

FAULT-TOLERANT CONTROL OF PROCESS SYSTEMS: INTEGRATING SUPERVISORY AND FEEDBACK CONTROL OVER NETWORKS

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

*Department of Chemical Engineering
University of California, Los Angeles, CA 90095-1592*

Abstract: This work proposes a methodology for the design of fault-tolerant control systems for nonlinear processes with actuator constraints. The proposed approach is predicated upon the idea of integrating supervisory and feedback control over networks. Initially, a family of candidate control configurations, characterized by different manipulated inputs, are identified. For each control configuration, a bounded nonlinear feedback controller, that enforces asymptotic closed-loop stability in the presence of constraints, is designed, and the constrained stability region associated with it is explicitly characterized. A switching policy is then derived, on the basis of the stability regions, to orchestrate the activation/deactivation of the constituent control configurations in a way that guarantees closed-loop stability in the event of control system failures. The switching laws are implemented by a higher-level supervisor that constantly monitors the process and communicates with the various control configurations over a network. The effects of delays in fault-detection, network communication and actuator activation are taken explicitly into account in executing the switching logic. The efficacy and implementation of the proposed approach are demonstrated through a chemical process example.

Keywords: Hybrid control, Switching laws, Constraints, Communication delays, Process systems.

1. INTRODUCTION

One of the central problems in the design of any practical process control system is the issue of fault-tolerance. Present-day process control systems are highly automated and therefore vulnerable to faults such as defects in control actuators, defects in measurement sensors, failures in the controllers or in the control loops. Such failures can cause a host of undesired reactions and consequences, if not appropriately accounted for in the control system design. Examples include degradation of the control system performance, instability, damage to technical parts of the plant, jeopardizing personnel and environmental safety, increasing downtime for process operation, increasing raw material waste, and resulting in significant production losses. As efficient and profitable process operation becomes more dependent on au-

tomated control systems, there is a greater need to design and implement advanced fault-tolerant control systems that can minimize the crippling effects of control system failures on process operation.

These considerations have consequently motivated many research studies on the problem of fault-tolerant control, particularly for linear and/or unconstrained processes (e.g., see (Willsky, 1998; Yang *et al.*, 1998; Bao *et al.*, 2002)). Many chemical processes, however, are inherently nonlinear and subject to hard constraints on the control actuators. In addition, the ability of the process control system to deal with failure situations requires, *inter alia*, inherent structural flexibility that allows the control system to safely transition from the failed control configuration to an alternative, well-functioning configuration. To this end, classical process control schemes, whereby a fixed controller

structure is used to achieve the desired control objectives, are in general not adequate for dealing with the problem because they are not properly equipped to cope with the discrete structural changes that these failures induce in the closed-loop system.

The necessary flexibility of the control system in dealing with failure situations requires consideration of hybrid control instead. Hybrid control refers to control structures that integrate lower-level continuous controllers together with higher-level logic-based supervisors that orchestrate switching between the constituent controllers. These structures have provided a natural setting for addressing a wide range of problems that cannot be addressed using classical control approaches, including fault-tolerant control of distributed systems (e.g., see (El-Farra and Christofides, 2003b)) and control of hybrid processes whose intrinsic dynamics exhibit switchings between multiple modes of operation (e.g., see (Bemporad and Morari, 1999; El-Farra and Christofides, 2002; El-Farra and Christofides, 2003a)).

In this work, we propose a methodology for the design of fault-tolerant process control systems for nonlinear processes with actuator constraints. The basic idea is that of integrating feedback control and logic-based switching between multiple constrained control configurations, each characterized by a different manipulated input and a different region of closed-loop stability. The switching policy, which is based on the stability regions, is implemented by a higher-level supervisor, that receives and transmits information to the feedback system over a network and activates/deactivates the appropriate control configuration accordingly in a way that ensures actuator fault-tolerance. The effects of delays in fault-detection, delays in network communication between the supervisor and the control loops, and delays in actuator activation are handled explicitly in designing the switching logic. Finally, the efficacy and implementation of the proposed approach are demonstrated through a chemical process example.

2. PRELIMINARIES

2.1 System description - problem formulation

We consider the class of continuous-time, single-input nonlinear processes with constraints on the manipulated input, represented by the following state-space description:

$$\begin{aligned} \dot{x}(t) &= f_{k(t)}(x(t)) + g_{k(t)}(x(t))u_{k(t)} \\ |u_{k(t)}| &\leq u_{max}^k \\ k(t) &\in \mathcal{K} = \{1, \dots, N\}, \quad N < \infty \end{aligned} \quad (1)$$

where $x(t) \in \mathbb{R}^n$ denotes the vector of process state variables and $u_k(t) \in [-u_{max}^k, u_{max}^k] \subset \mathbb{R}$ denotes the constrained manipulated input associated with the k -th control configuration. $k(t)$, which takes values in the finite index set \mathcal{K} , represents a discrete state that

indexes the vector fields $f_k(\cdot)$, $g_k(\cdot)$ as well as the manipulated input $u_k(\cdot)$. For each value that k assumes in \mathcal{K} , the process is controlled via a different manipulated input which defines a given control configuration. Switching between the available N control configurations is controlled by a higher-level supervisor that monitors the process and orchestrates, accordingly, the transition between the different control configurations in the event of control system failure. This in turn determines the temporal evolution of the discrete state, $k(t)$. The supervisor ensures that only one control configuration is active at any given time, and allows only a finite number of switches over any finite interval of time.

It is assumed that the origin is the equilibrium point of the nominal process (i.e. $f_k(0) = 0$) and that the vector functions $f_k(\cdot)$ and $g_k(\cdot)$ are sufficiently smooth, for all k , on \mathbb{R}^n . The control objective is to stabilize the process of Eq.1 in the presence of actuator constraints and faults in the control system. The basic problem is how to coordinate switching between the different control configurations (or manipulated inputs) in a way that respects actuator constraints and guarantees closed-loop stability in the event of faults. To simplify the presentation of our results, we will focus only on the state feedback problem where measurements of all process states are available for all times.

2.2 Motivating example

To motivate our fault-tolerant control system design methodology (presented in section 3), we introduce in this section a benchmark chemical reactor example that will be used throughout the paper to illustrate the design and implementation of the fault-tolerant control system. To this end, consider a well-mixed, non-isothermal continuous stirred tank reactor where three parallel irreversible elementary exothermic reactions of the form $A \xrightarrow{k_1} B$, $A \xrightarrow{k_2} U$ and $A \xrightarrow{k_3} R$ take place, where A is the reactant species, B is the desired product and U , R are undesired byproducts. The feed to the reactor consists of pure A at flow rate F , molar concentration C_{A0} and temperature T_{A0} . Due to the non-isothermal nature of the reactions, a jacket is used to remove/provide heat to the reactor. Under standard modeling assumptions, a mathematical model of the process can be derived from material and energy balances and takes the following form:

$$\begin{aligned} \frac{dT}{dt} &= \frac{F}{V}(T_{A0} - T) + \sum_{i=1}^3 R_i(C_A, T) + \frac{Q}{\rho c_p V} \\ \frac{dC_A}{dt} &= \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^3 k_{i0} e^{\frac{-E_i}{RT}} C_A \\ \frac{dC_B}{dt} &= -\frac{F}{V}C_B + k_{10} e^{\frac{-E_1}{RT}} C_A \end{aligned} \quad (2)$$

where $R_i(C_A, T) = \frac{(-\Delta H_i)}{\rho c_p} k_{i0} e^{\frac{-E_i}{RT}} C_A$, C_A and C_B denote the concentrations of the species A and B , T denotes the temperature of the reactor, Q denotes rate of heat

input/removal from the reactor, V denotes the volume of the reactor, ΔH_i , k_i , E_i , $i = 1, 2, 3$, denote the enthalpies, pre-exponential constants and activation energies of the three reactions, respectively, c_p and ρ denote the heat capacity and density of the reactor. The values of the process parameters and the corresponding steady-state values can be found in (El-Farra and Christofides, 2001). It was verified that under these conditions, the process of Eq.2 has three steady-states (two locally asymptotically stable and one unstable at $(T_s, C_{As}, C_{Bs}) = (388 \text{ K}, 3.59 \text{ mol/L}, 0.41 \text{ mol/L})$).

The control objective considered here is the typical one of stabilizing the reactor at the (open-loop) unstable steady-state. Operation at this point is typically sought to avoid high temperatures, while simultaneously achieving reasonable conversion. To accomplish this objective in the presence of control system failures, we consider the following manipulated input candidates (see Fig.1):

- (1) Rate of heat input, $u_1 = Q$, subject to the constraints $|Q| \leq u_{max}^1 = 748 \text{ KJ/s}$.
- (2) Inlet stream temperature, $u_2 = T_{A0} - T_{A0s}$, subject to the constraints $|u_2| \leq u_{max}^2 = 100 \text{ K}$.
- (3) Inlet reactant concentration, $u_3 = C_{A0} - C_{A0s}$, subject to the constraints $|u_3| \leq u_{max}^3 = 4 \text{ mol/L}$.

Each of the above manipulated inputs represents a unique control configuration (or control-loop) that, by itself, can stabilize the reactor. The first loop involving the heat input, Q , will be considered as the primary configuration. In the event of some failure in this configuration, however, the plant supervisor, will have to activate one of the other two backup configurations in order to maintain closed-loop stability. The main question, which we address in the next section, is how can the supervisor determine which control loop to activate once failure is detected in the active configuration.

3. INTEGRATING SUPERVISORY AND FEEDBACK CONTROL OVER NETWORKS

3.1 Fault-tolerant design methodology

Having identified the candidate control configurations that can be used, we outline in this section the main steps involved in the fault-tolerant control system design procedure. These include: 1) the synthesis of a stabilizing feedback controller for each control configuration, 2) the explicit characterization of the constrained stability region associated with each configuration, and 3) the design of a switching law that orchestrates the re-configuration of control system in a way that guarantees closed-loop stability in the event of failures in the active control configuration. Below is a brief description of each step as applied to the chemical reactor example introduced in section 2.2.

(a) Constrained feedback controller synthesis:

In this step, we synthesize, for each control configuration, a feedback controller that enforces asymp-

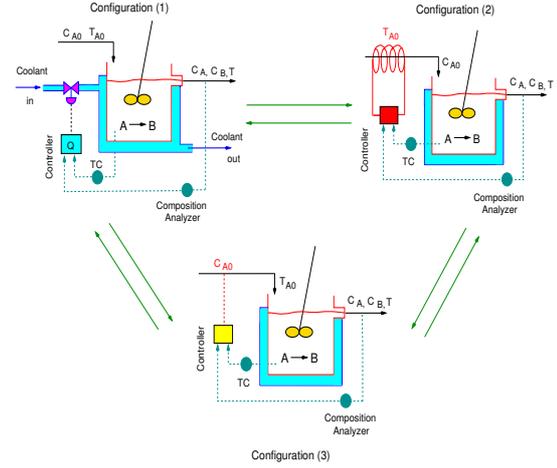


Fig. 1. Switching between multiple control configurations, each characterized by a different manipulated input

totic closed-loop stability in the presence of actuator constraints. This task is carried out on the basis of the process input/output dynamics. While our control objective is to achieve full state stabilization (and not output tracking), process outputs are introduced only to facilitate transforming the system of Eq.2 into a form more suitable for explicit controller synthesis. In the case of Eq.2, a further simplification can be obtained by noting that C_B does not affect the evolution of either T or C_A , and therefore the controller design can be addressed on the basis of the T and C_A equations only. A controller that stabilizes the (T, C_A) system will automatically stabilize the full system.

1. For the first configuration with $u_1 = Q$, we consider the output $y_1 = C_A - C_{As}$. This choice yields a relative degree of $r_1 = 2$ for the output with respect to the manipulated input. The coordinate transformation (in error variables form) takes the form: $e_1 = C_A - C_{As}$, $e_2 = \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^3 k_{i0} e^{-\frac{E_i}{RT}} C_A$.

2. For the second configuration with $u_2 = T_{A0} - T_{A0s}$, we choose the output $y_2 = C_A - C_{As}$ which yields the same relative degree as in the first configuration, $r_2 = 2$, and the same coordinate transformation.

3. For the third configuration with $u_3 = C_{A0} - C_{A0s}$, we choose the output $y_3 = T - T_s$ which yields a relative degree of $r_3 = 2$ and a coordinate transformation of the form: $e_1 = T - T_s$, $e_2 = \frac{F}{V}(T_{A0} - T) + \frac{Q}{\rho c_p V} + \sum_{i=1}^3 R_i(C_A, T)$.

Note that since our objective is full state stabilization, the choice of the output in each case is really arbitrary. However, to facilitate our controller design and subsequent stability analysis, we have chosen in each case an output that produces a system of relative degree 2. For each configuration, the corresponding state transformation yields a system, describing the input/output dynamics, of the following form

$$\begin{aligned} \dot{e} &= Ae + l_k(e) + b\alpha_k u_k \\ &:= \bar{f}_k(e) + \bar{g}_k(e)u_k \end{aligned} \quad (3)$$

where $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $l_k(\cdot) = L_{f_k}^2 h_k(x)$, $\alpha_k(\cdot) = L_{g_k} L_{f_k} h_k(x)$, $h_k(x) = y_k$ is the output associated with the k -th configuration, $x = [x_1 \ x_2]^T$ with $x_1 = T - T_s$, $x_2 = C_A - C_{As}$, and the functions $f_k(\cdot)$ and $g_k(\cdot)$ can be obtained by re-writing the (T, C_A) model equations in Eq.2 in the form of Eq.1. The explicit forms of these functions are omitted for brevity. Using a quadratic Lyapunov function of the form $V_k = e^T P_k e$, where P_k is a positive-definite symmetric matrix that satisfies the Riccati inequality $A^T P_k + P_k A - P_k b b^T P_k < 0$, we synthesize, for each control-loop, a bounded nonlinear feedback control law (see (Lin and Sontag, 1991; El-Farra and Christofides, 2001)) of the form:

$$u = -r(x, u_{max}^k) L_{\bar{g}_k} V_k \quad (4)$$

where $r(x, u_{max}^k) =$

$$\frac{L_{\bar{f}_k}^* V_k + \sqrt{(L_{\bar{f}_k}^* V_k)^2 + (u_{max}^k |L_{\bar{g}_k} V_k|)^4}}{(|L_{\bar{g}_k} V_k|)^2 \left[1 + \sqrt{1 + (u_{max}^k |L_{\bar{g}_k} V_k|)^2} \right]} \quad (5)$$

and $L_{\bar{f}_k}^* V_k = L_{\bar{f}_k} V_k + \rho |e|^2$, $\rho > 0$. The scalar function $r(\cdot)$ in Eqs.4-5 can be considered as a nonlinear controller gain. This Lyapunov-based gain, which depends on both the size of actuator constraints, u_{max}^k , and the particular configuration used is shaped in a way that guarantees constraint satisfaction and asymptotic closed-loop stability within a well-characterized region in the state space. The characterization of this region is discussed in the next step.

(b) Characterization of constrained stability regions

Given that actuator constraints place fundamental limitations on the initial conditions that can be used for stabilization, it is important for the control system designer to explicitly characterize these limitations by identifying, for each control configuration, the set of admissible initial conditions starting from where the constrained closed-loop system is asymptotically stable. As discussed in step (c) below, this characterization is necessary for the design of an appropriate switching policy that ensures the fault-tolerance of the control system. The control law designed in step (a) provides such a characterization. Specifically, using a Lyapunov argument, one can show that the set

$$\Theta(u_{max}^k) = \{x \in \mathbb{R}^n : L_{\bar{f}_k}^* V_k \leq u_{max}^k |L_{\bar{g}_k} V_k|\} \quad (6)$$

describes a region in the state space where the control action satisfies the constraints and the time-derivative of the corresponding Lyapunov function is negative-definite along the trajectories of the closed-loop system. Note that the size of this set depends, as expected, on the magnitude of the constraints. In particular, the set becomes smaller as the constraints become tighter (smaller u_{max}^k). For a given control configuration, one can use the above inequality to estimate the stability region associated with this configuration. This can be

done by constructing the largest invariant subset of Θ , which we denote by $\Omega(u_{max}^k)$. Confining the initial conditions within the set $\Omega(u_{max}^k)$ ensures that the closed-loop trajectory stays within the region defined by $\Theta(u_{max}^k)$, and thereby V_k continues to decay monotonically, for all times that the k -th control configuration is active (see (El-Farra and Christofides, 2001) for further discussion on this issue).

(c) Supervisory switching-logic

Having designed the feedback control laws and characterized the stability region associated with each control configuration, the third step is to derive the switching policy that the supervisor needs to employ to activate/deactivate the appropriate control configurations in the event of failures. The key idea here is that, because of the limitations imposed by constraints on the stability region of each configuration, the supervisor can only activate the control configuration for which the closed-loop state is within the stability region at the time of control system failure. Without loss of generality, let the initial actuator configuration be $k(0) = 1$ and let T be the time when this configuration fails, then the switching rule given by

$$k(T) = j \text{ if } x(T) \in \Omega(u_{max}^j) \quad (7)$$

for some $j \in \{2, 3, \dots, N\}$ guarantees asymptotic closed-loop stability. The implementation of the above switching law requires monitoring the closed-loop state trajectory with respect to the stability regions associated with the various actuator configurations. This idea of tying the switching logic to the stability regions was first proposed in (El-Farra and Christofides, 2002) for the control of switched nonlinear systems.

3.2 Implementation over communication networks

Figure 2 is a schematic representation of the structure and implementation of the fault-tolerant control system over a communication network. In this setting, the multiple control loops or configurations (with their sets of sensors and actuators) are connected to the process unit (e.g., the reactor) through a network cable that transmits information to and from the plant supervisor which is physically located far from the process unit (e.g., a computer in a distant control room).

The use of a network introduces additional time-delays (e.g., see (Zhang *et al.*, 2001)) between the supervisor and the constituent control configurations due to the time sharing of the communication medium as well as the computing time required for the physical signal coding and communication processing. The characteristics of these time delays depend on the network protocols adopted as well as the hardware chosen. For our purposes here, we will consider an overall fixed time-delay (which we denote by τ_{max}) that includes the contribution of several delays, including: (1) the time for fault detection and transmission of the information to the supervisor, (2) the decision time

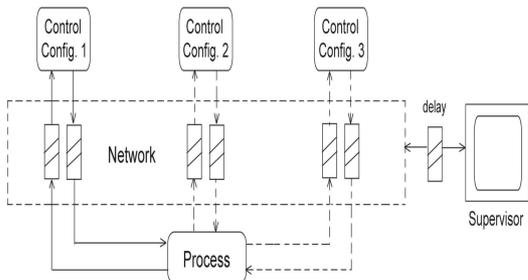


Fig. 2. Fault-tolerant control structure integrating supervisory and feedback control over network

for the supervisor, (3) the time it takes the supervisor's decision to reach and activate the target control configuration, and (4) the inherent time delays associated with the various actuators and sensors. Failure to take such delays into account can result in activating the wrong control configuration and subsequent instability. For example, even though failure of a given loop may take place at $t = T$, the backup configuration will not be switched in before $t = T + \tau_{max}$, where τ_{max} is the overall delay. If the delay is significant, then the switching rule of Eq.7 should be modified such that the supervisor activates the configuration for which $x(T + \tau_{max}) \in \Omega(u_{max}^j)$. The implementation of this rule requires that the supervisor be able to predict where the trajectory will be at $t = T + \tau_{max}$ and choose, accordingly, the appropriate configuration. This can be accomplished by running fast simulations, on-line, using the available process model.

4. SIMULATION RESULTS

In this section, we illustrate, through computer simulations, the implementation of the proposed fault-tolerant control methodology to the chemical reactor example introduced in section 2.2. We have already described in section 3.1 how the feedback controllers can be designed and the stability regions characterized for each of the three control configurations. Figure 3 depicts the stability region, in the (T, C_A) space, for each configuration. The stability region of configuration 1 includes the entire area of the plot. The stability region of configuration 2 is the entire area to the left of the solid line, while the stability region of configuration 3 covers the area to the right of the dashed vertical line. The desired steady-state is depicted with an asterisk that lies in the intersection of the three stability regions. We consider first the case where no delays are present and the supervisor can switch immediately between the different control-loops in the event of failures. To this end, the reactor is initialized at $T(0) = 300$ K, $C_A(0) = 4.0$ mol/L, $C_B(0) = 0.0$ mol/L, using the Q -control configuration, and the supervisor proceeds to monitor the evolution of the closed-loop trajectory. Due to space limitations, we present only the state profiles. As shown by the solid parts of the closed-loop trajectory in Fig.3 and the state profiles in Fig.4, the controller proceeds to drive the closed-loop trajectory towards the desired

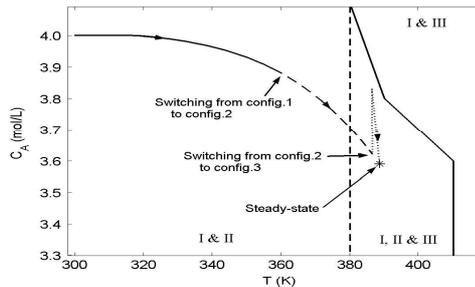


Fig. 3. Stability regions for the three control configurations (I, II, III).

steady-state, up until the Q -configuration fails after 2.0 hr of reactor startup. From the solid part of the trajectory in Fig.3, it is clear that the failure of the primary control configuration occurs when the closed-loop trajectory is within the stability region of the second control configuration, and outside the stability region of the third control configuration. Therefore, on the basis of the switching logic of Eq.7, the supervisor immediately activates the second configuration (with T_{A0} as the manipulated input). The result is shown by the dashed parts of the closed-loop trajectory in Fig.3 and the state profiles in Fig.4 where it is seen that, upon switching to the T_{A0} -configuration, the corresponding controller continues to drive the closed-loop trajectory closer to the desired steady-state. Before reaching the steady-state, however, we consider the case when a second failure occurs (this time in the T_{A0} -configuration) at $t = 15.0$ hr (which is simulated by fixing T_{A0} for all $t \geq 15.0$ hr). From the dashed part of the trajectory in Fig.3, it is clear that the failure of the second control configuration occurs when the closed-loop trajectory is within the stability region of the third configuration. Therefore, the supervisor immediately activates the third control configuration (with C_{A0} as the manipulated input) which finally stabilizes the reactor at the desired steady-state (see the dotted parts of the closed-loop trajectory in Fig.3 and the state profiles in Fig.4).

To demonstrate the effect of delays on the implementation of the switching logic, we consider an overall delay, between the supervisor and the constituent control configurations, of $\tau_{max} = 8.0$ min (accounting for delays in fault-detection, transmission and actuator activation). In this case, the reactor is initialized at $(T(0), C_A(0), C_B(0)) = (300$ K, 4.0 mol/L, 0 mol/L) under the first control configuration (with Q as the manipulated input). The actual failure of this configuration occurs at $t = 10$ hr, which, as can be seen from Fig.5, is a time when the state trajectory is within the intersection of all stability regions. In the absence of delays, this suggests that switching to either configuration 2 or 3 should preserve closed-loop stability. We observe however from Fig.6 that, when the delay is present, activation of configuration 3 leads to instability (dotted profile) while activation of configuration 2 achieves stabilization at the desired steady-state (dashed profiles). The reason is the fact that, for

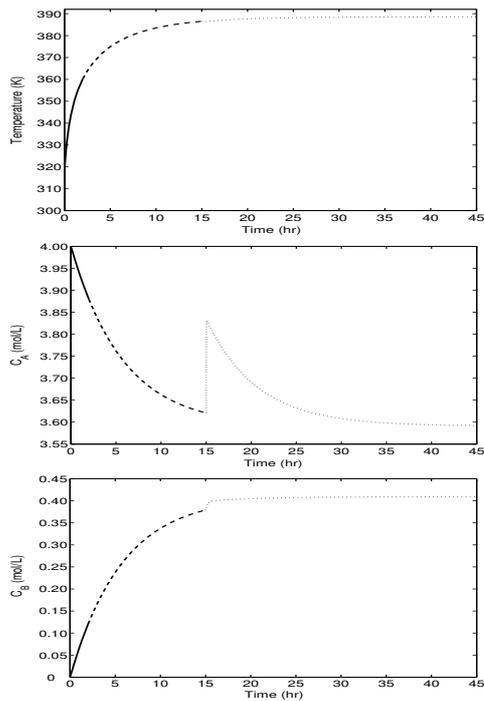


Fig. 4. Evolution of closed-loop state profiles under repeated control system failures and subsequent switching from configuration 1 (solid lines) to 2 (dashed lines) to 3 (dotted lines).

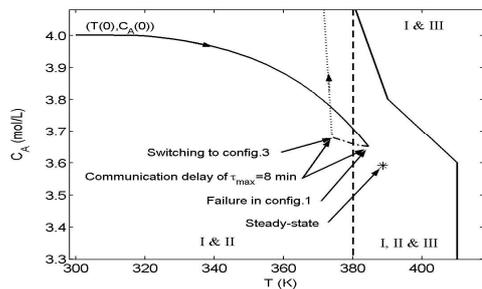


Fig. 5. A phase plot showing the closed-loop state trajectory leaving the intersection zone (I, II & III) during the delay period (dashed-dotted lines) rendering configuration 3 destabilizing (dotted trajectory).

the time period between the actual failure ($t = 10$ hr) and the activation of the backup configuration ($t = 10.13$ hr), the process evolves in an open-loop fashion leading the trajectory to move out of the intersection zone, such that at $t = 10.13$ hr, the state is within the stability region of configuration 2 and outside that of configuration 3. This is shown in Fig.5. To activate the correct configuration in this case, the supervisor needs to predict where the state trajectory will be at the end of the communication delay period.

5. REFERENCES

Bao, J., W. Z. Zhang and P. L. Lee (2002). Passivity-based decentralized failure-tolerant control. *Ind. & Eng. Chem. Res.* **41**, 5702–5715.

Bemporad, A. and M. Morari (1999). Control of systems integrating logic, dynamics and constraints. *Automatica* **35**, 407–427.

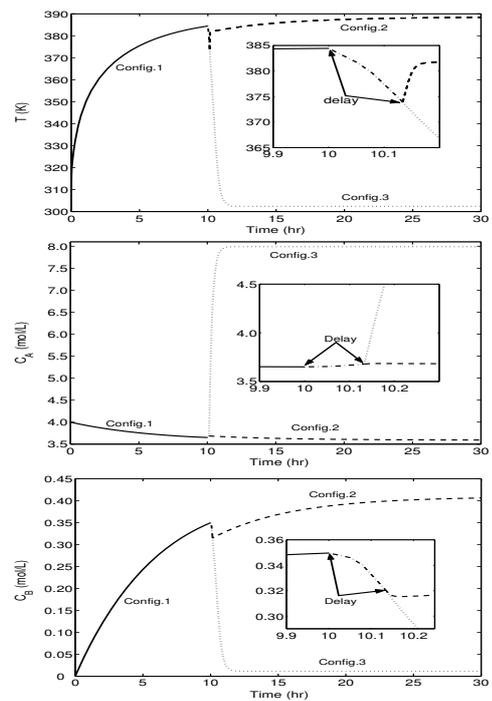


Fig. 6. Closed-loop state profiles when configuration 1 (solid lines) fails at $t = 10$ hr and an overall delay of $\tau_{max} = 8.0$ min elapses before the backup configuration is activated.

El-Farra, N. H. and P. D. Christofides (2001). Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem. Eng. Sci.* **56**, 1841–1868.

El-Farra, N. H. and P. D. Christofides (2002). Switching and feedback laws for control of constrained switched nonlinear systems. In: *Lecture Notes in Computer Science Series*. Vol. 2289. Tomlin, C. J. and M. R. Greenstreet (Eds.), Berlin, Germany: Springer-Verlag, pp. 164–178.

El-Farra, N. H. and P. D. Christofides (2003a). Coordinating feedback and switching for control of hybrid nonlinear processes, to appear. *AIChE J.*

El-Farra, N. H. and P. D. Christofides (2003b). Hybrid control of parabolic PDEs: Handling faults of constrained control actuators. In: *Lecture Notes in Computer Science Series*. Vol. 2623. Maler, O. and A. Pnueli (Eds.), Berlin, Germany: Springer-Verlag, pp. 172–187.

Lin, Y. and E. D. Sontag (1991). A universal formula for stabilization with bounded controls. *Systems & Control Letters* **16**, 393–397.

Willsky, A. S. (1998). A survey of design methods for failure detection in dynamic systems. *Automatica* **12**, 601–611.

Yang, G. H., S. Y. Zhang, J. Lam and J. Wang (1998). Reliable control using redundant controllers. *IEEE Trans. Autom. Contr.* **43**, 1588–1593.

Zhang, W., M. S. Branicky and S. M. Phillips (2001). Stability of networked control systems. *IEEE Control Systems Magazine* **21**, 84–99.