AIChE WILEY InterScience® DISCOVER SOMETHING GREAT

Integrated Fault-Detection and Fault-Tolerant Control of Process Systems

Prashant Mhaskar, Adiwinata Gani, Nael H. El-Farra, Charles McFall, Panagiotis D. Christofides, and James F. Davis
Dept. of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095

DOI 10.1002/aic.10806
Published online March 22, 2006 in Wiley InterScience (www.interscience.wiley.com).

The problem of implementing fault-tolerant control to nonlinear processes with input constraints subject to control actuator failures is considered, and an approach predicated upon the idea of integrating fault-detection, feedback and supervisory control is presented and demonstrated. To illustrate the main idea behind the proposed approach, availability of measurements of all the process state variables is initially assumed. For the processes under consideration, a family of candidate control configurations, characterized by different manipulated inputs, is first identified. For each control configuration, a Lyapunov-based 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 fault-detection filter is used to compute the expected closed-loop behavior in the absence of faults. Deviations of the process states from the expected closed-loop behavior are used to detect faults. 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 that a failure is detected. Often, in chemical process applications, not all state variables are available for measurement. To deal with the problem of lack of process state measurements, a nonlinear observer is designed to generate estimates of the states, which are then used to implement the state feedback controller and the fault-detection filter. A switching policy is then derived to orchestrate the activation/deactivation of the constituent control configurations in a way that accounts for the estimation error. Finally, simulation studies are presented to demonstrate the implementation and evaluate the effectiveness of the proposed fault-tolerant control scheme, as well as to investigate an application in the presence of uncertainty and measurement noise. © 2006 American Institute of Chemical Engineers *AIChE J,* 52: 2129–2148, 2006

Keywords: fault-tolerant control, fault-detection, input constraints, stability region, Lyapunov-based control

Introduction

Modern-day chemical plants involve a complex arrangement of processing units connected, in series and/or in parallel, and highly integrated with respect to material and energy flows through recycle streams, and to information flow through tightly interacting control approaches. Increasingly faced with the requirements of safety, reliability and profitability, chemical plant operation is relying extensively on highly automated process control systems. Automation, however, tends to also increase vulnerability of the plant to faults (for example, defects/malfunctions in process equipment, sensors and actuators, failures in the controllers or in the control loops), potentially causing a host of economic, environmental, and safety prob-

Correspondence concerning this article should be addressed to P. D. Christofides at pdc@seas.ucla.edu.

lems that can seriously degrade the operating efficiency of the plant if not addressed within a time appropriate to the context of the process dynamics. Examples include physical damage to the plant equipment, increase in the wasteful use of raw material and energy resources, increase in the downtime for process operation resulting in significant production losses, and jeopardizing personnel and environmental safety. Management of abnormal situations is a challenge in the chemical industry since abnormal situations account annually for at least $10 billion in lost revenue in the U.S. alone.[1] These considerations provide a strong motivation for the development of methods and strategies for the design of advanced fault-tolerant control structures that ensure an efficient and timely response to enhance fault recovery, prevent faults from propagating or developing into total failures, and reduce the risk of safety hazards. Given the geographically-distributed, interconnected nature of the plant units and the large number of distributed sensors and actuators typically involved,[2] the success of a fault-tolerant control method requires efficient fault detection, control designs that account for the complex nonlinear dynamics and constraints, and a high-level supervisor that coordinates the overall plant response to achieve fault-tolerant control.

Fault-tolerant control has been an active area of research for the past ten years, and has motivated many research studies in the context of aerospace engineering applications (see, for example,[3,4]), and is based on the underlying assumption of the availability of more control configurations than is required. Under this assumption, the reliable control approach dictates use of all the control loops at the same time so that failure of one control loop does not lead to the failure of the entire control structure (for example,[5]). The use of only as many control loops as is required at a time, is often motivated by economic considerations (to save on unnecessary control action), and in this case, fault-tolerant control can be achieved through control-loop reconfiguration. Recently, fault-tolerant control has gained increasing attention in the context of chemical process control; however, the available results are mostly based on the assumption of a linear process description (for example,[6,7]), and do not account for complexities such as control constraints or the unavailability of state measurements.

In process control, given the complex dynamics of chemical processes (for example, nonlinearities, uncertainties and constraints) the success of any fault-tolerant control method requires an integrated approach that brings together several essential elements, including: (1) the design of advanced feedback control algorithms that handle complex dynamics effectively, (2) the quick detection of faults, and (3) the design of supervisory switching schemes that orchestrate the transition from the failed control configuration to available well-functioning fallback configurations to ensure fault-tolerance. The realization of such an approach is increasingly aided by a confluence of recent, and ongoing, advances in several areas of process control research, including advances in nonlinear controller designs, advances in the analysis and control of hybrid process systems and advances in fault detection. In the remainder of this section, we will briefly review the state-of-the-art in these areas, as pertinent to the focus of this article.

The highly nonlinear behavior of many chemical processes has motivated extensive research on nonlinear process control. Excellent reviews of results in the area of nonlinear process control can be found, for example, in:[8,9,10]; for a more recent review, see.[11] The problems caused by input constraints have motivated numerous studies on the dynamics and control of systems subject to input constraints. Important contributions in this area include results on optimization-based control methods, such as model predictive control (for example,[12,13,14]) Lyapunov-based control (for example,[15,16,17,18,19,20]) and hybrid predictive control (for example,[21,22]).

The occurrence of faults in chemical processes and subsequent switching to fallback control configurations naturally leads to the superposition of discrete events on the underlying continuous process dynamics, thereby making a hybrid systems framework a natural setting for the analysis and design of fault-tolerant control structures. Proper coordination of the switching between multiple (or redundant) actuator/sensor configurations provides a means for fault-tolerant control. However, at this stage, despite the large and growing body of research work on a diverse array of hybrid system problems (for example,[23,24,25,26,27,28]), the use of a hybrid system framework for the study of fault-tolerant control problems for nonlinear systems subject to constraints has received limited attention. In a previous work,[29] a hybrid systems approach to fault-tolerant control was employed where, under the assumption of full state measurements and knowledge of the fault, stability region-based reconfiguration is implemented to achieve fault-tolerant control.

Existing results on the design of fault-detection filters include those that use historical plant data, and those that use fundamental process models for the purpose of fault-detection filter design. Statistical and pattern recognition techniques for data analysis and interpretation (for example,[30,31,32,33,34,35,36,37,38,39]) use historical plant data to construct indicators that identify deviations from normal operation to detect faults. The problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of linear systems;[40,41,42,43] and more recently, some existential results in the context of nonlinear systems have been derived.[44,45]

In summary, a close examination of the existing literature indicates the lack of general and practical methods for the design of integrated fault-detection and fault-tolerant control structures for chemical plants accounting explicitly for actuator/controller failures, process nonlinearities and input constraints. Motivated by these considerations, we consider in this work the problem of implementing fault-tolerant control on nonlinear processes with input constraints subject to control actuator failures, and present and demonstrate an approach predicated upon the idea of integrating fault-detection, feedback and supervisory control. To illustrate the main idea behind the proposed approach, we first assume availability of measurements of all the process state variables. For the processes under consideration, a family of candidate control configurations, characterized by different manipulated inputs, is first identified. For each control configuration, a Lyapunov-based 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 fault-detection filter is used to compute the expected closed-loop behavior in the absence of faults. Deviations of the process states from the expected closed-loop behavior are used to detect faults. 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 that a failure is detected. Often, in chemical process applications, not all state variables are available for measurement. To deal with the problem of missing but needed process state measurements, a nonlinear observer is designed to generate estimates of the states, which are then used to implement the state feedback controller and the fault-detection filter. A switching policy is then derived to orchestrate the activation/deactivation of the constituent control configurations in a way that accounts for the estimation error. Finally, simulation studies are presented to demonstrate the implementation and evaluate the effectiveness of the proposed fault-tolerant control scheme as well as to investigate an application in the presence of uncertainty and measurement noise.

Preliminaries

Process description

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

$$\dot{x}(t) = f(x(t)) + g_{k(t)}(x(t))(u_{k(t)} + m_{k(t)}), \quad y_m = h_m(x)$$
$$k(t) \in \mathcal{K} = \{1, \ldots, N\}, \quad N < \infty, \quad |u_{k(t)}| \leq u^k_{\max} \quad (1)$$

where $x(t) \in \mathbb{R}^n$ denotes the vector of process state variables, $y_m \in \mathbb{R}$ denotes the measured variable, $u_k(t) \in [-u^k_{\max}, u^k_{\max}] \subset \mathbb{R}$ denotes the constrained manipulated input associated with the k-th control configuration, and $m_{k(t)} \in \mathbb{R}$ denotes the fault in the k-th control configuration. For each value that k assumes in $\mathcal{K}$, the process is controlled via a different manipulated input which defines a given control configuration.

It is assumed that the origin is the equilibrium point of the nominal process (that is, $f(0) = 0$), $g_k(x) \neq 0 \; \forall x \in \mathbb{R}^n$, and that the vector functions $f(\cdot)$ and $g_k(\cdot)$ are sufficiently smooth, for all k, on $\mathbb{R}^n$. Throughout this article, a function $\beta(r, s)$ is said to belong to class $\mathcal{KL}$ if, for each fixed s, the mapping $\beta(\cdot, s)$ belongs to class $\mathcal{K}$ (a continuous function $\alpha(\cdot)$ is said to belong to class $\mathcal{K}$ if it is strictly increasing, and $\alpha(0) = 0$) and for each fixed r, the mapping $\beta(r, \cdot)$ is decreasing, and $\beta(r, s) \to 0$ as $s \to \infty$; see also.[46] The notation $\|\cdot\|$ is used to denote the standard Euclidean norm of a vector, the notation $|\cdot|$ is used to denote the absolute value of a scalar, x' denotes the transpose of x, and the notation $R = [r_1 \quad r_2]$ is used to denote the augmented vector $R \in \mathbb{R}^{m+n}$ comprising of the vectors $r_1 \in \mathbb{R}^m$, and $r_2 \in \mathbb{R}^n$. The notation $L_f h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $f(\cdot)$, and the notation $x(T^+)$ denotes the limit of the trajectory $x(t)$ as T is approached from the right, that is, $x(T^+) = \lim_{t \to T^+} x(t)$. Throughout the manuscript, we assume that for any $|u_k| \leq u^k_{\max}$ the solution of the system of Eq. 1 exists, and is continuous for all t.

Motivating example

To motivate our fault-tolerant control design methodology, we introduce in this subsection a bench-mark chemical reactor example that will be used to illustrate the design and implementation of the fault-tolerant control structure. To this end, consider a well-mixed, nonisothermal continuous stirred tank reactor (see Figure 1), 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. Under standard modeling assumptions, a mathematical model of the process can be derived from material and energy balances and takes the following form

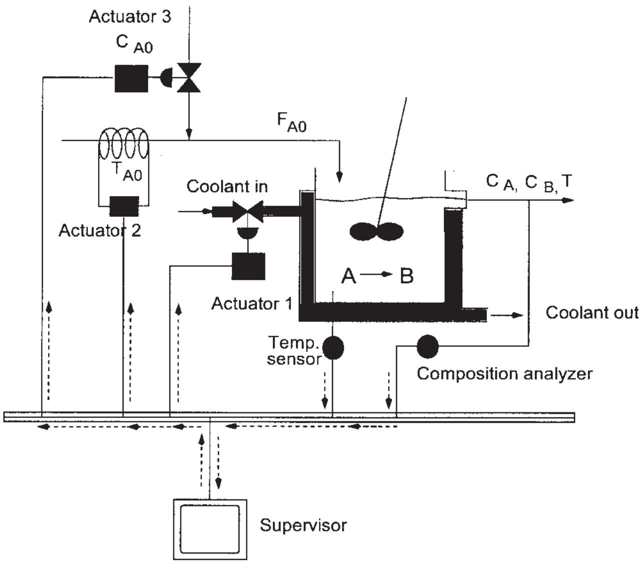


Figure 1. CSTR showing the three candidate control configurations.

$$\frac{dT}{dt} = \frac{F}{V}(T_{A0} - T) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} k_{i0} \exp\left(\frac{-E_i}{RT}\right) C_A + \frac{Q}{\rho c_p V}$$

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^{3} k_{i0} \exp\left(\frac{-E_i}{RT}\right) C_A$$

$$\frac{dC_B}{dt} = -\frac{F}{V} C_B + k_{10} \exp\left(\frac{-E_1}{RT}\right) C_A \quad (2)$$

where C_A and C_B denote the concentrations of the species A and B, T denotes the temperature of the reactor, Q denotes the 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 fluid in the reactor, respectively. The values of the process parameters and the corresponding steady-state values can be found in.[29] 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}) = (388.57 K, 3.59 kmol/m^3, 0.41 kmol/m^3)).

The control objective considered here is the one of stabilizing the reactor at the (open-loop) unstable steady-state. Operation at this point is typically sought to avoid high temperature while simultaneously achieving reasonable conversion. To accomplish this objective in the presence of control system failures, we consider as manipulated inputs the rate of heat input, $u_1 = Q$, subject to the constraint $|Q| \leq u_{max}^1 = 748$ KJ/s, the inlet stream temperature, $u_2 = T_{A0} - T_{A0s}$, subject to the constraint $|u_2| \leq u_{max}^2 = 100$ K, with $T_{A0s} = 300$ K, and the inlet reactant concentration, $u_3 = C_{A0} - C_{A0s}$, subject to the constraint $|u_3| \leq u_{max}^3 = 4$ kmol/m^3, with $C_{A0s} = 4$ kmol/m^3.

Each of these manipulated inputs, together with measurements of reactor temperature and/or concentration, represents a unique control configuration (or control-loop) that, by itself, can stabilize the reactor. In the event of some failure in the primary configuration (involving the heat input Q), the important questions that arise include how can the supervisor detect this fault (note that measurements of the control actuator output that is implemented on the process are not available), and which control loop to activate once failure is detected in the active configuration. The answer to the first question involves the design of an appropriate fault-detection filter. The approach that we will utilize to answer the second question—that of deciding which backup controller should be activated in the event of a fault—will be based on the stability regions under the individual control configuration. To this end, we next review a state feedback control design that allows for characterizing the constrained stability region under each control configuration. Note that this particular choice of the controller is presented only as an example to illustrate our results, and that any other controller design that allows for an explicit characterization of the constrained stability region can be used instead. Note also, that while the earlier example will be used to illustrate the main ideas behind the proposed fault-detection and fault-tolerant control method, we also investigate in the simulation studies an application to a network of chemical reactors in the presence of uncertainty and measurement noise.

Bounded Lyapunov-based control

Consider the system of Eq. 1, for which a family of control Lyapunov functions (CLFs), $V_k(x)$, $k \in \mathcal{K} \equiv \{1, \ldots, N\}$ has been found (see the last paragraph of this subsection for a discussion on the construction of CLFs). Using each control Lyapunov function, we construct, using the results in[15] (see also[19]), the following continuous bounded control law

$$u_k(x) = -\frac{L_f^* V_k(x) + \sqrt{(L_f^* V_k(x))^2 + (u_{\max}^k \|(L_{g_k} V_k)(x)\|)^4}}{\|(L_{g_k} V_k)(x)\|^2 [1 + \sqrt{1 + (u_{\max}^k \|(L_{g_k} V_k)(x)\|)^2}]} \times (L_{g_k} V_k)(x) \quad (3)$$

when $(L_{g_k} V_k)(x) \neq 0$ and $u_k(x) = 0$ when $(L_{g_k} V_k)(x) = 0$, $L_f^* V_k(x) = [\partial V_k(x)/\partial x] f(x) + \rho_k V_k(x)$, $\rho_k > 0$ and $L_{g_k} V_k(x) = [\partial V_k(x)/\bar{\partial} x] g_k(x)$. Let Π_k be the set defined by

$$\Pi_k(u_{\max}^k) = \{x \in \mathbb{R}^n : L_f^* V_k(x) \leq u_{\max}^k \|(L_{g_k} V_k)(x)\|\} \quad (4)$$

and assume that

$$\Omega_k := \{x \in \mathbb{R}^n : V_k(x) \leq c_k^{\max}\} \subseteq \Pi_k(u_{\max}^k) \quad (5)$$

for some $c_k^{\max} > 0$. It can be shown, using standard Lyapunov arguments, that in the absence of faults ($m_{k(t)} = 0$), Ω_k provides an estimate of the stability region, starting from where the control law of Eq. 3 guarantees asymptotic (and local exponential) stability of the origin of the closed-loop system under each control configuration. This implies that there exist class $\mathcal{KL}$ functions β_i, $i = 1, \ldots, N$, such that $\|x(t)\| \leq \beta_i(\|x(0)\|, t)$. We will use this property later in the design of the output feedback controllers.

Referring to the earlier controller design, it is important to make the following remarks. First, a general procedure for the construction of CLFs for nonlinear systems of the form of Eq. 1 is currently not available. Yet, for several classes of nonlinear systems that arise commonly in the modeling of engineering applications, it is possible to exploit system structure to construct CLFs (see, for example,[47,48]). Second, given that a CLF, V_k, has been obtained for the system of Eq. 1, it is important to clarify the essence and scope of the additional assumption that there exists a level set, Ω_k, of V_k that is contained in Π_k. Specifically, the assumption that the set, Π_k, contains an invariant subset around the origin, is necessary to guarantee the existence of a set of initial conditions for which closed-loop stability is guaranteed (note that even though $\dot{V}_k < 0 \ \forall x \in \Pi_k \backslash \{0\}$, there is no guarantee that trajectories starting within Π_k remain within Π_k for all times). Moreover, the assumption that Ω_k is a level set of V_k is made only to simplify the construction of Ω_k. This assumption restricts the applicability of the proposed control method because a direct method for the construction of a CLF with level sets contained in Π_k is not available. However, the proposed control method remains applicable if the invariant set Ω_k is not a level set of V_k, but can be constructed in some other way (which, in general, is a difficult task). Note also that possibly larger estimates of the stability region can be computed using constructive procedures such as Zubov's method[49] or by using a combination of several Lyapunov functions.

Integrated Fault-Detection and Fault-Tolerant Control: State Feedback Case

State feedback fault-tolerant control

Consider the system of Eq. 1, where all process states are available as measurements, that is, $h_m(x) = x$, and without loss of generality, assume that it starts operating using control configuration i, under the controller of Eq. 3. At some unknown time, T_i^f, a fault occurs in the first control configuration such that for all $t \geq T_i^f$, $m_i = -u_i$, that is, control configuration i fails. The problems at hand are those of detecting that a fault has occurred and, upon detection, deciding which of the available backup configurations should be implemented in the closed-loop to achieve fault-tolerant control. To this end, we consider a fault-detection filter and a switching logic of the form

$$\dot{w}(t) = f_f(w, x), \quad r(t) = h_f(w, x), \quad k(t) = \varphi(r, w, x) \quad (6)$$

where $w \in \mathbb{R}^n$ is the state of the filter, $r(t) \in \mathbb{R}$ is a residual that indicates the occurrence of a fault, and is the output of the filter, $f_f \in \mathbb{R}^n$ is the vector field describing the evolution of the filter state w, and $\varphi(r, w, x)$ is the switching logic that dictates which of the available control configurations should be activated.

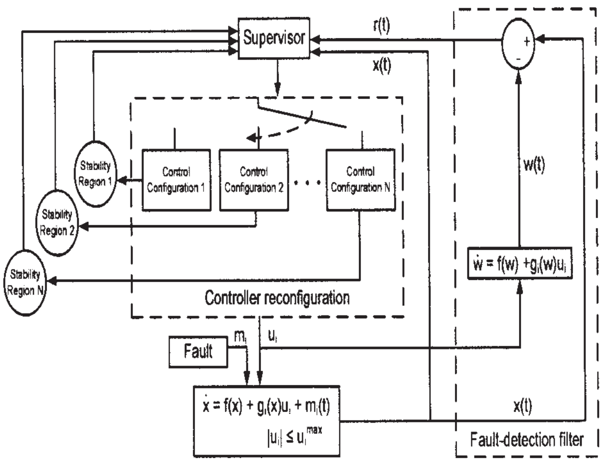


Figure 2. Integrated fault-detection and fault-tolerant control design: state feedback case.

The main idea behind the fault-tolerant control design is as follows: (1) use the available state measurements, the process model, and the computed control action to simulate the evolution of the closed-loop process in the absence of actuator faults, compare it with the actual evolution of the states, and use the difference between the two behaviors, if any, to detect faults, and (2) having detected the fault, activate a backup control configuration for which the closed-loop state is within its stability region estimate. To formalize this idea, consider the constrained system of Eq. 1 for which a bounded controller of the form of Eq. 3 has been designed for each control configuration, and the stability region, Ω_j, $j = 1, \ldots, N$ has been explicitly characterized. The fault-detection filter and the fault-tolerant control design are described in Theorem 1 below. The proof is given in the Appendix.

Theorem 1: *Let $k(0) = i$ for some $i \in \mathcal{K}$ and $x(0) := x_0 \in \Omega_i$. Set $w(0) = x(0)$, and consider the system*

$$\dot{w} = f(w) + g_i(w)u_i(w); \quad r = \|w - x\| \tag{7}$$

where $w \in \mathbb{R}^n$ is the filter state and $u_i(\cdot)$ is the feedback control law defined in Eq. 3. Let T_i^f be such that $m_i(t) = 0$ $\forall 0 \leq t \leq T_i^f$, then $r(T_i^{f+}) > 0$ if and only if $m_i(T_i^f) \neq 0$. Furthermore, let T_i^s be the earliest time such that $r(t) > 0$, then the following switching rule

$$k(t) = \begin{Bmatrix} i, & 0 \leq t < T_i^s \\ j \neq i, & t \geq T_i^s, x(T_i^s) \in \Omega_j \end{Bmatrix} \tag{8}$$

guarantees asymptotic stability of the origin of the closed-loop system.

The fault-detection filter and fault-tolerant controller are designed and implemented as follows (see also Figure 2):

- Given any $x_0 \in \Omega_i$, initialize the filter states as $w(0) = x_0$, and integrate the filter dynamics using Eq. 7.
- Compute the norm of the difference between the filter states and the process states, $r(t) = \|w(t) - x(t)\|$, and if $r(t) = 0$, continue to implement control configuration i.
- At any time T_i^s that $r(T_i^s) > 0$, switch to a control configuration $j \neq i$, for which $x(T_i^s) \in \Omega_j$ to achieve asymptotic stability of the origin of the closed-loop system.

Note that the fault-detection filter uses a replica of the process dynamics, and that the state of the filter w is initialized at the same value as the process states $x(0)$. In the absence of faults, the evolution of $w(t)$ is identical to $x(t)$, and, hence, $r(t) = 0$. In the presence of faults, however, the effect of the fault is registered by a change in the evolution of the process, but not in that of the filter state (since the filter state dynamics include the computed control action, $u_i(w)$, and not the implemented control action, $u_i(w) + m_i$). This change is detected by a change in the value of $r(t)$, and declared as a fault. Note also, that the fact that the faults m_i appear as additive terms to the manipulated input variable is a natural consequence of focussing on the problem of detecting (through the design of appropriate fault-detection filters) and dealing (via reconfiguration) with faults in control actuators. The approach employed in the design of the fault-detection filter can also be used to detect faults that do not necessarily appear in the control actuators, as long as they influence the evolution of the state variables.

Remark 1: Once a fault is detected, the switching logic ensures that the backup control configuration that is implemented in the closed-loop system is one that can guarantee closed-loop stability in the presence of constraints, and this is achieved by verifying that the state of the process, at the time that a fault is detected, is present in the constrained stability region of the candidate control configuration. Note that while the bounded controller is used for a demonstration of the main ideas, other control approaches, that provide an explicit characterization of the set of initial conditions for which closed-loop stability is guaranteed (achieved, for example, via the use of the hybrid predictive control approach[21] or via a Lyapunov-based model predictive control design[50]) can be used within the proposed framework. Note also that early detection of a fault enhances the chances that corrective action can be taken in time to achieve fault-tolerant control (Theorem 1 guarantees that a fault is detected as soon as it occurs). Specifically, it may happen that a fault occurs when the closed-loop state resides in the stability region of one of the backup configurations, but if the fault is not immediately detected, the destabilizing effect of the fault may drive the state outside the stability region of the backup configuration by the time a fault is detected (for a demonstration, see the simulation example).

In the event that the process state, at the time of the failure of the primary control configuration, lies in the stability region of more than one backup control configuration, additional performance considerations such as ease and/or cost of implementing one control configuration over another, can be used in choosing which control configuration should be implemented in the closed-loop system.[51] If the state at the time of a failure lies outside the stability region of all the backup controllers, then this indicates that the backup controllers do not have enough control action available and calls for increasing the allowable control action in the fallback configurations. Note that the set of initial conditions starting from where a given control configuration can stabilize a steady state—the so-called null-controllable region—is fundamentally limited by the constraints on the available control action, and that different control laws typically provide estimates of the stability region which are subsets of the null-controllable region.

Remark 2: In the presence of plant model mismatch or unknown disturbances, the value of $r(t)$ will be nonzero even in the absence of faults. The fault-detection and fault-tolerant control (FDFTC) problem in the presence of time varying disturbances with known bounds on the disturbances can be handled by (1) redesigning the filter to account for the disturbances; specifically, requiring that a fault be declared only if the value of $r(t)$ increases beyond some threshold δ, where δ accounts for the deviation of the plant dynamics from the nominal dynamics in the absence of faults (please see the simulation example for a demonstration of this idea in an application to a network of chemical reactors in the presence of uncertainty and measurement noise), and (2) by redesigning the controllers for the individual control configurations to mitigate the effect of disturbances on the process characterizing the robust stability regions and using them as criteria for deciding which backup controller should be implemented in the closed-loop. Note that while Theorem 1 presents the FDFTC design for a fault in the primary control configuration, extensions to faults in successive backup configurations are straightforward and involve similar filter designs for the active control configuration and a switching logic that orchestrates switching to the remaining control configurations.

Remark 3: While we illustrate our idea using a single input, extensions to multi-input systems are possible, and fault-detection filters can be designed in the same way, using a replica of the process dynamics. The case of multi-input systems, however, introduces an additional layer of complexity due to the need of identifying which particular manipulated input has failed, that is, the additional problem of fault-isolation. For the purpose of presenting the integrated fault-detection and fault-tolerant control structure, we focus here on multiple control configurations, where each control configuration comprises of a single input that does not require the filter to perform the additional task of fault-isolation. For a simple illustration of a fault-detection and isolation filter design, see the simulation example.

Remark 4: Note that the fault-detection filter presented in Theorem 1 detects the presence of both complete and partial failures. Once a fault is detected, the control reconfiguration strategy is the same for both cases, and that is to shut down the faulty configuration and switch to some well-functioning fallback configuration. Note that in the case of a partial failure, unless the faulty configuration is shut down, the backup control configurations will have to be redesigned to be robust with respect to the bounded disturbance generated by the faulty configuration (for the backup control configuration, the unmeasured actuator action of the faulty control configuration will act as a disturbance and will be bounded because of the fact that the actuator itself has a limited capacity and, therefore, even if the implemented control action is not the same as that prescribed by the controller, it cannot exceed the physical limitations and will remain bounded). By shutting down the faulty configuration, however, the source of the disturbance is eliminated and no controller redesign is needed for the backup control configurations.

Simulation results

In this subsection, we illustrate the implementation of the proposed fault-detection/fault-tolerant control methodology to the chemical reactor introduced as a motivating example. We first describe the controller design for the individual control configurations. Note that our objective is full state stabilization; however, to facilitate the controller design and subsequent stability analysis, we use a state transformation to transform the system of Eq. 2 into the following one describing the input/output dynamics

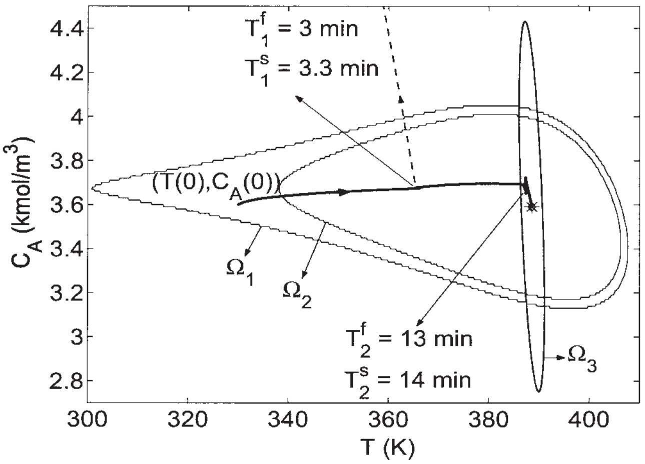


Figure 3. Evolution of the closed-loop state profiles under the switching rule of Eq. 8 subject to failures in control systems 1 and 2 (solid line) and under arbitrary switching (dashed line).

$$\dot{e} = Ae + l(e) + b\alpha_k u_k := \bar{f}(e) + \bar{g}_k(e)u_k \qquad (9)$$

where $e \in \mathbb{R}^n$ is the variable in transformed co-ordinate (for the specific transformations used for each control configuration, please see below), $A = [\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}]$, $b = [\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}]$, $l(\cdot) = L_f^2 h_k(x)$, $\alpha_k(\cdot) = L_{g_k} L_f h_k(x)$, $h_k(x) = y_k$ is the output associated with the k-th configuration, $x = [x_1 \quad x_2]^T$ with $x_1 = T - T_s$, $x_2 = C_A - C_{As}$, and the functions $f(\cdot)$ and $g_k(\cdot)$ can be obtained by rewriting 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. 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 $A^T P_k + P_k A - P_k b b^T P_k < 0$, is used for controller design. In particular:

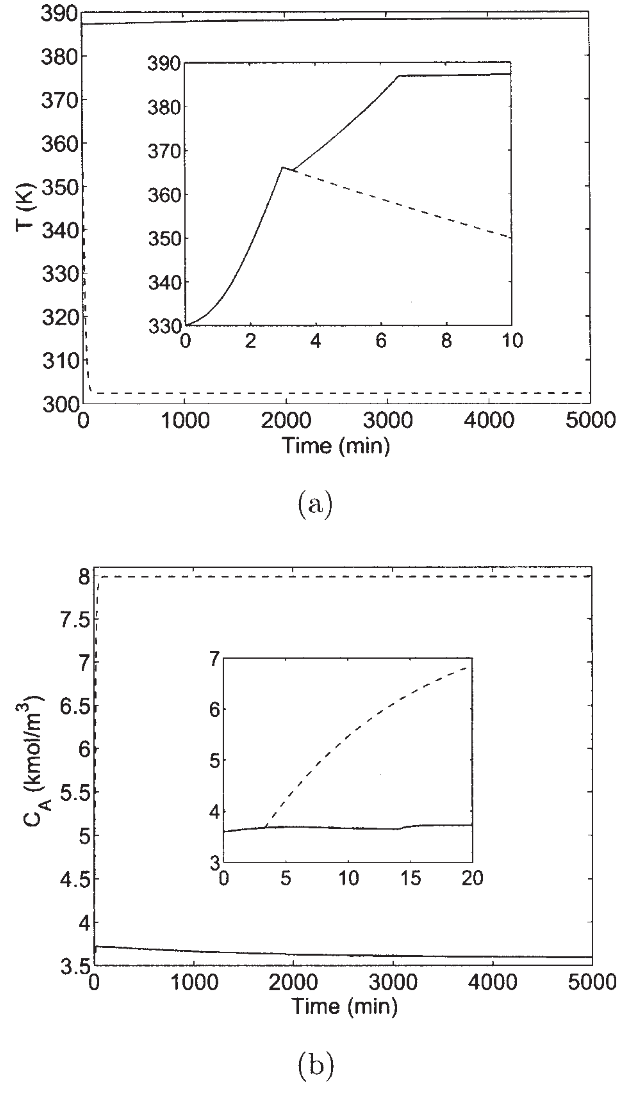
1. For the first configuration with $u_1 = Q$, we consider the controlled output $y_1 = C_A - C_{As}$. The coordinate transformation (in error variables form) takes the form: $e_1 = C_A - C_{As}$, $e_2 = (F/V)(C_{A0} - C_A) - \Sigma_{i=1}^3 k_{i0} e^{(-E_i/RT)} C_A$, and yields a relative degree of two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

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 $u_3 = C_{A0} - C_{A0s}$, a coordinate transformation of the form used for configurations 1 and 2 earlier does not yield a sufficiently large estimate of the stability region, we therefore choose a candidate Lyapunov function of the form $V_3(x) = x'Px$, where $P > 0$, and $x = [T - T_s \quad C_A - C_{As}]'$ with $P = [\begin{smallmatrix} 0.011 & 0.019 \\ 0.019 & 0.101 \end{smallmatrix}]$.

Figure 3 depicts the stability region, in the (T, C_A) space, for each configuration. The desired steady-state is depicted with an asterisk that lies in the intersection of the three stability regions. The reactor, as well as the fault-detection filter for the first control configuration is initialized at $T(0) = 330$ K, $C_A(0) = 3.6$ kmol/m^3, $C_B(0) = 0.0$ kmol/m^3, using the Q-control configuration, and the supervisor proceeds to monitor the evolution of the closed-loop trajectory.

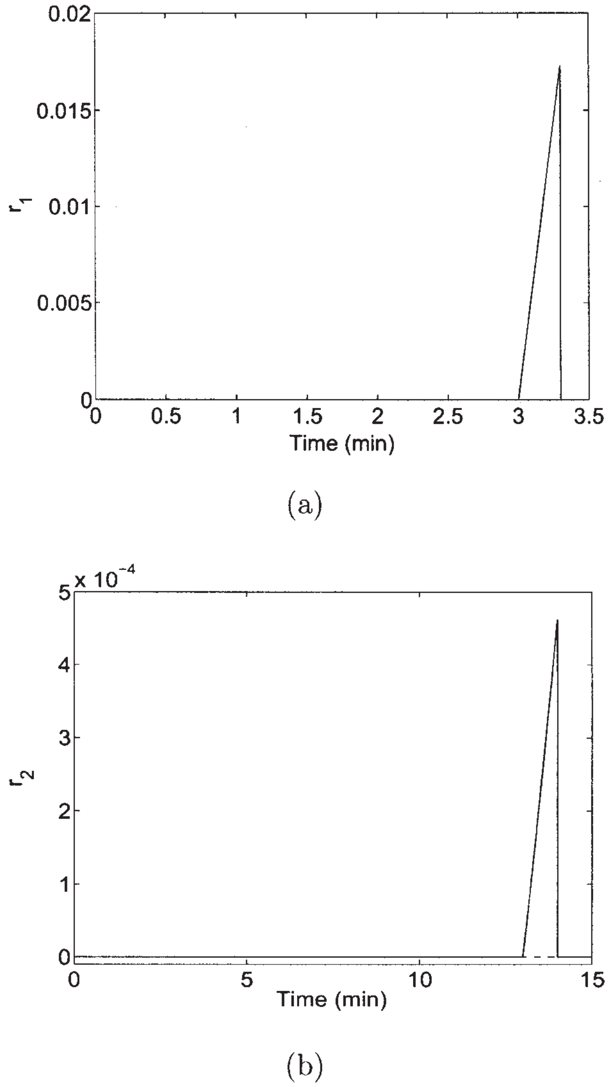
As shown by the solid lines in Figures 3–4, the controller proceeds to drive the closed-loop trajectory towards the desired steady-state, until the Q-configuration fails after 3 min of reactor startup (see Figure 6a). As can be seen in Figure 5a, at this time the value of $r_1(t)$ becomes non-zero, and the fault-detection filter detects this fault. If the supervisor switches arbitrarily, and in particular, switches to backup configuration 3, closed-loop stability is not achieved (dashed lines in Figures 3–4). Note that this happens because the closed-loop state is outside the stability region of the third control configuration, and even though the third control configuration does not encounter a fault ($r_3(t) = 0$; see dashed line in Figure 5b), the limited control action available in this configuration is unable to achieve closed-loop stability. On the basis of the switching logic of Eq. 8, the supervisor activates the second configuration (with T_{A0} as the manipulated input, see Figure 6b), which continues to drive the state trajectory closer to the desired steady-state.



(a)

(b)

Figure 4. Evolution of the closed-loop (a) temperature and (b) concentration under the switching rule of Eq. 8 subject to failures in control systems 1 and 2 (solid lines), and under arbitrary switching (dashed lines).



(a)

(b)

Figure 5. Evolution of the closed-loop residual under the fault-detection filter for (a) control configuration 1, and (b) control configurations 2 and 3 under the switching rule of Eq. 8 subject to failures in control systems 1 and 2 (solid lines), and under arbitrary switching (dashed lines).

To demonstrate the implementation of the proposed FDFTC strategy when faults occur in successive control configurations, we consider the case when a second failure occurs (this time in the T_{A0}-configuration) at $t = 13$ min. Once again, the filter detects this failure via an increase in the value of $r_2(t)$ (solid line in Figure 5b) using the fault-detection filter for control

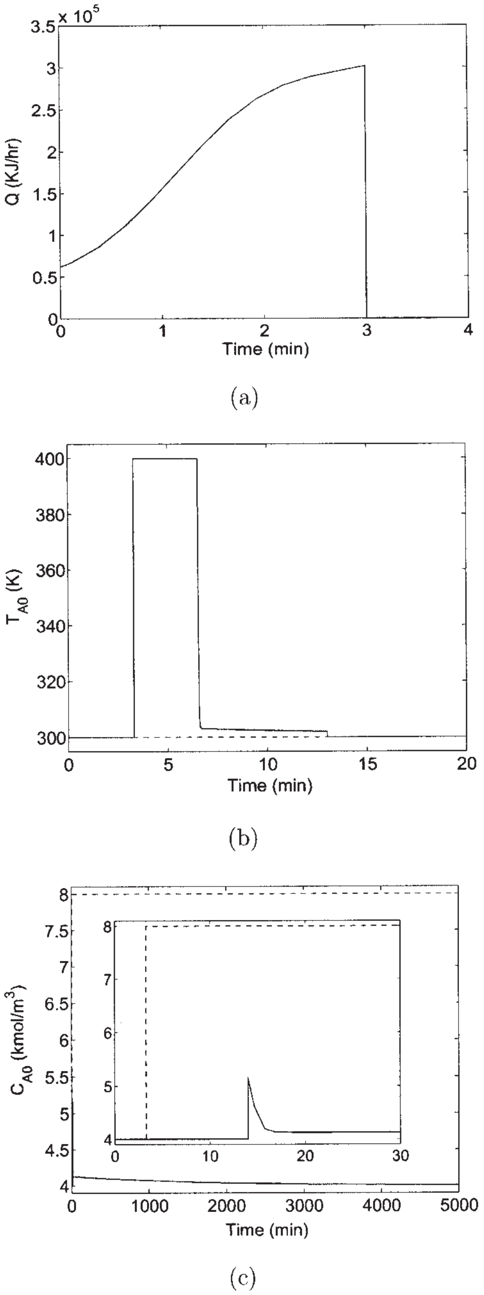


Figure 6. Manipulated input profiles under (a) control configuration 1, (b) control configuration 2, and (c) control configuration 3 under the switching rule of Eq. 8 subject to failures in control systems 1 and 2 (solid lines), and under arbitrary switching (dashed lines).

configuration 2. From Figure 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, see Figure 6c) which finally stabilizes the reactor at the desired steady-state.

Integrated Fault-Detection and Fault-Tolerant Control: Output Feedback Case

The feedback controllers, the fault-detection filters and the switching rules in the previous section were designed under the assumption of availability of measurements of all the process states. The unavailability of full state measurements has several implications. First, it necessitates generating estimates of the states to be used in conjunction with both the state feedback controller and the fault-detection filter. The state estimates, however, contain errors, and this results in a difference between the expected closed-loop behavior of the measured variables (computed using the state estimates) and the evolution of the measured variables, even in the absence of actuator faults. The fault-detection filter has to be redesigned to account for this fact so that it does not treat this difference to be an indicator of an actuator fault (i.e., a false alarm). Also, the switching logic has to account for the fact that the supervisor can monitor only the state estimates and needs to make inferences about the true values of the states using the state estimates.

In the remainder of this section, we first review an output feedback controller design, proposed in,[20] based on a combination of a high-gain observer and a state feedback controller (see also[52,53,54,55,56] for results on observer designs and output feedback control for unconstrained nonlinear systems), and characterize the stability properties of the closed-loop system under output feedback control. Then, we present the fault-detection filter and fault-tolerant controller and demonstrate its application via a simulation example.

Output feedback control

To facilitate the design of a state estimator with the required convergence properties, we make the following assumption:

Assumption 1: *For each $i \in \mathcal{K}$, there exists a set of coordinates*

$$[\xi_i] = \begin{bmatrix} \xi_i^1 \\ \xi_i^2 \\ \vdots \\ \xi_i^n \end{bmatrix} = \chi_i(x) = \begin{bmatrix} h_m(x) \\ L_f h_m(x) \\ \vdots \\ L_f^{n-1} h_m(x) \end{bmatrix} \tag{10}$$

such that the system of Eq. 1 takes the form

$$\begin{aligned} \dot{\xi}_i^1 &= \xi_i^2 \\ &\vdots \\ \dot{\xi}_i^{n-1} &= \xi_i^n \\ \dot{\xi}_i^n &= L_f^n h_m(\chi_i^{-1}(\xi)) + L_{g_i} L_f^{n-1} h_m(\chi_i^{-1}(\xi))(u_{i(t)} + m_{i(t)}) \end{aligned} \tag{11}$$

where $L_{g_i} L_f^{n-1} h_m(x) \neq 0$ for all $x \in \mathbb{R}^n$. Also, $\xi_i \to 0$ if and only if $x \to 0$.

We note that the change of variables is invertible, since for every x, the variable ξ_i is uniquely determined by the transformation $\xi_i = \chi_i(x)$. This implies that if one can estimate the values of ξ_i for all times, using an appropriate state observer, then we automatically obtain estimates of x for all times which can be used to implement the state feedback controller. The existence of such a transformation will facilitate the design of high-gain observers which will be instrumental in preserving the same closed-loop stability properties achieved under full state feedback.

Proposition 1 below presents the output feedback controller used for each mode and characterizes its stability properties. The proof of the proposition, which invokes singular perturbation arguments (for a result on input-to-state stability with respect to singular perturbations, and further references, see[57]), is a special case of the proof of Theorem 2 in,[20] and is omitted for brevity. To simplify the statement of the proposition, we first introduce the following notation. We define $\alpha_i(\cdot)$ as a class $\mathcal{K}$ function that satisfies $\alpha_i(\|x\|) \leq V_i(x)$. We also define the set $\Omega_{b,i} := \{x \in \mathbb{R}^n : V_i(x) \leq \delta_{b,i}\}$, where $\delta_{b,i}$ is chosen such that $\beta_i(\alpha_i^{-1}(\delta_{b,i}), 0) < \alpha_i^{-1}(c_i^{max})$, where $\beta_i(\cdot, \cdot)$ is a class $\mathcal{KL}$ function and c_i^{max} is a positive real number defined in Eq. 5.

Proposition 1: *Consider the nonlinear system of Eq. 1, for a fixed mode, $k(t) = i$, and with $m_i(t) \equiv 0$, under the output feedback controller:*

$$\dot{\tilde{y}} = \begin{bmatrix} -L_i a_1^{(i)} & 1 & 0 & \cdots & 0 \\ -L_i^2 a_2^{(i)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -L_i^n a_n^{(i)} & 0 & 0 & \cdots & 0 \end{bmatrix} \tilde{y} + \begin{bmatrix} L_i a_1^{(i)} \\ L_i^2 a_2^{(i)} \\ \vdots \\ L_i^n a_n^{(i)} \end{bmatrix} y_m$$

$$u_i = u_i^c(\hat{x}) \tag{12}$$

where u_i^c is defined in Eq. 3, the parameters, $a_1^{(i)}, \ldots, a_n^{(i)}$ are chosen such that the polynomial $s^n + a_1^{(i)}s^{n-1} + a_2^{(i)}s^{n-2} + \ldots + a_n^{(i)} = 0$ is Hurwitz, $\hat{x} = \chi_i^{-1}(sat(\tilde{y}))$, $sat(\cdot) = \min\{1, \zeta_{max,i}/|\cdot|\}(\cdot)$, with $\zeta_{max,i} = \beta_\zeta(\delta_{\zeta,i}, 0)$ where β_ζ is a class $\mathcal{KL}$ function and $\delta_{\zeta,i}$ is the maximum value of the norm of the vector $[h_m(x) \ldots L_f^{n-1}h_m(x)]$ for $V_i(x) \leq c_i^{max}$ and let $\varepsilon_i = 1/L_i$. Then, given $\Omega_{b,i}$, there exists $\varepsilon_i^* > 0$ such that if $\varepsilon_i \in (0, \varepsilon_i^*]$, $x(0) \in \Omega_{b,i}$, and $\|\tilde{y}(0)\| \leq \delta_{\zeta,i}$, the origin of the closed-loop system is asymptotically (and locally exponentially) stable. Furthermore, given any positive real numbers, $e_{m,i}$ and T_i^b, there exists a real positive number ε_i^{**} such that if $\varepsilon_i \in (0, \varepsilon_i^{**}]$ then $\|x(t) - \hat{x}(t)\| \leq e_{m,i}$ for all $t \geq T_i^b$.

The state observer in Eq. 12 ensures sufficiently fast convergence of the state estimation error necessary for the implementation of both the state feedback controller (and preserving its stability properties under output feedback control), and the fault-detection filter. The most important feature of this estimator (and one that will be used in the fault-detection filter design) is that the estimation error is guaranteed to fall below a certain value in a small period of time T_i^b, which can be chosen arbitrarily small by sufficiently increasing the observer gain. This requirement or constraint on the error dynamics is needed even when other estimation schemes, such as moving horizon observers, are used in the context of estimation-based output feedback control (for example, see[58,59]). For such observers, however, it is difficult in general to obtain a transparent relationship between the tunable observer parameters and the error decay rate.

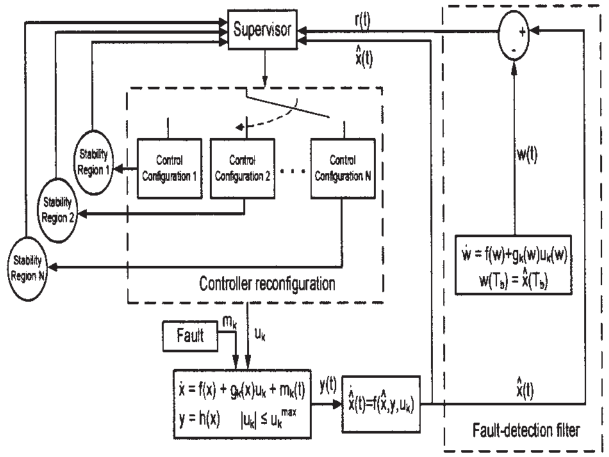


Figure 7. Integrated fault-detection and fault-tolerant control design under output feedback.

Due to the lack of full state measurements, the supervisor can rely only on the available state estimates to decide whether switching at any given time is permissible, and, therefore, needs to make reliable inferences regarding the position of the states based upon the available state estimates. Proposition 2 below establishes the existence of a set, $\Omega_{s,i} := \{x \in \mathbb{R}^n : V_i(x) \leq \delta_{s,i}\}$, such that once the state estimation error has fallen below a certain value (note that the decay rate can be controlled by adjusting L_i), the presence of the state within the output feedback stability region, $\Omega_{b,i}$, can be guaranteed by verifying the presence of the state estimates in the set $\Omega_{s,i}$. A similar approach was employed in the construction of the output feedback stability regions $\Omega_{b,i}$, and the regions for the state estimates $\Omega_{s,i}$ in the context of output feedback control of linear systems in [60]. The proof of the proposition is given in the appendix.

Proposition 2: *Given any positive real number $\delta_{b,i}$, there exist positive real numbers $e_{m,i}^*$ and $\delta_{s,i}$ such that if $\|x - \hat{x}\| \leq e_{m,i}$, where $e_{m,i} \in (0, e_{m,i}^*]$, and $V_i(\hat{x}) \leq \delta_{s,i}$, then $V_i(x) \leq \delta_{b,i}$.*

Note that for the inference that $\hat{x} \in \Omega_{s,i} \Rightarrow x \in \Omega_{b,i}$ to be useful in executing the switching, the set $\Omega_{s,i}$ needs to be contained within $\Omega_{b,i}$. From Proposition 2, this can be ensured if $e_{m,i}$ is sufficiently small, which in turn is ensured for all times greater than T_i^b provided that the observer gain is sufficiently large. In practice, use of a sufficiently high observer gain leads to an $\Omega_{b,i}$ that is almost identical to Ω_i, and, furthermore, once the error has sufficiently decreased, $\Omega_{s,i}$ can be taken to be almost equal to $\Omega_{b,i}$.

Integrating fault-detection and fault-tolerant output feedback control

In this subsection we present a fault-tolerant controller that uses the estimates generated by the high-gain observer for the implementation of the fault-detection filter, the state feedback controllers and the switching logic (see Figure 7). We proceed by first showing how the implementation of the design and implementation of the fault-detection filter should be modified to handle the absence of full state measurements. To this end, we consider the following system

$$\dot{w}(t) = f(w) + g_i(w)u_i(w)$$

$$r(t) = \|\hat{x}(t) - w(t)\| \tag{13}$$

Note that, as in the full state feedback case, the state equation for the filter in Eq. 13 is a replica of the closed-loop state equation under full state feedback and in the absence of faults. However, because of the absence of full state measurements, the residual can only be defined in terms of the state estimates, not the actual states. The residual therefore provides a measure of the discrepancy between the evolution of the nominal closed-loop system (that is, with no faults) under full state feedback and the evolution of the closed-loop state estimates under output feedback. Since the discrepancy can be solely due to estimation errors and not necessarily due to faults, it is important to establish a bound on the residual which captures the expected difference in behavior in the absence of faults. This bound, which is given in Proposition 3 below, will be used as a threshold by the supervisor in declaring when a fault has occurred and consequently when switching becomes necessary. The proof of the proposition is given in the appendix.

Proposition 3: *Consider the nonlinear system of Eq. 1, for a fixed mode, $k(t) = i$, and with $m_i(t) \equiv 0$, under the output feedback controller of Eq. 12. Consider also the system of Eq. 13. Then, given the set of positive real numbers $\{\delta_{b,i}, \delta_{\zeta,i}, \delta_{m,i}, T_i^b\}$, there exists a positive real number, $\varepsilon_i' > 0$, such that if $\varepsilon_i \in (0, \varepsilon_i']$, $V_i(x(0)) \leq \delta_{b,i}$, $\|\tilde{y}(0)\| \leq \delta_{\zeta,i}$, $w(T_i^b) = \hat{x}(T_i^b)$, the residual satisfies a relation of the form $r(t) \leq \delta_{m,i}$ for all $t \geq T_i^b$.*

Note that the bound $\delta_{m,i}$ can be chosen arbitrarily small by choosing the observer gain to be sufficiently large. Note also that, unlike the case of full state feedback, the fault-detection filter is initialized only after the passage of some short period of time, $[0, T_i^b]$ (which can be chosen arbitrarily small by increasing the observer gain), to ensure that the closed-loop state estimates have converged sufficiently close to the true closed-loop states, and, thus, by setting the filter state w at this time equal to the value of the state estimate—ensure that the filter state is initialized sufficiently close to the true values of the state. From this point onwards, the filter simply integrates a replica of the dynamics of the process in the absence of errors. In the absence of actuator faults, the difference between the filter states and the process states is a function of the initial error, which can be bounded from above by a value that can be made as small as desired by decreasing the initial error, which in turn can be done by appropriate choice of the observer parameters.

Having established a bound on the residual in the absence of faults, we proceed with the design of the switching logic. To this end, consider the nonlinear system of Eq. 1 where, for each control configuration, an output feedback controller of the form of Eq. 12 is available and, given the desired output feedback stability regions $\Omega_{b,i} \subset \Omega_i$, $i = 1, \ldots, N$, as well as the desired values for $\delta_{m,i}$, T_b^i, an appropriate observer gain has been determined (for example, $\varepsilon_i \leq \min\{\varepsilon_i^*, \varepsilon_i', \varepsilon_i^{**}\}$ to guarantee both stability and satisfaction of the desired bound on the residual), and the sets $\Omega_{s,i}$ (see Proposition 2) have been computed. The implementation of the fault-detection filter and fault-tolerant controller is described in Theorem 2 below (see the Appendix for the proof).

Theorem 2: *Let $k(0) = i$ for some $i \in \mathcal{K}$, $x(0) \in \Omega_{b,i}$, $w(T_i^b) = \hat{x}(T_i^b)$, and consider a fault for which $r(T_i^s) \geq \delta_{m,i}$, where $T_i^s > T_i^b$ is the earliest time for which $r(t) \geq \delta_{m,i}$. Then under the switching rule*

$$k(t) = \begin{Bmatrix} i, & 0 \leq t < T_i^s \\ j \neq i, & t \geq T_i^s, \hat{x}(T_i^s) \in \Omega_j^s \end{Bmatrix} \tag{14}$$

the origin of the closed-loop system is asymptotically stable.

The design and implementation of the fault-detection filter and fault-tolerant controller proceed as follows:

1. Given the nonlinear process of Eq. 1, identify the available control configurations, $k = 1, \ldots, N$. For each configuration, design the output feedback controller of Eq. 12, and for a given choice of the output feedback stability region $\Omega_{b,i}$, determine a stabilizing observer gain ε_i^*.
2. Given any positive real numbers $\delta_{m,i}$ and T_i^b, determine the observer gain, ε_i', for which the maximum possible difference between the filter states and the state estimates, in the absence of faults, is less than the threshold $\delta_{m,i}$ for all times greater than T_i^b.
3. Given the output feedback stability region $\Omega_{b,i}$, determine the maximum error $e_{m,i}^*$, and the set $\Omega_{s,i}$, such that if $\|x - \hat{x}\| \leq e_{m,i} \leq e_{m,i}^*$ (that is, the error between the estimates, and the true values of the states is less than $e_{m,i}$) and $\hat{x} \in \Omega_{s,i}$ (that is, the state estimates belong to $\Omega_{s,i}$), then $x \in \Omega_{b,i}$ (that is, the state belongs to the output feedback stability region).
4. For a choice of $e_{m,i} \in (0, e_{m,i}^*]$ and given T_i^b, determine the observer gain, ε_i^{**}, for which the maximum possible difference between the states and the state estimates, in the absence of faults, is less than the threshold $e_{m,i}$ for all times greater than T_i^b. Set $\varepsilon_i := \min\{\varepsilon_i^*, \varepsilon_i', \varepsilon_i^{**}\}$. Note that this choice guarantees that by time T_i^b: (1) the residual is within the desired threshold and (2) the presence of $\hat{x}$ within $\Omega_{s,i}$ guarantees that x belongs to $\Omega_{b,i}$.
5. Initialize the closed-loop system such that $x(0) \in \Omega_{b,i}$, for some $i \in \mathcal{K}$, and start generating the state estimates $\hat{x}(t)$. At time T_i^b, initialize and start integrating the filter dynamics of Eq. 13 with $w(T_i^b) = \hat{x}(T_i^b)$, where $\hat{x}$ is the state estimate generated by the high-gain observer.
6. At the earliest time $T_i^s > T_i^b$ that $r(t) \geq \delta_{m,i}$ (implying that the difference between the expected evolution of the process states and the estimates of the process states is more than what can be accounted for by the error in the initialization of the filter states, implying that a fault has occurred), activate the backup configuration for which $\hat{x}(T_i^s) \in \Omega_{s,j}$ (note that since $t = T_i^s > T_i^b$, we have that $\|x(T_i^s) - \hat{x}(T_i^s)\| \leq e_{m,i}$; this together with $\hat{x}(T_i^s) \in \Omega_{s,j}$ implies that $x(T_i^s) \in \Omega_{b,j}$, that is, the state belongs to the stability region of configuration j). Implement the backup configuration j to achieve closed-loop stability.

Theorem 2 considers faults that are "observable" from the filter's residual, in the sense that if the residual in Eq. 13 exceeds the allowable threshold $\delta_{m,i}$ at any time, then the supervisor can conclude with certainty that a fault has occurred. On the other hand, if the residual does not exceed the allowable threshold, it might still be possible that some "unobservable" fault—the effect of which is within the filter threshold—has taken place. Note that in contrast to the case of full state feedback, the states in this case are only known up to a certain degree of accuracy. Therefore, any fault that causes a difference in the closed-loop behavior that is within the margin of (that is, indistinguishable from) the effect of the estimation error will, in principle, go undetected. While the result of Theorem 2 excludes these (small) faults to prove asymptotic stability, these faults can be easily considered, the only tradeoff being that instead of asymptotic stability, ultimate boundedness to a small ball whose size depends on the magnitude of these faults will be achieved (this magnitude of course decreases as the threshold gets smaller). Ultimately, the choice of $\delta_{m,i}$ reflects a fundamental tradeoff between the need to avoid false alarms that could be caused by estimation errors (this favors a relatively large threshold), and the need to minimize the possibility of some faults going undetected (this favors a relatively small threshold).

Note that for all times prior to T_i^b, the filter is inactive. Up until this time, the state estimates have not yet converged close enough to the true values of the states, and no inference about the state of the system can be drawn by looking at the evolution of the state estimate, and, therefore, no inference about any possible faults can be drawn via the fault-detection filter. If a fault occurs within this time, the filter will detect its occurrence only after the time T_i^b. By choosing a larger value of the observer gain, however, the time T_i^b can be reduced further, if so desired. Note also that while we consider the problem of unavailability of some of the state variables as measurements, we do not consider the problem of sensor faults, that is, we assume that the sensors do not malfunction both in the state and output feedback cases. In the event of availability of multiple measurements in a way that each of them can be used to estimate the process states, the estimates of the states generated using the different measurements can be used to also detect sensor faults.

Remark 5: The central idea behind the model-based fault-detection filter design, that of comparing the evolution of the process to the expected evolution of the process in the absence of faults, can be used in ways other than that used in Theorem 2 to detect the occurrence of a fault. Specifically, if the expected fault-free evolution is characterized by the evolution of the closed-loop states within the stability region then a fault could be declared if the state estimates, after a time T_i^b, touch the boundary of $\Omega_{s,i}$, which implies that the closed-loop states themselves may be about to escape the output feedback stability region $\Omega_{b,i}$, i.e. use the stability region to establish detection limits. Such an approach to detect faults, however, would be able to detect the fault only when the state estimates hit the boundary of $\Omega_{s,i}$, and could take longer than the model-based fault detection filter, which detects a fault as soon as the effect of the fault on the closed-loop evolution goes beyond a prescribed threshold. The selection of detection approaches can have an important effect in that differences in detection times can be the difference in the state escaping the stability region of the available backup configurations (see the simulation for an example). Also, it may happen that the fault causes the closed-loop process states evolving within $\Omega_{s,i}$ to neither escape $\Omega_{s,i}$ nor converge to the origin. Only monitoring the position of the states with respect to the stability region would not be able to detect such a fault. In contrast, the model-based fault-detection filter of Theorem 2 is able to detect faults that have an effect, up-to a desirable threshold, on the evolution of the closed-loop process. Note also that the model-based fault-detection filter of Theorem 2 and the alternative way to detect a fault (discussed above) differ only in that the model-based filter of Theorem 2 uses a more quantitative knowledge of the closed-loop dynamics to predict the expected closed-loop trajectory, instead of using the qualitative knowledge that the fault-free closed-loop state trajectory does not escape the stability region.

Simulation results

In this subsection, we first illustrate the implementation of the proposed output-feedback fault-tolerant control methodology to the chemical reactor introduced as a motivating example to clearly explain the main ideas behind the application of the proposed fault-detection and fault-tolerant control method, and then demonstrate an application to a networked chemical reactor example, investigating issues such as uncertainty and measurement noise.

For the chemical reactor of the motivating example, Figure 11 depicts the stability region, in the (T, C_A) space, for each configuration. The desired steady-state is depicted with an asterisk that lies in the intersection of the three stability regions. For the first two control configurations, a state estimator of the form of Eq. 12 is designed. For thresholds of δ_m = 0.0172 and 0.00151 in the fault detection filters, the parameters in the observer of Eq. 12 are chosen as $L_1 = L_2 = 100$, $a_1^{(1)} = a_1^{(2)} = 10$ and $a_2^{(1)} = a_2^{(2)} = 20$. For the third configuration, the estimates $\hat{T}$, $\hat{C}_A$ are generated as follows

$$\frac{d\hat{T}}{dt} = \frac{F}{V}(T_{A0} - \hat{T}) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} k_{i0} e^{(-E_i/R\hat{T})} \hat{C}_A + \alpha_1 (C_A - \hat{C}_A)$$

$$\frac{d\hat{C}_A}{dt} = \frac{F}{V}(C_{A0} - \hat{C}_A) - \sum_{i=1}^{3} k_{i0} e^{(-E_i/R\hat{T})} \hat{C}_A + \alpha_2 (C_A - \hat{C}_A) \quad (15)$$

where $\alpha_1 = -10^4$ and $\alpha_2 = 10$ and C_A is the measured output. The reactor is initialized at $T(0) = 330$ K, $C_A(0) = 3.6$ kmol/m^3, $C_B(0) = 0.0$ kmol/m^3, using the Q-control configuration, while the state estimates are initialized at $\hat{T}(0) = 390$ K, $\hat{C}_A(0) = 3.6$ kmol/m^3, and the supervisor proceeds to monitor the evolution of the closed-loop estimates.

We first demonstrate the need to wait for a sufficient time before initializing the filter. To this end, consider the fault-detection filter initialized at $t = 0.005$ minutes $\equiv T_1^b$ at which

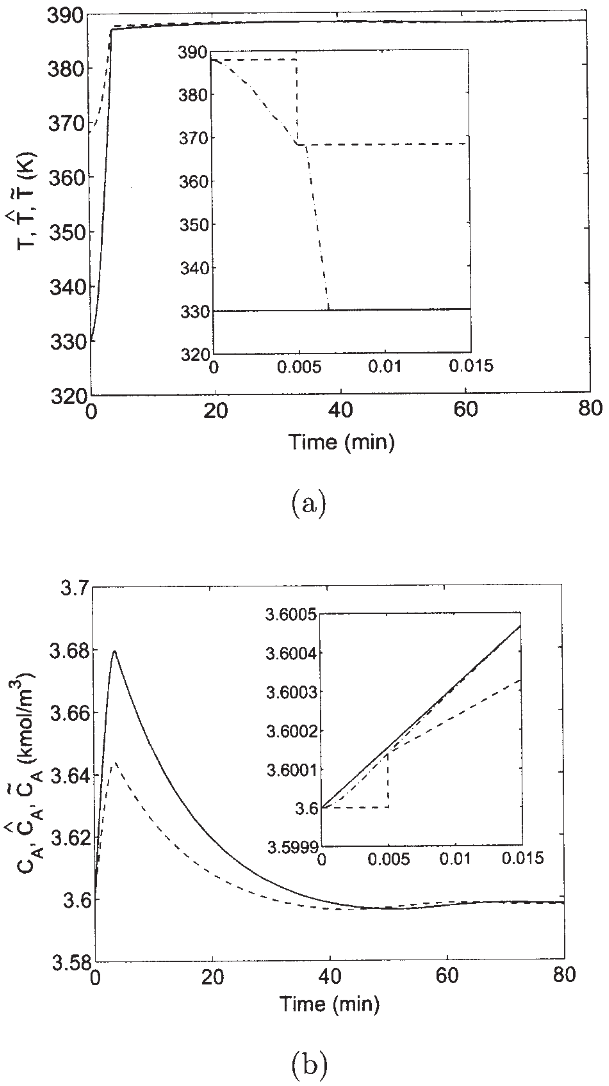


Figure 8. Evolution of the closed-loop (a) temperature (solid line), estimate of temperature (dash-dotted line) and the temperature profile generated by the filter (dashed line), and (b) concentration (solid line), estimate of concentration (dash-dotted line) and the concentration profile generated by the filter (dashed line) under control configuration 1, when the fault detection filter is initialized at t = 0.005 min.

time the state estimates (dash-dotted lines in Figure 8) have not converged to the true values (solid lines in Figure 8). As a result, the fault-detection filter shows a false alarm (see Figure 9a) by crossing the threshold even when control configuration 1 is functioning properly (see Figure 9b) and stabilizes the closed-loop system. Note that while the initialization of the filter at a time when the state estimates have not converged leads to the residual crossing the threshold, the residual eventually goes to zero as expected, since both the filter states and the closed-loop process states eventually stabilize and go to the same equilibrium point.

We now demonstrate the application of the fault-detection filter and fault-tolerant controller of Theorem 2. Starting from the same initial conditions, the estimates of T and C_A (dash-dotted lines in Figures 10a,b) converge very quickly to the true values of the states (solid lines in Figures 10a,b). The states in the fault-detection filter are initialized and set equal to the value of the state estimates at $t = 0.01$ min $\equiv T_1^b$; note that by this time the estimates have converged to the true values. By initializing the fault-detection filter appropriately, a false alarm is prevented (the value of $r_1(t)$ does not hit the threshold in the absence of a fault after a time $t = 0.01$ min, see Figure 12a). As shown by the solid lines in Figure 11, the controller proceeds to drive the closed-loop trajectory towards the desired steady-state, up until the Q-configuration fails after 3.0 min $\equiv T_1^f$ of reactor startup (see solid lines as will be shown in Figure 14a). Note that at this time, the value of $r_1(t)$ becomes nonzero and hits the threshold at $t = 3.3$ min $\equiv T_1^s$. From Figure

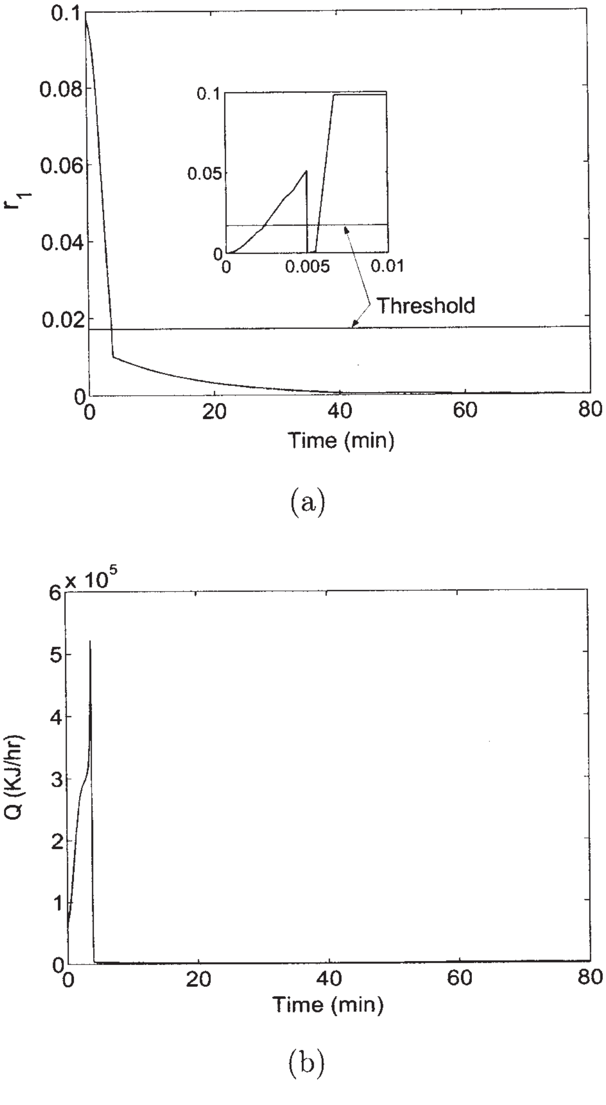


Figure 9. Evolution of (a) the residual, and (b) the manipulated input profile for the first control configuration when the fault detection filter is initialized at t = 0.005 min.

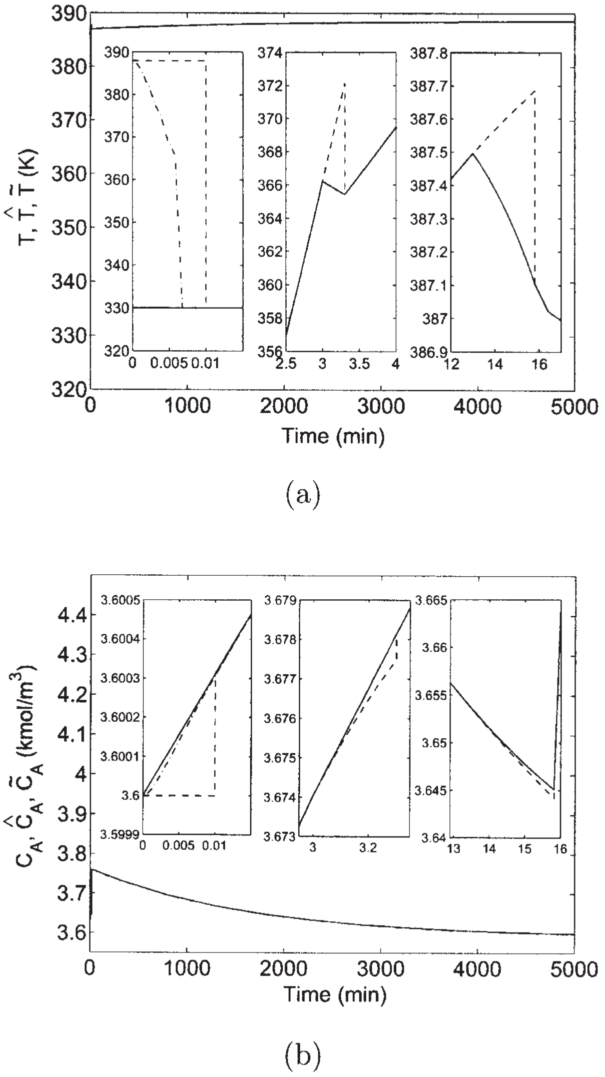


Figure 10. Evolution of the closed-loop (a) temperature (solid line), estimate of temperature (dash-dotted line), and the temperature profile generated by the filter (dashed line), and (b) concentration (solid line), estimate of concentration (dash-dotted line) and the concentration profile generated by the filter (dashed line) under the switching rule of Eq. 14 subject to failures in control systems 1 and 2.

11, 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. 14, the supervisor activates the second configuration (with T_{A0} as the manipulated input). The result is shown by the solid line in Figure 11 where it is seen that upon switching to the T_{A0}-configuration, the corresponding controller continues to drive the state trajectory closer to the desired steady-state.

When a second failure occurs (this time in the T_{A0}-configuration) at $t = 13.0$ min $\equiv T_2^f$ (which is simulated by fixing T_{A0} for all $t \geq 13.0$ min, see solid lines in Figure 14b) before the process has reached the steady state, the filter detects this failure via the value of $r_2(t)$ hitting the threshold (see Figure 12b). From the solid line in Figure 11, 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. However, if the fault-detection filter were not in place and the backup configuration is implemented late in the closed-loop (at $t = 30$ min $\equiv T_3^s$), by this time the state of the closed-loop system would have moved out of the stability region of the third control configuration, and closed-loop stability would not be achieved (see dashed line in Figure 11, see also Figure 13 and dashed lines in Figure 14). In contrast, when the fault-detection filter is in place, it detects a fault at $t = 15.82$ min $\equiv T_2^s$ and when the supervisor switches to configuration 3, closed-loop stability is achieved (see solid line in Figure 11).

Having illustrated the application and effectiveness of the proposed fault-detection and fault-tolerant control method in the case of a single reactor, we next demonstrate an application of the method to a networked chemical reactor example in the presence of uncertainty and measurement noise. To this end, consider the two well-mixed, nonisothermal continuous stirred-tank reactors shown in Figure 15. Three parallel irreversible elementary exothermic reactions of the form $A \rightarrow_{k_1} B$, $A \rightarrow_{k_2} U$ and $A \rightarrow_{k_3} R$ take place in each reactor, where A is the reactant species, B is the desired product, U and R are undesired byproducts. The feed to the first reactor consists of pure A at a flow rate F_0, molar concentration C_{A0}, and temperature T_0. The output from the first reactor is fed to the second reactor along with a fresh feed that consists of pure A at a flow rate F_3, molar concentration C_{A03}, and temperature T_{03}. Due to the nonisothermal nature of the reactors, a jacket is used to remove heat from or 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

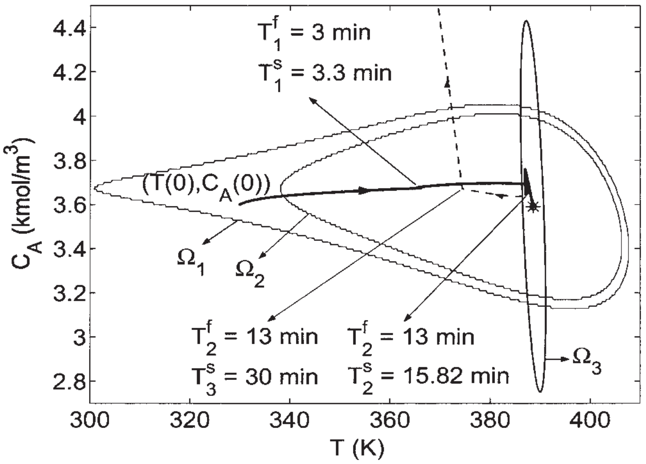


Figure 11. Evolution of the closed-loop state trajectory under the switching rule of Eq. 14 subject to failures in control systems 1 and 2, using an appropriate fault-detection filter (solid line), and in the absence of a fault-detection filter (dashed line).

$$
\begin{aligned}
\frac{dT_1}{dt} &= \frac{F_0}{V_1}(T_0 - T_1) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A1}, T_1) + \frac{Q_1}{\rho c_p V_1} \\
\frac{dC_{A1}}{dt} &= \frac{F_0}{V_1}(C_{A0} - C_{A1}) - \sum_{i=1}^{3} R_i(C_{A1}, T_1) \\
\frac{dT_2}{dt} &= \frac{F_0}{V_2}(T_1 - T_2) + \frac{F_3}{V_2}(T_{03} - T_2) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A2}, T_2) + \frac{Q_2}{\rho c_p V_2} \\
\frac{dC_{A2}}{dt} &= \frac{F_0}{V_2}(C_{A1} - C_{A2}) + \frac{F_3}{V_2}(C_{A03} - C_{A2}) - \sum_{i=1}^{3} R_i(C_{A2}, T_2) \qquad (16)
\end{aligned}
$$

where, $R_i(C_{Aj}, T_j) = k_{i0}\exp(-E_i/RT_j)C_{Aj}$, for $j = 1, 2$. T, C_A, Q_i ($i = 1, 2$), and V denote the temperature of the reactor, the concentration of species A, the rate of heat input/removal from the reactor, and the volume of reactor, respectively, with subscript 1 denoting CSTR 1 and subscript 2 denoting CSTR 2. 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 fluid in the reactor. For the values of the process parameters given in Table 1 and for $Q_1 = Q_2 = 0$ the process model of Eq. 16 has multiple steady states.

The control objective is to stabilize the reactor at the open-loop unstable steady-state where $(T_1^s, C_{A1}^s) = (388.57$ K, 3.59 kmol/m$^3)$ and $(T_2^s, C_{A2}^s) = (433.96$ K, 2.8811 kmol/m$^3)$. The measurements of temperature and concentrations are assumed to contain noise of magnitude 1 K and 0.1 kmol/m^3, respectively. Also, the concentrations of A in the inlet streams C_{A0} and C_{A03} used in the process model are 10% smaller than the values used in the filter equations and the controller. The available manipulated inputs include the rate of heat input into reactor one, Q_1, subject to the constraint $|Q_1| \leq 2.333 \times 10^6$ kJ/h, the rate of heat input into reactor two, Q_2, subject to the constraint $|Q_2| \leq 1.167 \times 10^6$ kJ/h and a duplicate backup heating configuration for reactor two, Q_3, subject to the constraint $|Q_3| \leq 1.167 \times 10^6$ kJ/h.

The primary control configuration consists of the manipulated inputs Q_1 and Q_2, while the backup configuration is comprised of manipulated inputs Q_1 and Q_3. As before, quadratic Lyapunov functions of the form $V_k = x^TP_kx$ are used for controller design, where P_k is a positive-definite symmetric matrix that satisfies the Riccati inequality $A^TP_k + P_kA - P_kb_kb_k^TP_k < 0$ for A and b obtained via linearization of the system around the desired steady-state with $x = [T_1 - T_{1s} \;\; C_{A1} - C_{A1s} \;\; T_2 - T_{2s} \;\; C_{A2} - C_{A2s}]'$, and are not reported here for the sake of brevity. The controller design yields a stability region estimate with c_1^{max} and c_2^{max} both approximately equal to 9.4. Note that all the information about the stability region is completely contained in the values of c_1^{max} and c_2^{max}, and the computation of these values is sufficient for the task of implementing the proposed method to the four-state system in this example. Specifically, the presence of the closed-loop state in the stability region can be ascertained by simply evaluating the value of the Lyapunov-function and checking against the value of c^{max} (for example, $V(x) < c_1^{max}$ implies that $x \in \Omega_1$).

Note that unlike the single reactor example, each control configuration consists of more than one manipulated input, which necessitates designing filters that detect as well as *isolate* faults. To this end, fault detection and isolation filters are designed that are dedicated to each manipulated input in the control configurations. The filter designs for Q_1 and Q_2 in the primary control configuration take the form

$$
\begin{aligned}
\frac{d\tilde{T}_1}{dt} &= \frac{F_0}{V_1}(T_0 - \tilde{T}_1) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A1}, \tilde{T}_1) + \frac{Q_1}{\rho c_p V_1} \\
r_1 &= \tilde{T}_1 - T_1 \qquad (17)
\end{aligned}
$$

$$
\begin{aligned}
\frac{d\tilde{T}_2}{dt} &= \frac{F_0}{V_2}(T_1 - \tilde{T}_2) + \frac{F_3}{V_2}(T_{03} - \tilde{T}_2) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A2}, \tilde{T}_2) + \frac{Q_2}{\rho c_p V_2} \\
r_2 &= \tilde{T}_2 - T_2 \qquad (18)
\end{aligned}
$$

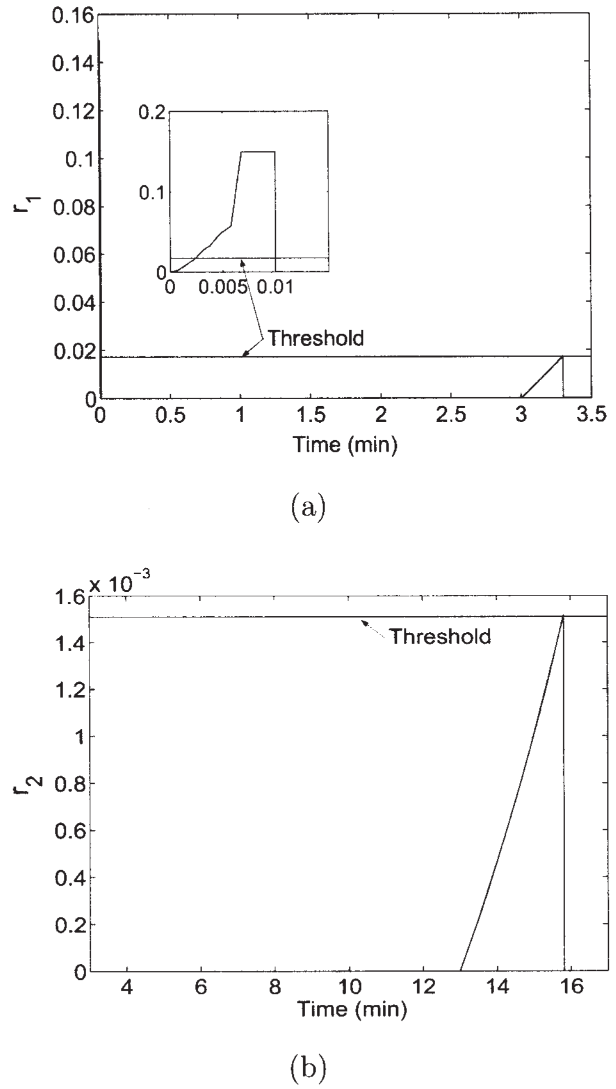


Figure 12. Evolution of the residual for (a) the first control configuration, and (b) the second control configuration.

As can be seen, the fault-detection and isolation filter for Q_1 includes a state $\tilde{T}_1$ whose dynamics are a copy of the model state, however, the dynamics are evaluated using the state measurements together with using $\tilde{T}_1$ in place of T_1. The value of the manipulated variable is also calculated in the same manner. For example, Q_1 in the filter is computed using ($\tilde{T}_1$, C_{A1}, T_2, C_{A2}). The filters for the other manipulated inputs are designed similarly. Note that due to the presence of measurement noise and disturbances, the values of the residual are nonzero even in the absence of faults, therefore, faults are declared only if the value of the residual exceeds a nonzero threshold value, where the threshold is obtained by evaluating the maximum value of the residual in the *absence* of faults to account for the effects of uncertainty and measurement noise.

In the first scenario the ability to detect a fault in the presence of multiple disturbances and noise is demonstrated. The reactors, as well as the fault detection filter for the first control configuration are initialized at the desired steady state $T_1(0) = 388.57$ K, $C_{A1}(0) = 3.591$ kmol/m^3, $T_2(0) = 433.96$ K and $C_{A2}(0) = 2.881$ kmol/m^3. For the sake of brevity, we show here only the evolution of T_2 and of the residuals. As can be seen in Figure 16a, the controller maintains the closed-loop trajectory near the desired steady-state until heating jacket two (Q_2) fails 40 min after reactor startup. If a fault-detection filter is not in place, and the fault is not detected, closed-loop stability is not achieved (dotted lines in Figure 16a). The fault-detection filter design of the form of Eqs. 17–18, however, detects this fault, when the value of residual $r_2(t)$ becomes greater than the threshold value of 2.0

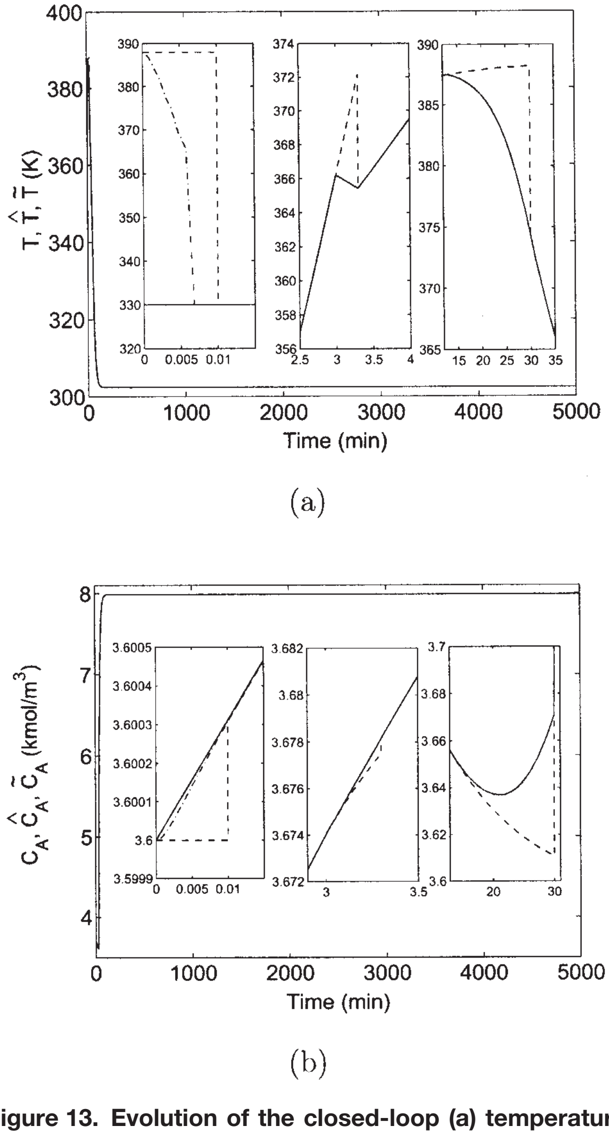
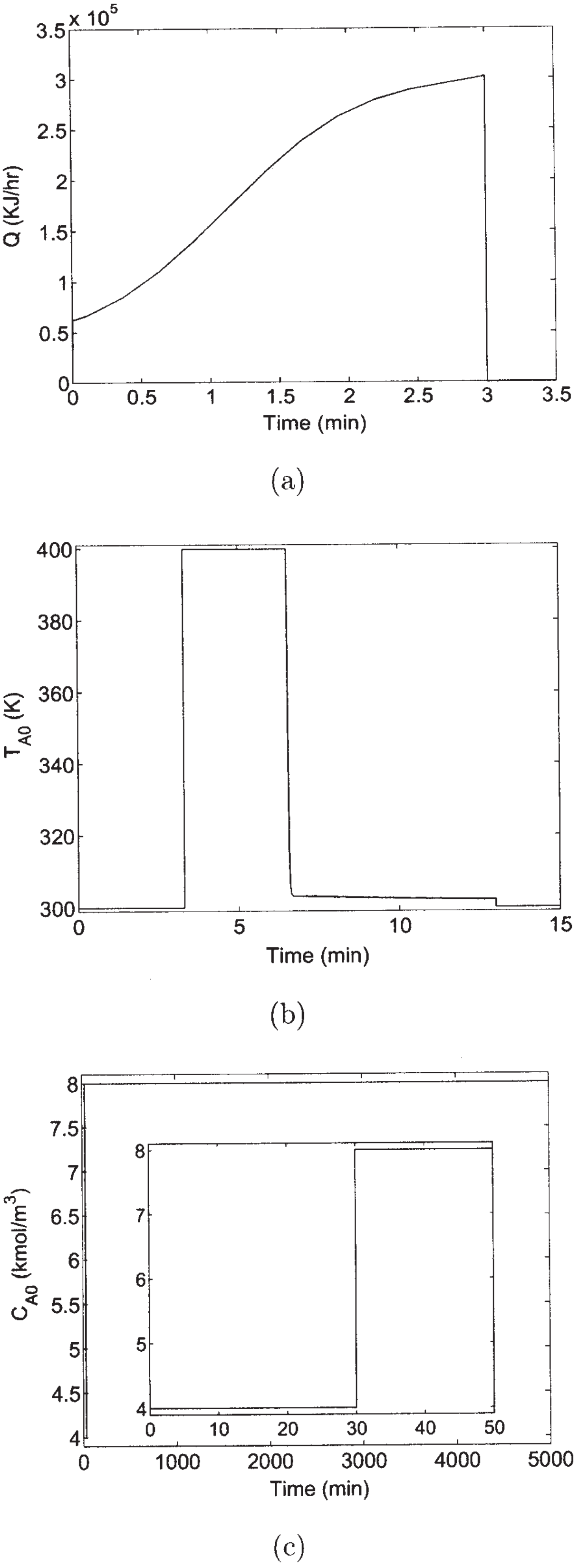


Figure 13. Evolution of the closed-loop (a) temperature (solid line), estimate of temperature (dash-dotted line), and the temperature profile generated by the filter (dashed line) and (b) concentration (solid line), estimate of concentration (dash-dotted line) and the concentration profile generated by the filter (dashed line) under the switching rule of Eq. 14 subject to failures in control systems 1 and 2 in the absence of a fault-detection filter.

at 40.79 min (see Figure 16c) while $r_1(t)$ (Figure 16b) remains below the threshold of 2.0, allowing the detection and isolation of the fault. While at the time of the failure (t = 40 min), the state of the closed-loop system is within the stability region of the backup-configuration, by the time that the failure is detected (at t = 40.79 min), operation of reactor 2 in an open-loop fashion (for 0.79 min) results in the closed-loop state moving out of the stability region of the backup configuration ($V_2 = 73.17 > c_2^{max} = 9.4$) and stability is not guaranteed after switching. However, it is possible that stability may still be achieved by using the fallback configuration. In particular, having been alerted by the fault-detection filter of the occurrence of the fault, the supervisor activates the fallback configuration (with Q_1 and Q_3 as the manipulated inputs, solid lines in Figure 16a) and is able to drive the system to the desired steady state and enforce closed-loop stability.



(a)

(b)

(c)

Figure 14. Manipulated input profiles under (a) control configuration 1, (b) control configuration 2, and (c) control configuration 3 under the switching rule of Eq. 14 subject to failures in control systems 1 and 2 in the presence (solid lines) and absence (dashed lines) of a fault-detection filter.

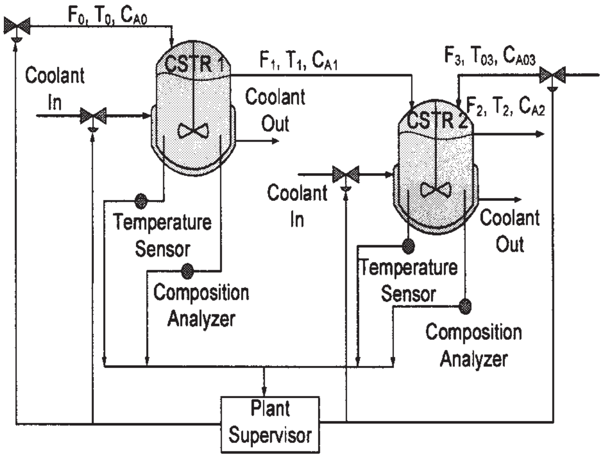


Figure 15. Flow diagram showing two CSTRs operating in series.

Detection of faults in the presence of process disturbances and noise is clearly possible using the methodology above. In order to guarantee stability after switching, however, the disturbances acting on the system should be reduced or the constraints on the control action should be relaxed to enlarge the closed-loop stability region. In the second scenario, the ability to detect a fault in the presence of noise and a single disturbance (in contrast to two disturbances in the first scenario), then switch to a fallback configuration with guaranteed stability is demonstrated. In this case, the measurements of temperature and concentrations are again assumed to contain noise of magnitude 1 K and 0.1 kmol/m^3, respectively. Also, the concentration of A in the inlet stream C_{A03} used in the process model is 10% smaller than the values used in the filter equations and the controller.

The reactors, as well as the fault detection filter for the first control configuration are initialized at the desired steady state $T_1(0)$ = 388.57 K, $C_{A1}(0)$ = 3.591 kmol/m^3, $T_2(0)$ = 433.96 K, $C_{A2}(0)$ = 2.881 kmol/m^3. As can be seen in Figure 17a, the controller maintains the closed-loop trajectory near the

Table 1. Process Parameters and Steady-State Values for the Chemical Reactors of Eq. 16

$F_0 = 4.998$	m^3/h
$F_1 = 4.998$	m^3/h
$F_3 = 4.998$	m^3/h
$V_1 = 1.0$	m^3
$V_2 = 0.5$	m^3
$R = 8.314$	KJ/kmol · K
$T_0 = 300.0$	K
$T_{03} = 300.0$	K
$C_{A0} = 4.0$	$kmol/m^3$
$C^s_{A03} = 3.0$	$kmol/m^3$
$\Delta H_1 = -5.0 \times 10^4$	KJ/kmol
$\Delta H_2 = -5.2 \times 10^4$	KJ/kmol
$\Delta H_3 = -5.4 \times 10^4$	KJ/kmol
$k_{10} = 3.0 \times 10^6$	h^{-1}
$k_{20} = 3.0 \times 10^5$	h^{-1}
$k_{30} = 3.0 \times 10^5$	h^{-1}
$E_1 = 5.0 \times 10^4$	KJ/kmol
$E_2 = 7.53 \times 10^4$	KJ/kmol
$E_3 = 7.53 \times 10^4$	KJ/kmol
$\rho = 1000.0$	kg/m^3
$c_p = 0.231$	KJ/kg · K
$T^s_1 = 388.57$	K
$C^s_{A1} = 3.59$	$kmol/m^3$
$T^s_2 = 433.96$	K
$C^s_{A2} = 2.88$	$kmol/m^3$

desired steady-state until heating jacket two (Q_2) fails 40 min after reactor startup. If a fault-detection filter is not in place, and the fault is not detected, closed-loop stability is not achieved (dotted lines in Figure 17a). The fault-detection filter design of the form of Eqs. 17–18, however, detects this fault, when the value of residual $r_2(t)$ becomes greater than the threshold value of 2.0 at 41.33 min (see Figure 17c) while $r_1(t)$ (Figure 17b) remains below the threshold of 2.0, allowing the detection and isolation of the fault. In this scenario, by the time that the fault is detected, the state of the closed-loop system resides within the stability region of configuration two ($V_2 = 8.03 < c_2^{max} = 9.4$). Therefore, the supervisor activates the fallback configuration (with Q_1 and Q_3 as the manipulated inputs, solid lines in Figure 17a) and the control system is able to drive the process to the desired steady state and enforce closed-loop stability.

Conclusions

In this work, an integrated fault-detection and fault-tolerant control (FDFTC) structure, for nonlinear processes with input constraints subject to control actuator failures, was presented. Under the assumption of full state feedback, the FDFTC structure comprised of (1) a family of control configurations, each with a stabilizing feedback controller and an explicitly characterized stability region, (2) a fault-detection filter that detects faults by comparing the fault-free behavior of the closed-loop states with their actual behavior, and (3) a high-level supervisor that orchestrates switching between the control configurations, based on the stability regions, once a fault is detected. When measurements of the full state were not available, a nonlinear observer with sufficiently fast convergence properties was incorporated into the FDFTC structure to generate appropriate state estimates that were used to implement the state feedback controllers, the fault-detection filter and the switching logic. It was shown that by properly tuning the observer parameters and

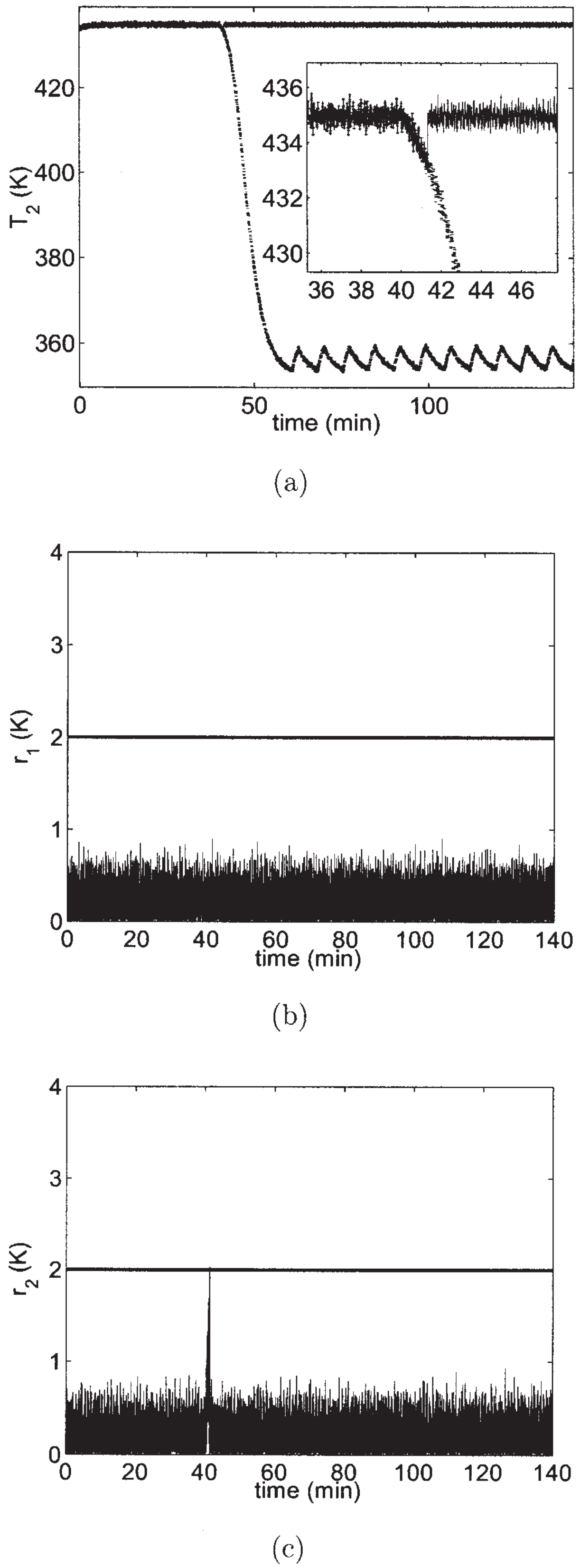
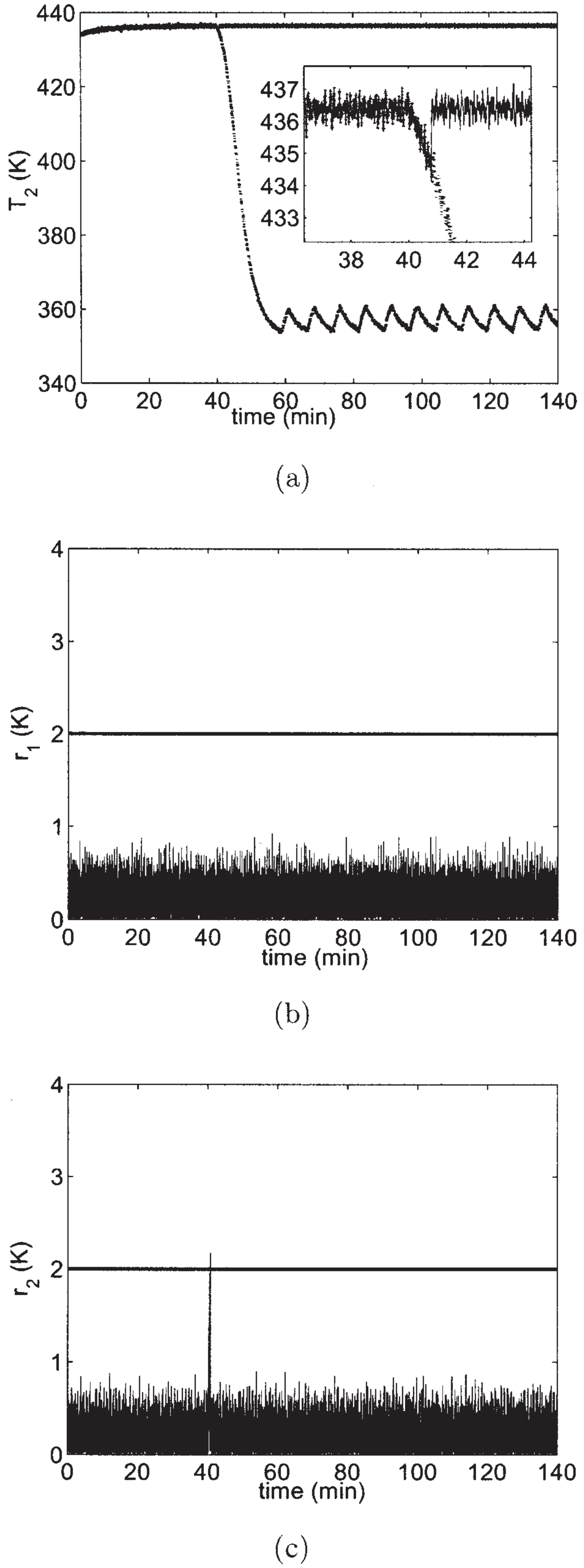


Figure 16. Two reactors in series scenario one: (a) temperature profile of reactor two with reconfiguration (solid line) and without reconfiguration (dotted line), (b) Q_1 residual profile, and (c) Q_2 residual profile (note fault detection at time t = 40.79 min).

modifying the implementation of the filter, the effect of the estimation error on the filter's residual could be decoupled from the effect of faults, thus preventing unnecessary false alarms. Finally, simulation studies were presented to illustrate the main ideas behind the proposed method, as well as to successfully demonstrate an application in the presence of model uncertainty and measurement noise.



(a)

(b)

(c)

Figure 17. Two reactors in series scenario two: (a) temperature profile of reactor two with reconfiguration (solid line) and without reconfiguration (dotted line), (b) Q_1 residual profile, (c) Q_2 residual profile (note fault detection at time t = 41.33 min).

Acknowledgment

Financial support from the National Science Foundation, CTS-0529295, is gratefully acknowledged.

Literature Cited

1. Nimmo I. Adequately address abnormal operations. *Chem Eng Prog.* 1995;91:36–45.
2. Ydstie EB. New vistas for process control: Integrating physics and communication networks. *AIChE J.* 2002;48:422–426.
3. Patton RJ. Fault-Tolerant Control Systems: The 1997 Situation. In: *Proceedings of the IFAC Symposium SAFEPROCESS 1997.* Hull: U. K.; 1997:1033–1054.
4. Zhou DH, Frank PM. Fault Diagnostics and Fault Tolerant Control. *IEEE Transactions on Aerospace and Electronic Systems.* 1998;34: 420–427.
5. Yang GH, Wang JL, Soh YC. Reliable H_∞ control design for linear systems. *Automatica.* 2001;37:717–725.
6. Bao J, Zhang WZ, Lee PL. Decentralized fault-tolerant control system design for unstable processes. *Chem Eng Sci.* 2003;58:5045–5054.
7. Wu NE. Coverage in fault-tolerant control. *Automatica.* 2004;40:537–548.
8. Bequette WB. Nonlinear control of chemical processes: A Review. *Ind & Eng Chem Res.* 1991;30:1391–1413.
9. Ydstie EB. Certainty Equivalence Adaptive Control: Paradigms Puzzles and Switching. In: *Proceedings of 5th International Conference on Chemical Process Control.* Tahoe City, CA; 1997. p. 9–23.
10. Henson MA, Seborg DE. *Nonlinear Process Control.* Englewood Cliffs, NJ: Prentice-Hall; 1997.
11. Christofides PD, El-Farra NH. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays.* New York: Springer; 2005.
12. Garcia CE, Prett DM, Morari M. Model predictive control—Theory and practice—a survey. *Automatica.* 1989;25:335–348.
13. Mayne DQ, Rawlings JB, Rao CV, Scokaert POM. Constrained model predictive control: stability and optimality. *Automatica.* 2000;36:789–814.
14. Findeisen R, Imsland L, Allgower F, Foss BA. State and output feedback nonlinear model predictive control: An overview. *Eur J Contr.* 2003;9:190–206.
15. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Sys & Contr Lett.* 1991;16:393–397.
16. Teel AR. Global stabilization and restricted tracking for multiple integrators with bounded controls. *Syst & Contr Lett.* 1992;18:165–171.
17. Kapoor N, Daoutidis P. Stabilization of systems with input constraints. *Int J Contr.* 1998;34:653–675.
18. Kokotovic PV, Arcak M. Constructive nonlinear control: a historical perspective. *Automatica.* 2001;37:637–662.
19. El-Farra NH, Christofides PD. Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem Eng Sci.* 2001;56: 1841–1868.
20. El-Farra NH, Christofides PD. Bounded robust control of constrained multivariable nonlinear Processes. *Chem Eng Sci.* 2003;58:3025–3047.
21. El-Farra NH, Mhaskar P, Christofides PD. Hybrid predictive control of nonlinear systems: method and applications to chemical processes. *Inter J Rob & Non Contr.* 2004;14:199–225.
22. Mhaskar P, El-Farra NH, Christofides PD. Robust hybrid predictive control of nonlinear systems. *Automatica.* 2005;41:209–217.
23. Grossmann IE, van den Heever SA, Harjukoski I. Discrete optimization methods and their role in the integration of planning and scheduling. In: *Proceedings of 6th International Conference on Chemical Process Control.* Tucson, AZ; 2001. p. 124–152.

24. Garcia-Onorio V, Ydstie BE. Distributed, asynchronous and hybrid simulation of process networks using recording controllers. *Int J Rob & Non Contr.* 2004;14:227–248.
25. Hespanha JP, Morse AS. Stability of switched systems with average dwell time. In: *Proceedings of 38th IEEE Conference on Decision and Control.* Phoenix, AZ; 1999:2655–2660.
26. Decarlo RA, Branicky MS, Petterson S, Lennartson B. Perspectives and results on the stability and stabilizability of hybrid systems. *Proceedings of the IEEE.* 2000;88:1069–1082.
27. Bemporad A, Morari M. Control of systems integrating logic, dynamics and constraints. *Automatica.* 1999;35:407–427.
28. El-Farra NH, Christofides PD. Coordinated feedback and switching for control of hybrid nonlinear processes. *AIChE J.* 2003;49:2079–2098.
29. El-Farra NH, Gani A, Christofides PD. Fault-tolerant control of process systems using communication networks. *AIChE J.* 2005;51:1665–1682.
30. Kresta JV, Macgregor JF, Marlin TE. Multivariate statistical monitoring of process operating performance. *Can J Chem Eng.* 1991;69:35–47.
31. Rollins DR, Davis JF. An unbiased estimation technique when gross errors exist in process measurements. *AIChE J.* 1992;38:563–572.
32. Nomikos P, Macgregor JF. Monitoring batch processes using multiway principal component analysis. *AIChE J.* 1994;40:1361–1375.
33. Dunia R, Qin SJ, Edgar TF, McAvoy TJ. Identification of faulty sensors using principal component analysis. *AIChE J.* 1996;42:2797–2812.
34. Negiz A, Cinar A. Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE J.* 1997;43:2002–2020.
35. Dunia R, Qin SJ. Subspace approach to multidimensional fault identification and reconstruction. *AIChE J.* 1998;44:1813–1831.
36. Davis JF, Piovoso ML, Kosanovich K, Bakshi B. Process data analysis and interpretation. *Advances in Chem Eng.* 1999;25:1–103.
37. Tatara E, Cinar A. An intelligent system for multivariate statistical process monitoring and diagnosis. *ISA Transactions.* 2002;41:255–270.
38. Aradhye HB, Bakshi BR, Davis JF, Ahalt SC. Clustering in wavelet domain: A multiresolution ART network for anomaly detection. *AIChE J.* 2004;50:2455–2466.
39. Zhang XD, Parisini T, Polycarpou MM. Adaptive fault-tolerant control of nonlinear uncertain systems: An information-based diagnostic approach. *IEEE Trans Automat Contr.* 2004;49:1259–1274.
40. Massoumnia M, Verghese GC, Wilsky AS. Failure detection and identification. *IEEE Trans Automat Contr.* 1989;34:316–321.
41. Frank PM. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy—A survey and some new results. *Automatica.* 1990;26:459–474.
42. Frank PM, Ding X. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *J Proc Contr.* 1997;7:403–424.
43. Mehranbod N, Soroush M, Panjapornpon C. A method of sensor fault detection and identification. *J Proc Contr.* 2005;15:321–339.
44. Saberi A, Stoorvogel AA, Sannuti P, Niemann H. Fundamental problems in fault detection and identification. *Int J Rob & Non Contr.* 2000;10:1209–1236.
45. DePersis C, Isidori A. A geometric approach to nonlinear fault detection and isolation. *IEEE Trans Automat Contr.* 2001;46:853–865.
46. Khalil HK. *Nonlinear Systems.* 2nd ed. New York: Macmillan Publishing Company; 1996.
47. Krstic N, Kanellakopoulos I, Kokotovic P. *Nonlinear and Adaptive Control Design.* 1st ed. New York: Wiley; 1995.
48. Freeman RA, Kokotovic PV. *Robust Nonlinear Control Design: State-Space and Lyapunov Techniques.* Boston: Birkhauser; 1996.
49. Dubljevic S, Kazantzis N. A new Lyapunov design approach for nonlinear systems based on Zubov's method. *Automatica.* 2002;38:1999–2007.
50. Mhaskar P, El-Farra NH, Christofides PD. Predictive control of switched nonlinear systems with scheduled mode transitions. *IEEE Trans Automat Contr.* 2005;50:1670–1680.
51. Mhaskar P, Gani A, Christofides PD. Fault-tolerant control of nonlinear processes: performance-based reconfiguration and robustness. *Int J Rob & Non Contr.* 2006;16:91–111.
52. Mahmoud NA, Khalil HK. Asymptotic regulation of minimum phase nonlinear systems using output feedback. *IEEE Trans Automat Contr.* 1996;41:1402–1412.
53. Kazantzis N, Kravaris C. Nonlinear observer design using Lyapunov's auxiliary theorem. *Syst & Contr Lett.* 1999;34:241–247.
54. Kazantzis N, Kravaris C, Wright RA. Nonlinear observer design for process monitoring. *Ind & Eng Chem Res.* 2000;39:408–419.
55. Soroush M, Zambare N. Nonlinear output feedback control of a class of polymerization reactors. *IEEE Trans Contr Syst Tech.* 2000;8:310–320.
56. Christofides PD. Robust output feedback control of nonlinear singularly perturbed systems. *Automatica.* 2000;36:45–52.
57. Christofides PD, Teel AR. Singular perturbations and input-to-state stability. *IEEE Trans Automat Contr.* 1996;41:1645–1650.
58. Michalska H, Mayne DQ. Moving horizon observers and observer-based control. *IEEE Trans Automat Contr.* 1995;40:995–1006.
59. Rao CV, Rawlings JB. Constrained process monitoring: Moving-horizon approach. *AIChE J.* 2002;48:97–109.
60. Mhaskar P, El-Farra NH, Christofides PD. Hybrid predictive control of process systems. *AIChE J.* 2004;50:1242–1259.

Appendix

Proof of Theorem 1: We split the proof of the theorem in two parts. In the first part we show that the filter detects a fault if and only if one occurs, and in the second part we establish closed-loop stability under the switching rule of Eq. 8.

Part 1: Let $x(T_i^f) := x_{T_i^f}$ and $w(T_i^f) := w_{T_i^f}$, and consider

$$\dot{w}(T_i^f) - \dot{x}(T_i^f) = f(x_{T_i^f}) + g(x_{T_i^f})(u_i(x_{T_i^f}) + m_i(T_i^f)) - (f(w_{T_i^f}) + g(w_{T_i^f})u_i(w_{T_i^f})) \quad \text{(A1)}$$

with $m_i(T_i^f) \neq 0$. Since $w_{T_i^f} = x_{T_i^f}$, we have that

$$f(x_{T_i^f}) + g(x_{T_i^f})(u_i(x_{T_i^f}) + m_i(T_i^f)) - (f(w_{T_i^f}) + g(w_{T_i^f})u_i(w_{T_i^f})) = g(x_{T_i^f})m_i(T_i^f) \quad \text{(A2)}$$

Furthermore, since $g(x_{T_i^f}) \neq 0$, we have that

$$\dot{w}(T_i^f) - \dot{x}(T_i^f) = g(x_{T_i^f})m_i(T_i^f) \neq 0 \quad \text{(A3)}$$

if and only if $m_i(T_i^f) \neq 0$. Since $w_{T_i^f} - x_{T_i^f} = 0$ and $\dot{w}(T_i^f) - \dot{x}(T_i^f) \neq 0$ if and only if $m_i(T_i^f) \neq 0$, we have that

$$w(T_i^{f+}) - x(T_i^{f+}) \neq 0 \quad \text{(A4)}$$

or

$$r(T_i^{f+}) = \|w(T_i^{f+}) - x(T_i^{f+})\| > 0 \quad \text{(A5)}$$

if and only if $m_i(T_i^f) \neq 0$.

Part 2: We prove closed-loop stability for the two possible cases; first if no switching occurs, and second if a switch occurs at a time T_i^s.

Case 1: The absence of a switch implies $r_i(t) = 0$. Furthermore, $r_i(t) = 0 \Rightarrow x(t) = w(t)$. Since $x(0) = w(0) \in \Omega_i$, and control configuration i is implemented for all times in this case, we have that asymptotic closed-loop stability is achieved.

Case 2: At time T_i^s, the supervisor switches to a control configuration j for which $x(T_i^s) \in \Omega_j$. From this time onwards, since configuration j is implemented in the closed-loop system for all times, and since $x(T_i^s) \in \Omega_j$, closed-loop stability follows. This completes the proof of Theorem 1.

Proof of Proposition 2: From the continuity of the function $V_i(\cdot)$, we have that for any positive real number $e_{m,i}$, there exists a positive real number γ_i such that $\|x - \hat{x}\| \leq e_{m,i} \Rightarrow |V_i(x) - V_i(\hat{x})| \leq \gamma_i \Rightarrow V_i(x) \leq V_i(\hat{x}) + \gamma_i$. Since γ_i can be made small by choosing $e_{m,i}$ small, it follows that given any positive real number $\delta_{b,i}$, there exists a positive real number, $e^*_{m,i}$, such that for all $e_{m,i} \in (0, e^*_{m,i}]$, $\gamma_i < \delta_{b,i}$. Now, let $\delta_{s,i}$ be any positive real number that satisfies $\delta_{s,i} + \gamma_i \leq \delta_{b,i}$. Then if $\|x - \hat{x}\| \leq e_{m,i} \leq e^*_{m,i}$ and $V_i(\hat{x}) \leq \delta_{s,i}$, we have $V_i(x) \leq V_i(\hat{x}) + \gamma_i \leq \delta_{s,i} + \gamma_i \leq \delta_{b,i}$. This completes the proof of the proposition.

Proof of Proposition 3: Consider the system of Eq. 1 with $m_i(t) \equiv 0$ under the output feedback controller of Eq. 12. From the result of Proposition 1, we have that given $x(0) \in \Omega_{b,i}$ and any positive real number T^b_i, there exists a real positive number ε^{**}_i such that $\|x(t) - \hat{x}(t)\| \leq k_1\varepsilon_i$, for all $t \geq T^b_i$, $\varepsilon_i \in (0, \varepsilon^{**}_i]$, for some $k_1 > 0$, that is, $x(t) = \hat{x}(t) + O(\varepsilon_i)$, where $O(\varepsilon_i)$ is the standard order of magnitude notation. Now, consider the following two systems for $t \geq T^b_i$:

$$\dot{x}(t) = f(x(t)) + g_i(x(t))u_i(\hat{x}(t)) \tag{A6}$$

$$\dot{w}(t) = f(w(t)) + g_i(w(t))u_i(w(t)) \tag{A7}$$

where $w(T^b_i) = \hat{x}(T^b_i)$. The system of Eq. A7 is exactly the closed-loop system under full state feedback and has an asymptotically (and exponentially) stable equilibrium at the origin, for all initial conditions within Ω_i. The system of Eq. A6 is the closed-loop system under output feedback and (from Proposition 1) has an asymptotically (and locally exponentially) stable equilibrium at the origin, for all initial conditions within $\Omega_{b,i} \subset \Omega_i$ and for all $\varepsilon_i \leq \varepsilon^*_i$. Since $x(t) = \hat{x}(t) + O(\varepsilon_i)$ for all $t \geq T^b_i$, we have that $x(T^b_i) = \hat{x}(T^i_b) + O(\varepsilon_i)$, and when $\varepsilon_i = 0$, the two systems of Eqs. A6–A7 become identical. Let $F_i(\cdot) = f(\cdot) + g_i(\cdot)u_i(\cdot)$, and $x(T^b_i) = \hat{x}(T^i_b) + O(\varepsilon_i) := \eta(\varepsilon_i)$, where η is a continuous function that depends smoothly on ε_i, then we can write

$$\dot{x}(t) = F_i(x(t), \varepsilon_i), \quad x(T^b_i) = \eta(\varepsilon_i)$$

$$\dot{w}(t) = F_i(w(t)), \quad w(T^b_i) = \eta(0) \tag{A8}$$

It is clear from the above representation that the state equations for both the filter system and the closed-loop system, as well as their initial conditions at T^b_i, are identical when $\varepsilon_i = 0$. Therefore, we can use the theory of regular perturbations (see Chapter 8 in [46]) to establish the closeness of solutions between the two systems over the infinite time interval. In particular, since $F_i(\cdot)$ is continuous and bounded on $\Omega_{b,i}$, and the w-system is exponentially stable, an application of the result of Theorem 8.2 in [46] yields that there exists $\varepsilon''_i > 0$ such that for all $\varepsilon_i \in (0, \varepsilon''_i]$, $x(t) = w(t) + O(\varepsilon_i)$ for all $t \geq T^b_i$. We, therefore, have that, for $\varepsilon_i \in (0, \min\{\varepsilon^{**}_i, \varepsilon''_i\}]$, $r(t) = \|\hat{x}(t) - w(t)\| = \|\hat{x}(t) - x(t) + x(t) - w(t)\| \leq \|\hat{x}(t) - x(t)\| + \|x(t) - w(t)\| \leq (k_1 + k_2)\varepsilon_i$ for all $t \geq T^b_i$. This implies that given any positive real number $\delta_{m,i}$, there exists $\varepsilon'_i > 0$ such that $\|\hat{x}(t) - w(t)\| \leq \delta_{m,i}$ for all $\varepsilon_i \in (0, \varepsilon'_i]$, for all $t \geq T^b_i$, where $\varepsilon'_i = \min\{\varepsilon^{**}_i, \varepsilon''_i, \delta_{m,i}/(k_1 + k_2)\}$.

To summarize, we conclude that given the set of positive real numbers $\{\delta_{b,i}, \delta_{\zeta,i}, \delta_{m,i}, T^b_i\}$, there exists a positive real number, $\varepsilon'_i > 0$, such that if $\varepsilon_i \in (0, \varepsilon'_i]$, $V_i(x(0)) \leq \delta_{b,i}$, $\|\tilde{y}(0)\| \leq \delta_{\zeta,i}$, $w(T^b_i) = \hat{x}(T^b_i)$, the residual satisfies a relation of the form $r(t) \leq \delta_{m,i}$ for all $t \geq T^b_i$. This completes the proof of the proposition.

Proof of Theorem 2: Consider the nonlinear system of Eq. 1, under the output feedback controller of Eq. 12, and the system of Eq. 13, where $k(0) = i$ for some $i \in \mathcal{K}$, $x(0) \in \Omega_{b,i}$, $w(T^b_i) = \hat{x}(T^b_i)$, $\varepsilon_i \leq \min\{\varepsilon^*_i, \varepsilon'_i, \varepsilon^{**}_i\}$, where ε^*_i, ε^{**}_i were defined in Proposition 1 and ε'_i was defined in Proposition 3. Since we consider only faults for which $r(T^s_i) \geq \delta^i_m$, where $T^s_i > T^b_i$ is the earliest time for which $r(t) \geq \delta^i_m$, it follows that:

(a) in the absence of such faults, no switching takes place and configuration i is implemented for all times. Since $x(0) \in \Omega_{b,i}$ and $\varepsilon_i \leq \varepsilon^*_i$, asymptotic closed-loop stability of the origin follows directly from Proposition 1.

(b) in the case that such faults take place, the earliest time a fault is detected is $T^s_i > T^b_i$ and we have, from Eq. 14, that $k(t) = i$ for $0 \leq t < T^s_i$. From the stability of the i-th closed-loop system established in Proposition 1, we have that the closed-loop trajectory stays bounded within $\Omega_{b,i}$ for $0 \leq t < T^s_i$. At time T^s_i, the supervisor switches to a control configuration j for which $\hat{x}(T^s_i) \in \Omega_{s,j}$. By design, $\hat{x}(t) \in \Omega_{s,j} \Rightarrow x(t) \in \Omega_{b,j}$ for all $t \geq T^s_i > T^b_i$. From this point onwards, configuration j is implemented in the closed-loop system for all future times and, since $x(T^s_i) \in \Omega_{b,j}$, asymptotic closed-loop stability of the origin follows from the result of Proposition 1. This completes the proof of Theorem 2.

Manuscript received Jan. 27, 2005, and revision received Oct. 24, 2005, and final revision received Feb. 3, 2006.