Caltech

A Multi-Layer Approach to Safety-Critical Dynamic CPS

Ugo Rosolia
Postdoctoral scholar
Mechanical and Civil Engineering
Control and Dynamical Systems
California Institute of Technology

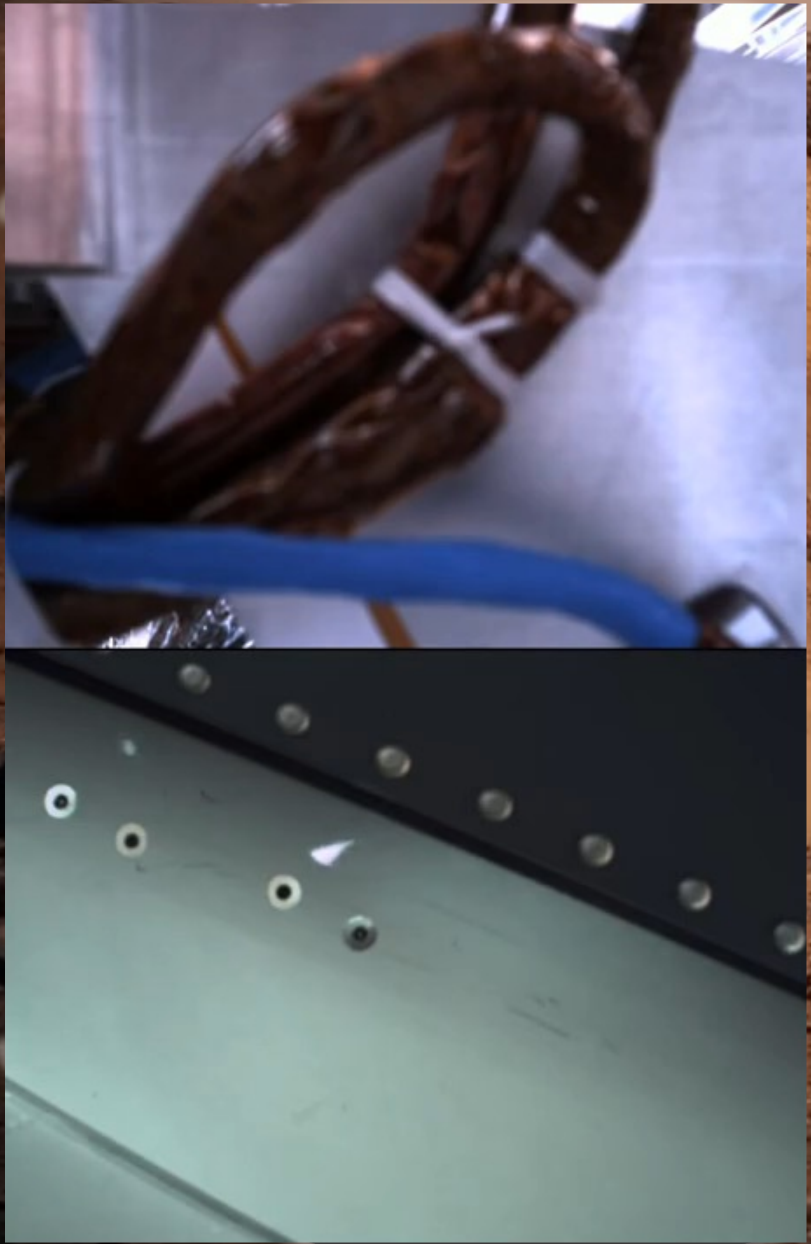
Prof. A. D. Ames
Caltech

Dr. M. Ahmadi
Caltech

A. Singletary
Caltech

AMBER LAB
www.bipedalrobotics.com

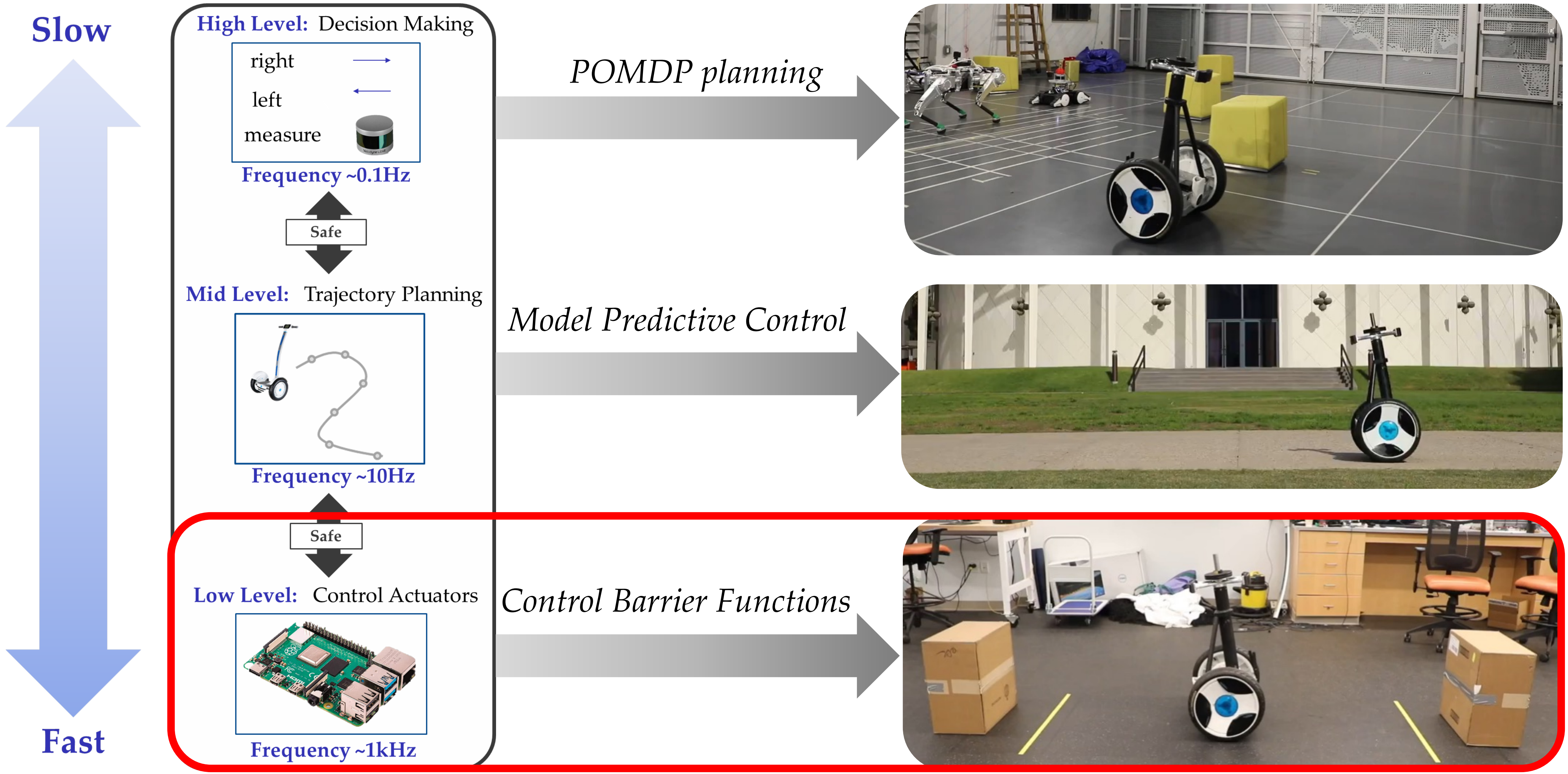
Application: Space Exploration



Guaranteeing Safe Autonomy?

Multi-Agent Autonomy

Caltech



Low-level Controllers - Bipeds

Lyapunov Controller

$$u^*(x) = \underset{(u,\delta)\in U\times\mathbb{R}}{\operatorname{argmin}} \quad \|u - u_{\text{des}}(x)\|^2$$

$$\text{s.t.} \quad \dot{V}(x,u) \leq -\alpha V(x)$$

+ Theorem ⟹ Stable Walking

Low Level: Control Actuators

Frequency ~1kHz

AMBER www.bipedalrobotics.com

Reher, AA, TRO 2021 (in prep)

Low-level Controllers - Quadrupeds

Lyapunov Controller

$$u^*(x) = \underset{(u,\delta)\in U\times\mathbb{R}}{\operatorname{argmin}} \quad \|u - u_{\text{des}}(x)\|^2$$

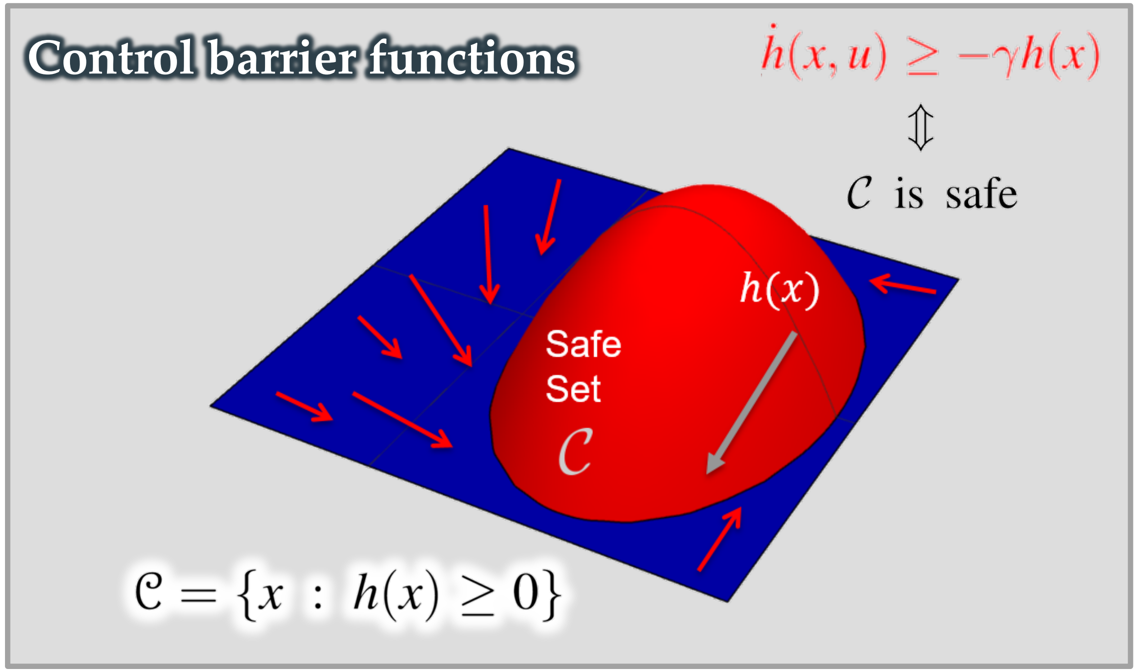
$$\text{s.t.} \quad \dot{V}(x,u) \leq -\alpha V(x)$$

+ Theorem $\Longrightarrow$ Stable Walking

Low Level: Control Actuators

Frequency ~1kHz

- Ma, AA, ICRA 2020, CSL 2020
- Ma, Csomay-Shanklin, AA, RAL/ICRA 2021 (to appear)



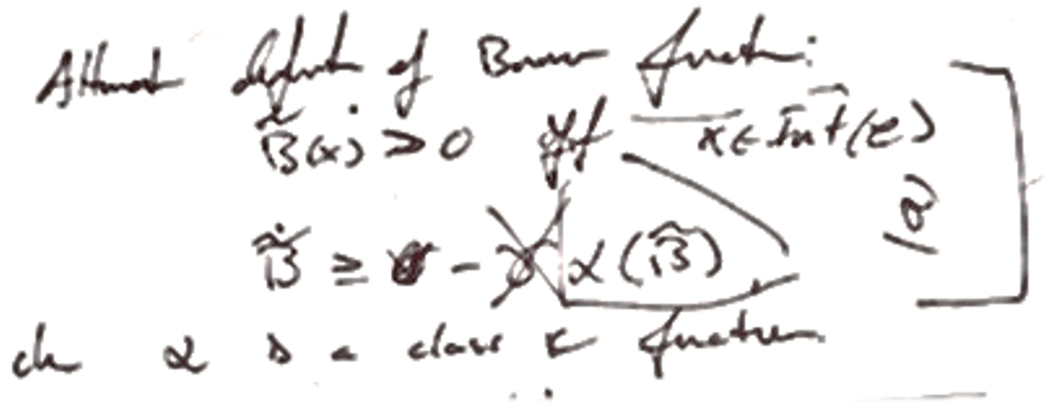
Control Barrier Functions

Provide a framework for safety-critical control:
Necessary and sufficient conditions for set invariance

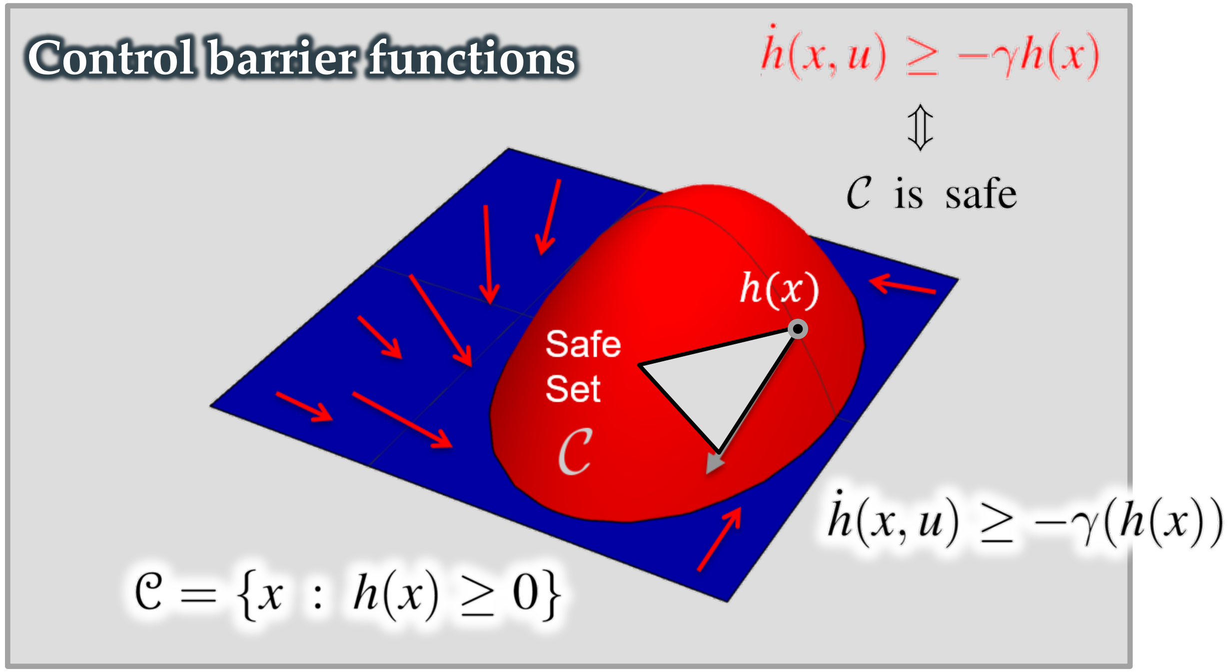
- **Dynamics:** $\dot{x} = f(x) + g(x)u$
- Safe set $\mathcal{C}$: defined by h:

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

Ames, Tabuada Grizzle (2014)



- AA, Tabuada Grizzle, CDC 2014
- AA, Xu, Tabuada Grizzle, TAC 2017



Caltech

Control Barrier Functions

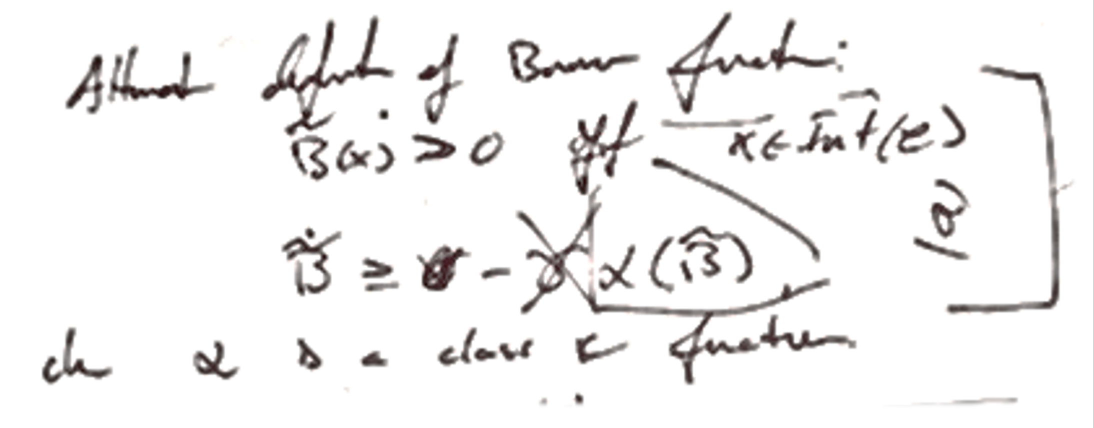
Provide a framework for safety-critical control:

Necessary and sufficient conditions for set invariance

- **Dynamics:** $\dot{x} = f(x) + g(x)u$
- Safe set $\mathcal{C}$: defined by h:

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

Ames, Tabuada Grizzle (2014)



Control Barrier Function

For all $x \in \mathcal{C}$, there exists $u \in \mathbb{R}^m$ such that:

$$\dot{h}(x,u) = \frac{\partial h}{\partial x}(x)(f(x) + g(x)u) \geq -\gamma(h(x))$$

$$\Updownarrow$$

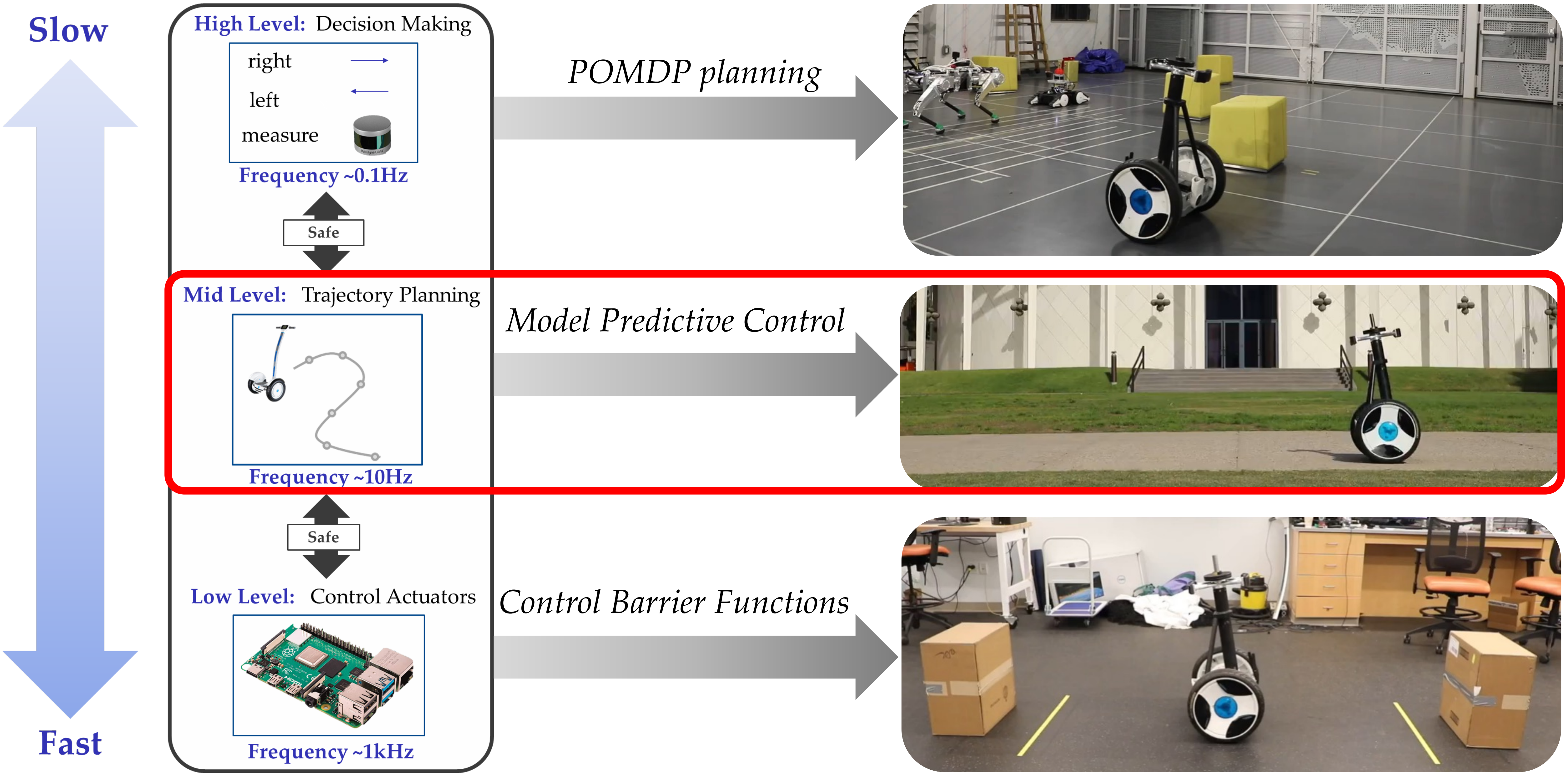
$\mathcal{C}$ is safe

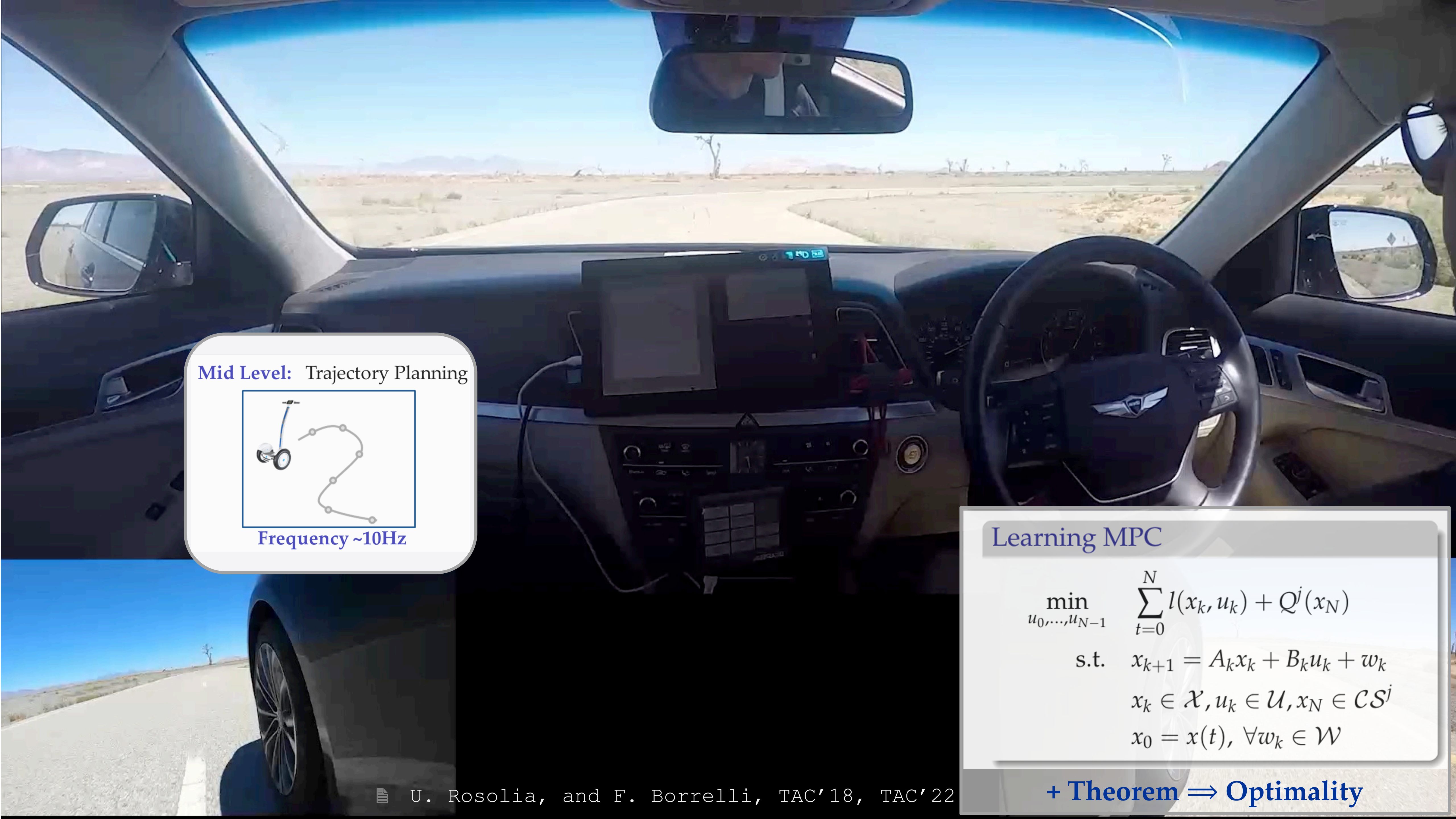
Here $\gamma : \mathbb{R} \to \mathbb{R}$ is an extended class $\mathcal{K}$ function (strictly increasing with $\gamma(0) = 0$).

- AA, Tabuada Grizzle, CDC 2014
- AA, Xu, Tabuada Grizzle, TAC 2017

Multi-Agent Autonomy

Caltech





Mid Level: Trajectory Planning

Frequency ~10Hz

Learning MPC

$$\min_{u_0,\ldots,u_{N-1}} \quad \sum_{t=0}^{N} l(x_k, u_k) + Q^j(x_N)$$

$$\text{s.t.} \quad x_{k+1} = A_k x_k + B_k u_k + w_k$$

$$x_k \in \mathcal{X}, u_k \in \mathcal{U}, x_N \in \mathcal{CS}^j$$

$$x_0 = x(t), \ \forall w_k \in \mathcal{W}$$

+ Theorem $\Longrightarrow$ Optimality

U. Rosolia, and F. Borrelli, TAC'18, TAC'22

Multi-Agent Autonomy

Caltech

Slow

Fast

High Level: Decision Making

right →

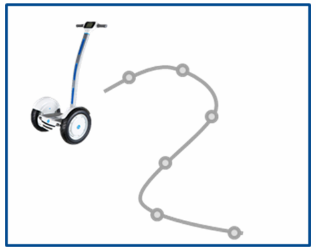
left ←

measure 

Frequency ~0.1Hz

Safe

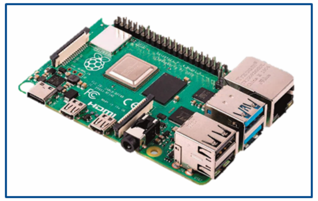
Mid Level: Trajectory Planning



Frequency ~10Hz

Safe

Low Level: Control Actuators



Frequency ~1kHz

Model Predictive Control →

Robust MPC

$$\min_{u_0,\ldots,u_{N-1}} \sum_{t=0}^{N} l(x_k, u_k) + Q(x_N)$$

$$\text{s.t.} \quad x_{k+1} = A_k x_k + B_k u_k + w_k$$

$$x_k \in \mathcal{X}, u_k \in \mathcal{U}, \ \forall w_k \in \mathcal{W}$$

$$x_0 = x(t),$$

Linearized model

Model errors

Control Barrier Functions →

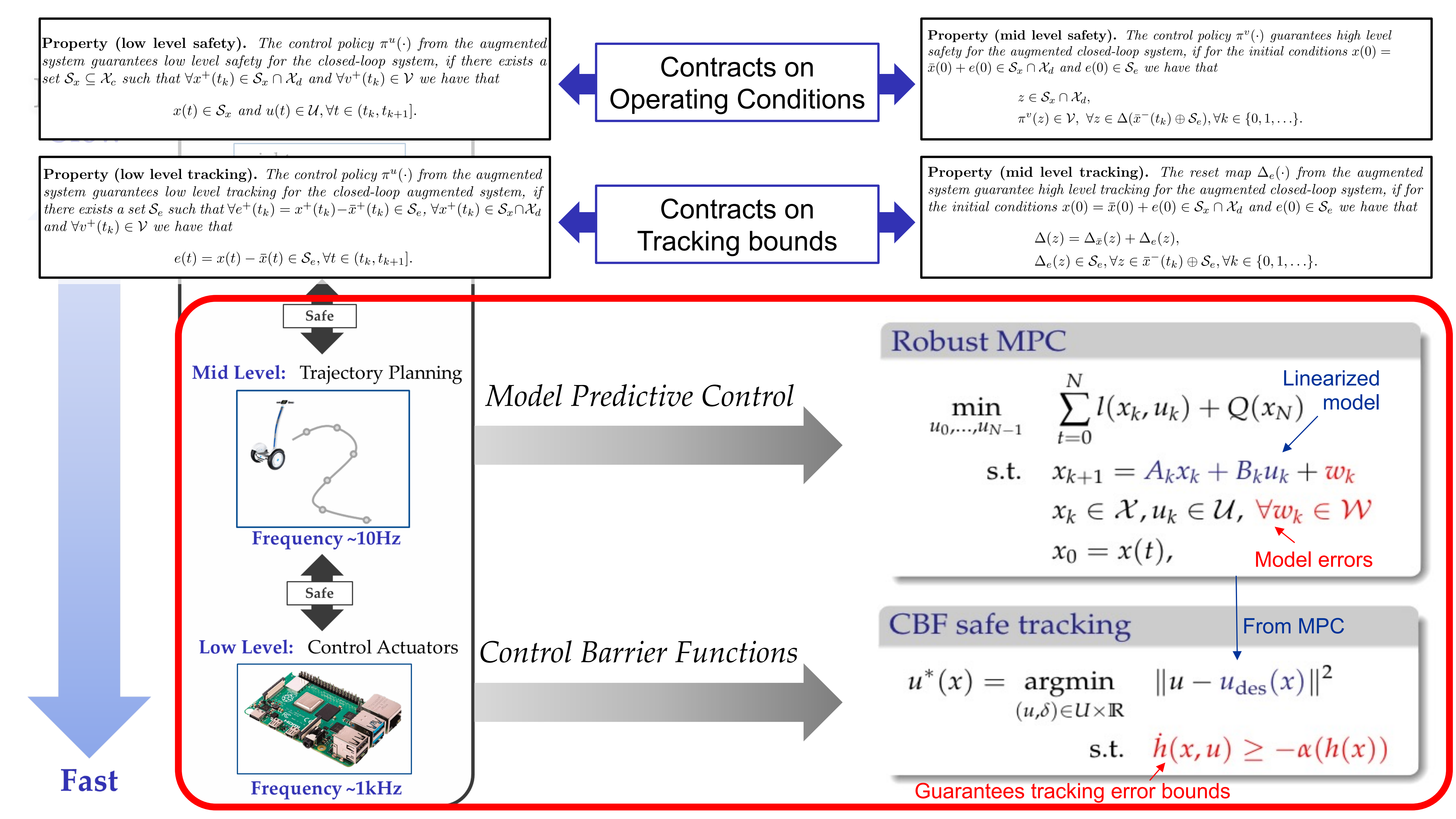
CBF safe tracking

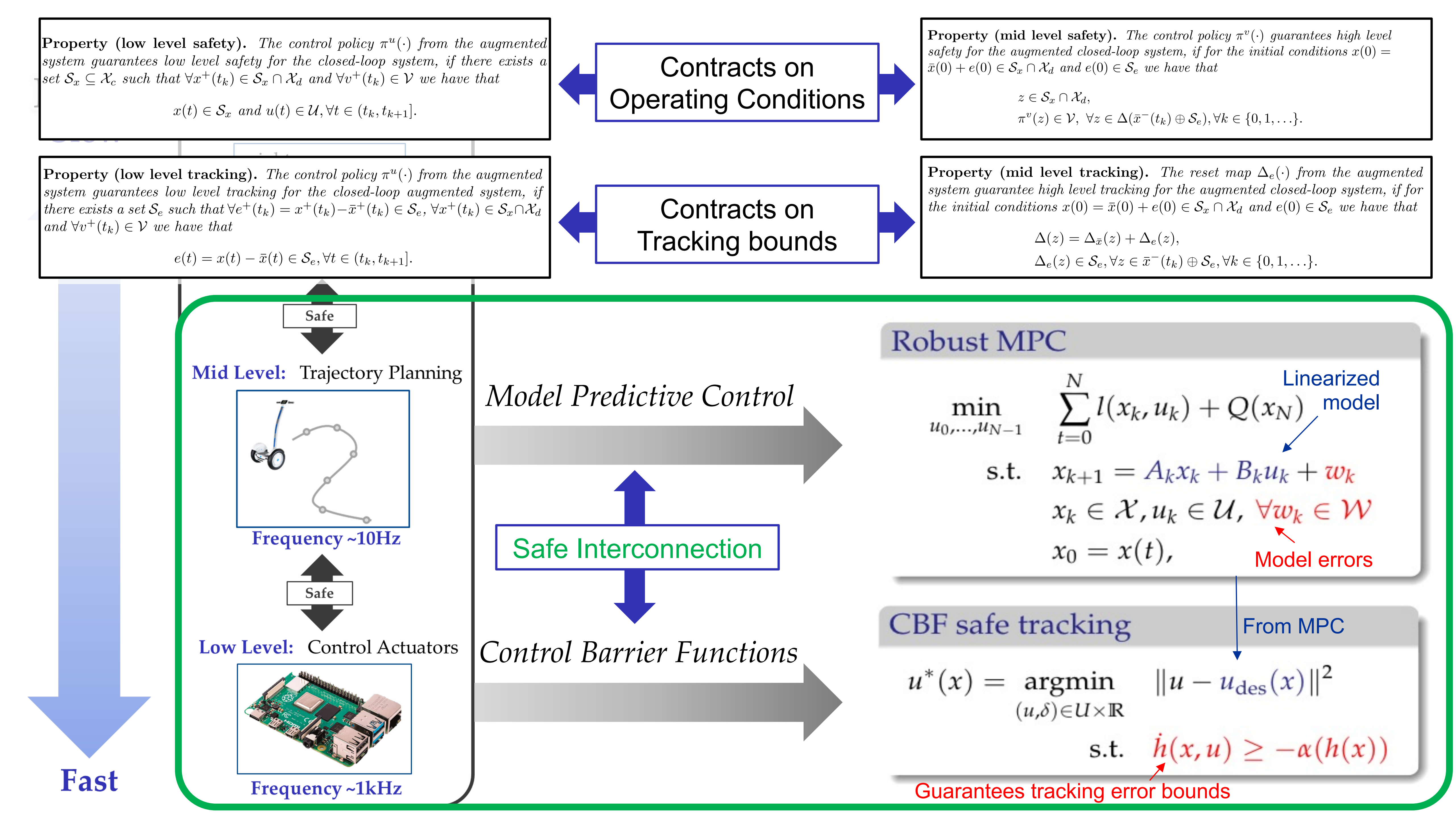
From MPC

$$u^*(x) = \underset{(u,\delta)\in U\times\mathbb{R}}{\operatorname{argmin}} \ \|u - u_{\text{des}}(x)\|^2$$

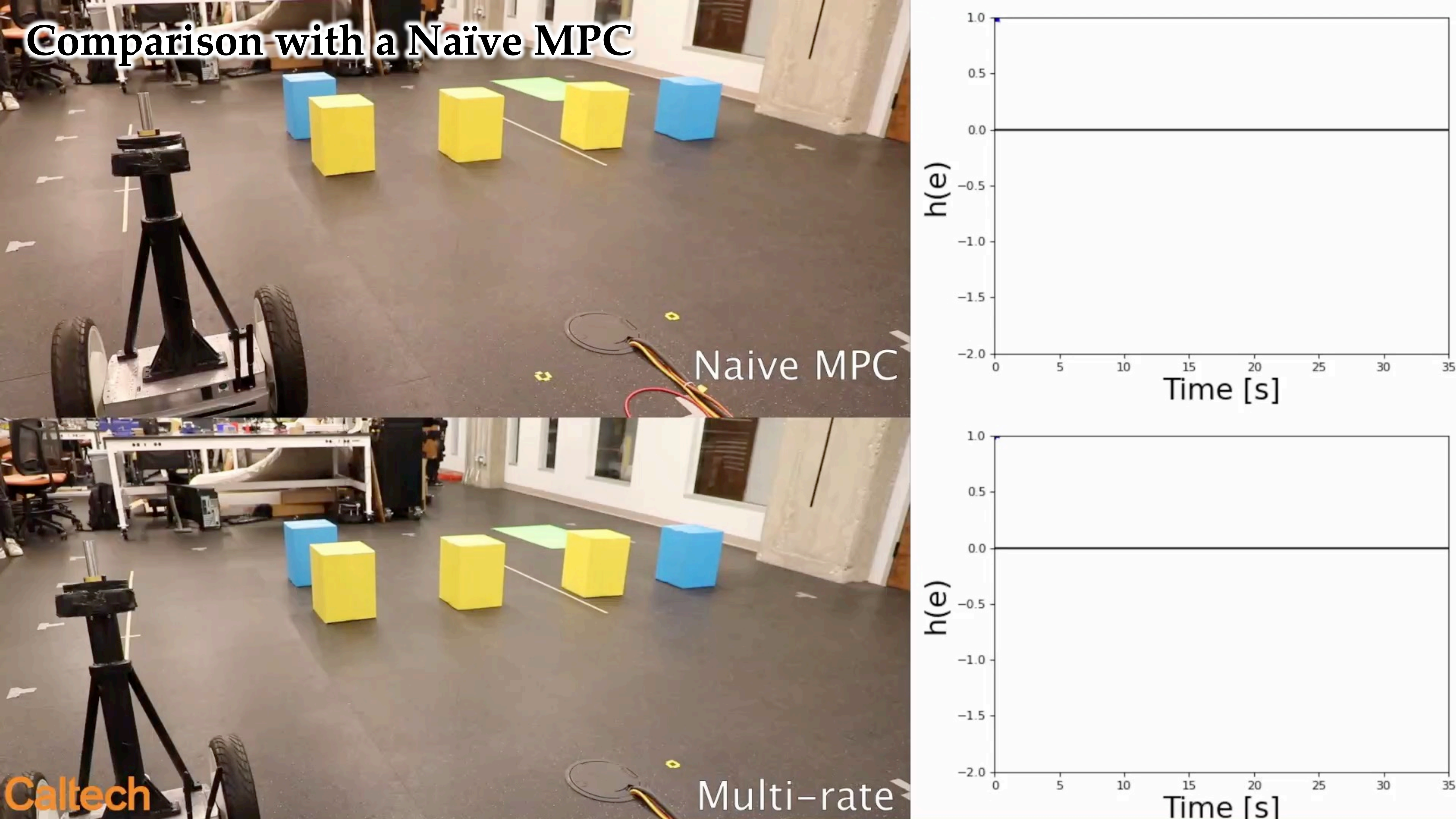
$$\text{s.t.} \quad \dot{h}(x,u) \geq -\alpha(h(x))$$

Guarantees tracking error bounds


Property (low level safety). The control policy $\pi^u(\cdot)$ from the augmented system guarantees low level safety for the closed-loop system, if there exists a set $\mathcal{S}_x \subseteq \mathcal{X}_c$ such that $\forall x^+(t_k) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $\forall v^+(t_k) \in \mathcal{V}$ we have that
$x(t) \in \mathcal{S}_x$ and $u(t) \in \mathcal{U}, \forall t \in (t_k, t_{k+1}]$.
Contracts on Operating Conditions
Property (mid level safety). The control policy $\pi^v(\cdot)$ guarantees high level safety for the augmented closed-loop system, if for the initial conditions $x(0) = \bar{x}(0) + e(0) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $e(0) \in \mathcal{S}_e$ we have that
$z \in \mathcal{S}_x \cap \mathcal{X}_d$,
$\pi^v(z) \in \mathcal{V}, \ \forall z \in \Delta(\bar{x}^-(t_k) \oplus \mathcal{S}_e), \forall k \in \{0, 1, \ldots\}$.
Property (low level tracking). The control policy $\pi^u(\cdot)$ from the augmented system guarantees low level tracking for the closed-loop augmented system, if there exists a set $\mathcal{S}_e$ such that $\forall e^+(t_k) = x^+(t_k) - \bar{x}^+(t_k) \in \mathcal{S}_e$, $\forall x^+(t_k) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $\forall v^+(t_k) \in \mathcal{V}$ we have that
$e(t) = x(t) - \bar{x}(t) \in \mathcal{S}_e, \forall t \in (t_k, t_{k+1}]$.
Contracts on Tracking bounds
Property (mid level tracking). The reset map $\Delta_e(\cdot)$ from the augmented system guarantee high level tracking for the augmented closed-loop system, if for the initial conditions $x(0) = \bar{x}(0) + e(0) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $e(0) \in \mathcal{S}_e$ we have that
$\Delta(z) = \Delta_{\bar{x}}(z) + \Delta_e(z)$,
$\Delta_e(z) \in \mathcal{S}_e, \forall z \in \bar{x}^-(t_k) \oplus \mathcal{S}_e, \forall k \in \{0, 1, \ldots\}$.
Safe
Mid Level: Trajectory Planning
Frequency ~10Hz
Safe
Low Level: Control Actuators
Frequency ~1kHz
Fast
Model Predictive Control
Control Barrier Functions
Robust MPC
$\min_{u_0,\ldots,u_{N-1}} \sum_{t=0}^{N} l(x_k, u_k) + Q(x_N)$
s.t. $x_{k+1} = A_k x_k + B_k u_k + w_k$
$x_k \in \mathcal{X}, u_k \in \mathcal{U}, \forall w_k \in \mathcal{W}$
$x_0 = x(t)$,
Linearized model
Model errors
From MPC
CBF safe tracking
$u^*(x) = \operatorname{argmin}_{(u,\delta) \in U \times \mathbb{R}} \|u - u_{des}(x)\|^2$
s.t. $\dot{h}(x, u) \geq -\alpha(h(x))$
Guarantees tracking error bounds

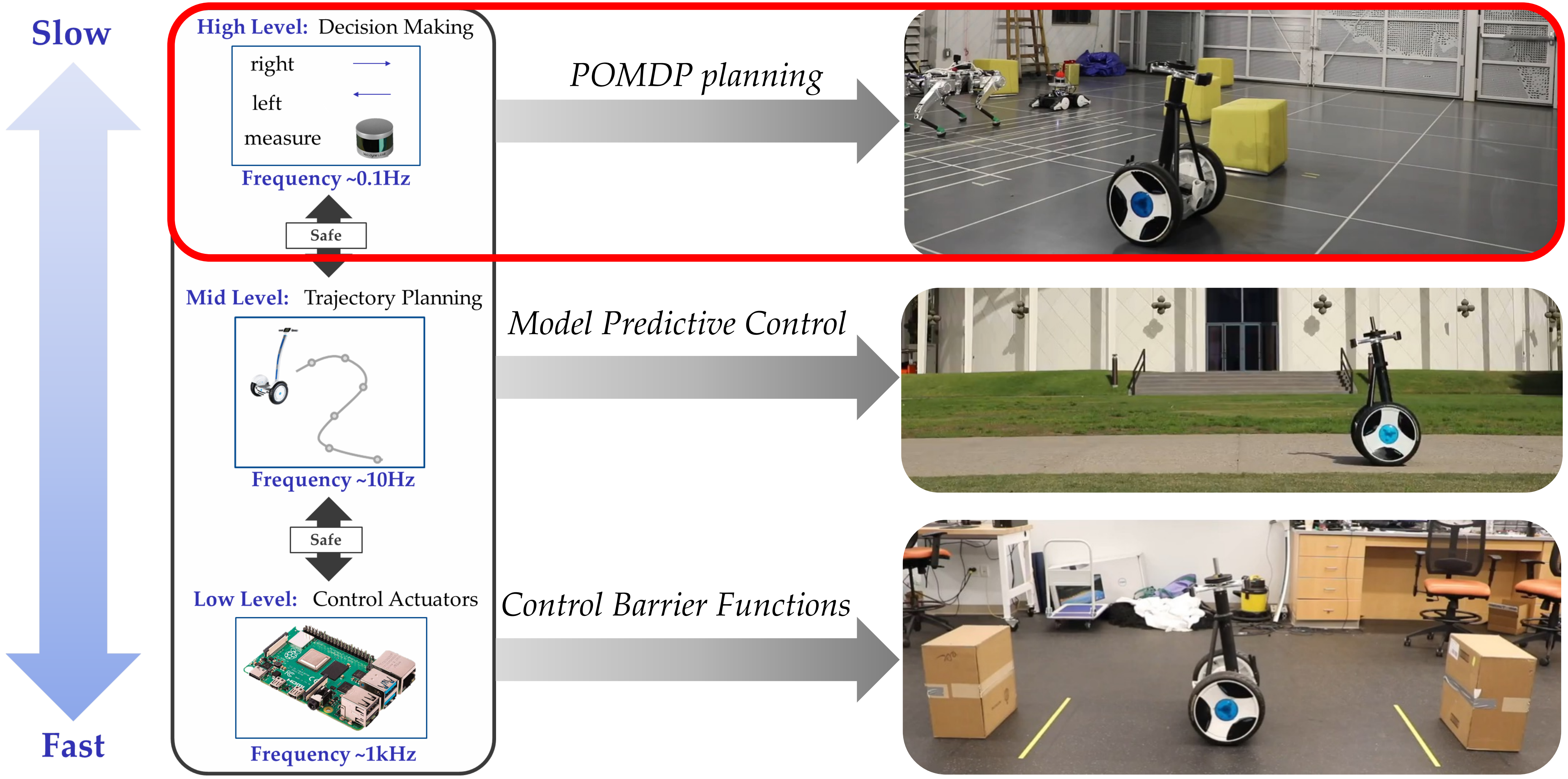


Property (low level safety). *The control policy $\pi^u(\cdot)$ from the augmented system guarantees low level safety for the closed-loop system, if there exists a set $\mathcal{S}_x \subseteq \mathcal{X}_c$ such that $\forall x^+(t_k) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $\forall v^+(t_k) \in \mathcal{V}$ we have that*
$$x(t) \in \mathcal{S}_x \text{ and } u(t) \in \mathcal{U}, \forall t \in (t_k, t_{k+1}].$$
Contracts on Operating Conditions
Property (mid level safety). *The control policy $\pi^v(\cdot)$ guarantees high level safety for the augmented closed-loop system, if for the initial conditions $x(0) = \bar{x}(0) + e(0) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $e(0) \in \mathcal{S}_e$ we have that*
$$z \in \mathcal{S}_x \cap \mathcal{X}_d,$$
$$\pi^v(z) \in \mathcal{V}, \ \forall z \in \Delta(\bar{x}^-(t_k) \oplus \mathcal{S}_e), \forall k \in \{0, 1, \dots\}.$$
Property (low level tracking). *The control policy $\pi^u(\cdot)$ from the augmented system guarantees low level tracking for the closed-loop augmented system, if there exists a set $\mathcal{S}_e$ such that $\forall e^+(t_k) = x^+(t_k) - \bar{x}^+(t_k) \in \mathcal{S}_e$, $\forall x^+(t_k) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $\forall v^+(t_k) \in \mathcal{V}$ we have that*
$$e(t) = x(t) - \bar{x}(t) \in \mathcal{S}_e, \forall t \in (t_k, t_{k+1}].$$
Contracts on Tracking bounds
Property (mid level tracking). *The reset map $\Delta_e(\cdot)$ from the augmented system guarantee high level tracking for the augmented closed-loop system, if for the initial conditions $x(0) = \bar{x}(0) + e(0) \in \mathcal{S}_x \cap \mathcal{X}_d$ and $e(0) \in \mathcal{S}_e$ we have that*
$$\Delta(z) = \Delta_{\bar{x}}(z) + \Delta_e(z),$$
$$\Delta_e(z) \in \mathcal{S}_e, \forall z \in \bar{x}^-(t_k) \oplus \mathcal{S}_e, \forall k \in \{0, 1, \dots\}.$$
Safe
Mid Level: Trajectory Planning
Frequency ~10Hz
Safe
Low Level: Control Actuators
Frequency ~1kHz
Fast
Model Predictive Control
Safe Interconnection
Control Barrier Functions
Robust MPC
$$\min_{u_0,\dots,u_{N-1}} \sum_{t=0}^{N} l(x_k, u_k) + Q(x_N)$$
Linearized model
$$\text{s.t.} \quad x_{k+1} = A_k x_k + B_k u_k + w_k$$
$$x_k \in \mathcal{X}, u_k \in \mathcal{U}, \ \forall w_k \in \mathcal{W}$$
$$x_0 = x(t),$$
Model errors
CBF safe tracking
From MPC
$$u^*(x) = \underset{(u,\delta) \in U \times \mathbb{R}}{\text{argmin}} \ \|u - u_{\text{des}}(x)\|^2$$
$$\text{s.t.} \quad \dot{h}(x,u) \geq -\alpha(h(x))$$
Guarantees tracking error bounds

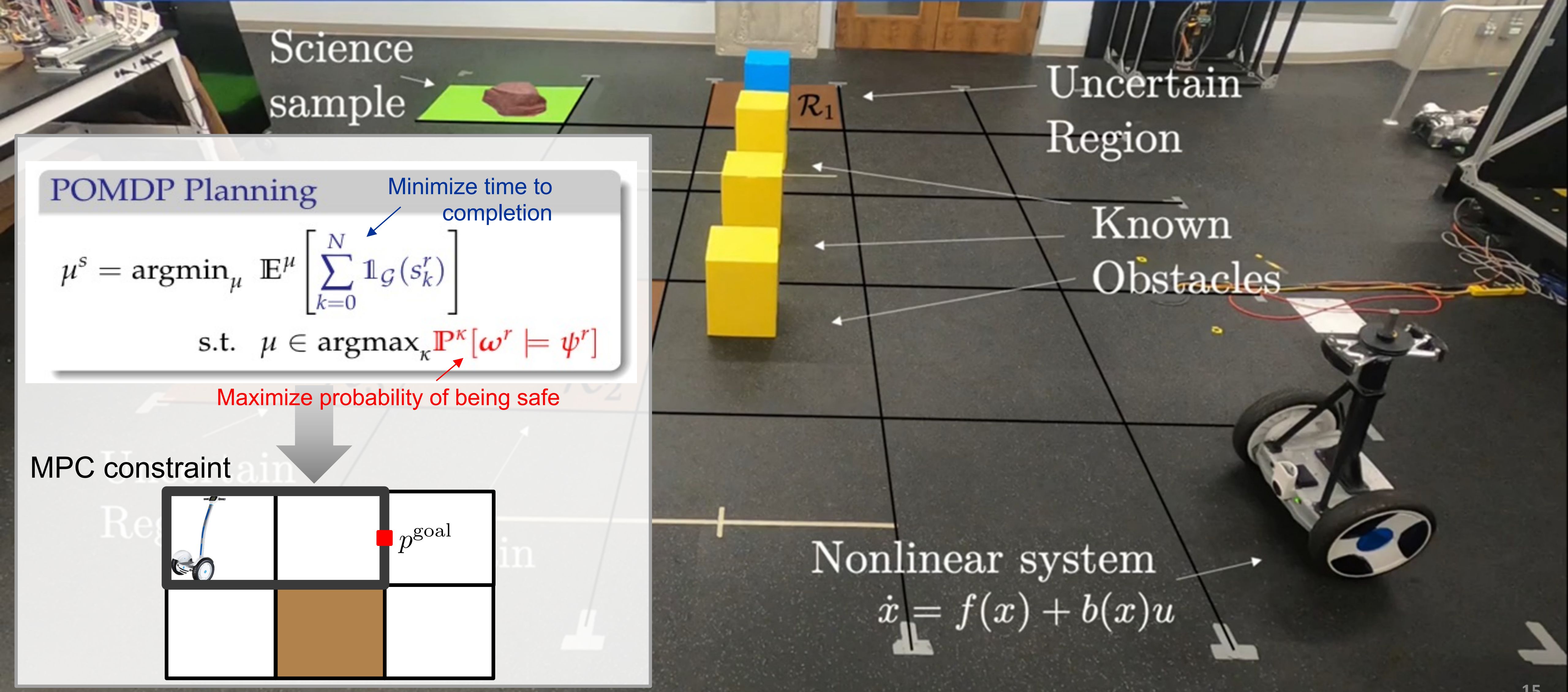

Comparison with a Naïve MPC
Naive MPC
Multi-rate
Caltech
h(e)
Time [s]
1.0
0.5
0.0
−0.5
−1.0
−1.5
−2.0
0
5
10
15
20
25
30
35
h(e)
Time [s]

Multi-Agent Autonomy

Caltech

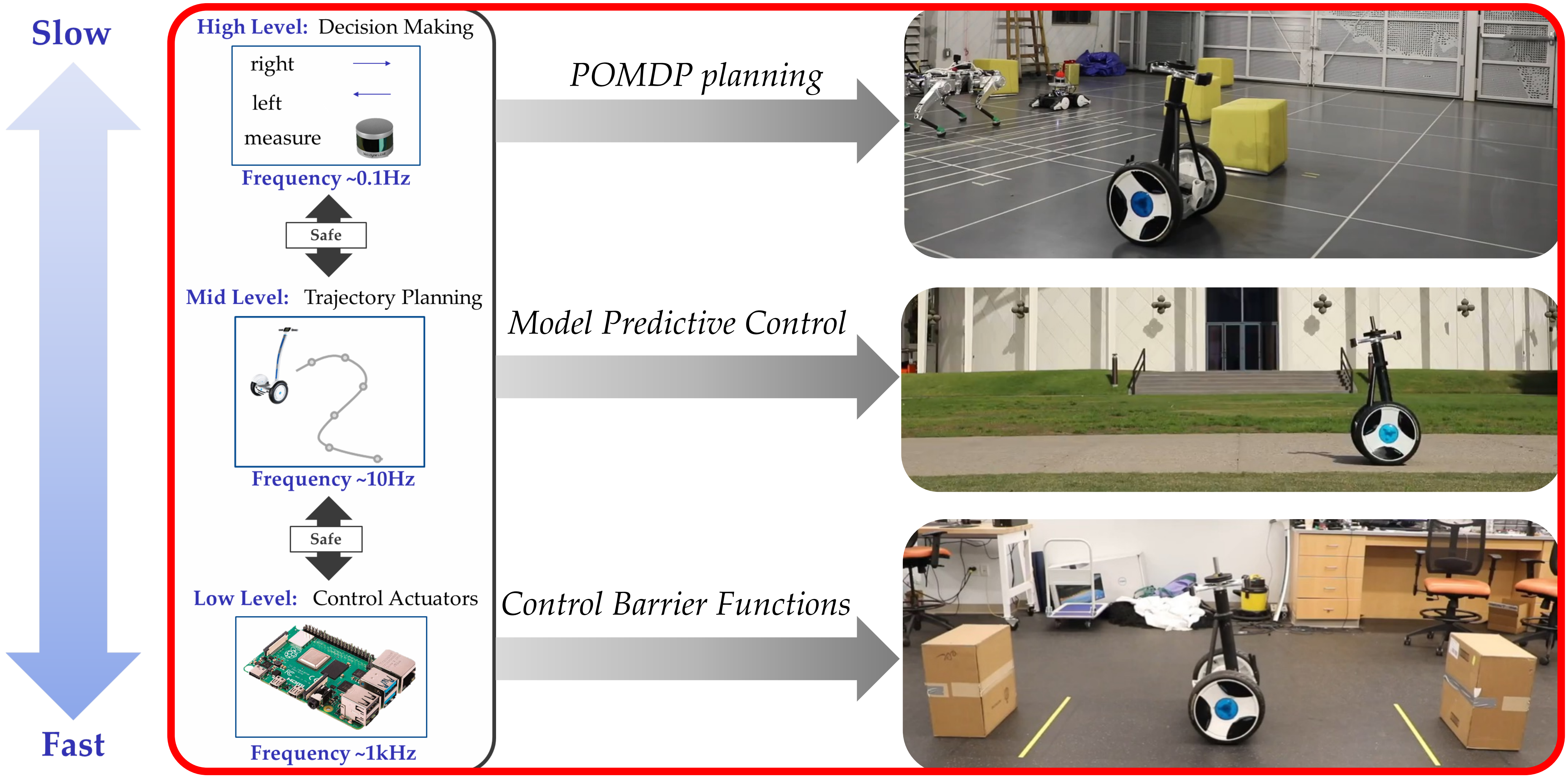


The mission objective is to find the science sample given partial environment observations



Rosolia and AA, CSL/CDC 2020, TAC 2021 (submitted)

Multi-Agent Autonomy



Multi-Agent Autonomy

Caltech

Slow

Fast

High Level: Decision Making

right →

left ←

measure

Frequency ~0.1Hz

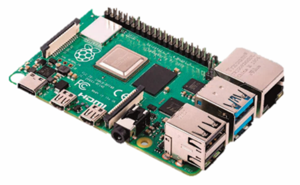
Safe

Mid Level: Trajectory Planning

Frequency ~10Hz

Safe

Low Level: Control Actuators



Frequency ~1kHz

POMDP planning

Model Predictive Control

Control Barrier Functions

POMDP Planning

Minimize time to completion

$$\mu^s = \text{argmin}_\mu \; \mathbb{E}^\mu \left[\sum_{k=0}^{N} \mathbb{1}_G(s_k^r) \right]$$

$$\text{s.t.} \quad \mu \in \text{argmax}_\kappa \mathbb{P}^\kappa[\omega^r \models \psi^r]$$

Maximize probability of being safe

Robust MPC

$$\min_{u_0,\ldots,u_{N-1}} \sum_{t=0}^{N} l(x_k, u_k) + Q(x_N)$$

$$\text{s.t.} \quad x_{k+1} = A_k x_k + B_k u_k + w_k$$

$$x_k \in \mathcal{X}, u_k \in \mathcal{U}, \; \forall w_k \in \mathcal{W}$$

$$x_0 = x(t),$$

Linearized model

Model errors

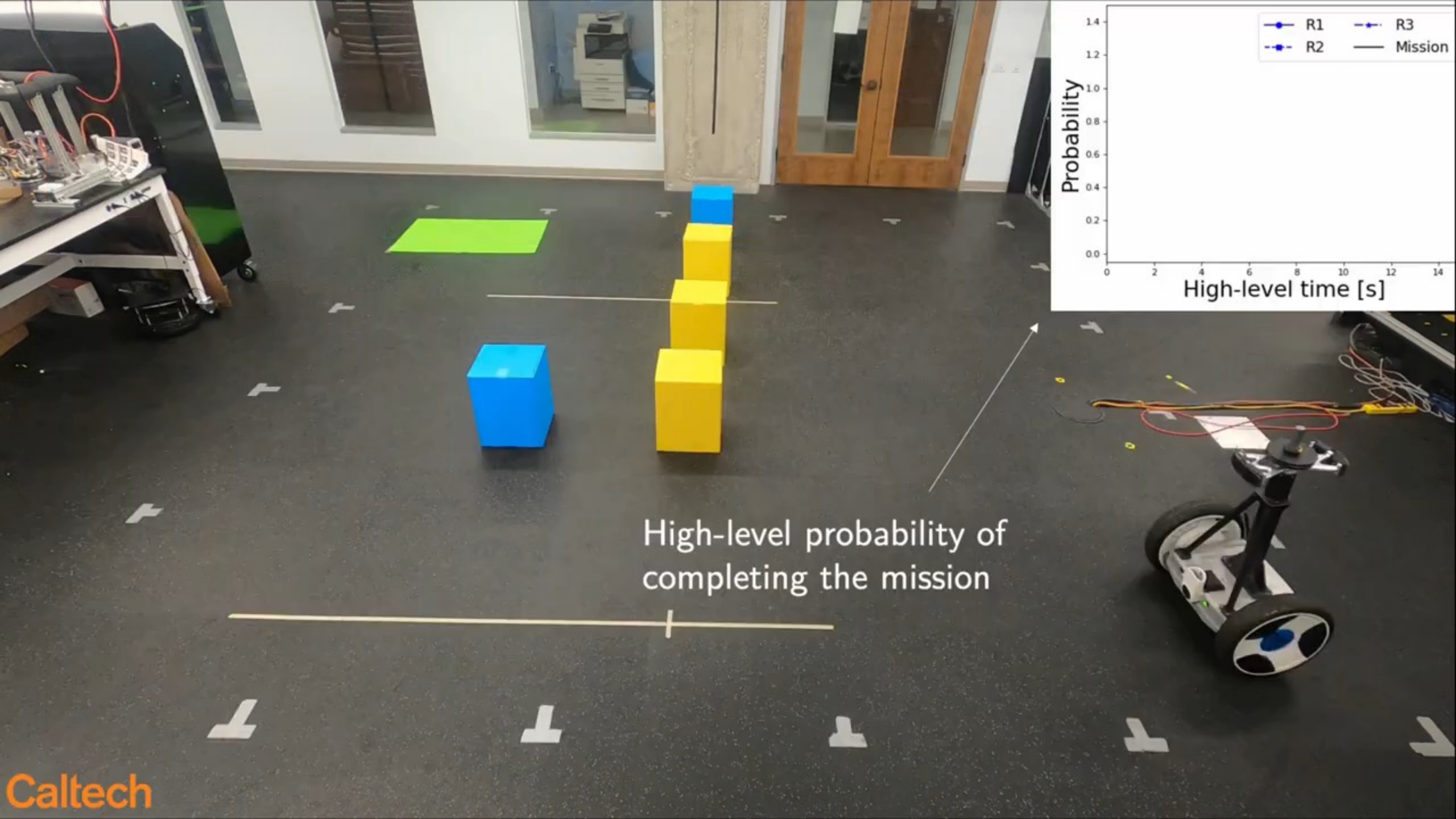
CBF safe tracking

From MPC

$$u^*(x) = \underset{(u,\delta) \in U \times \mathbb{R}}{\text{argmin}} \; \|u - u_{\text{des}}(x)\|^2$$

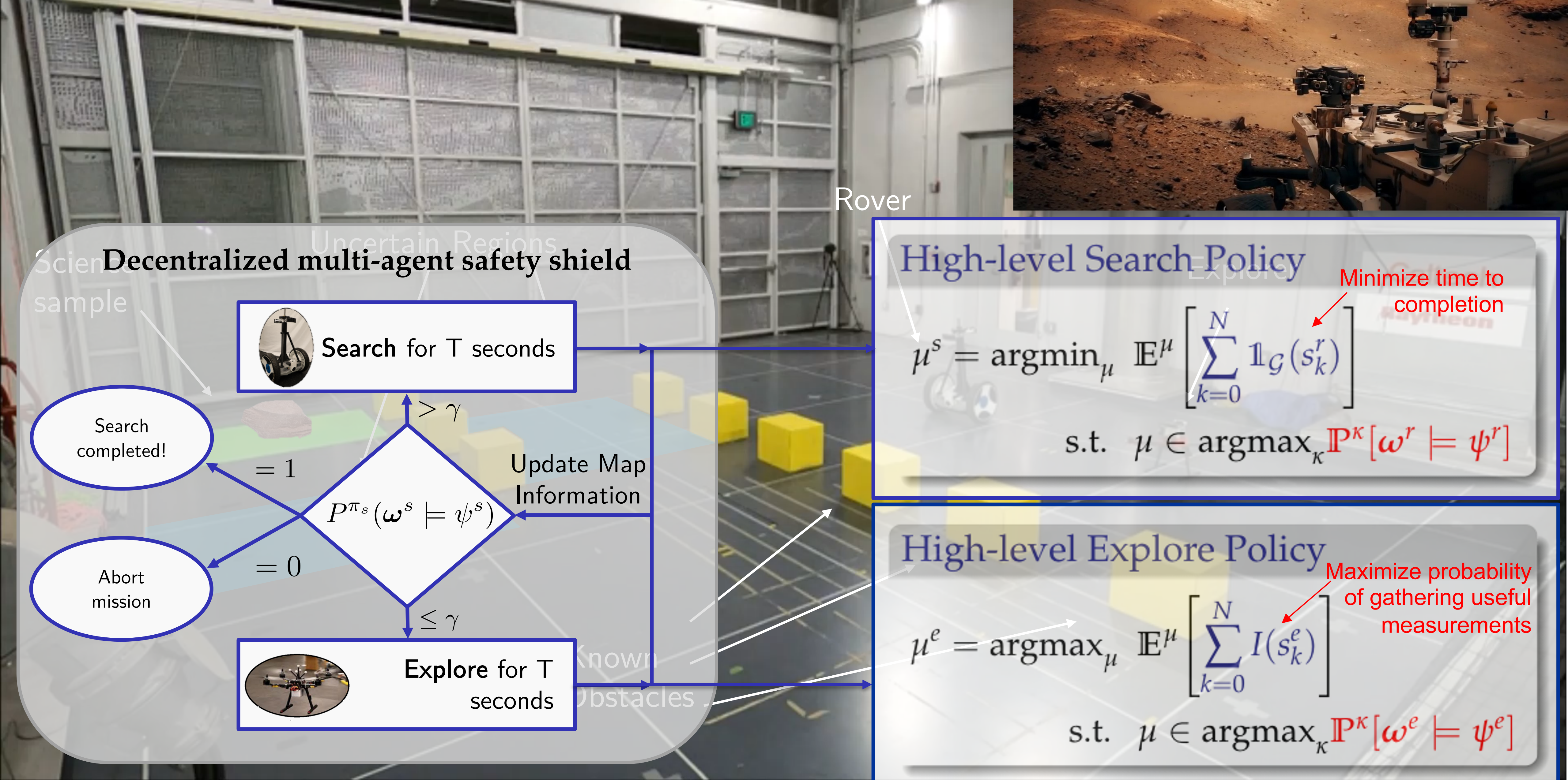
$$\text{s.t.} \quad \dot{h}(x, u) \geq -\alpha(h(x))$$

Guarantees tracking error bounds



R1
R2
R3
Mission
Probability
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
0
2
4
6
8
10
12
14
High-level time [s]
High-level probability of completing the mission
Caltech

Cooperative Task and Path Planning

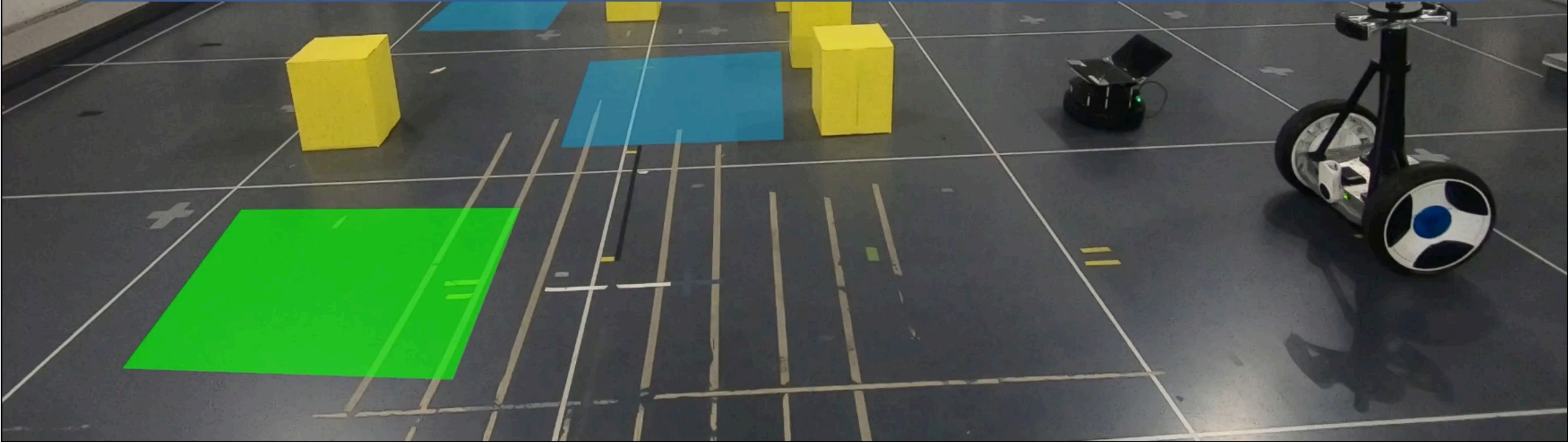


Cooperative Task and Path Planning

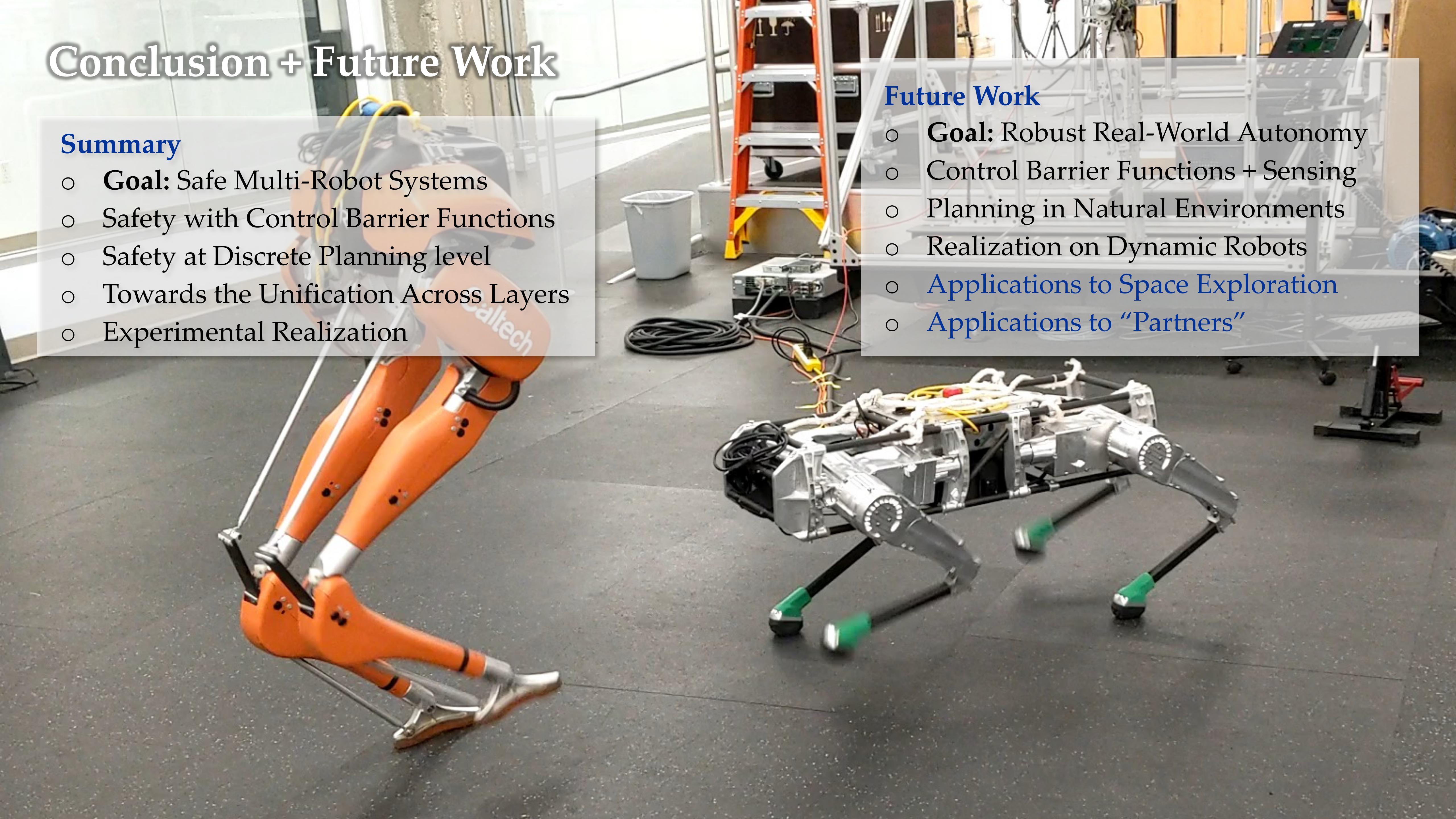
Caltech

A Hierarchical Approach for Mission Planning in Partially Observable Environments

Ugo Rosolia, Andrew Singletary, Yuxiao Chen, Aaron D. Ames



Conclusion + Future Work

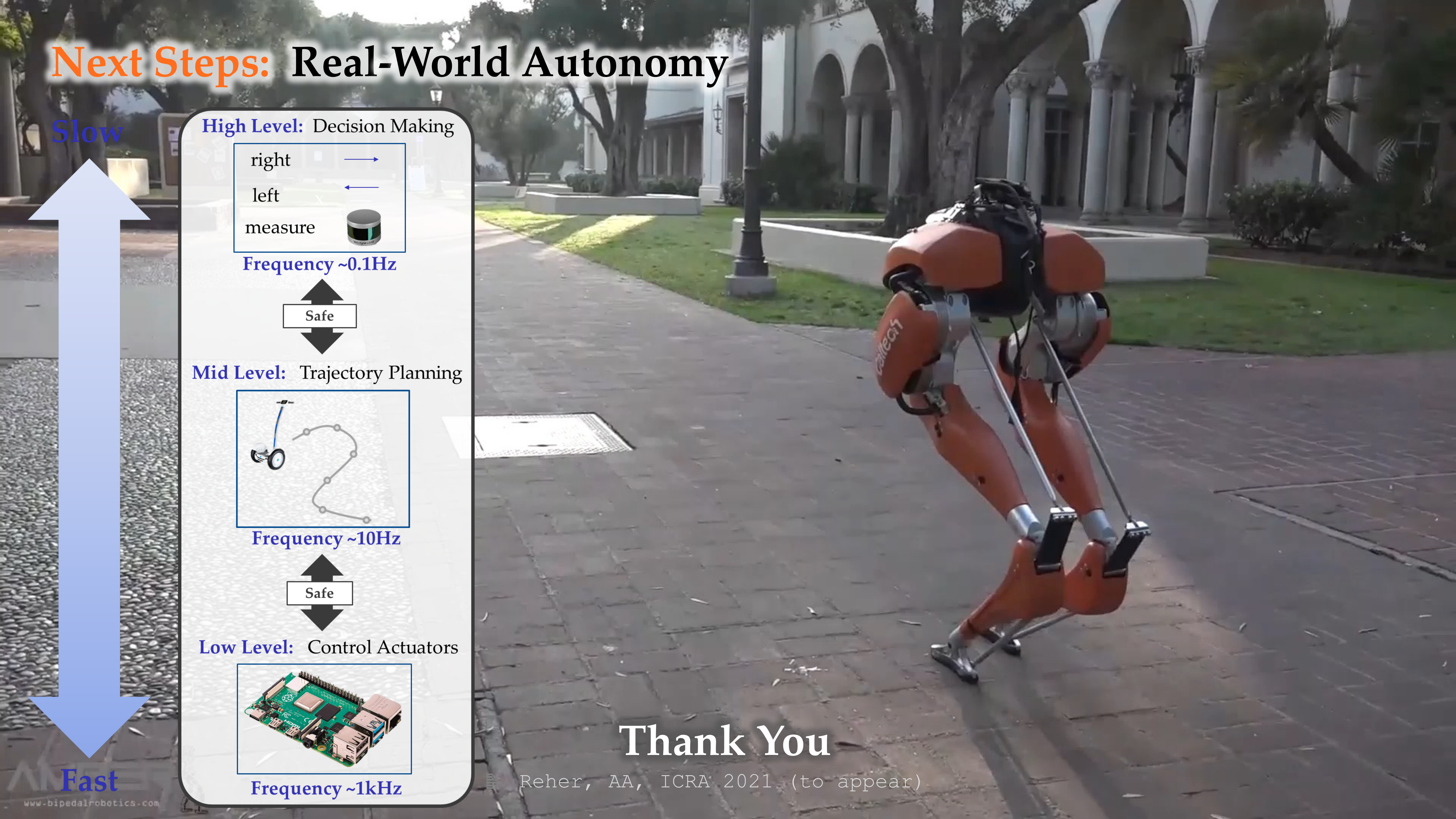


Summary

- **Goal:** Safe Multi-Robot Systems
- Safety with Control Barrier Functions
- Safety at Discrete Planning level
- Towards the Unification Across Layers
- Experimental Realization

Future Work

- **Goal:** Robust Real-World Autonomy
- Control Barrier Functions + Sensing
- Planning in Natural Environments
- Realization on Dynamic Robots
- Applications to Space Exploration
- Applications to "Partners"


Next Steps: Real-World Autonomy
Slow
High Level: Decision Making
right
left
measure
Frequency ~0.1Hz
Safe
Mid Level: Trajectory Planning
Frequency ~10Hz
Safe
Low Level: Control Actuators
Frequency ~1kHz
Fast
www.bipedalrobotics.com
Thank You
Reher, AA, ICRA 2021 (to appear)