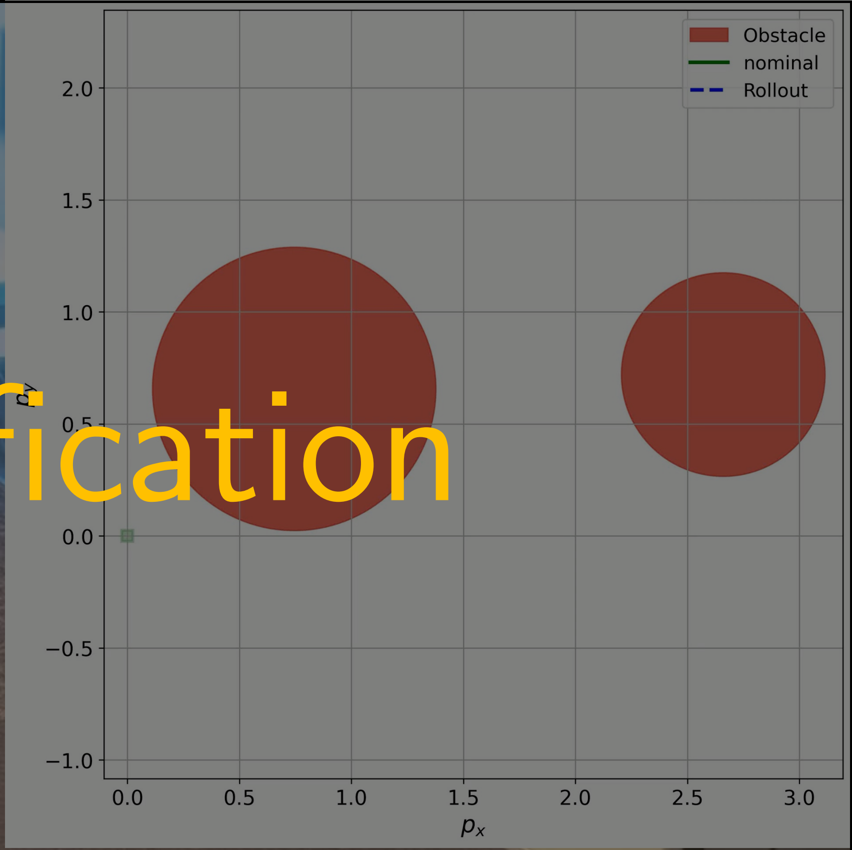
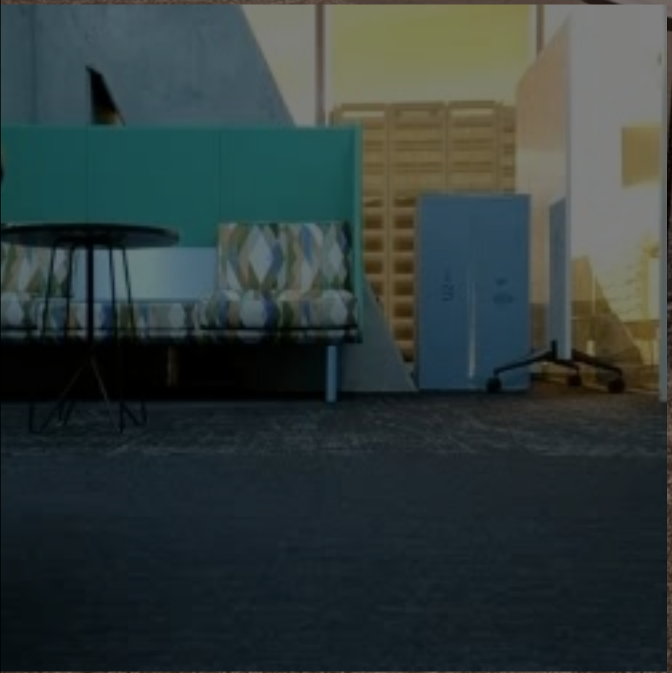
Uncertainty Quantification from Data



Glen Chou

Assistant Professor

Georgia Institute of Technology



Overview

Robust design needs two inputs

1. An (estimated) predictive model $\hat{f}$.
2. A certified error description $e \in \mathbb{W}$.

Focus today

Use data to obtain both pieces, then pass them to robust MPC/reachability.

Three-step safe-by-design pipeline

Data $\mathcal{D}$

$\Downarrow$

1. Learn model: $\hat{f}$ or predictor

$\Downarrow$

2. Choose/certify error set: $e \in \mathbb{W}$

$\Downarrow$

3. Verify closed-loop design: reachability

Overview

Learned dynamics or predictor

$$x_{k+1} = f(x_k, u_k) + w_k, \qquad \hat{x}_{k+1} = \hat{f}(x_k, u_k),$$
$$e(z) := f(z) - \hat{f}(z), \qquad z = (x, u).$$

Robust design asks from UQ:

$$e(z) \in \mathbb{W}(z) \quad \forall z \in \mathcal{Z}$$

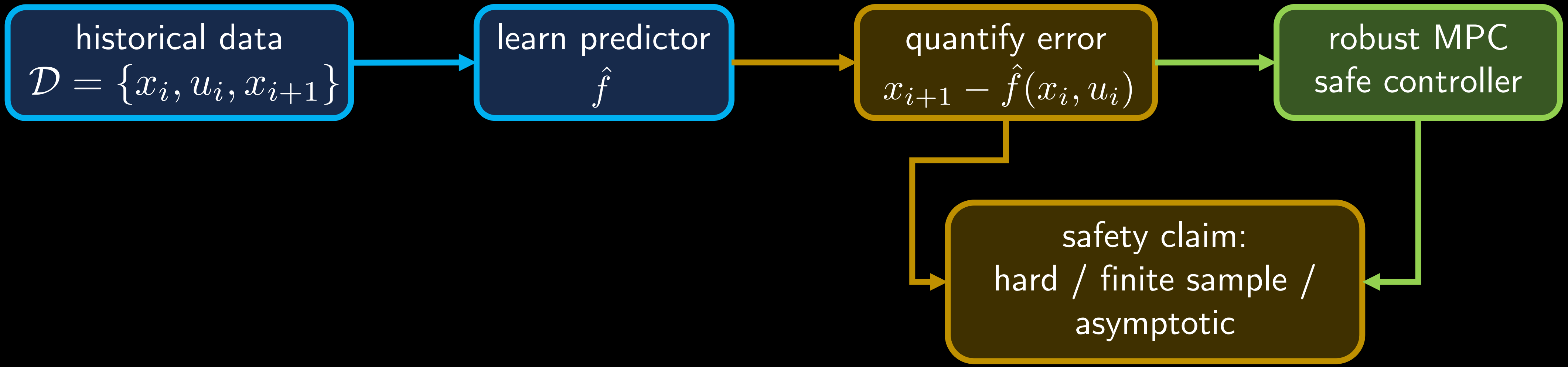
with a clearly stated guarantee type:

- deterministic: "if assumptions hold, the bound is valid";
- probabilistic: $\mathbb{P}\{e(z) \in \mathbb{W}(z) \text{ on deployment}\} \geq 1 - \delta$;
- asymptotic or exact finite-sample.

Main message

Different UQ tools produce different objects. The robust controller only sees the final uncertainty set, but the assumptions behind it determine the safety claim.

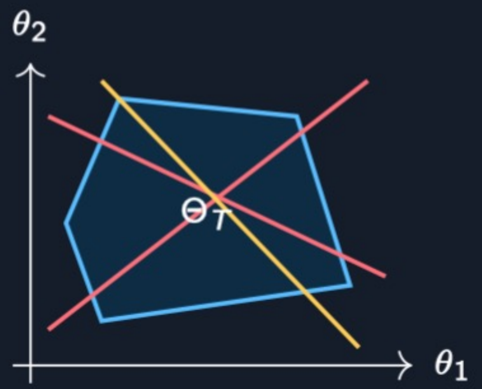
UQ ⇒ Robust Control Pipeline



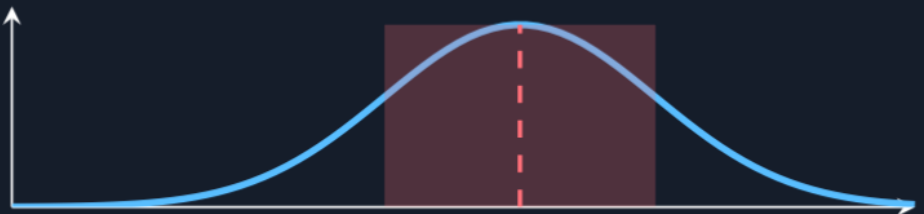
Training reduces nominal prediction error; uncertainty quantification determines what safety statement the controller can make.

Common UQ methods

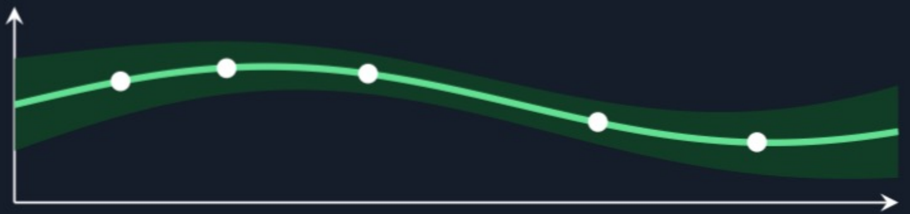
Set-membership: feasible parameter set



Maximum likelihood estimation: nominal and confidence region

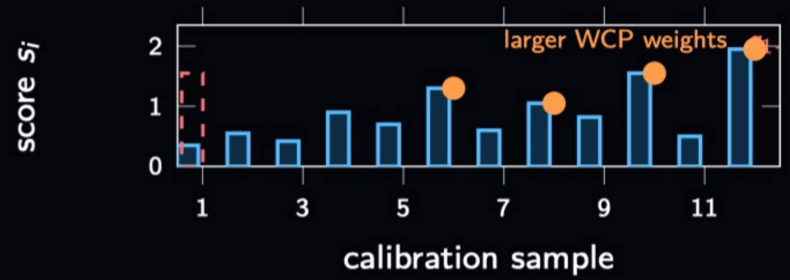


Gaussian process: local confidence band



Extreme value theory: rare-error tail

(Weighted) conformal prediction: finite sample bounds



Set membership estimation

Bounded-noise data model

$$y_t = \phi_t^\top \theta + v_t, \qquad v_t \in \mathbb{V}.$$

The data define a consistency set

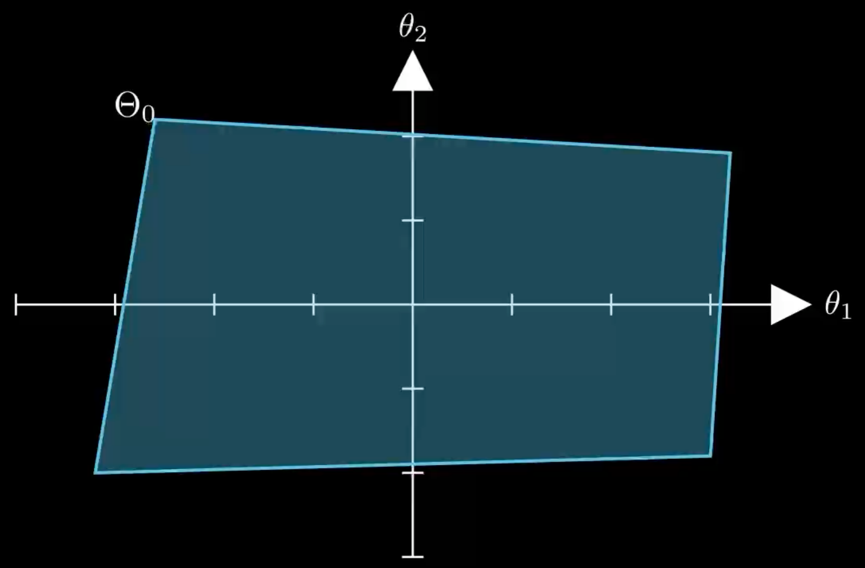
$$\Theta_T = \{\theta : y_t - \phi_t^\top \theta \in \mathbb{V},\ t = 1, \ldots, T\}.$$

For a learned nominal predictor $\hat{y} = \phi^\top \hat{\theta}$, compute the worst-case prediction error

$$\Delta_{\mathrm{SM}}(\phi) = \{\phi^\top(\theta - \hat{\theta}) + v : \theta \in \Theta_T,\ v \in \mathbb{V}\}.$$

Uncertainty set passed to robust MPC

$$\boxed{\mathbb{W}_{\mathrm{SM}} = \Delta_{\mathrm{SM}}(\phi)}$$



Guarantee profile

- $\mathbb{W}$ is deterministic and finite-sample if the bounded-noise model is true;
- Conservativeness comes from the assumed noise set $\mathbb{V}$ and the geometry used to represent $\mathbb{W}$.

Classical reference [1].

Maximum likelihood estimation

Statistical identification

Given a stochastic model

$$y_t = h_\theta(\xi_t) + \varepsilon_t, \qquad \varepsilon_t \sim p_\eta,$$

MLE solves

$$(\hat{\theta}, \hat{\eta}) = \arg\max_{\theta,\eta} \sum_{t=1}^{T} \log p_\eta(y_t - h_\theta(\xi_t)) .$$

Constructing $\mathbb{W}$

Choose a confidence/risk level $1-\delta$ and turn the estimated error law into a high-probability set:

$$\boxed{\mathbb{W}_{\mathrm{MLE}} = \{e : e^\top \hat{\Sigma}_e^{-1} e \leq \chi^2_{n,1-\delta}\}}$$

Example of MLE for predictive control [2].

Guarantee profile

- $\mathbb{W}$ is typically probabilistic, e.g. $\mathbb{P}\{e \in \mathbb{W}\} \geq 1-\delta$;
- classical confidence sets are often asymptotic;
- finite-sample claims need concentration or calibration.

Gaussian processes: local uncertainty

Nonparametric residual model

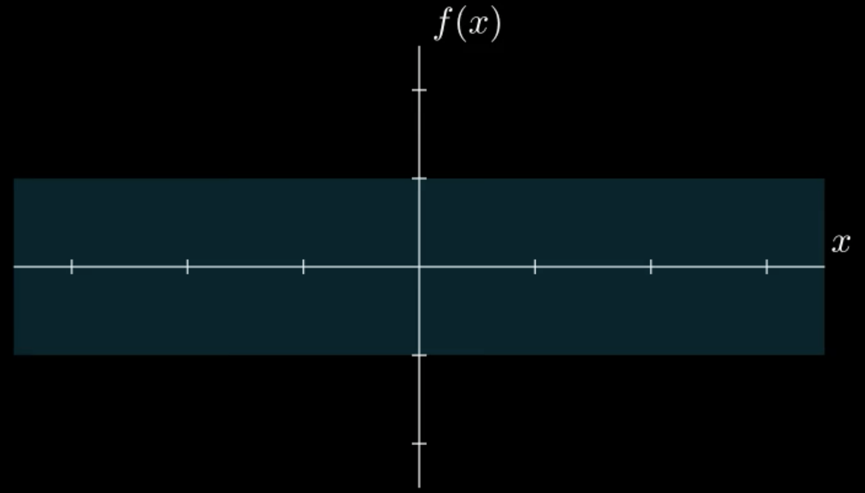
$$e(z) \sim \mathcal{GP}(m(z), k(z, z')),$$

$$e(z) \mid \mathcal{D} \approx \mu_T(z) \pm \beta_T^{1/2} \sigma_T(z).$$

Uncertainty set passed to robust MPC

$$\boxed{\mathbb{W}_{\mathrm{GP}}(z) = \mu_T(z) \oplus \{d : \|D_T(z)^{-1} d\|_\infty \leq \beta_T^{1/2}\}}$$

where $D_T(z) = \mathrm{diag}(\sigma_{T,1}(z), \ldots, \sigma_{T,n}(z))$.



Guarantee and modeling variants

- typical assumption: true error function has bounded RKHS norm within induced kernel, subgaussian measurement noise
- select β as $1 - \delta$ normal quantile + sample-size-dependent correction term $\rightarrow$ frequentist coverage guarantee.

GP references and GP control examples [4-7, 11].

Extreme value theory (EVT): rare error tails

Residual maxima and tail extrapolation

From residual samples $r_i = \|y_i - \hat{y}_i\|$, estimate a high quantile

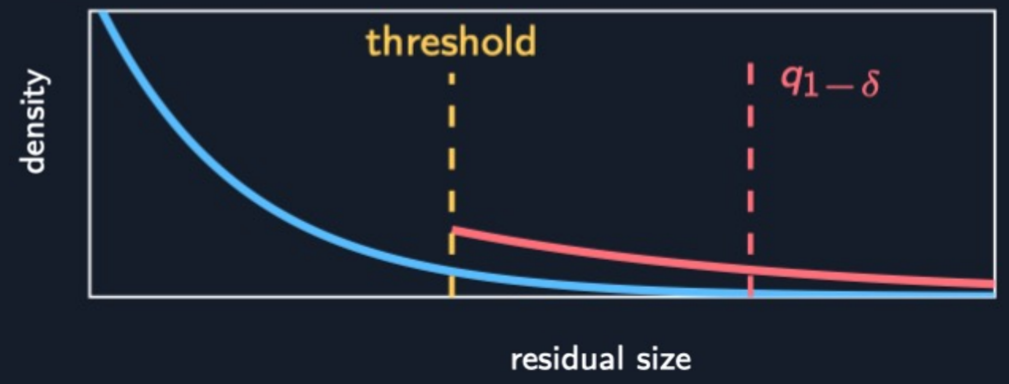
$$q_{1-\delta} \quad \text{such that} \quad \mathbb{P}\{r \le q_{1-\delta}\} \approx 1 - \delta.$$

EVT fits the distribution of extremes, e.g. block maxima or peaks over threshold; enables extrapolation *beyond* observed quantiles.

Uncertainty set passed to robust MPC

$$\boxed{\mathbb{W}_{\mathrm{EVT}} = \{e : \|e\| \le q_{1-\delta}\}}$$

Schematic



Caveat

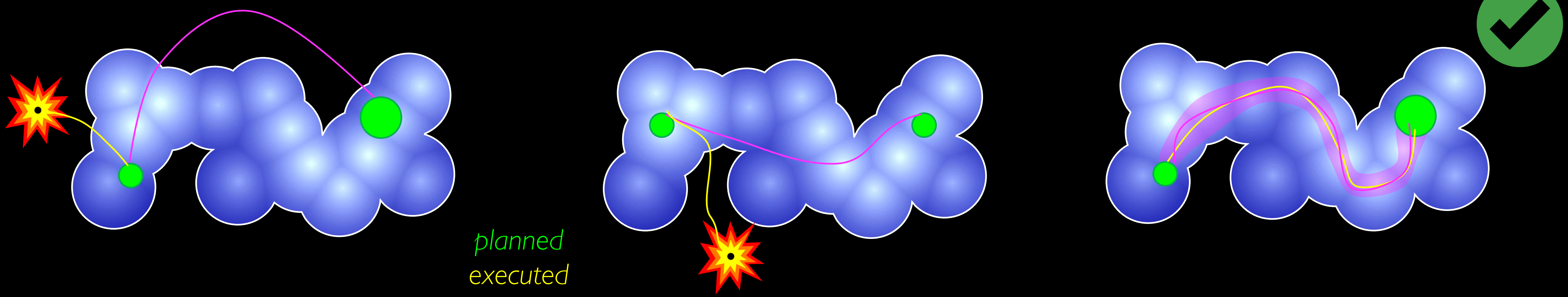
$\mathbb{W}$ is usually asymptotic (relies on convergence to generalized EV distribution) and yields probabilistic guarantees over sampled domain.

Used for probabilistic safety/reachability with learned dynamics and Lipschitz constants in [12, 13].

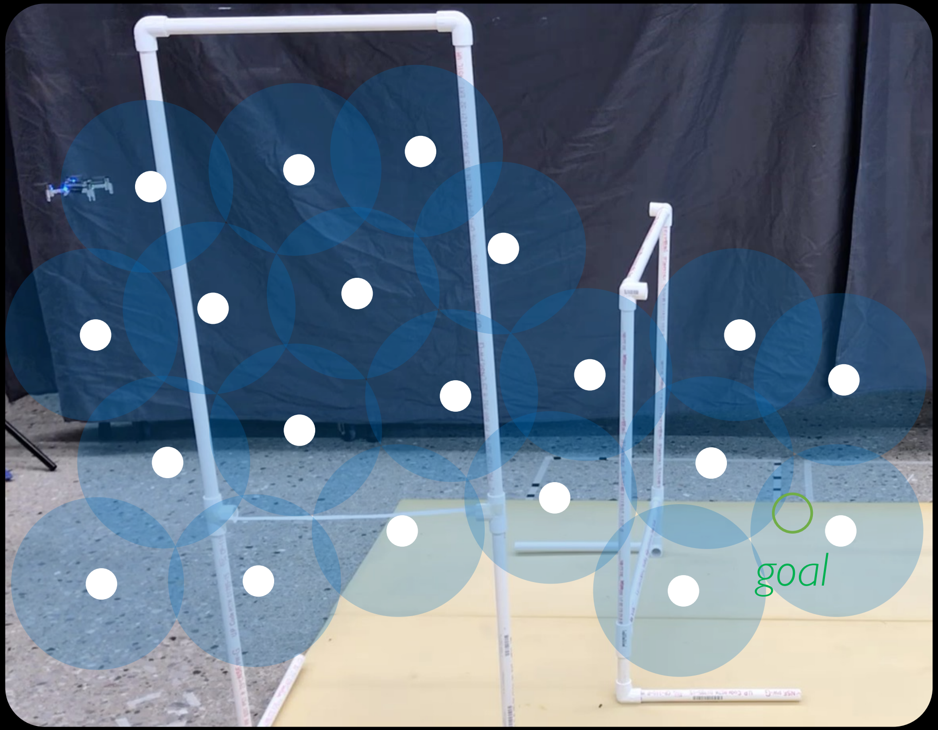
planning outside calibration domain D

ignoring EVT-informed reachability in D

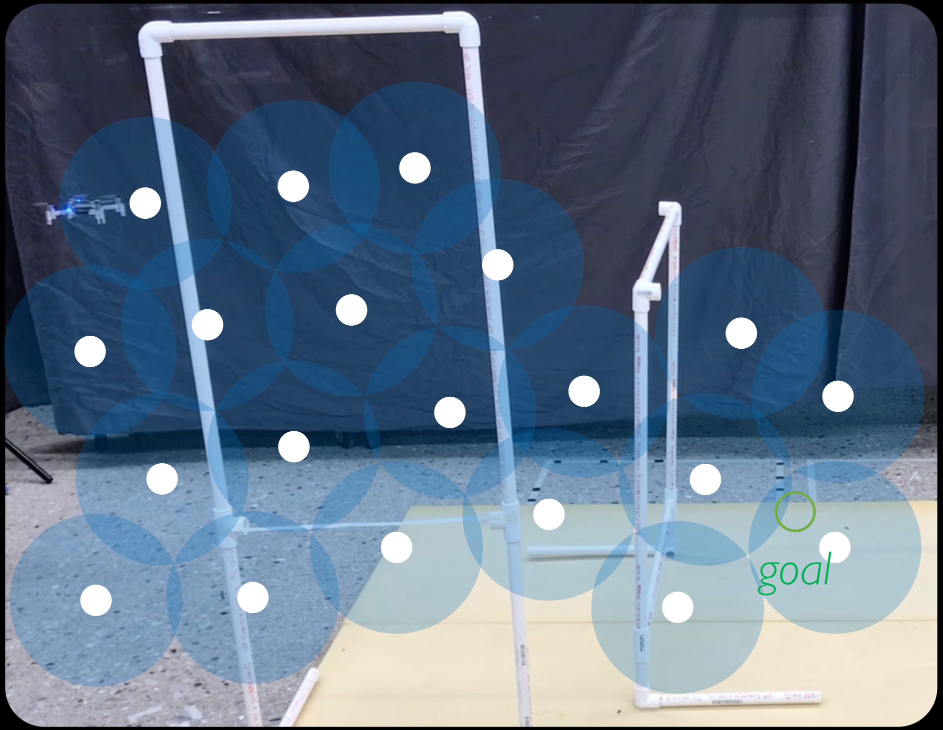
our method



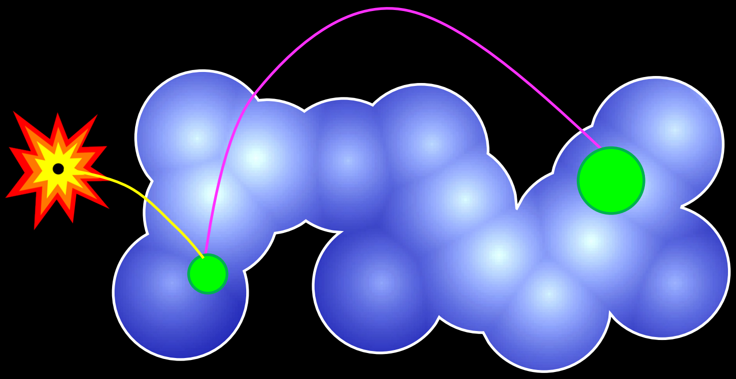
[12] Knuth*, **Chou***, et al. RA-L'21.
[13] Knuth, **Chou**, et al. ICRA'23.

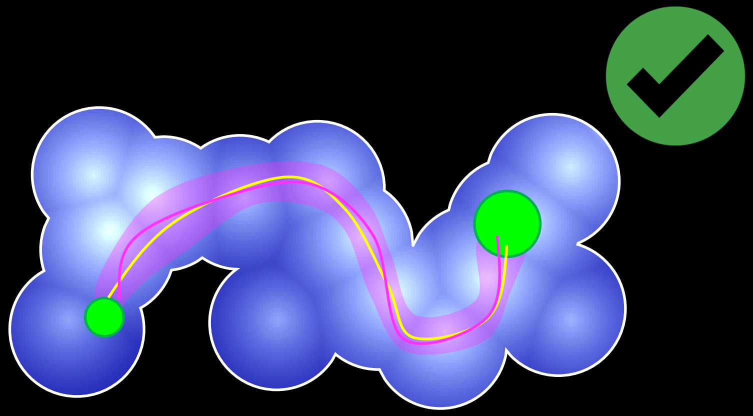


planning outside trusted domain D



our method





planned
executed

[12] Knuth*, **Chou***, et al. RA-L'21.
[13] Knuth, **Chou**, et al. ICRA'23.

Conformal prediction: finite-sample calibration

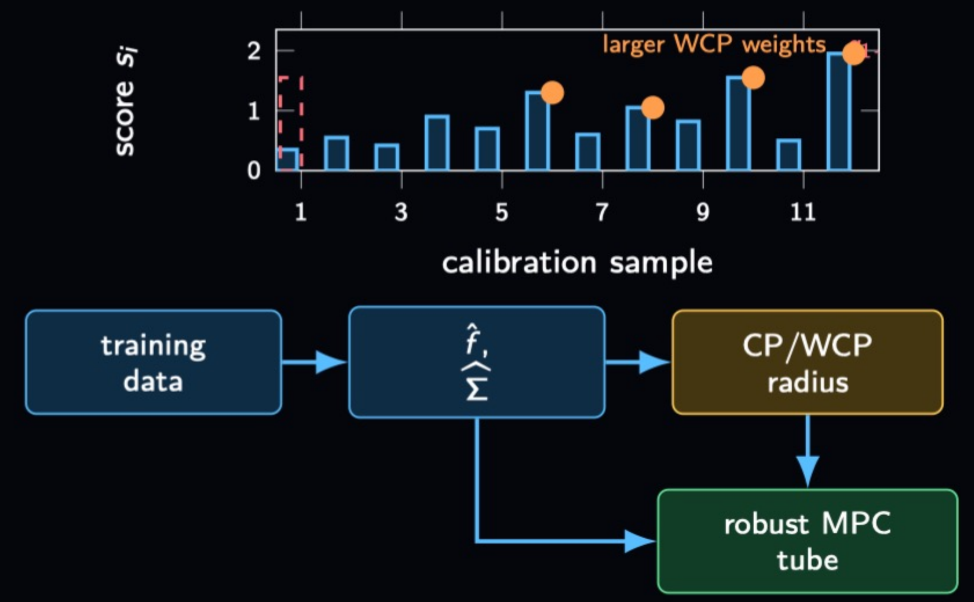
Split conformal recipe

Train $\hat{f}$ on one split of transitions (x_i, u_i, x_i^+); on held-out data compute residual scores

$$s_i = \|\widehat{\Sigma}(z_i)^{-1/2}(x_i^+ - \hat{f}(z_i))\|, \quad z_i = (x_i, u_i).$$

Choose the conformal quantile $\widehat{q}_{1-\delta}$ and certify

$$\widehat{\mathbb{W}}(z) = \{\widehat{\Sigma}(z)^{1/2}e : \|e\| \le \widehat{q}_{1-\delta}\}.$$



Weighted CP for distribution shift

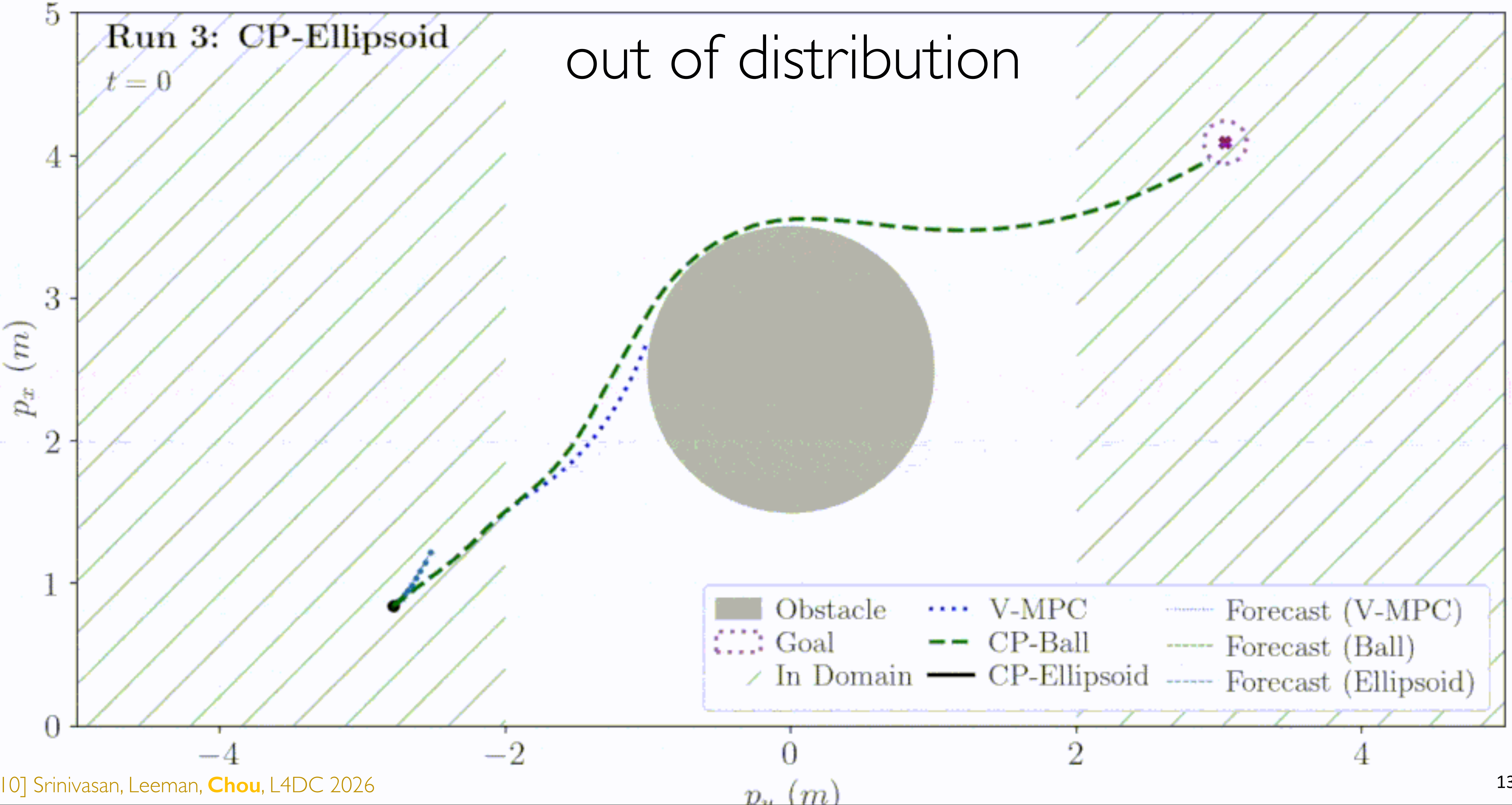
Use a weighted quantile of $\{s_i\}$ with weights $w_i(z_{\text{test}})$ so calibration samples near test-time states matter more.

Guarantee

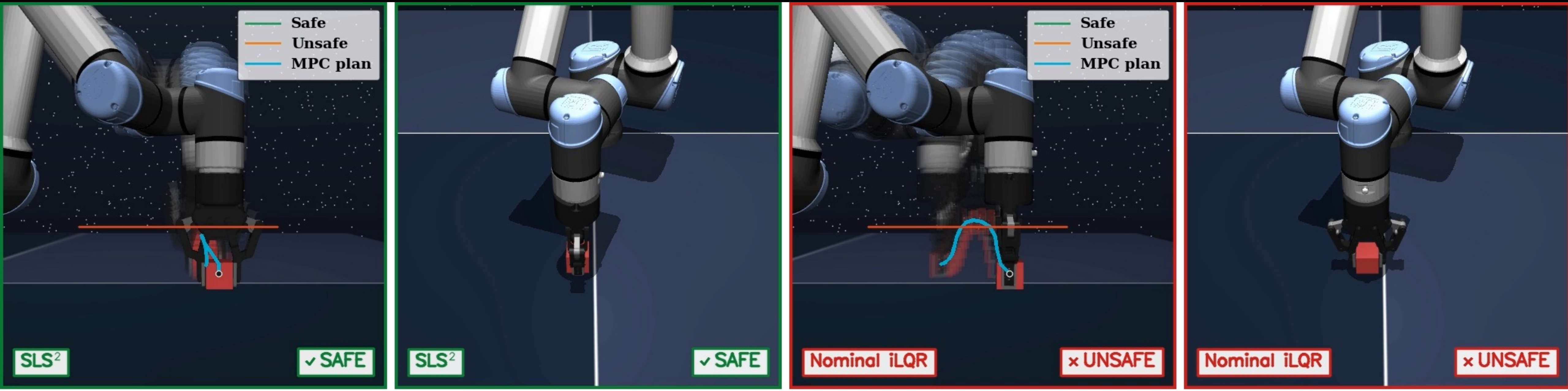
Exchangeable calibration data gives exact finite-sample marginal coverage; weighted CP adapts the quantile to account for covariate shift.

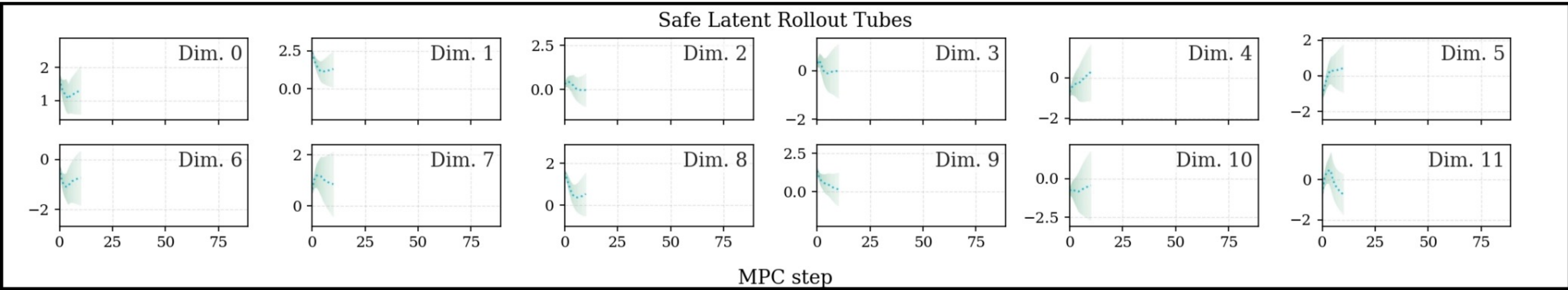
Examples of conformal prediction [8, 20] and weighted CP [19] in control [10].

out of distribution



[10] Srinivasan, Leeman, **Chou**, L4DC 2026





[8] Nath, Srinivasan, Yin, Jiang, Fang, **Chou**, 2026

Application: output feedback

When the state is not measured

$$x_{k+1} = f(x_k, u_k) + w_k, \qquad y_k = h(x_k) + v_k,$$

Must produce a perception map, observer, or latent model together with compatible uncertainty sets.

What must be certified?

- dynamics/model error $w_k \in \mathbb{W}$;
- measurement error $v_k \in \mathbb{V}$;
- estimator/latent-state error $\xi_k \in \Xi$;
- robust constraint satisfaction under all three.

Recent developments

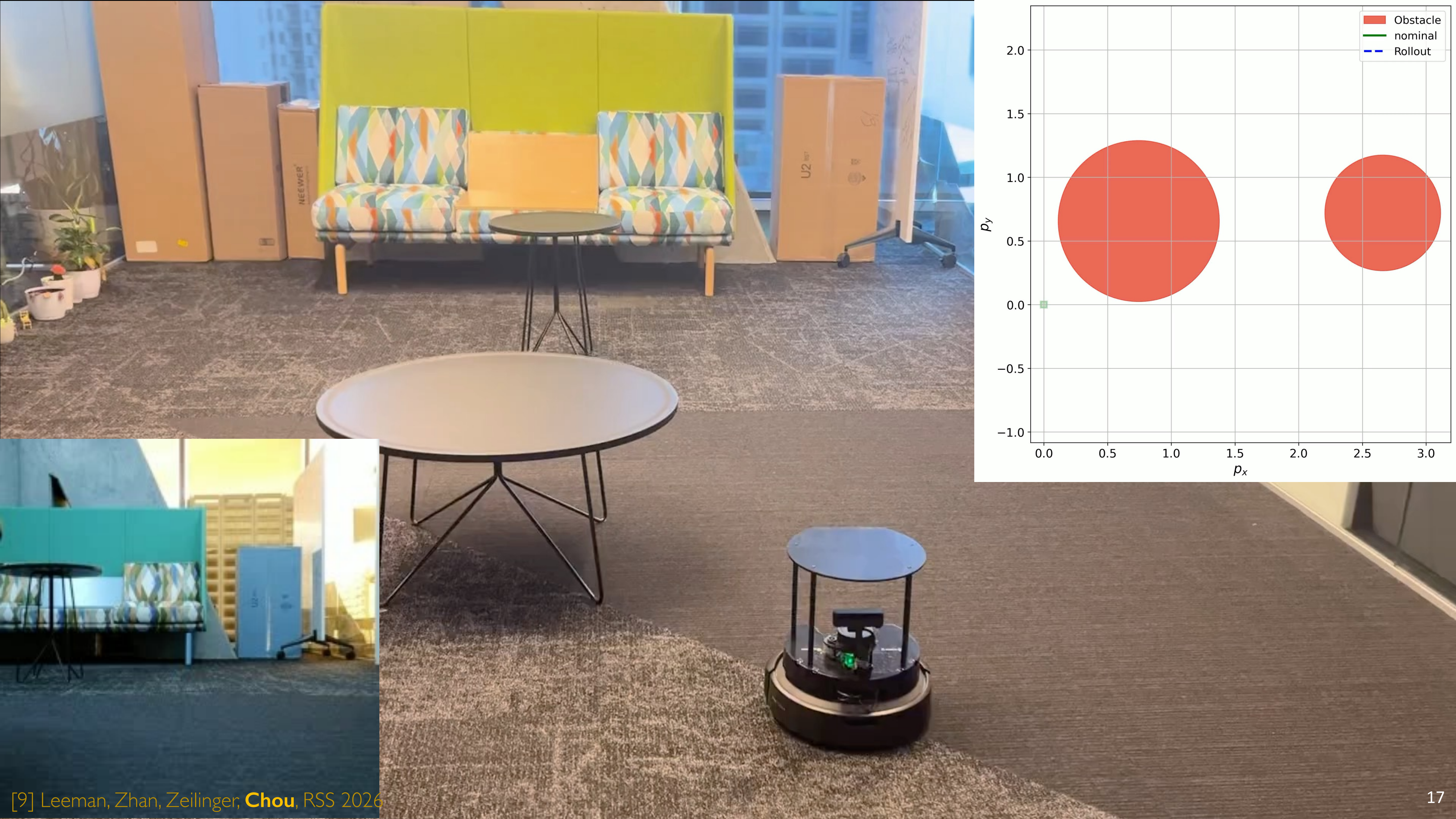
- Visual perception error bounds (EVT estimate) + contraction-based observer bounds [14]
- Visual features with state-dependent output bounds and SLS output feedback - certified info. gathering [8]
- Planning in latent world models with conformalized robust MPC in latent space [9].

Image-based output-feedback safety: [14]. VISION-SLS and latent conformal robust MPC: [8, 9]. Predictor-based stochastic/output-feedback MPC: [2, 17].

safe control from complex visual observations

active perception

[14] **Chou**, Ozay, Berenson. WAFR'22.
[15] **Chou** & Tedrake. CDC'23.
[9] Leeman, Zhan, Zeilinger, **Chou**. RSS'26.



[9] Leeman, Zhan, Zeilinger, **Chou**, RSS 2026

Method	Data/setup	Output $\mathbb{W}$ for the controller	Typical guarantee
Set-membership	bounded noise; often linear-in-parameters	projection of feasible parameter set plus noise: $\phi^\top(\Theta_T - \hat{\theta}) \oplus \mathbb{V}$	exact finite-sample if noise/model assumptions hold
Maximum likelihood	stochastic models; output measurements	likelihood-based residual level set, often covariance ellipsoid	asymptotic confidence intervals; finite-sample with extra calibration
Gaussian process	smooth residuals; kernels encode prior structure	local posterior band scaled by GP posterior	Local confidence bands, assuming true error has bounded RKHS norm for chosen kernel
Extreme value	residual extremes, estimate high quantiles by fitting generalized EVD	rare-error quantile $q_{1-\delta}$	asymptotic rare-event estimate
Conformal / weighted conformal	held-out residual scores / distribution shift weights	calibrated score sublevel set	exact finite-sample coverage under exchangeability; shifted coverage with valid weights

1. Learn a model

- dynamics, predictor, observer.
- optimize nominal prediction quality.

2. Choose an error set

- bounded set $\mathbb{W}$ or probabilistic set $\mathbb{W}_\delta$;
- specify assumptions and confidence semantics.

3. Verify the controller

- reachable tubes, CBFs, SLS, or safety filters;
- prove constraints under the certified set.

1. Learn a model

- dynamics, predictor, observer.
- optimize nominal prediction quality.

2. Choose an error set

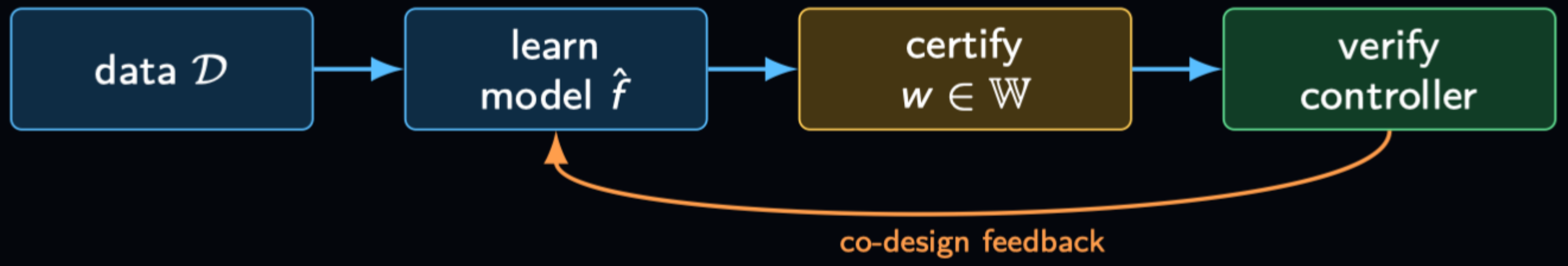
- bounded set $\mathbb{W}$ or probabilistic set $\mathbb{W}_\delta$;
- specify assumptions and confidence semantics.

3. Verify the controller

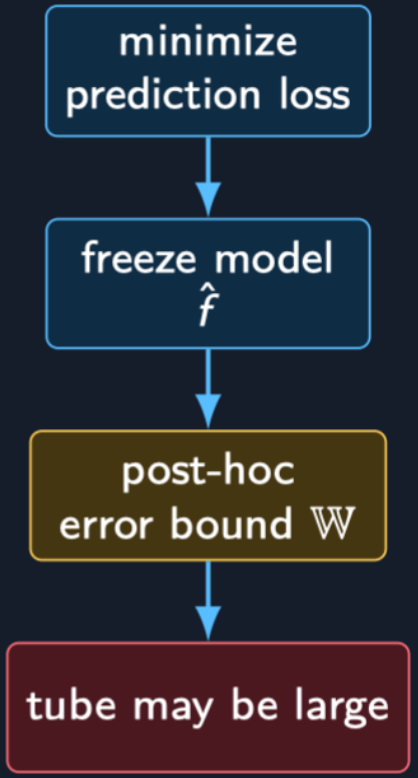
- reachable tubes, CBFs, SLS, or safety filters;
- prove constraints under the certified set.

Modularity is useful, but not always optimal

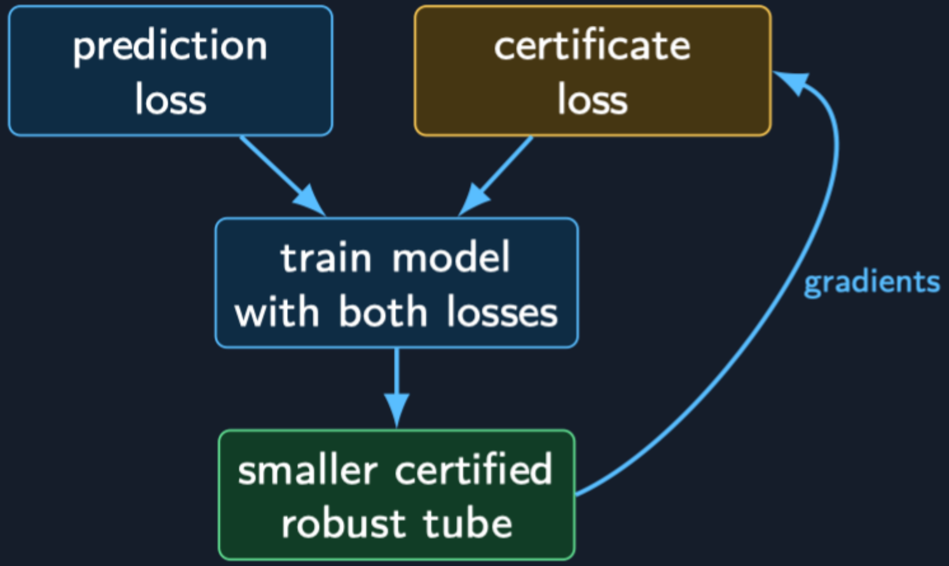
A clean interface $(\hat{f}, \mathbb{W}, \delta) \mapsto$ controller is simpler, but co-designing the model, error set, and verifier can reduce conservativeness.



Train then certify



Certificate-aware training



Key idea

Use differentiable reachability or verification bounds so training favors models/controllers with small certified tubes for fixed uncertainty sets, rather than post-hoc certifying an arbitrary predictor.

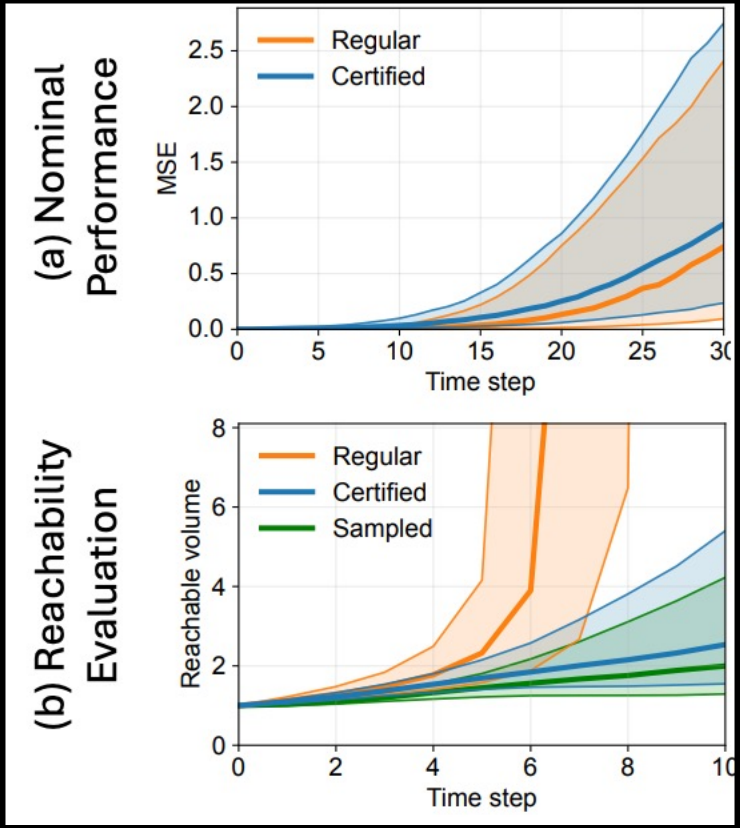
Train with the certificate in the loop

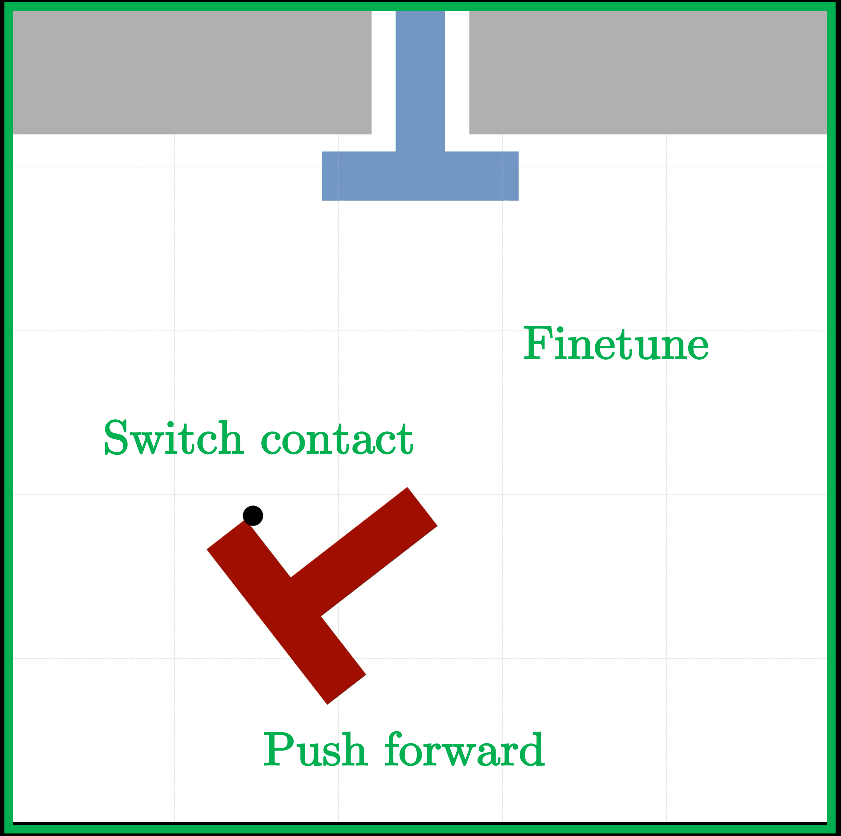
Instead of training only for prediction accuracy, optimize an objective such as

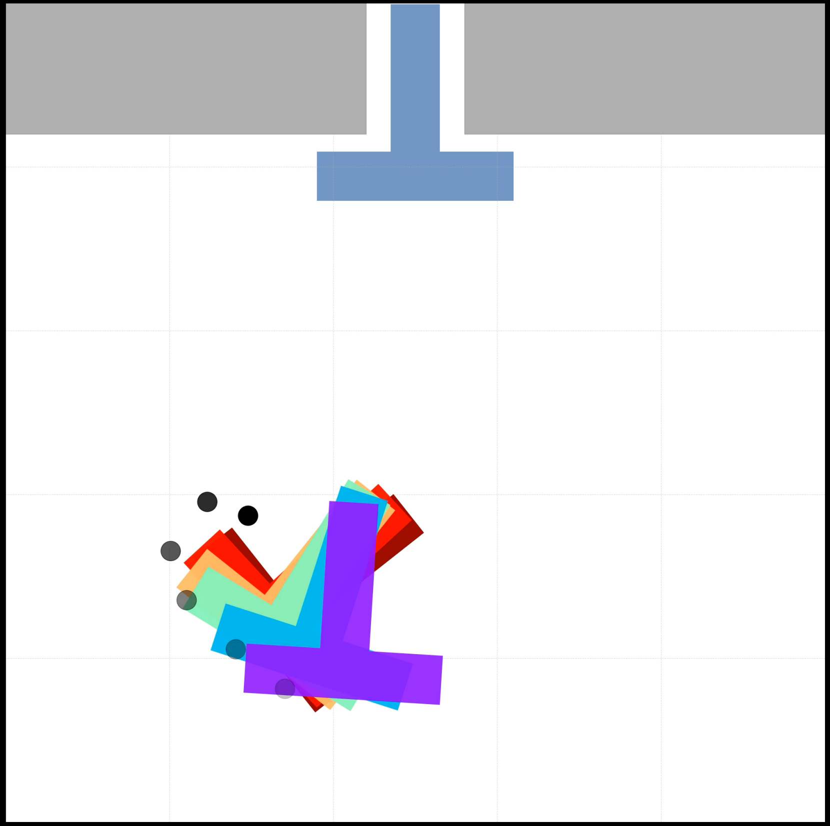
$$\min_{\psi} \underbrace{\mathcal{L}_{\text{fit}}(\psi)}_{\text{prediction}} + \lambda \underbrace{\mathcal{L}_{\text{cert}}(\psi)}_{\text{reachable set size}}$$

Differentiable reachability and certified training, implemented via Taylor model reachability on the GPU [18]

Reachability-aware MPC



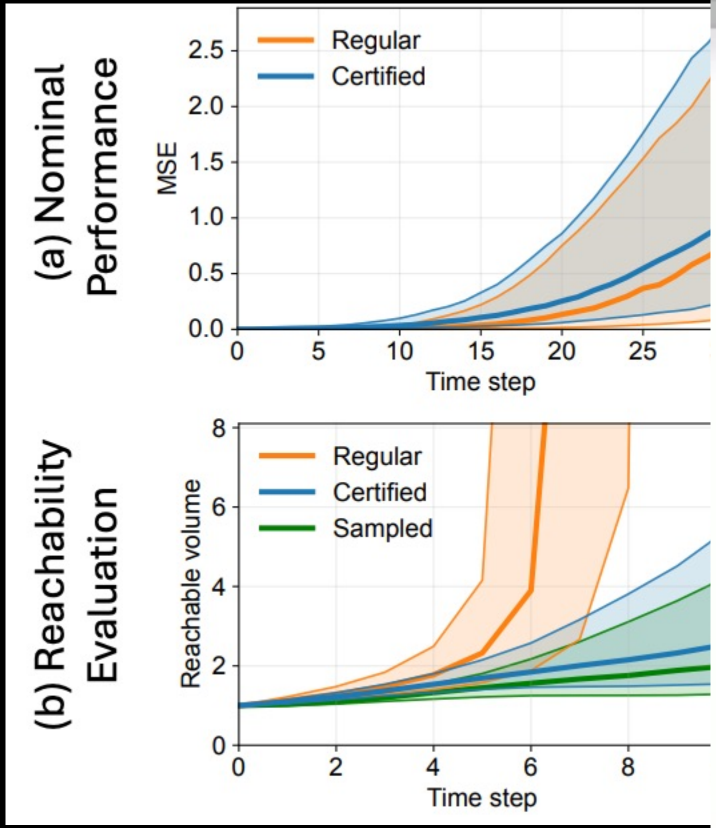


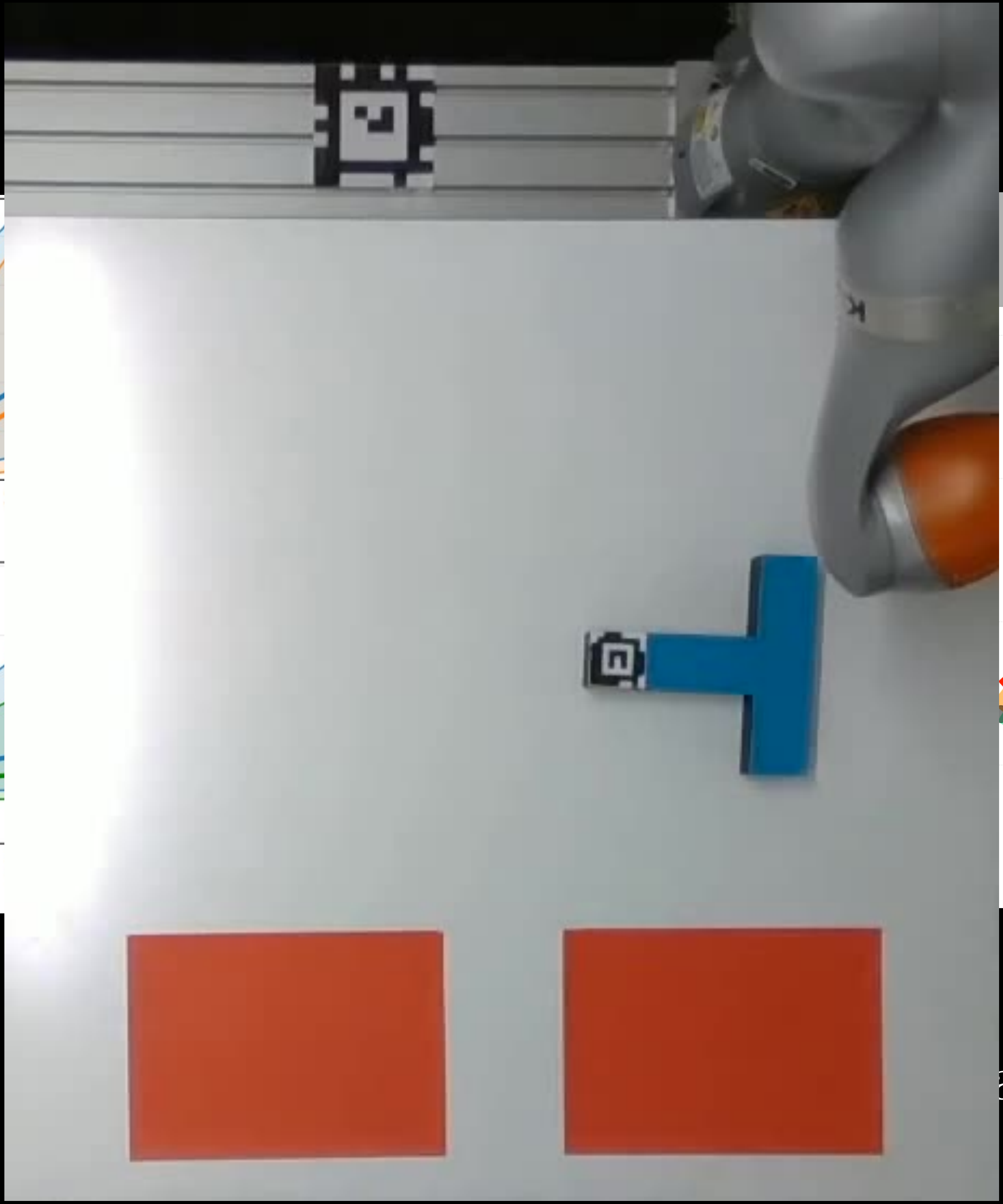


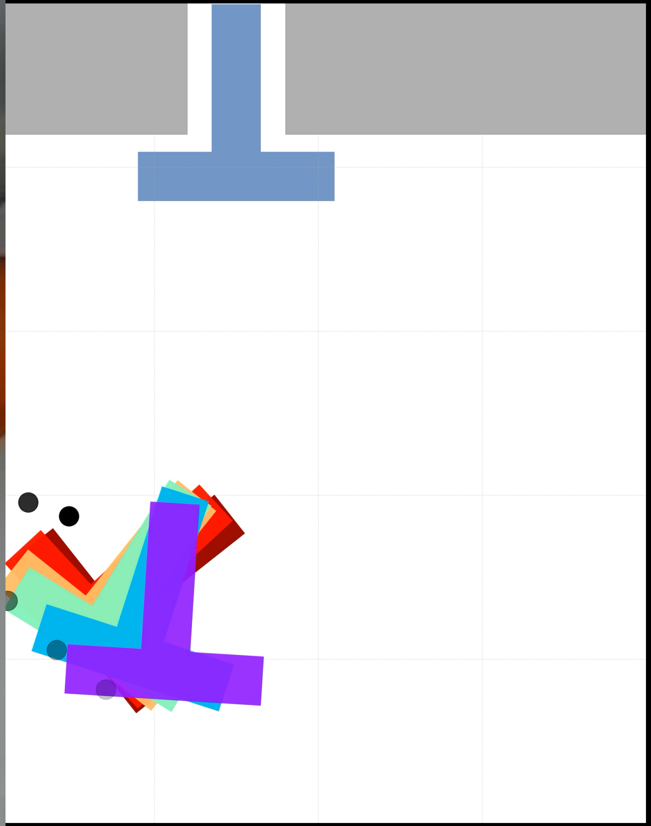
Ground truth
State

Nominal
planned trajectory

[18] Shen and Chou, RSS 2026.







Nominal
anned trajectory

[18] Shen and Chou, RSS 2026.

Summary

1. Key tasks for data-driven robust control design

1) Learn the model, 2) choose/certify an uncertainty set $\mathbb{W}$, and 3) verify the closed-loop controller.

2. UQ methods differ in assumptions and guarantees

Set-membership, MLE, GP, EVT, conformal prediction methods produce different safety claims.

3. The interface should be modular, but co-design can help

Design $\hat{f}$ and $\mathbb{W}$ so that they are computationally tractable for robust MPC; when possible, train models to make the verification certificate tighter.

References I

1. R. L. Kosut, M. K. Lau, and S. P. Boyd. Set-membership identification of systems with parametric and nonparametric uncertainty. *IEEE Transactions on Automatic Control*, 1992.
2. H. Balim, A. Carron, M. N. Zeilinger, and J. Köhler. From data to predictive control: A framework for stochastic linear systems with output measurements. arXiv preprint arXiv:2407.17277, 2024.
3. L. Hewing, J. Kabzan, and M. N. Zeilinger. Cautious model predictive control using Gaussian process regression. *IEEE Transactions on Control Systems Technology*, 2020.
4. C. K. I. Williams and C. E. Rasmussen. *Gaussian Processes for Machine Learning*. MIT Press, 2006.
5. G. Chou, H. Wang, and D. Berenson. Gaussian process constraint learning for scalable chance-constrained motion planning from demonstrations. *IEEE Robotics and Automation Letters*, 2022.
6. Y. Lin, G. Chou, and D. Berenson. Improving out-of-distribution generalization of learned dynamics by learning pseudometrics and constraint manifolds. *IEEE International Conference on Robotics and Automation*, 2024.
7. M. Prajapat, J. Köhler, A. Lahr, A. Krause, and M. N. Zeilinger. Finite-sample-based reachability for safe control with Gaussian process dynamics. arXiv preprint arXiv:2505.07594, 2025.
8. D. Nath, A. Srinivasan, H. Yin, R. Jiang, J. Fang, and G. Chou. Pixels to proofs: Probabilistically-safe latent world model control via parallel conformal robust MPC. arXiv:2606.15594, 2026.
9. A. Leeman, S. Zhan, M. Zeilinger, and G. Chou. VISION-SLS: Safe perception-based control from learned visual abstractions. Robotics: Science and Systems (RSS), 2026.
10. A. Srinivasan, A. Leeman, and G. Chou. Safety beyond the training data: Robust out-of-distribution MPC via conformalized system level synthesis. Learning for Dynamics and Control (L4DC), 2026.

References II

11. M. Dubied, A. Lahr, M. N. Zeilinger, and J. Köhler. A robust and adaptive MPC formulation for Gaussian process models. arXiv preprint arXiv:2507.02098, 2025.
12. C. Knuth, G. Chou, N. Ozay, and D. Berenson. Planning with learned dynamics: Probabilistic guarantees on safety and reachability via Lipschitz constants. *IEEE Robotics and Automation Letters*, 2021.
13. C. Knuth, G. Chou, J. Reese, and J. Moore. Statistical safety and robustness guarantees for feedback motion planning of unknown underactuated stochastic systems. *IEEE International Conference on Robotics and Automation*, 2023.
14. G. Chou, N. Ozay, and D. Berenson. Safe output feedback motion planning from images via learned perception modules and contraction theory. *WAFR*, 2022.
15. G. Chou and R. Tedrake. Synthesizing stable reduced-order visuomotor policies for nonlinear systems via sums-of-squares optimization. *IEEE Conference on Decision and Control*, 2023.
16. S. Dean, A. J. Taylor, R. K. Cosner, B. Recht, and A. D. Ames. Guaranteeing safety of learned perception modules via measurement-robust control barrier functions. arXiv:2010.16001, 2020.
17. J. Köhler, M. A. Müller, and F. Allgöwer. Robust output feedback model predictive control using online estimation bounds. arXiv preprint arXiv:2105.03427, 2021.
18. K. Shen and G. Chou. Parallel differentiable reachability for learning and planning with certified neural dynamics and controllers. Robotics: Science and Systems (RSS), 2026.
19. R. J. Tibshirani, R. F. Barber, E. J. Candès, and A. Ramdas. Conformal prediction under covariate shift. NeurIPS, 2019.
20. L. Lindemann, M. Cleaveland, G. Shim, GJ Pappas. Safe planning in dynamic environments using conformal prediction. RA-L 2023.