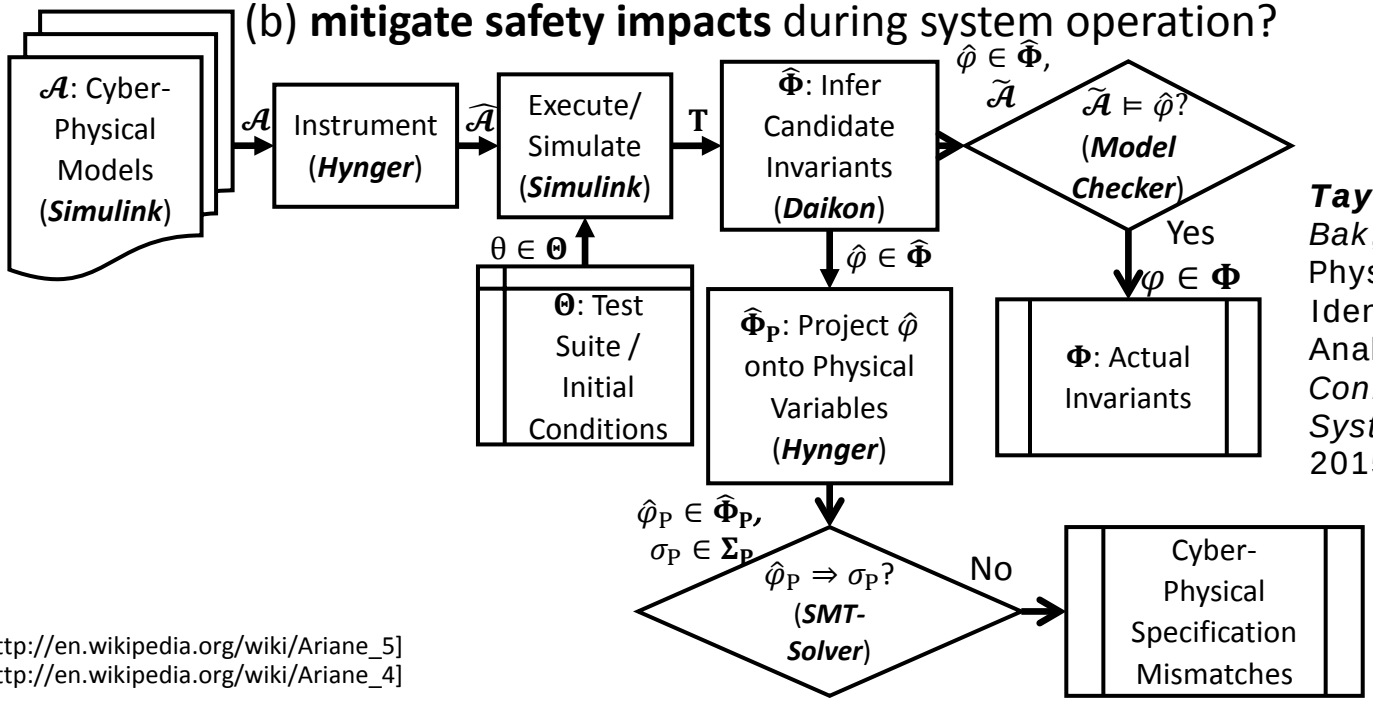
CRII: CPS: Safe Cyber-Physical Systems Upgrades

- Taylor T. Johnson
- Vanderbilt University
  - The Verification and Validation for Intelligent and Trustworthy Autonomy Laboratory (VeriVITAL)
  - Institute for Software Integrated Systems
  - Electrical Engineering & Computer Science (EECS)
- http://www.TaylorTJohnson.com
- Taylor.Johnson@Vanderbilt.edu

- NSF Awards: 1713253 (Vanderbilt), 1464311 (UT-Arlington)

Description

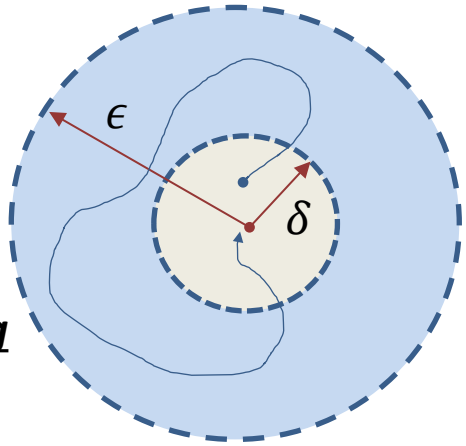
- ***Upgrades*** of cyber-physical systems (CPS) may involve (a) ***cyber components*** or (b) ***physical components***
- Design ***reuse*** common in CPS industries: e.g., Ariane 5 reused inertial measurement unit (IMU) from Ariane 4, motor vehicles across model years and models, etc.
- ***Physical system information may be encoded in software***, particularly with regards to control (e.g., parameters)
- Upgrades in CPS may yield ***cyber-physical specification mismatches***
- Can we (a) **detect mismatches** automatically at design-time and runtime and (b) **mitigate safety impacts** during system operation?



Taylor T. Johnson, *Stanley Bak*, Steven Drager, "Cyber-Physical Specification Mismatch Identification with Dynamic Analysis", *In 6th International Conference on Cyber-Physical Systems (ICCPS)*, ACM/IEEE, 2015.

[http://en.wikipedia.org/wiki/Ariane_5]
[http://en.wikipedia.org/wiki/Ariane_4]

Findings



Luan Viet Nguyen, James Kapinski, Xiaoqing Jin, Jyotirmoy Deshmukh, ***Taylor T. Johnson***, "Hyperproperties of real-valued signals", *In 15th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE)*, IEEE, 2017.

- Demonstrated feasibility to infer CPS specifications from black-box models through ***specification inference & mining*** (e.g., Daikon, s-Taliro, Breach, …)
- Automatically detect **more and/or less restrictive specifications**, indicating mismatches using satisfiability modulo theories (SMT) solvers
- Overall specification inference and mismatch detection with **Simplex architecture** to avoid safety violations at runtime
- Most impactful fundamental results are in defining generalized specifications for CPS using ***hyperproperties for signal temporal logic (HyperSTL)***, which generalize properties (sets of traces) to sets of properties (sets of sets of traces) over real-time, real-valued signals
- **Lyapunov stability is a hyperproperty**

- Specify over space of parameters and execution traces
- Cannot check Lyapunov stability with individual traces, so it is not a trace property
- Mapping parameters δ, ϵ to constant signals
- A trace $\mathbf{w} = \{w_\delta, w_\epsilon, w_{out}\}$

$$\phi_{Ly} = \{W \in P \mid \forall \mathbf{w} \in W : \exists \mathbf{w}' \in W : \forall \mathbf{w}'' \in W : w''_{out}(0) < w'_\delta(0) \Rightarrow (t > 0 \wedge w''_{out}(t) < w_\epsilon(t))\}$$

Hynger (hybrid invariant generator) software tool: https://bitbucket.org/verivital/hynger