Generating Formal Safety Assurances for High-Dimensional Reachability

Albert Lin and Somil Bansal

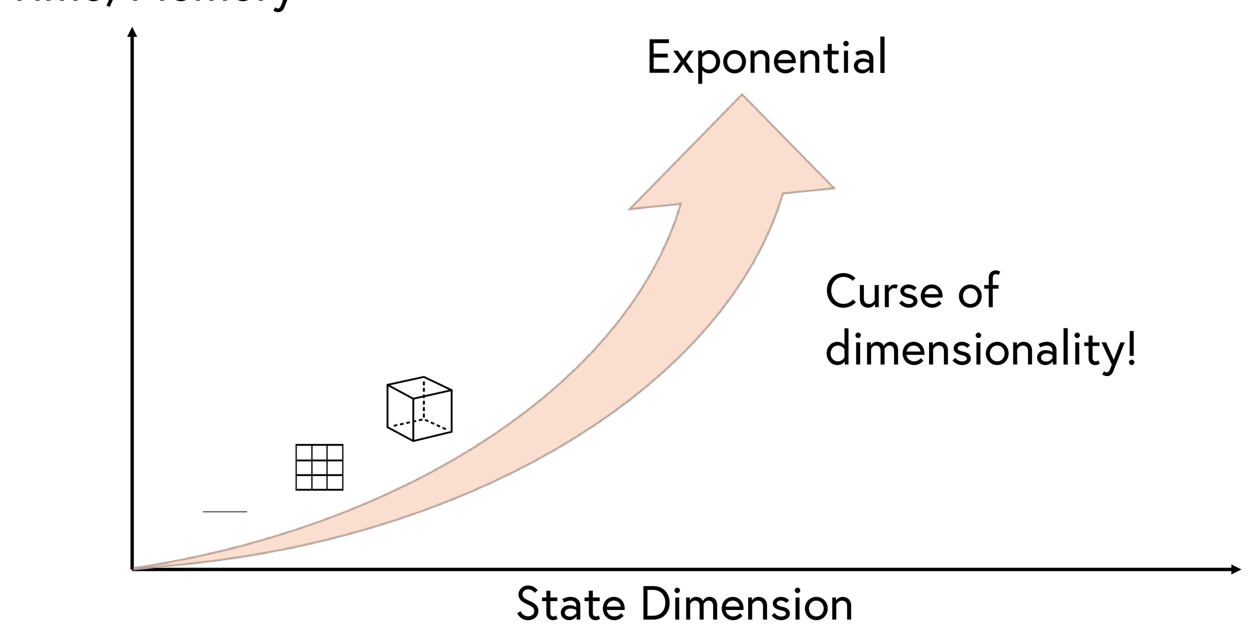
ICRA LONDON · 2023

Project Website

Motivation

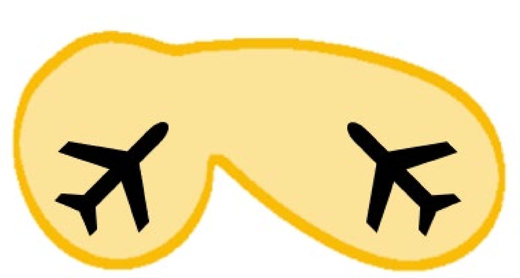
Reachability analysis is a powerful tool for synthesizing safety controllers for autonomous systems.

Grid-based reachability methods are intractable.



Learning-based reachability methods are approximate.

Trained DeepReach Solution



No formal guarantees.

Main Goal

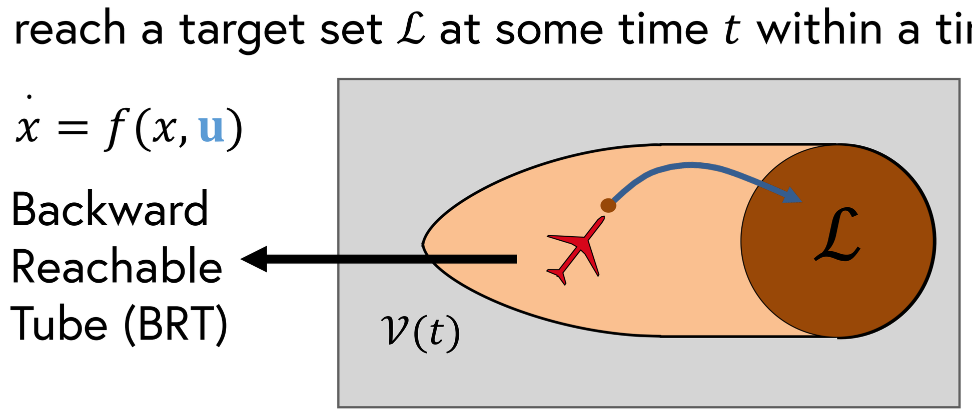
Compute formal safety guarantees for general nonlinear high-dimensional dynamical systems.

Background

Backward Reachable Tube

All states for which, for all possible control actions, the system state will reach a target set $\mathcal{L}$ at some time t within a time horizon T.

$\dot{x} = f(x, \mathbf{u})$



$$\text{BRT} = \{x : x \in X, V(x,0) \leq 0\}$$

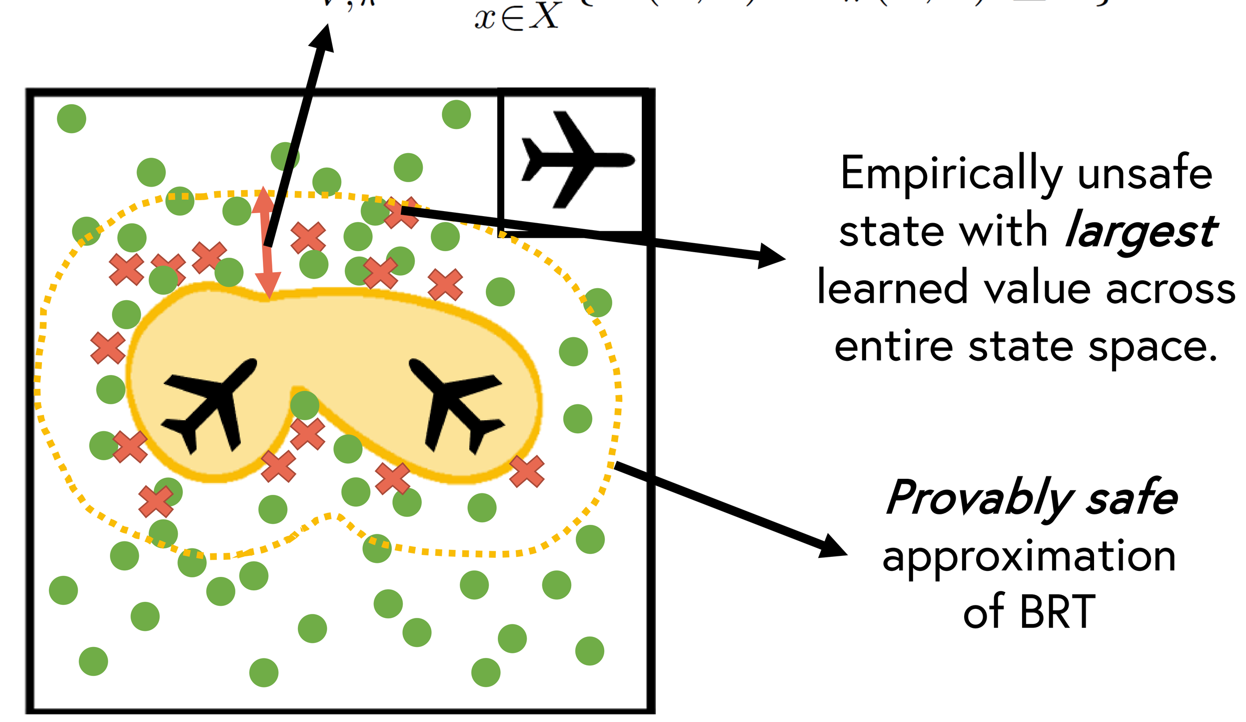
$$V(x,t) = \sup_{u(\cdot)} J_{u(\cdot)}(x,t)$$

$$u^*(x,t) = \arg\max_{u} \langle \nabla V(x,t), f(x,u) \rangle$$

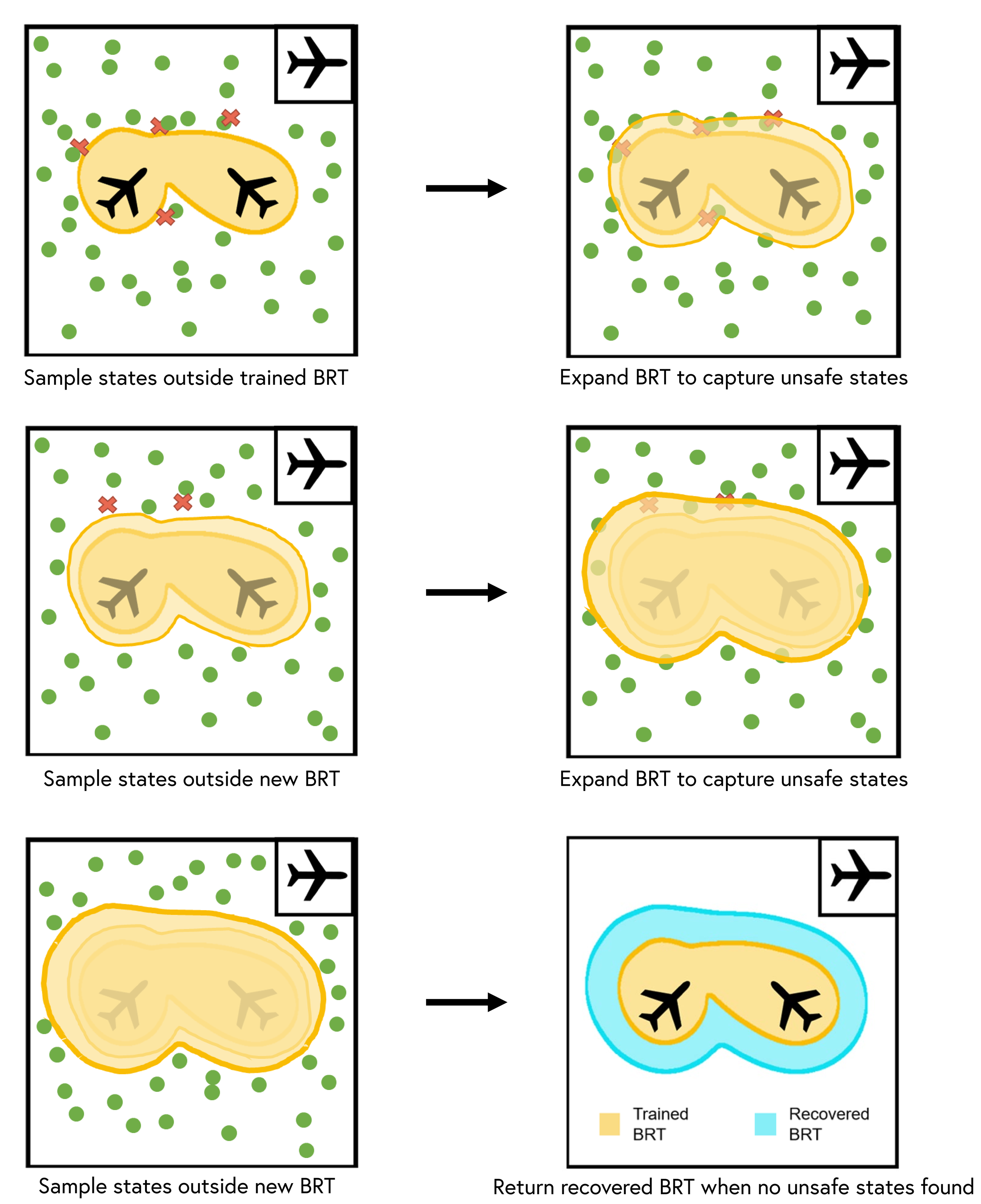
Main Contributions

Uniform Error Correction

$$\delta_{\tilde{V},\tilde{\pi}} := \max_{x \in X} \{\tilde{V}(x,0) : J_{\tilde{\pi}}(x,0) \leq 0\}$$



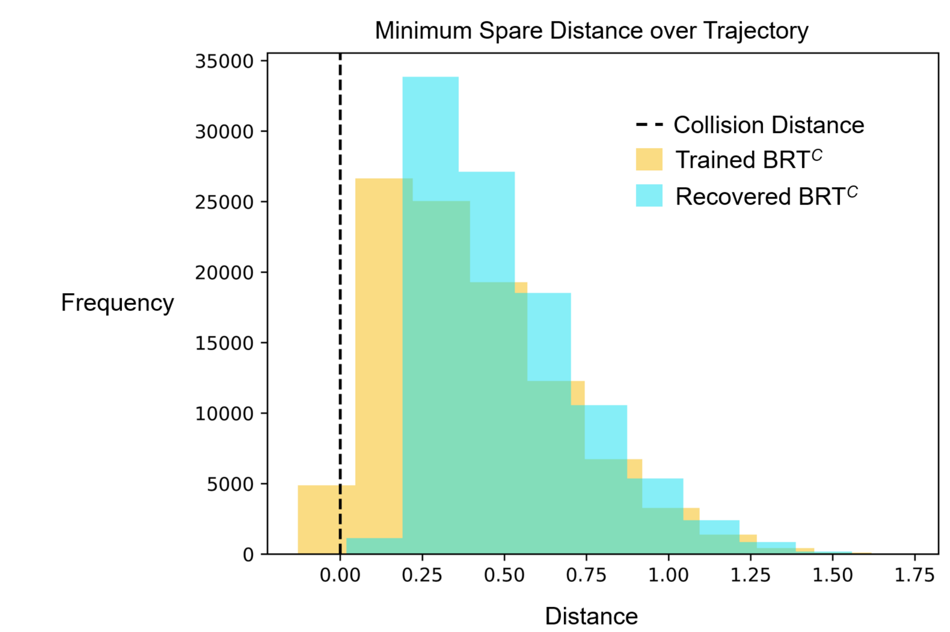
Computing a Probabilistic Error Bound

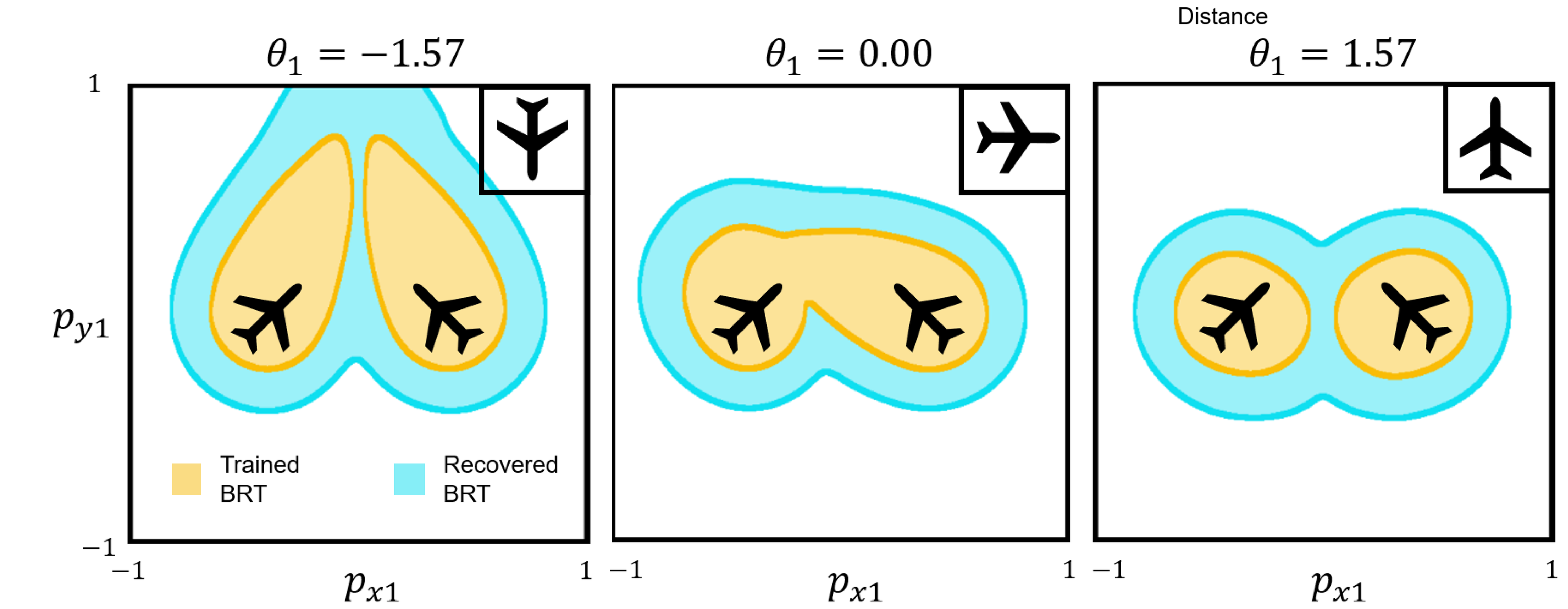


Results

Multi-Vehicle Collision Avoidance System

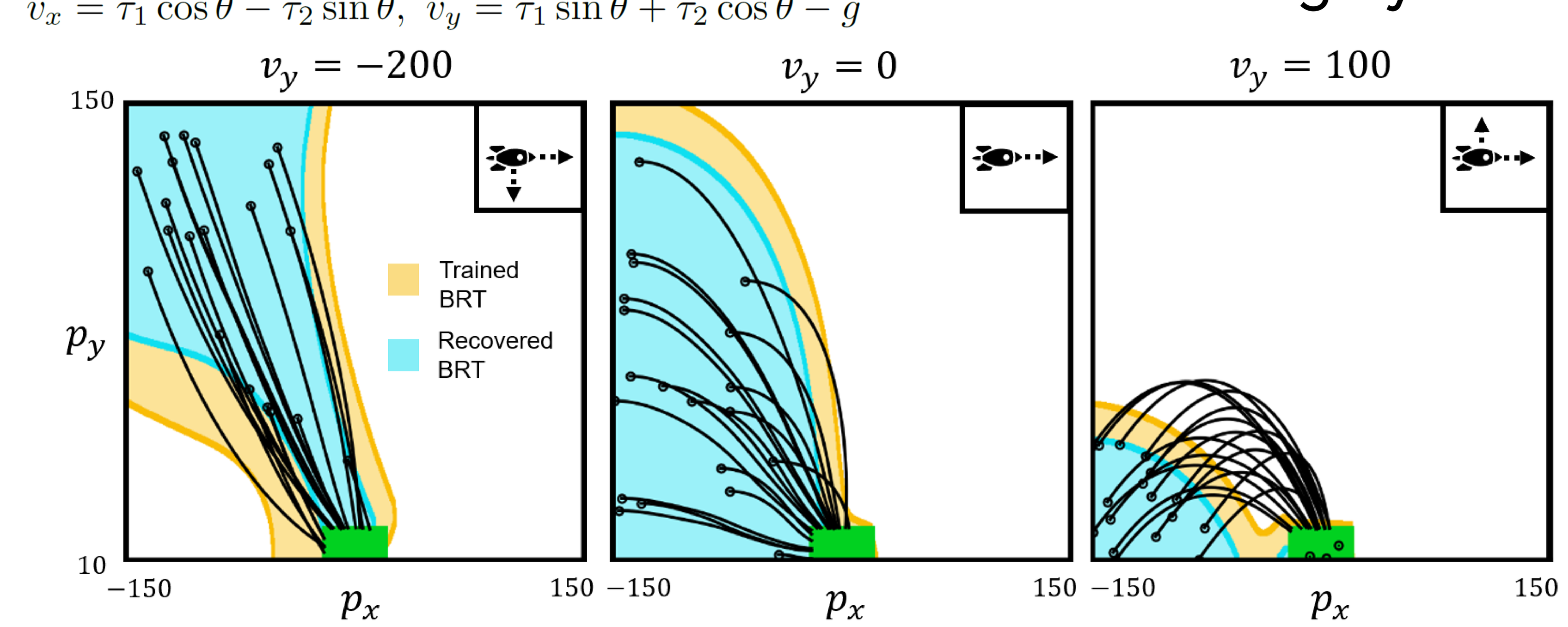
$$\dot{p_{xi}} = v\cos\theta_i$$
$$\dot{p_{yi}} = v\sin\theta_i$$
$$\dot{\theta}_i = u_i$$





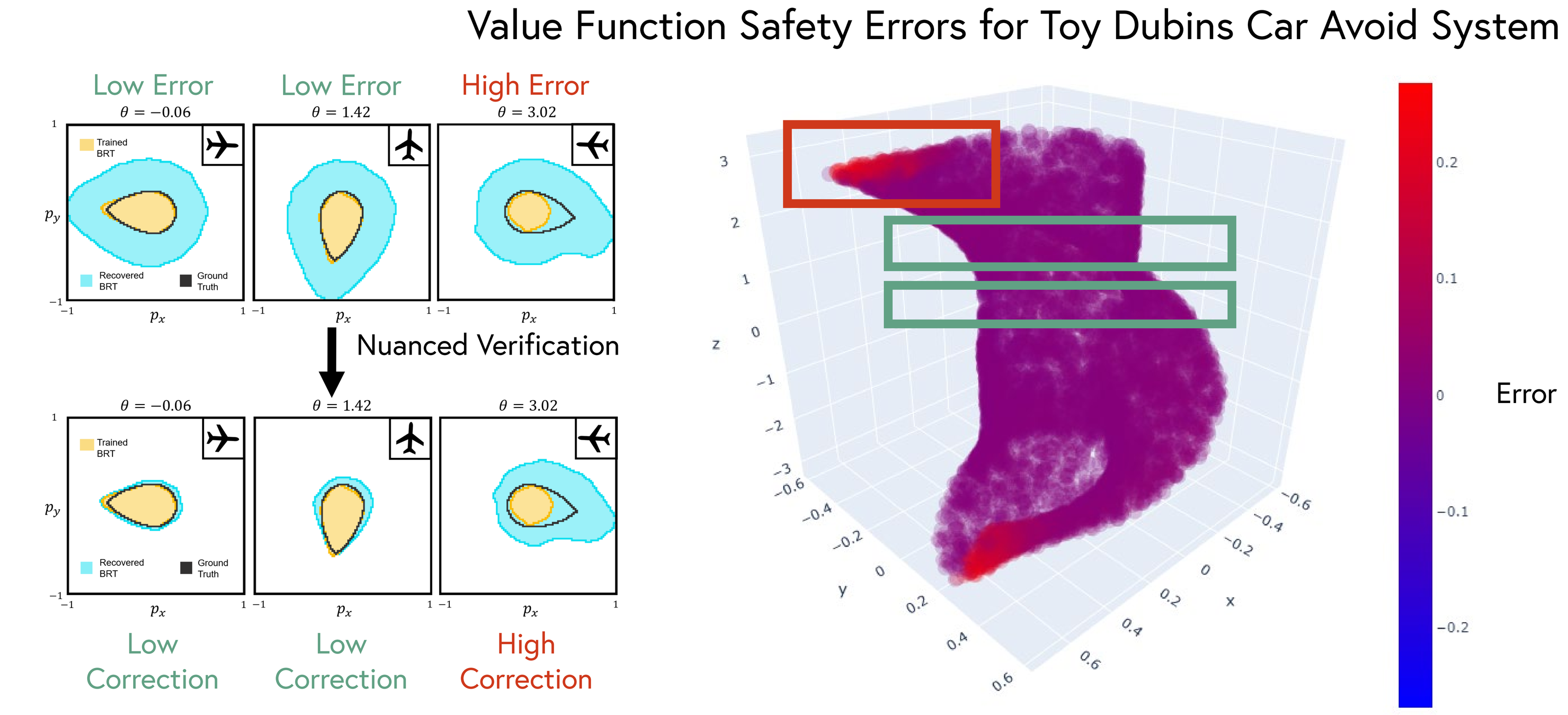
Rocket Landing System

$$\dot{p_x} = v_x,\ \dot{p_y} = v_y,\ \theta = \omega,\ \dot{\omega} = 0.3\tau_1,$$
$$\dot{v_x} = \tau_1\cos\theta - \tau_2\sin\theta,\ \dot{v_y} = \tau_1\sin\theta + \tau_2\cos\theta - g$$



Exploring a More Nuanced Approach

Value Function Safety Errors for Toy Dubins Car Avoid System



PRINCETON UNIVERSITY

USC University of Southern California