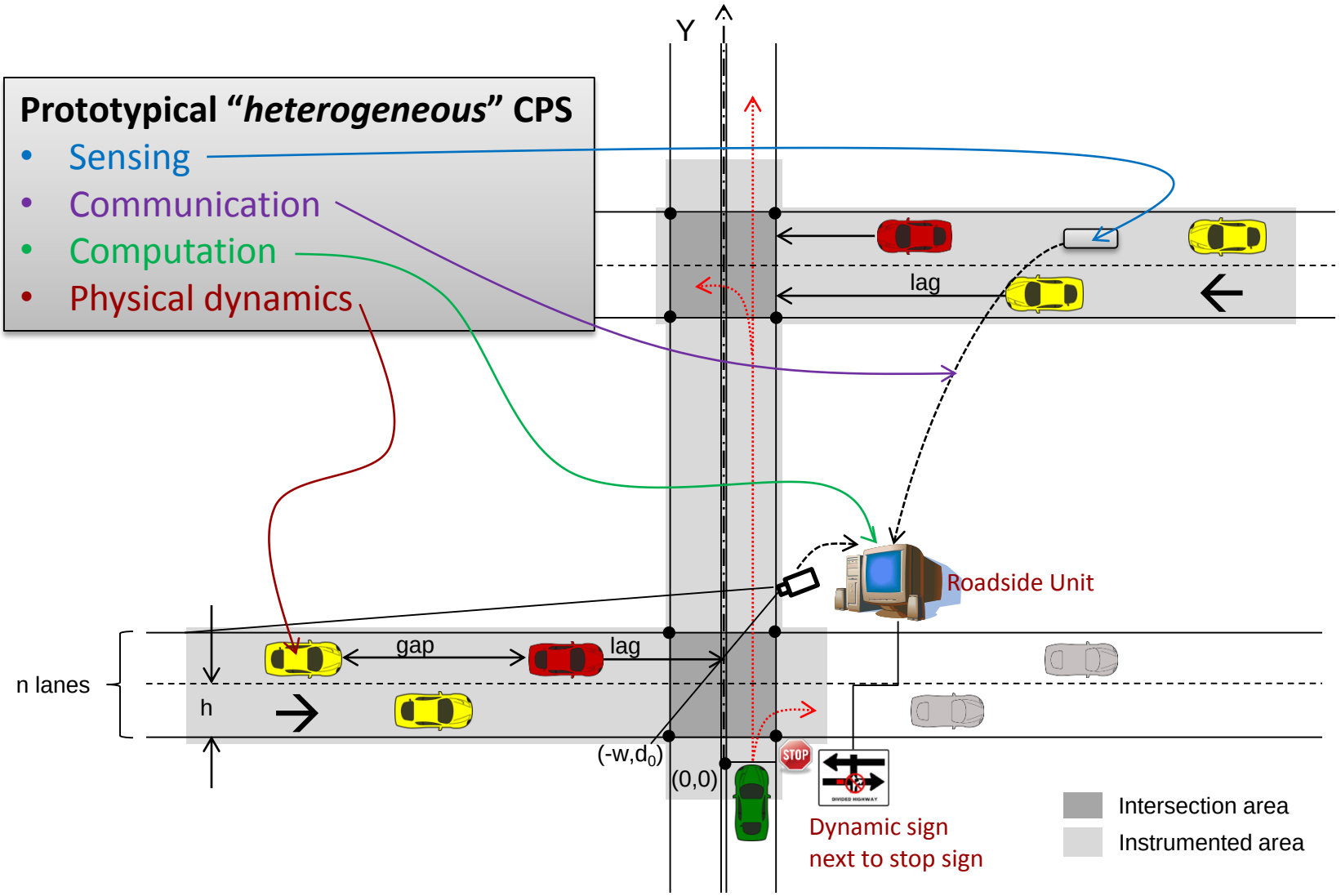
arajhans@ece.cmu.edu
http://users.ece.cmu.edu/~arajhans

Joint work with
Ajinkya Bhave, Bruce Krogh, David Garlan, Sarah Loos, Andre Platzer, Ivan Ruchkin, Bradley Schmerl
ECE Department, School of Computer Science, Carnegie Mellon University

Electrical & Computer ENGINEERING

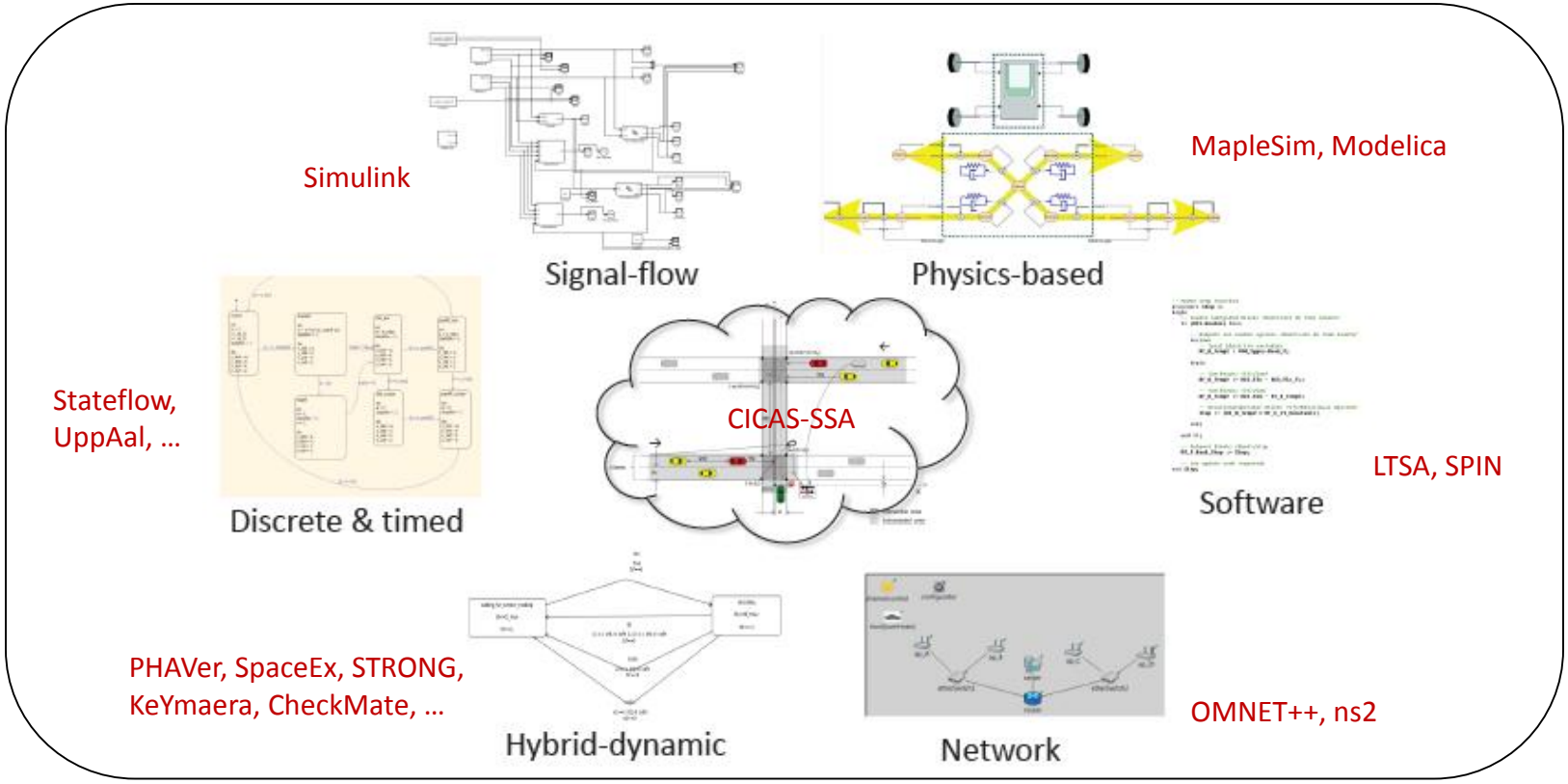
CPS are *heterogeneous*

Example: CICAS-SSA*



*Cooperative Intersection Collision Avoidance System for Stop-Sign Assist

Heterogeneity in Models & Analysis Tools



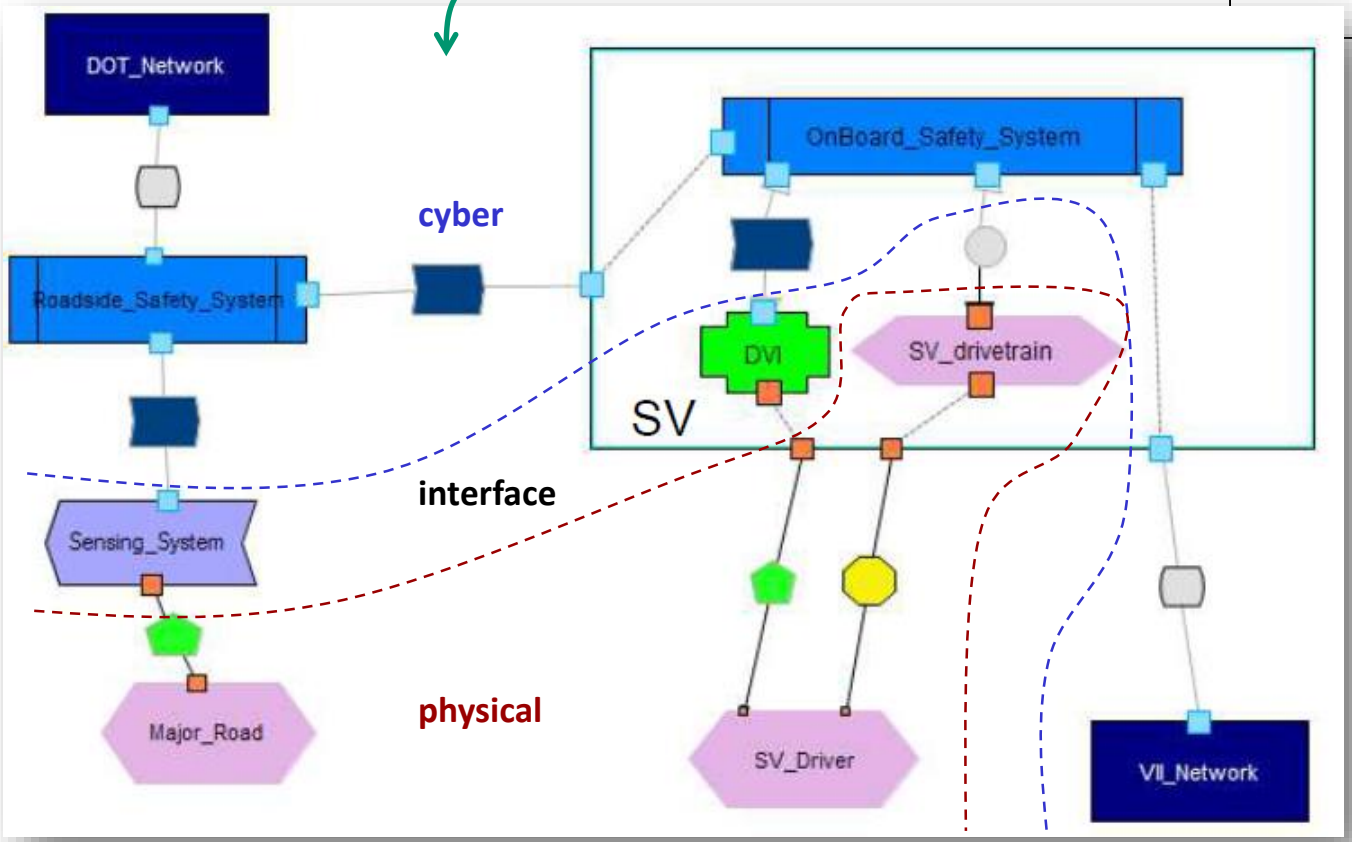
Challenges:

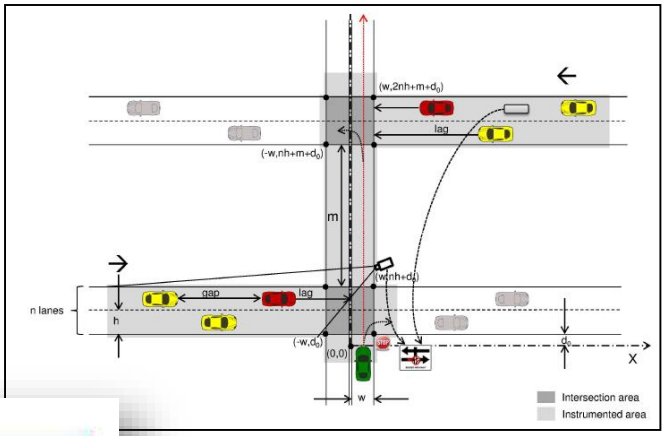
- *No "universal" modeling formalism* that can capture everything.
- Each model represents *some* design aspect well, but not the others.
- Models make *(interdependent) simplifying assumptions*.
- Different *tools* leverage different properties, *work only with their formalism*.

How do we ensure correctness of the system without a unifying formalism?

Architectural Modeling of CICAS

CICAS: Architectural modeling depicting interacting run-time components and connectors



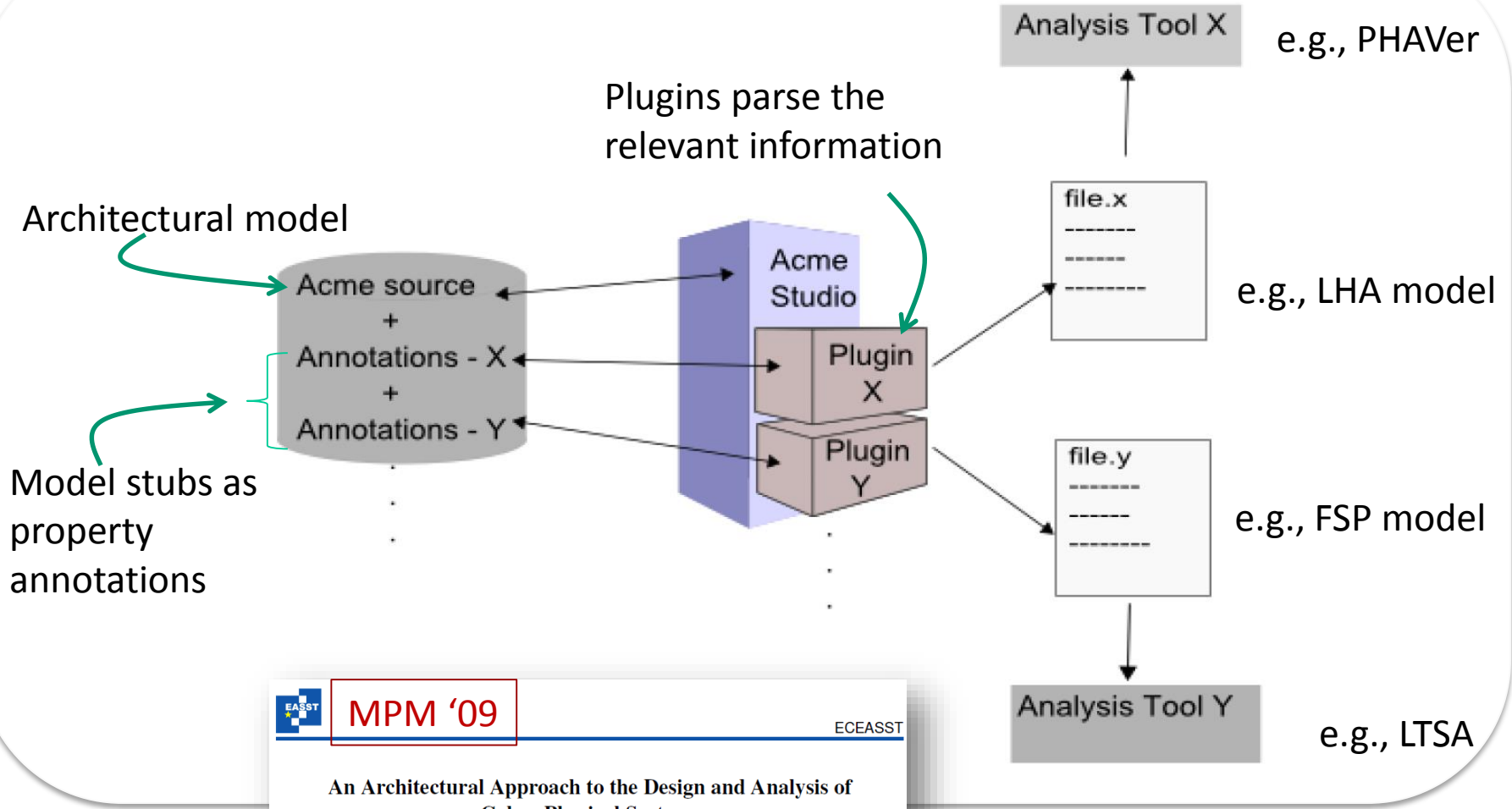


CICAS: Actual System

– *Visual representation with unambiguous* (but very basic) *semantics*

(no behavior info.)

“Heterogeneous models as annotations”



MPM ‘09

ECEASST

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

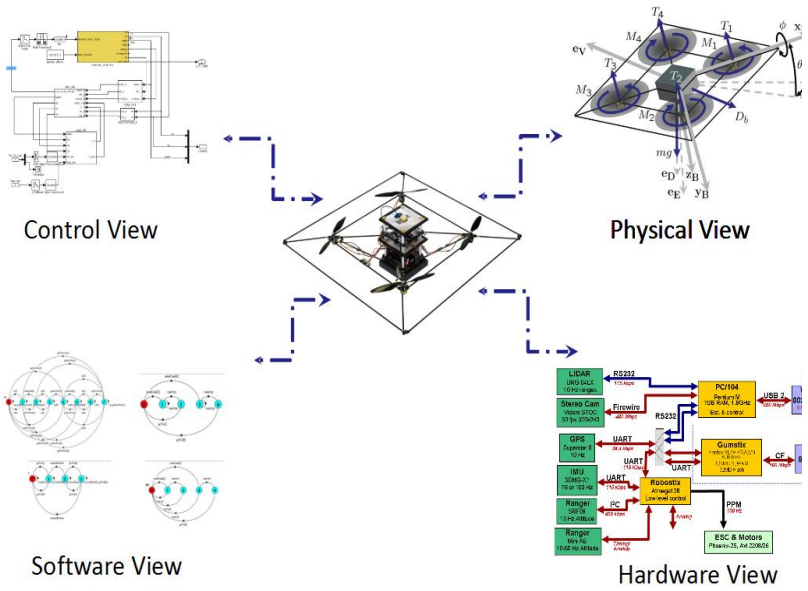
Akshay Rajhans[1], Shang-Wen Cheng[2], Bradley Schmerl[2], David Garlan[2], Bruce H. Krogh[1], Clarence Agbi[1] and Ajinkya Bhave[1]

Electrical & Computer ENGINEERING

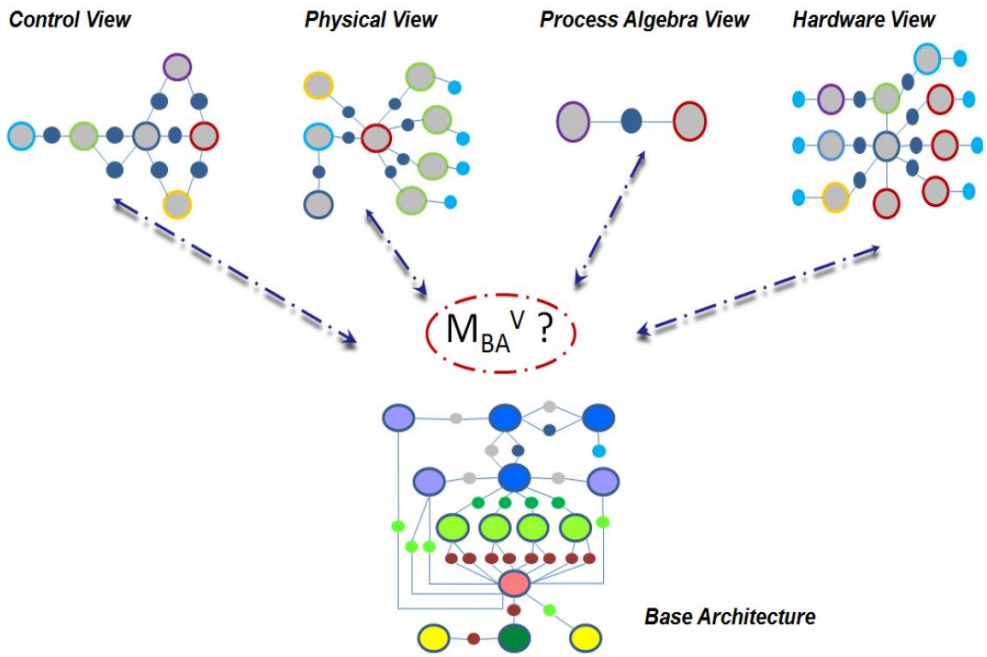
Enables verification by exporting to an external tool.

★ "Heterogeneous models as arch. views"

Example: STARMAC quadrotor



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]

ERTS[2] '10

[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

View Consistency in Architectures for Cyber-Physical Systems

ICCPS '11

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

★ Ensures consistent functional deployment in model subcomponents

Electrical & Computer ENGINEERING

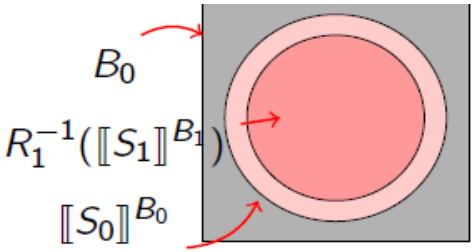
Heterogeneous abstraction/implication

Define semantic associations between behaviors from domains $B_0 \in \mathcal{B}_0$ and $B_1 \in \mathcal{B}_1$ in terms of *behavior relations* $R \subseteq B_0 \times B_1$, or special case *behavior abstraction functions* $\mathcal{A} : B_0 \to B_1$.

Heterogeneous Specification Implication

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

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



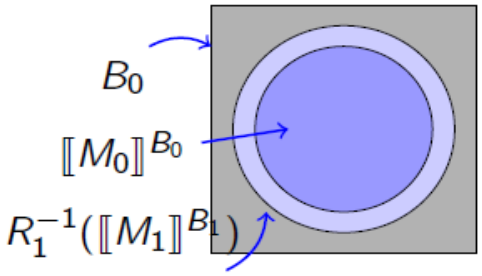
If

S_1 stronger than S_0 (via R_1)

Heterogeneous Abstraction

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

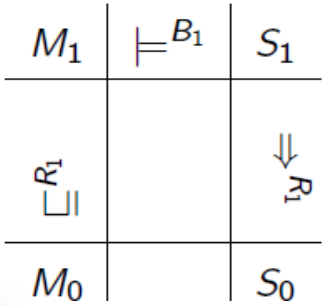
$$[\![M_0]\!]^{B_0} \subseteq R_1^{-1}([\![M_1]\!]^{B_1}).$$



M_1 abstracts M_0 (via R_1)

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 $M_0 \models^{B_0} S_0$.



then
M_1 satisfies S_1 in B_1
implies
M_0 satisfies S_0 in B_0

Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

HSCC '12

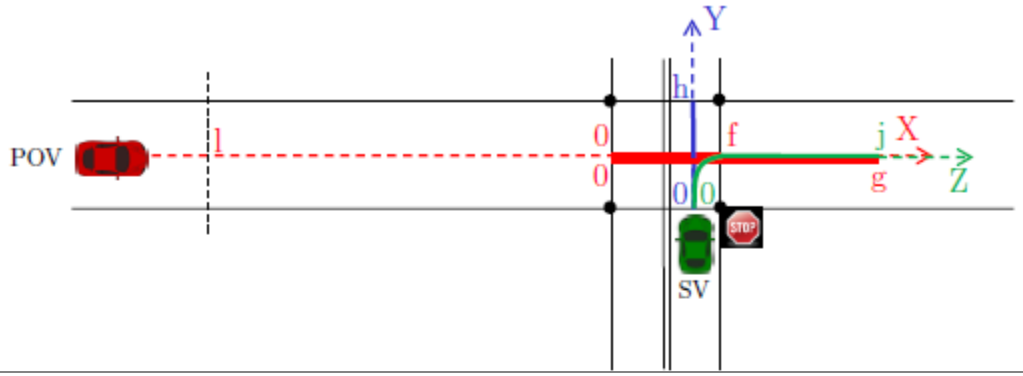
Akshay Rajhans
arajhans@ece.cmu.edu

Bruce H. Krogh
krogh@ece.cmu.edu

Enables heterogeneous verification

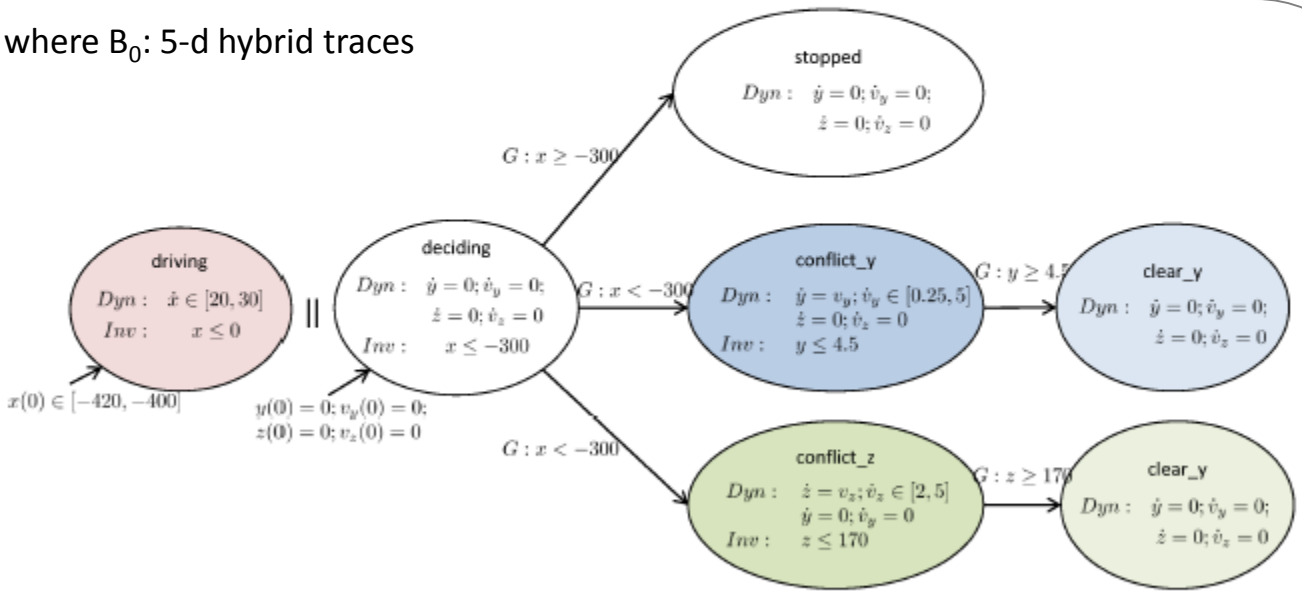
Heterogeneous verification of CICAS

CPS:



$M_0 \models^{B_0} S_0$ where B_0: 5-d hybrid traces

M_0:



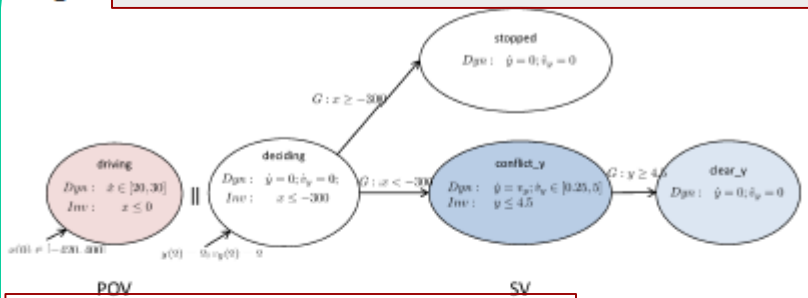
S_0: $\Box \neg ((x == 0 \wedge 0 < y < 4.5) \vee (x == 0 \wedge 0 < z < 170))$.

Heterogeneous verification of CICAS

Conjunctive (AND) analysis of $M_1 \models^{B_1} S_1$ continued on next slide

M_1 :

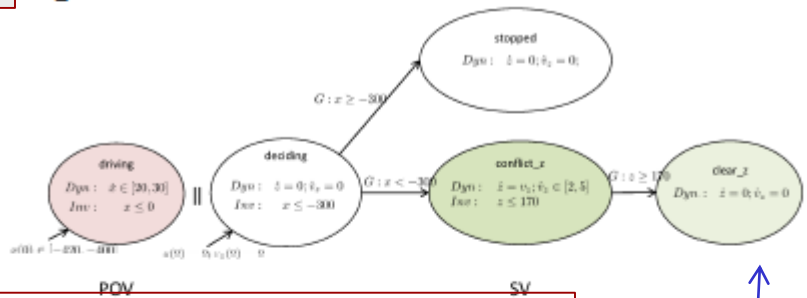
← Together overapproximate M_0 →



Stronger than S_0

$S_1 : \Box \neg (x == 0 \wedge 0 < y < 4.5)$

M_2 :



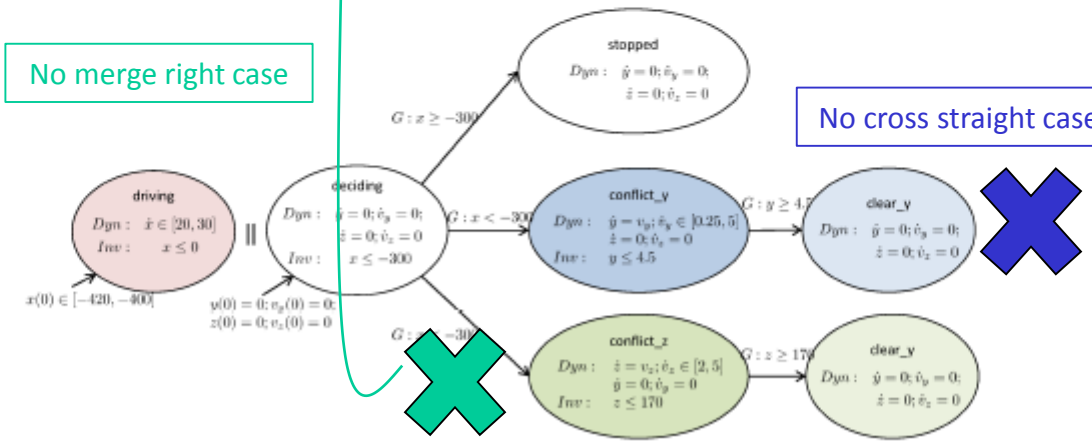
Stronger than S_0

$S_2 : \Box \neg (x == 0 \wedge 0 < z < 170)$

M_0 :

No merge right case

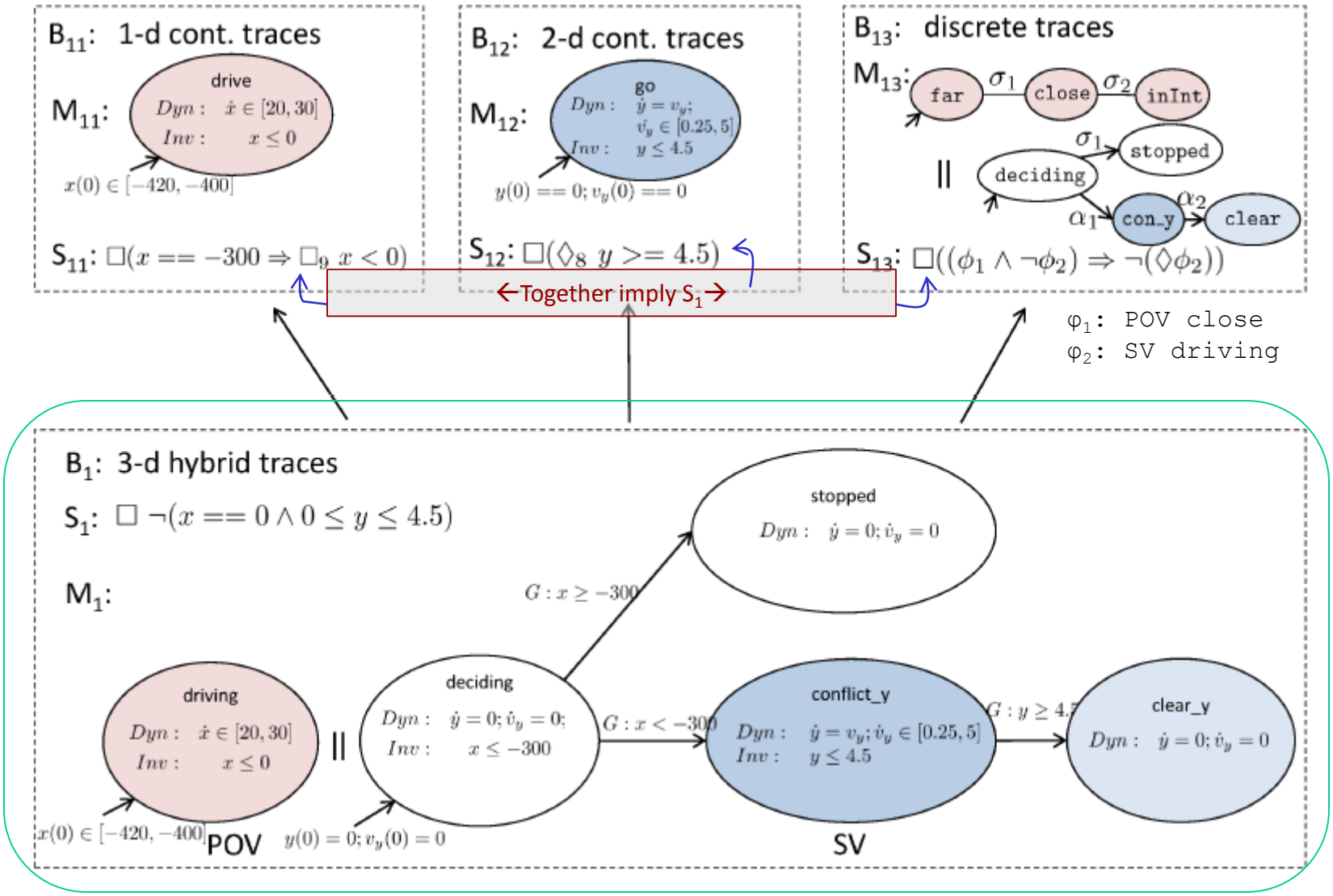
No cross straight case



$S_0 : \Box \neg ((x == 0 \wedge 0 < y < 4.5) \vee (x == 0 \wedge 0 < z < 170))$

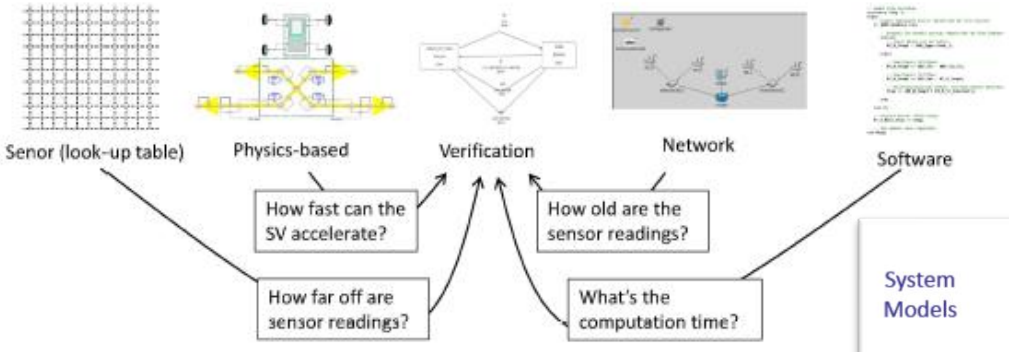
Disjunctive (OR) analysis of $M_0 \models^{B_0} S_0$

Heterogeneous verification of CICAS

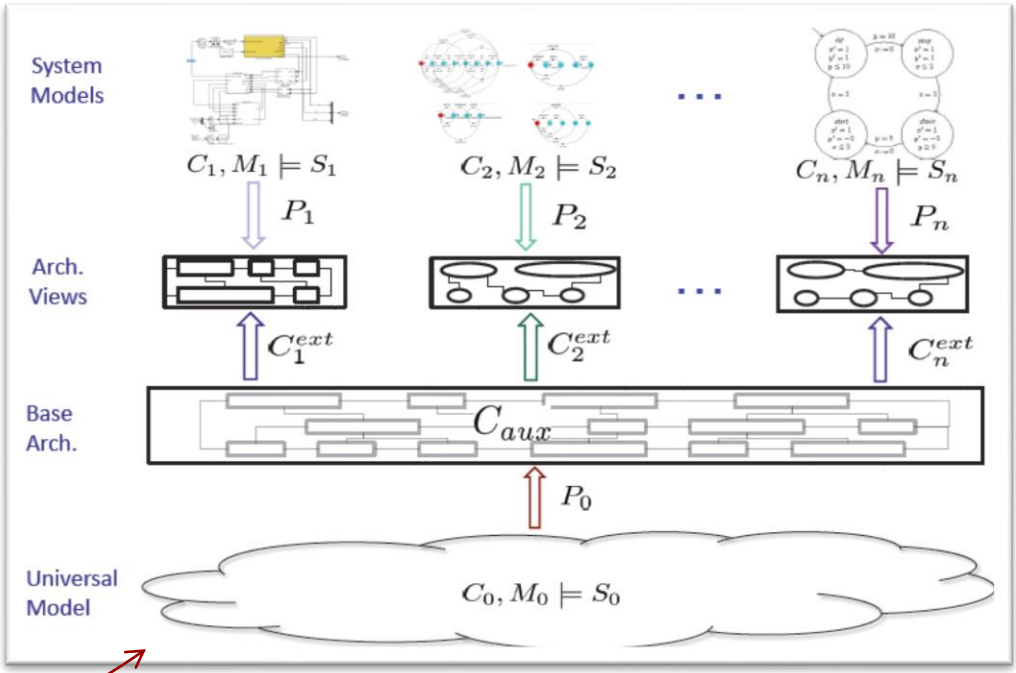


Conjunctive (AND) analysis of $M_1 \models^{B_1} S_1$

Semantic assumptions as parameter constraints



Parametric Verification in Architectural Views



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

Using Parameters in Architectural Views to Support Heterogeneous Design and Verification

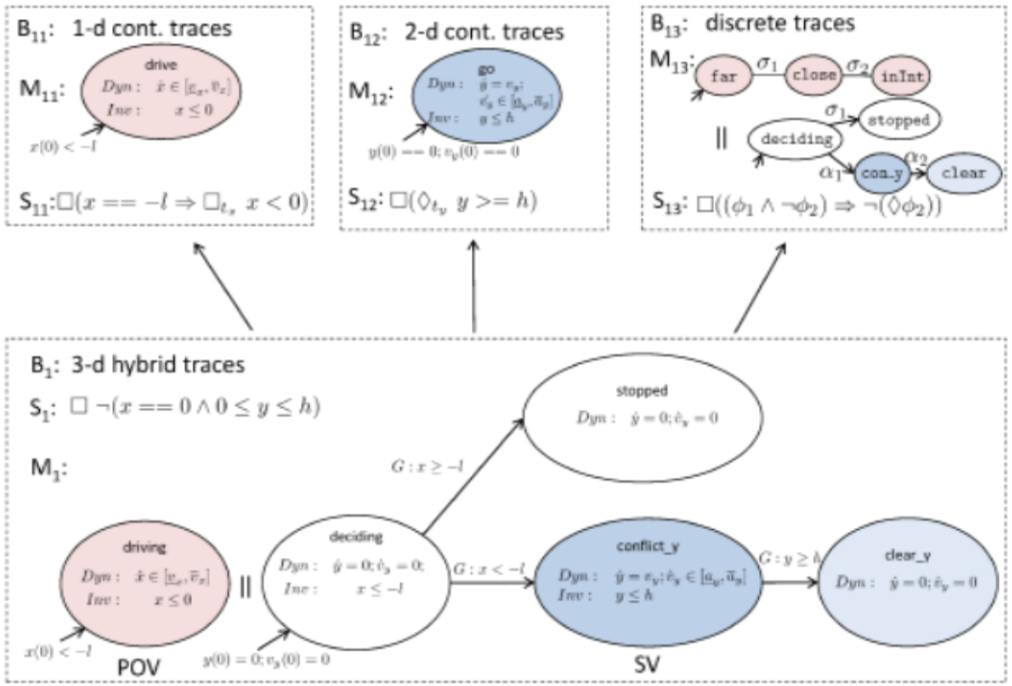
CDC '11

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

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

Parametric verification of CICAS

Parameterized models and specifications



Constraints

- C_1^M : $20 \leq M_1.\underline{v}_x \leq M_1.\overline{v}_x \leq 30 \wedge M_1.l == -300 \wedge M_1.h ==$
  $4.5 \wedge 0.25 \leq M_{12}.\underline{a}_y \leq M_{12}.\overline{a}_y \leq 5$
- C_1^S : $M_1.h == 4.5$
- C_{11}^M : $18 \leq M_{11}.\underline{v}_x \leq M_{11}.\overline{v}_x \leq 32 \wedge M_{11}.l == -300$
- C_{11}^S : $M_{11}.l == -300 \wedge 9 \leq M_{11}.t_x \leq 10$

Auxiliary constraints

$$C_{aux}: \quad (M_1.\underline{v}_x == M_{11}.\underline{v}_x) \wedge \ldots \wedge (M_1.\overline{a}_y == M_{12}.\overline{a}_y) \wedge \left(\sqrt{\frac{2h}{\overline{a}_y}} \leq t_y < t_x \leq \frac{-l}{\overline{v}_x}\right)$$

Heterogeneous Verification of Cyber-Physical Systems using Behavior Relations

HSCC '12

Akshay Rajhans
arajhans@ece.cmu.edu

Bruce H. Krogh
krogh@ece.cmu.edu

Electrical & Computer ENGINEERING