# Active Fault Isolation of Nonlinear Process Systems

**Miao Du and Prashant Mhaskar**
Dept. of Chemical Engineering, McMaster University, Hamilton, ON L8S 4L7, Canada

*DOI 10.1002/aic.14000*
*Published online February 25, 2013 in Wiley Online Library (wileyonlinelibrary.com)*

*This work considers the problem of designing an active fault-isolation scheme for nonlinear process systems subject to uncertainty. The faults under consideration include bounded actuator faults and process disturbances. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory feedback control. To this end, a dedicated fault-isolation residual and its time-varying threshold are generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults in the operating region under nominal operation. To make these residuals sensitive to faults, a switching rule is designed to drive the process states, upon detection of a fault, to move toward an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea is then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults for the case where the residuals are not simultaneously sensitive to faults at a single operating point. The effectiveness of the proposed active fault-isolation scheme is illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of methyl methacrylate and vinyl acetate*. © 2013 American Institute of Chemical Engineers *AIChE J*, 59: 2435–2453, 2013
*Keywords: fault diagnosis, process control, active fault isolation*

## Introduction

The last few decades have witnessed significant improvements in efficiency and profitability of chemical process operations due to the advances in automatic control techniques. The increased level of automation, however, also makes process control systems susceptible to control equipment or process abnormalities, such as actuator faults, sensor faults, and process disturbances. A fault is an unpermitted deviation of an input, output, or parameter of a process system from their usual conditions. Faults are ubiquitously present in chemical plants and take place due to reasons such as mechanical failures, long-term use, power failures, operator mistakes, and so on. The effects of faults range from process performance degradation, such as off-spec production, to catastrophic consequences, such as shutdown of the entire plant (which can lead to substantial economic losses), safety hazards to facilities and personnel, and damages to the environment. Timely and accurate detection of a fault and identification of the faulty equipment is a prerequisite for operators or fault-tolerant control (FTC) systems to turn the process back to normal conditions by taking corrective actions before it runs into a dangerous status that could lead to shutdown of the entire plant. This realization has motivated significant research efforts to develop automated techniques for fault detection and isolation (FDI) of chemical process systems.

One approach to FDI uses the information contained in process data to detect and isolate faults through multivariate statistical process monitoring (see, e.g., Refs. 1–6 for a review). From normal plant operating data, empirical correlation models can be built by using multivariate latent variable methods (see, e.g., Ref. 7), such as principal component analysis (PCA) and partial least squares, which have been successfully applied in process industries. These models are low dimensional and can capture the key information in normal process data. The current process data are compared with the normal variation contained in these low-dimensional models, and abnormal behavior is detected through statistical tests. Faults can then be isolated by using contribution plots,[8] which are able to isolate simple faults (i.e., those that only affect a particular variable). The isolation of complex faults (i.e., those that affect other variables) is improved by using additional data on past faults.[9] The major benefits of this approach are that it can handle the case where there are a large number of measured variables and first principles models are unavailable. The fault-isolation design, however, strongly relies on the availability of data on past faults (which in essence, provide a data-driven model for faulty operation), which may not always be available for fault diagnosis.

Another approach that uses the information embodied in a process (identification or deterministic) model has also been paid significant attention (see, e.g., Refs. 10–18 for reviews). In this approach, residuals are generated as fault indicators by using the analytical redundancy extracted from a process model and input/output data. Faults are detected and isolated by monitoring whether or not the residuals breach their thresholds and using certain isolation logics. This approach

Correspondence concerning this article should be addressed to P. Mhaskar at mhaskar@mcmaster.ca.

has been studied extensively for linear (see, e.g., Refs. 19 and [20]) and nonlinear (see, e.g., Refs. 21–24) systems. Due to the presence of plant-model mismatch, residuals that are sensitive to faults but insensitive to uncertainty and disturbances are desired. Unknown input observers are developed to decouple the effect of unknown inputs, such as disturbances, from that of the faults for linear systems.[19] Most chemical processes, however, exhibit nonlinear dynamics, which should be taken into account in FDI designs. In this direction, the problem has been studied by exploiting the system structure to generate dedicated residuals.[22] It has also been studied using adaptive estimation techniques to handle unstructured modeling uncertainty for a class of Lipschitz nonlinear systems.[23] Other approaches to FDI include those that use artificial neural networks[25] and Bayesian belief networks.[26,27] Most existing FDI methods, however, are passive in the sense that they use plant operating data from the closed-loop system under the controller designed only for the purpose of stabilizing the process at the nominal operating point. Therefore, these passive approaches may not remain effective, if the structure of the closed-loop system inherently does not allow isolation of certain faults under the nominal controller.

In comparison, there exist limited results on utilizing the control action to facilitate fault isolation, which we refer to as active fault isolation. Along this line, a feedback control law has recently been utilized to enforce a closed-loop system structure by decoupling the dependency between certain state variables, which enhances the isolation of faults through data-based methods, under the assumption of full state measurements.[28] More recently, this approach has been extended to handle the case where only output measurements are available and studied with the use of model predictive control to optimize the input cost.[29] These results, however, do not address problem of distinguishing between multiple faults that affect the evolution of the same process states. This problem is partly addressed for actuator faults by estimating the outputs of the actuators and comparing them with the corresponding prescribed values,[30] where it is assumed that the outputs of the (healthy or failed) actuators are constant between two consecutive discrete times, and there exists a subsystem of the plant that satisfies a full rank condition. In summary, although there are a plethora of results that rely on the ability to achieve FDI at nominal operation, the area of FTC stands to benefit from an active fault-isolation framework that takes process nonlinearity and uncertainty into account, and more importantly enables FDI that might not otherwise be possible under nominal operation.

Motivated by the above considerations, this work considers the problem of designing an active fault-isolation scheme for nonlinear systems subject to uncertainty. The rest of the manuscript is organized as follows. The process description and a fault detection design are first presented. The faults under consideration include bounded actuator faults and process disturbances that affect the evolution of the same process states. Following a motivating example of a solution copolymerization reactor, the proposed active fault-isolation design is presented. The key idea of this approach is to exploit the nonlinear way that faults affect the process evolution through supervisory feedback control. To this end, a dedicated fault-isolation residual and its time-varying threshold are generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. There residuals, however, may not be sensitive to faults in the operating region under nominal operation. To make these residuals sensitive to faults, a switching rule is designed to drive the process states, upon detection of a fault, to move toward an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea is then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults for the case where the residuals are not simultaneously sensitive to faults at a single operating point. The effectiveness of the proposed active fault-isolation scheme is illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of methyl methacrylate (MMA) and vinyl acetate (VAc). Finally, we conclude with a summary of results.

## Preliminaries

### Process description

Consider a nonlinear process system described by

$$\dot{x}=f(x)+G(x)u+w(x,t)+D(x)\theta(t) \tag{1}$$

where $x=[x_1,\ldots,x_n]^{\mathrm{T}}\in\mathbb{R}^n$ denotes the vector of state variables, $u\in\mathbb{R}^m$ denotes the vector of input variables, the vector and matrix functions $f=[f_1,\ldots,f_n]^{\mathrm{T}}:\mathbb{R}^n\to\mathbb{R}^n$, and $G=\left[g_1^{\mathrm{T}},\ldots,g_n^{\mathrm{T}}\right]^{\mathrm{T}}:\mathbb{R}^n\to\mathbb{R}^n\times\mathbb{R}^m$ are smooth, the vector function $w=[w_1,\ldots,w_n]^{\mathrm{T}}:\mathbb{R}^n\times[0,\infty)\to\mathbb{R}^n$ denotes process uncertainty, $D(\cdot)=\left[d_1^{\mathrm{T}}(\cdot),\ldots,d_n^{\mathrm{T}}(\cdot)\right]^{\mathrm{T}}$ denotes a fault distribution matrix function, with $d_i=\left[d_{i1}(\cdot),\ldots,d_{iq}(\cdot)\right]$, and $d_{ij}:\mathbb{R}^n\to\mathbb{R}$ being a continuous function for $j=1,\ldots,q$, and $\theta=\left[\theta_1,\ldots,\theta_q\right]^{\mathrm{T}}\in\mathbb{R}^q$ denotes the vector of faults, with $q\leq n$, which include actuator faults and process disturbances that are treated as faults. The origin is an equilibrium point of the nominal system (i.e., the system of Eq. 1 with $w(x,t)\equiv 0$ and $\theta\equiv 0$). To be able to differentiate between nominal uncertainty and faults, it is required that the system of Eq. 1 satisfies Assumption 1.

**Assumption 1.** For the system of Eq. 1, there exist known functions $w_{i,l}:\mathbb{R}^n\to\mathbb{R}^-$ and $w_{i,u}:\mathbb{R}^n\to\mathbb{R}^+$, $i\in\{1,\ldots,n\}$, such that

$$w_{i,l}(x)\leq w_i(x,t)\leq w_{i,u}(x) \tag{2}$$

for any $t\in[0,\infty)$.

Assumption 1 establishes bounding functions on uncertainty, which will be used in the robust fault detection design presented next.

### Fault detection design

The fault-isolation framework presented in this work requires a "trigger" resulting from fault detection. To this end, any of the existing fault detection methods can be utilized. A representative one is presented and formalized in Theorem 1. The key idea is to estimate the bounds on the current values of the process states and determine whether or not the current state measurements are in between these bounds. These bounds are estimated using state measurements over a moving estimation horizon, which is defined as follows

$$T=\begin{cases} t, & 0\leq t<T' \\ T', & t\geq T' \end{cases} \tag{3}$$

where $T'>0$ denotes the length of the horizon after the initialization period (i.e., after time $T'$).

**Theorem 1.** Consider the system of Eq. 1, for which Assumption 1 holds. Then, there exist vector functions $x_l(t)=\left[x_{1,l}(t),\ldots,x_{n,l}(t)\right]^{\mathrm{T}}$ and $x_u(t)=\left[x_{1,u}(t),\ldots,x_{n,u}(t)\right]^{\mathrm{T}}$ such that if $x_i(t)\notin\left[x_{i,l}(t),x_{i,u}(t)\right]$ for some $i\in\{1,\ldots,n\}$, then $\theta(\tau)\neq 0$ for some $\tau\in[t-T,t]$. Furthermore, if $d_i(x(\tau))\theta(\tau)<w_{i,l}(x(\tau))-w_i(x(\tau),\tau)$ for all $\tau\in[t-T,t]$, then $x_i(t)<x_{i,l}(t)$. Similarly, if $d_i(x(\tau))\theta(\tau)>w_{i,u}(x(\tau))-w_i(x(\tau),\tau)$ for all $\tau\in[t-T,t]$, then $x_i(t)>x_{i,u}(t)$.

**Proof.** The proof is divided into two parts. In the first part, we show the existence of vector functions $x_l$ $(t)$ and $x_u$ $(t)$ such that if $x_i(t)\notin\left[x_{i,l}(t),x_{i,u}(t)\right]$ for some $i\in\{1,\ldots,n\}$, then $\theta(\tau)\neq 0$ for some $\tau\in[t-T,t]$. In the second part, we show that if $d_i(x(\tau))\theta(\tau)<w_{i,l}(x(\tau))-w_i(x(\tau),\tau)$ for all $\tau\in[t-T,t]$, then $x_i(t)<x_{i,l}(t)$. By following a similar line of arguments, it then can be shown that if $d_i(x(\tau))\theta(\tau)>w_{i,u}(x(\tau))-w_i(x(\tau),\tau)$ for all $\tau\in[t-T,t]$, then $x_i(t)>x_{i,u}(t)$.
Part 1: Consider the time interval [*t*−*T*,*t*], with *t* being the current time. Integrating the system of Eq. 1 over [*t*−*T*,*t*] yields

$$x(t)-x(t-T)=\tilde{f}(t)+\tilde{w}(t)+\int_{t-T}^{t}D(x(\tau))\theta(\tau)d\tau \qquad (4)$$

where $\tilde{f}(t)=\int_{t-T}^{t}[f(x(\tau))+G(x(\tau))u(\tau)]d\tau$ and $\tilde{w}(t)=[\tilde{w}_1(t),\ldots,\tilde{w}_n(t)]^{\mathrm{T}}=\int_{t-T}^{t}w(x(\tau),\tau)d\tau$. Let

$$x_l(t)=x(t-T)+\tilde{f}(t)+\tilde{w}_l(t) \qquad (5)$$

and

$$x_u(t)=x(t-T)+\tilde{f}(t)+\tilde{w}_u(t) \qquad (6)$$

where $\tilde{w}_l(t)=\left[\tilde{w}_{1,l}(t),\ldots,\tilde{w}_{n,l}(t)\right]^{\mathrm{T}}=\int_{t-T}^{t}w_l(x(\tau))d\tau$ and $\tilde{w}_u(t)=\left[\tilde{w}_{1,u}(t),\ldots,\tilde{w}_{n,u}(t)\right]^{\mathrm{T}}=\int_{t-T}^{t}w_u(x(\tau))d\tau$. As $w_{i,l}(x(\tau))\leq w_i(x(\tau),\tau)\leq w_{i,u}(x(\tau))$ for any $\tau\in[t-T,t]$, $i=1,\ldots,n$, it follows that $\tilde{w}_{i,l}\leq\tilde{w}_i(t)\leq\tilde{w}_{i,u}(t)$. It then follows from Eqs. 4–6 that if $\theta(\tau)=0$ for any $\tau\in[t-T,t]$, then the following equation holds for $i\in\{1,\ldots,n\}$

$$x_{i,l}(t)\leq x_i(t)\leq x_{i,u}(t) \qquad (7)$$

Therefore, $x_i(t)\notin\left[x_{i,l}(t),x_{i,u}(t)\right]$ for some $i\in\{1,\ldots,n\}$ implies that $\theta(\tau)\neq 0$ for some $\tau\in[t-T,t]$.
Part 2: As $d_i(x(\tau))\theta(\tau)<w_{i,l}(x(\tau))-w_i(x(\tau),\tau)$ for all $\tau\in[t-T,t]$, we have

$$\begin{aligned}\int_{t-T}^{t}d_i(x(\tau))\theta(\tau)d\tau&<\int_{t-T}^{t}\left[w_{i,l}(x(\tau))-w_i(x(\tau),\tau)\right]d\tau\\&=\tilde{w}_{i,l}(t)-\tilde{w}_i(t)\end{aligned} \qquad (8)$$

It follows from Eqs. 4, 5, and 8 that

$$x_i(t)-x_{i,l}(t)=\tilde{w}_i(t)-\tilde{w}_{i,l}(t)+\int_{t-T}^{t}d_i(x(\tau))\theta(\tau)d\tau<0 \qquad (9)$$

which implies that

$$x_i(t)<x_{i,l}(t) \qquad (10)$$

**Remark 1.** The fault detection design of Theorem 1 explicitly accounts for process uncertainty. To this end, the lower and upper bounds, denoted by $x_l$ $(t)$ and $x_u$ $(t)$, on the process states at the current time *t* are evaluated by using the process model and measurements (which are used in the integrals of the proof of Theorem 1) over an estimation horizon of length *T* subject to the possible realization of uncertainty. If no faults take place, the process states should comply with these bounds (i.e., $x(t)\in[x_l(t),x_u(t)]$). Because the computation of these bounds considers the worst effect of uncertainty, the only way that any state breaches its bounds is that a fault takes place. Consequently, the fault detection design is robust in the sense that there will be no false alarms before a fault takes place (albeit at the cost of "small faults" that are indistinguishable from the effect of uncertainty). In addition, the fault detection design of Theorem 1 can be used to group faults that possibly take place. Specifically, the fault that takes place is among the group of the ones for which the elements in the corresponding row of the fault distribution matrix function are nonzero. As a special case, if that group contains only one fault, then the fault is also isolated.

**Remark 2.** In addition to the fault detection mechanism, Theorem 1 also gives explicit conditions on the class of faults that are detectable. These conditions can be interpreted from two perspectives. First, the faults should make $d_i(x(\tau))\theta(\tau)$ remain negative or positive over the time interval [*t*−*T*,*t*]. Second, the magnitude of $d_i(x(\tau))\theta(\tau)$ should be large enough over the same period (i.e., larger than that of the difference between $w_i(x(\tau),\tau)$ and $w_{i,l}(x(\tau))$ or $w_{i,u}(x(\tau))$). Although the satisfaction of these conditions guarantees that faults can be detected, the fault detection design is not limited to this particular class of faults. In fact, the integral form of these conditions exactly characterizes the class of faults that are detectable (e.g., $\int_{t-T}^{t}d_i(x(\tau))\theta(\tau)d\tau<\tilde{w}_{i,l}(t)-\tilde{w}_i(t)$ is used instead of $d_i(x(\tau))\theta(\tau)<w_{i,l}(x)-w_i(x,\tau)$ for all $\tau\in[t-T,t]$). It essentially considers possible changes in the sign of $d_i(x(\tau))\theta(\tau)$ and reflects the accumulating effect of faults. Note that faults that do not satisfy the conditions in the integral form may have similar effects as process uncertainty (reflecting the inherent tradeoff between robustness and fault sensitivity). If the process operates under an appropriately designed robust control law, they would not lead to instability of the closed-loop system.

## Motivating Example: A Solution Copolymerization Reactor

In this section, we consider a solution copolymerization of MMA and VAc, where monomers A (MMA) and B (VAc) are continuously fed to a continuous-stirred tank reactor (CSTR) with initiator (azobisisobutyronitrile), solvent (benzene), and chain-transfer agent (acetaldehyde). A cooling jacket is equipped to remove the heat of the copolymerization reaction. The mathematical model for this reactor (in the absence of recycle streams and inhibitors) is of the following form[31]

$$\begin{aligned}\dot{C}_j&=\left(\frac{Q_j}{M_j}-\frac{C_j\sum_k Q_k}{\rho}\right)\frac{1}{V}-R_j,\quad j=a,b,i,s,t\\ \dot{T}_{\mathrm{R}}&=(T_0-T_{\mathrm{R}})\frac{\sum_k Q_k}{\rho V}+\left[(-\Delta H_{paa})k_{paa}C_aC_{a\cdot}\right.\\&\quad+(-\Delta H_{pba})k_{pba}C_aC_{b\cdot}(-\Delta H_{pab})k_{pab}C_bC_{a\cdot}\\&\quad\left.+(-\Delta H_{pbb})k_{pbb}C_bC_{b\cdot}\right]\frac{1}{\rho c_{\mathrm{p}}}-\frac{UA(T_{\mathrm{R}}-T_{\mathrm{c}})}{\rho c_{\mathrm{p}}V}\end{aligned} \qquad (11)$$

where $C_j$ is the concentration of species $j$, with subscript $a$, $b$, $i$, $s$, and $t$ denoting monomer A, monomer B, initiator, solvent, and chain-transfer agent, respectively, $T_{\mathrm{R}}$ is the temperature in the reactor, $Q_k$ is the mass flow rate of species $k$, $k{=}a$, $b$, $i$, $s$, $t$, $T_{\mathrm{c}}$ is the temperature in the cooling jacket, $M_j$ is the molar mass of species $j$, $V$ is the volume of the reactor, $\Delta H$ is the enthalpy of the reaction, $\rho$ and $c_{\mathrm{p}}$ are the density and the heat capacity of the fluid in the reactor, respectively, $U$ is the overall heat-transfer coefficient, $A$ is the heat-transfer area of the reactor, $T_{\mathrm{c}}$ is the temperature in the cooling jacket, and

$$\begin{gathered}
R_a=\left[\left(k_{paa}+k_{xaa}\right)C_{a\cdot}+\left(k_{pba}+k_{xba}\right)C_{b\cdot}\right]C_a \qquad (12)\\
R_b=\left[\left(k_{pbb}+k_{xbb}\right)C_{b\cdot}+\left(k_{pab}+k_{xab}\right)C_{a\cdot}\right]C_b\\
R_i=k_iC_i\\
R_s=(k_{xas}C_{a\cdot}+k_{xbs}C_{b\cdot})C_s\\
R_t=(k_{xat}C_{a\cdot}+k_{xbt}C_{b\cdot})C_t\\
C_{a\cdot}=\frac{-l_2+\sqrt{l_2^2-4l_1l_3}}{2l_1}\\
C_{b\cdot}=\beta C_{a\cdot}\\
l_1=k_{caa}+k_{daa}+2\beta(k_{cab}+k_{dab})+\beta^2(k_{cbb}+k_{dbb})\\
l_2=0\\
l_3=-2k_iC_i\varepsilon\\
\beta=\frac{\left(k_{pab}+k_{xab}\right)C_b}{\left(k_{pba}+k_{xba}\right)C_a}
\end{gathered}$$

Each of the rate constants is computed through the Arrhenius equation

$$k=Ae^{-E/RT_{\mathrm{R}}} \qquad (13)$$

where $A$ is the pre-exponential constant, $E$ is the activation energy, and $R$ is the ideal gas constant. The process parameters can be found in Table 1 (see also Ref. 31).

The control objective under fault-free conditions is to operate the process at the nominal operating point, where $C_a{=}2.534 \times 10^{-1}$ kmol/m$^3$, $C_b{=}5.838$ kmol/m$^3$, $C_i{=}2.008 \times 10^{-3}$ kmol/m$^3$, $C_s{=}2.758$ kmol/m$^3$, $C_t{=}3.663 \times 10^{-1}$ kmol/m$^3$, and $T_{\mathrm{R}}{=}350.5$ K. It is assumed that all the state measurements are available, and the flow rates $Q_k$, $k{=}a$, $b$, $i$, $s$, $t$, and the temperature in the cooling jacket $T_{\mathrm{c}}$ are chosen as manipulated input variables. The inputs are bounded as $0{\leq}Q_a{\leq}50$ kg/h, $0{\leq}Q_b{\leq}120$ kg/h, $0{\leq}Q_i{\leq}0.5$ kg/h, $0{\leq}Q_s{\leq}100$ kg/h, $0{\leq}Q_t{\leq}10$ kg/h, and $320{\leq}T_{\mathrm{c}}{\leq}350$ K. The steady-state values of the inputs corresponding to the nominal operating point are $Q_a{=}18$ kg/h, $Q_b{=}90$ kg/h, $Q_i{=}0.18$ kg/h, $Q_s{=}36$ kg/h, $Q_t{=}2.7$ kg/h, and $T_j{=}336.15$ K. The offset-free model predictive control of Ref. 32 is used as the control law for this process. In the control design, the nonlinear model is linearized around a desired operating point, which gives a linear model in the following form: $x_{k+1}{=}Ax_k{+}Bu_k$, $y_k{=}Cx_k$, where $A,B \in \mathbb{R}^{6\times6}$, $C{=}I$, and the subscripts $k$ denote discrete times. Furthermore, a disturbance model is used to correct the model prediction, which is in the following form: $\tilde{x}_{k+1}{=}\tilde{A}\tilde{x}_k{+}\tilde{B}u_k$, $y_k{=}\tilde{C}\tilde{x}_k$, where $\tilde{x}{=}\begin{bmatrix} x \\ d \end{bmatrix} \in \mathbb{R}^{12}$ is the vector of states and disturbances, $\tilde{A}{=}\begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$, $\tilde{B}{=}\begin{bmatrix} B \\ 0 \end{bmatrix}$, and $\tilde{C}{=}[C \quad 0]$. The augmented state vector $\tilde{x}$ is estimated using a Luenberger observer. The hold-time for the control action is chosen as $\Delta{=}3$ min, control horizon $T_{\mathrm{c}}{=}2\Delta$, and the prediction horizon $T_{\mathrm{p}}{=}10\Delta$. In the objective function for model predictive control, the states are normalized against ranges [0, 1], [0, 8], [0, 5 $\times$ $10^{-3}$], [0, 10], [0, 1], and [340, 355], respectively, and the inputs are done against the constraints. The matrices used to penalize the deviations of the normalized states from the steady-state values and the increments of the inputs are diag[1, 1, 1, 1, 1, 1] and diag[1, 1, 50, 0.5, 1, 1], respectively.

**Table 1. Process Parameters for the Solution Copolymerization Example**

| Parameter | Value | Unit |
|---|---|---|
| $V$ | 1 | m$^3$ |
| $R$ | 8.314 | kJ/(kmol K) |
| $\rho$ | $8.79{\times}10^2$ | kg/m$^3$ |
| $c_{\mathrm{p}}$ | 2.01 | kJ/(kg K) |
| $U$ | $6.0{\times}10^{-2}$ | kJ/(m$^2$ s K) |
| $A$ | 4.6 | m$^2$ |
| $T_0$ | 353.15 | K |
| $\varepsilon$ | 1 | |
| $M_a$ | 100.12 | kg/kmol |
| $M_b$ | 86.09 | kg/kmol |
| $M_i$ | 164.21 | kg/kmol |
| $M_s$ | 78.11 | kg/kmol |
| $M_t$ | 44.05 | kg/kmol |
| $A_i$ | $4.5{\times}10^{14}$ | s$^{-1}$ |
| $A_{caa}$ | $4.209{\times}10^{11}$ | m$^3$/(kmol s) |
| $A_{cbb}$ | $1.61{\times}10^9$ | m$^3$/(kmol s) |
| $A_{daa}$ | 0 | m$^3$/(kmol s) |
| $A_{dbb}$ | 0 | m$^3$/(kmol s) |
| $A_{paa}$ | $3.207{\times}10^6$ | m$^3$/(kmol s) |
| $A_{pab}$ | $1.233{\times}10^5$ | m$^3$/(kmol s) |
| $A_{pba}$ | $2.103{\times}10^8$ | m$^3$/(kmol s) |
| $A_{pbb}$ | $6.308{\times}10^6$ | m$^3$/(kmol s) |
| $A_{xaa}$ | 32.08 | m$^3$/(kmol s) |
| $A_{xab}$ | 1.234 | m$^3$/(kmol s) |
| $A_{xas}$ | 86.6 | m$^3$/(kmol s) |
| $A_{xat}$ | 2085.0 | m$^3$/(kmol s) |
| $A_{xba}$ | $5.257{\times}10^4$ | m$^3$/(kmol s) |
| $A_{xbb}$ | 1577 | m$^3$/(kmol s) |
| $A_{xbs}$ | 1514 | m$^3$/(kmol s) |
| $A_{xbt}$ | $4.163{\times}10^5$ | m$^3$/(kmol s) |
| $E_i$ | $1.25{\times}10^5$ | kJ/kmol |
| $E_{caa}$ | $2.69{\times}10^4$ | kJ/kmol |
| $E_{cbb}$ | $4.00{\times}10^3$ | kJ/kmol |
| $E_{daa}$ | 0.0 | kJ/kmol |
| $E_{dbb}$ | 0.0 | kJ/kmol |
| $E_{paa}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{pab}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{pba}$ | $1.80{\times}10^4$ | kJ/kmol |
| $E_{pbb}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{xaa}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{xab}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{xas}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{xat}$ | $2.42{\times}10^4$ | kJ/kmol |
| $E_{xba}$ | $1.80{\times}10^4$ | kJ/kmol |
| $E_{xbb}$ | $1.80{\times}10^4$ | kJ/kmol |
| $E_{xbs}$ | $1.80{\times}10^4$ | kJ/kmol |
| $E_{xbt}$ | $2.42{\times}10^4$ | kJ/kmol |
| $-\Delta H_{paa}$ | $54.0{\times}10^3$ | kJ/kmol |
| $-\Delta H_{pba}$ | $54.0{\times}10^3$ | kJ/kmol |
| $-\Delta H_{pab}$ | $86.0{\times}10^3$ | kJ/kmol |
| $-\Delta H_{pbb}$ | $86.0{\times}10^3$ | kJ/kmol |

Practical issues, such as parametric uncertainty, time-varying disturbances, and measurement noise, are considered in the simulations. Specifically, the values of $A_{pab}$, $A_{pba}$, $A_{paa}$, $A_{pbb}$, $A_{xas}$, $A_{xbs}$, $A_{xat}$, and $A_{xbt}$ are 10% smaller than their nominal values, and those of $A_{xab}$, $A_{xba}$, $A_{xaa}$, and $A_{xbb}$ are 10% larger. The bounds on these uncertainties are $\pm$15% of their nominal values. It is assumed that the inlet streams of monomer B and solvent are impure. There exist a small amount of solvent and monomer B in the flows of monomer B and solvent, respectively. The mass fraction of monomer B in the flow of solvent is described by $0.02+0.02\ \sin(t)$, and the mass fraction of solvent in the flow of monomer B is $0.01+0.01\ \sin(2t)$. The upper bounds on the magnitudes of disturbances in the streams of monomer B and solvent are 3 and 5%, respectively. The measurement noise has a normal distribution of variance 0.02, 0.2, 0.0005, 0.2, 0.02, and 0.5 in $C_a$, $C_b$, $C_i$, $C_s$, $C_t$, and $T_{\mathrm{R}}$, respectively. It is assumed that measurements are sampled 20 times evenly between two successive times when control action is implemented. The noisy measurements are preprocessed through a moving average filter, which takes the mean of the previous 20 samples, before being used for control and FDI.

Consider actuator faults in the process of Eq. 11, which are denoted by $\theta_j$, $j=1,\dots,6$, for faults in $Q_a$, $Q_b$, $Q_i$, $Q_s$, $Q_t$, and $T_{\mathrm{c}}$, respectively. The faults are assumed to be bounded as $|\theta_1| \le 4.5\ \mathrm{kg/h}$, $|\theta_2| \le 25\mathrm{kg/h}$, $|\theta_3| \le 9\ \mathrm{kg/h}$, $|\theta_4| \le 25\ \mathrm{kg/h}$, $|\theta_5| \le 0.675\ \mathrm{kg/h}$, and $|\theta_6| \le 5$ K. The expression of the fault distribution matrix is as follows

$$D=\frac{1}{V}\begin{bmatrix} \frac{1}{M_a}-\frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & 0 \\ -\frac{C_b}{\rho} & \frac{1}{M_b}-\frac{C_b}{\rho} & -\frac{C_b}{\rho} & -\frac{C_b}{\rho} & -\frac{C_b}{\rho} & 0 \\ -\frac{C_i}{\rho} & -\frac{C_i}{\rho} & \frac{1}{M_i}-\frac{C_i}{\rho} & -\frac{C_i}{\rho} & -\frac{C_i}{\rho} & 0 \\ -\frac{C_s}{\rho} & -\frac{C_s}{\rho} & -\frac{C_s}{\rho} & \frac{1}{M_s}-\frac{C_s}{\rho} & -\frac{C_s}{\rho} & 0 \\ -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & \frac{1}{M_t}-\frac{C_t}{\rho} & 0 \\ \frac{T_0-T_{\mathrm{R}}}{\rho} & \frac{T_0-T_{\mathrm{R}}}{\rho} & \frac{T_0-T_{\mathrm{R}}}{\rho} & \frac{T_0-T_{\mathrm{R}}}{\rho} & \frac{T_0-T_{\mathrm{R}}}{\rho} & \frac{UA}{\rho c_{\mathrm{p}}} \end{bmatrix} \tag{14}$$

The above expression shows a typical case where there exist multiple faults that may directly affect the evolution of the same process states. For example, all the faults in the flow rate actuators directly affect the evolution of the concentration of monomer A, as well as all the other state variables. For this case, the system is not of the structure that can be utilized to build dedicated residuals as in Ref. 22. The FDI design in Ref. 28 would at best identify a group of possible faults, which may include all the faults in the worst case. Therefore, the process complexity asks for FDI designs that take into account the nonlinear way (in the sense that the fault distribution matrix is not constant, but a function of the process states) that faults affect the process evolution, as well as nonlinear dynamics and process uncertainty, motivating the fault-isolation approach presented next.

## Active Fault-Isolation Design

In this section, we present an active fault-isolation scheme. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory feedback control. To this end, a special operating point termed fault-isolation point is first defined, the property of which can be used to differentiate between multiple faults. In general, the fault-isolation point is not identical to the nominal operating point. For the purpose of fault isolation, a switching rule is then designed to drive the process states to move toward a fault-isolation point upon detection of a fault. To distinguish a particular fault from other faults, we require information on the magnitudes of faults, which are characterized in Assumption 2.

**Assumption 2.** For the system of Eq. 1, $\theta_{i,l} \le \theta_i \le \theta_{i,u}$, $i=1,\dots,q$, where $\theta_{i,l} \in \mathbb{R}^-$ and $\theta_{i,u} \in \mathbb{R}^+$ denote the lower and upper bounds on $\theta$, respectively.

**Remark 3.** The focus of this work is to design a methodology that is able to isolate complex faults for the case where multiple faults simultaneously appear on the right-hand side of a differential equation for the same state variable. Note that if the faults considered are unbounded, then any fault that takes place may be seen as the occurrence of any one of the other faults that affect the evolution of the same state no matter how small the absolute values of the corresponding weighting coefficient functions (i.e., $d_{ij}(\cdot)$ in the fault distribution matrix function) are. In contrast, this work considers faults such as biases or drifts, which are commonly encountered in practice, and take place due to control actuator malfunctions or process abnormalities, such as leakage of feedstocks. These faults can be modeled as bounded (although possibly time-varying) variables as formalized in Assumption 2.

We next define a fault-isolation point, which will be used to generate appropriate control action through a switching rule for fault isolation.

DEFINITION 1. A point $\tilde{x}$ is a fault-isolation point if there exists $\tilde{u} \in \mathbb{R}^m$ such that $f(\tilde{x})+G(\tilde{x})\tilde{u}=0$, and for any fault $\theta_j$, $j=1,\dots,q$, there exists a state $x_{\mathrm{i}}$, $i \in \{1,\dots,n\}$ such that $d_{ik}(\tilde{x})=0$ for all $k \in \{1,\dots,q\}\backslash\{j\}$ and $d_{ij}\neq 0$ for any $x \in D$, where $D \subseteq \mathbb{R}^n$.

**Remark 4.** Note that a fault-isolation point needs to satisfy three conditions. First, it is an equilibrium point for the nominal system (i.e., the system of Eq. 1 with $w(x,t) \equiv 0$ and $\theta(t) \equiv 0$). This requirement makes it possible to operate at a fault-isolation point, at which the remaining two conditions are defined. Second, for a given fault, at a fault-isolation point, there exists at least one system state for which that fault is the only one that essentially appears on the right-hand side of the corresponding differential equation. This requirement makes it possible to isolate a given fault (even if the third condition is not satisfied; see Remark 9 for a further discussion). Finally, it is also required that the second condition is satisfied for all the faults under consideration. This requirement implies that the number of state variables should not be less than that of the faults and makes it possible to isolate multiple faults.

**Remark 5.** Note that fault-isolation points may not always exist. One example is the case where the fault distribution matrix function is constant (e.g., in the case of a linear system, but not necessarily). In this case, however, the process dynamics are less complex, and existing methods may be used. To illustrate this point, we decompose the system state of Eq. 1 as follows: $x=\left[x_d^{\mathrm{T}},x_{\bar{d}}^{\mathrm{T}}\right]^{\mathrm{T}}$, where $x_d \in \mathbb{R}^q$ and $x_{\bar{d}} \in \mathbb{R}^{n-q}$, and consider the $x_d$ subsystem described by $\dot{x}_d=f_d(x)+G_d(x)u+w_d(x,t)+D_d\theta(t)$, where $D_d$ is constant, and $f_d(\cdot)$, $G_d(\cdot)$, and $w_d(\cdot,\cdot)$ are appropriately defined. Multiplying both sides of the $x_d$ subsystem by $D_d^{-1}$ (if $D_d$ is invertible) and defining a state vector $\hat{x}_d=D_d^{-1}x_d$ yields an equivalent subsystem described by $\dot{\hat{x}}_d=f_d(\hat{x})+G_d(\hat{x})+w_d(\hat{x},t)+\theta(t)$, where $\hat{x}=\left[(D_d\hat{x}_d)^{\mathrm{T}},x_{\bar{d}}^{\mathrm{T}}\right]^{\mathrm{T}}$. The system in the transformed coordinate satisfies the structure requirement specified in Ref. 22, where it is assumed that for each fault, there exists a state variable whose evolution is directly and uniquely affected by that fault. Therefore, this case can be handled by existing methods, and would not necessitate an active fault-isolation scheme. In contrast, this work addresses a more complex scenario, and process nonlinearity is utilized for fault isolation through a fault-isolation point.

A distinguishing feature of the proposed method is that control action is utilized for the purpose of fault isolation. In particular, we propose to move the process to a fault-isolation point upon fault detection, close to which the property of the fault distribution matrix can be utilized to differentiate between complex faults. This naturally implies that in the presence of faults, there should remain sufficient control effort that enables moving the process to a fault-isolation point. Note that the proposed method satisfies a very specific fault-isolation need. In particular, it addresses the kind of faults, which does not pose an immediate threat to the stability or operation of the process. In other words, under the occurrence of faults, nominal operation could still be continued (and, under the proposed method, the remaining control effort allows moving the process in the presence of faults). The motivation for fault isolation in this case is to catch a fault before it possibly turns into a bigger catastrophic failure. Note also that this work does not require a specific control design. Any robust control law that satisfies the property stated in Assumption 3 below can be used to move the process states.

**Assumption 3.** For the system of Eq. 1, there exists a robust control law $RC(x)$ such that given any $x(0) \in D$ and $d{>}0$, there exists a finite positive real number $T_{\mathrm{c}}$ such that $x(t) \in B_d$ for all $t{\geq}T_{\mathrm{c}}$, where $D \subseteq \mathbb{R}^n$ and $B_d$ is closed ball of radius $d$ around $\tilde{x}$.

Assumption 3 establishes the ability to drive the process states to an arbitrarily small neighborhood of a fault-isolation point $\tilde{x}$ for any initial condition within some region $D$ in finite time even under faulty conditions. With this ability available, the active fault-isolation design is formulated in Theorem 2. To this end, let $t_{\mathrm{d}}$ denote the time that a fault is detected, and $u_x$ and $u_{\tilde{x}}$ denote the control inputs to stabilize the system of Eq. 1 at the nominal equilibrium point and a fault-isolation point, respectively.

**Theorem 2.** Consider the system of Eq. 1, for which $\tilde{x}$ is a fault-isolation point and Assumptions 1–3 hold. Then, given a fault $\theta_j$ for any $j \in \{1,\ldots,q\}$, there exist functions $\tilde{x}_{i,l}(t)$ and $\tilde{x}_{i,u}(t)$ such that if $x_i(t) \notin \left[\tilde{x}_{i,l}(t),\tilde{x}_{i,u}(t)\right]$, then $\theta_j(\tau){\neq}0$ for some $\tau \in [t-T,t]$. Furthermore, there exists $d{>}0$ and $T'_{\mathrm{c}} > 0$ such that under the switching rule

$$u(t)=\begin{cases} u_x(t), & 0 \leq t < t_{\mathrm{d}} \\ u_{\tilde{x}}(t), & t \geq t_{\mathrm{d}} \end{cases} \tag{15}$$

if $x(t_d) \in D$, then for $t \geq T'_{\mathrm{c}}$, $x_i(t) \notin \left[x_{i,l}(t),x_{i,u}(t)\right]$ implies $x_i(t) \notin \left[\tilde{x}_{i,l}(t),\tilde{x}_{i,u}(t)\right]$.

**Proof.** The proof is divided into two parts. In the first part, we show that there exist threshold functions $\tilde{x}_l(t)$ and $\tilde{x}_u(t)$ such that if the corresponding state measurement breaches these thresholds, then a fault is isolated. In the second part, we show that under the switching rule of Eq. 15, for a given fault, if it can be differentiated from plant-model mismatch, then it can also be isolated as long as the system state is close enough to the fault-isolation point.

Part 1: Consider the following equation

$$\begin{aligned}\dot{x}_i&=f_i(x)+g_i(x)u+w_i(x,t)+d_i(x)\theta(t)\\&=f_i(x)+g_i(x)u+w_i(x,t)+h_i(x,t)+d_{ij}(x)\theta_j(t)\end{aligned} \tag{16}$$

where $h_i(x,t)=\sum_{k=1,k\neq j}^{q} d_{ik}(x)\theta_k(t)$. Integrating the above equation over $[t-T,t]$ yields

$$x_i(t)-x_i(t-T)=\tilde{f}_i(t)+\tilde{w}_i(t)+\tilde{h}_i(t)+\int_{t-T}^{t} d_{ij}(x(\tau))\theta_j(\tau)d\tau \tag{17}$$

where

$\tilde{f}_i(t)=\int_{t-T}^{t}[f_i(x(\tau))+g_i(x(\tau))u(\tau)]d\tau$ and $\tilde{h}_i(t)=\int_{t-T}^{t}\sum_{k=1,k\neq j}^{q} d_{ik}$ $(x(\tau))\theta_k(\tau)d\tau$. The lower and upper bounds on $\tilde{h}_i(t)$ are estimated as follows

$$\tilde{h}_{i,l}(t)=\int_{t-T}^{t}\sum_{k=1,k\neq j}^{q} d_{ik}(x(\tau))\hat{\theta}_{k,l}(\tau)d\tau \tag{18}$$

and

$$\tilde{h}_{i,u}(t)=\int_{t-T}^{t}\sum_{k=1,k\neq j}^{q} d_{ik}(x(\tau))\hat{\theta}_{k,u}(\tau)d\tau \tag{19}$$

where

$\hat{\theta}_{k,l}=\begin{cases}\theta_{k,u}, & \text{if } d_{ik}(x) \leq 0\\ \theta_{k,l}, & \text{if } d_{ik}(x) > 0\end{cases}$ and $\hat{\theta}_{k,u}=\begin{cases}\theta_{k,l}, & \text{if } d_{ik}(x) \leq 0\\ \theta_{k,u}, & \text{if } d_{ik}(x) > 0\end{cases}$.

Let

$$\tilde{x}_{i,l}(t)=x_i(t-T)+\tilde{f}_i(t)+\tilde{w}_{i,l}(t)+\tilde{h}_{i,l}(t) \tag{20}$$

and

$$\tilde{x}_{i,u}(t)=x_i(t-T)+\tilde{f}_i(t)+\tilde{w}_{i,u}(t)+\tilde{h}_{i,u}(t) \tag{21}$$

As $w_{i,l}(x(\tau)) \leq w_i(x(\tau),\tau) \leq w_{i,u}(x(\tau))$ for any $\tau \in [t-T,t]$ and $\theta_{k,l} \leq \theta_k \leq \theta_{k,u}$, $k=1,\ldots,q$, it follows that if $\theta_j(\tau)=0$ for any $\tau \in [t-T,t]$, then the following equation holds

$$\tilde{x}_{i,l}(t) \leq x_i(t) \leq \tilde{x}_{i,u}(t) \tag{22}$$

Therefore, $x_i(t) \neq \left[\tilde{x}_{i,l}(t),\tilde{x}_{i,u}(t)\right]$ implies that $\theta_j(\tau){\neq}0$ for some $\tau \in [t-T,t]$.

Part 2: Given $x_i(t) \notin \left[x_{i,l}(t),x_{i,u}(t)\right]$, there exists $\tilde{d} > 0$ such that $x_i(t) < x_{i,l}(t)-\tilde{d}$ or $x_i(t) > x_{i,u}(t)+\tilde{d}$. As $\theta$ is bounded, there exists $d'{>}0$ such that if $|d_{i,k}(x)| < d'$ over $[t-T,t]$ for all $k \in \{1,\ldots,q\}\backslash\{j\}$, then $\tilde{h}_{i,l}(t) > -\tilde{d}$ and $\tilde{h}_{i,u}(t) < \tilde{d}$. For any $k \in \{1,\ldots,q\}\backslash\{j\}$, since $d_{ik}$ $(\cdot)$ is continuous and $d_{ik}(\tilde{x})=0$, there exists $d{>}0$ such that $|d_{ik}(x)| < d'$ for any $x \in B_d$. Because $x(t_d) \in D$, it follows from Assumption 3 that under the switching rule of Eq. 15, there exists $T'_{\mathrm{c}} > 0$ such that $x(t) \in B_d$ for all $t \geq T'_{\mathrm{c}}-T$. Then, for $t \geq T'_{\mathrm{c}}$, we have $\tilde{h}_{i,l}(t) > -\tilde{d}$ and $\tilde{h}_{i,u}(t) < \tilde{d}$. It follows that

$$x_i(t) < x_{i,l}(t)-\tilde{d} < x_{i,l}(t)+\tilde{h}_{i,l}(t)=\tilde{x}_{i,l}(t) \tag{23}$$

or

$$x_i(t) > x_{i,u}(t)+\tilde{d} > x_{i,u}(t)+\tilde{h}_{i,u}(t)=\tilde{x}_{i,u}(t) \tag{24}$$

which implies that $x_i(t) \notin \left[\tilde{x}_{i,l}(t),\tilde{x}_{i,u}(t)\right]$.

Without loss of generality, let $\{1,\ldots,q\}$ be an index set of the states that satisfy the relationship between faults and

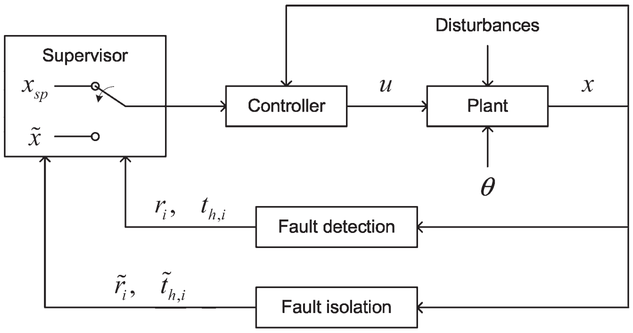


**Figure 1. Schematic of the active fault-isolation scheme.**

**The plant is subject to faults denoted by $\theta$ (actuator faults and process disturbances treated as faults). A fault is detected by checking whether some detection residual $r_i$ breaches its threshold $t_{h,i}$. Upon fault detection, the supervisor shifts the control objective from operating the process at the nominal operating point $x_{sp}$ to driving it to move toward a fault-isolation point $\tilde{x}$. A fault is isolated by checking which isolation residual $\tilde{r}_i$ breaches its threshold $\tilde{t}_{h,i}$.**

states at a fault-isolation point. Note that each state is associated with a unique fault. The implementation of the active fault-isolation scheme of Theorem 2, with the use of the robust fault detection design of Theorem 1, is illustrated in Figure 1 and proceeds as follows:

1. At time $t_k = k\Delta_{\mathrm{FDI}}$, $k=0,\ldots,\infty$, evaluate thresholds

$$t_{h,i}(k) = \frac{x_{i,u}(t_k) - x_{i,l}(t_k)}{2} \tag{25}$$

and residuals

$$r_i(k) = \left| x_i(t_k) - \frac{x_{i,l}(t_k) + x_{i,u}(t_k)}{2} \right| \tag{26}$$

for $i=1,\ldots,n$, according to Eqs. 5 and 6, where $\Delta_{\mathrm{FDI}}$ denotes the evaluation period (i.e., the time between two consecutive evaluations).

2. According to Theorem 1, if $r_i(k) > t_{h,i}(k)$ for some $i \in \{1,\ldots,n\}$, then a fault is detected, and let $t_\mathrm{d} = t_k$ be the time of fault detection if it is the first time that the fault is detected. Note that $x_i(t_k) \notin \left[ x_{i,l}(t_k), x_{i,u}(t_k) \right]$ iff $r_i(k) > t_{h,i}(k)$.

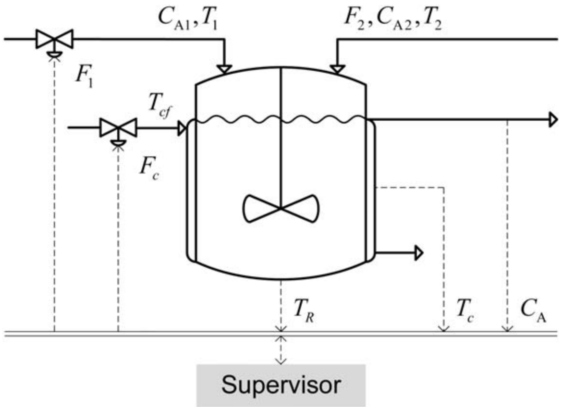


**Figure 2. Schematic of the chemical reactor example.**

**The feed to the reactor is composed of two streams at flow rate $F_1$ and $F_2$, respectively. The cooling stream to the jacket is at a flow rate $F_c$. The process is subject to faults in the actuator for the flow rate $F_1$, the disturbance in the flow rate $F_2$, and the actuator for the flow rate $F_c$.**

3. At time $t_k$, evaluate thresholds

$$\tilde{t}_{h,i}(k) = \frac{\tilde{x}_{i,u}(t_k) - \tilde{x}_{i,l}(t_k)}{2} \tag{27}$$

and residuals

$$\tilde{r}_i(k) = \left| x_i(t_k) - \frac{\tilde{x}_{i,l}(t_k) + \tilde{x}_{i,u}(t_k)}{2} \right| \tag{28}$$

for $i=1,\ldots,q$, according to Eqs. 20 and 21.

4. According to Theorem 2, if $\tilde{r}_i(k) > \tilde{t}_{h,i}(k)$, then a fault $\theta_j$ for some $j \in \{1,\ldots,q\}$ is isolated, and let $t_k$ be the time of fault isolation. Note that $x_i(t_k) \notin \left[ \tilde{x}_{i,l}(t_k), \tilde{x}_{i,u}(t_k) \right]$ iff $\tilde{r}_i(k) > \tilde{t}_{h,i}(k)$. Otherwise, go to Step 5.

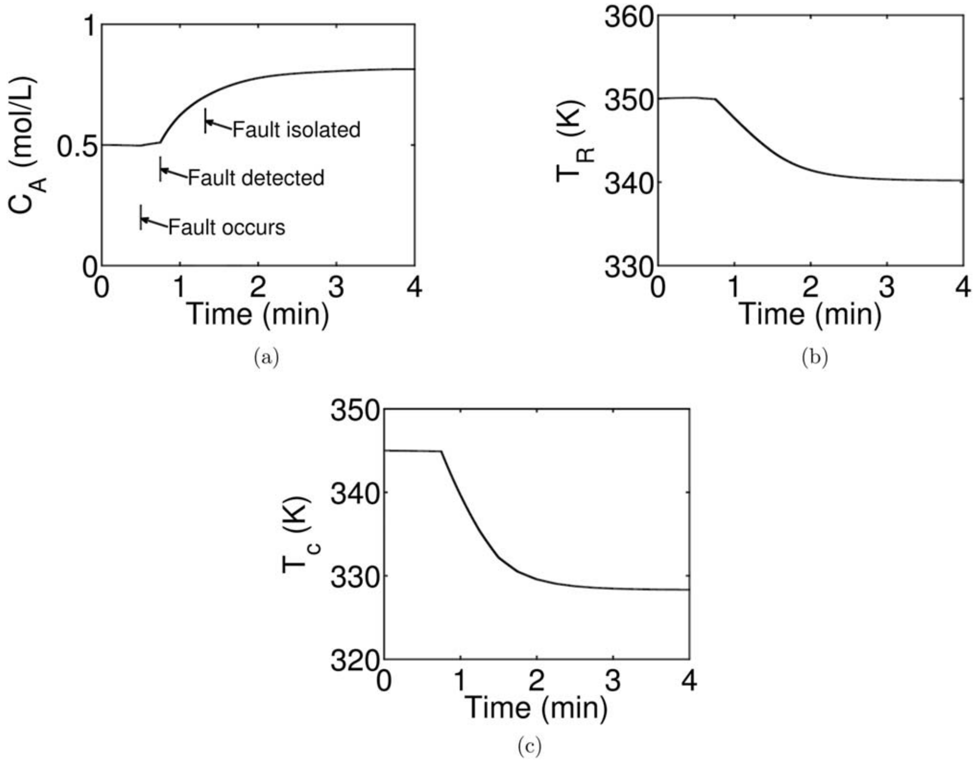
5. If a fault has been detected (i.e., $t_k \geq t_\mathrm{d}$), switch the control law according to Eq. 15. Repeat Step 1.

**Remark 6.** The idea of the active fault-isolation design in Theorem 2 is to move the process to a desired region where the dedicated residuals, denoted by $\tilde{r}_i$, become uniquely sensitive to the complex faults. To this end, a switching rule is designed to, upon fault detection, switch the control objective of operating the process at the nominal equilibrium point to driving it to move toward a fault-isolation point. For a given fault, the effect of the other faults on the evolution of the same process state then can be reduced to an insignificant level as the process approaches the fault-isolation point (or enters the desired region around that point), whereas the effect of the fault under consideration can still be retained and reflected. The declaration of this fault is based on a fault detection design by treating other faults as process disturbances. This is achieved by extending the fault detection design of Theorem 1. It is also shown in Theorem 2 that if the fault can be differentiated from process uncertainty (i.e., $x_i(t) \notin \left[ x_{i,l}(t), x_{i,u}(t) \right]$), then it can also be isolated (i.e., $x_i(t) \notin \left[ \tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t) \right]$) as long as the process states are sufficiently close to the fault-isolation point (i.e., $d$ is sufficiently small).

**Remark 7.** Note that the active fault-isolation scheme of Theorem 2 differs from the existing results (e.g., Ref. 22), where FDI are achieved simultaneously. The class of nonlinear systems studied in Ref. 22 naturally are of a favorable structure allowing the generation of dedicated residuals that are sensitive to faults regardless of the region where the

**Table 2. Process Parameters for the Chemical Reactor Example**

| Parameter | Value | Unit |
|---|---|---|
| $F_2$ | 115.90 | L/min |
| $V$ | 100 | L |
| $k_0$ | $7.2\times10^{10}$ | $\mathrm{min}^{-1}$ |
| $E/R$ | 8750 | K |
| $\Delta H$ | $-5\times10^{2}$ | J/mol |
| $\rho$ | 1000 | g/L |
| $c_\mathrm{p}$ | 0.239 | J/(g K) |
| $UA$ | $5\times10^{4}$ | J/(min K) |
| $V_\mathrm{c}$ | 20 | L |
| $\rho_\mathrm{c}$ | 1000 | g/L |
| $c_\mathrm{pc}$ | 4.2 | J/(g K) |
| $C_\mathrm{A1}$ | 1.2 | mol/L |
| $C_\mathrm{A2}$ | 0.8 | mol/L |
| $T_1$ | 340 | K |
| $T_2$ | 360 | K |
| $T_\mathrm{cf}$ | 293 | K |



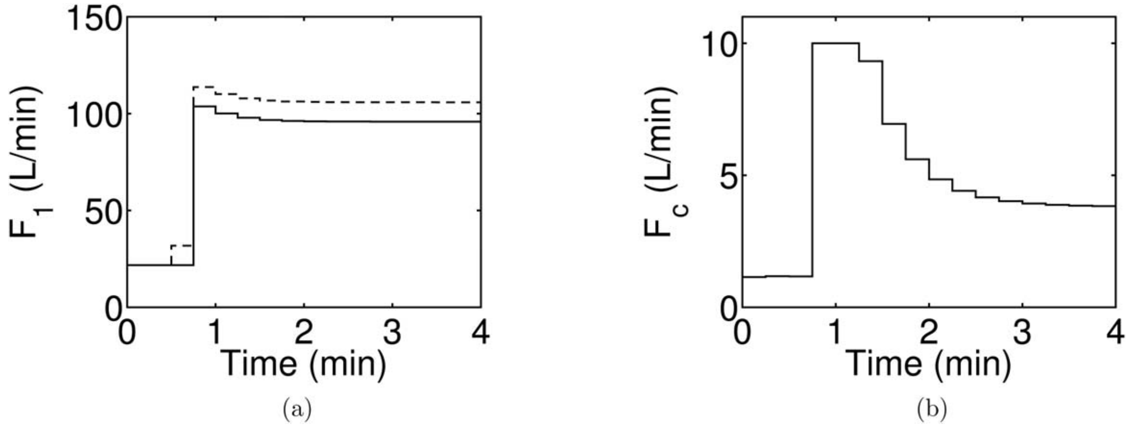
(a) (b) (c)

**Figure 3. Closed-loop state profiles for the chemical reactor example.**

**The process is driven to move toward a fault-isolation point upon fault detection according to the active fault-isolation scheme. The fault is isolated before it approaches the vicinity of the fault-isolation point.**

process operates. Because the occurrence of one fault is not eclipsed by others, the detection of a fault also indicates the location of the faulty component. As complex faults are concerned, however, the dedicated residuals may not be sensitive to faults in the region where the process operates under nominal operation, losing their ability as isolation indicators. Of course if the current operation allows for isolation of faults (as expected for a well-designed process and for most of the "expected" faults), the existing FDI schemes can be used. The applicability of the proposed method is for the "unexpected", which, while triggering the fault detection mechanism (making it obvious that something has gone wrong) might not allow isolation of the fault under nominal operation (determining what exactly has gone wrong). The triggering of the fault-isolation mechanism is, therefore, reliant on the "nominal" FDI mechanism, which at least detects that a fault has taken place, and is an independent fault detection design (see also Figure 1) activating the control law for the purpose of fault isolation.

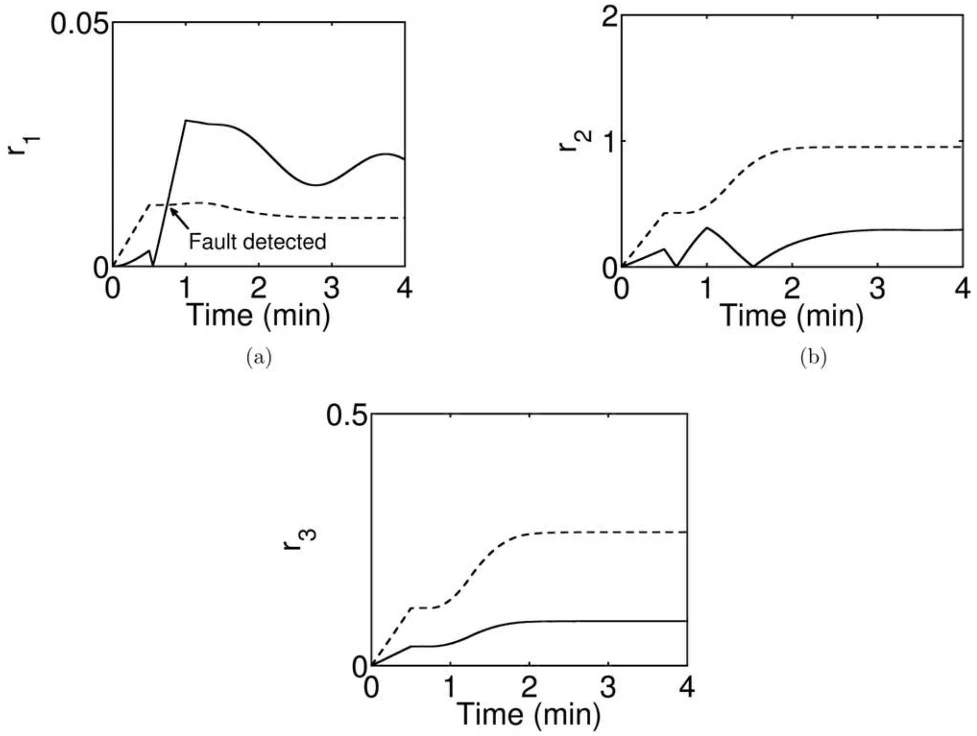
**Remark 8.** The proposed active fault-isolation design relies on the ability to drive the process to a fault-isolation point and the ability to differentiate between faults and plant-model mismatch. In the presence of input constraints, an explicit characterization of a stability region (see, e.g., Ref. 33) can be used to ascertain the ability to stabilize the process at a desired operating point from a certain region by treating faults as process disturbances. In addition to bias or drift faults, this method is also applicable to the case where an actuator possibly freezes as long as the remaining functioning actuators can still provide sufficient control action or



(a) (b)

**Figure 4. Prescribed (solid lines) and actual (dashed lines) input profiles for the chemical reactor example.**

**A fault takes place in $F_1$ at time $t_f$=0.5 min. The discrepancy between the solid and dashed lines shows the occurrence of the fault.**



(a)

(b)

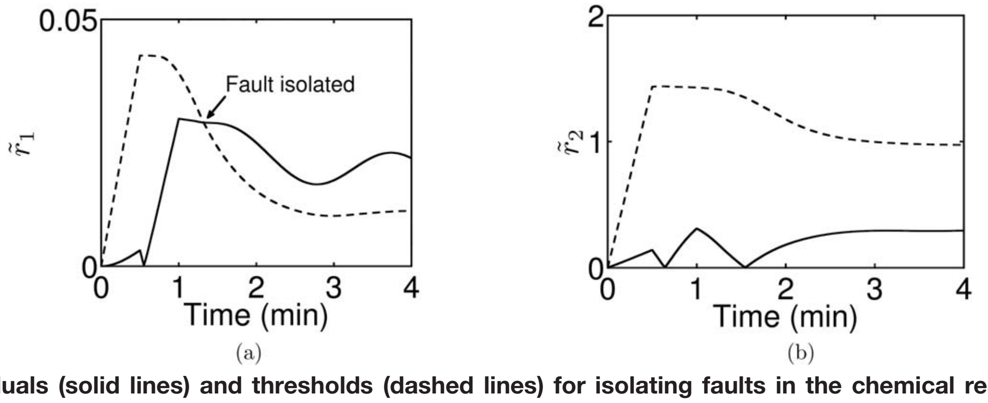
(c)

**Figure 5. Residuals (solid lines) and thresholds (dashed lines) for detecting faults in the chemical reactor example.**

**A fault is detected at 0.75 min via $r_1$ breaching its threshold.**

additional control action is available (e.g., through the use of a backup control actuator) during fault isolation. Note that a frozen actuator does not lead to an "unbounded" error, as constraints in the control design or actuator implementation can be used to determine appropriate bounds on this error. It should also be noted that the purpose of switching the control law is to reduce the possible effect of other faults, but not necessarily to stabilize the process at the fault-isolation point. An explicit consideration of plant-model mismatch makes it possible to quantify the effect of uncertainty and other faults on an isolation indicator. Consequently, even before the process approaches the vicinity of the fault-isolation point, the location of the fault could be identified (see the section of illustrative simulation example for an illustration).

**Remark 9.** The idea of active fault isolation can be extended to handle the case where there does not exist a single operating point that can make residuals sensitive to all the faults. For this case, fault isolation can be achieved by moving the process to a series of operating points. To illustrate this, consider a system described by $\dot{x}=f(x)+g(x)u+(x-a)\theta_1+(x+a)\theta_2$, where $x\in\mathbb{R}$ and $a>0$. In this example, there does not exist a single point at which the effects of $\theta_1$ and $\theta_2$ on the evolution of the system state can be simultaneously eliminated. For this system, we can switch the control law to, upon fault detection, sequentially operate the system at point $x=-a$ and $x=a$, at which isolation of faults $\theta_1$ and $\theta_2$ can be carried out, respectively. We also consider a system described by $\dot{x}=f(x)+g(x)u+(x^2+1)\theta_1+\theta_2$, where $x\in\mathbb{R}$. In this



(a)

(b)

**Figure 6. Residuals (solid lines) and thresholds (dashed lines) for isolating faults in the chemical reactor example in the presence of the active fault-isolation scheme.**

**A fault in $F_1$ is isolated at 1.325 min via $\tilde{r}_1$ breaching its threshold.**

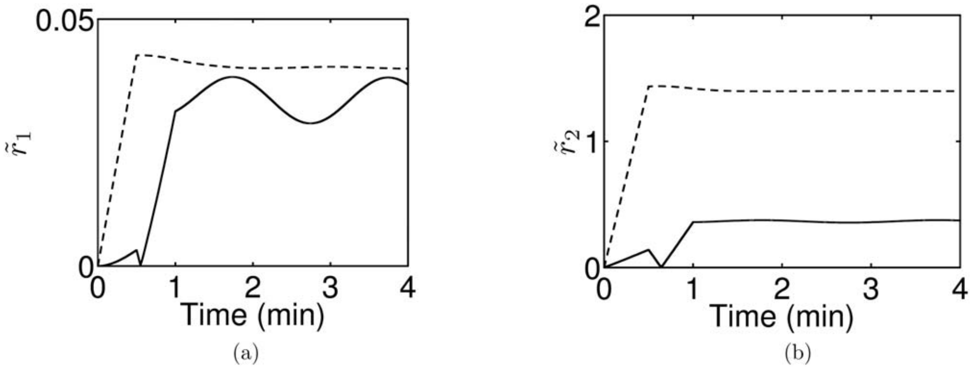


**Figure 7. Residuals (solid lines) and thresholds (dashed lines) for isolating faults in the chemical reactor example under nominal operation.**

**The residuals are not sufficiently sensitive to faults in the absence of the active fault-isolation scheme.**

example, there does not exist a point at which the effect of $\theta_1$ or $\theta_2$ can be eliminated. To differentiate between their effects, we can operate the system to move away from the origin to amplify the possible effect of $\theta_1$, facilitating isolation of the fault $\theta_1$. Isolating the fault $\theta_2$ will require operation at the origin, at which the effect of $\theta_1$ on the evolution of the state is minimum. The fault $\theta_2$ can only be isolated when its actual effect exceeds the possibly extreme effect of $\theta_1$.

**Remark 10.** Accurate and timely identification of a fault is required to trigger the implementation of active FTC

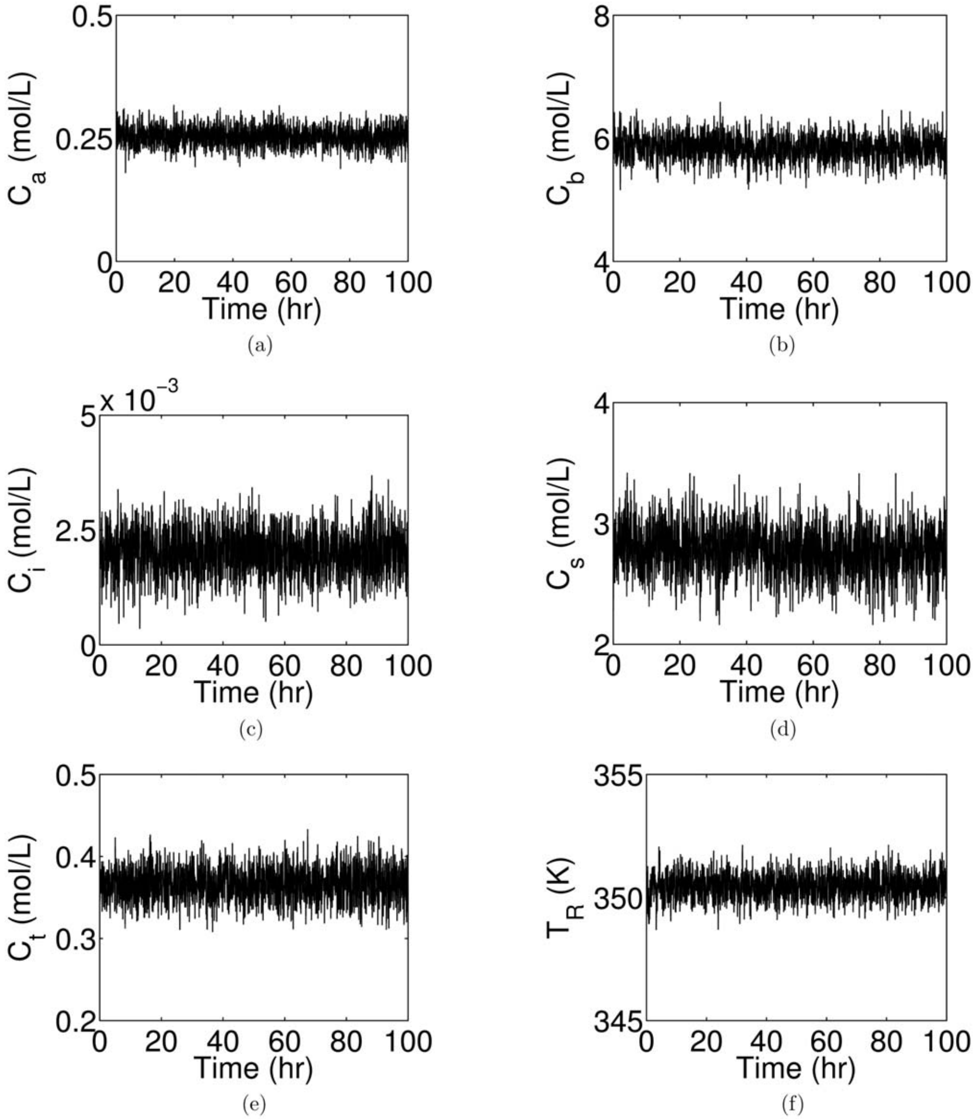


**Figure 8. State trajectories for the solution copolymerization reactor in the absence of active fault isolation.**

**The process states evolve around the nominal operating point even after the fault takes place.**

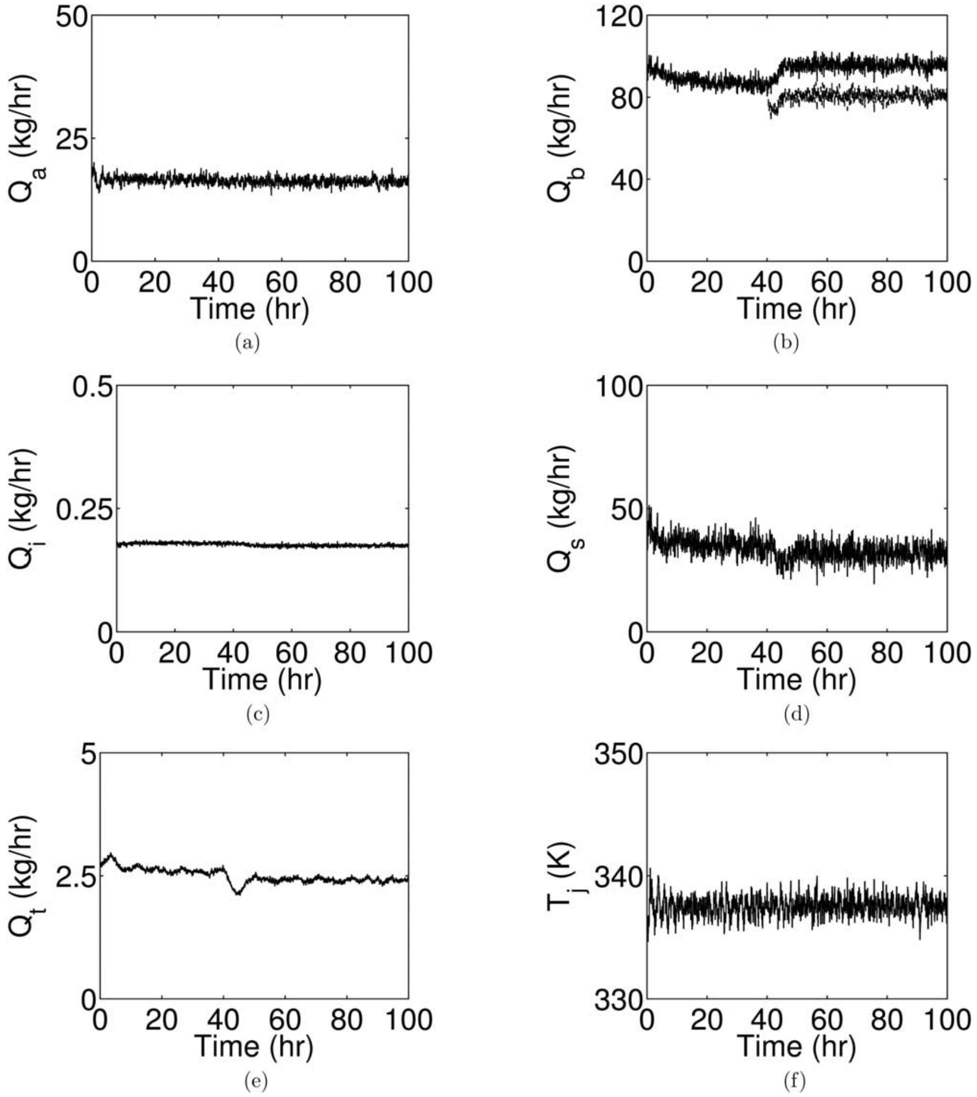


**Figure 9. Prescribed (solid lines) and actual (dashed line) input trajectories for the solution copolymerization reactor in the absence of active fault isolation.**

**A fault takes place in $Q_b$ at time $t_f$=40 h. The discrepancy between the solid and dashed lines shows the occurrence of the fault.**

schemes, such as control reconfiguration (see, e.g., Refs. 34 and 22) or safe-parking (see, e.g., Refs. 35–37), as a prerequisite. In the case of control reconfiguration, an appropriate backup control configuration that does not use the failed actuator is used to preserve nominal operation. If backup control actuators are not available, safe-parking techniques can be used to operate the process at an appropriate temporary operating point (which is referred to as a safe-park point), starting from where nominal operation is resumed upon fault repair. To implement these fault-handling methods, information on the location of faults is needed to choose a backup control configuration or a safe-park point. Without the ability to isolate complex faults, however, the aforementioned fault-handling techniques may not be able to deal with faults effectively.

**Remark 11.** Note that while the faults considered in this work are additive, they encompasses actuator faults and disturbances practically encountered in a well-designed control system. Given that control-affine systems represent a general class of nonlinear systems in the context of chemical process control, actuator faults typically enter the system in an affine manner. Furthermore, to ease the control design for operation under fault-free conditions, the manipulated variables could be appropriately chosen to make the concerned faults enter the system additively (i.e., to eliminate the possible multiplicative effect of actuator faults and disturbances). Note also that the idea proposed in this work could in principle be utilized in the context of sensor fault isolation, where at the nominal operating point, certain magnitudes of sensor faults could be indistinguishable from each other and the process would need to be moved to a different operating point to enhance fault isolation. An additional consideration in such a scenario would be to account for the effect on the state estimation (often a component of sensor fault-isolation schemes).

## Illustrative Simulation Example

In this section, we consider a CSTR example, where an irreversible elementary exothermic reaction of the form A $\overset{k}{\rightarrow}$ B takes place. The feed to the reactor is composed of two streams, as shown in Figure 2. One stream consists of reactant A at a flow rate $F_1$, concentration $C_{A1}$, temperature $T_1$,

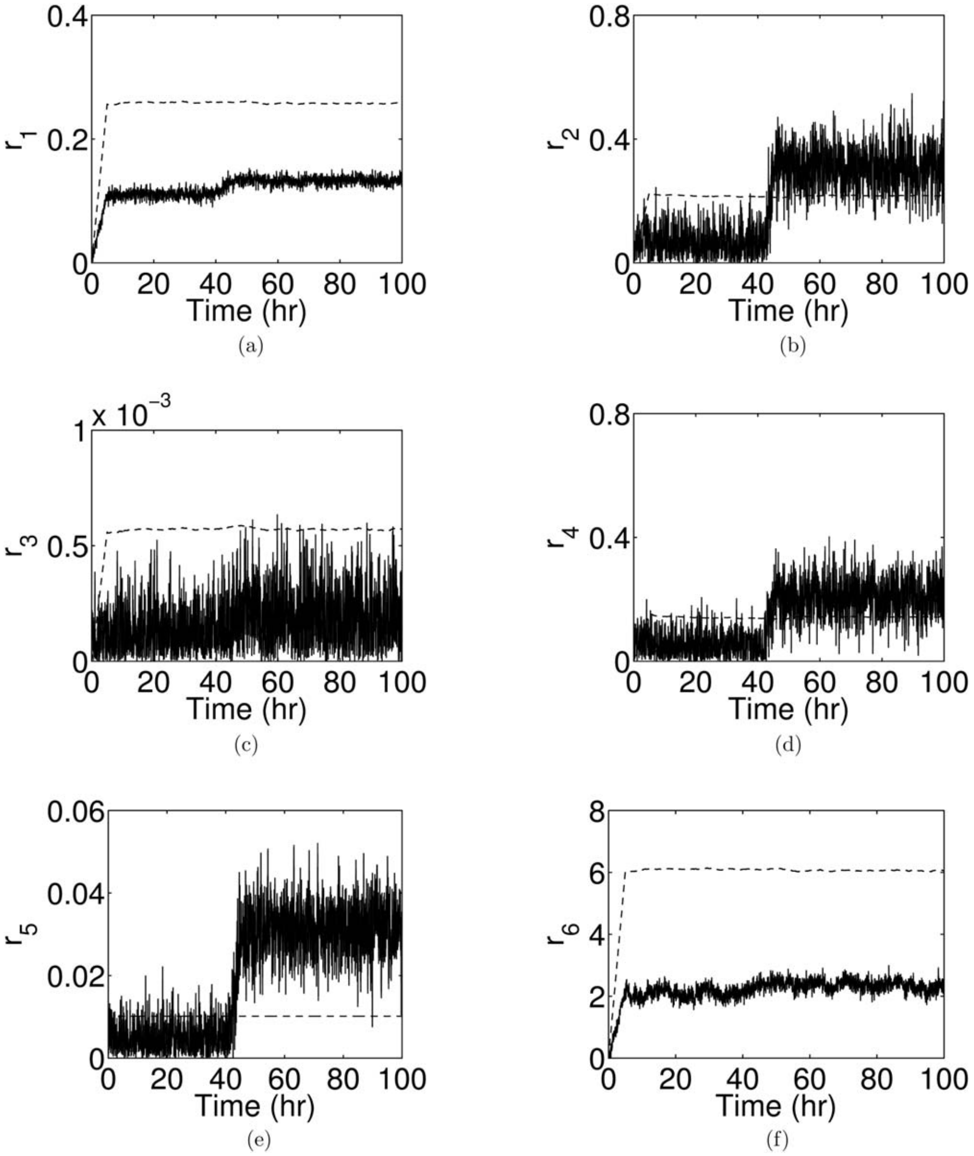


**Figure 10. Detection residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the absence of active fault isolation.**

**The fault is successfully detected at time $t_d$=44 h via $r_5$ breaching its threshold.**

and $F_1$ is adjustable. The other consists of reactant A at a flow rate $F_2$, concentration $C_{A2}$, temperature $T_2$, and $F_2$ is fixed under fault-free conditions. A cooling jacket is equipped to remove heat from the reactor. The cooling stream going to the jacket is at a flow rate $F_c$ and temperature $T_{cf}$. The mathematical model of this chemical reactor takes the following form

$$\begin{aligned}\dot{C}_A &= \sum_{i=1}^{2}\frac{F_i}{V}(C_{Ai}-C_A)-k_0e^{-E/RT_R}C_A\\ \dot{T}_R &= \sum_{i=1}^{2}\frac{F_i}{V}(T_i-T_R)+\frac{(-\Delta H)}{\rho c_p}k_0e^{-E/RT_R}C_A-\frac{UA}{\rho c_p V}(T_R-T_c)\\ \dot{T}_c &= \frac{F_c}{V_c}(T_{cf}-T_c)+\frac{UA}{\rho_c c_{pc} V_c}(T_R-T_c)\end{aligned} \tag{29}$$

where $C_A$ is the concentration of species A, $T_R$ is the temperature in the reactor, $T_c$ is the temperature in the cooling jacket, $V$ is the volume of the reactor, $k_0$, $E$, and $\Delta H$ are the pre-exponential constant, the activation energy, and the enthalpy of the reaction, respectively, $R$ is the ideal gas constant, $\rho$ and $c_p$ are the density and the heat capacity of the fluid in the reactor, respectively, $U$ is the overall heat-transfer coefficient, $A$ is the heat-transfer area of the CSTR, $V_c$ is the volume of the cooling jacket, and $\rho_c$ and $c_{pc}$ are the density and the heat capacity of the cooling stream, respectively. The process parameters can be found in Table 2.

The control objective under fault-free conditions is to stabilize the process at the nominal equilibrium point $C_A$=0.5 mol/L, $T_R$=350 K, and $T_c$=345 K by manipulating $u=[F_1, F_c]^T$, where $0 \le F_1 \le 150$ L/min and $0 \le F_c \le 10$ L/min. The corresponding steady-state values of the input variables are $F_1$=21.75 L/min and $F_c$=1.14 L/min. A Lyapunov-based predictive control design of Ref. 33 adapted as follows is used to illustrate the implementation of the proposed method

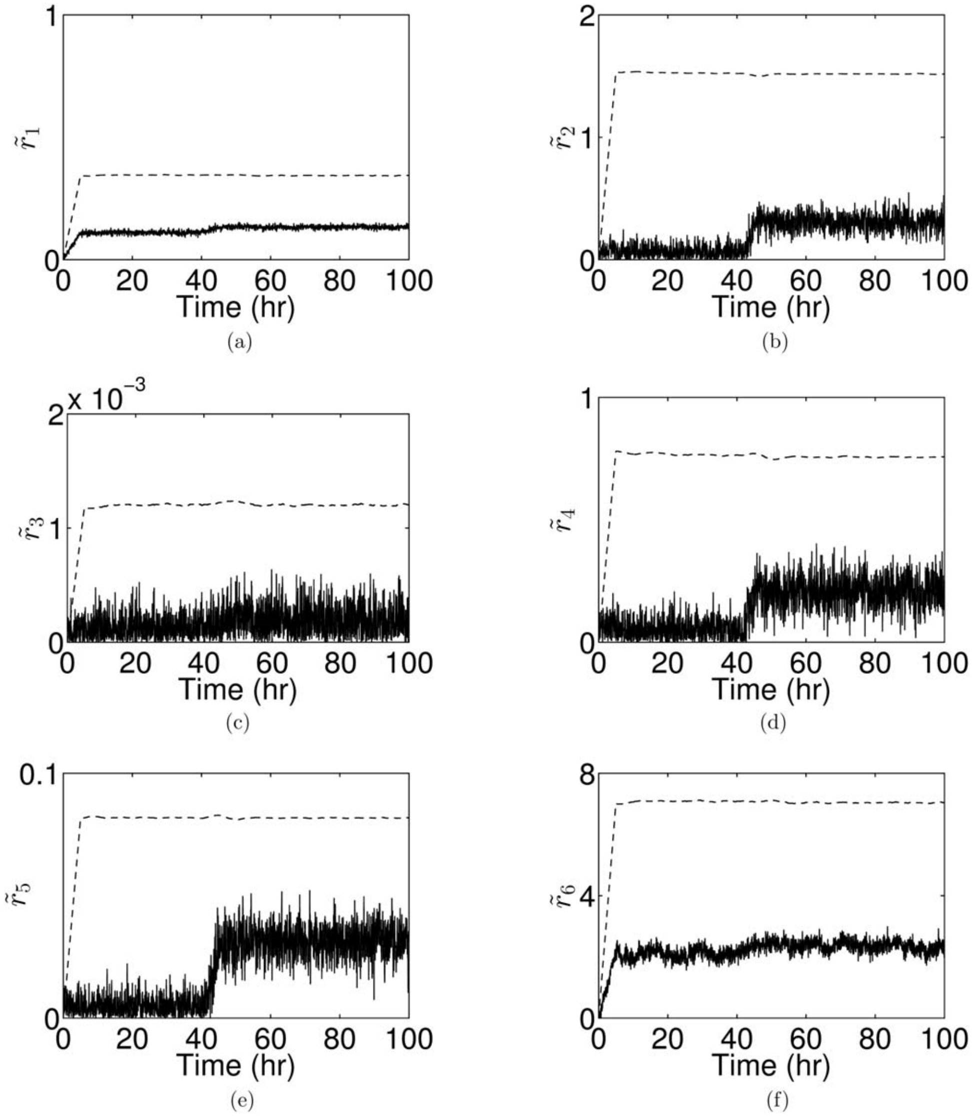


**Figure 11. Isolation residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the absence of active fault isolation.**

**The residual $\tilde{r}_2$ is not sufficiently sensitive to the fault under nominal operation.**

$$\begin{aligned}
u^*(\cdot)=&\text{argmin}\,\{J(x,t_k,u(\cdot))|u(\cdot)\in S\}\\
\text{s.t.}\quad &\dot{\tilde{x}}(\tau|t_k)=f(\tilde{x}(\tau|t_k))+G(\tilde{x}(\tau|t_k))u(\tau)+\frac{d}{\delta},\tau\in[t_k,t_k+T)\\
&\tilde{x}(t_k|t_k)=x(t_k)\\
&V(\tilde{x}(t_k+\delta))\le\alpha V(x(t_k)),\quad \text{if } V(x(t_k))>\delta'\\
&V(\tilde{x}(t_k+\delta))\le\delta',\quad \text{if } V(x(t_k))\le\delta'\\
&d=x(t_k)-\tilde{x}(t_k|t_{k-1})
\end{aligned}\tag{30}$$

where $\Delta$ is the hold-time, $t_k:=k\Delta$, $k=0,\ldots,\infty$, $T$ is the control horizon, $S=S(t,T)$ is a family of piecewise continuous functions (functions continuous from the right) mapping $[t,t+T)$ into a compact subset of $R^n$, a control $u(\cdot)$ in $S$ is characterized by the sequence $\{u(t_k)\}$ and satisfies $u(\tau)=u(t_k)$ for all $\tau\in[t_k,t_k+\Delta)$, $\tilde{x}(\tau|t_k)$ denotes the state prediction at time $\tau$ computed using the initial state at time $t_k$, $\tilde{x}(t_0|t_{-1})=x(t_0)$, $V$ is a Lyapunov function, and $d$ is a parameter used to correct the prediction model, which captures the discrepancy between the current measurement and the state prediction made at the previous time. The objective function is given by

$$J(x,t_k,u(\cdot))=\int_{t_k}^{t_k+T}\left[\|\tilde{x}(\tau)\|_{Q_w}^2+\|u(\tau)\|_{R_w}^2\right]d\tau \tag{31}$$

where $Q_w$ is a positive semidefinite symmetric matrix and $R_w$ is a strictly positive definite symmetric matrix. The minimizing control $u^*(\cdot)$ is applied to the system over $[t,t+\Delta)$, and the same procedure is repeated at the next instant. In this example, $\Delta=0.25$ min, $T=2\Delta$, $Q_w=\text{diag}\left[10^5,10^3,10\right]$, $R_w=\text{diag}\,[20,100]$, $\alpha=0.9$, $\delta'=0.02$, and a quadratic control Lyapunov function $\text{V}=x^{\text{T}}\ Px$ is used, where $P=\begin{bmatrix}0.2546 & 0.0547 & 0.0526\\ 0.0547 & 0.1544 & 0.0826\\ 0.0526 & 0.0826 & 0.3600\end{bmatrix}$ for the nominal equilibrium point.

Consider the process of Eq. 29 subject to actuator faults in $F_1$ and $F_\text{c}$, and a process fault in $F_2$; that is, the fault vector $\theta(t)=\left[\tilde{F}_1,\tilde{F}_2,\tilde{F}_c\right]^{\text{T}}$, where the tilde denotes faults. It follows that

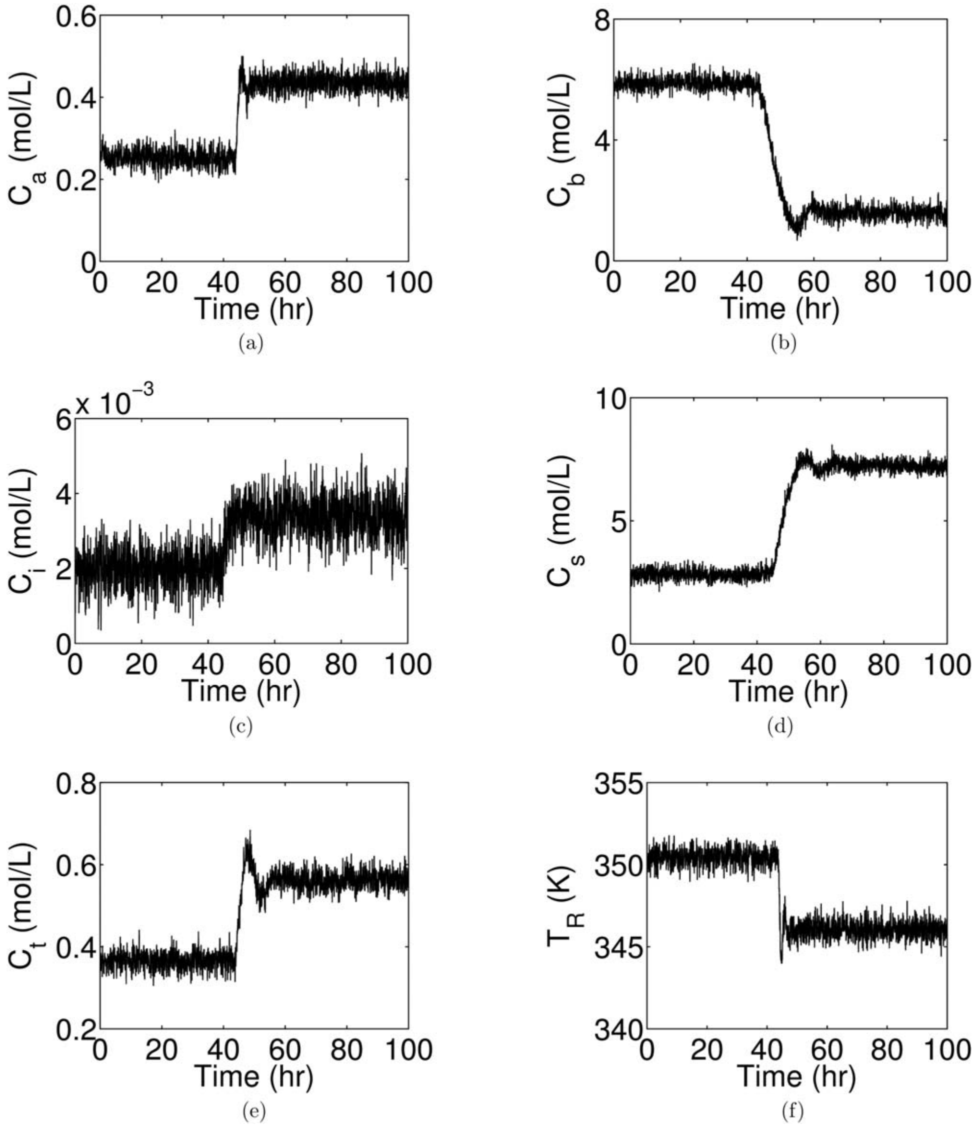


**Figure 12. State trajectories for the solution copolymerization reactor in the presence of active fault isolation.**

**The process is driven to move toward a point that facilitates isolation of a fault in $Q_b$ upon fault detection at time $t_d$=43.65 h.**

$$D(x)=\begin{bmatrix} \frac{C_{A1}-C_A}{V} & \frac{C_{A2}-C_A}{V} & 0 \\ \frac{T_1-T_R}{V} & \frac{T_2-T_R}{V} & 0 \\ 0 & 0 & \frac{T_{cf}-T_c}{V_c} \end{bmatrix} \tag{32}$$

According to Definition 1, the system has a fault-isolation point $\tilde{x}=[C_{A2}, T_1, T_c]^T$, with $C_A$=0.8 mol/L, $T_R$=340 K, and $T_c$=328.5 K. The corresponding steady-state values of the inputs are $F_1$=95.87 L/min and $F_c$=3.84 L/min. For this operating point, $P=\begin{bmatrix} 0.2845 & 0.0309 & 0.0432 \\ 0.0309 & 0.1602 & 0.1123 \\ 0.0432 & 0.1123 & 0.5062 \end{bmatrix}$ is used in the control design. The bounds on uncertain variables used in the FDI design are ±5% for $k_0$ and −10% and 5% for $UA$. The faults are bounded as $-20 \le \tilde{F}_i \le 20$ L/min, $i$=1,2. The fault detection horizon $T'=2\Delta$, and the evaluation period $\Delta_{FDI}=\Delta/10$.

To illustrate the active fault-isolation design for the system of Eq. 29 subject to plant-model mismatch, we consider a fault that takes place in the actuator used to adjust $F_1$ at time $t_f$=0.5 min. Specifically, the fault is described as follows

$$\tilde{F}_1=\begin{cases} 0, & \text{if } 0 \le t < t_f \\ 10, & \text{if } t \ge t_f \end{cases} \tag{33}$$

Furthermore, $k_0$ is 2% larger than its nominal value, and $UA$ is 5% smaller than its nominal value. The process starts from the nominal equilibrium point. The closed-loop state profiles with the implementation of the proposed active fault-isolation design are shown in Figure 3, where the times of fault occurrence, detection, and isolation are also indicated. It can be seen that the fault is isolated even before the process states approach the vicinity of the fault-isolation point. The corresponding prescribed and actual input profiles are shown by the solid and dashed lines, respectively, in Figure 4.

To detect faults, the residuals $r_i$, $i$=1, 2, 3, and the corresponding thresholds for the purpose of fault detection are

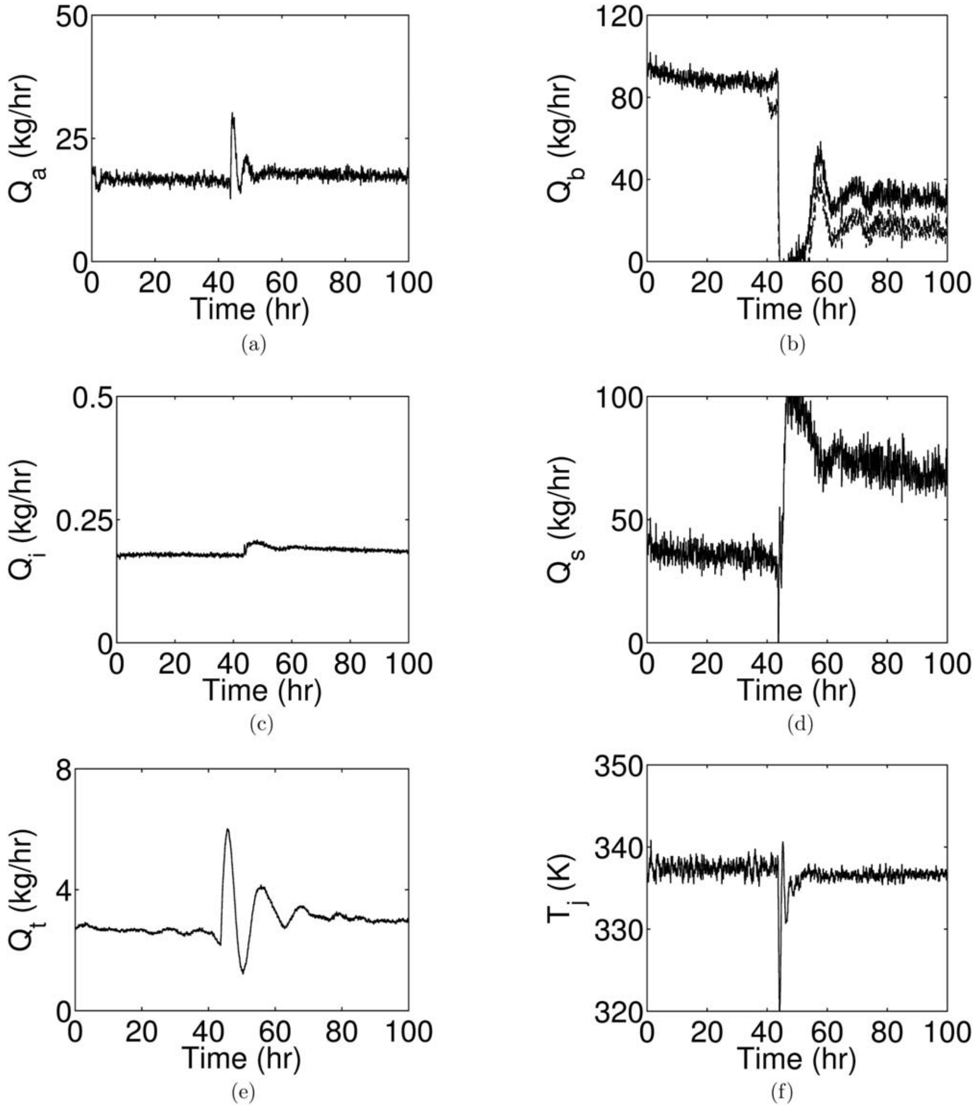


**Figure 13. Prescribed (solid lines) and actual (dashed line) input trajectories for the solution copolymerization reactor in the presence of active fault isolation.**

**A fault takes place in $Q_b$ at time $t_f$=40 h. The discrepancy between the solid and dashed lines shows the occurrence of the fault.**

generated, as shown by the solid and dashed lines, respectively, in Figure 5. It is observed that $r_1$ breaches its threshold at time 0.75 min, indicating the occurrence of a fault. Because $r_1$ is associated with faults in $F_1$ and $F_2$, it is only concluded that a fault takes place in $F_1$ or $F_2$. The residual $r_2$ does not breach its threshold, because the fault and uncertainty counteract the effect of each other in this specific example. The residual $r_3$ serves as a dedicated residual for $F_c$. It is also seen from Figures 5a,b that some residuals evolve sharply in the sense that they first approach zero and then increase. The sharp changes are mainly because of the way that the residuals are defined. Note that each residual is defined as the norm of the difference between the state measurement and the average of the lower and upper bounds. As there is a possibility that the state measurement goes across the profile of the average of the bounds, a residual may first approach zero and then increase at a similar rate in terms of its absolute value.

To isolate faults, the supervisor dictates switching the controller to drive the process to move toward the fault-isolation point $\tilde{x}$. The residuals $\tilde{r}_1$ and $\tilde{r}_2$ and the corresponding thresholds for the purpose of fault isolation are shown by the solid and dashed lines, respectively, in Figure 6. It can be seen that before the switching, $\tilde{r}_1$ and $\tilde{r}_2$ are below their thresholds, and after the switching, both the thresholds decrease as the process approaches the fault-isolation point. Furthermore, $\tilde{r}_1$ breaches its threshold at time 1.325 min, indicating the occurrence of a fault in $F_1$. Although they are dedicated residuals, $\tilde{r}_1$ and $\tilde{r}_2$ are not sufficiently sensitive to faults (i.e., the residuals are below the thresholds) under nominal operation, as shown in Figure 7. In contrast, they become sensitive to faults after the switching in the presence of the proposed active fault-isolation scheme, as shown in Figure 6.

## Application to the Solution Copolymerization Reactor

We first show that faults may not be isolated under nominal operation. At the nominal operating point, the fault distribution matrix normalized for each row is evaluated as follows

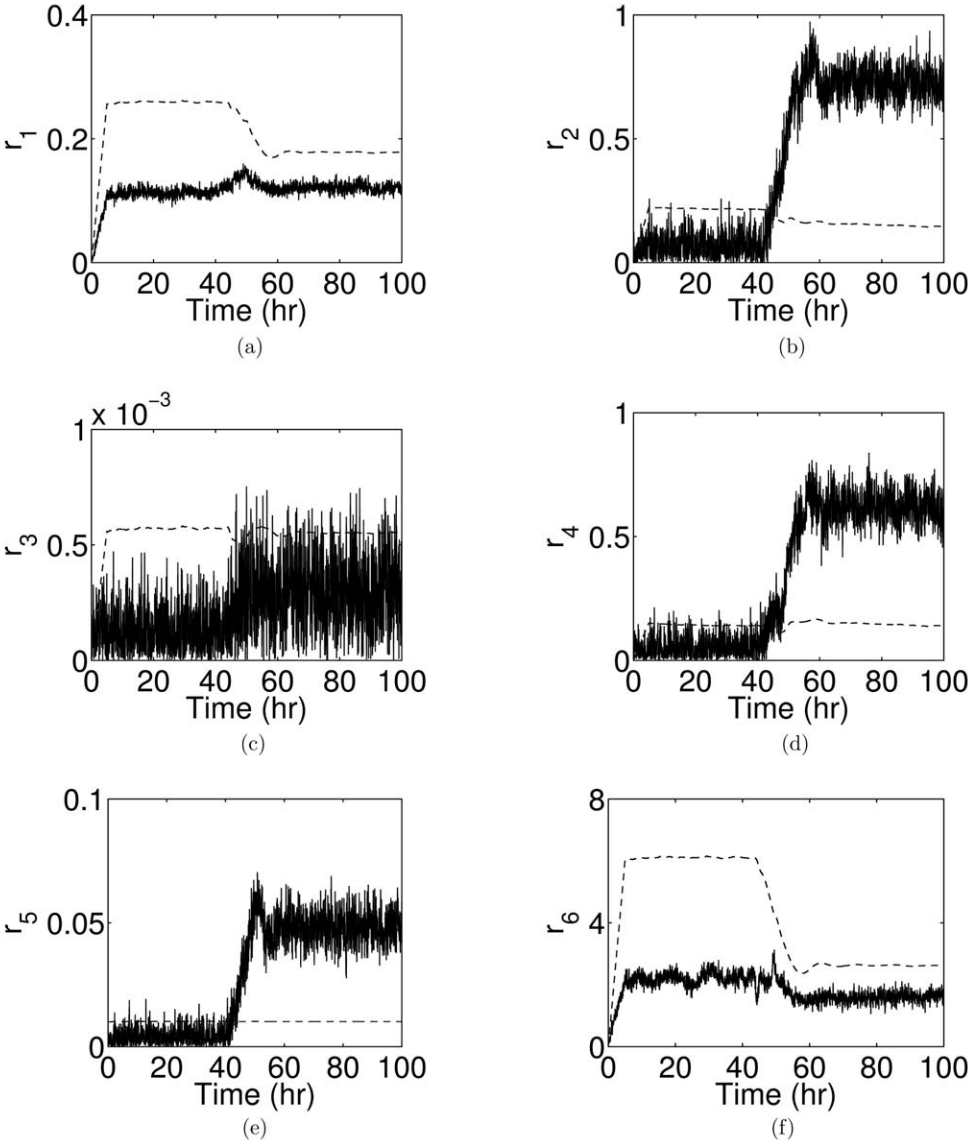


**Figure 14. Detection residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the presence of active fault isolation.**

**The fault is successfully detected at time $t_d$=43.65 h via $r_5$ breaching its threshold.**

$$D=\begin{bmatrix} \mathbf{0.9982} & -0.0297 & -0.0297 & -0.0297 & -0.0297 & 0 \\ -0.4682 & 0.3507 & -0.4682 & -0.4682 & -0.4682 & 0 \\ -0.0004 & -0.0004 & \mathbf{1.0000} & -0.0004 & -0.0004 & 0 \\ -0.2723 & -0.2723 & -0.2723 & 0.8387 & -0.2723 & 0 \\ -0.0187 & -0.0187 & -0.0187 & -0.0187 & \mathbf{0.9993} & 0 \\ 0.0054 & 0.0054 & 0.0054 & 0.0054 & 0.0054 & \mathbf{0.9999} \end{bmatrix} \tag{34}$$

It can be seen that the element in the first row and first column is approximately equal to one, which is much larger than the others in the same row. This implies that the effect of the fault in $Q_a$ on the evolution of $C_a$ is much more significant compared with the others. Therefore, we use the differential equation for $C_a$ to generate the residual $\tilde{r}_1$ as an isolation indicator, which should be sensitive to this fault under nominal operation. Similarly, residuals $\tilde{r}_3$, $\tilde{r}_5$, and $\tilde{r}_6$ are generated using the differential equations for $C_i$, $C_t$, and $T_R$ for faults in $Q_i$, $Q_t$, and $T_c$, respectively. Note that the differences between the element in row 2 (row 4) and column 2 (column 4), and other elements in the same row are not significant compared with other rows in the fault distribution matrix of Eq. 34. Therefore, the isolation residuals designed for faults in $Q_b$ and $Q_s$ using the differential equations for $C_b$ and $C_s$ may not be enough sensitive to those faults under nominal operation. To show this point, we consider a fault taking place in $Q_b$ at time $t_f$=40 h, which is described by

$$\theta_2=\begin{cases} 0, & \text{if } 0 \le t < t_f \\ -15\left[1-e^{-2(t-t_f)}\right], & \text{if } t \ge t_f \end{cases} \tag{35}$$

It can be seen from Figures 8 and 9 that the process states sill remain around the nominal operating point after the fault takes place, with inputs deviating from where they were before the fault occurrence. The fault detection residuals $r_j$, $j$=1, ..., 6, are generated using the corresponding differential equations. To reduce false alarms caused by

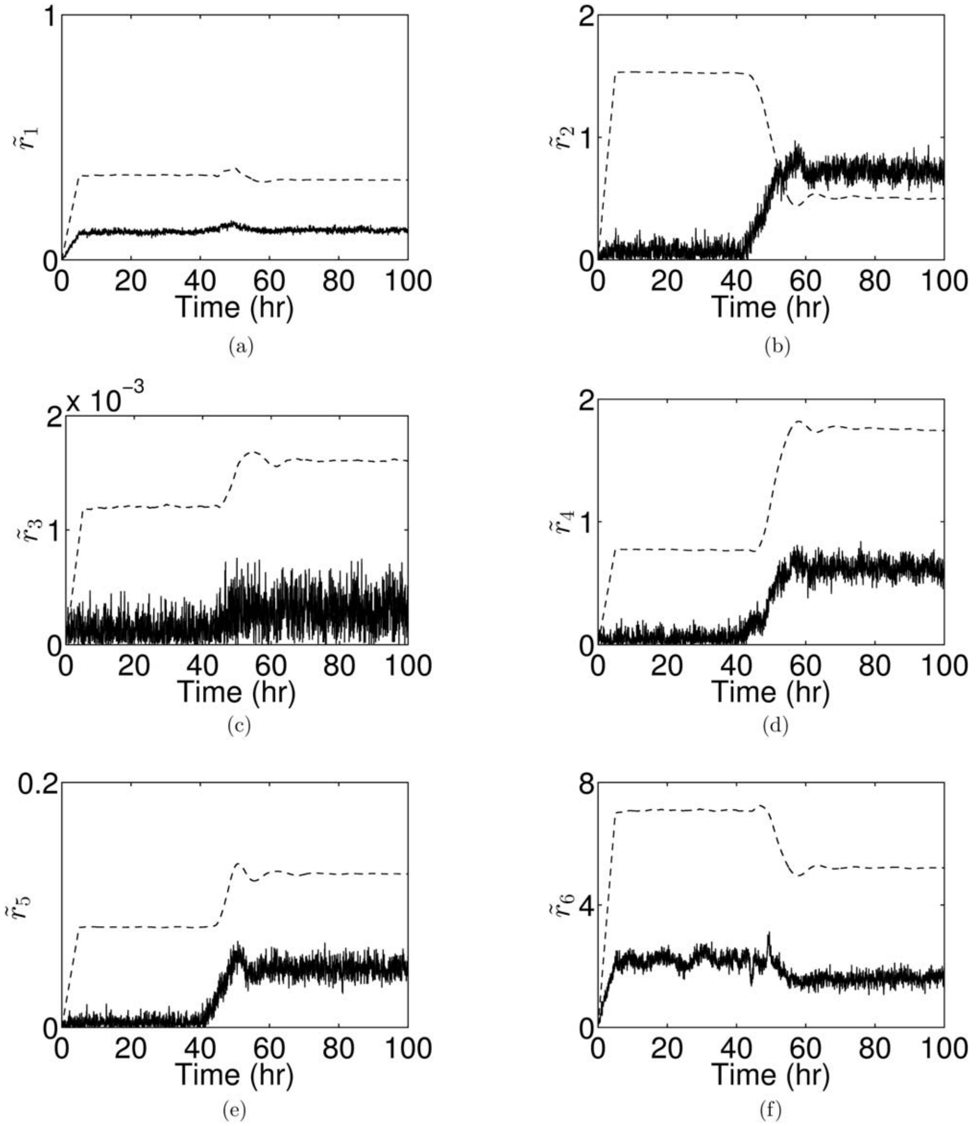


**Figure 15. Isolation residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the presence of active fault isolation.**

**The fault is isolated at time $t_i$=54.25 h via $\tilde{r}_2$ breaching its threshold.**

measurement noise, a fault is declared only when 90% of the residual values breach the corresponding threshold for 20 successive evaluations. Because measurement noise affects the residual $r_5$ much more than uncertainty, this residual is relaxed by 0.01 to reduce false alarms. As shown in Figure 10, the fault is first detected at time $t_d$=44 h through $r_5$ breaching its threshold. In addition, residuals $r_2$ and $r_4$ also breach their thresholds. However, none of the isolation residuals breach their thresholds, as shown in Figure 11. This is because the effects of faults in $Q_b$ and other inputs cannot be well differentiated under nominal operation as explained earlier.

We next show that the fault considered earlier can be isolated through active fault isolation for the solution copolymerization reactor. It can be seen from Eq. 14 that to amplify the effect of the fault in $Q_b$ ($Q_s$) on the evolution of $C_b$ ($C_s$), one can operate the process at a point where $C_b$ ($C_s$) is much smaller than its nominal value. To this end, we decrease the flow rate of monomer B to 15 kg/h and increase the flow rate of solvent to 60 kg/h at steady state, respectively, while keeping the others unchanged. This leads to an operating point at which $C_a$=4.340 × $10^{-1}$ kmol/m$^3$, $C_b$=1.457 kmol/m$^3$, $C_i$=3.340 × $10^{-3}$ kmol/m$^3$, $C_s$=7.042 kmol/m$^3$, $C_t$=5.610 × $10^{-1}$ kmol/m$^3$, and $T_R$=346.1 K. At this operating point, the fault distribution matrix is evaluated as follows

$$D=\begin{bmatrix} \mathbf{0.9946} & -0.0517 & -0.0517 & -0.0517 & -0.0517 & 0 \\ -0.1579 & \mathbf{0.9488} & -0.1579 & -0.1579 & -0.1579 & 0 \\ -0.0006 & -0.0006 & \mathbf{1.0000} & -0.0006 & -0.0006 & 0 \\ -0.4790 & -0.4790 & -0.4790 & 0.2865 & -0.4790 & 0 \\ -0.0289 & -0.0289 & -0.0289 & -0.0289 & \mathbf{0.9983} & 0 \\ 0.0144 & 0.0144 & 0.0144 & 0.0144 & 0.0144 & \mathbf{0.9995} \end{bmatrix} \tag{36}$$

It can be seen that the element in row 2 and column 2 is much larger compared with others in the same row. This implies that at this point, the corresponding residual should be more sensitive to the fault in $Q_b$ than at the nominal operating point. For this case, the state and input trajectories are plotted in Figures 12 and 13, respectively. The fault is first detected at time $t_d=43.65$ h through $r_5$ breaching its threshold, as shown in Figure 14. Upon fault detection, the controller is switched to drive the process to move toward the aforementioned operating point. As the process approaches the desired operating point, the threshold for the fault in $Q_b$ decreases (see Figure 15). Consequently, the residual $\tilde{r}_2$ becomes sensitive to the fault, and the fault is successfully isolated at time $t_i=54.25$ h via $\tilde{r}_2$ breaching its threshold. If no faults were isolated, the supervisor would subsequently dictate operating the process at a point that favors isolation of a fault in $Q_s$ by following the same idea as illustrated earlier.

## Conclusions

This work considered the problem of designing an active fault-isolation scheme for nonlinear process systems subject to uncertainty. In particular, the faults under consideration include bounded actuator faults and process disturbances that affect the evolution of the same process states. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory feedback control. To this end, a dedicated fault-isolation residual and its time-varying threshold were generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults in the operating region under nominal operation. To make these residuals sensitive to faults, a switching rule was designed to drive the process states, upon detection of a fault, to move toward an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea was then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults for the case where the residuals are not simultaneously sensitive to faults at a single operating point. The effectiveness of the proposed active fault-isolation scheme was illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of MMA and VAc.

## Acknowledgments

Financial support from the Natural Sciences and Engineering Research Council of Canada and the Ontario Graduate Scholarship for Miao Du is gratefully acknowledged.

## Literature Cited

1. Qin SJ. Statistical process monitoring: Basics and beyond. *J Chemometr.* 2003;17:480–502.
2. Mahadevan S, Shah SL. Fault detection and diagnosis in process data using one-class support vector machines. *J Process Control.* 2009;19:1627–1639.
3. Perk S, Teymour F, Cinar A. Statistical monitoring of complex chemical processes using agent-based systems. *Ind Eng Chem Res.* 2010;49:5080–5093.
4. Perk S, Teymour F, Cinar A. Adaptive agent-based system for process fault diagnosis. *Ind Eng Chem Res.* 2011;50:9138–9155.
5. Alcala CF, Qin SJ. Analysis and generalization of fault diagnosis methods for process monitoring. *J Process Control.* 2011;21:322–330.
6. Venkatasubramanian V, Rengaswamy R, Kavuri SN, Yin K. A review of process fault detection and diagnosis Part III: Process history based methods. *Comp Chem Eng.* 2003;27:327–346.
7. Kresta JV, MacGregor JF, Marlin TE. Multivariate statistical monitoring of process operating performance. *Can J Chem Eng.* 1991;69:35–47.
8. MacGregor JF, Jaeckle C, Kiparissides C, Koutoudi M. Process monitoring and diagnosis by multiblock PLS methods. *AIChE J.* 1994;40:826–838.
9. Yoon S, MacGregor JF. Fault diagnosis with multivariate statistical models. Part I: Using steady state fault signatures. *J Process Control.* 2001;11:387–400.
10. Armaou A, Demetriou MA. Robust detection and accommodation of incipient component and actuator faults in nonlinear distributed processes. *AIChE J.* 2008;54:2651–2662.
11. Li W, Shah SL, Xiao D. Kalman filters in non-uniformly sampled multirate systems: for FDI and beyond. *Automatica.* 2008;44:199–208.
12. McFall CW, Muñoz de la Peña D, Ohran B, Christofides PD, Davis JF. Fault detection and isolation for nonlinear process systems using asynchronous measurements. *Ind Eng Chem Res.* 2008;47:10009–10019.
13. Ghantasala S, El-Farra NH. Robust actuator fault isolation and management in constrained uncertain parabolic PDE systems. *Automatica.* 2009;45:2368–2373.
14. Ding SX, Zhang P, Naik A, Ding EL, Huang B. Subspace method aided data-driven design of fault detection and isolation systems. *J Process Control.* 2009;19:1496–1510.
15. Hu Y, El-Farra NH. Robust fault detection and monitoring of hybrid process systems with uncertain mode transitions. *AIChE J.* 2011;57:2783–2794.
16. Frank PM. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: a survey and some new results. *Automatica.* 1990;26:459–474.
17. Frank PM, Ding X. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *J Process Control.* 1997;7:403–424.
18. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN. A review of process fault detection and diagnosis. Part I. Quantitative model-based methods. *Comp Chem Eng.* 2003;27:293–311.
19. Chen J, Patton RJ, Zhang HY. Design of unknown input observers and robust fault detection filters. *Int J Control.* 1996;63:85–105.
20. Hamelin F, Sauter D. Robust fault detection in uncertain dynamic systems. *Automatica.* 2000;36:1747–1754.
21. Mhaskar P, Gani A, El-Farra NH, McFall C, Christofides PD, Davis JF. Integrated fault-detection and fault-tolerant control of process systems. *AIChE J.* 2006;52:2129–2148.
22. Mhaskar P, McFall C, Gani A, Christofides PD, Davis JF. Isolation and handling of actuator faults in nonlinear systems. *Automatica.* 2008;44:53–62.
23. Zhang X, Polycarpou MM, Parisini T. Fault diagnosis of a class of nonlinear uncertain systems with Lipschitz nonlinearities using adaptive estimation. *Automatica.* 2010;46:290–299.
24. Liu J, Ohran BJ, Muñoz de la Peña D, Christofides PD, Davis JF. Monitoring and handling of actuator faults in two-tier control systems for nonlinear processes. *Chem Eng Sci.* 2010;65:3179–3190.
25. Watanabe K, Matsuura I, Abe M, Kubota M, Himmelblau DM. Incipient fault diagnosis of chemical processes via artificial neural networks. *AIChE J.* 1989;35:1803–1812.
26. Mehranbod N, Soroush M, Piovoso M, Ogunnaike BA. Probabilistic model for sensor fault detection and identification. *AIChE J.* 2003;49:1787–1802.
27. Mehranbod N, Soroush M, Panjapornpon C. A method of sensor fault detection and identification. *J Process Control.* 2005;15:321–339.
28. Ohran BJ, Muñoz de la Peña D, Davis JF, Christofides PD. Enhancing data-based fault isolation through nonlinear control. *AIChE J.* 2008;54:223–241.
29. Ohran BJ, Liu J, Muñoz de la Peña D, Christofides PD, Davis JF. Data-based fault detection and isolation using feedback control: output feedback and optimality. *Chem Eng Sci.* 2009;64:2370–2383.
30. Du M, Nease J, Mhaskar P. An integrated fault diagnosis and safe-parking framework for fault-tolerant control of nonlinear systems. *Int J Rob Nonlin Control.* 2012;22:105–122.
31. Congalidis JP, Richards JR, Ray WH. Feedforward and feedback control of a solution copolymerization reactor. *AIChE J.* 1989;35:891–907.
32. Muske KR, Badgwell TA. Disturbance modeling for offset-free linear model predictive control. *J Process Control.* 2002;12:617–632.

33. Mahmood M, Gandhi R, Mhaskar P. Safe-parking of nonlinear process systems: handling uncertainty and unavailability of measurements. *Chem Eng Sci.* 2008;63:5434–5446.
34. Mhaskar P. Robust model predictive control design for fault-tolerant control of process systems. *Ind Eng Chem Res.* 2006;45: 8565–8574.
35. Gandhi R, Mhaskar P. Safe-parking of nonlinear process systems. *Comp Chem Eng*. 2008;32:2113–2122.
36. Du M, Gandhi R, Mhaskar P. An integrated fault detection and isolation and safe-parking framework for networked process systems. *Ind Eng Chem Res.* 2011;50:5667–5679.
37. Du M, Mhaskar P. A safe-parking and safe-switching framework for fault-tolerant control of switched nonlinear systems. *Int J Control.* 2011;84:9–23.

*Manuscript received May 30, 2012, and revision received Oct. 2, 2012*