FAULT-TOLERANT CONTROL OF CHEMICAL PROCESS SYSTEMS USING COMMUNICATION NETWORKS

Nael H. El-Farra, Adiwinata Gani
& Panagiotis D. Christofides

Department of Chemical Engineering
University of California, Los Angeles

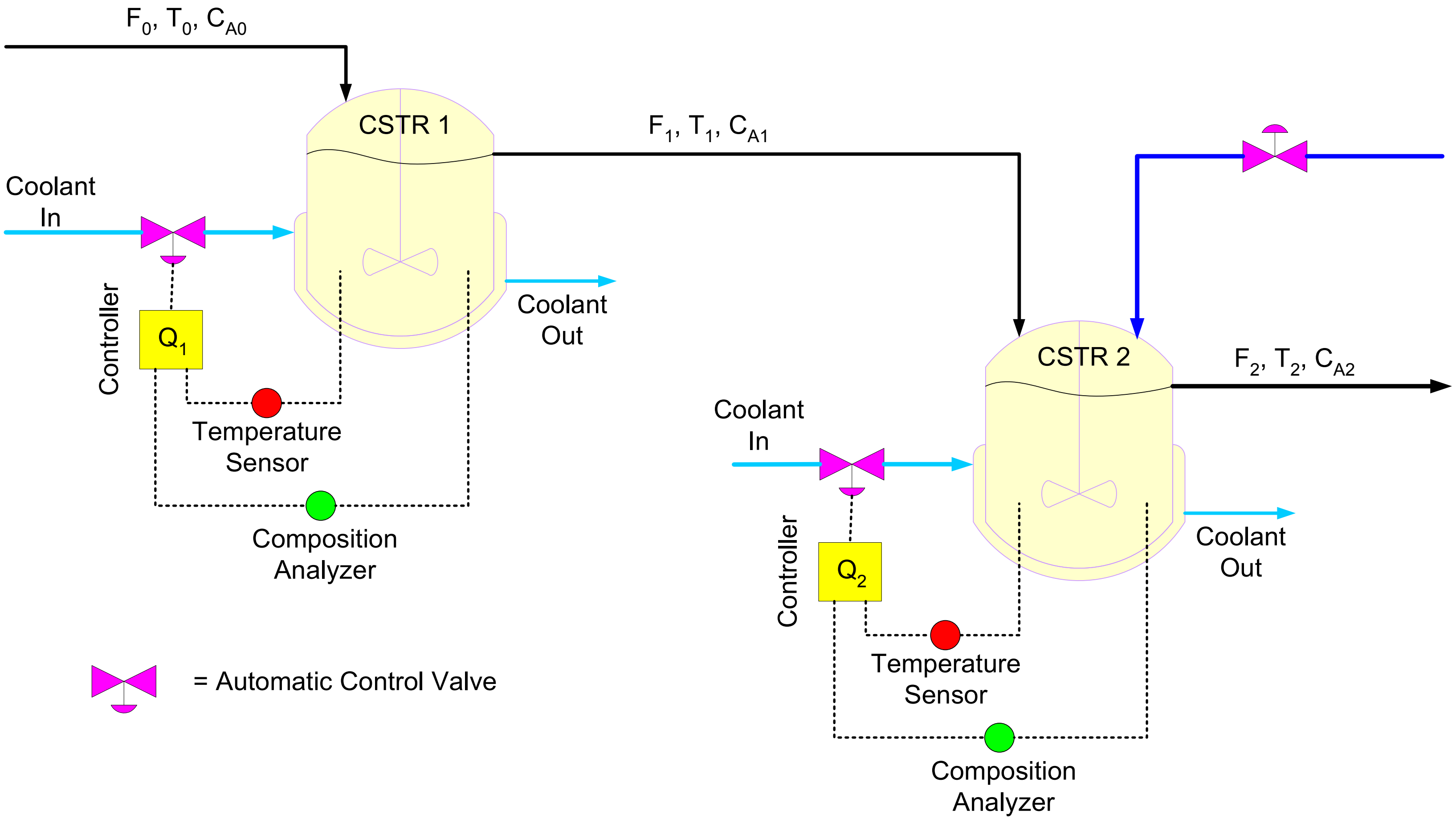
2003 AIChE Annual Meeting
San Francisco, CA.
November 20, 2003

INTRODUCTION

- **Process control system failure:**
  - ◇ Typical sources:
    - ⋆ Failure in control algorithm
    - ⋆ Faults in control actuators and/or measurement sensors
  - ◇ Induce discrete transitions in continuous dynamics
- **Motivation for fault-tolerant control:**
  - ◇ Preserve process integrity & dependability
  - ◇ Minimize negative economic & environmental impact:
    - ⋆ Raw materials waste, production losses, personnel safety, $\cdots$, etc.
- **Dynamics of chemical processes:**
  - ◇ Nonlinear behavior
    - ⋆ Complex reaction mechanisms
    - ⋆ Arrhenius reaction rates
  - ◇ Input constraints
    - ⋆ Finite capacity of control actuators

ISSUES IN FAULT-TOLERANT CONTROL OF CHEMICAL PROCESSES

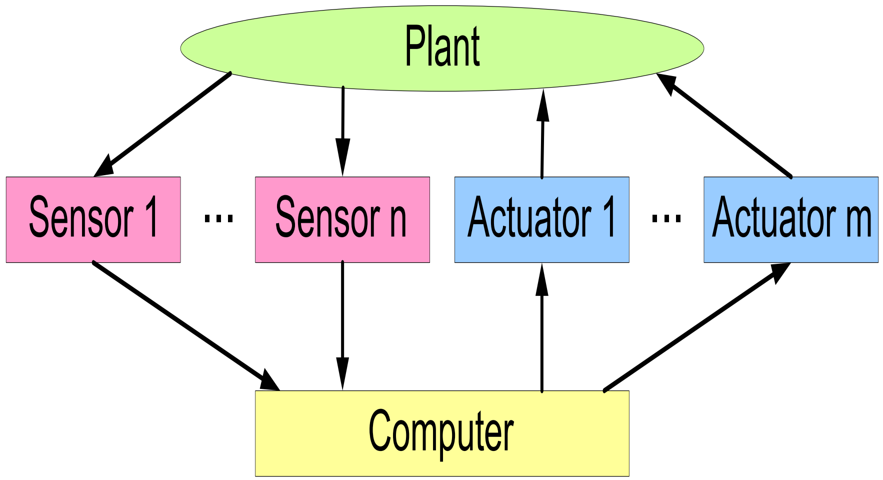
- **Availability of multiple control configurations:**
  - ◇ Actuator/sensor redundancy
  - ◇ Different manipulated variables
- **Illustrative example**



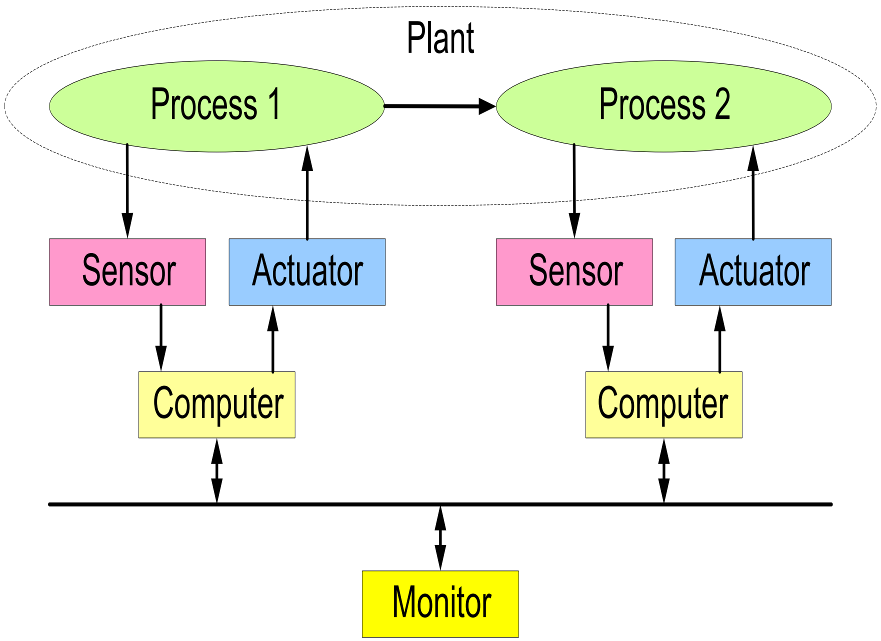
ISSUES IN FAULT-TOLERANT CONTROL OF CHEMICAL PROCESSES

- **Distributed interconnected nature of process units:**
  - ◇ Propagation of failure effects
  - ◇ Large numbers of distributed sensors & actuators involved
  - ◇ Efficient means of communication required

- **Types of control system architecture:**



⋆ Point-to-point connections



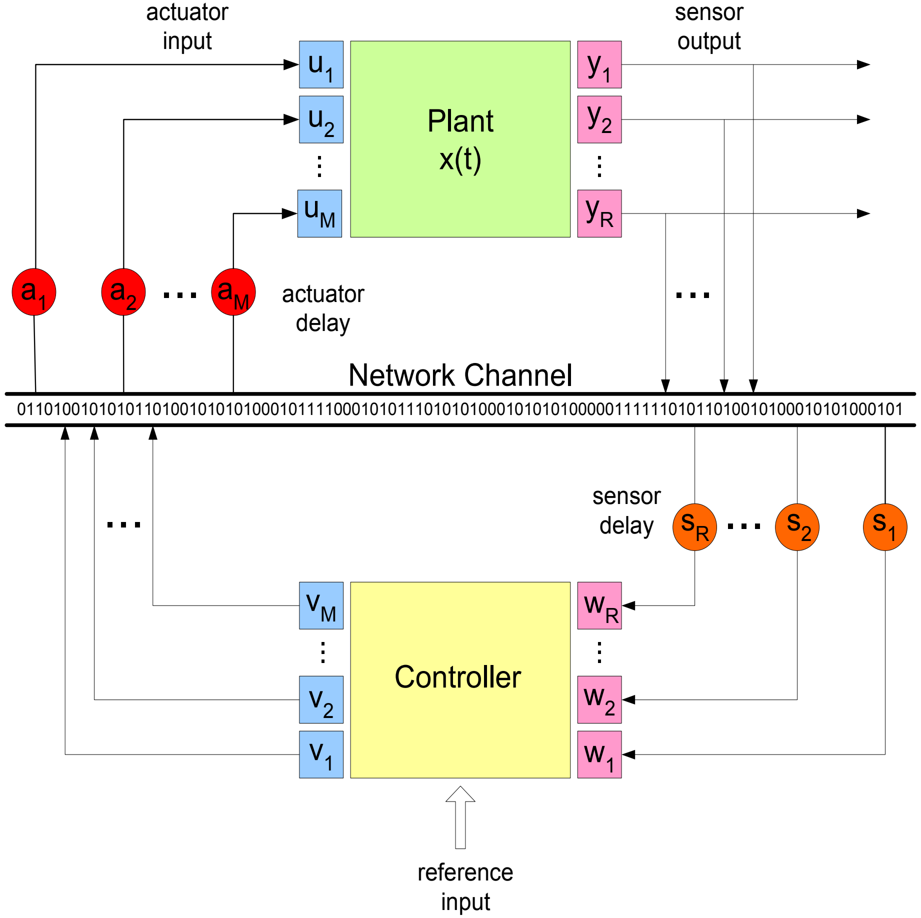
⋆ Distributed control system

INTEGRATING COMMUNICATION NETWORKS IN CONTROL

- **Defining feature:**

Information exchanged using a network among control system components

- **Networked control structure**



◇ Economic & operational benefits:

▷ Reduced system wiring

▷ Ease of diagnosis & maintenance

▷ Enhanced fault-tolerance:

⋆ Rerouting signals

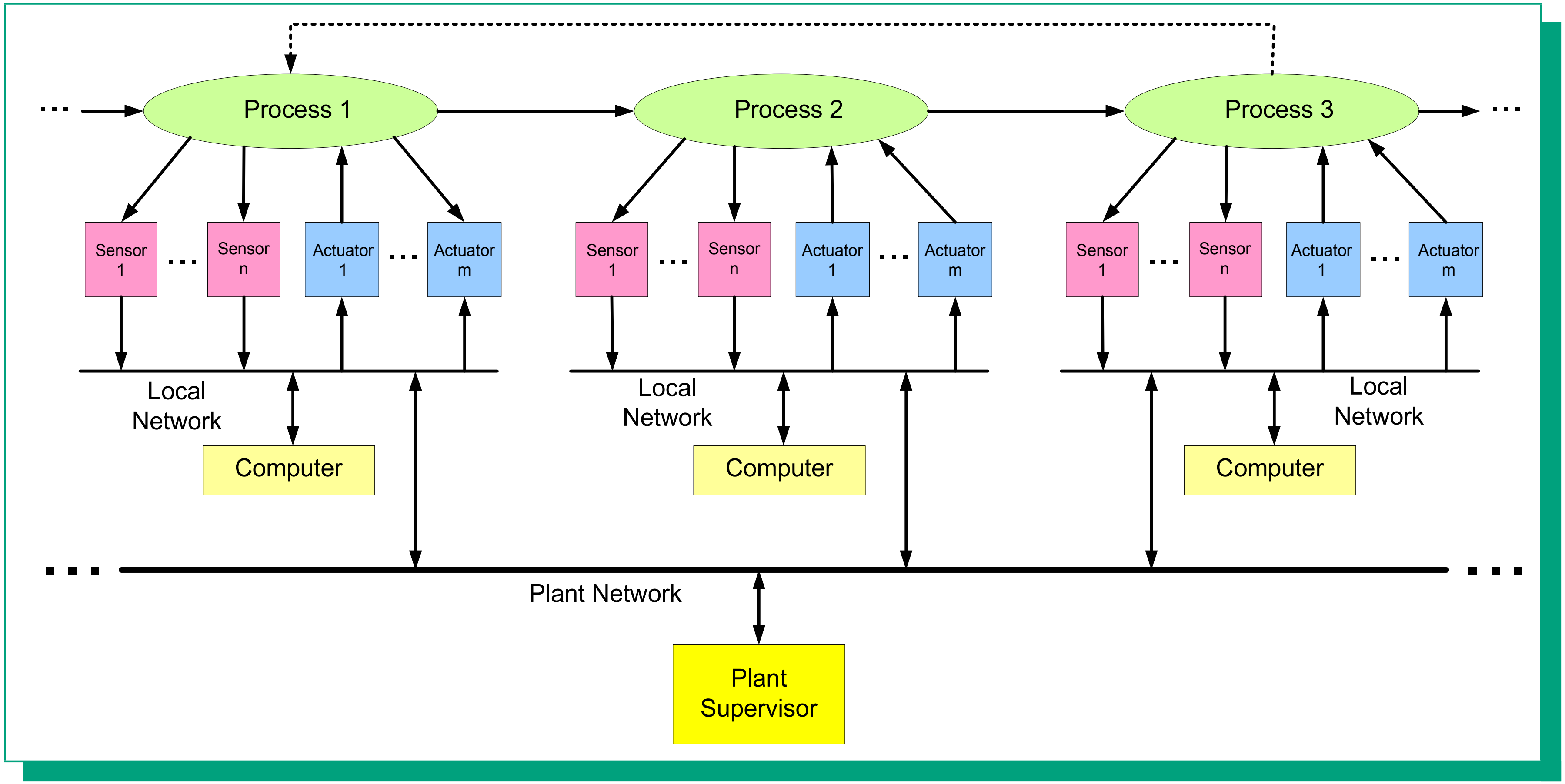
⋆ Activation of redundant components

◇ Implementation issues:

⋆ Bandwidth limitations

⋆ Network delays

INTEGRATING COMMUNICATION NETWORKS IN CONTROL



- **Practical implementation considerations:**
  - ◇ Size and complexity of the plant
  - ◇ Number of sensors & actuators
  - ◇ Bandwidth limitations in data transmission
  - ◇ Network scheduling and communication delays

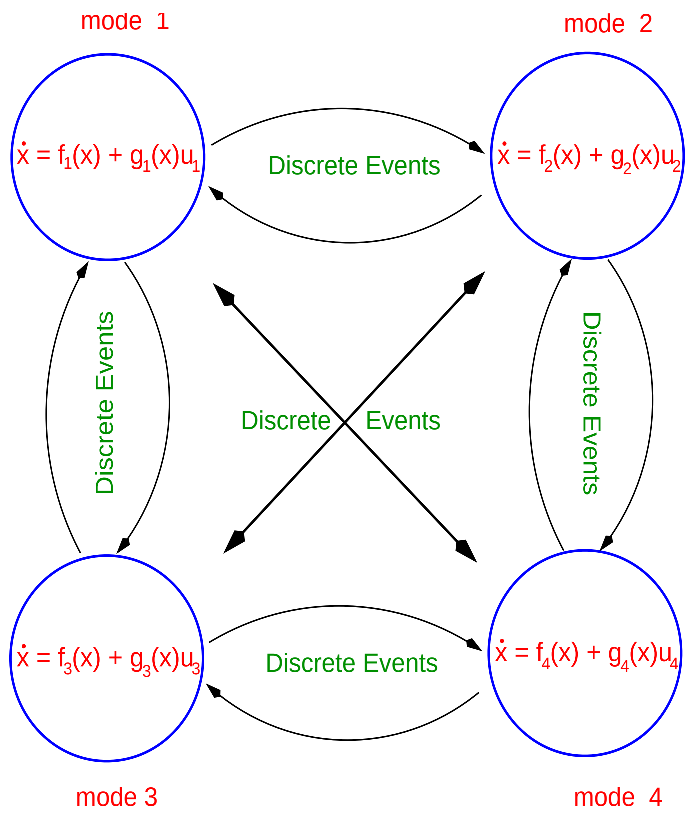
PRESENT WORK

- **Scope:**
  - ◇ Nonlinear process systems
    - ⋆ Input constraints
    - ⋆ Control system failures
- **Objectives:**
  - ◇ Integrated approach for fault-tolerant control system design
    - ▷ Design of nonlinear feedback controllers
      - ⋆ Nonlinear dynamics
      - ⋆ Input constraints
    - ▷ Design of supervisory switching laws
      - ⋆ Orchestrate transition between control configurations
    - ▷ Use of communication networks
  - ◇ Application to two chemical reactors in series
- **Approach:**
  - ◇ Lyapunov-based nonlinear control
  - ◇ Hybrid systems theory

A HYBRID SYSTEMS FRAMEWORK FOR FAULT-TOLERANT PROCESS CONTROL

- **State-space description:**

$$
\begin{aligned}
\dot{x}(t) &= f_i(x(t)) + \sum_{l=1}^{m} g_i^l(x(t))u_i^l(t) \\
i(t) &\in \mathcal{I} = \{1, 2, \cdots, N < \infty\} \\
u_{i,min}^l &\leq u_i^l(t) \leq u_{i,max}^l
\end{aligned}
$$



- ◇ $x(t) \in \mathbb{R}^n$: continuous process state variables
- ◇ $u_i(t) \in \mathbb{R}^m$: manipulated inputs for i-th mode
- ◇ $i(t) \in \mathcal{I}$: discrete variable controlled by supervisor
- ◇ N : total number of control configurations
- ◇ $f_i(x)$, $g_i^{(l)}(x)$: sufficiently smooth nonlinear functions

- **Faults induce discrete events superimposed on continuous dynamics**

FAULT-TOLERANT CONTROL PROBLEM FORMULATION

- **Coordinating feedback & switching over networks:**
  - ◇ Synthesis of a family of stabilizing feedback controllers
    - ⋆ Model for each mode of the hybrid plant: $\dot{x} \quad = \quad f_i(x) + G_i(x)u_i$
    - ⋆ Magnitude of input constraints: $|u_i| \quad \leq \quad u_{i,max}$
    - ⋆ Family of Lyapunov functions: $V_i, \quad i = 1, \cdots, N$
  - ◇ Design of supervisory switching laws that orchestrate mode transitions

$$\boxed{i(t) \quad = \quad \phi(x(t),\ i(t^{-}),\ t)}$$

  - ◇ Design of network communication logic
    - ⋆ Handling bandwidth limitations
    - ⋆ Handling transmission delays

- **Objective:**
  - ◇ Maintain closed-loop stability under failure situations

FEEDBACK CONTROLLER DESIGN

- **Lyapunov-based nonlinear control law:**

$$\boxed{u_i \quad = \quad -k_i(x, u_{i,max})(L_{g_i} V_i)^T}$$

◇ Example: bounded robust controller

(El-Farra & Christofides, Chem. Eng. Sci., 2001; 2003)

▷ Controller design accounts for constraints.

- **Explicit characterization of stability region:**

$$\boxed{\Omega_i(u_{i,max}) \quad = \quad \{x \in \mathbb{R}^n : V_i(x) \leq c_i^{max} \ \& \ \dot{V}_i(x) < 0\}}$$

◇ Explicit guidelines for mode switchings

◇ Larger estimates using a combination of several Lyapunov functions

MODEL PREDICTIVE CONTROL

- **Control problem formulation**
  - ◇ Finite-horizon optimal control:

$$\boxed{P(x,t) \quad : \quad \min\{J(x,t,u(\cdot))|\, u(\cdot) \in U_\Delta, V_\sigma(x(t+\Delta)) < V_\sigma(x(t))\}}$$

  - ◇ Performance index:

$$\boxed{J(x,t,u(\cdot)) \quad = \quad F(x(t+T)) + \int_t^{t+T} \left[\|x^u(s;x,t)\|_Q^2 + \|u(s)\|_R^2\right] ds}$$

▷ $\|\cdot\|_Q$: weighted norm.

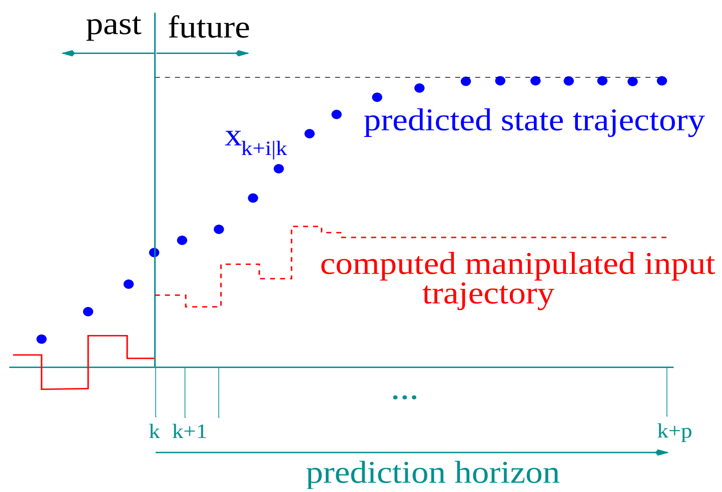
▷ T : horizon length.

▷ $Q,\ R > 0$: penalty weights.

▷ $F(\cdot)$: terminal penalty.

◇ Same V_σ as that for bounded controller design.

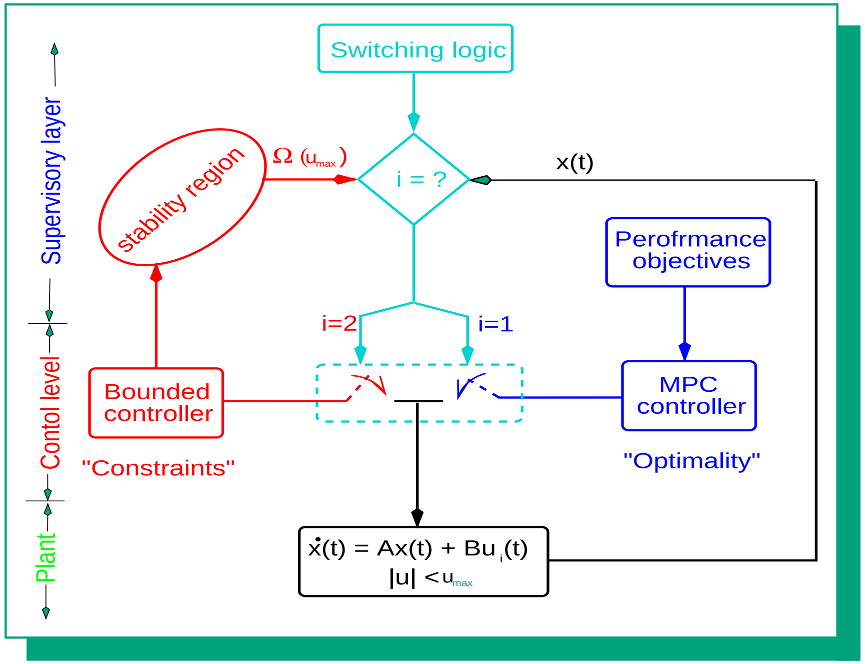
◇ Bounded controller may provide "good" initial guess.



HYBRID PREDICTIVE CONTROL

(El-Farra et. al., Automatica, 2004; IJRNC, 2004; AIChE J., 2004)

- **Switching logic:**



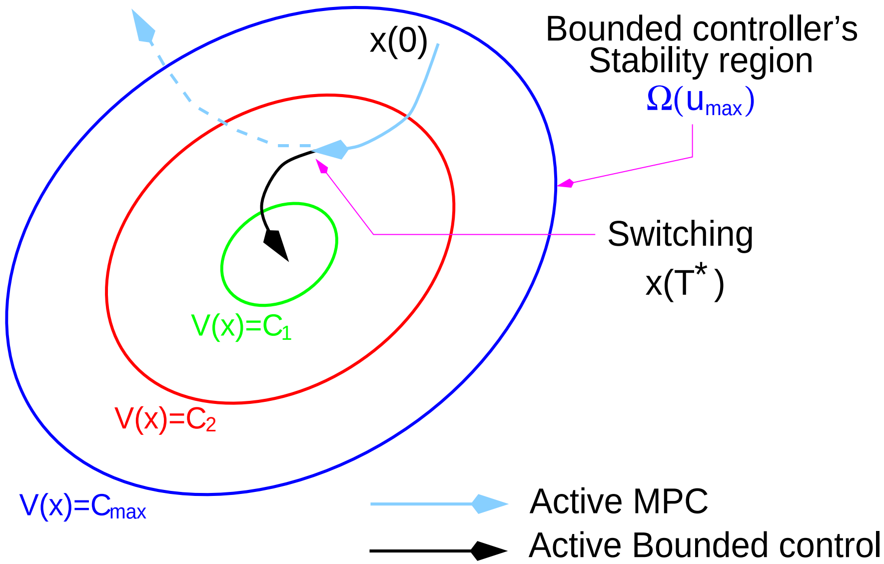
$$u_i(x(t)) = \begin{cases} M_i(x(t)), & 0 \leq t < T^* \\ b_i(x(t)), & t \geq T^* \end{cases}$$

$$\boxed{T^* = \inf\{T^* \geq 0 : L_{f_i} V_i(x) + L_{g_i} V_i(x) M_i(x(T^*)) \geq 0\}}$$

◇ Initially implement MPC, $x(0) \in \Omega_\sigma(u_{max})$

◇ Monitor temporal evolution of $V_\sigma(x^M(t))$

◇ Switch to bounded controller only if $V_\sigma(x^M(t))$ starts to increase

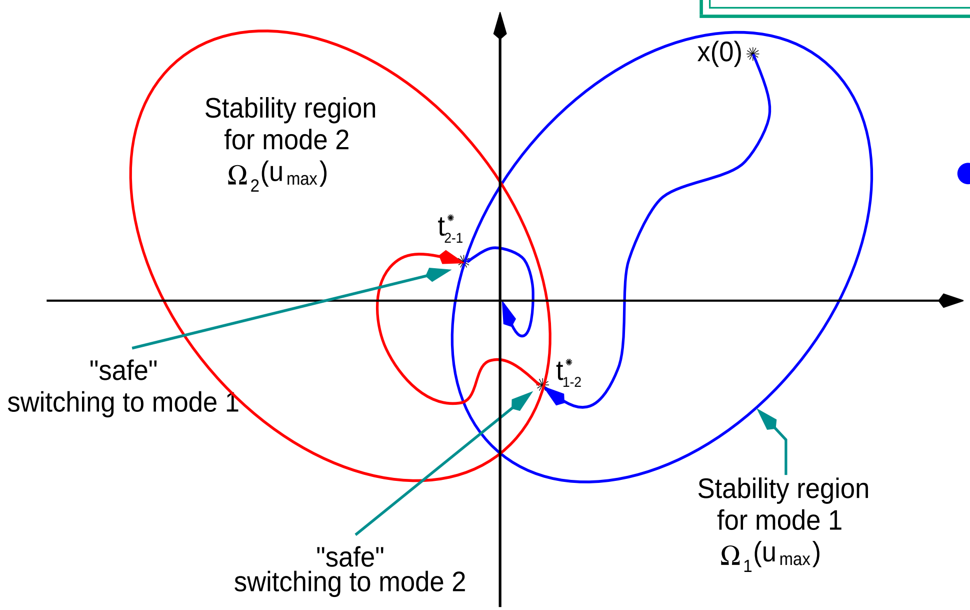


SUPERVISORY SWITCHING LOGIC FOR FAULT-RECOVERY

(El-Farra & Christofides, AIChE J., 2003)

- Basic mechanism for preserving closed-loop stability:
  - ◇ Switching between failed & well-functioning configurations
- Limitations imposed by input constraints
  - ◇ Stability regions of control configurations
- Switching policy: mode switching ensures fault-tolerance provided that
  - ◇ State within the stability region of fall-back configuration at time of failure

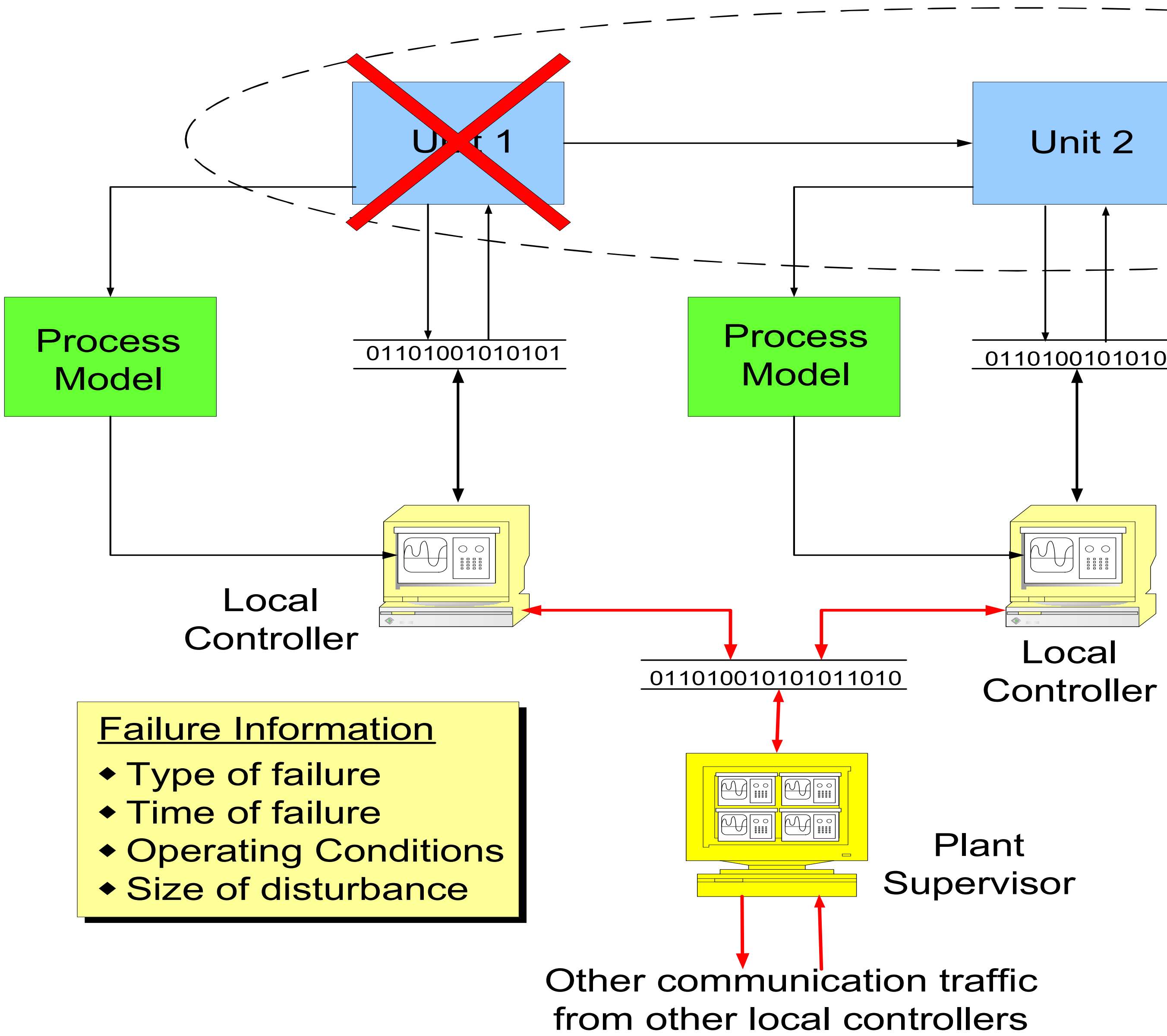
$$\boxed{x(T_f) \quad \in \quad \Omega_j(u_{j,max})}$$



Switching between stability regions

- Implications:
  - ⋆ Determines tolerable-failure times for a given reconfiguration strategy
  - ⋆ Determines selection of fall-back configuration for a given failure time

DESIGN & IMPLEMENTATION OF COMMUNICATION LOGIC



Fault-recovery Tasks

- Design robust controller

$$u = p(x, u_{max}, \theta_b)$$

- Compute fault-recovery region

$$\Omega := \Omega(x, u_{max}, \theta_b, t_{fail})$$

- Incorporate delays
- Select/activate fall-back config.

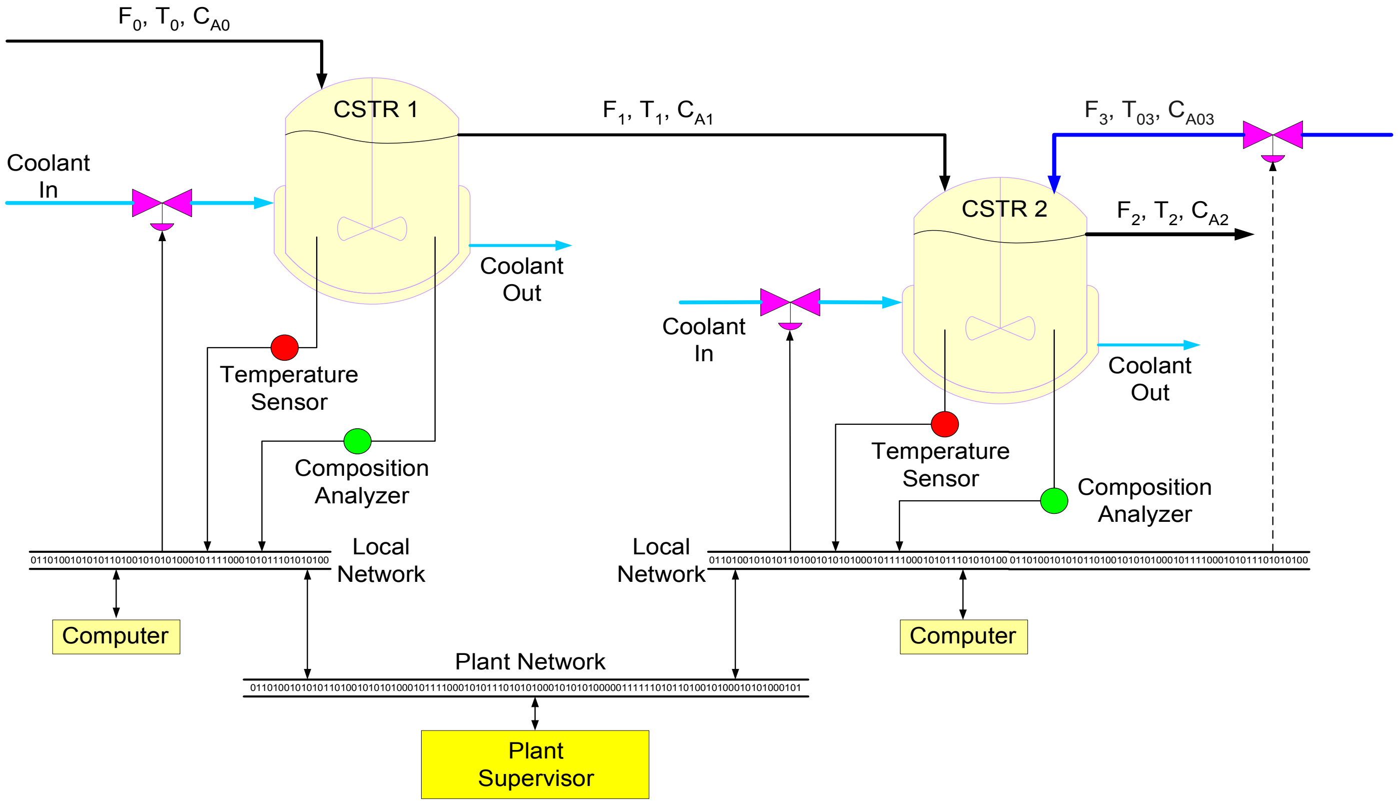
Failure Information

- Type of failure
- Time of failure
- Operating Conditions
- Size of disturbance

Objective:
Minimize effects of fault propagation

- Minimize unnecessary communication costs (tradeoff between network resources & control performance)
- Account for transmission delay

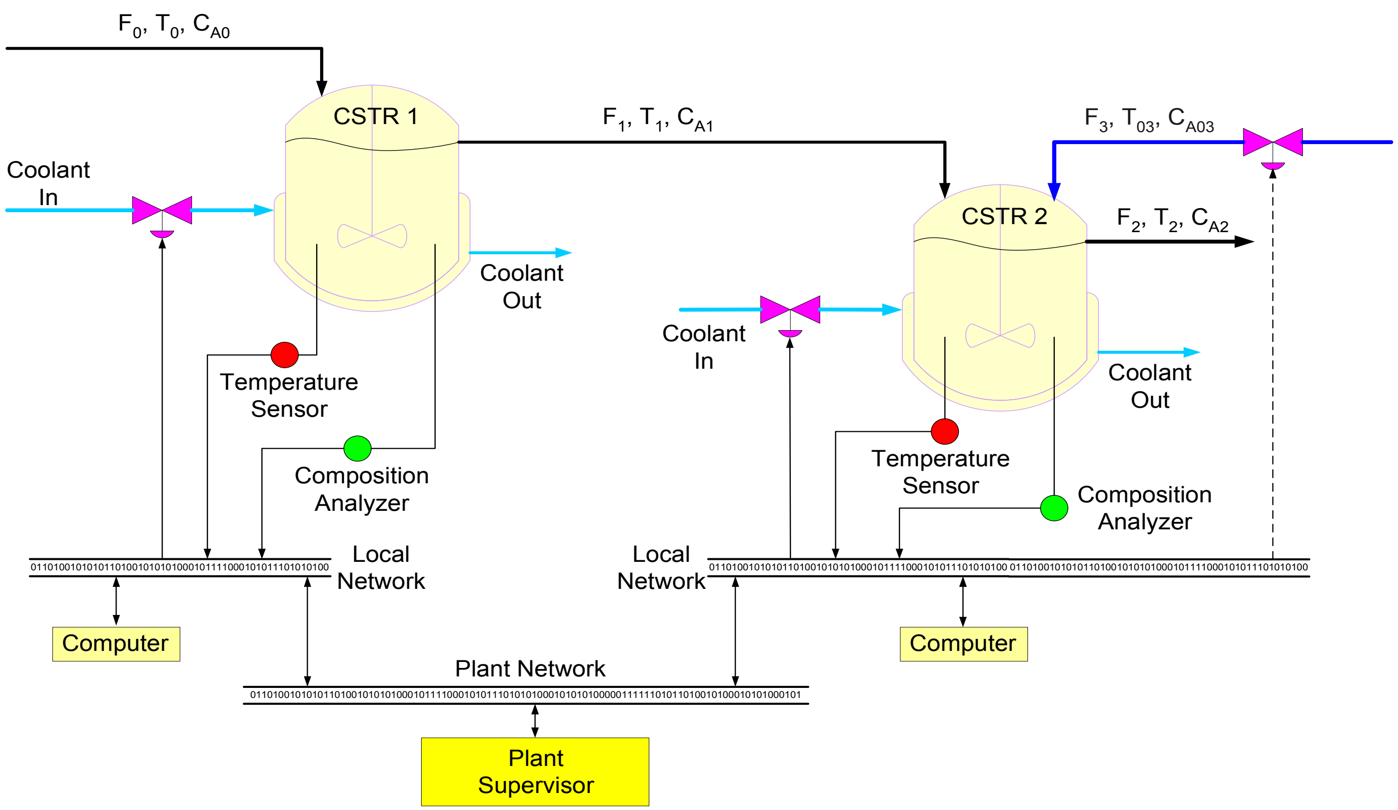
APPLICATION TO CHEMICAL REACTORS



- **Process dynamic model:**

$$
\begin{aligned}
\frac{dC_{A_1}}{dt} &= \frac{F_0}{V_1}(C_{A0} - C_{A_1}) - k_0 \exp\left(\frac{-E}{RT_1}\right) C_{A_1} \\
\frac{dT_1}{dt} &= \frac{F_0}{V_1}(T_0 - T_1) + \frac{(-\Delta H_r)}{\rho c_p} k_0 \exp\left(\frac{-E}{RT_1}\right) C_{A_1} + \frac{Q_1(t)}{\rho c_p V_1} \\
\frac{dC_{A_2}}{dt} &= \frac{F_1}{V_2}(C_{A_1} - C_{A_2}) - k_0 \exp\left(\frac{-E}{RT_2}\right) C_{A_2} + \frac{F_3}{V_2}(C_{A03} - C_{A_2}) \\
\frac{dT_2}{dt} &= \frac{F_1}{V_2}(T_1 - T_2) + \frac{(-\Delta H_r)}{\rho c_p} k_0 \exp\left(\frac{-E}{RT_2}\right) C_{A_2} + \frac{Q_2(t)}{\rho c_p V_2} + \frac{F_3}{V_2}(T_{03} - T_2)
\end{aligned}
$$

FAULT-TOLERANT CONTROL PROBLEM FORMULATION

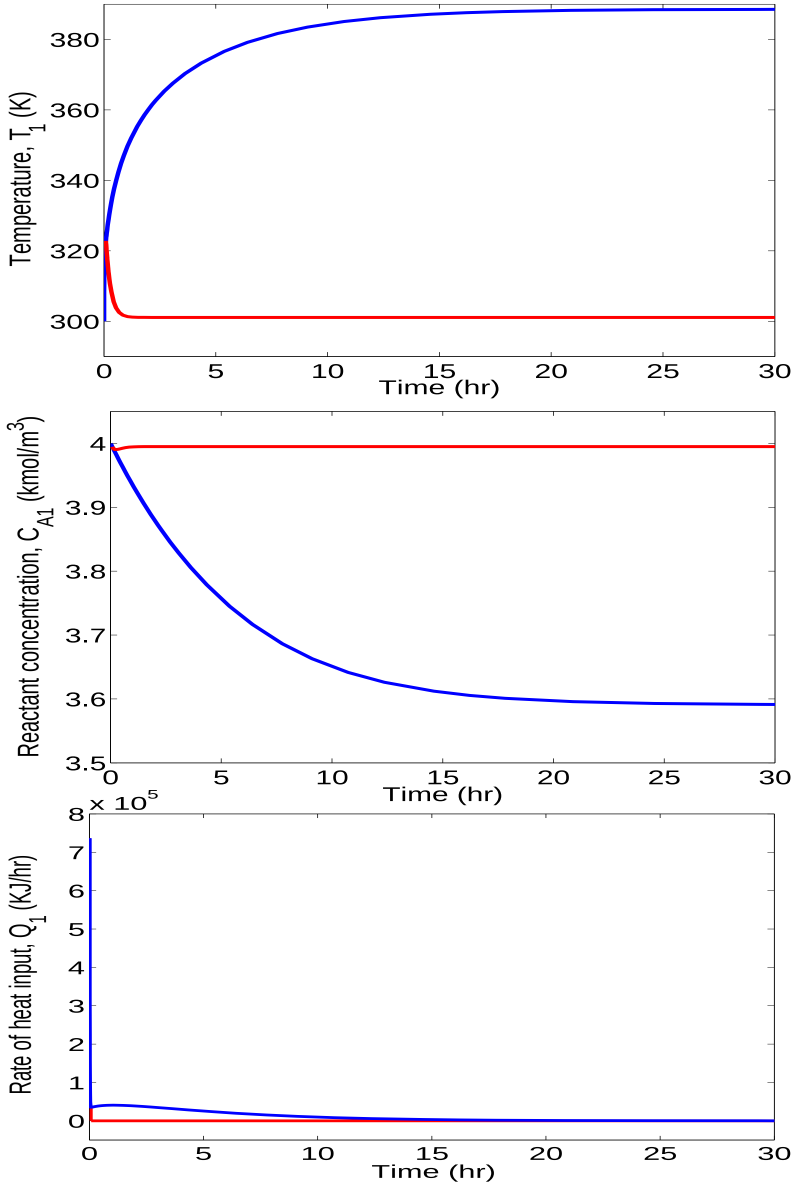


- **Control objective:**
  - ◇ Under normal operation: stabilize both reactors at unstable steady-states
  - ◇ Under controller failure: preserve closed-loop stability of CSTR 2

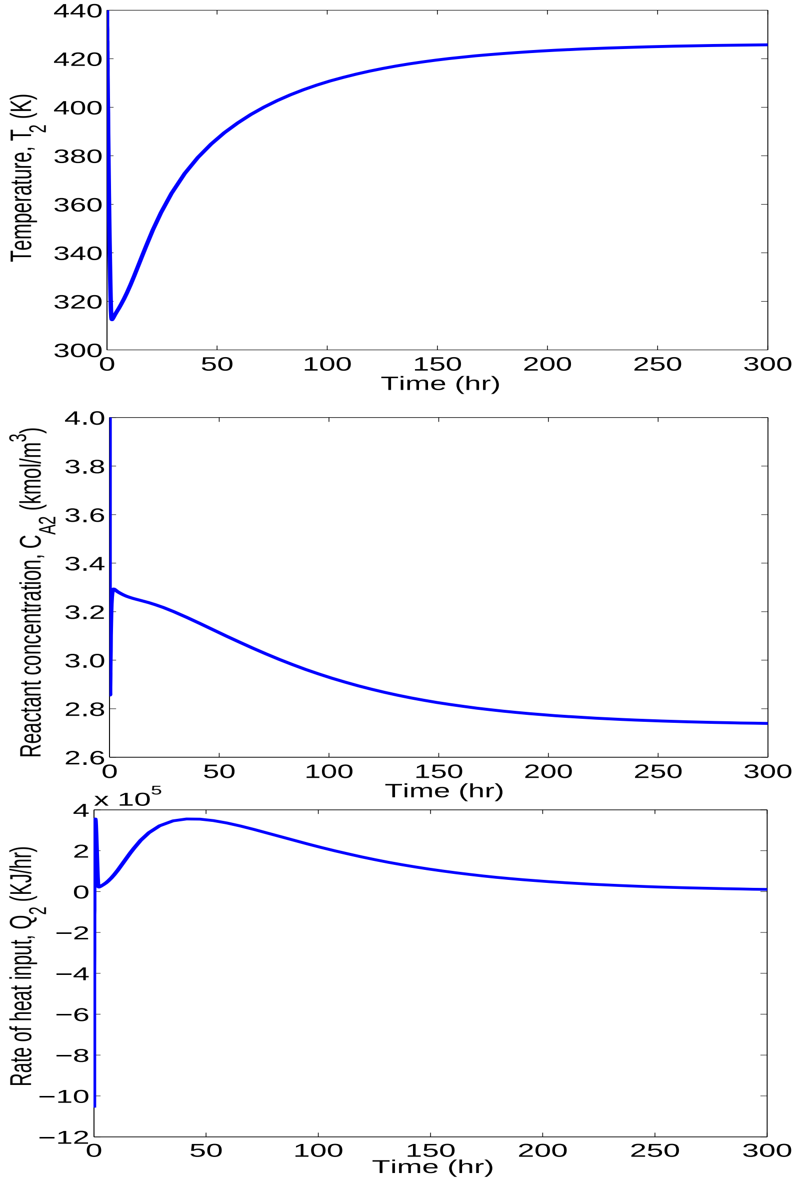
- **Candidate control configurations:**
  - ◇ Under normal operation: (Q_1, Q_2): $|Q_1| \leq Q_1^{max}$, $|Q_2| \leq Q_2^{max}$
  - ◇ Under failure conditions: (Q_2, C_{A03}): $|Q_2| \leq Q_2^{max}$, $|C_{A03} - C_{A03_s}| \leq C_{A03}^{max}$

CLOSED-LOOP SIMULATION RESULTS

⋆ Closed-loop state & input profiles under well-functioning & failed controllers (failure occurs at $t = 5$ min)



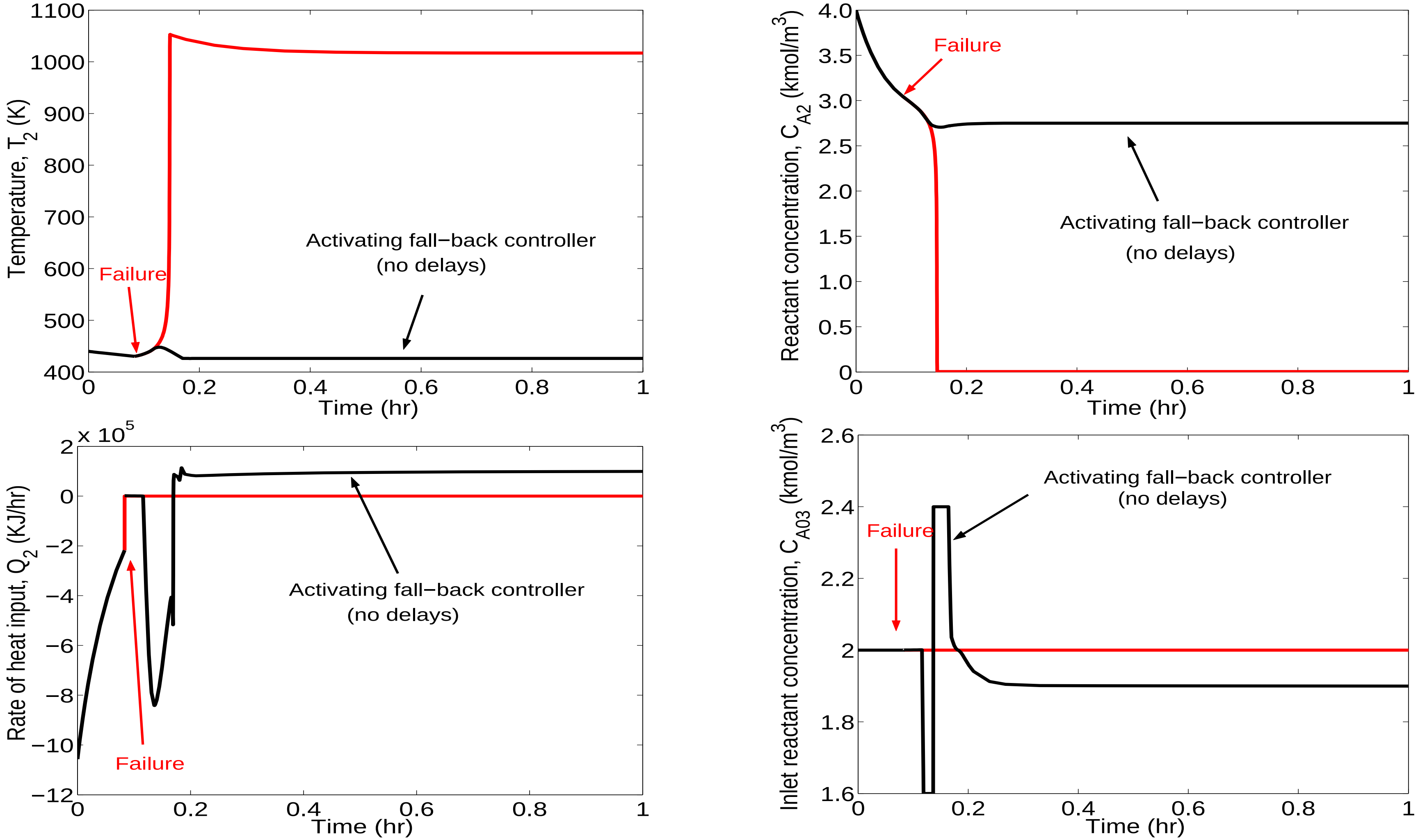
CSTR 1



CSTR 2

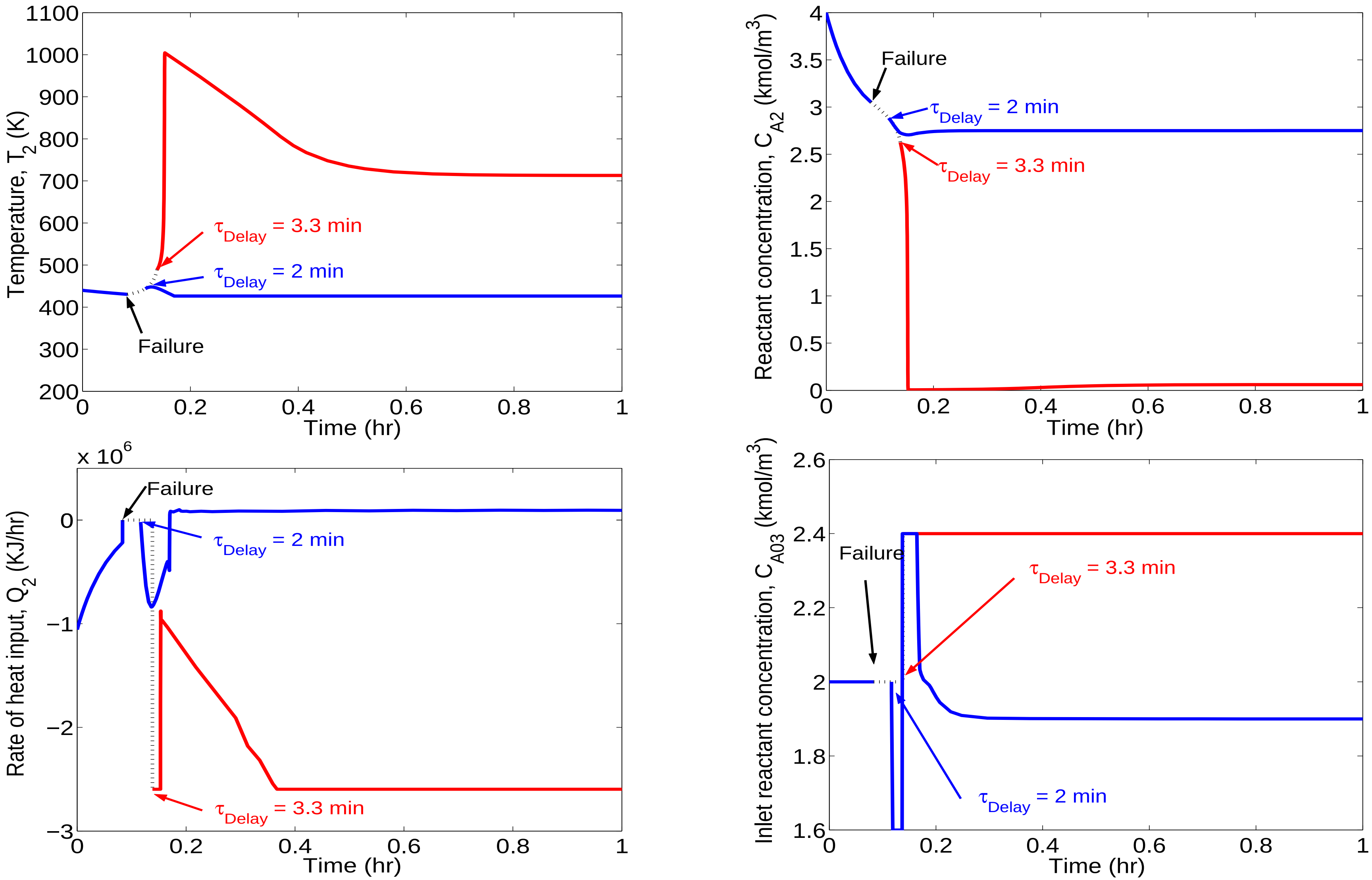
CLOSED-LOOP SIMULATION RESULTS

- ◇ Closed-loop state & input profiles for CSTR 2 when
  - ⋆ (Q_1, Q_2) configuration fails at $t = 5$ min
  - ⋆ (Q_2, C_{A03}) configuration activated (transmission of "disturbance bounds" over network – no delays)



CLOSED-LOOP SIMULATION RESULTS

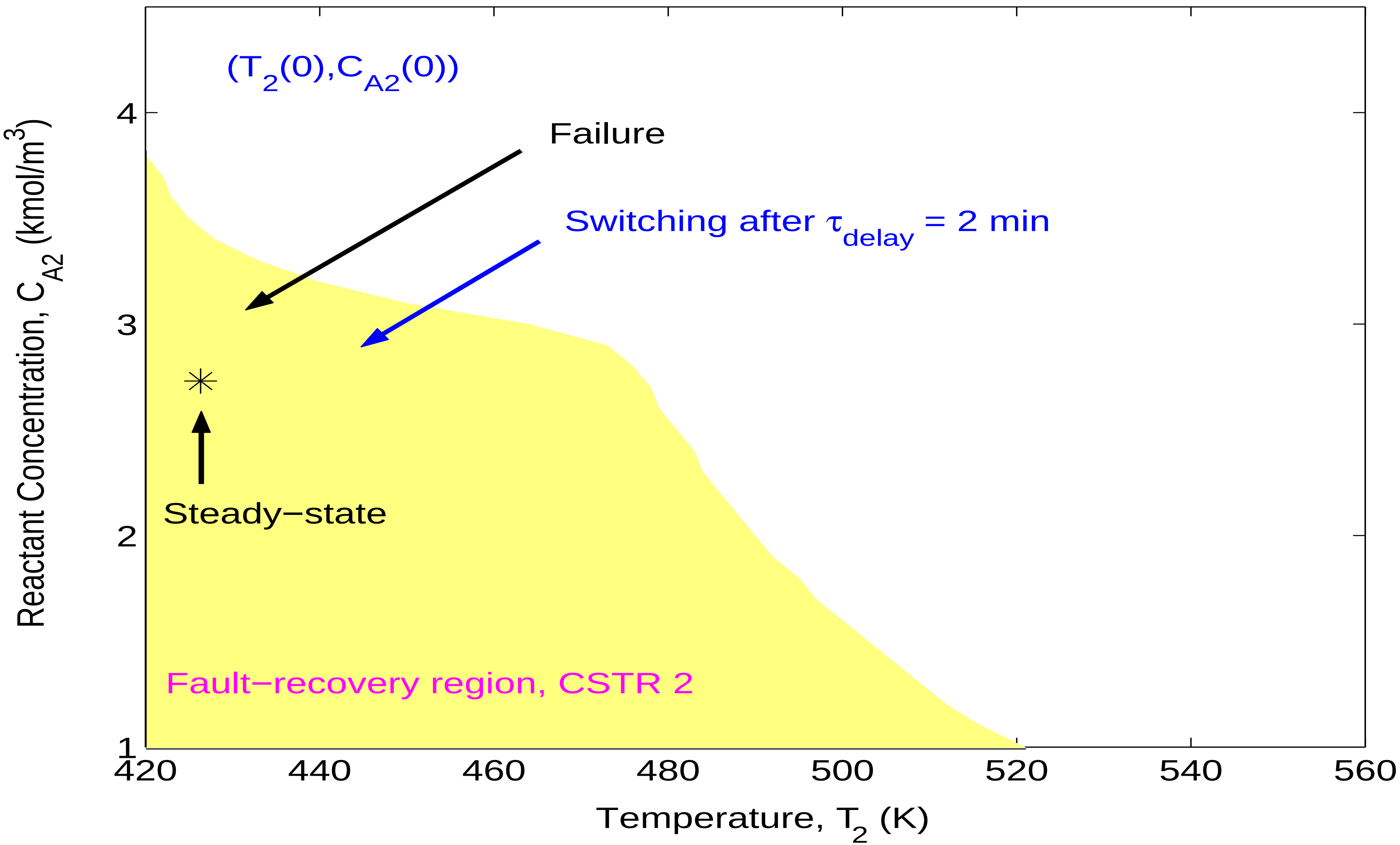
⋆ Implementation of fault-tolerant control strategy over network with total delay (fault-detection/communication/actuator activation) of $\tau_D = 2$ min & $\tau_D = 3.3$ min



EFFECT OF DELAYS ON FAULT-TOLERANCE

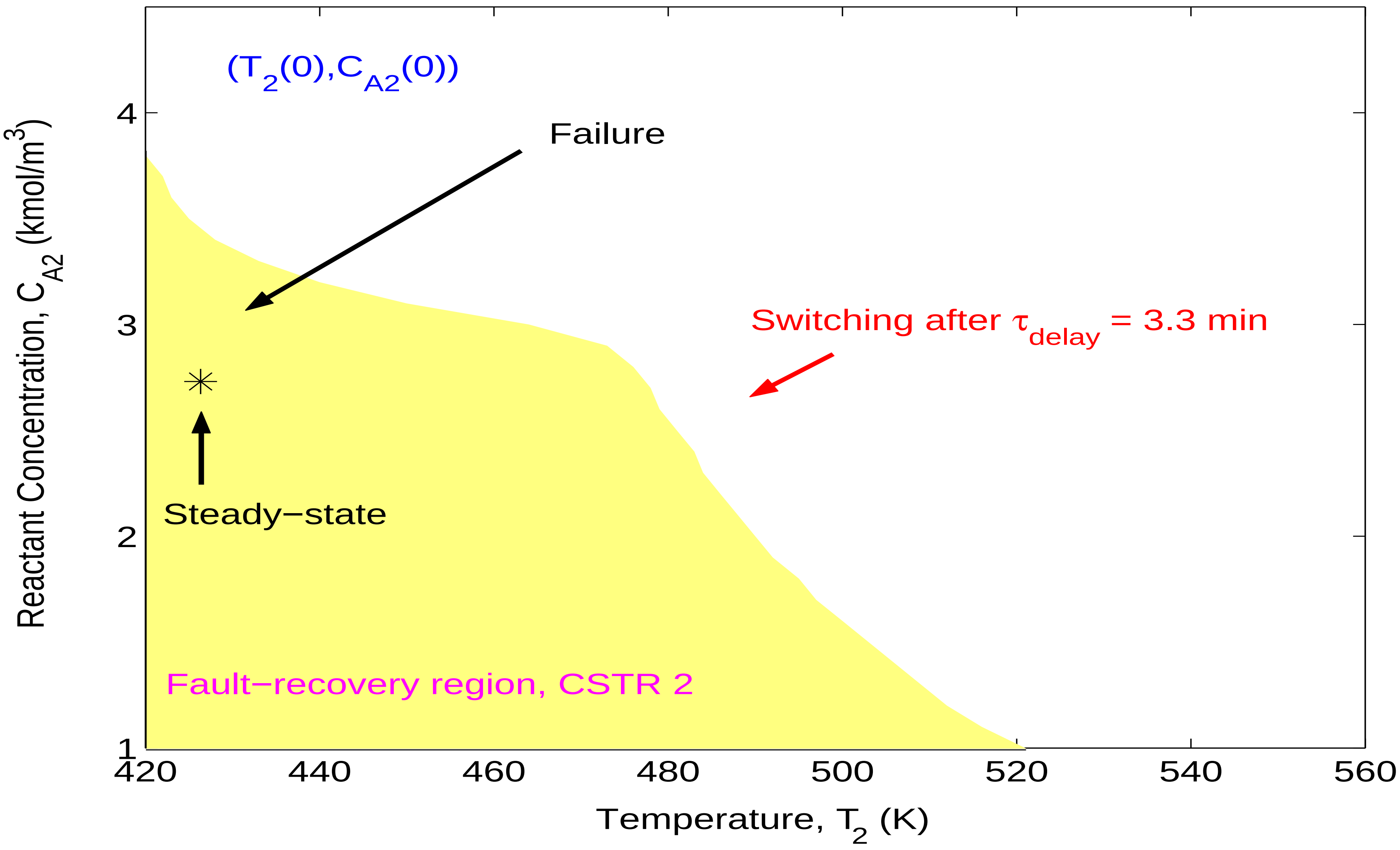
◇ Tradeoff between:

- ⋆ Network design (communication logic & delays)
- ⋆ Control system design (fault-recovery region, switching logic)



EFFECT OF DELAYS ON FAULT-TOLERANCE

- ◇ Tradeoff between:
  - ⋆ Network design (communication logic & delays)
  - ⋆ Control system design (fault-recovery region, switching logic)



CONCLUSIONS

- Chemical process systems with:
  - ⋆ Nonlinear dynamics ⋆ Input constraints ⋆ Control system failures
- Integrated approach for fault-tolerant control over communication networks:
  - ◇ Design of constrained nonlinear feedback controllers:
  - ◇ Design of fault-tolerant supervisory switching laws:
    - ⋆ Stability regions of control configurations
  - ◇ Design of communication logic:
    - ⋆ Accounting for network resource limitations
    - ⋆ Effects of delays on fault-tolerance
- Approach brings together tools from Lyapunov and hybrid systems theory
- Application to two chemical reactors in series

ACKNOWLEDGMENT

- Financial support from NSF, CTS-0129571, is gratefully acknowledged