# Cybersecurity and Quantum Computation in Control of Cyberphysical Systems for Next-Generation Manufacturing

**Helen Durand**

Department of Chemical Engineering and Materials Science
Wayne State University

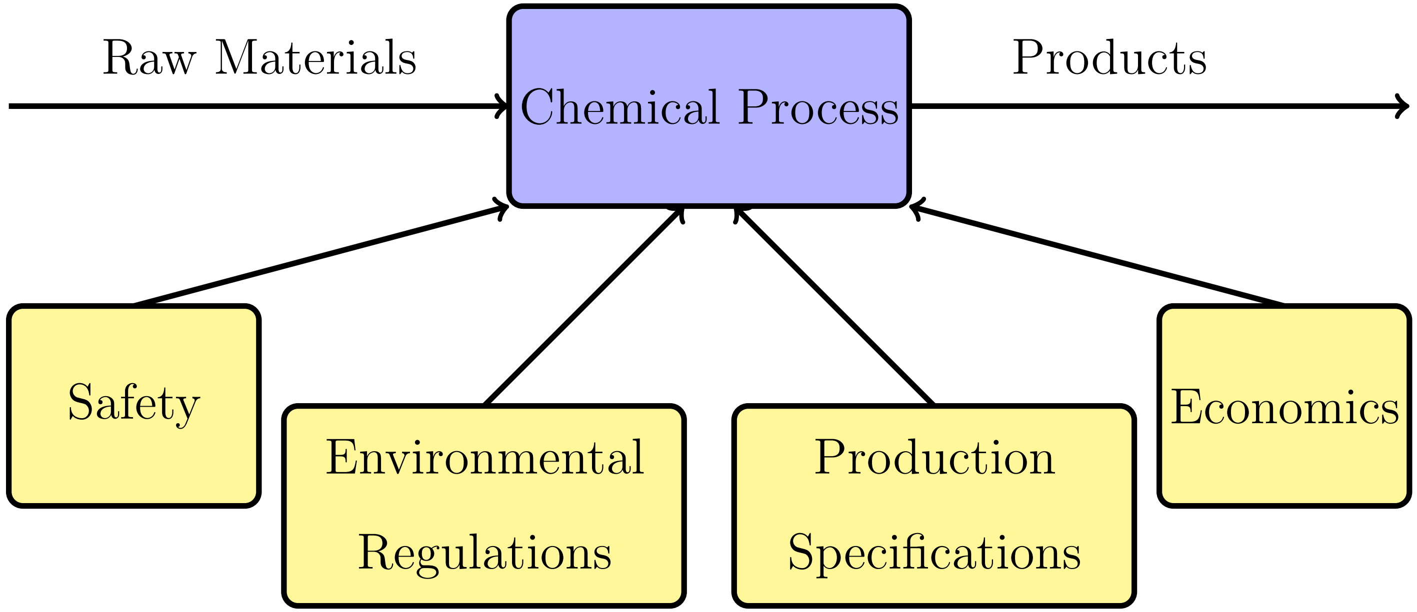
Academy of Scholars
Wayne State University
May 17, 2023

# PAST EXPERIENCES

- B.S. Chemical Engineering, University of California, Los Angeles
- Materials and Processes Engineering Department, Aerojet Rocketdyne
- M.S. and Ph.D. Chemical Engineering, University of California, Los Angeles
- Assistant Professor, Wayne State University

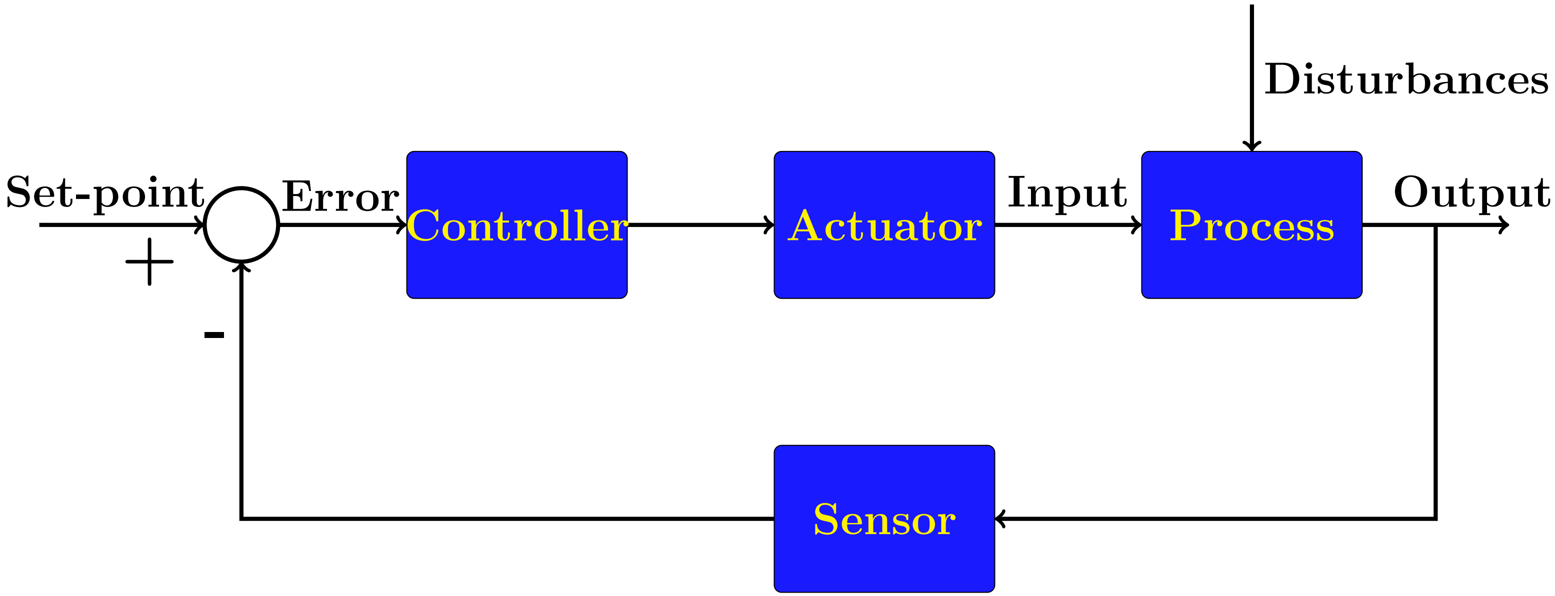
# INTRODUCTION

- Incentives for chemical process control



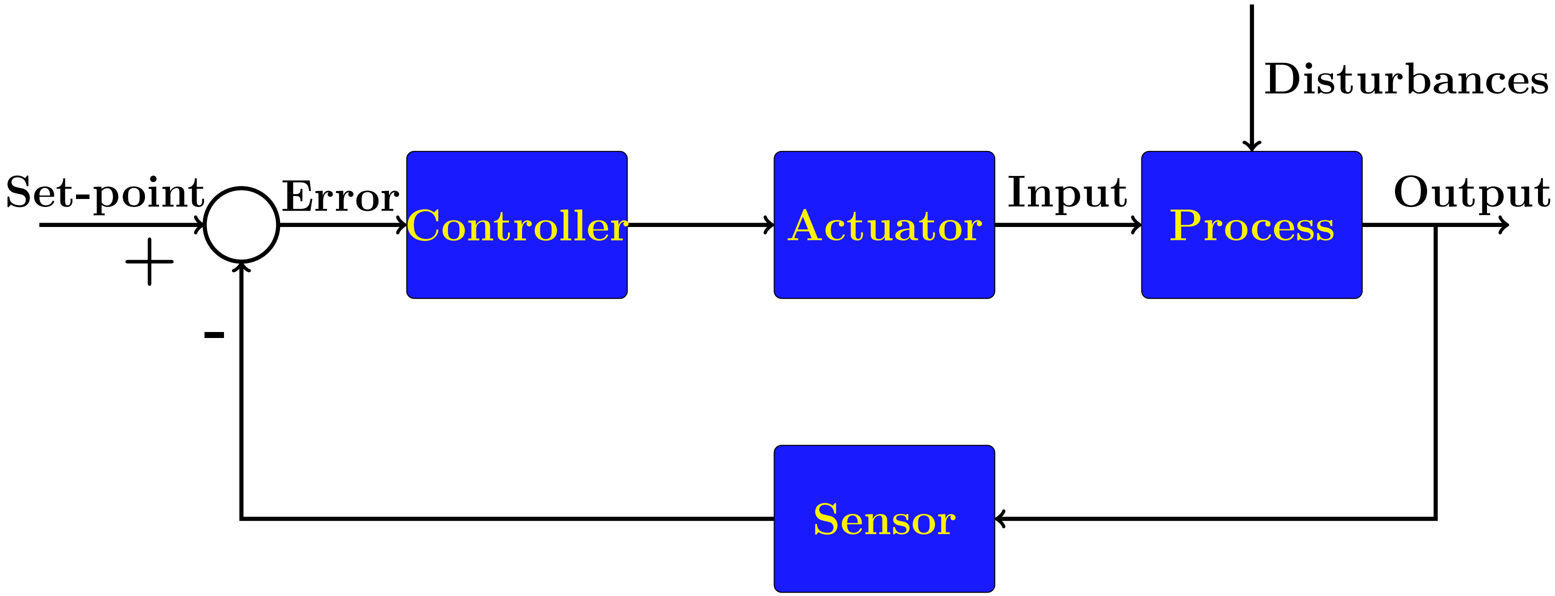

- Need for continuous monitoring and external intervention (process control)
- Objectives of a process control system
  - ◇ Ensuring stability of the process
  - ◇ Suppressing the influence of external disturbances
  - ◇ Optimizing process performance

# FEEDBACK CONTROL LOOP




- How a feedback control loop (closed-loop system) works:
  - ◇ A variable describing the condition of a process (e.g., temperature, pressure, species concentration; known as an output) is measured by a sensor
  - ◇ The error between the measured output value and the desired value of this output (set-point) is calculated and fed to the controller
  - ◇ The controller computes a value of the manipulated input to the process to reduce the error
  - ◇ A control actuator (typically a valve) is used to apply the manipulated input value to the process

# CLASSICAL CONTROL




- Classical control: single-input/single-output (SISO) control design
  - ◇ Proportional-integral-derivative (PID) control (error $e(t)$)
    - ▷ Error reflects difference between measured output and set-point
  - ◇ Input/control action $u(t)$

$$u(t) = \underbrace{K_c e(t)}_{\text{P}} + \underbrace{\frac{1}{\tau_I}\int_0^t e(\tau)d\tau}_{\text{I}} + \underbrace{\tau_D \frac{de(t)}{dt}}_{\text{D}}$$

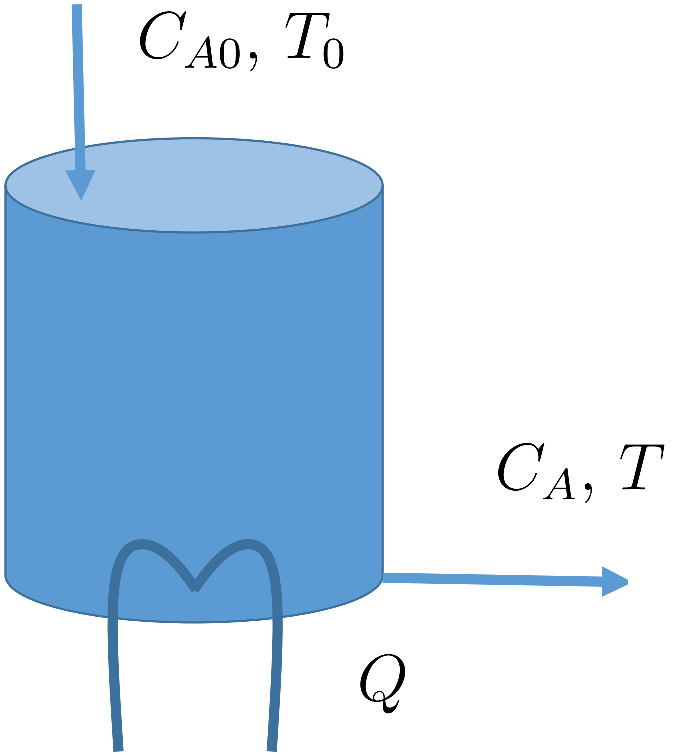
  - ◇ $K_c$, $\tau_I$, $\tau_D$: scalar values that can be picked (tuned)

# ADVANCED MODEL-BASED PROCESS CONTROL

- Advanced process control utilizes a process dynamic model explicitly in the controller design
  - ◇ A mathematical process model is developed:
    - ▷ Constructed from first-principles
    - ▷ Identified from input-output process data
  - ◇ The model describes the process dynamics (variation of the process state variables in time due to disturbances, inputs, and interactions between variables)
  - ◇ Controllers are synthesized based on the process model
- Advantages of model-based control
  - ◇ Possibility of improved closed-loop performance
  - ◇ Model accounts for inherent process characteristics (e.g., nonlinear behavior, multivariable interactions)
  - ◇ Characterization of limitations on achievable closed-loop stability, performance and robustness

# NONLINEAR MODEL-BASED PROCESS CONTROL

- Example: continuous stirred tank reactor (CSTR)




- Model: system of nonlinear ordinary differential equations (ODEs)

$$\frac{dT}{dt} = \frac{F}{V_r}(T_0 - T) + \frac{(-\Delta H)}{\rho C_p} k_0 e^{-E/RT} C_A + \frac{Q}{\rho C_p V_r}$$

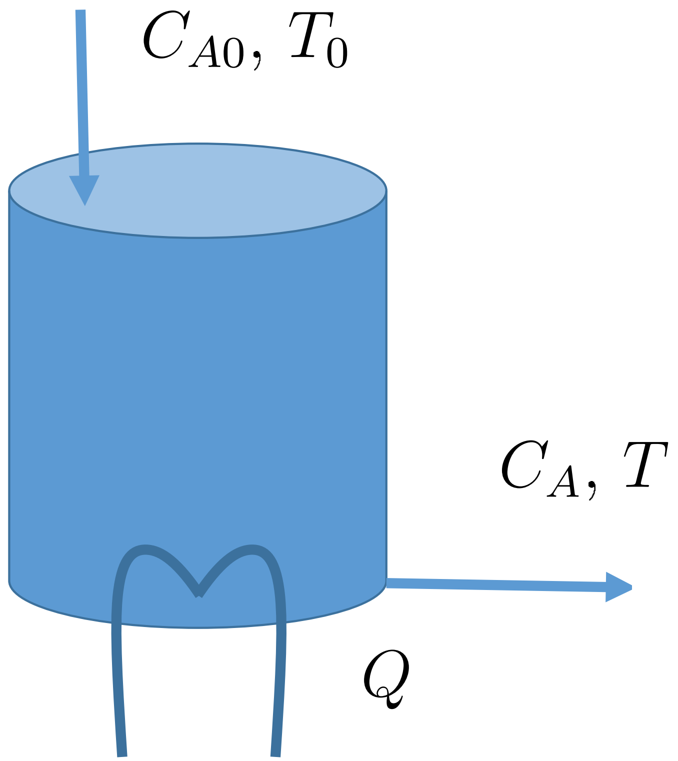
$$\frac{dC_A}{dt} = \frac{F}{V_r}(C_{A0} - C_A) - k_0 e^{-E/RT} C_A$$

$$\Rightarrow x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} T - T_s \\ C_A - C_{As} \end{bmatrix}, \ \dot{x} = \frac{dx}{dt}$$

$$u = Q - Q_s, \ w = C_{A0} - C_{A0s}$$

# NONLINEAR MODEL-BASED PROCESS CONTROL

- Example: continuous stirred tank reactor (CSTR)




- Model: system of nonlinear ordinary differential equations (ODEs)

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

- Techniques for nonlinear controller design for driving the process state to the operating steady-state

  ◇ Lyapunov-based control ◇ Model predictive control

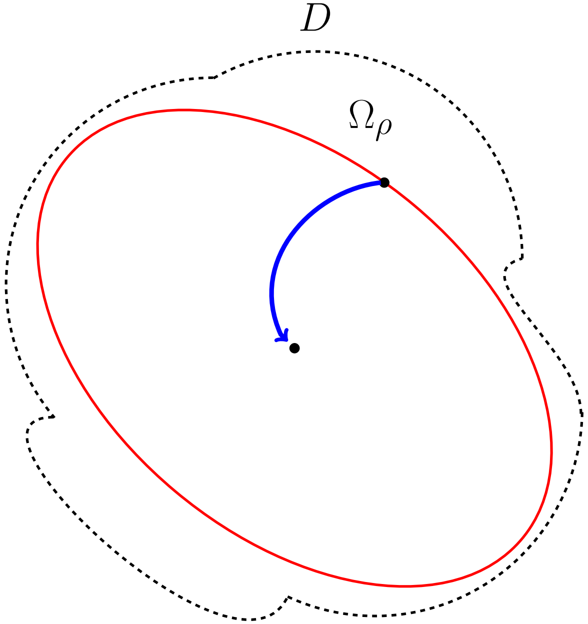
# NONLINEAR PROCESS SYSTEMS

- State-space description

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

  - ◇ $x \in X \subset \mathbb{R}^n$ is the state, $u \in U \subset \mathbb{R}^m$ is the manipulated input, $w \in W \subset \mathbb{R}^l$ is the disturbance, $f$ is a vector function

- Explicit nonlinear feedback control law: $u = h(x)$




  - ◇ Control design technique: Lyapunov-based control
    (Y. Lin and E.D. Sontag, *SCL*, 1991; H. Khalil, *Prentice Hall*, 2002; P. D. Christofides and N. H. El-Farra, *Springer-Verlag*, 2005)
  - ◇ Renders the origin (steady-state) asymptotically stable
  - ◇ There exists a Lyapunov function $V$ which satisfies

$$\dot{V} = \frac{\partial V(x)}{\partial x} f(x, h(x), 0) < 0, \ \forall \, x \in D$$

$V$ : energy of a physical system

  - ◇ Typically, $V(x) = x^T P x$ (quadratic) and $\Omega_\rho \subseteq D$ is a level set of $V$ where state constraints are met (i.e., $\Omega_\rho := \{x \ : \ V(x) \leq \rho\}$)
  - ◇ $u = h(x)$ possesses a degree of robustness to disturbances and uncertainty

- Performance considerations and constraints are not directly/explicitly taken into account

# MODEL PREDICTIVE CONTROL

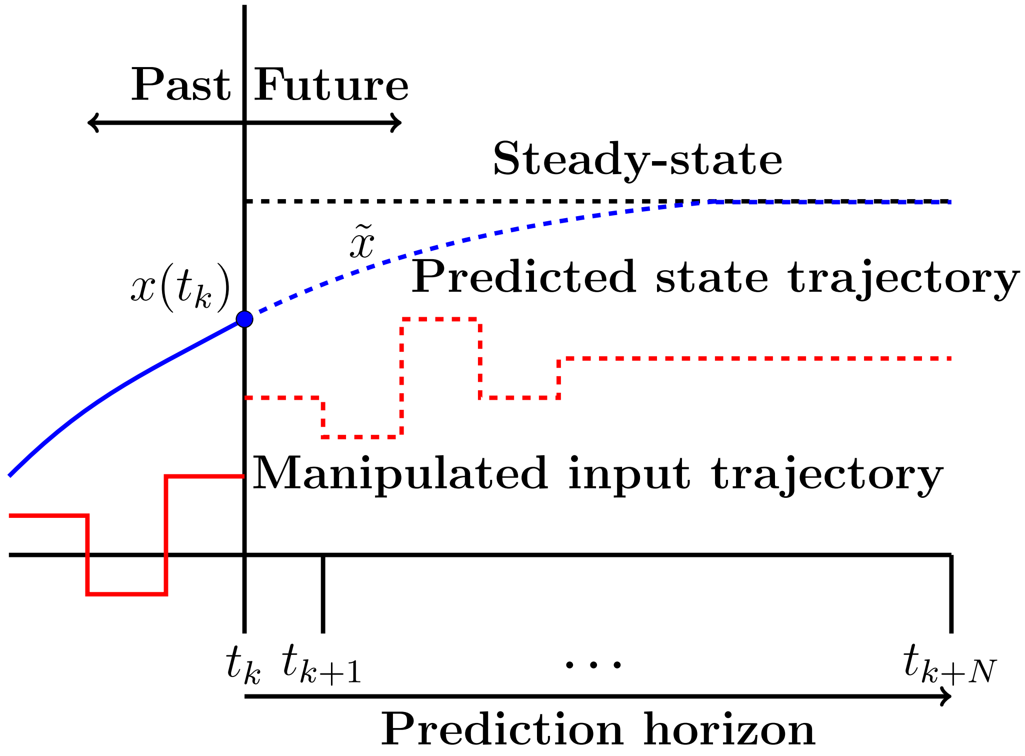
- Model predictive control (MPC)

$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} l_T(\tilde{x}(\tau), u(\tau))\, d\tau$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0)$$

$$\tilde{x}(t_k) = x(t_k)$$

$$u(t) \in U,\ \tilde{x}(t) \in X,\ \forall\ t \in [t_k, t_{k+N})$$




- Quadratic tracking stage cost:

$$l_T(x, u) = x^T Q x + u^T R u$$

  ◇ $Q$, $R$ are positive definite matrices

- Solve the optimization problem every $\Delta$ time units (sampling period)

  ◇ At each sampling time $t_k$

- Solution is a piecewise-constant input trajectory

  ◇ Each piece is held constant for a period $\Delta$

  ◇ Prediction horizon $N$

# MODEL PREDICTIVE CONTROL

- Model predictive control (MPC)

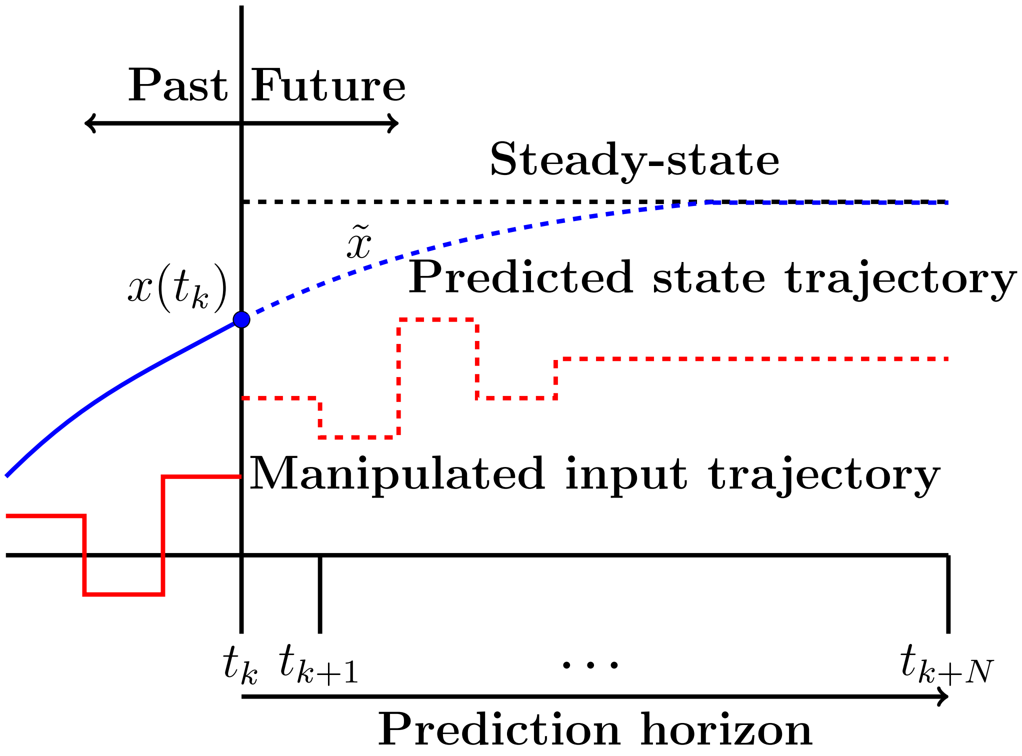
$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} \left[ \tilde{x}^T Q \tilde{x} + u^T R u \right] \, d\tau$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0)$$

$$\tilde{x}(t_k) = x(t_k)$$

$$u(t) \in U, \ \tilde{x}(t) \in X, \ \forall \, t \in [t_k, t_{k+N})$$

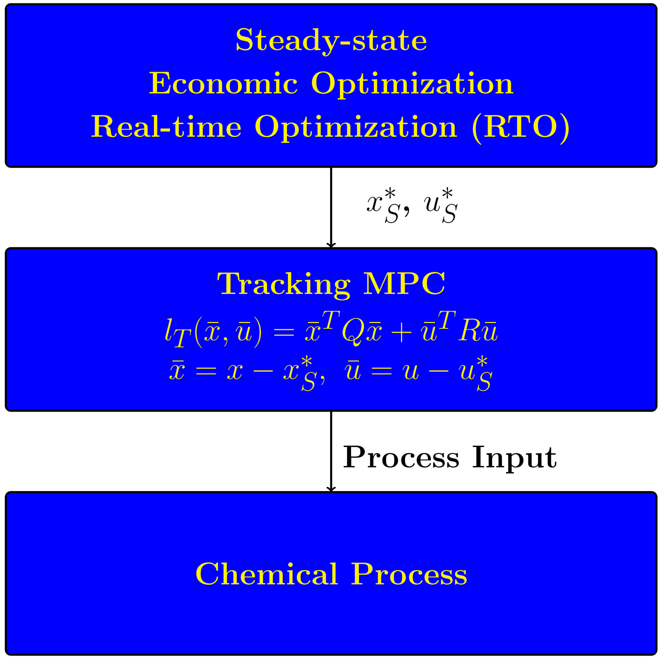
- Receding horizon implementation
  - ◇ Only the first piece of the input trajectory is applied
    - ▷ Allows for feedback at every $\Delta$
    - ▷ Accounts for effects of disturbances and plant/model mismatch on the optimal solution
  - ◇ Longer prediction horizon may improve closed-loop performance




- Closed-loop stability is not guaranteed
- Approaches for closed-loop stability
  - ◇ Infinite/sufficiently long prediction horizon
  - ◇ Terminal cost/constraint
  - ◇ Contractive constraint

# NEXT-GENERATION MANUFACTURING

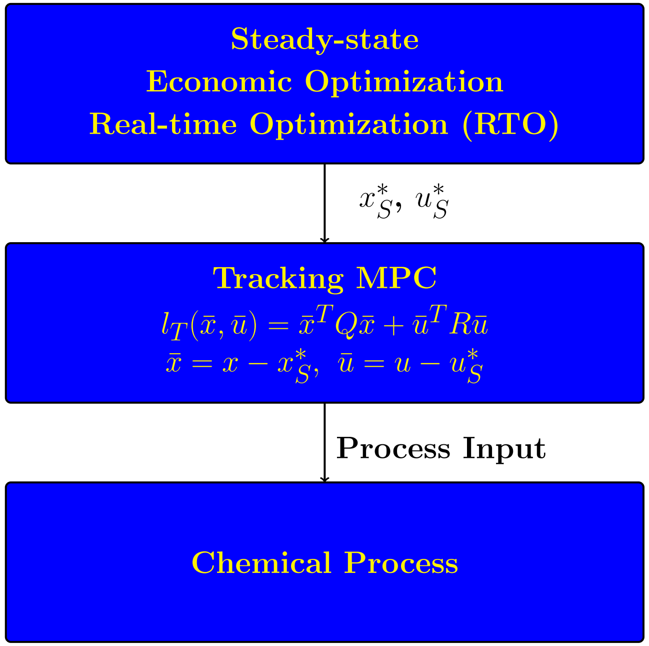
- Next-generation/smart manufacturing objectives (J. Davis, T. Edgar, J. Porter, J. Bernaden and M. Sarli, *Comput. Chem. Eng.*, 2012):
  - Profitability
  - Autonomy
  - Safety and cybersecurity




- Example: Moving away from a hierarchical approach to optimization and control
  - Upper layer:
    - Determine economically-optimal steady-state (real-time optimization (RTO)) (M. L. Darby, M. Nikolaou, J. Jones and D. Nicholson, *JPC*, 2011)
  - Lower layer:
    - Feedback control drives the state of the process to the optimal steady-state
- Tighter integration of plant operation and process economic optimization

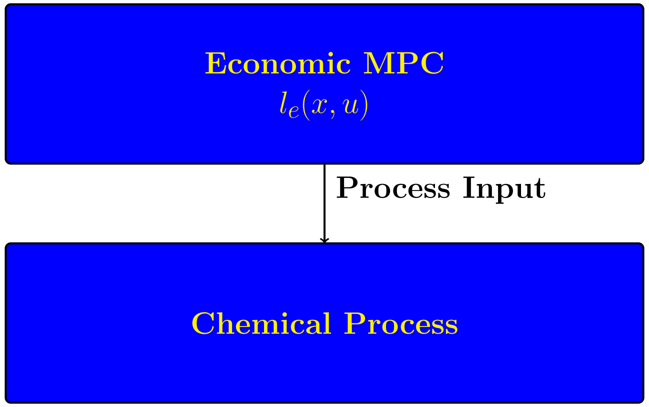
# PROCESS ECONOMICS AND CONTROL

- Traditional Paradigm




**Steady-state operation**

- Integration of economic optimization and process control
- Generalization of MPC
  - ◇ General (economic) stage cost




**Dynamic/time-varying operation**

- Economic MPC (EMPC) potential use cases:
  - ◇ Time-varying objective function or constraints (M. Ellis and P. D. Christofides, *AIChE J.*, 2013; A. Gopalakrishnan and L. T. Biegler, *CACE*, 2013)

(M. Ellis, H. Durand and P. D. Christofides, *JPC*, 2014)

# ECONOMIC MPC FORMULATION

- EMPC formulation:

$$\begin{aligned}
\min_{u(\cdot)\in S(\Delta)} \quad & \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(\tau), u(\tau)) \, d\tau \\
\text{s.t.} \quad & \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \\
& \tilde{x}(t_k) = x(t_k) \\
& u(t) \in U, \ \tilde{x}(t) \in X, \\
& \quad \forall \ t \in [t_k, t_{k+N}) \\
& |u(t_j) - u(t_{j-1})| \leq \epsilon_d \\
& j = k, \ldots, k+N-1
\end{aligned}$$

- Components of EMPC:
  - ◇ Economic cost function
  - ◇ Dynamic model
  - ◇ State feedback measurement
  - ◇ Input and state magnitude constraints
  - ◇ Input rate of change constraints

- System equipped with a measure of instantaneous economics $l_e$
- Computes control actions that optimize economics
- Accounts for input and state constraints
  - ◇ Examples: temperature or flow rate bounds
- Prevents rapid variations in inputs which may damage actuators

# LYAPUNOV-BASED ECONOMIC MPC

## Boundedness / Time-varying Operation (Mode 1)

(M. Heidarinejad *et al.*, *AIChE J.*, 2012)

$$\min_{u(\cdot)\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(\tau), u(\tau))\, d\tau$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0)$$

$$\tilde{x}(t_k) = x(t_k)$$

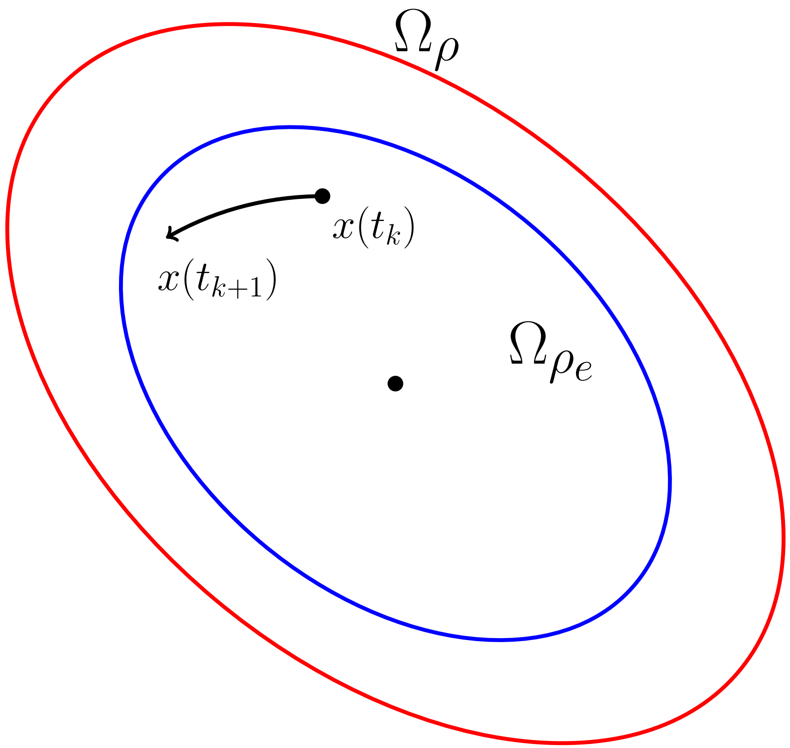
$$u(t) \in U,\ \tilde{x}(t) \in X,\ \forall\, t \in [t_k, t_{k+N})$$

$$|u_i(t_j) - h_i(\tilde{x}(t_j))| \leq \epsilon_r,\ i = 1, \ldots, m,$$

$$j = k, \ldots, k+N-1$$

$$V(\tilde{x}(t)) \leq \rho_e,\ \forall\, t \in [t_k, t_{k+N})$$

$$\text{if } V(x(t_k)) \leq \rho_e \text{ and } t_k < t_s$$




- Provable stability: boundedness of the closed-loop state in $\Omega_\rho$ ($\Omega_{\rho_e} \subset \Omega_\rho$)
- Provable feasibility: $h(x)$ meets all state and input constraints

# LYAPUNOV-BASED ECONOMIC MPC

## Convergence to the Steady-State (Mode 2)

$$\min_{u(\cdot)\in S(\Delta)} \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(\tau), u(\tau))\, d\tau$$

s.t.

$$\dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0)$$

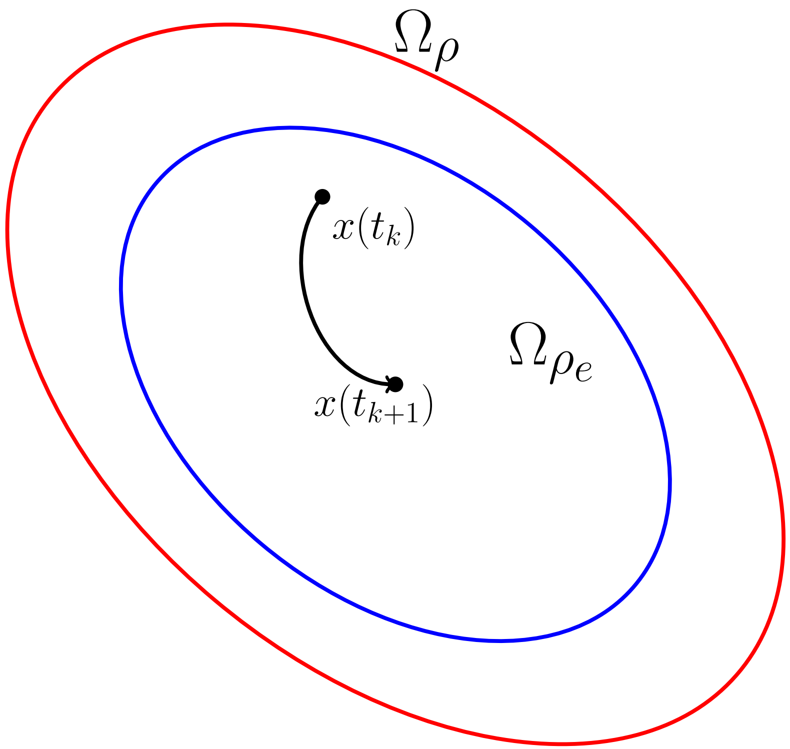
$$\tilde{x}(t_k) = x(t_k)$$

$$u(t) \in U,\ \tilde{x}(t) \in X,\ \forall\, t \in [t_k, t_{k+N})$$

$$|u_i(t_j) - h_i(\tilde{x}(t_j))| \leq \epsilon_r,\ i = 1, \ldots, m,$$
$$j = k, \ldots, k+N-1$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0)$$

if $V(x(t_k)) > \rho_e$ or $t_k \geq t_s$




- Compute control actions that decrease the Lyapunov function
- Provable stability: convergence to a small neighborhood of the steady-state

# CYBERSECURITY AND PROCESS CONTROL SYSTEMS

- Cyberattacks on control systems seek to impact a physical process and can impact safety, profit, and production rates (A.A. Cárdenas *et al.*, *ASIACCS*, 2011)
- Do cyberattackers care about attacking control and manufacturing systems?
  - ◇ 2010: Stuxnet (trellix.com)
    - ▷ Attack on Iranian nuclear facilities
    - ▷ Worm entered systems via USB sticks and spread
    - ▷ Searched for control system software
    - ▷ Ran centrifuges at conditions that cause breakdown
    - ▷ Falsified information to main controller so that there was no indication of a problem
  - ◇ December 2015: Part of Ukraine power grid (K. Zetter, *Wired*, 2016)
    - ▷ Remote manipulation of circuit breakers
    - ▷ Locking real operators out of their accounts
    - ▷ Malicious firmware prevented operators from un-doing attacks
    - ▷ Turned off backup power for operators
    - ▷ Telephone denial of service to prevent operators from finding out about power outages too quickly

# CYBERSECURITY AND PROCESS CONTROL SYSTEMS

- Cyberattacks on control systems seek to impact a physical process and can impact safety, profit, and production rates (A.A. Cárdenas *et al.*, *ASIACCS*, 2011)
- Do cyberattackers care about attacking control and manufacturing systems?
  - ◇ 2017: Triton (M. Giles, *MIT Technology Review*, 2019)
    - ▷ Malware that can prevent safety instrumented systems from activating when needed
    - ▷ Present on a petrochemical plant in Saudi Arabia
    - ▷ Flaw caused safety systems to act up in a way that revealed it before it could cause an incident
  - ◇ 2021: Florida water treatment plant (J. Bergal, *PEW*, 2021)
    - ▷ Remote user changed sodium hydroxide level to be 100 times higher than it should have been
    - ▷ Operator saw this and changed it back
  - ◇ 2021: Colonial Pipeline (W. Turton and K. Mehrotra, *Bloomberg*, 2021)
    - ▷ Ransom note requesting payment appeared on company computer
    - ▷ Company closed down pipeline due to uncertainty as to whether operational technology was compromised

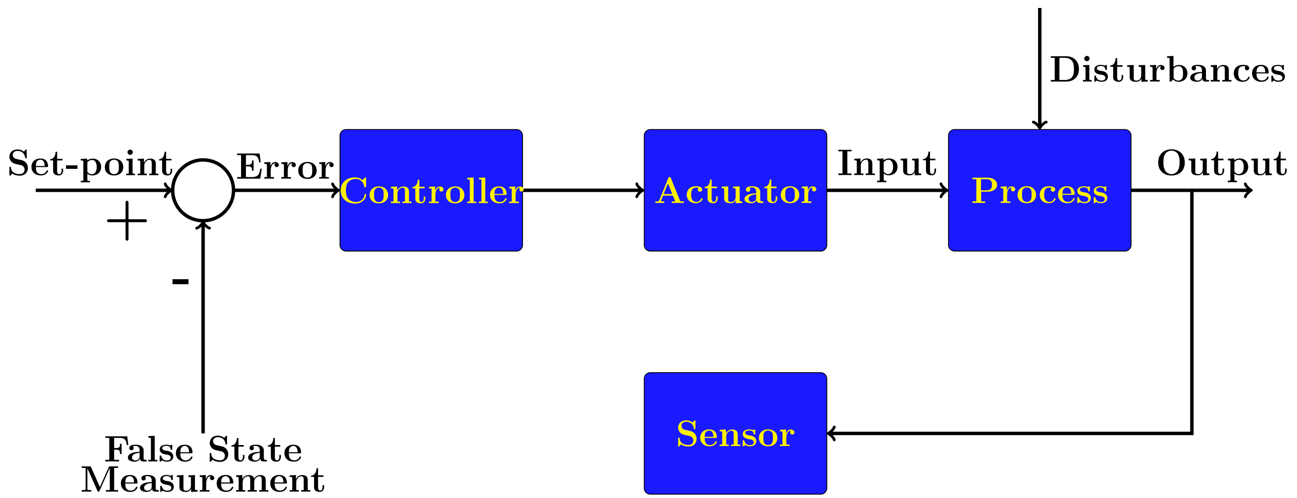
# CYBERATTACK-RESILIENT CHEMICAL PROCESSES

- Examples of attack types: (N. Tuptuk and S. Hailes, *Journal of Manufacturing Systems*, 2018)
  - ◇ Denial of Service: Preventing parts of a network from delivering to others
  - ◇ Eavesdropping: Attackers quietly learn about the system to prepare for more active attacks
  - ◇ False data injection
  - ◇ Time delay attack: Delay occurs in measurements or control actions
  - ◇ Data tampering attack: Data can be altered in storage or transmittal
  - ◇ Replay attack: Correct information from before is sent again
- Cyberattacks on feedback controllers are problematic because they remove associations between state measurements and inputs
  - ◇ Undesired inputs $u \in U$ can be applied at a given state
  - ◇ Defies standard notions of feedback control
- Desirable to understand how elements of a control loop can contribute to detection and handling of attacks
  - ◇ Goal: Understand how and whether control theory-based cyberattack-handling can aid in providing security with flexibility for next-generation manufacturing

# CYBERATTACK-RESILIENT CHEMICAL PROCESSES: A NONLINEAR SYSTEMS DEFINITION

(H. Durand, *Mathematics*, 2018)

- Physical damage from attacks can come from manipulating actuators in a rogue manner (directly or indirectly)
- Focus on sensor and actuator attacks individually to build toward handling both at once
- Cyberattack-resilience for state measurement falsification requires:
  - ◇ There exist no possible input policies given the controllers used and their implementation strategies such that $x(t) \notin X$, for any allowable initial state $x_0 \in \bar{X}$ and $w(t) \in W$, $t \in [0, \infty)$

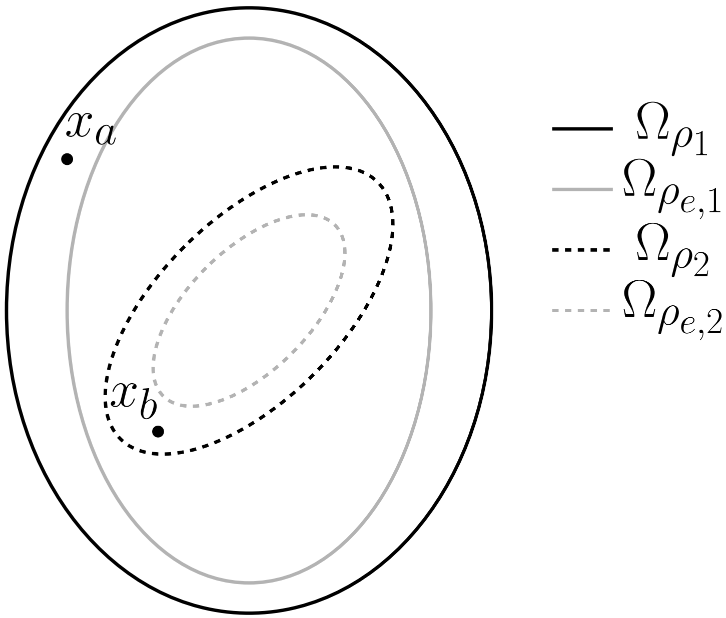


# DISCOVERING PROPERTIES OF CYBERATTACK-RESILIENT PROCESS CONTROL DESIGNS

- The definition of cyberattack-resilient control design is non-constructive
- Developing cyberattack-resilient control strategies will require a better understanding of which designs do and do not work and why
- Explore 2 ideas for cyberattack-resilient controllers:
  - ◇ Controller implementation incorporating randomness
  - ◇ Integrating feedback control/open-loop control
- Conclusions:
  - ◇ Nonlinear systems definition of cyberattack-resilience must be met
    - ▷ Hoping the attacker lacks knowledge about the control design is insufficient
  - ◇ Other techniques (e.g., process design perspectives or techniques which combine control with detection) should be investigated

# CONTROLLER IMPLEMENTATION INCORPORATING RANDOMNESS

- Attacks may be designed by reverse engineering known control laws
  - ◇ Suggests that randomly selecting the controller to be used at a given sampling time may make cyberattack design more difficult
  - ◇ Randomness in control design can only be considered if closed-loop stability is maintained under normal operation
    - ▷ Closed-loop stability and feasibility guarantees can be made with a randomized LEMPC implementation strategy
    - ▷ Cyberattack-resiliency is not guaranteed




- Implementation strategy:
  - ◇ Develop $n_p$ LEMPC's and $h_1(x)$
  - ◇ At each $t_k$, randomly select one of the controllers until one is found for which:
    - ▷ $x(t_k) \in \Omega_{\rho_i}$, $i = 1, \ldots, n_p$, for the $n_p - th$ LEMPC
    - ▷ $x(t_k) \in \Omega_{\rho_1}$ for $h_1(x)$

# CHEMICAL PROCESS EXAMPLE

## Process Description

- Continuous stirred tank reactor (CSTR) with second-order, exothermic, irreversible reaction of the form $A \rightarrow B$:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2$$
$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V}$$

- Control objective: regulate the process in an economically optimal time-varying fashion while maintaining closed-loop stability

  ◇ Economic cost:

$$\int_{t_k}^{t_{k+N}} [k_0 e^{-\frac{E}{RT(\tau)}} C_A(\tau)^2] d\tau$$

  ◇ Manipulated input constraints

$$0.5 \leq C_{A0} \leq 7.5 \text{ kmol/m}^3 \qquad -5.0 \times 10^5 \leq Q \leq 5.0 \times 10^5 \text{ kJ / h}$$

  ◇ Deviation variables:

$$x_1 = C_A - C_{As}, \quad x_2 = T - T_s$$

  ◇ Process model in input-affine form $\dot{x} = \tilde{f}(x) + gu$

# CHEMICAL PROCESS EXAMPLE

## Lyapunov-Based Controller Design

- Lyapunov-based controller for the inlet concentration: $h_{1,1}(x) = 0\ \text{kmol/m}^3$
  - ◇ Lyapunov-based controller for the heat rate input:
    - ▷ Sontag's Formula (Y. Lin and E.D. Sontag, *SCL*, 1991)

$$h_{2,1}(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V_1 + \sqrt{L_{\tilde{f}}V_1^2 + L_{g_2}V_1^4}}{L_{g_2}V_1}, & \text{if } L_{g_2}V_1 \neq 0 \\ 0, & \text{if } L_{g_2}V_1 = 0 \end{cases}$$

  - ◇ A quadratic Lyapunov function of the form $V_1(x) = x^T P x$ with:

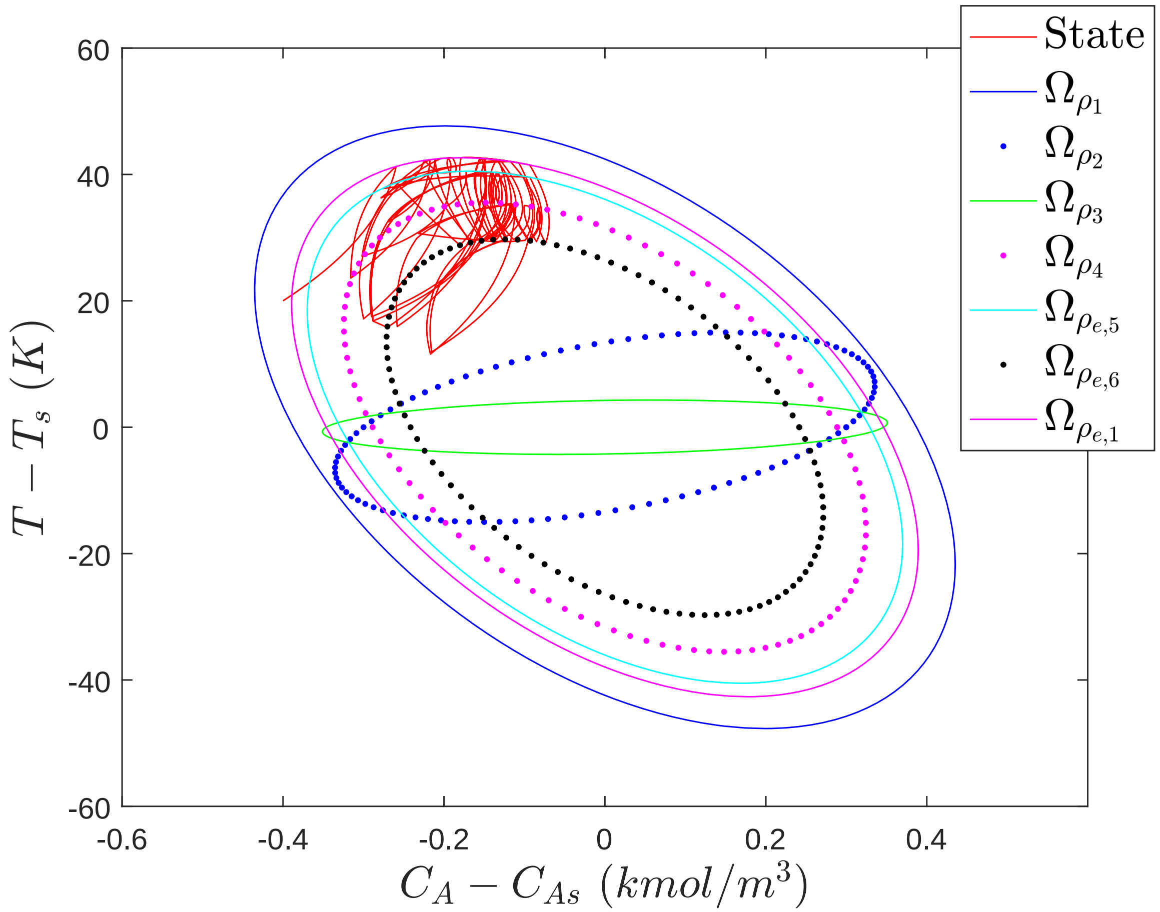
$$P = \begin{bmatrix} 1200 & 5 \\ 5 & 0.1 \end{bmatrix}$$

  - ◇ Stability region $\rho_1 = 180$ (i.e., $\Omega_{\rho_1} = \{x \in R^2 : V_1(x) \leq \rho_1\}$)
- Process state initialized at $x_{init} = [-0.4\ \text{kmol/m}^3\ 20\ \text{K}]^T$
- LEMPC parameters: $N = 10$, $\Delta = 0.01$ h
- Process simulated with an integration step size of $10^{-4}$ h

# CHEMICAL PROCESS EXAMPLE

## Randomized LEMPC Development

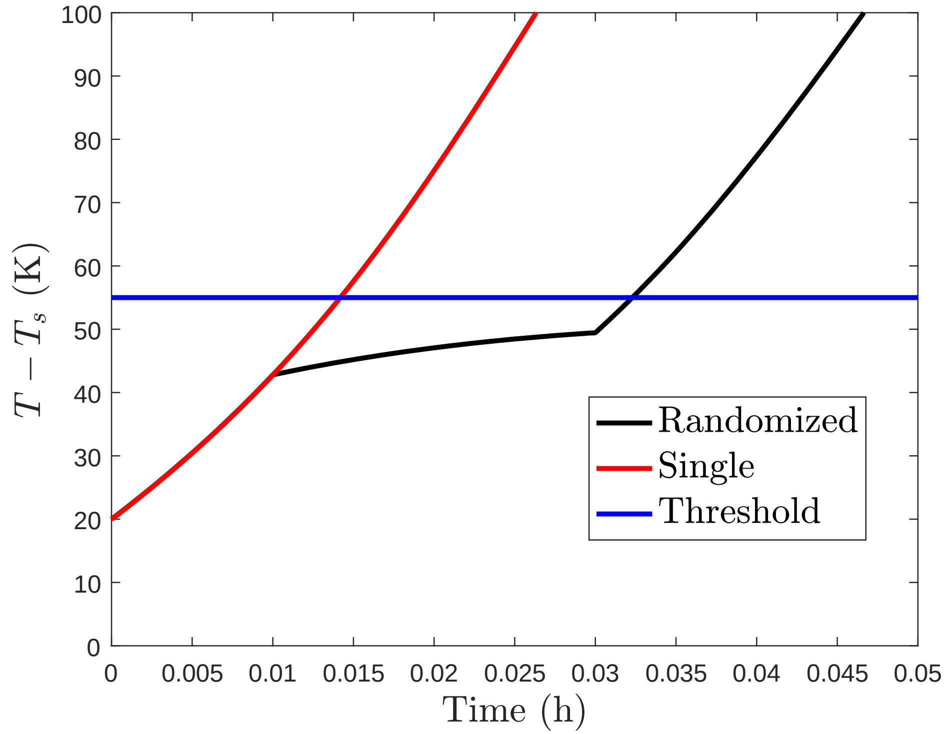
- 6 LEMPC's were designed
  - ◇ $\Omega_{\rho_i} \subseteq \Omega_{\rho_1},\ i = 1, \ldots, 6$
  - ◇ $h_{i,1} = 0$ kmol/m$^3$
  - ◇ $h_{i,2}$ designed via Sontag's control law
  - ◇ Closed-loop state is maintained within $\Omega_{\rho_1}$ throughout 1 h of operation in the absence of a cyberattack



# CHEMICAL PROCESS EXAMPLE

## Randomized LEMPC and LEMPC Under a Cyberattack

- Cyberattack with $x_f = [-0.0521 \text{ kmol/m}^3 \; -8.3934 \text{ K}]^T$ is applied to a single LEMPC and the randomized LEMPC implementation strategy
- Randomized LEMPC results depend on seed to random number generator
- Randomized LEMPC barely delayed the time until $x_2 > 55$ K compared to the single LEMPC (0.0142 h)




| Seed | Time $x_2 > 55$ (h) |
|---|---|
| 5 | 0.0231 |
| 10 | 0.0144 |
| 15 | 0.0142 |
| 20 | 0.0323 |
| 25 | 0.0247 |
| 30 | 0.0142 |
| 35 | 0.0142 |
| 40 | 0.0146 |
| 45 | 0.0247 |
| 50 | 0.0142 |

# INTEGRATING FEEDBACK CONTROL/OPEN-LOOP CONTROL

- Randomized LEMPC implementation strategy could not guarantee that no problematic inputs could be applied over time (even for steady-state tracking)
- Cyberattack resilience against state measurement falsification could be achieved for systems with an open-loop stable steady-state
  - ◇ Applying the steady-state input $u_s$ bypasses the issues with cyberattacks on feedback and drives the closed-loop state to the origin
  - ◇ Loses benefits of feedback control
- Cyberattack-resilience definition must be met
- Three concepts for utilizing LEMPC to attempt to detect attacks were explored (H. Durand and M. Wegener, *Mathematics*, 2020; H. Oyama and H. Durand, *AIChE J.*, 2020)
  - ◇ LEMPC with random control law modifications to probe for cyberattacks
  - ◇ State feedback LEMPC with an attack detection strategy based on state predictions at each sampling time
  - ◇ Output feedback LEMPC (M. Ellis, J. Zhang, J. Liu and P. D. Christofides, *SCL*, 2014; L. Lao, M. Ellis, H. Durand and P. D. Christofides, *AIChE J.*, 2015) with an attack detection strategy based on redundant state estimators

# OBSERVABILITY ASSUMPTION

- $M$ sets of measurements are continuously available:

$$y_i(t) = k_i(x(t)) + v_i(t)$$

  - ◇ $k_i$ is vector-valued function, and $v_i$ represents the measurement noise associated with the measurements $y_i$
  - ◇ $v_i \in V_i \subset \mathbb{R}_i^q$ $(|v_i| \leq \theta_{v,i})$, $i = 1, \dots, M$

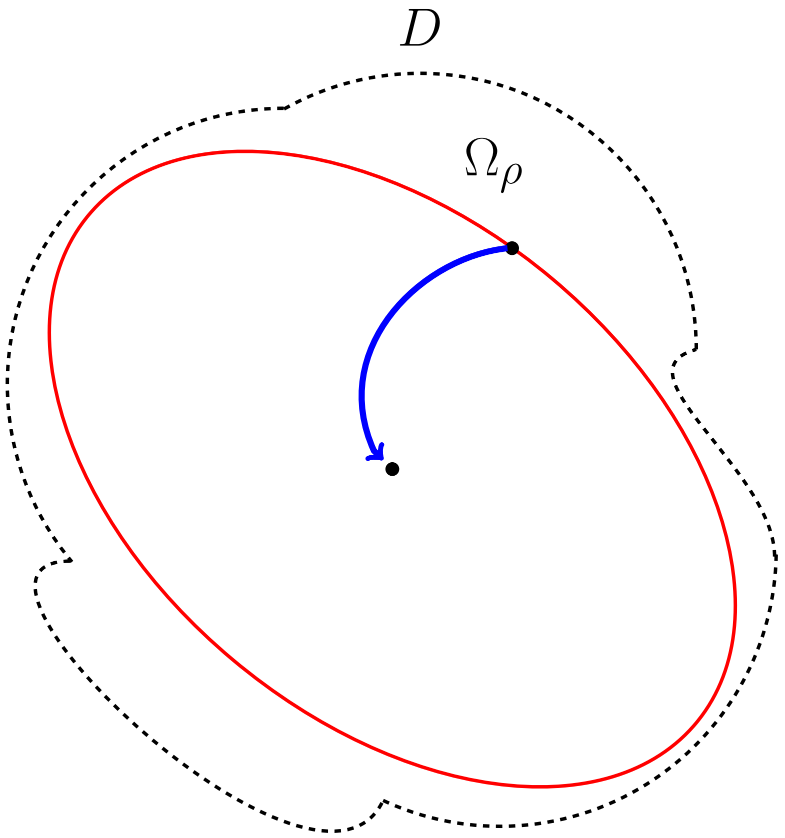
- A deterministic observer exists for each of the $M$ sets of measurements:

$$\dot{z}_i = F_i(\epsilon_i, z_i, y_i)$$

  - ◇ Observer estimate $z_i$; $\epsilon_i > 0$

- Assumptions:
  - ◇ For an initial state estimate with sufficiently low error between $z_i$ and $x$, $h(z_i)$ maintains the closed-loop state in $\Omega_\rho$
  - ◇ There exists a time $t_{bi}$ such that:

$$|z_i(t) - x(t)| \leq \epsilon_{mi}$$



# CYBERATTACK-RESILIENT OUTPUT FEEDBACK LEMPC

- Cyberattacks on state measurements could impact the state estimate used by the LEMPC
- If the estimate is sufficiently incorrect, the closed-loop state may exit $\Omega_\rho$
- Estimator properties suggest an attack detection methodology
  - $|z_i(t) - x(t)| \leq \max\{e_{mi}\}$, $i = 1, \ldots, M$
  - Implies $|z_i(t) - z_j(t)| \leq \epsilon_{\max}$, $i, j = 1, \ldots, M$, when no attack occurs
  - Condition can be used with redundant estimators to attempt to flag falsified sensor measurements

$$
\begin{aligned}
\min_{u(t) \in S(\Delta)} \quad & \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(\tau), u(\tau))\, d\tau \\
\text{s.t.} \quad & \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t)) \\
& \tilde{x}(t_k) = z_1(t_k) \\
& \tilde{x}(t) \in X, \; \forall\, t \in [t_k, t_{k+N}) \\
& u(t) \in U, \;\; \forall\, t \in [t_k, t_{k+N}) \\
& V(\tilde{x}(t)) \leq \rho_{e,1}, \;\; \forall\, t \in [t_k, t_{k+N}), \\
& \qquad \text{if } \tilde{x}(t_k) \in \Omega_{\rho_{e,1}} \\
& \frac{\partial V(\tilde{x}(t_k))}{\partial x} (f(\tilde{x}(t_k), u(t_k))) \\
& \leq \frac{\partial V(\tilde{x}(t_k))}{\partial x} (f(\tilde{x}(t_k), h(x(t_k)))) \\
& \quad \text{if } \tilde{x}(t_k) \in \Omega_\rho / \Omega_{\rho_{e,1}}
\end{aligned}
$$

# CYBERATTACK-RESILIENT OUTPUT FEEDBACK LEMPC

- Consider that at least one state estimate is not impacted by an attacker
- If $|z_i(t) - z_j(t)| > \epsilon_{\max}$, $i, j = 1, \ldots, M$, flag an attack
- If $|z_i(t) - z_j(t)| \leq \epsilon_{\max}$, $i, j = 1, \ldots, M$, but an attack occurred:
  - ◇ Closed-loop state will be maintained in $\Omega_\rho$ over the subsequent sampling period under sufficient conditions
    - ▷ Examples: sufficiently small $\rho_{e,1}$, $\theta$, and $\Delta$

$$
\begin{aligned}
\min_{u(t) \in S(\Delta)} \quad & \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(\tau), u(\tau))\, d\tau \\
\text{s.t.} \quad & \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t)) \\
& \tilde{x}(t_k) = z_1(t_k) \\
& \tilde{x}(t) \in X, \forall\, t \in [t_k, t_{k+N}) \\
& u(t) \in U, \ \forall\, t \in [t_k, t_{k+N}) \\
& V(\tilde{x}(t)) \leq \rho_{e,1}, \ \ \forall\, t \in [t_k, t_{k+N}), \\
& \qquad \text{if } \tilde{x}(t_k) \ \in \ \Omega_{\rho_{e,1}} \\
& \frac{\partial V(\tilde{x}(t_k))}{\partial x}(f(\tilde{x}(t_k), u(t_k))) \\
& \leq \frac{\partial V(\tilde{x}(t_k))}{\partial x} \ (f(\tilde{x}(t_k), h(x(t_k)))) \\
& \ \text{if } \ \tilde{x}(t_k) \in \Omega_\rho / \Omega_{\rho_{e,1}}
\end{aligned}
$$

# MOTIVATION FOR HANDLING SIMULTANEOUS ACTUATOR AND SENSOR ATTACKS

- Continuous stirred tank reactor (CSTR) with second-order $A \rightarrow B$ reaction:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2$$
$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V}$$

- Control objective: Optimize process economics while maintaining the closed-loop state in $\Omega_{\rho_1}$

  - ◇ Economic cost:

$$\int_{t_k}^{t_{k+N}} [k_0 e^{-\frac{E}{RT(\tau)}} C_A(\tau)^2] d\tau$$

  - ◇ Manipulated input constraint

$$0.5 \leq C_{A0} \leq 7.5 \text{ kmol/m}^3$$

  - ◇ Deviation variables:

$$x_1 = C_A - C_{As}, \quad x_2 = T - T_s$$

  - ◇ Process model in input-affine form $\dot{x} = \tilde{f}(x) + gu$

# MOTIVATION FOR HANDLING SIMULTANEOUS ACTUATOR AND SENSOR ATTACKS

- Lyapunov-based controller: $h(x) = -1.6x_1 - 0.01x_2$ (M. Heidarinejad, J. Liu, and P. D. Christofides, *SCL*, 2012)
  - ◇ A quadratic Lyapunov function of the form $V_1(x) = x^T P x$ with:

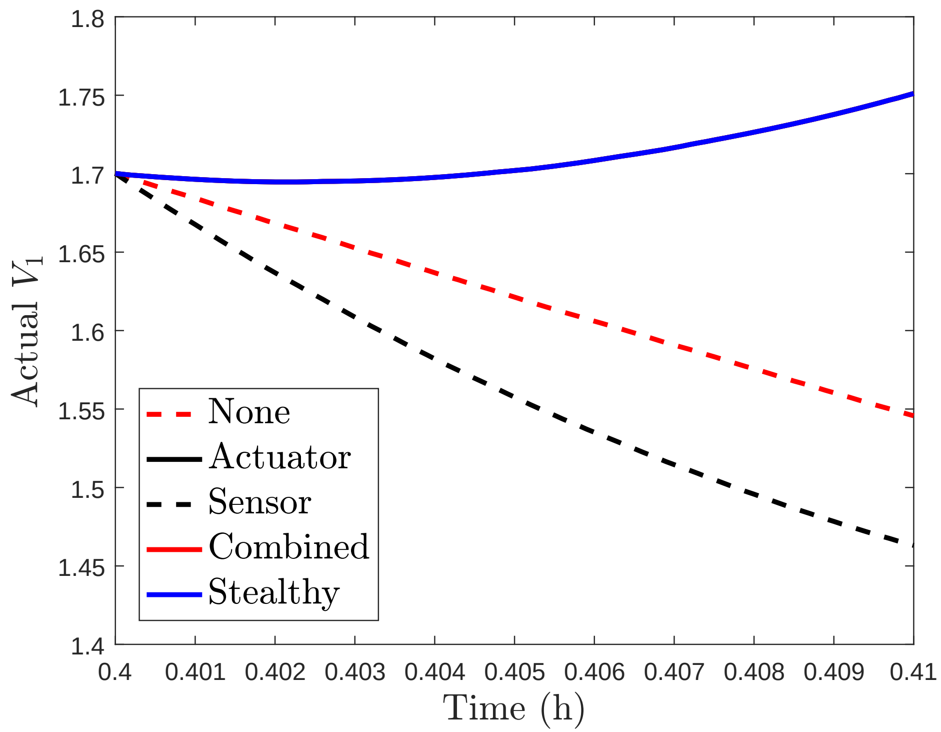
$$P = \begin{bmatrix} 110.11 & 0 \\ 0 & 0.12 \end{bmatrix}$$

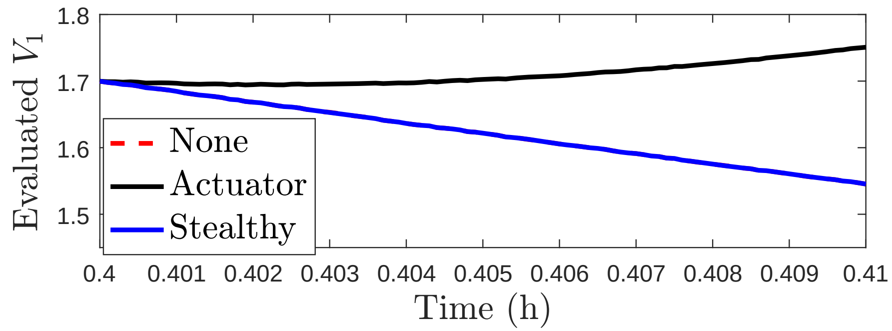
  - ◇ Stability region $\rho_1 = 440$ (i.e., $\Omega_{\rho_1} = \{x \in R^2 : V(x) \leq \rho_1\}$)
  - ◇ $\Omega_{\rho_{e_1}} \subset \Omega_\rho$, $\rho_{e_1} = 330$
- LEMPC parameters: $N = 10$, $\Delta = 0.01$ h
- Process simulated with an integration step size of $10^{-3}$ h
- The LEMPC receives full state feedback with the full system state $x = [x_1 \; x_2]^T$
- Attack detection policy (initialized at 0.4 h when attack begins): Check if Lyapunov function evaluated at the state measurement decreases over $\Delta$

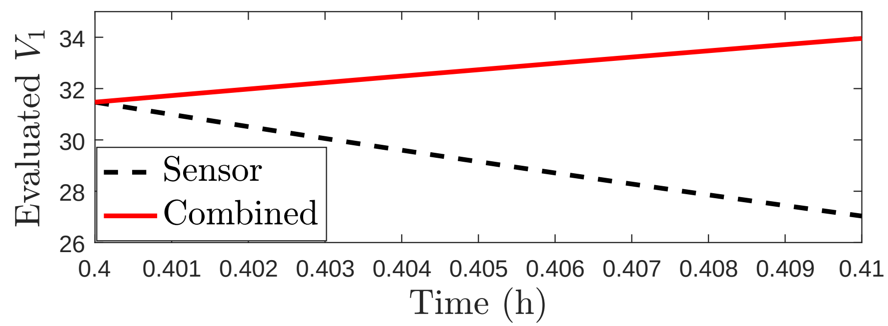
# VARIOUS ATTACK POLICIES

(H. Oyama, D. Messina, K. K. Rangan, and H. Durand, *Frontiers in Chemical Engineering*, 2022)

- Actuator attack ($u = 0.5$ kmol/m$^3$): Discoverable
- False sensor measurement ($x_1 + 0.5$ kmol/m$^3$): Not discoverable (no safety issue)
- Combined actuator and sensor attack: Discoverable
- Stealthy actuator and sensor attack (sensor measurements follow trajectory they should have taken): Not discoverable
  - ◇ State moves closer to safe operating region boundary



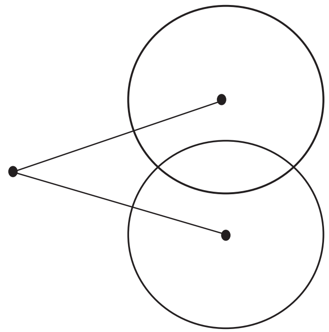
# PREVENTING SAFETY ISSUES DURING SIMULTANEOUS ATTACKS

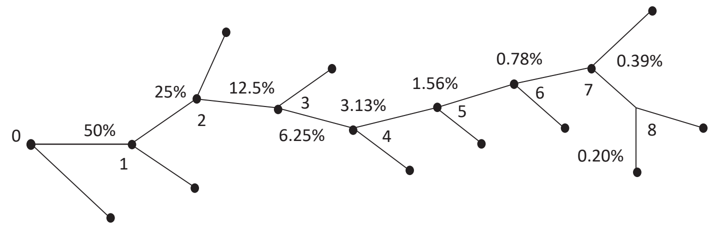
- Multiple detector types can be used to aid in cornering an attacker
  - Examples:
    - Redundant estimators and forcing the decrease of the Lyapunov function across a sampling period
    - Redundant estimators and state predictions with a redundant control law
  - Resilient under sufficient conditions
    - Closed-loop state cannot leave a safe operating region in the presence of individual or simultaneous attacks before attack detection
    - Potentially challenging to obtain reasonable control law parameters satisfying resilience theory
- Fundamental notion of cyberattack discoverability:
  - Whether it is possible to distinguish between a state trajectory coming from attacked sensors and/or actuators and the actual
  - Integrated control and detection policies attempt to use the controller to force differences to show themselves

# EXAMPLE OF DISCOVERABILITY-INSPIRED CYBERATTACK DETECTION

(H. Oyama et al., *Digital Chemical Engineering*, 2023)

- Need a strategy for detecting attacks on sensors that might flag them even with all sensors being compromised
- Set up expectations for measurements that would be "hard" to fake
  - ◇ At every sampling time, two control actions are available
  - ◇ Should result in non-overlapping potential sets of measured states
  - ◇ One of the two is randomly selected
- Random selection many times in a row
  - ◇ May make it challenging to predict how to not get "caught"

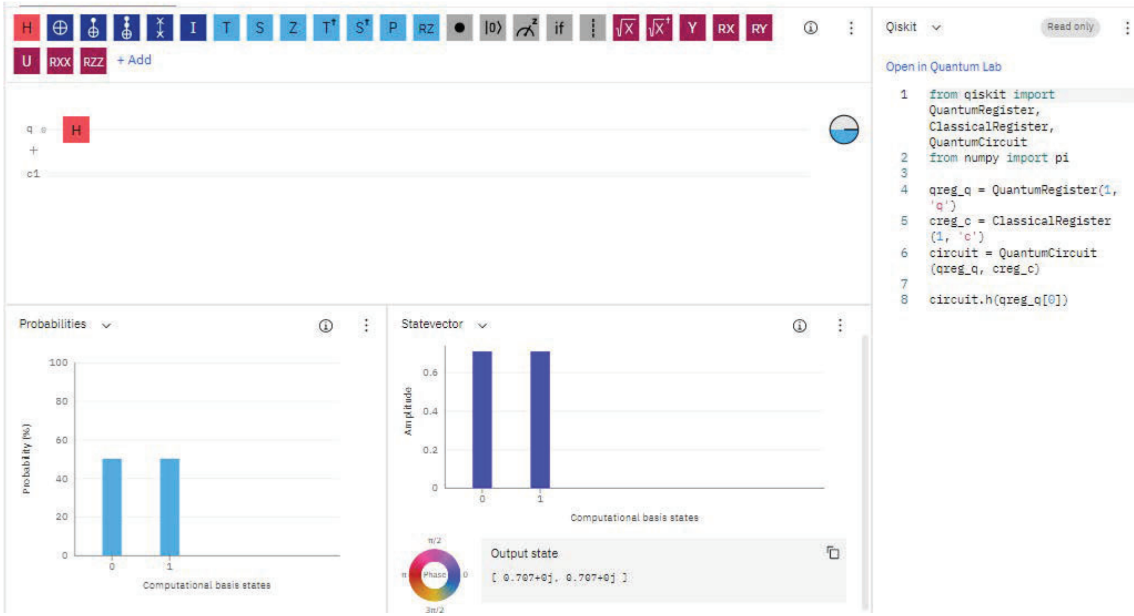




# IMPLEMENTING CONTROL ON QUANTUM COMPUTERS

## Quantum Computing

- Quantum computing is a technology of recent interest in chemical engineering (D.E Bernal et al., AIChE J., 2022)
- Quantum computers exist today of different types




- Quantum annealing
  - ◇ Hardware designed to solve certain optimization problems
- Gate-based computers
  - ◇ Considered a path toward "universal" computation

# QUANTUM MECHANICS FOR QUANTUM COMPUTING VS. CHEMISTRY

- Reminders from chemistry:
  - "Time-independent Schrödinger equation" (eigenvalue-eigenvector relationship)
  $$\hat{H}(x,t)\psi(x,t) = E\psi(x,t)$$
  - Time-dependent Schrödinger equation
  $$\hat{H}(x,t)\psi(x,t) = i\hbar\frac{\partial\psi(x,t)}{\partial t}$$
- $\hat{H}(x,t)$: Hamiltonian (total energy operator)
- Energy $E$
- $\hbar$: Reduced Planck constant
- $\psi(x,t)$: Wavefunction of the quantum system
  - Contains information about position of a quantum system
  - Example: $\psi(x,t)$ is the wavefunction of an electron
    - $\psi(x_0,t_0)^*\psi(x_0,t_0)dx$ conveys the probability that the quantum particle will be found in a spatial interval with width $dx$ around $x_0$ at time $t_0$ (T. Engel, *Prentice Hall*, 2010)

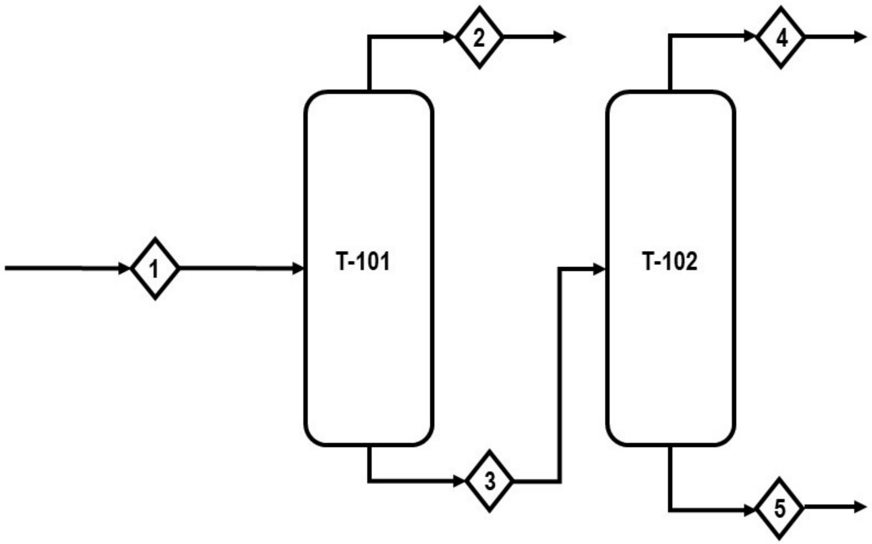
# QUANTUM MECHANICS FOR QUANTUM COMPUTING VS. CHEMISTRY

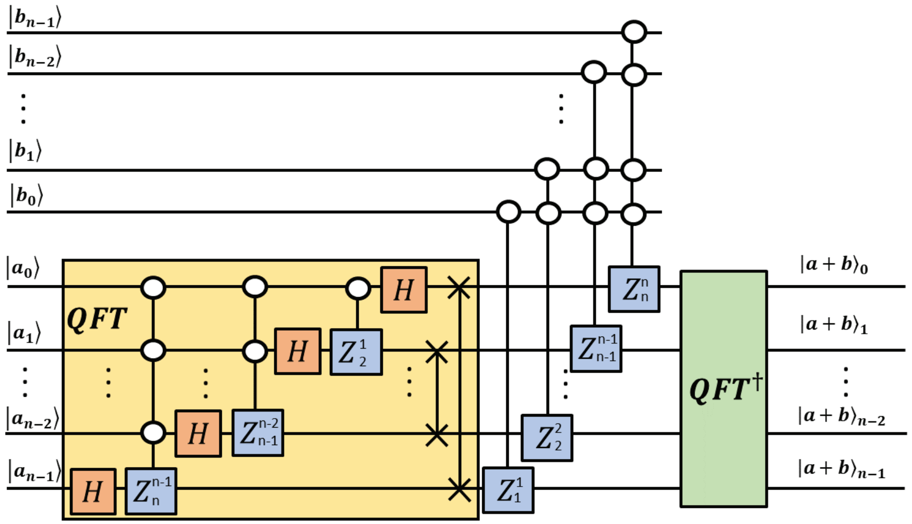
- Wavefunctions are derived from a more fundamental notion of "quantum states"
  - ◇ "Time-independent Schrödinger equation" (eigenvalue-eigenvector relationship)
$$\bar{H}(t)\left|\Psi(t)\right\rangle = E\left|\Psi(t)\right\rangle$$
  - ◇ Time-dependent Schrödinger equation
$$\bar{H}(t)\left|\Psi(t)\right\rangle = i\hbar\frac{\partial\left|\Psi(t)\right\rangle}{\partial t}$$
- $\left|\Psi(t)\right\rangle$ is the "quantum state"
  - ◇ "Dirac notation"
- Wavefunctions are derived from the quantum state in a way that makes them particularly good for representing information about position
- Position is continuous
- Gate-based quantum computers generally stay with the binary concept of classical computing
  - ◇ We only want to have 2 possible quantum states for the system
  - ◇ Position will not work for this

# QUANTUM MECHANICS FOR QUANTUM COMPUTING VS. CHEMISTRY

- Wavefunctions are derived from a more fundamental notion of "quantum states"
  - ◇ "Time-independent Schrödinger equation" (eigenvalue-eigenvector relationship)
  $$\bar{H}(t)\,|\Psi(t)\rangle = E\,|\Psi(t)\rangle$$
  - ◇ Time-dependent Schrödinger equation
  $$\bar{H}(t)\,|\Psi(t)\rangle = i\hbar\frac{\partial\,|\Psi(t)\rangle}{\partial t}$$
- $|\Psi(t)\rangle$ is the "quantum state"
  - ◇ "Dirac notation"
- Wavefunctions are derived from the quantum state in a way that makes them particularly good for representing information about position
- Position is continuous
- Gate-based quantum computers generally stay with the binary concept of classical computing
  - ◇ Wavefunctions are not used in quantum computing
  - ◇ Two possible quantum states: $|0\rangle$ and $|1\rangle$ (regardless of actual implementation)

# CONCEPTUALIZING QUANTUM CIRCUITS

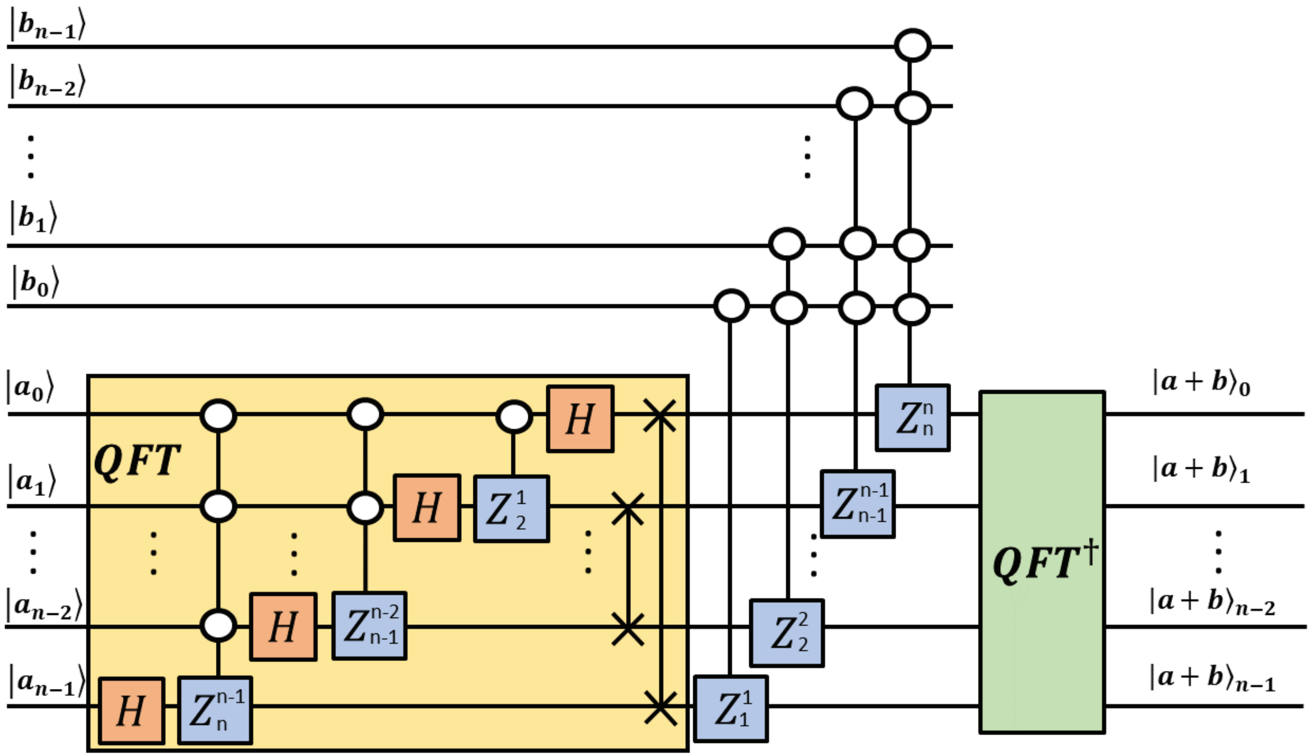



- Each unit of a chemical plant changes the state of a process stream
  - ◇ Symbols and labeling for process units create meaning for chemical engineers regarding the expected state changes
- Each block ("gate") in a quantum circuit changes the state of a quantum system
  - ◇ Symbols and labeling for the gates create meaning regarding the expected state changes
  - ◇ Example: *H* gate puts a qubit in an equal superposition of two states

# QFT-BASED ADDITION

(Ruiz-Perez, L., Garcia-Escartin, J.C., *Quantum Information Processing*, 2017)

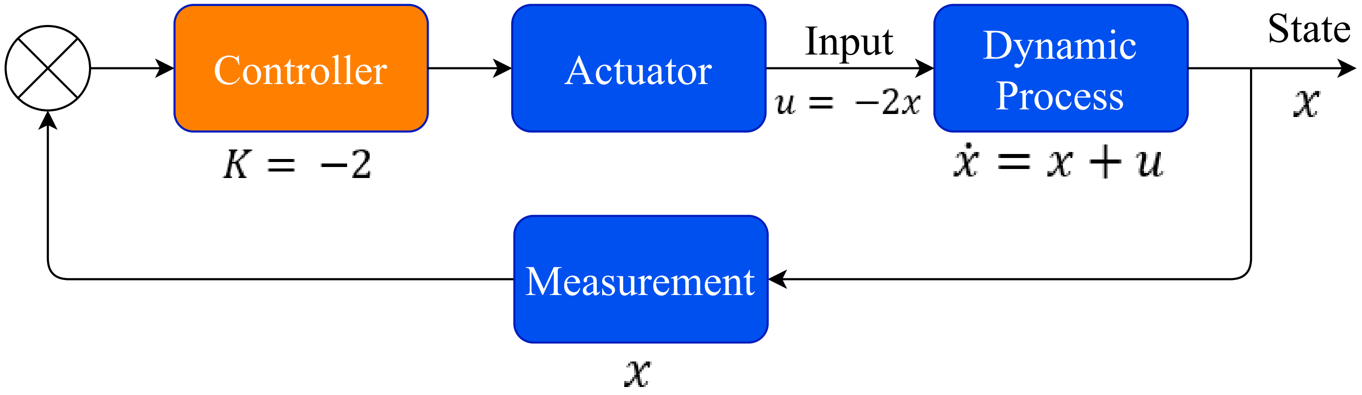



- QFT-based addition: Add two integers $a$ and $b$ (S. Anagolum, Github)
- Binary representations of both numbers are translated to qubit states
- Quantum gates are applied (including those in the inverse QFT, QFT$^\dagger$) to obtain final qubit states representative of the bits of the sum

# QUANTUM COMPUTING-IMPLEMENTED CONTROL EXAMPLE

## Motivation

(K. K. Rangan *et al.*, *DYCOPS*, 2022; K. Nieman, K. K. Rangan, and H. Durand, *IECR*, 2022)

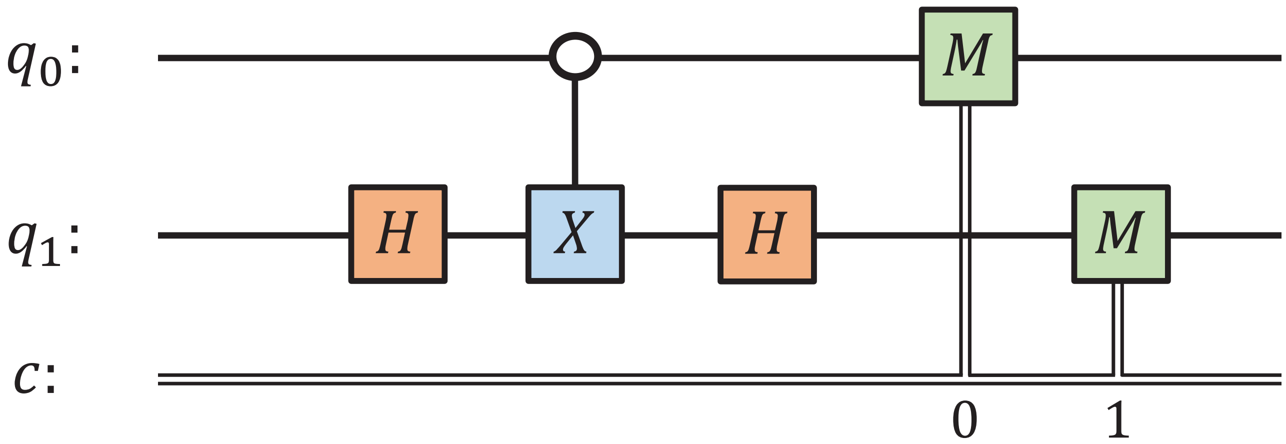



- Today's quantum computers are noisy
  - ◇ Can cause results of a series of gates to be non-deterministic in practice even if it should be deterministic in theory
- If control was implemented on today's quantum computers, noise could make applied inputs non-deterministic for deterministic process behavior
  - ◇ Raises question of when control could be implemented on quantum computers
- Initial study of these effects: a linear dynamic process, $\dot{x} = x + u$, classically stabilized using the control law $u = -2x$

# QUANTUM COMPUTING-IMPLEMENTED CONTROL EXAMPLE

## Noise Model

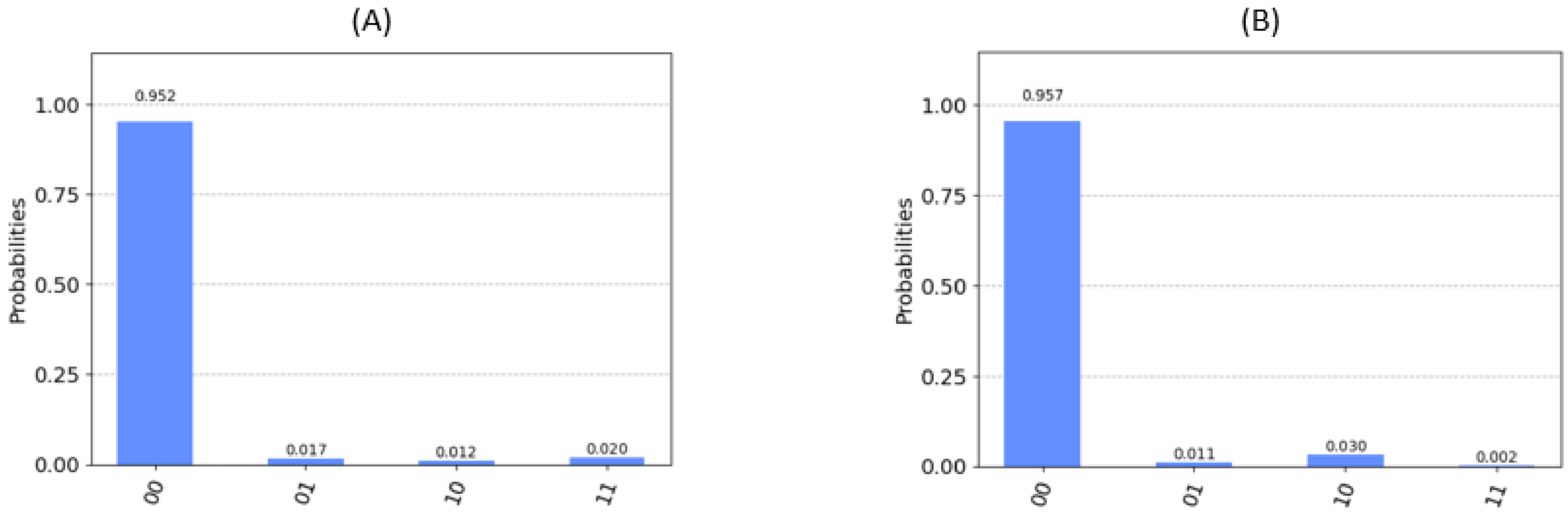
(Garcia-Escartin, J.C., Chamorro-Posada, P., *arXiv*, 2011)




- $u = -2x$ is evaluated using a quantum simulator (qasm_simulator) accessed via Qiskit
  - ◇ Use QFT-based addition to compute $u = -2x$ from $x + x$
- Quantum simulator does not inherently have noise
  - ◇ Required to select a noise model
  - ◇ Evaluated using a controlled $Z$ gate implementation (2 $H$ gates and CNOT gate) as a special case of a controlled phase rotation $Z_k$

# QUANTUM COMPUTING-IMPLEMENTED CONTROL EXAMPLE

## Noise Models

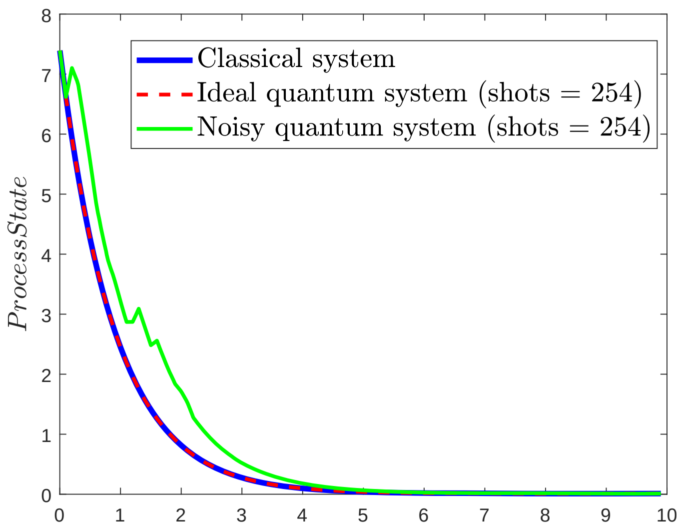


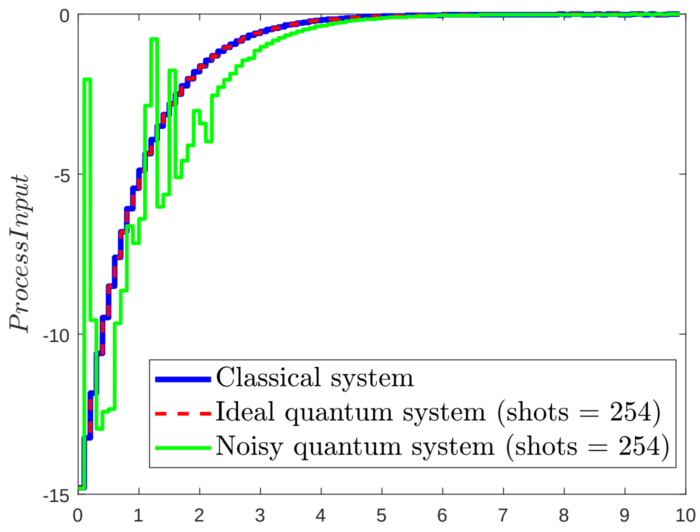

- A depolarizing error parameter for qasm_simulator was selected using command for modeling the noise from the 5-qubit quantum device, ibmq_manila, on the qasm_simulator
  - ◇ The controlled $Z$ gate was simulated with both the qasm_simulator using this noise model from the device backend and with the depolarizing error parameter set to a fixed value on qasm_simulator
- A depolarizing error parameter of 0.05 was determined to sufficiently approximate the results from the simulations based on ibmq_manila

# QUANTUM COMPUTING-IMPLEMENTED CONTROL

## Results

- Comparison between the state trajectories (left) and input trajectories (right) when run with 254 shots for $x(0) = 7.4$
  - ◇ Classical computer (“Classical system”),
  - ◇ Quantum simulator with 254 shots and no noise (“Ideal quantum system”)
  - ◇ Quantum simulator with 254 shots and noise (“Noisy quantum system”)
- Some deviation is observed between the noisy system and the other two, related to the size (in binary) of the state measurement and number of shots

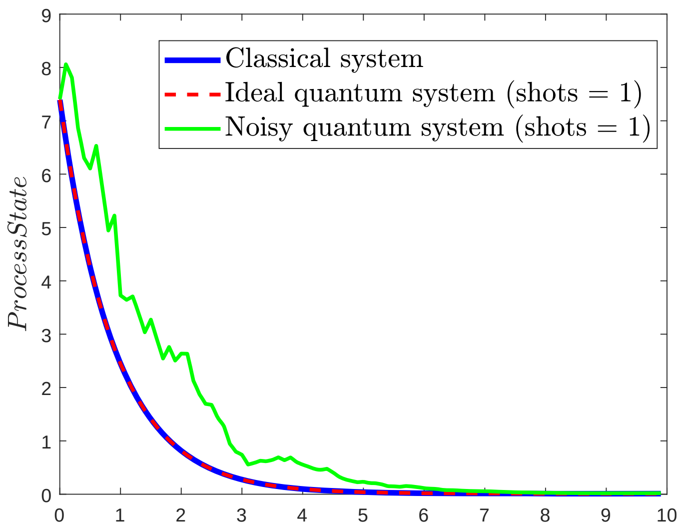


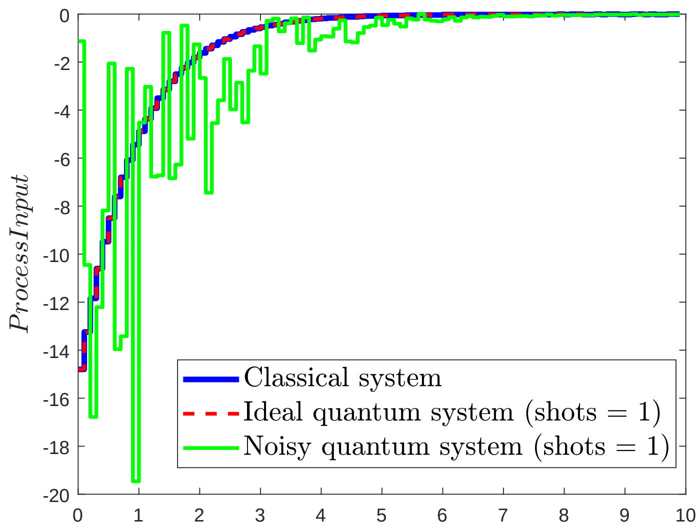



# QUANTUM COMPUTING-IMPLEMENTED CONTROL

## Results

- Comparison between the state trajectories (left) and input trajectories (right) when run with 1 shot for $x(0) = 7.4$
  - ◇ Classical computer ("Classical system"),
  - ◇ Quantum simulator with 1 shot and no noise ("Ideal quantum system")
  - ◇ Quantum simulator with 1 shot and noise ("Noisy quantum system")
- A significant deviation is observed between the noisy system and the other two, related to the size (in binary) of the state measurement and number of shots

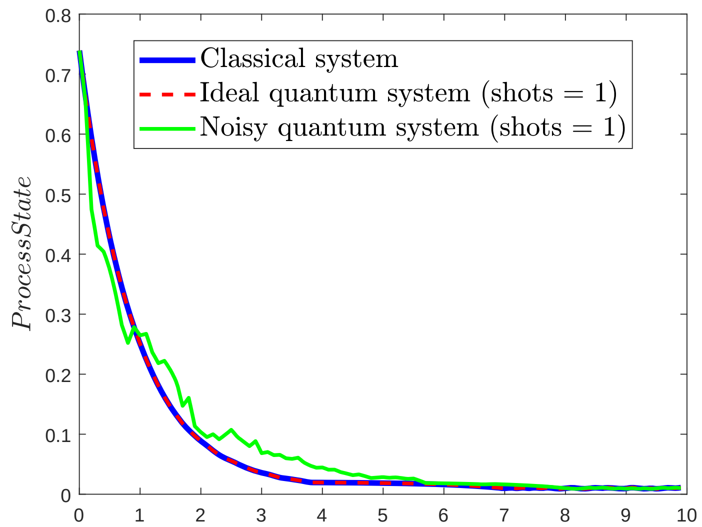


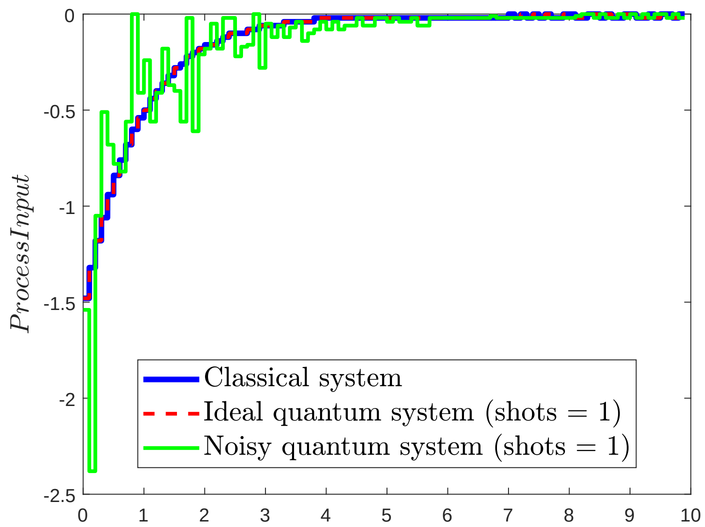



# QUANTUM COMPUTING-IMPLEMENTED CONTROL

## Results

- Comparison between the state trajectories (left) and input trajectories (right) when run with 1 shot for $x(0) = 0.74$
  - ◇ Classical computer ("Classical system"),
  - ◇ Quantum simulator with 1 shot and no noise ("Ideal quantum system")
  - ◇ Quantum simulator with 1 shot and noise ("Noisy quantum system")
- A significant deviation is observed between the noisy system and the other two as a result of the small number of shots

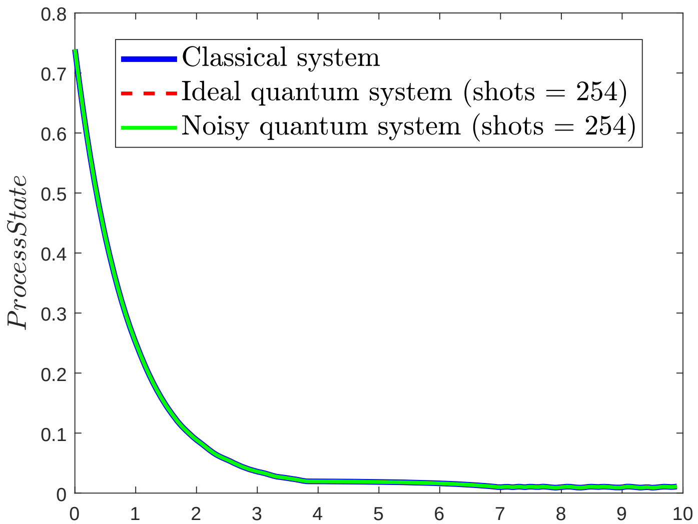


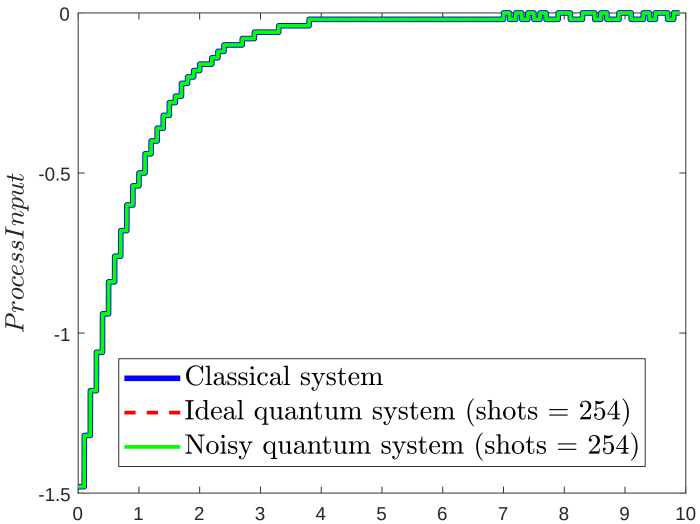



# QUANTUM COMPUTING-IMPLEMENTED CONTROL

## Results

- Comparison between the state trajectories (left) and input trajectories (right) when run with 254 shots for $x(0) = 0.74$
  - ◇ Quantum simulator with 254 shots and noise ("Noisy quantum system")
- No deviation is observed between the noisy system and the other two as a result of the number of shots
- Should we put controllers on quantum computers?
  - ◇ Trying algorithms and evaluating theory to show benefits/limitations



# ADVANCED CONTROL AND QUANTUM COMPUTATION

- Rigorous theory for LEMPC makes it attractive for considering the implications of non-deterministic inputs on stability guarantees
  - ◇ Initial investigations of closed-loop stability of quantum computing-implemented inputs should focus on simple quantum computing algorithms

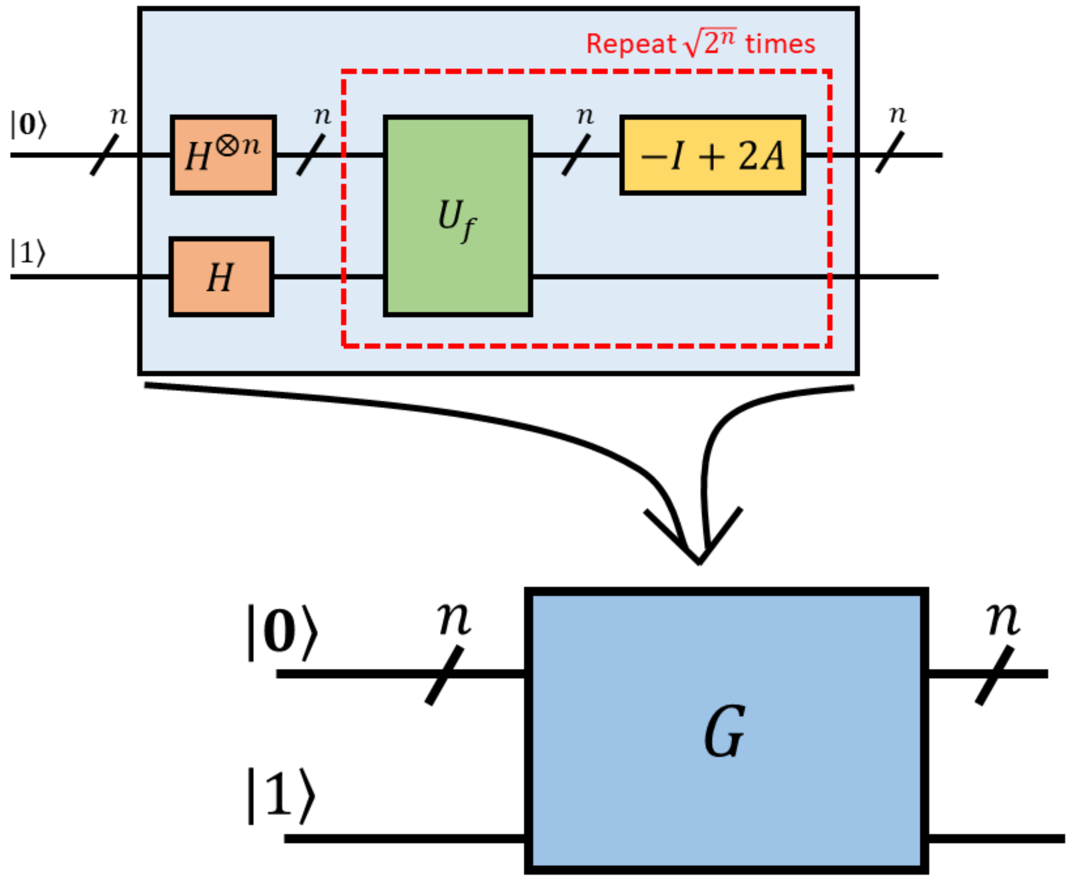
Table 1: LEMPC solution lookup table

| State Measurement | Control Action |
|---|---|
| 0000 | 1111 |
| 0001 | 1110 |
| 0010 | 1010 |
| ⋮ | ⋮ |

- Consider LEMPC solutions in a look-up table
  - ◇ For relating to quantum computing, must express state measurements and inputs in binary
  - ◇ Requires quantization of state measurements for LEMPC
  - ◇ Also quantize control actions output by LEMPC

# SEARCHING AN LEMPC LOOKUP TABLE VIA MODIFIED GROVER'S SEARCH

- Grover's search algorithm is a quantum computing algorithm for searching an unsorted list (Yanofsky and Mannucci, *Cambridge University Press*, 2008)
- A modified version of Grover's algorithm could be used to search the LEMPC lookup table
  - ◇ Not efficient for solving this problem
  - ◇ Show how non-deterministic inputs can be generated by a quantum computing algorithm tied to LEMPC




- Modified Grover's algorithm implementation strategy:
  - ◇ Use a series of controlled Grover blocks to represent the state/input pairings
  - ◇ Measurements return the "correct" input with probability $\lambda$

# IMPLICATIONS FOR CLOSED-LOOP STABILITY

- Probability of obtaining the expected control action from Grover's algorithm: $\lambda$
- Consider $x(t)$ and $\bar{x}(t) \in \Omega_{\rho_e}$
  - ◇ Control action computed by the LEMPC on a classical computer would maintain $x(t_k)$ and $\bar{x}(t_k)$ in $\Omega_\rho$ for $t \in [t_k, t_{k+1})$
  - ◇ The modified Grover algorithm would return the same control action as the classical computer with probability $\lambda$
  - ◇ Conclusion:
    - ▷ $\mathbf{P}(x(t), \bar{x}(t) \in \Omega_\rho \forall\ t \in [t_k, t_{k+1})) \geq \lambda$
- Consider $x(t)$ and $\bar{x}(t) \in \Omega_\rho / \Omega_{\rho_e}$
  - ◇ Control action computed by the LEMPC on a classical computer would maintain $x(t_k)$ and $\bar{x}(t_k)$ in $\Omega_\rho$ for $t \in [t_k, t_{k+1})$
  - ◇ The modified Grover algorithm would return the same control action as the classical computer with probability $\lambda$
  - ◇ Conclusion:
    - ▷ $\mathbf{P}(x(t), \bar{x}(t) \in \Omega_\rho \forall\ t \in [t_k, t_{k+1})) \geq \lambda$

# CONCLUSIONS

- Next-generation manufacturing values flexibility and profitability
  - ◇ Facilitated by automation advances such as economic model predictive control
  - ◇ Flexible and profitable systems may not be secure
    - ▷ Attacks on control systems may undermine process safety
- Integrated detection and control policies geared toward nonlinear systems have potential to enable attacks of various types to be detected before causing safety issues
  - ◇ Requires sufficient control-theoretic conditions
  - ◇ May require at least some sensors to be secure
    - ▷ Handling attacks after detection likely requires some actuators to be secure
- Fundamental notions of cyberattack-resilience and discoverability for nonlinear systems provide insights into potential future directions for securing controllers
- Quantum computing provides another interesting potential direction for the future of next-generation manufacturing
  - ◇ Control theory and practice require further exploration to determine if benefit exists for quantum computing-implemented control

# ACKNOWLEDGEMENTS


- Financial support the National Science Foundation CBET-1839675 and CNS-1932026, the Air Force Office of Scientific Research award number FA9550-19-1-0059, the Wayne State University University Research Grant, Wayne State University Engineering's Research Opportunities for Engineering Undergraduates program, Wayne State Grants Boost funding, and Wayne State University startup funding is gratefully acknowledged.

- Student work presented:
  - ◇ Henrique Oyama, PhD student, Wayne State University
  - ◇ Kip Nieman, PhD student, Wayne State University
  - ◇ Keshav Rangan, PhD student, Wayne State University
  - ◇ Dominic Messina, PhD student, Wayne State University