Carnegie Mellon

Electrical & Computer ENGINEERING

Heterogeneous Verification of CPS Using Behavior Semantics

Akshay Rajhans† and Bruce H. Krogh‡

Deparment of ECE, Carnegie Mellon University

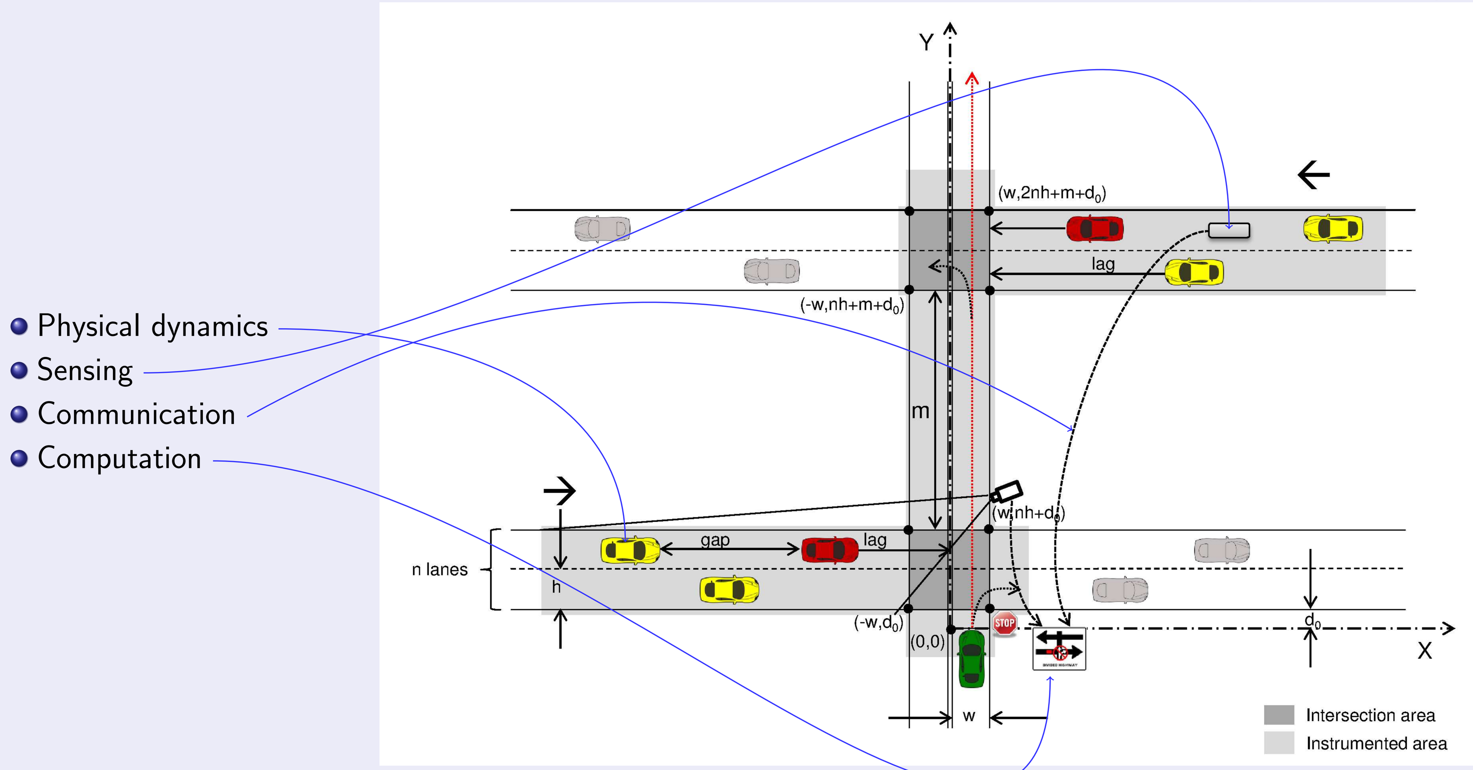
†http://users.ece.cmu.edu/~arajhans, {†arajhans, ‡krogh}@ece.cmu.edu

NSF Award # 1035800 (MEDIUM GOALI)

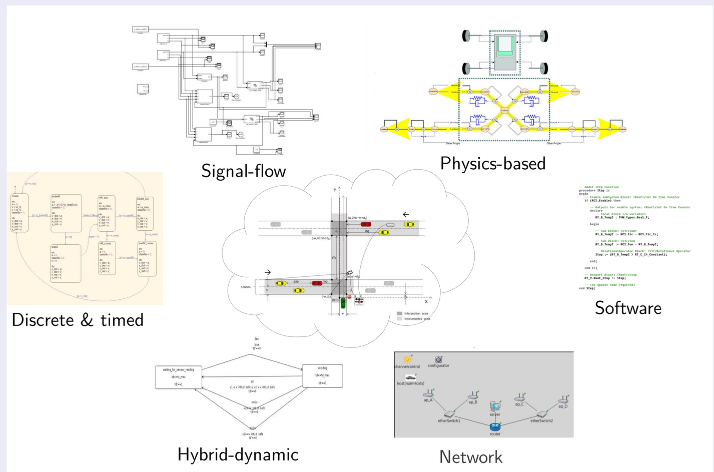
Problem Statement

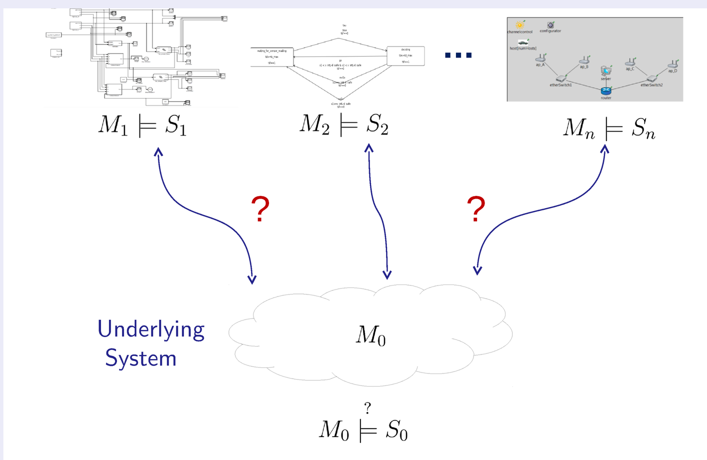
CPS are inherently heterogeneous due to tight coupling between computation, communication and physical dynamics.

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



No single modeling formalism that can capture everything.





A collection of heterogeneous models. Objective: Establish $M_0 \models S_0$ without using M_0. (M_0 cannot be modeled and/or analyzed.)

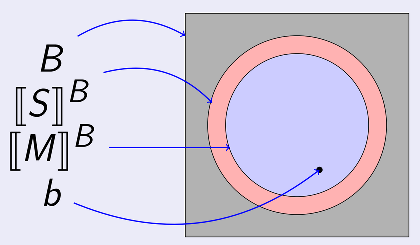
Research Challenges

How do we

- address *heterogeneity* in order to use models from different formalisms?
- use *several* heterogeneous models to verify a single underlying system?
- ensure *consistency* across heterogeneous system models?
- leverage *compositionality* in the system structure?

Behavior Semantics

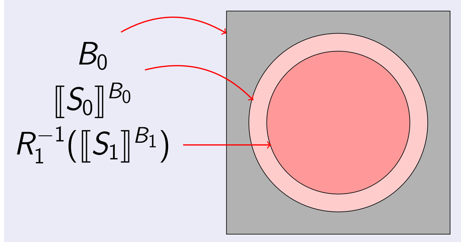
- Behaviors b are system trajectories
- Behavior domains $B \in \mathcal{B}$ are sets of behaviors in some behavior class $\mathcal{B}$. Examples: continuous trajectories, discrete traces, hybrid trajectories, ...
- Behavior semantics in a given domain B: subset of behaviors $[\![M]\!]^B \subseteq B$, $[\![S]\!]^B \subseteq B$ allowed by a model M or specification S.
- Abstraction $M_0 \sqsubseteq^B M_1$, implication $S_1 \Rightarrow^B S_0$ and entailment $M \models^B S$ are set inclusions $[\![M_0]\!]^B \subseteq [\![M_1]\!]^B$, $[\![S_1]\!]^B \subseteq [\![S_0]\!]^B$, and $[\![M]\!]^B \subseteq [\![S]\!]^B$.



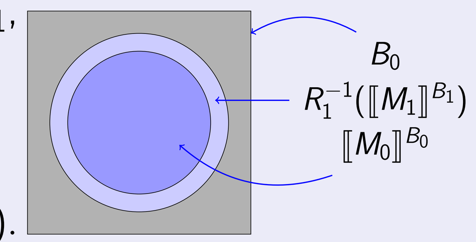
- Several analysis procedures to establish $M \models^B S$: reachability, theorem proving, (robust, Monte carlo, sensitivity) simulation, checking simulation relation, ...

Heterogeneous Verification

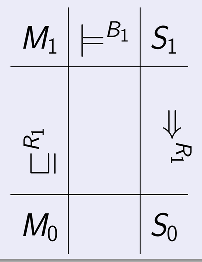
Define semantic associations between behaviors from domains $B_0 \in \mathcal{B}_0$ and $B_1 \in \mathcal{B}_1$ in terms of *behavior relations* $R \subseteq B_0 \times B_1$, or special case *behavior abstraction functions* $\mathcal{A} : B_0 \to B_1$.



Given a behavior relation $R_1 \subseteq B_0 \times B_1$,
Heterogeneous Implication:
$S_1 \Rightarrow^{R_1} S_0$, if $R_1^{-1}([\![S_1]\!]^{B_1}) \subseteq [\![S_0]\!]^{B_0}$.
Heterogeneous Abstraction:
$M_0 \sqsubseteq^{R_1} M_1$, if $[\![M_0]\!]^{B_0} \subseteq R_1^{-1}([\![M_1]\!]^{B_1})$.

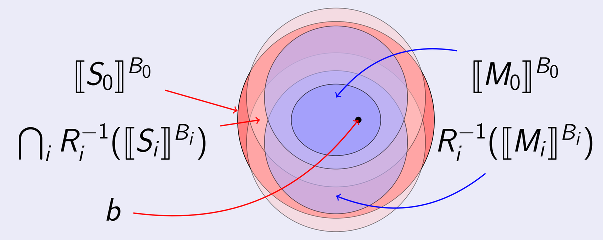


Heterogeneous Verification:
If $M_0 \sqsubseteq^{R_1} M_1$, $M_1 \models^{B_1} S_1$ and $S_1 \Rightarrow^{R_1} S_0$, then $M_0 \models^{B_0} S_0$.



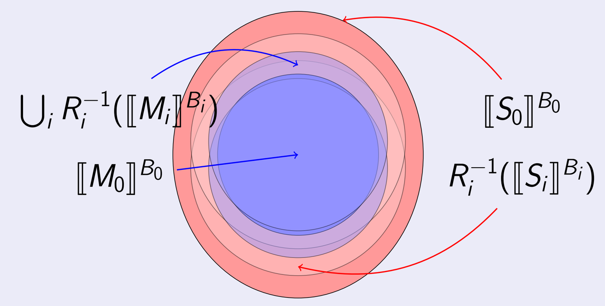
Multi-Model Heterogeneous Verification

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



Conjunctive Heterogeneous Analysis. [HSCC' 12]
If $M_0 \sqsubseteq^{R_i} M_i$, specifications S_i conjunctively imply S_0, and $M_i \models^{B_i} S_i$ for each $i = 1, \ldots, n$, $M_0 \models^{B_0} S_0$.
Proof. $[\![M_0]\!]^{B_0} \underbrace{\subseteq}_{\text{From } M_0 \sqsubseteq^{R_i} M_i} \bigcap_i R_i^{-1}([\![M_i]\!]^{B_i}) \underbrace{\subseteq}_{\text{From } M_i \models^{B_i} S_i} \bigcap_i R_i^{-1}([\![S_i]\!]^{B_i}) \underbrace{\subseteq}_{\text{Conj. Spec. Impl.}} [\![S_0]\!]^{B_0}$.

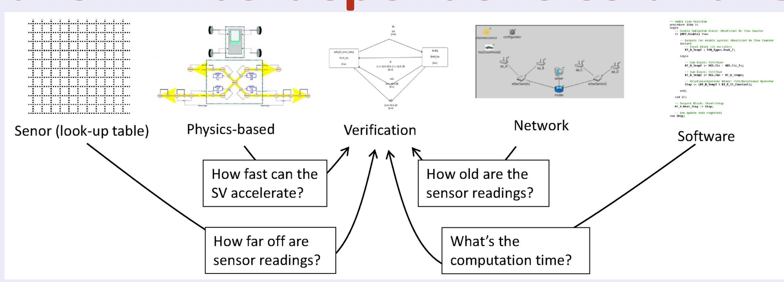
Model coverage (disjunctive abstraction).
Given behavior relations $R_i \subseteq B_0 \times B_i$, a set of models $M_1, \ldots M_n$ *cover* M_0 if $[\![M_0]\!]^{B_0} \subseteq \bigcup_i R_i^{-1}([\![M_i]\!]^{B_i})$.



Disjunctive Heterogeneous Analysis. [HSCC' 12]
If M_i cover M_0, $S_i \Rightarrow^{R_i} S_0$, and $M_i \models^{B_i} S_i$ for each $i = 1, \ldots, n$, $M_0 \models^{B_0} S_0$.
Proof. $[\![M_0]\!]^{B_0} \underbrace{\subseteq}_{\text{Coverage}} \bigcup_i R_i^{-1}([\![M_i]\!]^{B_i}) \underbrace{\subseteq}_{\text{From } M_i \models^{B_i} S_i} \bigcup_i R_i^{-1}([\![S_i]\!]^{B_i}) \underbrace{\subseteq}_{\text{From } S_i \Rightarrow^{R_i} S_0} [\![S_0]\!]^{B_0}$.

Conjunctive and disjunctive analysis constructs can be nested arbitrarily.

Inter-Formalism Interdependencies and Consistency



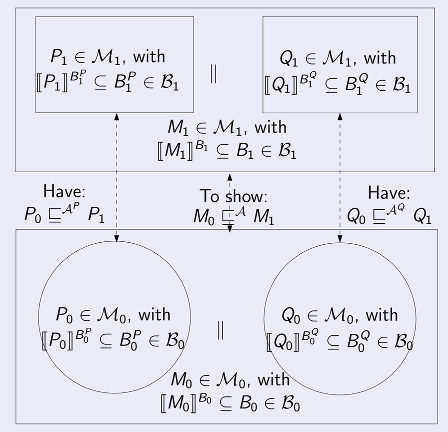
Parametric Heterogeneous Verification [CDC '11, HSCC' 12]

- **Parametric Verification:** $C_i^M(P_i), M_i \models^{B_i} C_i^S(P_i), S_i$ if $[\![C_i^M, M_i]\!]^{B_i} \subseteq [\![C_i^S, S_i]\!]^{B_i}$.
- **Verification Objective:** Establish $C_0^M, M_0 \models^{B_0} C_0^S, S_0$.
- **Interdependencies:** Auxiliary constraints $C_{aux}(P = \bigcup_{j=0}^n P_j)$ capture interdependencies between the parameter sets P_j.
- **Original-Constraint Consistency:** $E_i^M := (C_0^M \wedge C_{aux}) \downarrow_{P_i} \Rightarrow C_i^M$ and $C_i^S \Rightarrow (C_0^S \wedge C_{aux}) \downarrow_{P_i} =: E_i^S$

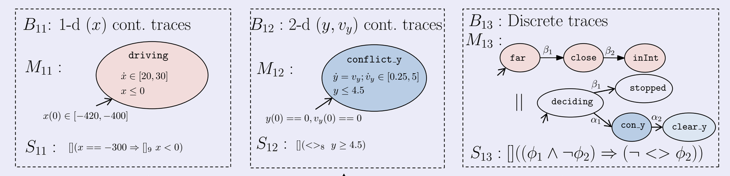
Compositional Heterogeneous Abstraction

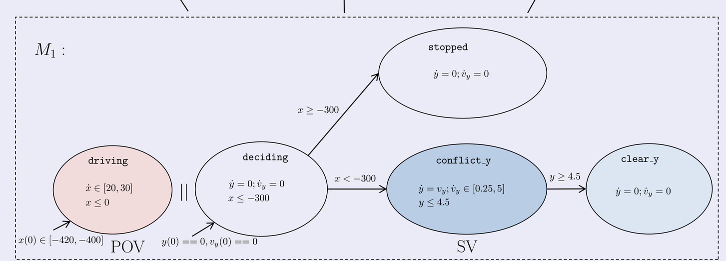
Compositional heterogeneous verification [MPM' 12]

- Need behavior abstraction functions (behavior relations not strong enough)
- Local (B_i^P, B_i^Q) vs. global (B_i) behavior domains for components and system
- Define *localization* of behavior domains and abstraction functions in terms of projection functions
- If $\mathcal{A}^P$ and $\mathcal{A}^Q$ are localizations of $\mathcal{A}$, then $P_0 \sqsubseteq^{\mathcal{A}^P} P_1$ and $Q_0 \sqsubseteq^{\mathcal{A}^Q} Q_1$ imply $M_0 \sqsubseteq^{\mathcal{A}} M_1$.



Example: CICAS-SSA



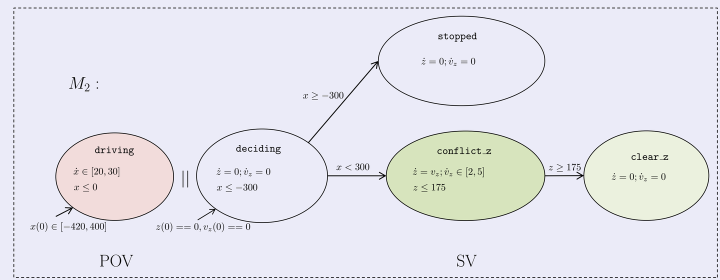


B_1 : 3-d $((x, y, v_y))$ hybrid traces

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

R_1: equal values along x, y, v_y; z, v_z zero over all time

$R_1^{-1}([\![S_1]\!]^{B_1}) : \Box\,((\neg(x == 0 \wedge 0 < y < 4.5)) \wedge (z == 0 \wedge v_z == 0))$

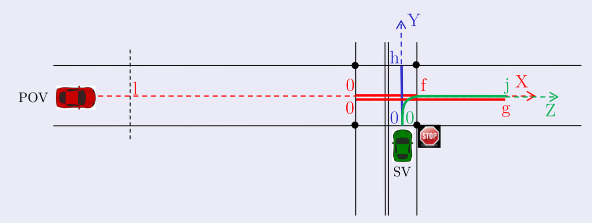


B_2 : 3-d $((x, z, v_z))$ hybrid traces

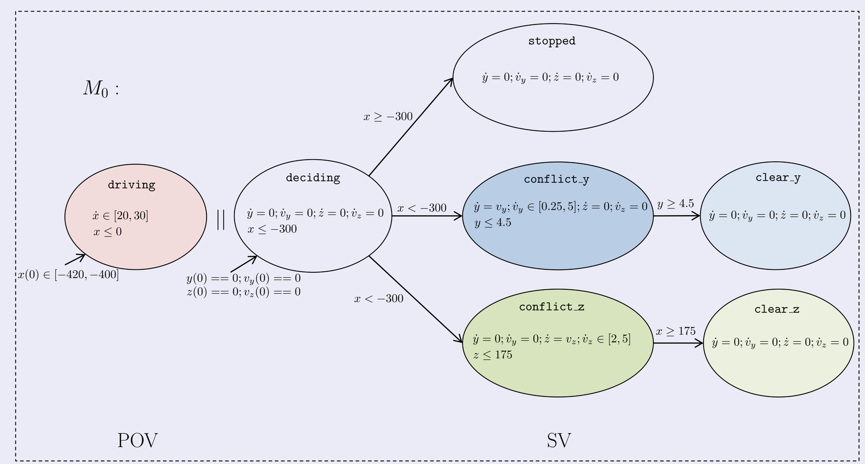
$S_2 : \Box \neg (x == 0 \wedge 0 < z < 170)$

R_2: equal values along x, z, v_z; y, v_y zero over all time

$R_2^{-1}([\![S_2]\!]^{B_2}) : \Box\,((\neg(x == 0 \wedge 0 < z < 170)) \wedge (y == 0 \wedge v_y == 0))$



A simple CICAS-SSA with one highway lane and one oncoming vehicle.



B_0 : 5-d $((x, y, v_y, z, v_z))$ hybrid traces

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

- $M_0 \models^{B_0} S_0$ established using two-level hierarchical heterogeneous verification [HSCC' 12].
- $M_1 \sqsubseteq^{\mathcal{A}} M_{13}$ established using compositional heterogeneous abstraction analysis [MPM' 12].

References

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.
In *50th IEEE Conference on Decision and Control*, Orlando, Dec 2011.

A. Rajhans and B. H. Krogh.
Heterogeneous verification of cyber-physical systems using behavior relations.
In *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control (HSCC) 2012.*

A. Rajhans and B. H. Krogh.
Compositional heterogeneous verification.
Submitted to the *6th International Workshop on Multi-Paradigm Modeling 2012 - MPM'12.*