Available online at www.sciencedirect.com
ScienceDirect
Automatica 44 (2008) 53–62
automatica
www.elsevier.com/locate/automatica

# Isolation and handling of actuator faults in nonlinear systems ☆

Prashant Mhaskar[a], Charles McFall[b], Adiwinata Gani[b], Panagiotis D. Christofides[b,*], James F. Davis[b]

[a] Department of Chemical Engineering, McMaster University, Hamilton, ON, Canada L8S 4L7
[b] Department of Chemical & Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA

Received 20 July 2006; received in revised form 7 May 2007; accepted 13 May 2007
Available online 13 August 2007

**Abstract**

This work considers the problem of control actuator fault detection and isolation and fault-tolerant control for a multi-input multi-output nonlinear system subject to constraints on the manipulated inputs and proposes a fault detection and isolation filter and controller reconfiguration design. The implementation of the fault detection and isolation filters and reconfiguration strategy are demonstrated via a chemical process example.


*Keywords:* Fault-tolerant control; Fault detection and isolation; Input constraints; Stability region; Lyapunov-based control

## 1. Introduction

The operation of chemical processes is characterized by the complexity of the individual units together with an intricate interconnection of these geographically distributed units via a network of material and energy streams, and control loops. The nonlinear behavior exhibited by most chemical processes, together with the presence of constraints on the operating conditions, modeling uncertainty and disturbances, and the lack of availability of state measurements has motivated several research results in the area of nonlinear process control focusing on these issues (see, e.g., El-Farra & Christofides, 2001, 2001; El-Farra, Mhaskar, & Christofides, 2005; Lin & Sontag, 1991; Mhaskar, El-Farra, & Christofides, 2004; Soroush, Valluri, & Mehranbod, 2005 and, for a review of results, Allgöwer & Doyle, 1997; Bequette, 1991; Christofides & El-Farra, 2005; Henson & Seborg, 1997 and the references therein). The development of the advanced control algorithms outlined above (alongside development in sensing, communicating and computing technologies) has led to extensive automation of plant operation. Increased automation, however, also makes the plant susceptible to faults (e.g., defects/malfunctions in process equipment, sensors and actuators, failures in the controllers or in the control loops), which, if not appropriately handled in the control system design, can potentially cause a host of undesired economic, environmental, and safety problems that seriously degrade the operating efficiency of the plant.

The above considerations provide a strong motivation for the development of advanced fault-tolerant controllers that account for system complexities such as nonlinearity, uncertainty and constraints and provide a mechanism for an efficient and timely response to enhance fault recovery. One of the prerequisites for implementing fault-tolerant control is the ability to detect and isolate the faults. Statistical and pattern recognition techniques for data analysis and interpretation (e.g., Aradhye, Bakshi, Davis, & Ahalt, 2004; Davis, Piovoso, Kosanovich, & Bakshi, 1999; Kresta, Macgregor, & Marlin, 1991; Negiz & Cinar, 1997; Nomikos & Macgregor, 1994; Rollins & Davis, 1992) 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

☆ This paper was not presented at any IFAC meeting. This paper was recommended for publication in revised form by Associate Editor Michael Henson under the direction of Editor Frank Allgöwer. Financial support from the National Science Foundation, CTS-0529295, is gratefully acknowledged.
* Corresponding author. Tel.: +1 3107941015; fax: +1 3102064107.
*E-mail addresses:* mhaskar@mcmaster.ca (P. Mhaskar), cmcfall@ucla.edu (C. McFall), agani@ucla.edu (A. Gani), pdc@ucla.edu (P.D. Christofides), jdavis@oit.ucla.edu (J.F. Davis).

0005-1098/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2007.05.006

linear systems (e.g., Frank, 1990; Frank & Ding, 1997; Massoumnia, Verghese, & Wilsky, 1989; Mehranbod, Soroush, & Panjapornpon, 2005); and more recently, fundamental results in the context of nonlinear systems have been derived (e.g., DePersis & Isidori, 2001; Pisu, Serrani, You, & Jalics, 2006; Saberi, Stoorvogel, Sannuti, & Niemann, 2000).

Fault-tolerant control can be achieved, in one approach, via controller designs using enough actuators to withstand the failure of some of the control actuators (e.g., see Bonivento, Isidori, Marconi, & Paoli, 2004; Yang, Wang, & Soh, 2001) and the robustness of the active control configuration to such faults can be analyzed. Economic considerations (to save on unnecessary control action), however, dictate the use of only as many control loops as is required at a time. In such cases, faults in a control actuator cannot be handled via changing the control algorithm and necessitates control-loop reconfiguration (activating appropriate backup control actuators). Using these approaches, fault-tolerant control has been actively pursued in the context of aerospace engineering applications (see, e.g., Patton, 1997; Zhou & Frank, 1998). Recently it has also gained attention in the context of chemical process control; however, most available results are based on the assumption of a linear process description (e.g., Bao, Zhang, & Lee, 2003; Wu, 2004) and do not account for process nonlinearity, constraints and lack of state measurements.

Controller reconfiguration to achieve fault-tolerant control via switching to well-functioning control actuators makes the closed-loop system a hybrid system, since the closed-loop system exhibits discrete transitions between continuous modes of operations. While a large number of research works have focused on a diverse array of hybrid system problems (e.g., DeCarlo, Branicky, Pettersson, & Lennartson, 2000; El-Farra & Christofides, 2003b; El-Farra et al., 2005; Garcia-Onorio & Ydstie, 2004), the use of a hybrid system framework for the study of fault-tolerant control problems has received limited attention. Under the assumption of state feedback and knowledge of fault, in El-Farra, Gani, and Christofides (2005), a hybrid systems approach to fault-tolerant control was employed where upon occurrence of a fault, stability region-based reconfiguration is done to achieve fault-tolerant control and in Mhaskar, Gani, and Christofides (2006), performance and robustness considerations were incorporated in the fault-tolerant control structure. In Mhaskar et al. (2006) the problem of fault detection and fault-tolerant control for single input systems was considered and the problem of deciding which backup control configuration should be implemented to preserve closed–loop stability was addressed. In Mhaskar et al. (2006), however, only single input systems were considered which did not require isolating the fault in a given control configuration. In a multi-input system, where the faults can occur in any of the actuators, the inability to isolate which actuator has failed can negatively impact the selection of the backup control configuration, and if incorrectly chosen, may fail to preserve closed–loop stability (due to the fact that the faulty actuator may be a member of the backup control configuration).

Motivated by these considerations, this work considers the problem of implementing fault-tolerant control on a multi-input multi-output nonlinear system subject to faults in the control actuators and constraints on the manipulated inputs. The case where all the states of the system are measured is first considered. The state measurements and the model is used to design filters that essentially capture the difference between fault-free evolution and the observed evolution of the system to detect and isolate faults. In the event of a fault, a configuration is chosen that (1) does not use the failed control actuator, and (2) guarantees stability of the closed-loop system starting from the system state at the time of the failure. To be able to ascertain the second condition, Lyapunov-based controllers, which provide an explicit characterization of the closed-loop stability region, are used in designing the control laws for the individual control configurations. Next the problem where not all the system states are measured is considered. First, output-feedback controllers are designed that allow for an explicit characterization of the output-feedback stability region. The state estimates are employed in implementing the fault detection and isolation filters, and the reconfiguration rule. While this work focusses on the rigorous development of fault-detection and isolation filter designs for the state and output-feedback cases, other practical issues such as uncertainty, disturbances, measurement noise and sampling delays are investigated in the implementation of the fault detection and isolation filters and reconfiguration strategy on a chemical process example.

## 2. Preliminaries

Consider nonlinear systems with input constraints, described by

$$\begin{aligned} &\dot{x} = f(x) + G_{k(t)}(x)(u_{k(t)}(y) + \tilde{u}_{k(t)}(t)),\\ &y(x) = h(x), \quad u_k(y) \in \mathbf{U}_k, \quad (u_{k(t)}(y) + \tilde{u}_{k(t)}(t)) \in \mathbf{U}_k,\\ &k(t) \in \mathbf{K} = \{1, \ldots, N\}, \quad N < \infty, \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $y \in \mathbf{R}^m$ denotes the vector of measured variables and $u_{k(t)}(y) \in \mathbb{R}^m$ denotes the control action prescribed by the control law for the vector of constrained manipulated inputs under the $k$th configuration. $\tilde{u}_{k(t)}$ denotes the unknown fault vector with $u_{k(t)}(y) + \tilde{u}_{k(t)}$ taking values in a non-empty convex subset $\mathbf{U}_k$ of $\mathbb{R}^m$, where $\mathbf{U}_k = \{u_k + \tilde{u}_k \in \mathbb{R}^m : \|u_k + \tilde{u}_k\| \leqslant u_k^{\max}\}$, $\|\cdot\|$ is the Euclidean norm of a vector, $u_k^{\max} > 0$ is the magnitude of input constraints and $f(0) = 0$. The vector function $f(x)$ and the matrices $G_k(x) = [g_{1,k}(x) \cdots g_{m,k}(x)]$ are assumed to be sufficiently smooth on their domains of definition. $k(t)$, which takes values in the finite index set $\mathbf{K}$, represents a discrete state that indexes the matrix $G_k(\cdot)$ as well as the manipulated input $u_k(\cdot)$ and the possible faults in the manipulated inputs $\tilde{u}_k(\cdot)$. For each value that $k$ assumes in $\mathbf{K}$, the process is controlled via a different set of manipulated inputs which defines a given control configuration. 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, i.e., $x(T^+) = \lim_{t \to T^+} x(t)$.

Throughout the manuscript, it is assumed that for any $u_k \in \mathbf{U}_k$ the solution of the system of Eq. (1) exists and is

continuous for all $t$. Next, one example of a state-feedback controller that provides an explicit estimate of the stability region for the closed-loop system subject to constraints is reviewed (for more details on the controller design, and the proof, see El-Farra & Christofides, 2001; Lin & Sontag, 1991).

**Theorem 1** (*El-Farra and Christofides, 2001*). *Consider the switched nonlinear system of Eq.* (1) *for a configuration k for which a control Lyapunov function $V_k$ exists, with $\tilde{u}_k(t) \equiv 0$, under state-feedback using the following bounded nonlinear feedback controller*:

$$u_k = -w_k(x, u_k^{\max})(L_{G_k} V_k(x))^{\mathrm{T}}, \tag{2}$$

*where*

$$w_k(x, u_k^{\max}) = \begin{cases} \dfrac{\alpha_k(x) + \sqrt{\alpha_k^2(x) + (u_k^{\max}\|b_k^{\mathrm{T}}(x)\|)^4}}{\|b_k^{\mathrm{T}}(x)\|^2[1 + \sqrt{1 + (u_k^{\max}\|b_k^{\mathrm{T}}(x)\|)^2}]}, & b_k^{\mathrm{T}}(x) \neq 0, \\ 0, & b_k^{\mathrm{T}}(x) = 0 \end{cases} \tag{3}$$

*with $\alpha_k(x) = L_{f_k} V_k(x) + \rho_k V_k(x)$, $\rho_k > 0$ and $b_k(x) = L_{G_k} V_k(x)$. Assume that the set $\Phi_k(u_k^{\max})$ of $x$ satisfying*

$$L_{f_k} V_k(x) + \rho_k V_k(x) \leqslant u_k^{\max}\|(L_{G_k} V_k(x))^{\mathrm{T}} \tag{4}$$

*contains the origin and a neighborhood of the origin. Also, let $\Omega_k(u_k^{\max}) := \{x \in \mathbf{R}^n : V_k(x) \leqslant c_k^{\max}\}$ be a level set of $V_k$, completely contained in $\Phi_k$, for some $c_k^{\max} > 0$. Then $\forall x(0) \in \Omega_k(u_k^{\max})$ the control law guarantees that the origin of the closed–loop system is asymptotically stable.*

## 3. State-feedback fault-tolerant control

In this section, the state-feedback problem is first considered to illustrate the main idea behind the fault detection and isolation and fault-tolerant controller design.

### 3.1. State-feedback fault detection and isolation filter

To be able to detect the occurrence of a fault in a control actuator via observing the state evolution, it is necessary that the control actuator influences the evolution of at least some of the states. To be able to isolate the occurrence of a fault, it becomes further necessary that the control actuator in question be the only one influencing at least some state. To understand this better, consider the following single state, two input example: $\dot{x} = x + u_1(x) + \tilde{u}_1 + u_2(x) + \tilde{u}_2$. As is clear from the equation, the faults in the manipulated inputs $u_1$ and $u_2$ effect the evolution of the state additively, i.e., as the sum $(\tilde{u}_1 + \tilde{u}_2)$. While it may be possible to detect that a fault has occurred in either $u_1$ or $u_2$ (if the faults do not cancel out each other, i.e., if $\tilde{u}_1 + \tilde{u}_2 \neq 0$), it is not possible, in this case, to determine by observing the evolution of the system (and finding it to be different when compared to the expected evolution with $\tilde{u}_1 = \tilde{u}_2 = 0$) whether $\tilde{u}_1 \neq 0$ or $\tilde{u}_2 \neq 0$, or both. In other words, while it may be possible to detect the occurrence of a fault, it is not possible to isolate it using any available technique (data-based or model-based). Below a verifiable assumption on the structure of the system of Eq. (1) that allows for fault detection and isolation is formulated.

**Assumption 1.** Consider the system of Eq. (1) in configuration $k$ under state-feedback. Then for every input $u_{j,k}$, $j = 1, \ldots, m$, there exists a unique state $x_{i,k}$, $i \in \{1, \ldots, n\}$ such that with $x_{i,k}$ as output, the relative degree of $x_{i,k}$ with respect to $u_{j,k}$ and only with respect to $u_{j,k}$ is equal to 1.

**Remark 1.** Assumption 1 rigorously states a fundamental requirement to achieve fault-detection and isolation and does not represent a limitation of the proposed approach. It simply states that the effect of a specific control actuator on the system evolution needs to be completely distinguishable to allow for isolation of fault in that specific control actuator. If this effect is not fundamentally distinguishable, then no fault-isolation technique (model-based or data-based) will be able to isolate the occurrence of such fault (see Remark 3 for further discussion on this point).

Consider now the system of Eq. (1) in configuration $k$ for which Assumption 1 holds. Theorem 2 formulates the fault detection and isolation filter.

**Theorem 2.** *Consider the system of Eq.* (1) *in configuration k which satisfies Assumption* 1, *under the control law of Eq.* (2). *Let the fault detection and isolation filter for the jth manipulated input in the kth configuration be described by*

$$\begin{aligned} \dot{\tilde{x}}_{i,k} &= f_i(x_1, \ldots, \tilde{x}_{i,k}, \ldots, x_n) + g_{j,k}[i](x_1, \ldots, \tilde{x}_{i,k}, \ldots, x_n) \\ &\quad \times u_{j,k}(x_1, \ldots, \tilde{x}_{i,k}, \ldots, x_n), \\ e_{i,k} &= \tilde{x}_{i,k} - x_i, \end{aligned} \tag{5}$$

*where $g_{j,k}[i]$ denotes the ith element of the vector $g_{j,k}$, $\tilde{x}_{i,k}(0) = x_i(0)$ and the subscripts $i, k$ refer to the ith state under the kth control configuration. Let $T_{j,k}^f$ be the earliest time for which $\tilde{u}_{j,k} \neq 0$, then the fault detection and isolation filter of Eq.* (5) *ensures that $e_{i,k}(T_{j,k}^{f\,+}) \neq 0$. Also, $e_{i,k}(t) \neq 0$ only if $\tilde{u}_{j,k}(s) \neq 0$ for some $0 \leqslant s < t$.*

**Proof of Theorem 2.** *Part* 1: First, the *only if* part of the theorem is shown by contradiction. To this end, consider the equation describing the evolution of the $i$th state, $x_i$ described by

$$\dot{x}_i = f_i(x) + g_{j,k}[i](x)(u_{j,k}(x) + \tilde{u}_{j,k}(t)) \tag{6}$$

and let us assume that $\tilde{u}_{j,k}(s) = 0$, for all $0 \leqslant s < t$. Then for all $0 \leqslant s < t$ Eq. (6) reduces to

$$\dot{x}_i = f_i(x) + g_{j,k}[i](x) u_{j,k}(x). \tag{7}$$

Since $x_i(0) = \tilde{x}_{i,k}(0)$, therefore $\dot{x}_i(s) = \dot{\tilde{x}}_{i,k}(s)$ for $s = 0$ and subsequently for all $0 \leqslant s < t$. Therefore, $e_{i,k}(s) = 0$ for all $0 \leqslant s < t$, which leads to a contradiction. This means that the assumption that $\tilde{u}_{j,k}(s) = 0$, for all $0 \leqslant s < t$ does not hold, i.e., $\tilde{u}_{j,k}(s) \neq 0$ for some $0 \leqslant s < t$. This completes the proof of the first part of the theorem.

*Part* 2: To prove the *if* part of the theorem, consider once again Eqs. (5) and (6) with $\tilde{u}_j^k(t) = 0$ for all $t \leqslant T_k^f$. Then following the line of reasoning as in Part 1, $x_i(T_{j,k}^f) = \tilde{x}_{i,k}(T_{j,k}^f)$. From $\tilde{u}_{j,k}(T_{j,k}^f) \neq 0$ follows $\dot{x}_i(T_{j,k}^f) \neq \dot{\tilde{x}}_{i,k}(T_{j,k}^f)$, and therefore, that $x_i(T_{j,k}^{f\,+}) \neq \tilde{x}_{i,k}(T_{j,k}^{f\,+})$, i.e., $e_{i,k}(T_{j,k}^{f\,+}) \neq 0$. This completes the proof of Theorem 2. □

**Remark 2.** The *if* part of Theorem 2 characterizes the detection capabilities where the residual for a manipulated input becomes non-zero if a fault occurs in the given manipulated input. The *only if* part of the theorem allows isolation since a residual is non-zero only if a fault has occurred at some previous time in the given manipulated input. Note that in general it is possible that a fault occurs for some time and disappears, and also the fault profile is such that after some time the evolution of the system becomes identical again to the fault-free system, in which case the residual would once again go back to zero. The immediate detection capability of the filter above, however, precludes the possibility that such a fault goes undetected.

**Remark 3.** Note that Assumption 1 is a sufficient condition that allows fault detection and isolation filter design, and can be readily relaxed. For instance, if the inputs influence the evolution of the states in an 'upper triangular' or 'lower triangular' form, fault detection and isolation is possible using the same idea as in Theorem 2. As an illustration, consider a two state two input system, of the form

$$\begin{aligned}\dot{x}_1 &= f_1(x) + g_1[1](x)(u_1(x) + \tilde{u}_1(t)),\\ \dot{x}_2 &= f_2(x) + g_1[2](x)(u_1(x) + \tilde{u}_1(t))\\ &\quad + g_2[2](x)(u_2(x) + \tilde{u}_2(t)),\end{aligned} \tag{8}$$

where $f_i(\cdot)$ denotes the $i$th elements of the vector function $f(\cdot)$ and $g_i[j]$ denotes the $j$th element of the vector $g_i$. While this system does not satisfy Assumption 1, fault detection and isolation can still be achieved. Specifically, a filter design of the form of Eq. (5) can be used to build a detection filter for the first manipulated input. The second filter can then be designed as

$$\begin{aligned}\dot{\tilde{x}}_2 &= f_2(x_1, \tilde{x}_2) + g_1[2](x_1, \tilde{x}_2)(u_1(x_1, \tilde{x}_2))\\ &\quad + g_2[2](x_1, \tilde{x_2})(u_2(x_1, \tilde{x_2})),\\ e_2 &= \tilde{x}_2 - x_2.\end{aligned} \tag{9}$$

In this setup, faults in $u_1$ will be captured in both $e_1$ and $e_2$, while faults in $u_2$ will only effect $e_2$. The task of fault detection and isolation can therefore be carried out via a simple process of elimination.

### 3.2. State-feedback fault-tolerant controller

In this section we address the problem of determining an appropriate backup configuration. The first requirement for an appropriate backup control configuration is that it does not use the faulty control actuator. Secondly, the limitations imposed by the presence of input constraints must be accounted for, and in particular, a backup configuration should be implemented for which the state of the closed-loop system resides in its stability region. This idea is formalized in Theorem 3.

**Theorem 3.** *Consider the closed-loop system of Eqs.* (1)–(2) *under state-feedback and let* $x(0) := x_0 \in \Omega_{k_0}$ *for some* $k_0 \in \mathbf{K}$. *Let* $T_{j,k_0}$ *be the earliest time such that* $e_{i,k_0} \neq 0$ *for some* $i$ *corresponding to a manipulated input* $u_{j,k_0}$ *in Eq.* (5). *Then the following switching rule*:

$$k(t) = \left\{ \begin{array}{ll} k_0, & 0 \leqslant t < T_{j,k_0},\\ q \neq k_0, & t \geqslant T_{j,k_0}, x(T_{j,k_0}) \in \Omega_q,\\ & u_{j,k_0} \notin u_q \end{array} \right\} \tag{10}$$

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

**Proof of Theorem 3.** Consider the two cases, (1) $e_{i,k_0}(t) = 0$ for all $t \geqslant 0$ for all $i \in \{1, \ldots, n\}$ and (2) $e_{i,k_0}(t) \neq 0$ for some $T_{j,k_0}$ for some $j \in \{1, \ldots, m\}$.

*Case* 1: $e_{i,k_0}(t) = 0\ \forall t \geqslant 0$ for all $j \in \{1, \ldots, m\}$ implies (using Theorem 2) that $\tilde{u}_{j,k}(t) = 0$ for all $t \geqslant 0$ and for all $j \in \{1, \ldots, m\}$. The switching rule of Eq. (10) then dictates that $k(t) = k_0\ \forall t \geqslant 0$. Since $x(0) \in \Omega_{k_0}$, asymptotic stability of the origin of the closed-loop system follows from Theorem 1.

*Case* 2: If $e_{i,k_0}(t) \neq 0$ for some $T_{j,k_0}$ for some $j \in \{1, \ldots, m\}$, the switching rule dictates switching to configuration $q$ such that $x(T_{j,k_0}) \in \Omega_q$. Closed-loop stability of the origin of the closed-loop system again follows from Theorem 1. This completes the proof of Theorem 3. □

**Remark 4.** In the event that a given control configuration can continue to be stabilizing even with one failed control actuator (verified by the presence of the state at the time of the failure in the stability region of this 'reduced' control configuration) Theorem 3 dictates the continued use of the control configuration while preserving stability (without needing to invoke a backup control actuator). However, for faults that do not preserve the stability of the active control configuration, early detection of a fault enhances the chances that corrective action can be taken in time to achieve fault-tolerant control. Note also that in the presence of plant model mismatch or unknown disturbances, the value of $e_{i,k}(t)$ will be non-zero even in the absence of faults. The presence of time varying disturbances $\theta(t)$ with known bounds $\theta_b$ on the disturbances can be accounted for in the filter design as well as reconfiguration. Specifically, the filter can be redesigned to declare a fault only if the value of $\|e_{i,k}(t)\|$ increases beyond some threshold, $\delta(\theta_b)$, where $\delta(\theta_b)$ accounts for the deviation of the plant dynamics from the nominal dynamics in the absence of faults. Furthermore, robust controllers can be utilized and the robust stability regions can be used as criteria for deciding which backup configuration should be implemented in the closed-loop system.

## 4. Output-feedback fault-tolerant control

In this section, the case where only some of the process states are available for measurement is considered and an

output–feedback controller design (El-Farra & Christofides, 2001) that provides estimates of the states (for other examples of nonlinear observer and output-feedback controller designs, see Kazantzis & Kravaris, 1999; Khalil & Esfandiari, 1993) along with an explicit characterization of the output-feedback stability region is first reviewed.

### 4.1. Output feedback controller

In the absence of full state measurement, at least enough measurements need to be available to 'reconstruct' or estimate the states from the available measurements. Assumption 2 states this requirement which will be used in designing the output feedback controllers for the individual configurations (see El-Farra & Christofides, 2001 for further discussion on the necessity of such an assumption).

**Assumption 2.** Consider the system of Eq. (1) in configuration $k$ with $\tilde{u}_k \equiv 0$. There exists a set of integers $r_{1,k}, r_{2,k}, \ldots, r_{m,k}$ (with $r_{1,k} + r_{2,k} + \cdots + r_{m,k} = n$ for each $k$) and a coordinate transformation $\zeta_k = \chi_k(x)$ such that the representation of the system of Eq. (1), in the $\zeta_k$ coordinates, takes the form:

$$\begin{aligned}
&\dot{\zeta}^{(i)}_{1,k} = \zeta^{(i)}_{2,k},\\
&\vdots\\
&\dot{\zeta}^{(i)}_{r_{i,k}-1} = \zeta^{(i)}_{r_{i,k}},\\
&\dot{\zeta}^{(i)}_{r_{i,k}} = L_f^{r_{i,k}} h_i(x) + L_{g_{i,k}} L_f^{r_{i,k}-1} h_i(x) u_{i,k},
\end{aligned} \tag{11}$$

where $x = \chi_k^{-1}(\zeta_k)$ and $\zeta_k = [\zeta_k^{(1)\mathrm{T}} \cdots \zeta_k^{(m)\mathrm{T}}]^{\mathrm{T}}$.

**Theorem 4** (*El-Farra and Christofides, 2001*). *Consider the constrained nonlinear process of Eq.* (1) *with* $\tilde{u}_k(t) \equiv 0$ *for which Assumption* 2 *holds, under the output-feedback controller using the kth control configuration*:

$$\dot{\tilde{y}}_{i,k} = \begin{bmatrix} -L_{i,k}a^{(1)}_{i,k} & 1 & 0 & \cdots & 0\\ -L^2_{i,k}a^{(2)}_{i,k} & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ -L^{r_i-1}_{i,k}a^{(r_i-1)}_{i,k} & 0 & 0 & \cdots & 1\\ -L^{r_i}_{i,k}a^{(r_i)}_{i,k} & 0 & 0 & \cdots & 0 \end{bmatrix} \tilde{y}_{i,k} + \begin{bmatrix} L_{i,k}a^{(1)}_{i,k}\\ L^2_{i,k}a^{(2)}_{i,k}\\ \vdots\\ L^{n-1}_{i,k}a^{(r_i-1)}_{i,k}\\ L^n_{i,k}a^{(r_i)}_{i,k} \end{bmatrix} y_{i,k},$$

$$u_k = -w_k(\hat{x}, u_k^{\max})(L_{G_k} V_k(\hat{x}))^{\mathrm{T}}, \tag{12}$$

*where* $\hat{x} = \chi_k^{-1}(sat(\tilde{y}_k))$, $\tilde{y}_k = [\tilde{y}^{\mathrm{T}}_{(1,k)} \cdots \tilde{y}^{\mathrm{T}}_{(m,k)}]^{\mathrm{T}}$, $i = 1, \ldots, m$ *where the parameters,* $a^{(1)}_{i,k}, \ldots, a^{(r_i)}_{i,k}$ *are chosen such that the polynomial* $s^{r_i} + a^{(1)}_{i,k} s^{n-1} + a^{(2)}_{i,k} s^{r_i-2} + \cdots + a^{(r_i)}_{i,k} = 0$ *is Hurwitz,* $\hat{x} = \chi_k^{-1}(sat(\tilde{y}))$, $sat(\cdot) = \min\{1, \zeta_{\max,k}/\|\cdot\|\}(\cdot)$, *with* $\zeta_{\max,k} = \beta_\zeta(\delta_{\zeta,k}, 0)$ *where* $\beta_\zeta$ *is a class* **KL** *function and* $\delta_{\zeta,k}$ *is the maximum value of the vector* $[l_1^{\mathrm{T}}(x) l_2^{\mathrm{T}}(x) \cdots l_m^{\mathrm{T}}(x)]^{\mathrm{T}}$ *for* $V_k(x) \leqslant \delta_{b,k}$, *where* $l_i(x) = [h_i(x) L_f h_i(x) \cdots L_f^{r_i-1} h_i(x)]^{\mathrm{T}}$, *and let* $\varepsilon_k = \max_i 1/L_{i,k}$. *Then, given* $\Omega_{b,k} := \{x \in \mathbf{R}^n | V_k(x) \leqslant \delta_{b,k}\}$ *and positive real numbers* $e_{m,k}$, $\tilde{u}_k^*$ *and* $d_k$ *there exists* $\varepsilon_k^* > 0$, $T_k^b > 0$ *such that if* $\varepsilon_k \in (0, \varepsilon_k^*]$, $x(0) \in \Omega_{b,k}$, *and* $\|\tilde{y}(0)\| \leqslant \delta_{\zeta,k}$, *the origin of the closed-loop system is asymptotically* (*and locally exponentially*) *stable, and if* $\|\tilde{u}_k(t)\| \leqslant \tilde{u}_k^*$ *then* $\|x(t) - \hat{x}(t)\| \leqslant e_{m,k}$ *for all* $t \geqslant T_k^b$ *and* $\limsup_{t\to\infty} x(t) = d_k$.

Theorem 4 provides the estimation and controller design that guarantees asymptotic stability in the case of fault-free system as well as practical stability in the presence of 'small' faults (that preserve stability). The result relies on closeness of the state estimates to the true states over the infinite time interval. In fault detection and isolation, the closeness of solution would be required to hold even in the presence of large, possibly destabilizing faults, at least up to some finite time to be able to detect and isolate the faults. In other words, it should not happen that the actuator fault causes the process states to become unobservable (i.e., results in a loss of confidence on the state estimates) even before the state estimates can be used to isolate the fault. This inherent requirement is formalized in Assumption 3.

**Assumption 3.** Consider the system of Eq. (1) in configuration $k$ under the output-feedback controller of Theorem 4. There exist positive real numbers $T_{\mathrm{close}} > T_k^b$ and $\delta_k$ such that if $\|\tilde{u}_k(t)\| > \tilde{u}_k^*$ for some $T_{\mathrm{fault}} > T_k^b$ where $\tilde{u}_k^*$ was defined in Theorem 4, then $\|x(t) - \hat{x}(t)\| \leqslant e_{m,k}$ for all $t \in [T_k^b, T_{\mathrm{fault}} + T_k^{\mathrm{close}}]$ and $\| \int_{T_k^b}^t g_{j,k}[i](x(\tau)) \tilde{u}_{j,k}(\tau)\, \mathrm{d}\tau \| > \delta_k$ for some $t \in [T_{\mathrm{fault}}, T_{\mathrm{fault}} + T_k^{\mathrm{close}}]$.

Due to the lack of full state measurements, the reconfiguration decision needs to be done based only on the available state estimates. It is therefore necessary to be able to make reliable inferences regarding the states using the state estimates. Proposition 1 establishes the existence of a set, $\Omega_{s,k} := \{x \in \mathbf{R}^n : V_k(x) \leqslant \delta_{s,k}\}$, such that once the state estimation error has fallen below a certain value (note that the decay rate can be controlled by adjusting $L_k$), the presence of the state within the output-feedback stability region, $\Omega_{b,k}$, can be guaranteed by verifying the presence of the state estimates in the set $\Omega_{s,k}$. A similar approach was employed in the construction of the output-feedback stability regions $\Omega_{b,k}$ and the regions for the state estimates $\Omega_{s,k}$ in the context of output-feedback control of linear systems in Mhaskar et al. (2004), and for nonlinear systems in El-Farra et al. (2005). For a proof of the proposition, see El-Farra et al. (2005).

**Proposition 1.** *Given any positive real number* $\delta_{b,k}$, *there exist positive real numbers* $e^*_{m,k}$ *and* $\delta_{s,k}$ *such that if* $\|x - \hat{x}\| \leqslant e_{m,k}$, *where* $e_{m,k} \in (0, e^*_{m,k}]$, *and* $V_k(\hat{x}) \leqslant \delta_{s,k}$, *then* $V_k(x) \leqslant \delta_{b,k}$.

### 4.2. Output-feedback fault detection and isolation filter

For the system of Eq. (1), the fault detection and isolation filter for the $j$th manipulated input in the $k$th configuration is designed as

$$\begin{aligned}\dot{\tilde{x}}_{i,k} &= f_i(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) \\ &\quad + g_{j,k}[i](\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) \\ &\quad \times u_{j,k}(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}), \\ e_{i,k} &= \hat{x}_{i,k} - \tilde{x}_{i,k}, \end{aligned} \tag{13}$$

where $g_{j,k}[i]$ denotes the $i$th element of the vector $g_{j,k}$, and $\tilde{x}_{i,k}(T_k^b) = \hat{x}_{i,k}(T_k^b)$, where $T_k^b$ was defined in Theorem 4.

**Proposition 2.** *Consider the nonlinear system of Eq.* (1), *for a fixed mode under the output-feedback controller of Eq.* (12) *and the filter of Eq.* (13). *Given* $\tilde{u}_{j,k}^*$, $\delta_k$ *and* $T_k^{\text{close}}$ *there exist positive real numbers* $\delta_{j,k}$ *and* $\varepsilon_k^{**}$ *such that if* $|\tilde{u}_{j,k}(t)| \geqslant \tilde{u}_{j,k}^*$ *for some* $T_k^{\text{fault}} \geqslant T_{b,k}$ *and* $\varepsilon_k \leqslant \min\{\varepsilon_k^*, \varepsilon_k^{**}\}$ *then* $\|e_{i,k}(t)\| > \delta_{j,k}$ *for some* $t \in [T_k^{\text{fault}}, T_k^{\text{fault}} + T_k^{\text{close}}]$.

**Proof of Proposition 2.** Consider, the filter of Eq. (13) and the evolution of $x_i$ for $t \in [T_k^b, T_k^{\text{fault}} + T_k^{\text{close}}]$, i.e., consider the systems

$$\begin{aligned}\dot{\tilde{x}}_{i,k} &= f_i(x) + g_{j,k}[i](x)(u_{j,k}(x)) \\ &\quad + (f_i(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) - f_i(x)) \\ &\quad + (g_{j,k}[i](\hat{x}_{1,k}), \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) \\ &\quad \times u_{j,k}(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) \\ &\quad - g_{j,k}[i](x)u_{j,k}(x), \end{aligned} \tag{14}$$

$$\dot{x}_{i,k} = f_i(x) + g_{j,k}[i](x)(u_{j,k}(x) + \tilde{u}_{j,k}(t)). \tag{15}$$

We have that

$$\begin{aligned}\dot{x}_{i,k} - \dot{\tilde{x}}_{i,k} &= g_{j,k}[i](x)\tilde{u}_{j,k}(t) \\ &\quad + (f_i(x) - f_i(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k})) \\ &\quad + (g_{j,k}[i](x)u_{j,k}(x)) \\ &\quad - g_{j,k}[i](\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, \hat{x}_{n,k}) \\ &\quad \times u_{j,k}(\hat{x}_{1,k}, \ldots, \tilde{x}_{i,k}, \ldots, x_{n,k} + \hat{x}_{n,k}). \end{aligned} \tag{16}$$

Note that $\hat{x}(T_b) - x(T_b)$ can be made as small as desired by choosing a sufficiently small $\varepsilon$. From the continuity of $f_i(\cdot)$ and $g_{j,k}[i](\cdot)$, this implies that the last two terms in Eq. (16) can be made as small as desired. The difference between $\dot{x}_{i,k}$ and $\dot{\tilde{x}}_{i,k}$ can therefore be made as close as desired to $g_{j,k}[i](x)(\tilde{u}_{j,k}(t))$. Using Assumption 3, therefore, given a time $T^{\text{close}} > T_k^b$, there exists a positive real number $\delta_{j,k}^* = \delta_k^*$ such that if $|\tilde{u}_{j,k}(t)| > \tilde{u}_{j,k}^*$ for some $T_k^{\text{fault}} \geqslant T_k^b$ then $\|x_{i,k}(t) - \tilde{x}_{i,k}(t)\| \geqslant \delta_{j,k}^*$ for some $t \in [T_k^{\text{fault}}, T_k^{\text{fault}} + T_k^{\text{close}}]$.Finally, once again since $\hat{x}(t) - x(t)$ can be made as close as desired (up until $T_k^{\text{close}}$), then given that $\|x_{i,k}(t) - \tilde{x}_{i,k}(t)\| \geqslant \delta_{j,k}^*$, there exists a positive real number $\delta_{j,k}$ such that $\|e_{i,k}\| = \|\hat{x}_{i,k}(t) - \tilde{x}_{i,k}(t)\| \geqslant \delta_{j,k}$ for some $t \in [T_k^{\text{fault}}, T_k^{\text{fault}} + T_k^{\text{close}}]$. In summary, there exists a positive real number $\varepsilon_k^{**}$ such that if $\varepsilon_k \leqslant \min\{\varepsilon_k^*, \varepsilon_k^{**}\}$ and $|\tilde{u}_{j,k}(t)| \geqslant \tilde{u}_{j,k}^*$ for some $T_k^{\text{fault}} \geqslant T_{b,k}$ then $\|e_{i,k}(t)\| > \delta_{j,k}$ for some $t \in [T_k^{\text{fault}}, T_k^{\text{fault}} + T_k^{\text{close}}]$. □

**Remark 5.** Note that unlike the case of full state-feedback, the fault detection filter is initialized only after the passage of some short period of time, $T_k^b$ (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 $\tilde{x}_{i,k}$ 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. While the use of a higher observer gain impacts negatively on the noise handling capabilities of the state estimator, an observer gain is chosen that represents a desirable tradeoff between handling measurement noise and the necessity to achieve early fault detection (note that fault isolation is an added consideration over and above that of obtaining state estimates to implement feedback control alone). Note that unlike the case of full state availability, where the filter is able to immediately detect and isolate the occurrence of fault, the lack of measurements which induces the error in the initialization of the filter states allows detection of only such faults that impact the states of the closed–loop system above a certain threshold. The key is to ensure that the only faults that may go undetected do not undesirably impact the stability of the closed-loop system.

### 4.3. Output-feedback fault detection and isolation and fault-tolerant control

Consider the nonlinear system of Eq. (1), for which the output-feedback controller of Eq. (12) and the filters of Eq. (13) have been designed for each manipulated input under the primary configuration, $k(0) = k_0$ under possible faults in only one control actuator. The theorem below formalizes the integrated output-feedback fault detection and isolation and fault-tolerant control structure.

**Theorem 5.** *Let* $k(0) = k_0$ *for some* $k_0 \in \mathbf{K}$, $x(0) \in \Omega_{b,k_0}$, $\tilde{x}_{i,k}(T_{i,k}^b) = \hat{x}(T_{i,k}^b)$. *Given a positive real number* $d_{k_0}$ *there exist positive real numbers* $\delta_{i,k}$ *and* $\varepsilon_k^{***}$ *such that if* $\varepsilon_k \in (0, \varepsilon_k^{***}]$ *then under the switching rule*

$$k(t) = \left\{ \begin{array}{ll} k_0, & 0 \leqslant t < T_{\text{detect}}, \\ q \neq k_0, & t \geqslant T_{\text{detect}}, \hat{x}(T_{\text{detect}}) \in \Omega_{s,q}, \\ & u_{j,k_0} \notin u_q \end{array} \right\} \tag{17}$$

*where* $T_{\text{detect}}$ *is the earliest time for which* $\|e_{i,k}\| > \delta_{i,k}$ *for some* $i \in [0, \ldots, n]$, *we have that* $\limsup_{t\to\infty} x(t) \leqslant d_{k_0}$.

**Proof of Theorem 5.** Consider the two cases, (1) $\|e_{i,k}(t)\| \leqslant \delta_{i,k}$ $\forall t$ and (2) $\|e_{i,k}(t)\| > \delta_{i,k}$ for some $t = T_{\text{detect}}$.

*Case* 1: From Theorem 4, we have that given a positive real number $d_k$, there exist positive real numbers $\varepsilon_k^{**}$ and $\tilde{u}_k^*$ such that if $\|\tilde{u}_{j,k}(t)\| \leqslant \tilde{u}_k^*$, then $\limsup_{t\to\infty} x(t) = d_{k_0}$. For such choices of $\varepsilon_k^{**}$ and $\tilde{u}_k^*$, we have from Proposition 2 that there exists a positive real number $\delta_{i,k}$ such that if $\varepsilon_k \in (0, \min\{\varepsilon_k^*, \varepsilon_k^{**}\} = \varepsilon_k^{***}]$ then $\|e_{i,k}\| \leqslant \delta_{i,k} \Rightarrow \|\tilde{u}_{j,k}(t)\| \leqslant \tilde{u}_k^*$. Therefore, for the above choices of $\tilde{u}_k^*$,$\varepsilon_k^{***}$ and $\delta_{j,k}$, we have that $\|e_{i,k}(t)\| \leqslant \delta_{i,k}$ implies $\|\tilde{u}_{i,k_0}(t)\| \leqslant \tilde{u}_{i,k_0}^*$ yielding $\limsup_{t\to\infty} x(t) = d_{k_0}$.

*Case* 2: The switching rule of Eq. (17) ensures that at $t = T_{\text{detect}}$, $\hat{x}(t) \in \Omega_{s,q}$, which in turn implies that $x(t) \in \Omega_{b,q}$ (Proposition 1). This, together with the switching to the $q$th control configuration ensures asymptotic stability of the origin of the closed–loop system (Theorem 4). In either cases we get that $\limsup_{t\to\infty} x(t) \leqslant d_{k_0}$. This completes the proof of the theorem. □

**Remark 6.** Note that the above switching rule provides a sufficient condition for practical stability. In other words, the value of the residual going above the threshold does not imply that a destabilizing fault has occurred. However, the value of the residual being less than the threshold does ensure that no destabilizing fault has occurred. This is not a limitation of the proposed filter, but stems simply from the fundamental problem of differentiating between the error introduced in the filtering system due to the presence of estimation errors and those due to the faults. Note also that while the algorithm above is written for the case of a single fault, generalization to multiple faults, whether simultaneous or otherwise, is straightforward: the current fault detection filter design can detect and isolate multiple faults, while the reconfiguration rule can be 're-initialized' after the first backup control configuration is activated to handle subsequent faults.

## 5. Simulation example

Consider two well mixed, non-isothermal continuously stirred tank reactors, 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. $A$ is the reactant species, $B$ is the desired product and $U$ 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 $T_{03}$. Under standard modeling assumptions, a mathematical model of the process can be derived from material and energy balances and takes the following form:

$$\frac{dT_1}{dt} = \frac{F_0}{V_1}(T_0 - T_1) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A1}, T_1) + \frac{Q_1 + Q_3}{\rho c_p V_1},$$

$$\frac{dC_{A1}}{dt} = \frac{F_0}{V_1}(C_{A0} - C_{A1}) - \sum_{i=1}^{3} R_i(C_{A1}, T_1),$$

$$\frac{dT_2}{dt} = \frac{F_0}{V_2}(T_1 - T_2) + \frac{F_3}{V_2}(T_{03} - T_2) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{A2}, T_2) + \frac{Q_2}{\rho c_p V_2},$$

Table 1
Process parameters and steady state values for the chemical reactors of Eq. (18)

| | |
|---|---|
| $F_0 = 4.998\,\text{m}^3/\text{h}$ | $F_1 = 4.998\,\text{m}^3/\text{h}$ |
| $F_3 = 4.998\,\text{m}^3/\text{h}$ | $V_1 = 0.5\,\text{m}^3$ |
| $R = 8.314\,\text{kJ/kmol K}$ | $V_2 = 0.5\,\text{m}^3$ |
| $T_0 = 300\,\text{K}$ | $T_{03} = 300\,\text{K}$ |
| $C_{A0} = 4.0\,\text{kmol/m}^3$ | $C^s_{A03} = 3.0\,\text{kmol/m}^3$ |
| $\Delta H_1 = -5.0 \times 10^4\,\text{kJ/kmol}$ | $k_{10} = 3.0 \times 10^6\,\text{h}^{-1}$ |
| $\Delta H_2 = -5.2 \times 10^4\,\text{kJ/kmol}$ | $k_{20} = 3.0 \times 10^5\,\text{h}^{-1}$ |
| $\Delta H_3 = -5.4 \times 10^4\,\text{kJ/kmol}$ | $k_{30} = 3.0 \times 10^5\,\text{h}^{-1}$ |
| $E_1 = 5.0 \times 10^4\,\text{kJ/kmol}$ | $c_p = 0.231\,\text{kJ/kg K}$ |
| $E_2 = 7.53 \times 10^4\,\text{kJ/kmol}$ | $\rho = 1000.0\,\text{kg/m}^3$ |
| $E_3 = 7.53 \times 10^4\,\text{kJ/kmol}$ | $T^s_1 = 388.57\,\text{K}$ |
| $C^s_{A1} = 3.59\,\text{kmol/m}^3$ | $T^s_2 = 433.96\,\text{K}$ |
| $C^s_{A2} = 2.88\,\text{kmol/m}^3$ | |

$$\frac{dC_{A2}}{dt} = \frac{F_0}{V_2}(C_{A1} - C_{A2}) + \frac{F_3}{V_2}(C_{A03} - C_{A2}) - \sum_{i=1}^{3} R_i(C_{A2}, T_2), \tag{18}$$

where $R_i(C_{Aj}, T_j) = k_{i0}\exp(-E_i/RT_j)C_{Aj}$, for $j = 1, 2$. $T$, $C_A$, $Q$, 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. $\Delta H_i$, $k_i$, $E_i$, $i = 1, 2, 3$, denote the enthalpies, pre-exponential constants and activation energies of the three reactions, respectively, $c_p$ and $\rho$ denote the heat capacity and density of the fluid. The values of the process parameters can be found in Table 1. CSTR 1, with $Q_1 = Q_3 = 0$, has three steady states: two locally asymptotically stable and one unstable at $(T^s_1, C^s_{A1}) = (388.57\,\text{K}, 3.59\,\text{kmol/m}^3)$. The unstable steady state of CSTR 1 corresponds to three steady states for CSTR 2 (with $Q_2 = 0$), one of which is unstable at $(T^s_2, C^s_{A2}) = (433.96\,\text{K}, 2.88\,\text{kmol/m}^3)$.

The control objective is to stabilize the reactors at the (open-loop) unstable steady state. Operation at this point is typically sought to avoid high temperatures while simultaneously achieving reasonable reactant conversion. To accomplish this objective in the presence of actuator failures, we consider as input candidates $Q_1$, subject to the constraint $|Q_1| \leqslant 2.33(10^6)\,\text{kJ/h}$, $Q_2$, subject to the constraint $|Q_2| \leqslant 1.17(10^6)\,\text{kJ/h}$, and $Q_3$ (an emergency fall-back heat exchanger on reactor one), subject to the constraint $|Q_3| \leqslant 2.33(10^6)\,\text{kJ/h}$. The primary control configuration ($k = 1$) involves two inputs consisting of the two primary heating jackets ($Q_1$, $Q_2$). In the event of a partial failure in this configuration the supervisor needs to detect and isolate the fault and activate a fall-back configuration ($Q_3$, $Q_2$) in order to maintain closed–loop stability.

We first illustrate the application of the fault detection and isolation and fault-tolerant control under state-feedback control. Several steps have been taken to account for practical considerations such as plant-model mismatch, measurement sampling, noise and delay. The temperature measurements are assumed to have a gaussian noise with a standard deviation of

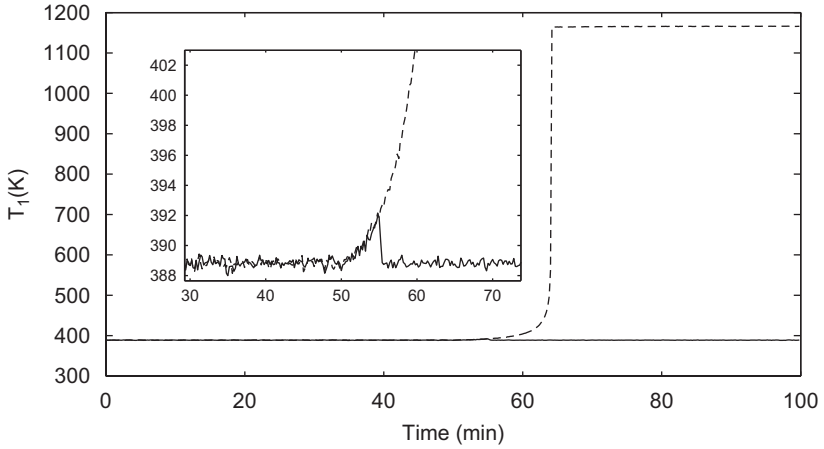



Fig. 1. Evolution of reactor one closed-loop temperature profile under the switching rule of Theorem 3 (solid line) and in the absence of fault-tolerant control (dashed line) subject to failure reactor one heating jacket.

0.2 K, and the concentration measurements are assumed to have a gaussian noise with a standard deviation of 0.01 kmol/m$^3$. The measurements are sampled at a rate of one measurement every 12 s with a 12 s delay. $F_0$ and $F_3$ for the process are each 5% smaller than the $F_0$ and $F_3$ used in the model. The residual threshold to account for the presence of plant-model mismatch and noise is chosen as 3 K.

A quadratic Lyapunov function of the form $V_k = x^{\mathrm{T}} P_k x$, where $P_k$ is a diagonal (and therefore positive-definite symmetric) matrix with 0.01, 0.001, 0.008 and 0.001 as the elements on the diagonal is chosen. Note that this particular choice of the Lyapunov function is driven by the desire to appropriately 'scale' the variables, and not by the necessity for the Lyapunov function to be a control Lyapunov function. In the simulation example, the construction of the set $\Phi$ is executed by specifically ensuring that for all points in the set, negative definiteness of $\dot{V}$ can be achieved (either with or without control effort), thereby ensuring that the chosen Lyapunov function is a control Lyapunov function.

The state-feedback controller of Eq. (2) is subsequently designed for both the control configurations, and their stability region characterized, yielding $c_1^{\max} = c_2^{\max}$ equal to 0.2. The reactors as well as the filter states for the first control configuration are initialized at the steady state $T_1(0) = 388.57$ K, $C_{A1}(0) = 3.59$ kmol/m$^3$, $T_2(0) = 433.96$ K, $C_{A2}(0) = 2.88$ kmol/m$^3$ with a $V_1(x) = 0 \leqslant c_1^{\max} = 0.2$. As shown by the solid line in Fig. 1 the controller keeps the process states close to the desired steady state until $Q_1$ fails 50 min after reactor startup. As can be seen in Figs. 2 and 3 the value of only the residual $e_1(t)$ increases to the detection threshold of 3, thereby detecting as well as isolating the faults in the control actuator $Q_1$. If the supervisor does not perform any switching at this point, closed-loop stability is not achieved (dashed lines in Fig. 1). Since the fall-back configuration does not use the failed actuators and the state of the closed loop system is within the stability region of the backup control configuration ($V_2(x(t = 54.8 \text{ min})) = 0.1188 < c_2^{\max} = 0.2$), the supervisor activates the fall-back configuration with the manipulated inputs $Q_3$ and $Q_2$ (solid line in Fig. 1) which stabilizes the closed-loop system and achieves fault-tolerant control.

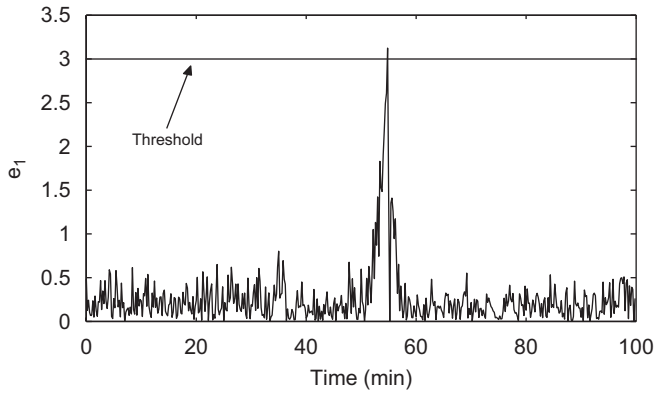



Fig. 2. Evolution of residual $e_1$ corresponding to the manipulated input for reactor one. $e_1$ is initialized at $t = 0$ and again at $t = 54.8$ min.

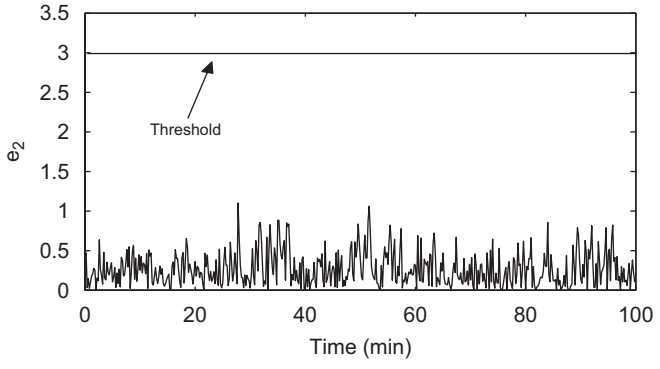



Fig. 3. Evolution of residual $e_2$ corresponding to the manipulated input for reactor two. $e_2$ is initialized at $t = 0$ and again at $t = 54.8$ min.

The next simulation illustrates the case when not all process states are available for measurement. For the output-feedback case, the $P$ matrix for the Lyapunov function was obtained by solving the Riccati inequality for the linearized system.

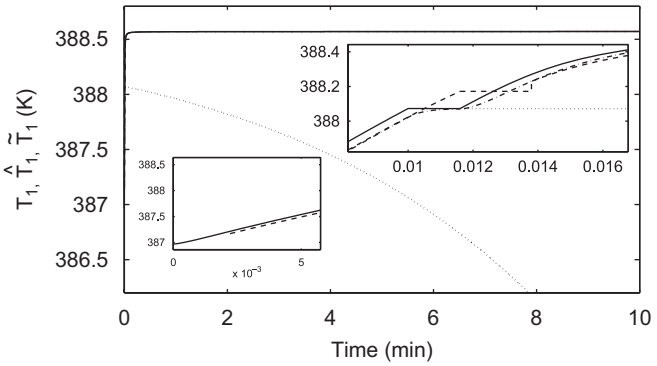



Fig. 4. Evolution of the closed-loop temperature (solid line), estimate of temperature (dash-dotted line), and the temperature profile generated by the FDI filter (dashed line) with fault-tolerant control in place. Evolution of the temperature (dotted line) without fault-tolerant control in place.

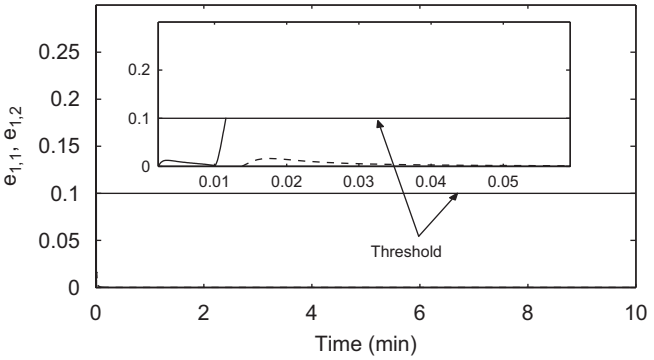



Fig. 5. Evolution of the residual corresponding to $Q_1$ for before switching ($k = 1$, solid line), and $Q_3$ after switching ($k = 2$, dashed line). A fault is declared when $e_{1,1}$ reaches the threshold at 0.1.

In order to implement the state-feedback Lyapunov-based controllers, estimates of $T_1$ and $T_2$ are generated using a state estimator of the form of Eq. (12) with $L_{i,k} = 10\,000$, $a_{i,k}^{(1)} = 5$, and $a_{i,k}^{(2)} = 1$ for $i = 1, 2$ and $k = 1, 2$. The reactors are initialized at $T_1(0) = 386.97\,\text{K}$, $C_{A1}(0) = 3.59\,\text{kmol/m}^3$, $T_2(0) = 432.36\,\text{K}$, and $C_{A2}(0) = 2.88\,\text{kmol/m}^3$. The state estimator is initialized at the steady-state values for this system ($\tilde{T}_1(0) = 388.57\,\text{K}$, $\tilde{C}_{A1}(0) = 3.59\,\text{kmol/m}^3$, $\tilde{T}_2(0) = 433.96\,\text{K}$, and $\tilde{C}_{A2}(0) = 2.88\,\text{kmol/m}^3$). The fault detection filter states are initialized with the value of the state estimates at $t = 0.00132\,\text{s} \equiv T_1^b$. Note that by this time the estimates have converged sufficiently close to the true values as can be seen as the dash-dotted lines in Fig. 4.

As shown by the solid line in Fig. 4, the controller drives the closed-loop system to the desired steady state (for the sake of brevity, only $T_1$ is shown). A complete failure occurs in $Q_1$ early on at $T_f = 0.01\,\text{s}$ while the system is still moving toward the desired steady state. If the fault is not detected and no switching takes place the value of $T_1$ moves away from the desired operating temperature as shown by the dotted line in Fig. 4. However, when the fault detection and isolation filter is utilized we can see that the value of the filter state $\hat{T}_1$, dashed line in Fig. 4, diverges from the estimated value $\tilde{T}_1$. This discrepancy causes the residual $e_{1,1}(t)$ corresponding to $Q_1$ to rise to the threshold value of 0.1 K (chosen to ensure that all destabilizing faults are detected) at time $t = 0.012\,\text{s}$, as shown in Fig. 5. A fault in $Q_1$ is declared at this time, and the supervisor checks the value of the Lyapunov function for $k = 2$. Since $V_2(x(0.012\,\text{s})) = 0.38 < c_2^{\max} = 9.4$ the supervisor activates the fall-back configuration to achieve closed-loop stability (solid line in Fig. 4).

## 6. Conclusions

This work considered the problem of fault detection and isolation and fault-tolerant control for a multi-input multi-output nonlinear system subject to faults in the control actuators and constraints on the manipulated inputs for both the state and output-feedback cases. Necessary conditions for the design of state- and output-feedback fault detection and isolation filters were derived. Filters were designed that essentially capture the difference between fault-free evolution of the system and the observed (or estimated) evolution of the system states to detect and isolate faults in the control actuators. Reconfiguration rules were devised to identify the appropriate backup control configuration accounting for the faulty actuator and constraints. The impact of lack of complete state measurements in the filter design, control law and the reconfiguration logic was illustrated. Finally, the implementation of the fault detection and isolation filters and reconfiguration strategy as well as robustness with respect to plant-model mismatch, measurement sampling and delay and measurement noise were demonstrated via a chemical process example.

## References

Allgöwer, F., & Doyle, F. J. (1997). Nonlinear process control—which way to the promised land?. In *Proceedings of 5th international conference on chemical process control* (pp. 24–45). Tahoe City, CA.

Aradhye, H. B., Bakshi, B. R., Davis, J. F., & Ahalt, S. C. (2004). Clustering in wavelet domain: A multiresolution art network for anomaly detection. *AIChE Journal*, *50*, 2455–2466.

Bao, J., Zhang, W. Z., & Lee, P. L. (2003). Decentralized fault-tolerant control system design for unstable processes. *Chemical Engineering Science*, *58*, 5045–5054.

Bequette, W. B. (1991). Nonlinear control of chemical processes: A review. *Industrial & Engineering Chemistry Research*, *30*, 1391–1413.

Bonivento, C., Isidori, A., Marconi, L., & Paoli, A. (2004). Implicit fault-tolerant control: Application to induction motors. *Automatica*, *40*, 355–371.

Christofides, P. D., & El-Farra, N. H. (2005). *Control of nonlinear and hybrid process systems: Designs for uncertainty, constraints and time-delays*. New York: Springer.

Davis, J. F., Piovoso, M. L., Kosanovich, K., & Bakshi, B. (1999). Process data analysis and interpretation. *Advances in Chemical Engineering*, *25*, 1–103.

DeCarlo, R. A., Branicky, M. S., Pettersson, S., & Lennartson, B. (2000). Perspectives and results on the stability and stabilizability of hybrid systems. *Proceedings of the IEEE*, *88*, 1069–1082.

DePersis, C., & Isidori, A. (2001). A geometric approach to nonlinear fault detection and isolation. *IEEE Transactions on Automatic Control*, *46*, 853–865.

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

El-Farra, N. H., & Christofides, P. D. (2001). Bounded robust control of constrained multivariable nonlinear processes. *Chemical Engineering Science*, *58*, 3025–3047.

El-Farra, N. H., & Christofides, P. D. (2003b). Coordinated feedback and switching for control of hybrid nonlinear processes. *AIChE Journal*, *49*, 2079–2098.

El-Farra, N. H., Gani, A., & Christofides, P. D. (2005). Fault-tolerant control of process systems using communication networks. *AIChE Journal*, *51*, 1665–1682.

El-Farra, N. H., Mhaskar, P., & Christofides, P. D. (2005). Output feedback control of switched nonlinear systems using multiple Lyapunov functions. *Systems & Control Letters*, *54*, 1163–1182.

Frank, P. M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy—a survey and some new results. *Automatica*, *26*, 459–474.

Frank, P. M., & Ding, X. (1997). Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control*, *7*, 403–424.

Garcia-Onorio, V., & Ydstie, B. E. (2004). Distributed, asynchronous and hybrid simulation of process networks using recording controllers. *International Journal of Robotics & Nonlinear Control*, *14*, 227–248.

Henson, M. A., & Seborg, D. E. (1997). *Nonlinear process control*. Englewood Cliffs, NJ: Prentice-Hall.

Kazantzis, N., & Kravaris, C. (1999). Nonlinear observer design using Lyapunov's auxiliary theorem. *Systems & Control Letters*, *34*, 241–247.

Khalil, H. K., & Esfandiari, F. (1993). Semiglobal stabilization of a class of nonlinear systems using output feedback. *IEEE Transactions on Automatic Control*, *38*, 1412–1415.

Kresta, J. V., Macgregor, J. F., & Marlin, T. E. (1991). Multivariate statistical monitoring of process operating performance. *Canadian Journal of Chemical Engineering*, *69*, 35–47.

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

Massoumnia, M., Verghese, G. C., & Wilsky, A. S. (1989). Failure detection and identification. *IEEE Transactions on Automatic Control*, *34*, 316–321.

Mehranbod, N., Soroush, M., & Panjapornpon, C. (2005). A method of sensor fault detection and identification. *Journal of Process Control*, *15*, 321–339.

Mhaskar, P., El-Farra, N. H., & Christofides, P. D. (2004). Hybrid predictive control of process systems. *AIChE Journal*, *50*, 1242–1259.

Mhaskar, P., Gani, A., & Christofides, P. D. (2006). Fault-tolerant control of nonlinear processes: Performance-based reconfiguration and robustness. *International Journal of Robotics & Nonlinear Control*, *16*, 91–111.

Mhaskar, P., Gani, A., El-Farra, N. H., McFall, C., Christofides, P. D., & Davis, J. F. (2006). Integrated fault-detection and fault-tolerant control for process systems. *AIChE Journal*, *52*, 2129–2148.

Negiz, A., & Cinar, A. (1997). Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE Journal*, *43*, 2002–2020.

Nomikos, P., & Macgregor, J. F. (1994). Monitoring batch processes using multiway principal component analysis. *AIChE Journal*, *40*, 1361–1375.

Patton, R. J. (1997). Fault-tolerant control systems: The 1997 situation. In *Proceedings of the IFAC symposium SAFEPROCESS 1997* (pp. 1033–1054). Hull, UK.

Pisu, P., Serrani, A., You, S., & Jalics, L. (2006). Adaptive threshold based diagnostics for steer-by-wire systems. *Journal of Dynamic Systems Measurement Control—Transactions of the ASME.*

Rollins, D. R., & Davis, J. F. (1992). An unbiased estimation technique when gross errors exist in process measurements. *AIChE Journal*, *38*, 563–572.

Saberi, A., Stoorvogel, A. A., Sannuti, P., & Niemann, H. (2000). Fundamental problems in fault detection and identification. *International Journal of Robotics & Nonlinear Control*, *10*, 1209–1236.

Soroush, M., Valluri, S., & Mehranbod, N. (2005). Nonlinear control of input-constrained systems. *Computers & Chemical Engineering*, *30*, 158–181.

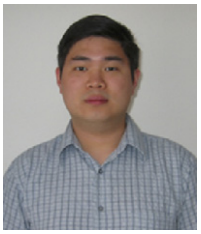
Wu, N. E. (2004). Coverage in fault-tolerant control. *Automatica*, *40*, 537–548.

Yang, G. H., Wang, J. L., & Soh, Y. C. (2001). Reliable $H_\infty$ control design for linear systems. *Automatica*, *37*, 717–725.

Zhou, D. H., & Frank, P. M. (1998). Fault diagnostics and fault tolerant control. *IEEE Transactions on Aerospace and Electronic Systems*, *34*, 420–427.

**Prashant Mhaskar** was born in Varanasi, India, in 1977. He received a B.Tech degree from the Indian Institute of Technology, Bombay, in May 1999, a master's degree from the Louisiana State University in May 2001, and a Ph.D., all in Chemical Engineering, from the University of California, Los Angeles, in 2005. Since September 2005, he has been an Assistant Professor with the Department of Chemical Engineering at the McMaster University. His research interests include nonlinear model predictive control and fault-tolerant control.

**Charles McFall** was born in Wyoming in 1980 and was raised in Olympia, Washington. After completing his B.S. degree in Chemical Engineering at Washington State in 2004, he began his studies at the University of California, Los Angeles. He earned a M.S. degree from UCLA in 2006 and, as a Ph.D. candidate, he conducts research in non-linear control and implementation on reverse osmosis desalination systems. He is an avid cyclist and commutes daily by bicycle.



**Adiwinata Gani** was born in Jakarta, Indonesia, in 1979. He received his B.S. degree, M.S. degree and Ph.D. in Chemical Engineering from the University of California, Los Angeles, in December 2002, December 2003, and April 2007, respectively. He is currently a Scientist in the Department of Bioinformatics High Performance Computing Software Applications Institute at the Henry M. Jackson Foundation for the Advancement of Military Medicine in Fort Detrick, Maryland. His research interests include fault-detection and fault-tolerant control systems.

**Panagiotis D. Christofides** was born in Athens, Greece, in 1970. He received a Diploma in Chemical Engineering in 1992 from the University of Patras, Greece, a M.S. degree in Electrical Engineering and Mathematics in 1995 and 1996, respectively, and a Ph.D. in Chemical Engineering in 1996, all from the University of Minnesota. Since July 1996 he has been with the University of California, Los Angeles, where he is currently a Professor in the Department of Chemical and Biomolecular Engineering and the Department of Electrical Engineering. A description of his research interests and a list of his publications can be found at http://www.chemeng.ucla.edu/pchristo/index.html.

**Jim Davis** is the Associate Vice Chancellor, Information Technology & CIO and a Professor in the Department of Chemical and Biomolecular Engineering at UCLA. In the Department of Chemical and Biomolecular Engineering at UCLA, Jim's research is in the area of data analysis, decision support, and intelligent systems. Jim began his academic career following several years of industrial experience at Amoco Chemicals Corporation. Prior to joining UCLA, Jim was in the Department of Chemical Engineering at Ohio State University. He earned his M.S. and Ph.D. in Chemical Engineering from Northwestern University.