2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

CPS: Medium: Safety-Critical Cyber-Physical Systems: From Validation & Verification to Test & Evaluation

Aaron D. Ames and Richard M. Murray, Caltech

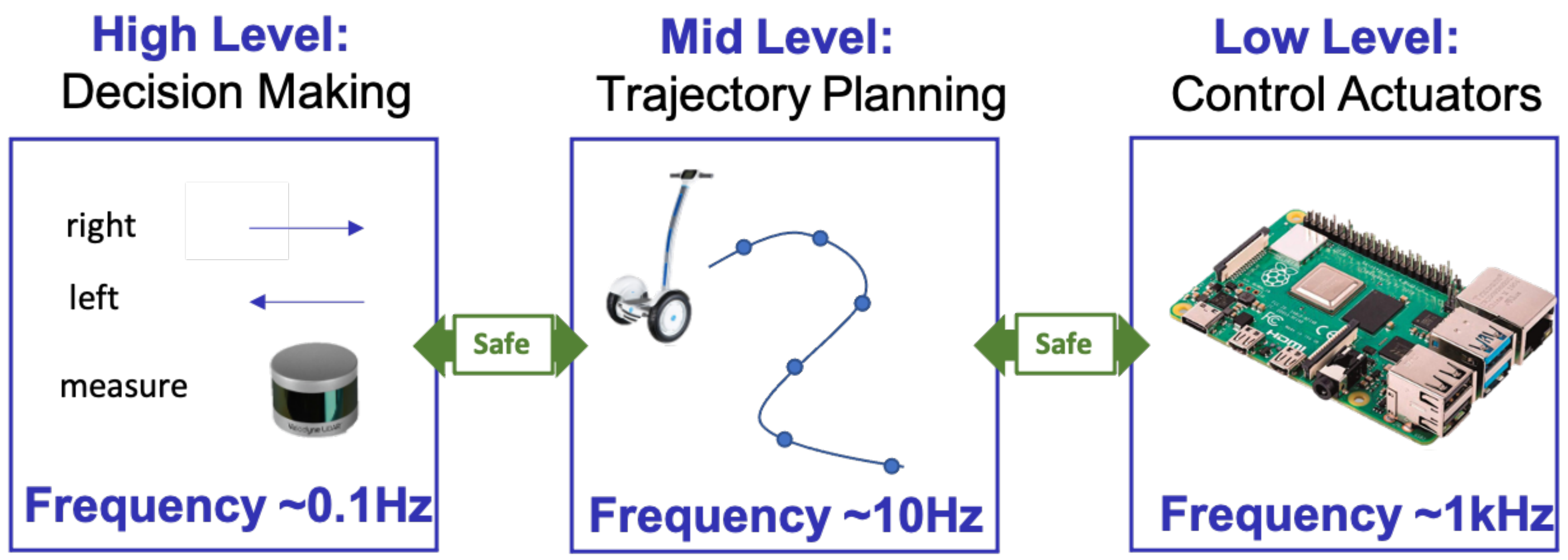
Challenge:

- *Goal:* Create a mathematical framework for T&E of safety-critical CPS, unifying formal methods and real-time constraint satisfaction
- Guarantee safety for highly dynamical systems operating in uncertain environments
- Demonstrate formal concepts experimentally

Solution:

- Developed *hierarchal multi-rate architecture* with different model abstractions at each layer
- Leverage recent advances in nonlinear control, robust predictive control, and MDPs to guarantee safety across layers
- Allows for both synthesis of provably safe controllers, and T&E of existing controllers across all layers

Award #: 1932091
Award Date: October 1, 2019
Institution: Caltech



POMDP planning

POMDP Planning

$$\mu^s = \operatorname{argmin}_\mu \ \mathbb{E}^\mu\left[\sum_{k=0}^{N} \mathbb{1}_{\mathcal{G}}(s_k^r)\right] \quad \text{s.t.} \quad \mu \in \operatorname{argmax}_\kappa \mathbb{P}^\kappa[\omega^r \models \psi^r]$$

Model Predictive Control

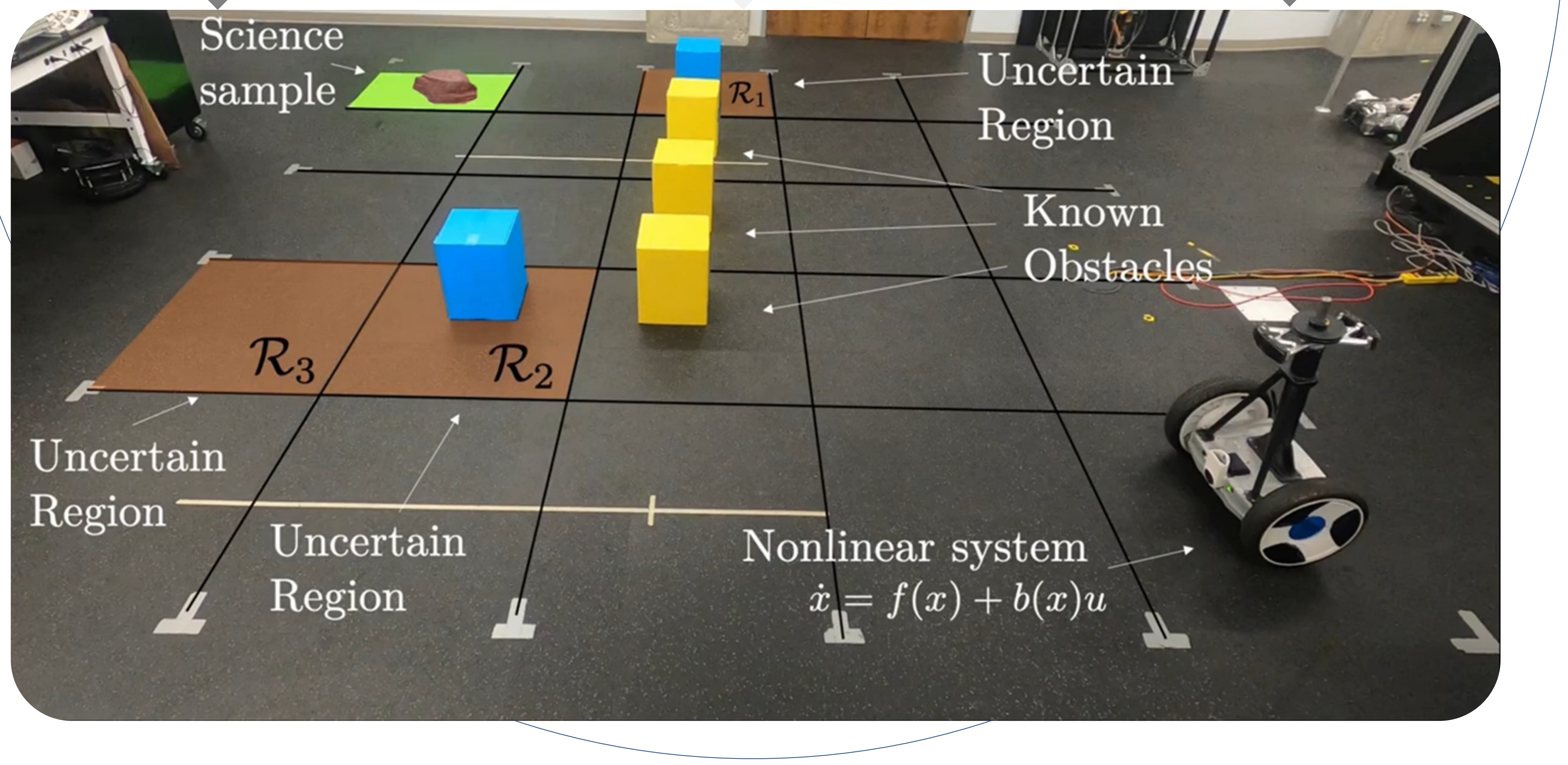
Robust MPC

$$\begin{aligned} \min_{u_0,\ldots,u_{N-1}} \quad & \sum_{t=0}^{N} l(x_k,u_k) + Q(x_N) \\ \text{s.t.} \quad & x_{k+1} = A_k x_k + B_k u_k + w_k \\ & x_k \in \mathcal{X}, u_k \in \mathcal{U}, \ \forall w_k \in \mathcal{W} \\ & x_0 = x(t), \end{aligned}$$

Control Barrier Function

CBF safe tracking

$$u^*(x) = \operatorname*{argmin}_{(u,\delta)\in U\times\mathbb{R}} \quad \|u - u_{\text{des}}(x)\|^2 \quad \text{s.t.} \quad \dot{h}(x,u) \geq -\alpha(h(x))$$



Graphical representation of multi-rate architecture and its application to a search mission with robots emulating the Mars rover.

Scientific Impact:

- Safety-critical paradigm across all layers of CPS
- Unifying framework to handle both discrete and continuous state and actions occurring at different loop rates common in CPS
- New paradigm to unify methods that are typically developed in isolation

Broader Impact:

- Guarantee Safe behavior on complex CPS: from safe synthesis to T&E
- Critical for industries deploying autonomous systems that are safety-critical: autonomous cars to space exploration
- BPC plan: leveraging Caltech WAVE program to increase representation: 2 WAVE fellows this summer.
- *Potential Impact: single test to evaluate safety-critical CPS*