UNIVERSITY OF CONNECTICUT

Robust Simulation of Safety-Critical Systems

Matthew D. Stuber, PhD

Assistant Professor, Chemical & Biomolecular Eng.

Process Systems and Operations Research Laboratory

Outline

- Introduction & Background
  - What is meant by “robust simulation”?
  - Steady-state vs. dynamical systems
- Preliminaries
  - Problem formulation & foundational results
- New Results
  - Extending steady-state to dynamical
- Conclusions and Future Work

Key Contributor

Matthew Wilhelm

PhD Candidate

PSOR Lab, Dept. of Chemical and Biomolecular Eng.

University of Connecticut

UCONN

Introduction

- A “Robust System” mitigates the effects of uncertainty to ensure performance/safety constraints are satisfied.

Introduction

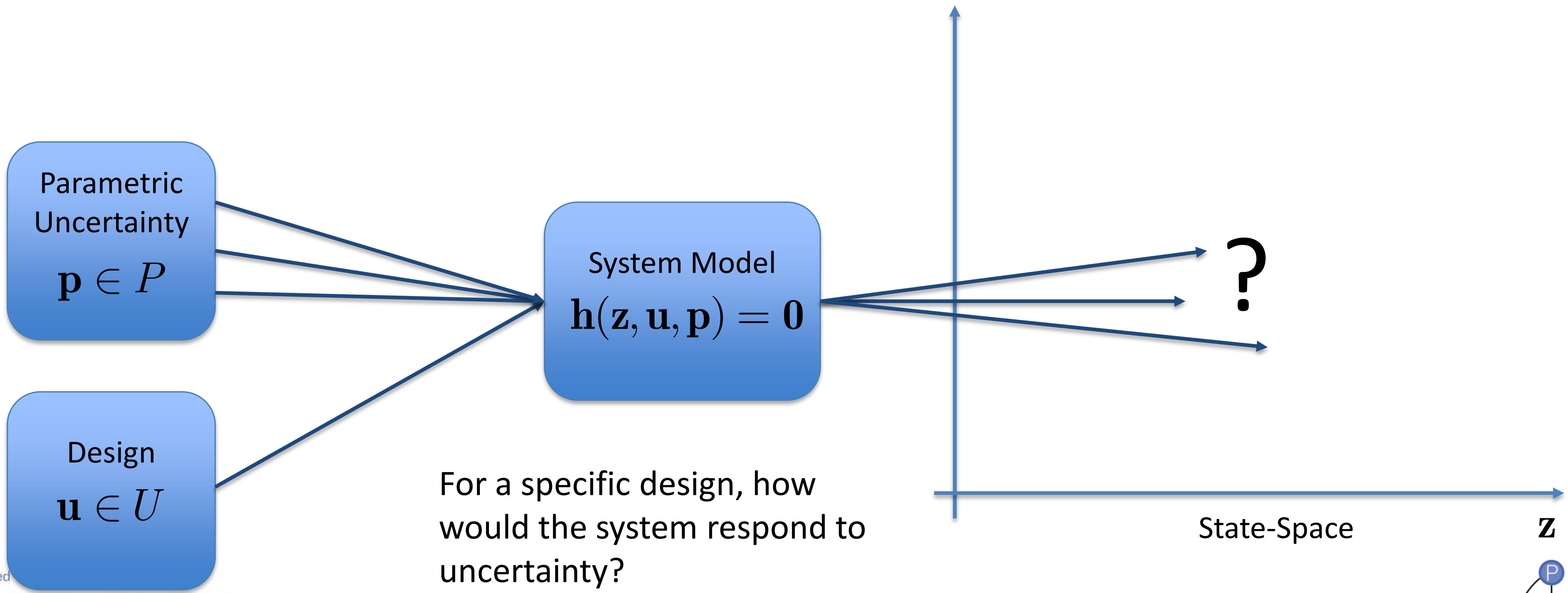
- A “Robust System” mitigates the effects of uncertainty to ensure performance/safety constraints are satisfied.
- “Robust Simulation” refers to the ability to rigorously account for the impacts of uncertainty via a model-based (i.e., simulation) approach
  - Conclude whether or not a system can meet the desired performance/safety constraints in the face of uncertainty using mathematical models

Introduction

- A “Robust System” mitigates the effects of uncertainty to ensure performance/safety constraints are satisfied.
- “Robust Simulation” refers to the ability to rigorously account for the impacts of uncertainty via a model-based (i.e., simulation) approach
  - Conclude whether or not a system can meet the desired performance/safety constraints in the face of uncertainty using mathematical models

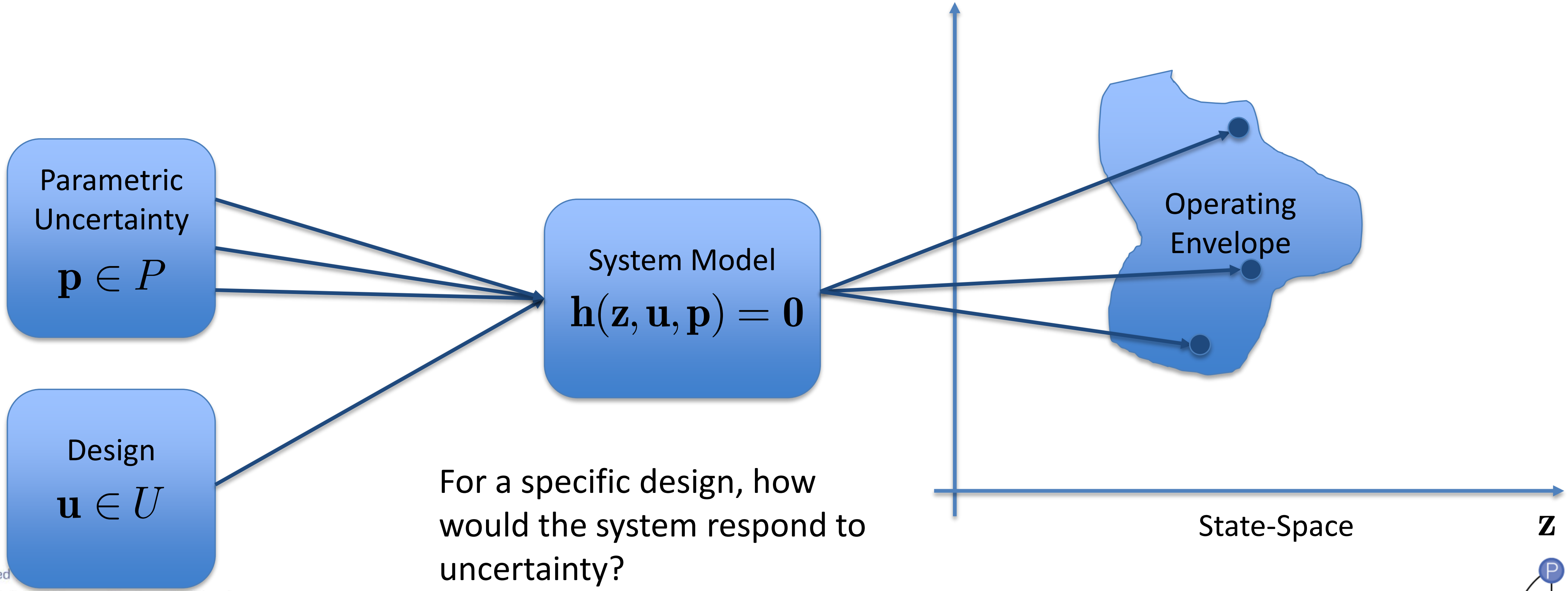
Research Challenge: How can we use model-based optimal design principles to improve reliability and safety of systems at the design stage?

Accounting for Uncertainty



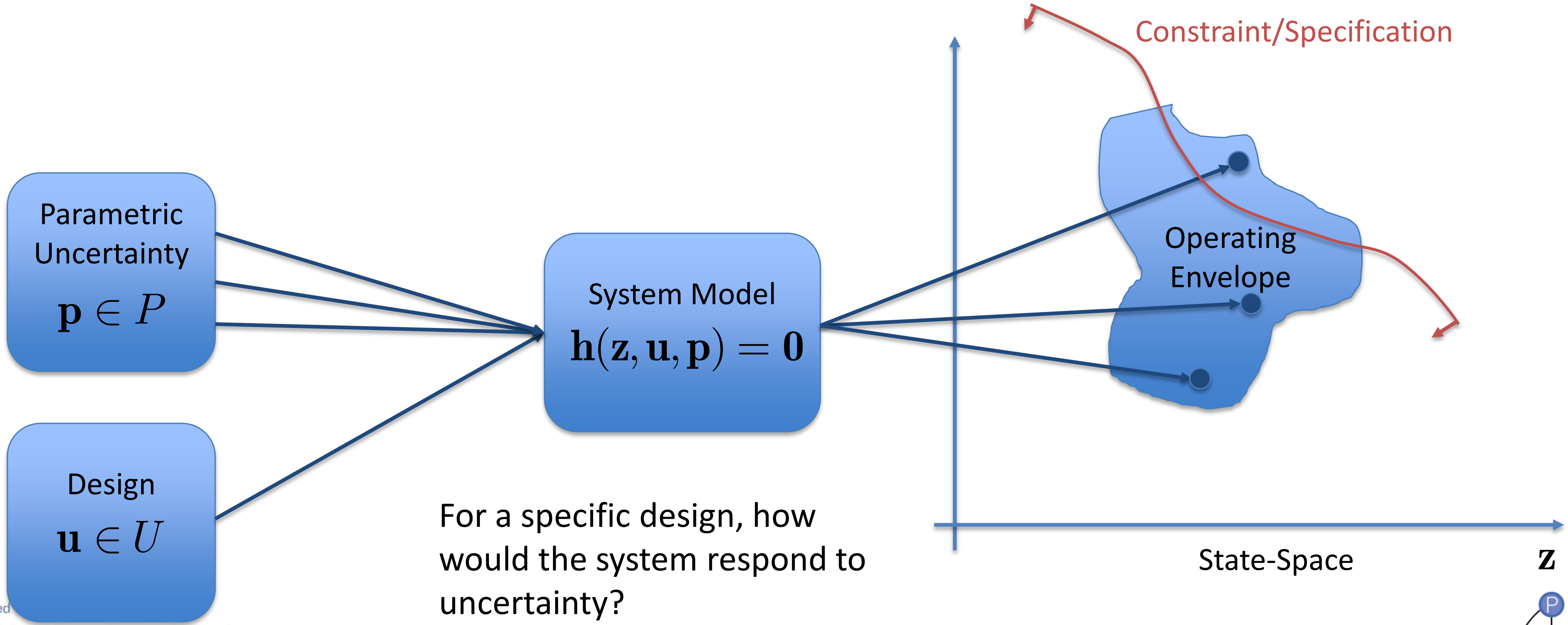
For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty



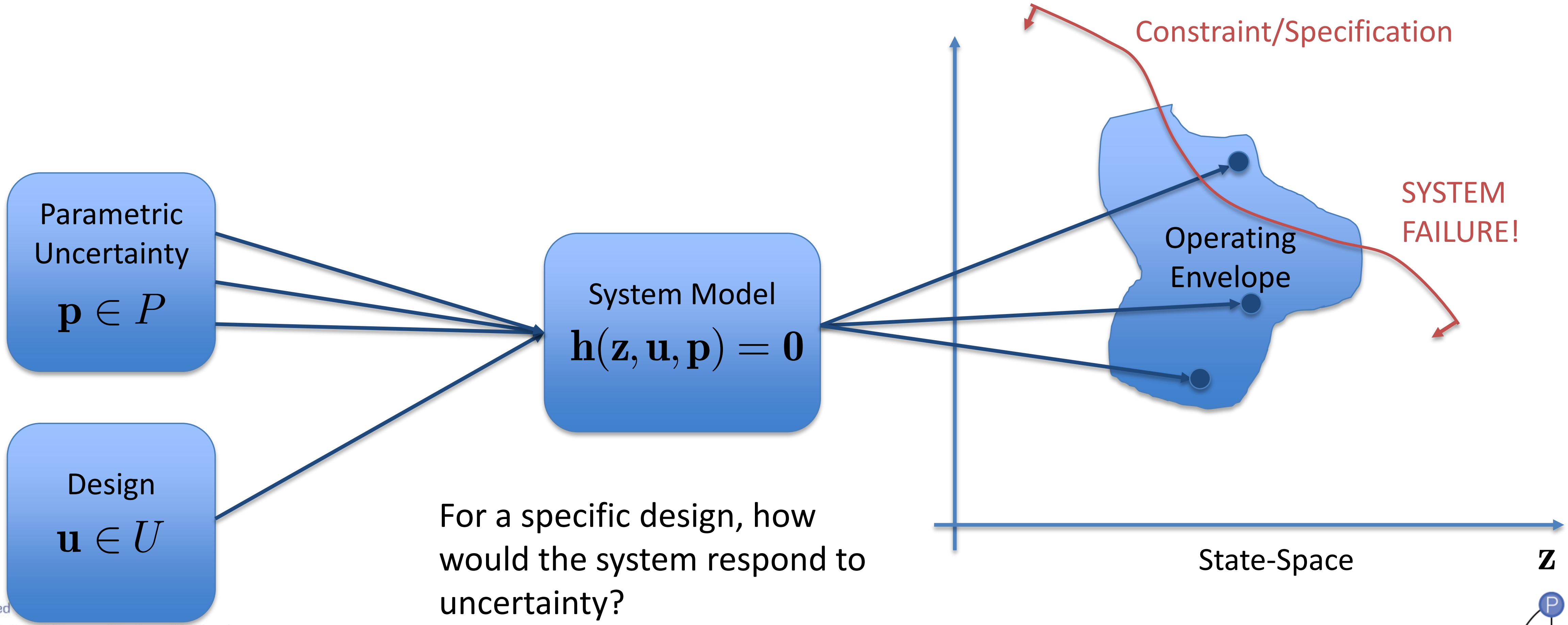
For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty



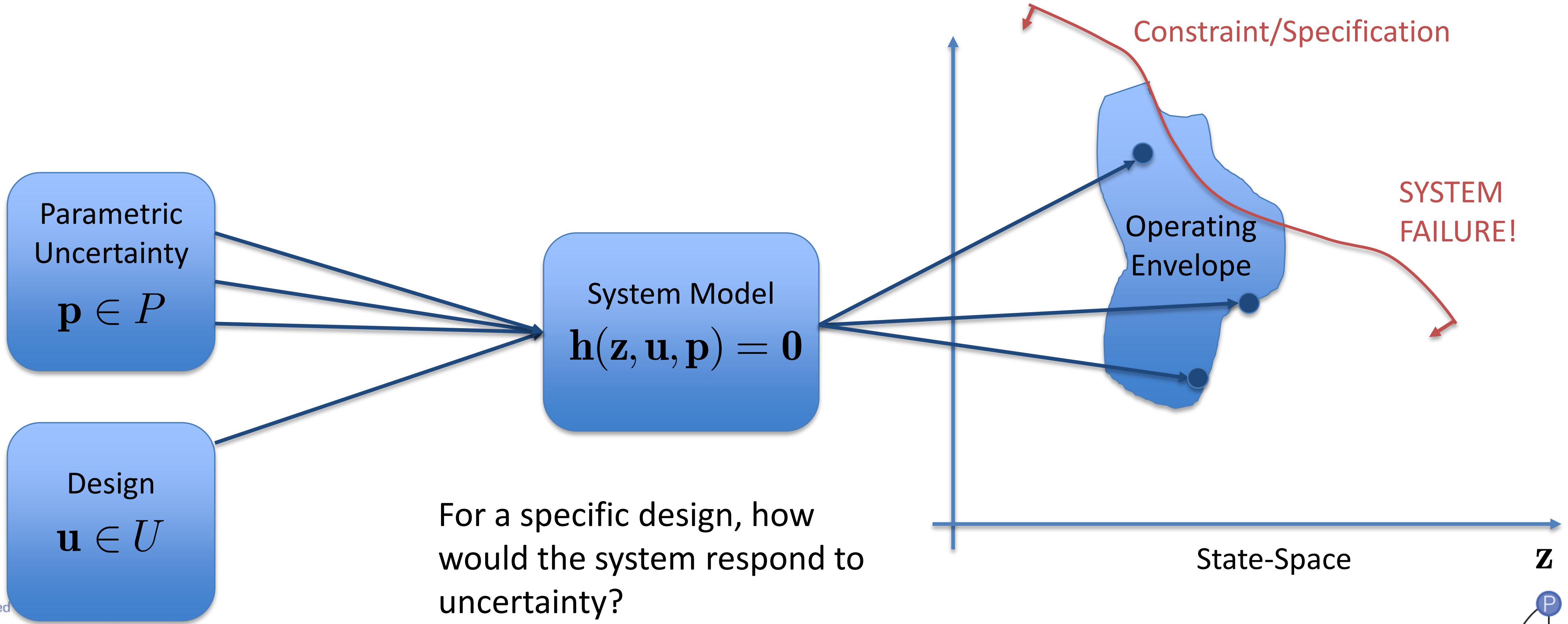
For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty



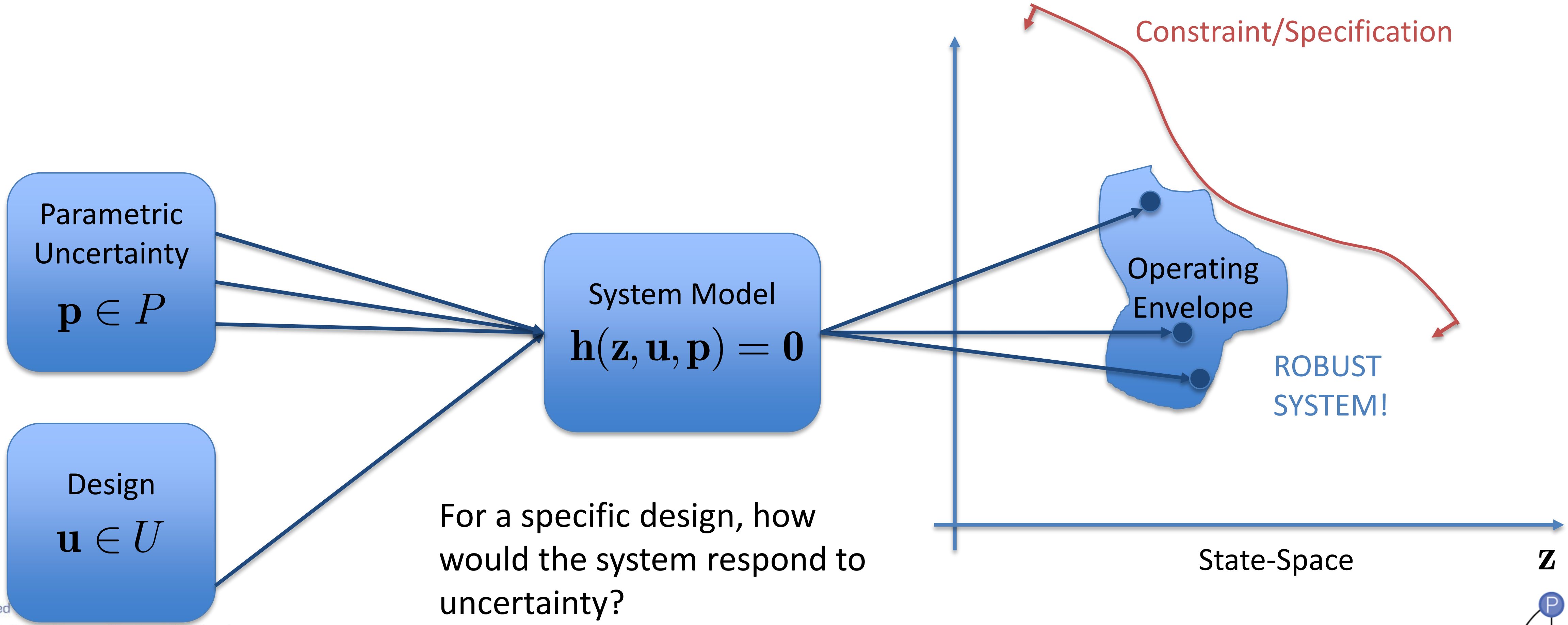
For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty



For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty



For a specific design, how would the system respond to uncertainty?

Accounting for Uncertainty

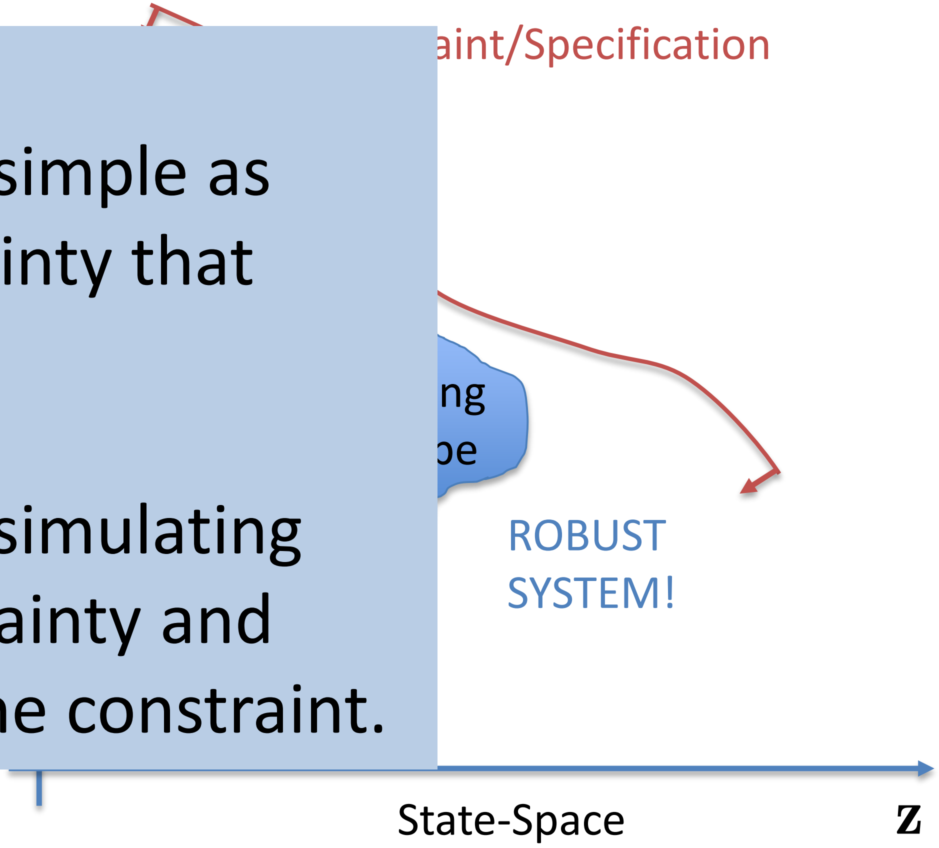
Research Challenge:

Verifying a system is not robust is as simple as finding a single realization of uncertainty that violates the constraint.

Verifying a system is robust requires simulating infinitely-many realizations of uncertainty and ensuring the system never violates the constraint.

Design $\mathbf{u} \in U$

would the system respond to uncertainty?



Introduction

- Steady-state vs. dynamical systems models

System Model

$$\mathbf{h}(\mathbf{z}, \mathbf{u}, \mathbf{p}) = \mathbf{0}$$

nonlinear algebraic system

System Model

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

nonlinear ODE system

Introduction

- Steady-state vs. dynamical systems models

System Model

$$\mathbf{h}(\mathbf{z},\mathbf{u},\mathbf{p}) = \mathbf{0}$$

nonlinear algebraic system

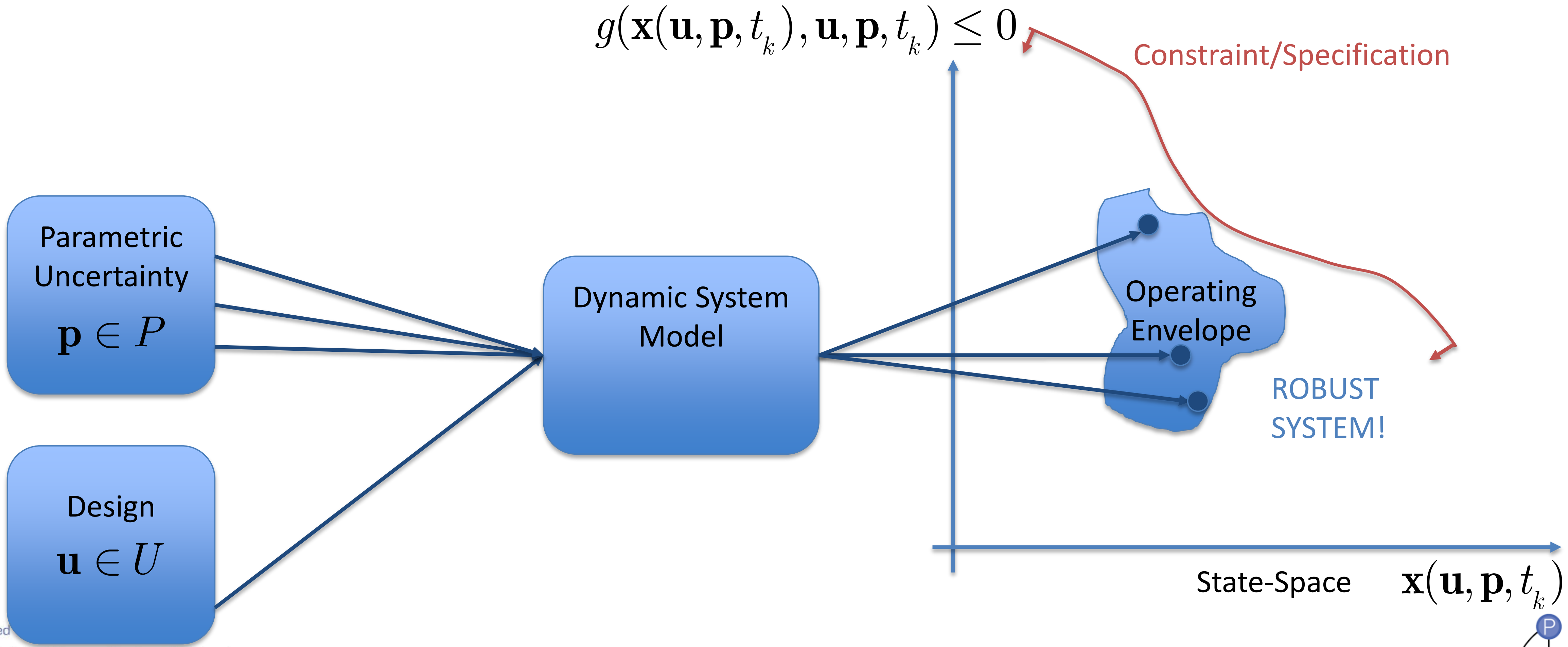
System Model

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

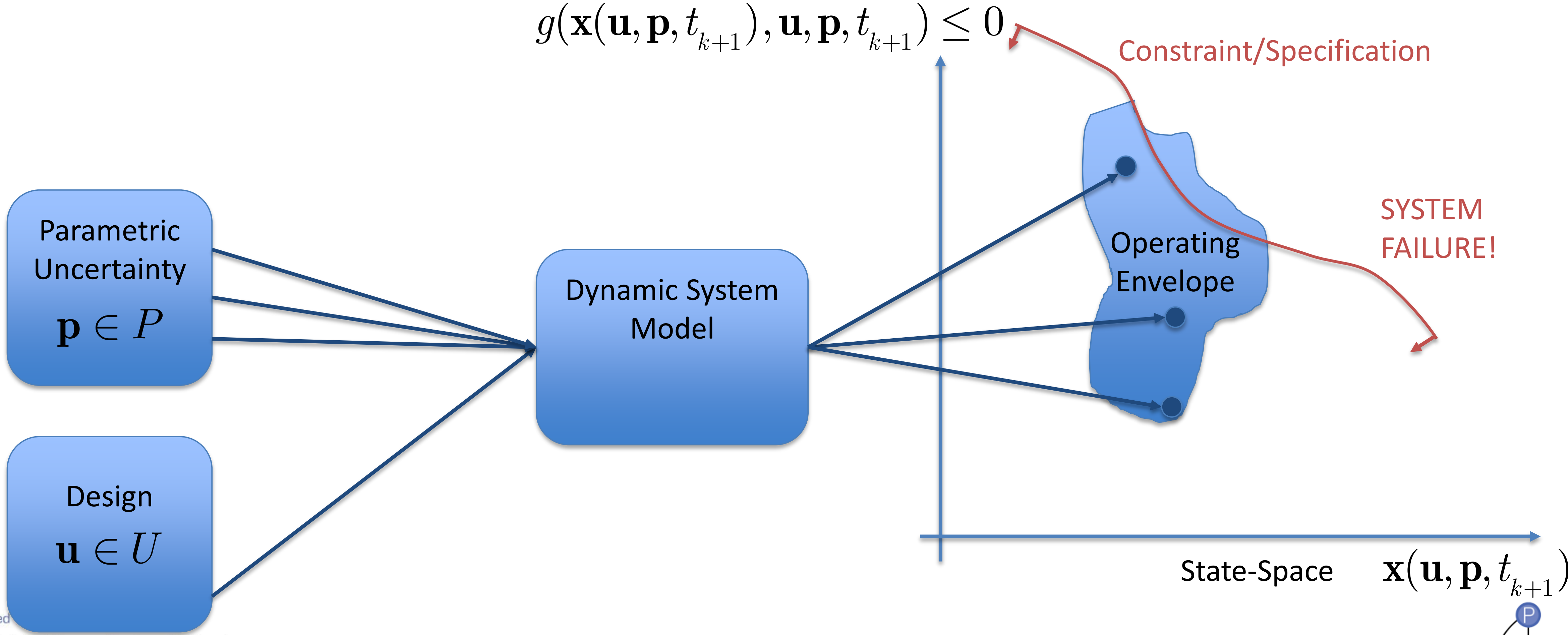
nonlinear ODE system

Now, we must account for the transient response to uncertainty in our design.

Accounting for Uncertainty



Accounting for Uncertainty



Preliminaries

- From a design perspective, our objective is to verify performance/safety in the face of (the worst-case) uncertainty over the time horizon.

$$\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t\in I} g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t)$$
$$\text{s.t.}\ \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t)$$
$$\mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})$$

Preliminaries

- From a design perspective, our objective is to verify performance/safety in the face of (the worst-case) uncertainty over the time horizon.

$$
\begin{aligned}
\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t\in I} &\; g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
\text{s.t.} &\; \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
&\; \mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})
\end{aligned}
$$

If $\gamma(\mathbf{u}) \leq 0$, we have verified the robustness of our design **u**.

"For a given design, the system does not violate performance/safety at any point in time, even in the face of the worst-case uncertainty"

Preliminaries

Discrete-time reformulation, e.g., implicit Euler:

$$\dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t)$$
$$\mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})$$

$\Rightarrow$

$$\mathbf{y}_0 = \mathbf{x}_0(\mathbf{u},\mathbf{p})$$
$$\mathbf{y}_{i+1} = \mathbf{y}_i + h\mathbf{f}(\mathbf{y}_{i+1},\mathbf{u},\mathbf{p},t_{i+1}),\ \ i = 1,\ldots,K$$

Where we have $\mathbf{y}_i(\mathbf{u},\mathbf{p}) \approx \mathbf{x}(\mathbf{u},\mathbf{p},t_i)$

Preliminaries

Discrete-time reformulation, e.g., implicit Euler:

$$\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t\in I} g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t)$$
$$\text{s.t.}\ \ \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t)$$
$$\mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})$$

$$\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t_k\in I, \mathbf{y}} g(\mathbf{y},\mathbf{u},\mathbf{p},t_k)$$
$$\text{s.t.}\ \ \mathbf{y}_0 = \mathbf{x}_0(\mathbf{u},\mathbf{p})$$
$$\underbrace{\begin{array}{l} \mathbf{y}_1 - \mathbf{y}_0 - h\mathbf{f}(\mathbf{y}_1,\mathbf{u},\mathbf{p},t_1) = \mathbf{0} \\ \vdots \qquad \vdots \\ \mathbf{y}_K - \mathbf{y}_{K-1} - h\mathbf{f}(\mathbf{y}_K,\mathbf{u},\mathbf{p},t_K) = \mathbf{0} \end{array}}_{\mathbf{h}(\mathbf{y},\mathbf{u},\mathbf{p}) = \mathbf{0}}$$

Preliminaries

Discrete-time reformulation, e.g., implicit Euler:

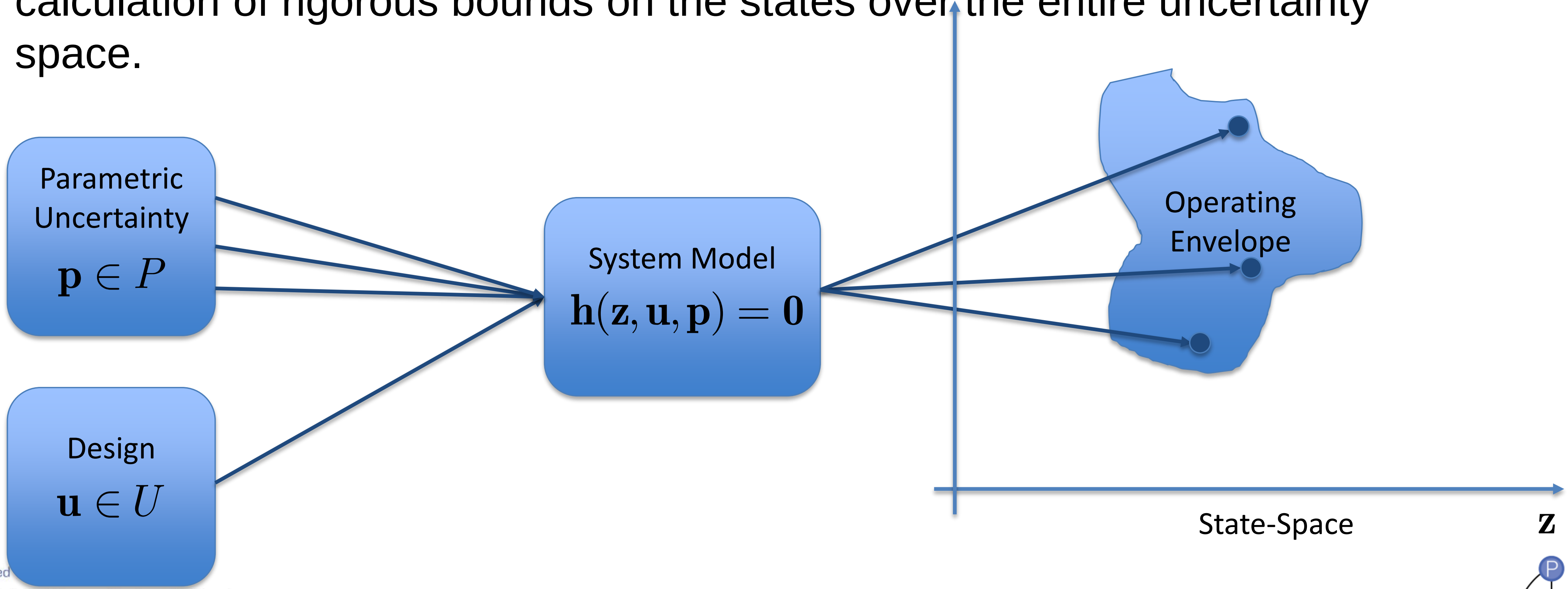
$$
\begin{aligned}
\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t\in I} \; & g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
\text{s.t.} \; & \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
& \mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})
\end{aligned}
$$

$$
\begin{aligned}
\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t_k\in I, \mathbf{y}} \; & g(\mathbf{y},\mathbf{u},\mathbf{p},t_k) \\
\text{s.t.} \; & \mathbf{y}_0 = \mathbf{x}_0(\mathbf{u},\mathbf{p}) \\
& \underbrace{\begin{aligned}
& \mathbf{y}_1 - \mathbf{y}_0 - h\mathbf{f}(\mathbf{y}_1,\mathbf{u},\mathbf{p},t_1) = \mathbf{0} \\
& \vdots \qquad \vdots \\
& \mathbf{y}_K - \mathbf{y}_{K-1} - h\mathbf{f}(\mathbf{y}_K,\mathbf{u},\mathbf{p},t_K) = \mathbf{0}
\end{aligned}}_{\mathbf{h}(\mathbf{y},\mathbf{u},\mathbf{p}) = \mathbf{0}}
\end{aligned}
$$

Related to “orthogonal collocation” approach: Biegler (1983)

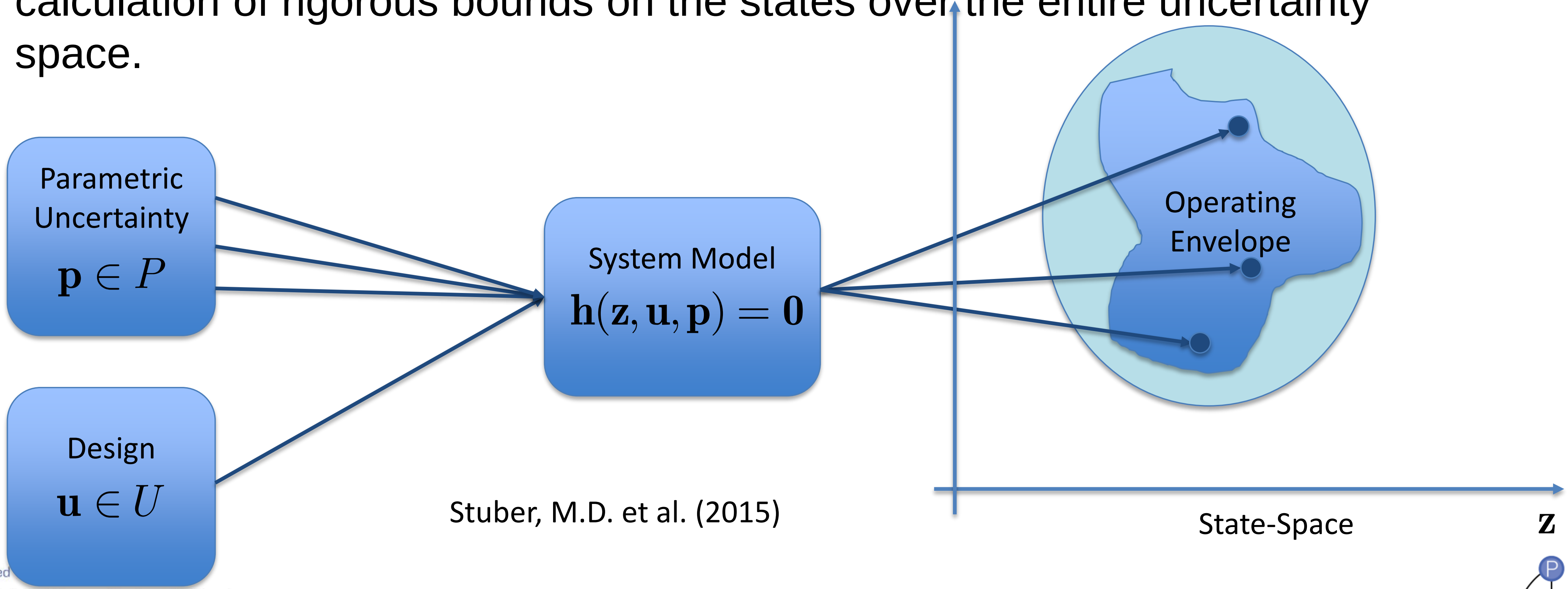
Robust Steady-State Simulation

- Previous developments: a set-valued mapping theory that enables the calculation of rigorous bounds on the states over the entire uncertainty space.



Robust Steady-State Simulation

- Previous developments: a set-valued mapping theory that enables the calculation of rigorous bounds on the states over the entire uncertainty space.



Stuber, M.D. et al. (2015)

Robust Steady-State Simulation

- How does this work mathematically?
  - Implicit function theorem

$$\mathbf{h}(\mathbf{z},\mathbf{u},\mathbf{p}) = \mathbf{0} \Rightarrow \mathbf{z} = \mathbf{x}(\mathbf{u},\mathbf{p}) : \mathbf{h}(\mathbf{x}(\mathbf{u},\mathbf{p}),\mathbf{u},\mathbf{p}) = \mathbf{0}$$

  - (parametric) mean value theorem

$$\mathbf{M}(\mathbf{u},\mathbf{p})(\mathbf{x}(\mathbf{u},\mathbf{p}) - \boldsymbol{\gamma}(\mathbf{u},\mathbf{p})) = -\mathbf{h}(\boldsymbol{\gamma}(\mathbf{u},\mathbf{p}),\mathbf{u},\mathbf{p})$$

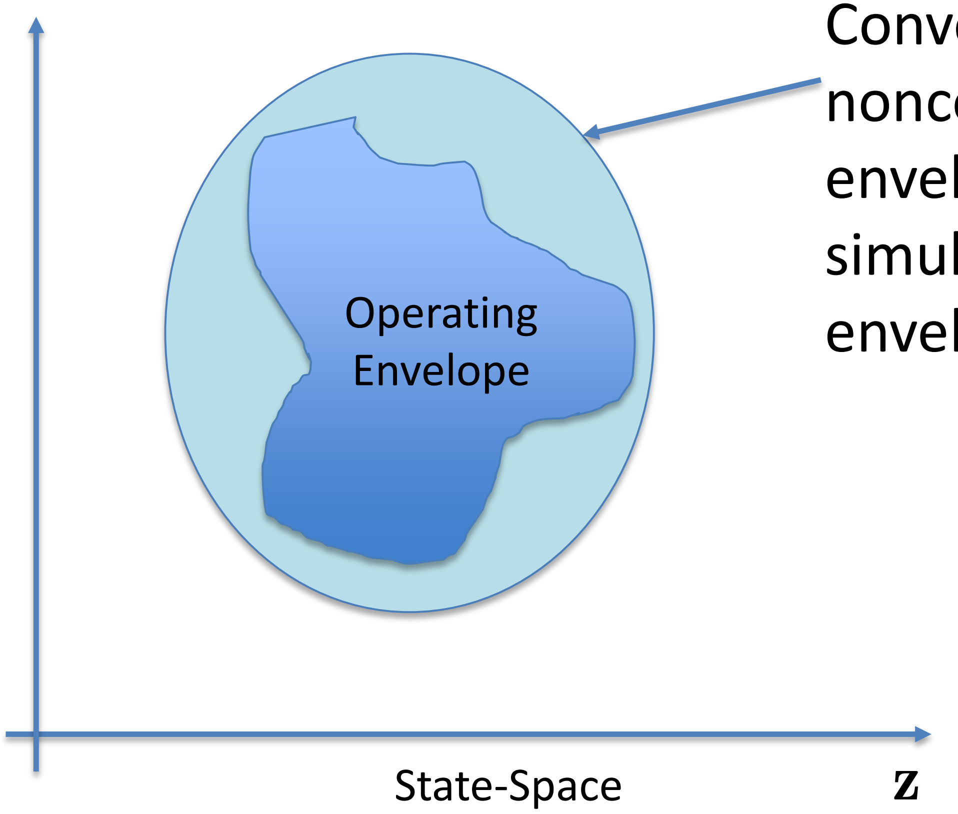
  - Fixed-point iterations

$$\mathbf{x}^{k+1}(\mathbf{u},\mathbf{p}) := \boldsymbol{\Phi}(\mathbf{x}^{k}(\mathbf{u},\mathbf{p}))$$

  - Rigorous (global) set-valued arithmetic
    - Interval arithmetic
    - generalized McCormick convex relaxations

Stuber, M.D. et al. (2015)

Robust Steady-State Simulation



Convex relaxation of nonconvex operating envelope (without actually simulating the operating envelope)

Stuber, M.D. et al. (2015)

Robust Dynamic Simulation

- Our dynamic model is reformulated in the discrete form as a nonlinear algebraic system:

$$\mathbf{h}(\mathbf{y},\mathbf{u},\mathbf{p}) = \begin{pmatrix} \mathbf{y}_0 - \mathbf{x}_0(\mathbf{u},\mathbf{p}) \\ \mathbf{y}_1 - \mathbf{y}_0 - h\mathbf{f}(\mathbf{y}_1,\mathbf{u},\mathbf{p},t_1) \\ \vdots \\ \mathbf{y}_K - \mathbf{y}_{K-1} - h\mathbf{f}(\mathbf{y}_K,\mathbf{u},\mathbf{p},t_K) \end{pmatrix} = \mathbf{0}$$

$$\mathbf{h} : \mathbb{R}^{n_x(K+1)} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_p} \rightarrow \mathbb{R}^{n_x(K+1)}$$

Robust Dynamic Simulation

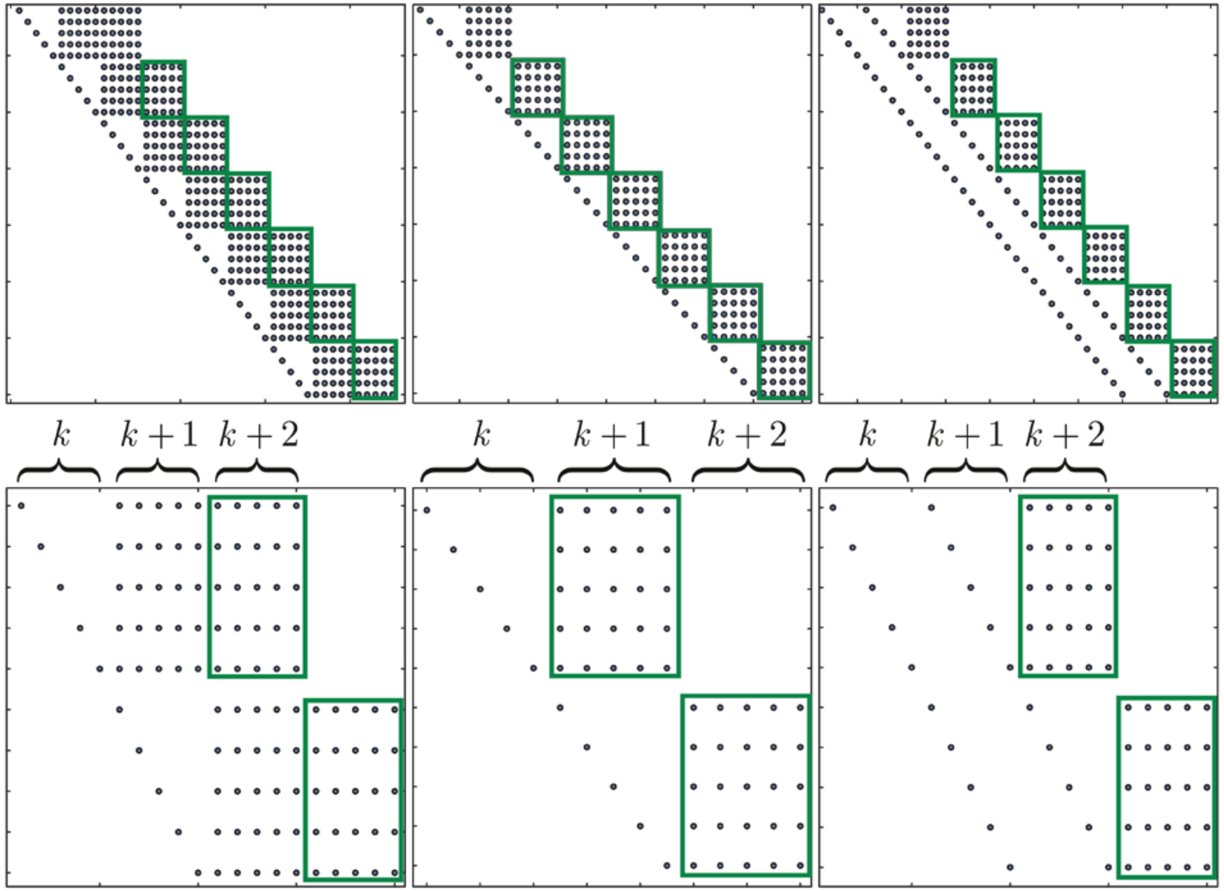
- Our dynamic model is reformulated in the discrete form as a nonlinear algebraic system:

$$\mathbf{h}(\mathbf{y},\mathbf{u},\mathbf{p}) = \begin{pmatrix} \mathbf{y}_0 - \mathbf{x}_0(\mathbf{u},\mathbf{p}) \\ \mathbf{y}_1 - \mathbf{y}_0 - h\mathbf{f}(\mathbf{y}_1,\mathbf{u},\mathbf{p},t_1) \\ \vdots \\ \mathbf{y}_K - \mathbf{y}_{K-1} - h\mathbf{f}(\mathbf{y}_K,\mathbf{u},\mathbf{p},t_K) \end{pmatrix} = \mathbf{0}$$

Very large!

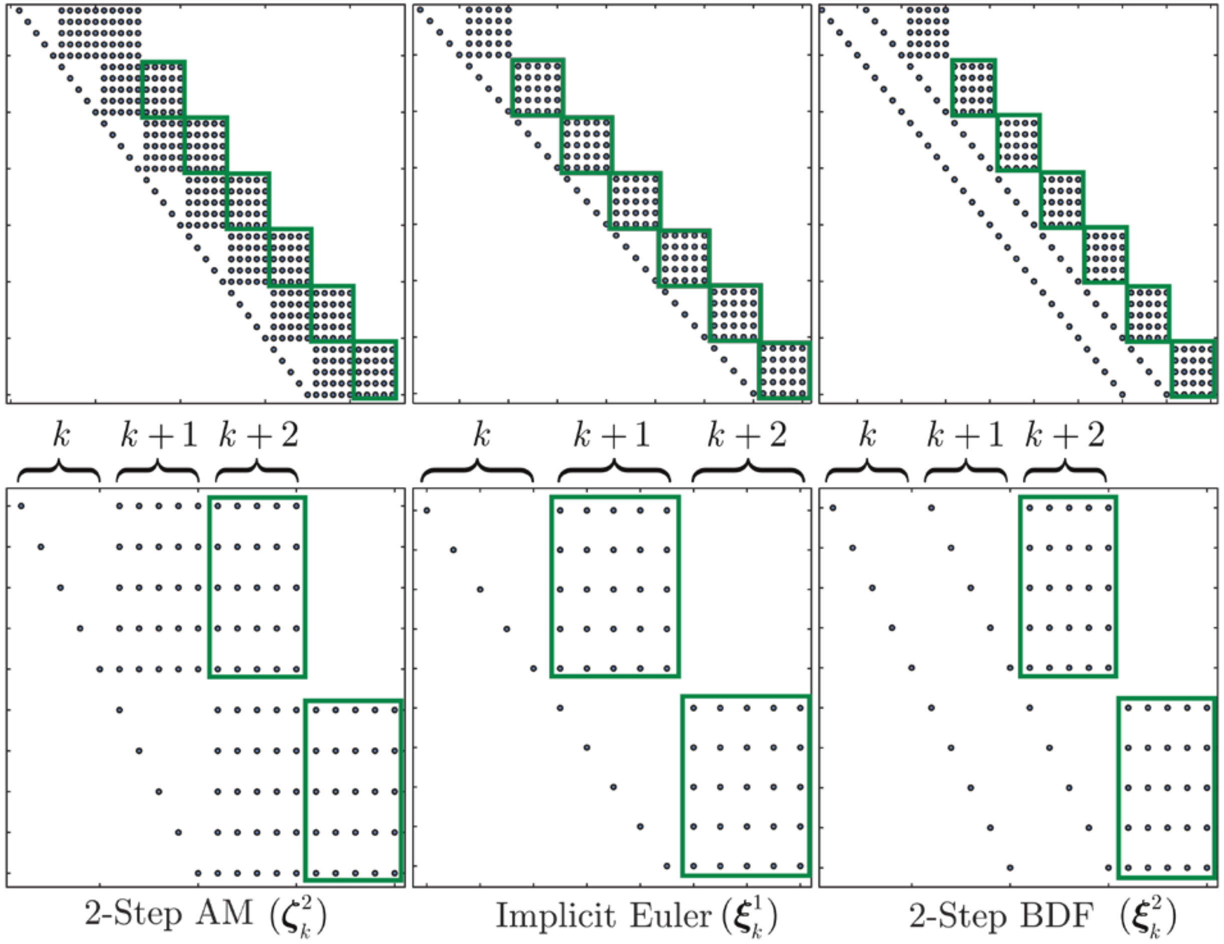
$$\mathbf{h} : \mathbb{R}^{n_x(K+1)} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_p} \to \mathbb{R}^{n_x(K+1)}$$

Robust Dynamic Simulation



2-Step AM (ζ_k^2)   Implicit Euler (ξ_k^1)   2-Step BDF (ξ_k^2)

Robust Dynamic Simulation

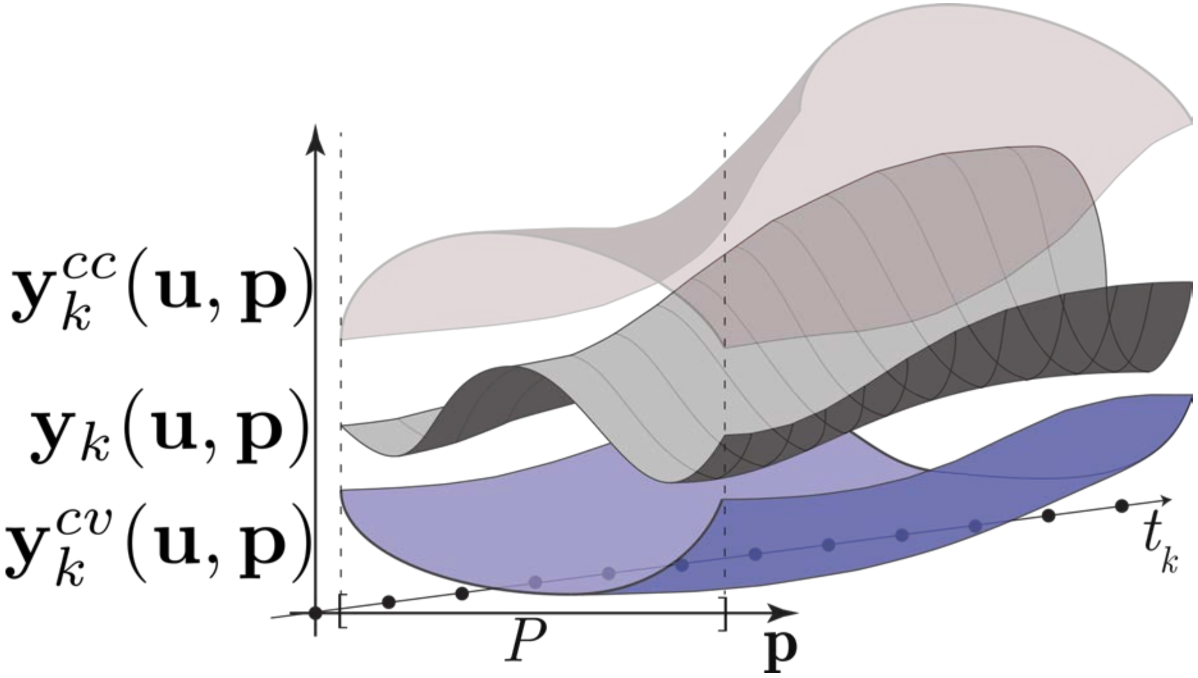


Here, we have 5 states. For a system with K=1000, we would need to account for a 5000-dimension system simultaneously.

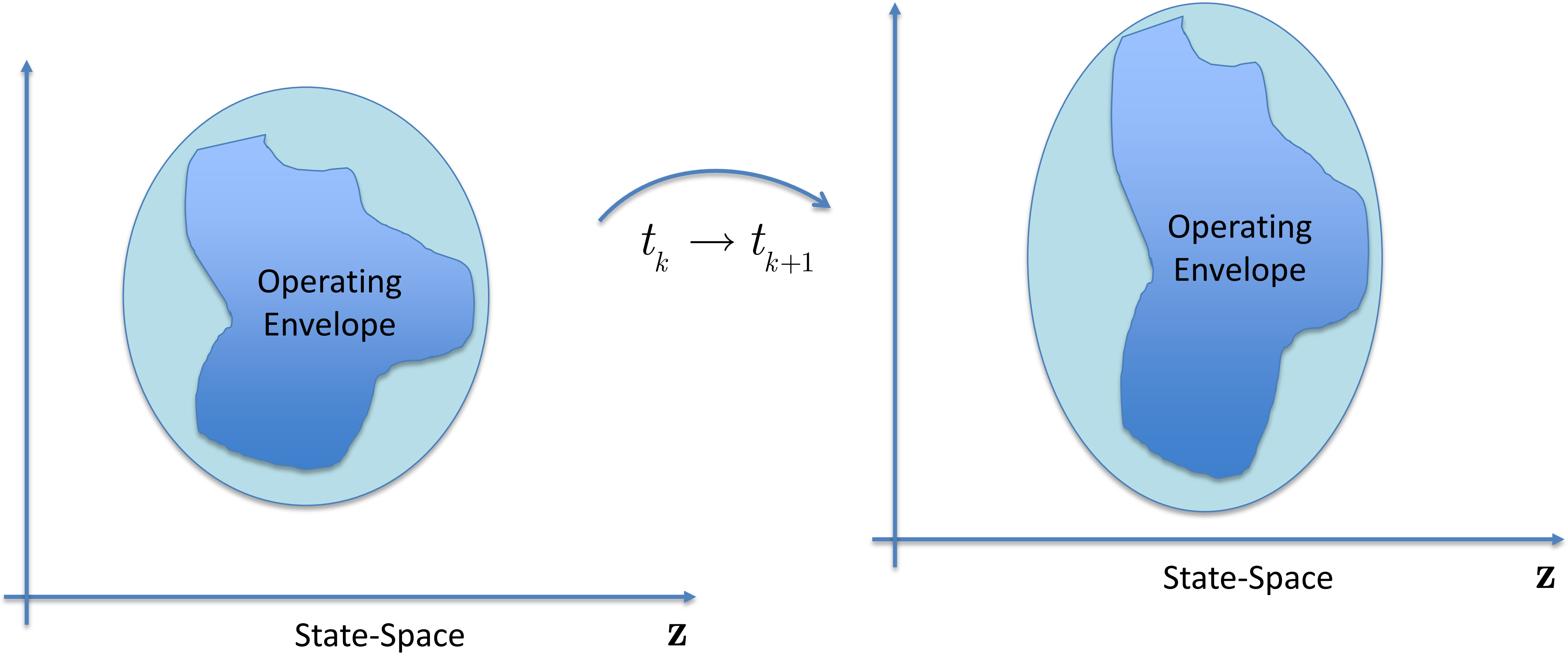
Each block of unknowns only depends on the previous timesteps (known). Thus, we only need to account for a single 5-dimensional system sequentially.

Robust Dynamic Simulation

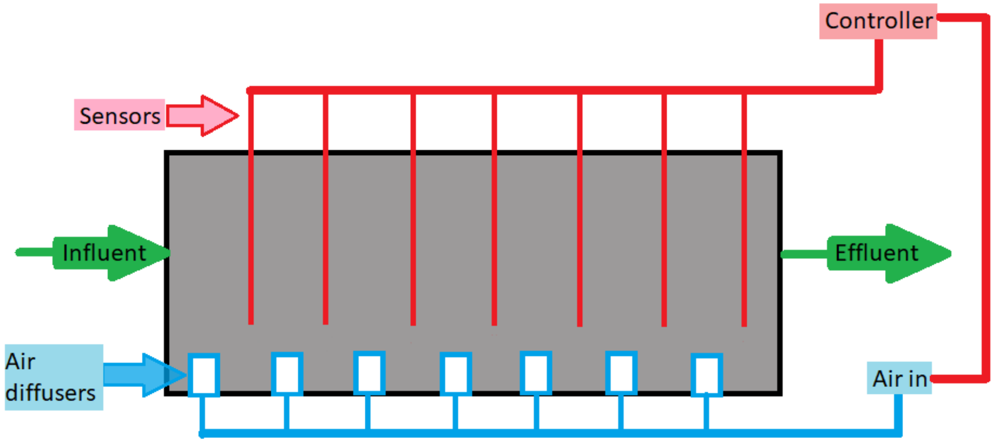
Apply the theory introduced previously for robust steady-state simulation to our system $\mathbf{h}(\mathbf{y}, \mathbf{u}, \mathbf{p}) = \mathbf{0}$ to calculate rigorous bounds on the state variables over the range of uncertainty variables **p** and design variables **u**, block-by-block.



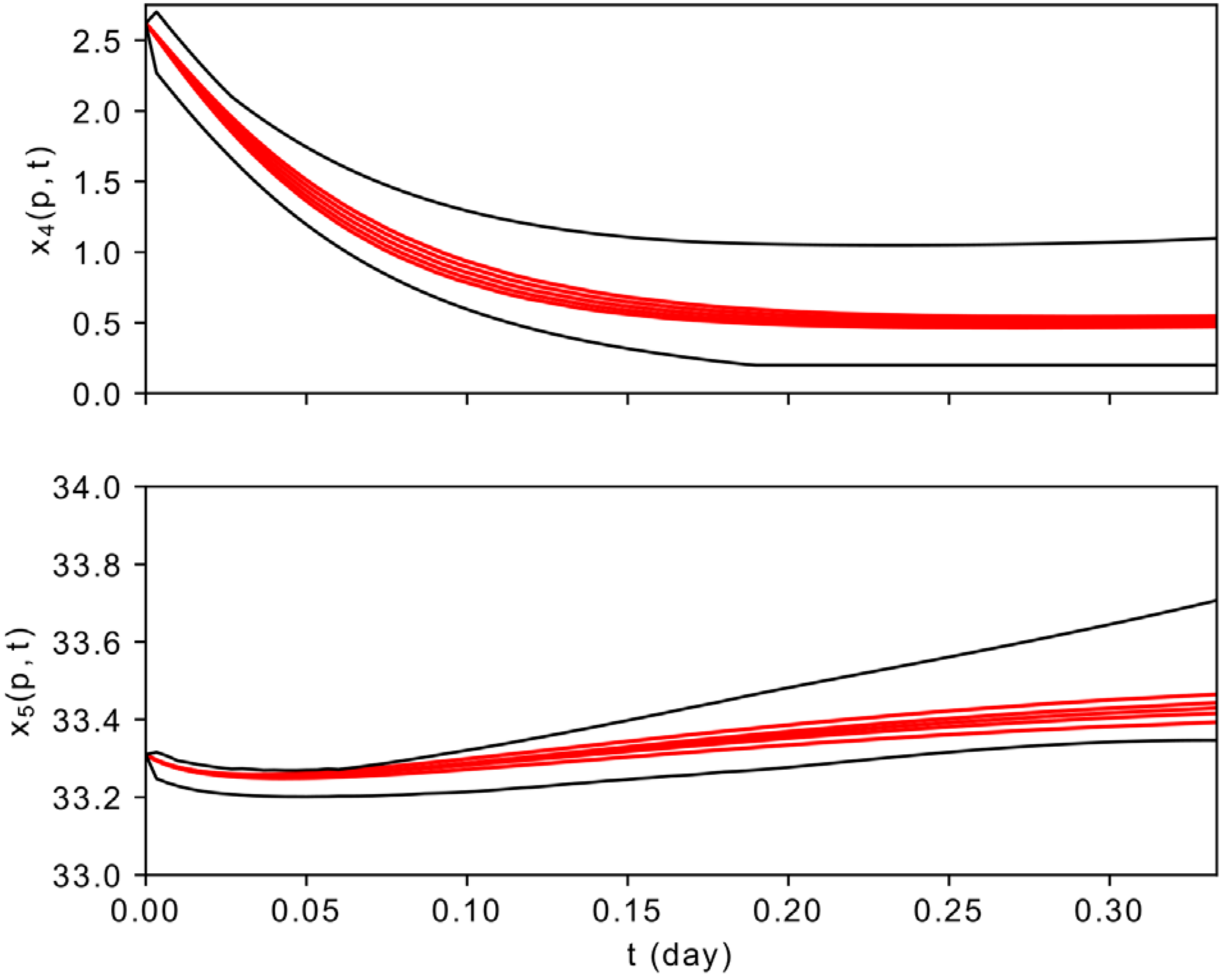
Robust Dynamic Simulation



Robust Dynamic Simulation



Control of a 9-species biological reaction for wastewater treatment.



Future Work

- Extend the worst-case uncertainty verification to the robust design problem to “minimize the maximum impact of uncertainty”

$$
\begin{aligned}
\gamma(\mathbf{u}) = \max_{\mathbf{p}\in P, t\in I} \; & g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
\text{s.t.} \;\; & \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
& \mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})
\end{aligned}
$$

$$
\begin{aligned}
\min_{\mathbf{u}\in U, \eta\in\mathbb{R}} \; & \eta \\
\text{s.t.} \;\; & \eta \geq \max_{\mathbf{p}\in P, t\in I} g(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
& \qquad \text{s.t.} \;\; \dot{\mathbf{x}}(\mathbf{u},\mathbf{p},t) = \mathbf{f}(\mathbf{x}(\mathbf{u},\mathbf{p},t),\mathbf{u},\mathbf{p},t) \\
& \qquad\qquad \mathbf{x}(\mathbf{u},\mathbf{p},0) = \mathbf{x}_0(\mathbf{u},\mathbf{p})
\end{aligned}
$$

Conclusion

- We have developed a method for rigorously bounding the operating envelope of a dynamical system
- We enable a simulation-based approach with deterministic global optimization for worst-case safety verification
- We have developed the theory for higher-order implicit integration methods (parametric implicit linear multistep methods).
- Focused on two-step (2^{nd}-order) methods
  - Much greater accuracy than implicit Euler
  - Unconditionally stable

Thank you!

Any Questions?

This material is based upon work supported by the National Science Foundation under Grant No. 1932723. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.