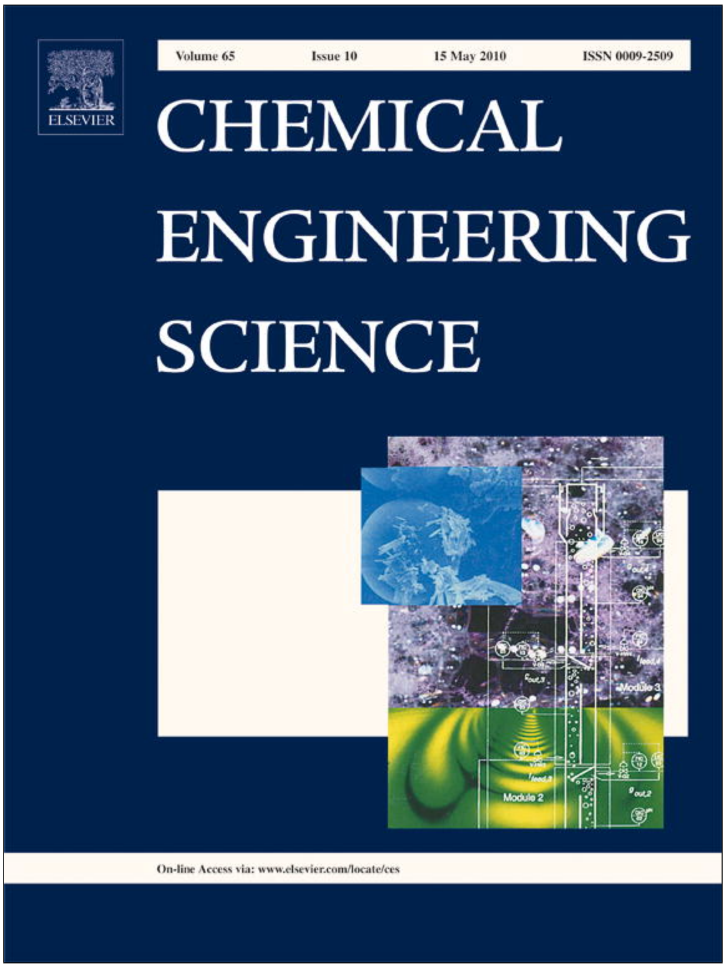

Volume 65 Issue 10 15 May 2010 ISSN 0009-2509

ELSEVIER

CHEMICAL ENGINEERING SCIENCE

On-line Access via: www.elsevier.com/locate/ces

Chemical Engineering Science 65 (2010) 3179–3190

Contents lists available at ScienceDirect

Chemical Engineering Science

journal homepage: www.elsevier.com/locate/ces

Monitoring and handling of actuator faults in two-tier control systems for nonlinear processes

Jinfeng Liu [a], Benjamin J. Ohran [a], David Muñoz de la Peña [b], Panagiotis D. Christofides [a,c,*], James F. Davis [a]

[a] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA
[b] Departamento de Ingeniería de Sistemas y Automática, Universidad de Sevilla, Camino de los Descubrimientos S/N, 41092 Sevilla, Spain
[c] Department of Electrical Engineering, University of California, Los Angeles, CA 90095-1592, USA

ARTICLE INFO

Article history:
Received 3 April 2009
Received in revised form
15 January 2010
Accepted 1 February 2010
Available online 10 February 2010

Keywords:
Two-tier control systems
Fault detection and isolation
Fault-tolerant control
Asynchronous measurements
Nonlinear processes

ABSTRACT

This work focuses on the monitoring and reconfiguration of two-tier control systems applied to general nonlinear processes in the presence of control actuator faults. Specifically, a general class of nonlinear process systems is first considered and is controlled by a two-tier control system integrating a local control system using continuous sensing/actuation with a networked control system using asynchronous sensing/actuation. To deal with control actuator faults that may occur in the closed-loop system and eliminate the ability of the two-tier control system to stabilize the process, a fault detection and isolation (FDI) and fault-tolerant control (FTC) system is designed which detects and isolates actuator faults and determines how to reconfigure the two-tier control system to handle the actuator faults and ensure closed-loop stability. The FDI/FTC system uses continuous measurements of process variables like temperature and asynchronous measurements of variables like species concentrations. We develop reconfiguration-based FTC schemes that effectively deal with faults in the actuators of both the local and networked control systems. A detailed mathematical analysis is carried out to determine precise conditions for the stabilizability of the FDI/FTC system. The method is demonstrated using a reactor-separator process consisting of two continuously stirred tank reactors and a flash tank separator with recycle stream.

1. Introduction

Over the last few decades, advancements in monitoring and control technology have led to higher efficiency and improved economics in the process industries through better monitoring and control of process systems. More recently, we have seen a trend towards "smart" plants that are capable of highly automated control with decision making at the plant level taking into account environmental, health, safety and economic considerations (Christofides et al., 2007). Specifically, some of the recent advances in process monitoring and control have been achieved due to a shift from traditional control systems that utilize point-to-point wired communication links using a small number of sensors and actuators to control systems that take advantage of an efficient integration of the existing, point-to-point communication networks and additional networked (wired or wireless) actuator/sensor devices. Such an augmentation in sensor information and network-based availability of wired and wireless data is now well underway in the process industries (Christofides et al., 2007; Ydstie, 2002; Davis, 2007; Neumann, 2007) and clearly has the potential to dramatically improve the ability of the single-process and plant-wide control systems to optimize process and plant performance. Along with the move towards "smart plant" operation that uses networked control systems, improved methods of fault detection, isolation and handling are necessary due to the issues raised by automation itself. Specifically, despite the many benefits of automatic process control, increased complexity and instrumentation can cause automated plants to become more susceptible to control system failures. As part of the continuing improvements to process monitoring and control, it is important to design systems capable of detecting and handling such process or control system abnormalities (Mhaskar et al., 2007, 2008; McFall et al., 2008).

Although there are many works focusing on the analysis and design of networked control systems (Nešić and Teel, 2004a; Montestruque and Antsaklis, 2003, 2004), from a control design standpoint, augmenting preexisting, local control networks with additional networked sensors and actuators poses a number of challenges including the feedback of additional measurements that may be asynchronous and/or delayed, for example, additional

[*] Corresponding author at: Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

0009-2509/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ces.2010.02.001

species concentrations or particle size distributions measurements. In a previous work (Liu et al., 2010) (see also Muñoz de la Peña and Christofides, 2008; Liu et al., 2008), we introduced a two-tier control architecture for nonlinear process systems with both continuous and asynchronous sensing and/or actuation. This class of systems arises naturally in the context of process control systems based on point-to-point wired links integrated with networked wired/wireless communication and utilizing multiple heterogeneous measurements (e.g., temperature and concentration). In this architecture, the local, pre-existing control system uses continuous sensing and actuation and an explicit control law (for example, the local controller may be a classical controller, like a proportional-integral-derivative controller, or a nonlinear controller designed via geometric or Lyapunov-based control methods for which an explicit formula for the calculation of the control action is available). In addition, a networked control system was designed using Lyapunov-based model predictive control to profit from both the continuous and the asynchronous measurements as well as from additional networked control actuators. The two-tier control architecture preserves the stability properties of the local control system while improving the closed-loop performance. Within process control, other important recent work on the subject of networked process control includes the development of a quasi-decentralized control framework for multi-unit plants that achieves the desired closed-loop objectives with minimal cross communication between the plant units (Sun and El-Farra, 2008).

The occurrence of faults in chemical processes poses a number of challenges in process monitoring and has been studied using both model-based and data-based approaches. Specifically, the problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of linear systems (Frank, 1990; Garcia and Frank, 1997); and recently, some existential results in the context of nonlinear systems have been derived (DePersis and Isidori, 2001; Saberi et al., 2000). The analytical (model-based) approach to fault detection relies on the use of fundamental models for the construction of residuals, that capture some measure of the difference between the normal and "faulty" dynamics, to achieve fault detection and isolation. Statistical and pattern recognition techniques for data analysis and interpretation (Raich and Çinar, 1996; Ohran et al., 2008), on the other hand, use past plant data to construct indicators that identify deviations from normal operation, and help in detecting faults. Recently, model-based monitoring systems which utilize asynchronous measurements from sensor networks have been developed (McFall et al., 2008).

This work focuses on the monitoring and reconfiguration of two-tier control systems applied to a general nonlinear processes in the presence of control actuator faults. Specifically, a general class of nonlinear process systems is first considered and is controlled by a two-tier control system integrating a local control system using continuous sensing/actuation with a networked control system using asynchronous sensing/actuation. To deal with control actuator faults that may occur in the closed-loop system and eliminate the ability of the two-tier control system to stabilize the process, a fault detection and isolation (FDI) and fault-tolerant control (FTC) system is designed which detects and isolates actuator faults and determines how to reconfigure the two-tier control system to handle the actuator faults and ensure closed-loop stability. The FDI/FTC system uses continuous and asynchronous measurements and deals with faults in the actuators of both the local and networked control systems. A detailed mathematical analysis is carried out to determine precise conditions under which the proposed FDI/FTC scheme guarantees closed-loop system stability. The method is demonstrated using a reactor-separator process consisting of two continuously stirred tank reactors and a flash tank separator with recycle stream.

2. Problem formulation and preliminaries

2.1. Class of nonlinear systems

In this work, we consider nonlinear process systems described by the following state-space model:

$$\dot{x}_s = f_s(x_s, x_a, u_s + \tilde{u}_s, u_a + \tilde{u}_a)$$

$$\dot{x}_a = f_a(x_s, x_a, u_s + \tilde{u}_s, u_a + \tilde{u}_a) \qquad (1)$$

where $x_s \in R^{n_s}$ denotes the set of state variables that are available continuously, $x_a \in R^{n_a}$ denotes the set of state variables that are sampled asynchronously, $u_s \in R^{m_s}$ denotes the inputs controlled by the local control system (see discussion in Section 2.4), $\tilde{u}_s \in R^{m_s}$ denotes the unknown fault vector for the inputs of the local control system with $u_s + \tilde{u}_s$ taking values in a non-empty convex set $U_1 \in R^{m_s}$ where $U_1 = \{u_s + \tilde{u}_s \in R_{m_s} : |u_s + \tilde{u}_s| \leq u_s^{\max}\}$,[1] $u_a \in R^{m_a}$ denotes the inputs of the networked control system and $\tilde{u}_a \in R^{m_s}$ denotes the unknown fault vector for the inputs of the networked control system with $u_a + \tilde{u}_a$ taking values in a non-empty convex set $U_2 \in R^{m_a}$ where $U_2 = \{u_a + \tilde{u}_a \in R_{m_a} : |u_a + \tilde{u}_a| \leq u_a^{\max}\}$. The entire state vector of the process is given by the vector $x = [x_s^T \; x_a^T]^T \in R^{n_s + n_a}$. Using this definition for x, the system of Eq. (1) can be written in the following equivalent compact form:

$$\dot{x} = f(x, u_s + \tilde{u}_s, u_a + \tilde{u}_a) \qquad (2)$$

We consider a different fault $\tilde{u}_j$, j=1,…,m_s+m_a, for each element of the vector $[\tilde{u}_s^T \; \tilde{u}_a^T]^T \in R^{m_s + m_a}$. Under fault-free operating conditions $\tilde{u}_s = 0$ and $\tilde{u}_a = 0$, and hence, $\tilde{u}_j = 0$ for all j=1,…,m_s+m_a. When fault j occurs, $\tilde{u}_j$ takes a non-zero value.

We assume that f is a locally Lipschitz vector function and that f(0,0,0)=0. This means that the origin is an equilibrium point for the fault-free system ($\tilde{u}_s = 0$ and $\tilde{u}_a = 0$ for all t) with u_s=0 and u_a=0.

Remark 1. In this work, we assume that the variables in the state vector x can be either available continuously (i.e., variables in x_s) or sampled asynchronously (i.e., variables in x_a). However, the results presented in this work can be extended to the case that some of the variables in the state vector are unmeasurable but observable by designing an observer to estimate the unmeasured state variables and designing the networked control system (see Liu et al., 2010, 2008) based on the measured and estimated states.

Remark 2. Note that in general an FDI system can only detect faults, declare fault alarms and wait for process operators to deal with the faults. However, when we focus on the faults that happen in a known set of inputs, we can design an FTC system to deal with such faults automatically and effectively. We note also that even though we assume that the set of faults is known, we do not limit its size, so we can consider any number of faults with respect to fault detection. Further, if fault isolation is not done, then the resulting reconfiguration (fault handling) strategy (assuming a worst case scenario with respect to the possible faults) would be very conservative.

Remark 3. The variable $\tilde{u}_j$ associated with the j th element in $[u_s^T, u_a^T]^T$ can be used to model different kinds of faults that may occur in an actuator. For example, $\tilde{u}_j$ can model a constant deviation of the control input from its calculated value u_j; or it can

[1] $|\cdot|$ denotes Euclidean norm of a vector.

be a function of the form $\tilde{u}_j = -u_j + c$ to model faults in an actuator that keep the output of the actuator constant.

2.2. Modeling of asynchronous measurements

The system of Eq. (1) is controlled using both continuous and asynchronous measurements. We assume that each state in x_s is sampled continuously (i.e., at intervals of fixed size $\Delta > 0$ where Δ is a sufficiently small positive number). Each state in x_a is sampled asynchronously and is only available at some time instants t_k where $\{t_{k \geq 0}\}$ is a random increasing sequence of times. A controller design that takes advantage of the asynchronous measurements must take into account that it will have to operate in open loop when asynchronous measurements are unavailable. This kind of systems are common in process control or networked control systems.

In order to maintain reasonable stability and system performance, we consider systems where there is a limit on the maximum period of time in which measurements of x_a are not available between two successive asynchronous measurements, i.e., $\max(t_{k+1}-t_k) \leq \Delta_{\max}$. This bound on the maximum period of time in which the loop is open has been also used in other works in the literature (Walsh et al., 2002; Nešić and Teel, 2004b; Mhaskar et al., 2007). Note that this bound is also required for the design of FDI systems which take advantage of asynchronous measurements to detect faults within a reasonable time frame.

2.3. Local control system

The continuous measurement $x_s(t)$ can be used to design a continuous output-feedback controller to stabilize the closed-loop system. We term the control system based only on the continuous measurements $x_s(t)$ as local control system. This control scheme does not use the asynchronous measurements $x_a(t)$. We assume that there exists a Lyapunov-based control law $u_s = h_1(x_s)$ which satisfies the input constraint on u_s for all x inside a given stability region and renders the origin $x=0$ of the fault-free system asymptotically stable with $u_a=0$. Using converse Lyapunov theorems (Massera, 1956; Lin et al., 1996), this assumption on h_1 implies that there exist functions $\alpha_i(\cdot), i=1,2,3,4$ of class $\mathcal{K}$[2] and a continuously differentiable Lyapunov function $V(x)$ for the fault-free system of Eq. (2) with $u_s = h_1(x_s)$ and $u_a=0$ that satisfy the following inequalities:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|)$$

$$\frac{\partial V(x)}{\partial x} f(x, h_1(x), 0) \leq -\alpha_3(|x|)$$

$$\left| \frac{\partial V(x)}{\partial x} \right| \leq \alpha_4(|x|)$$

$$h_1(x) \in U_1 \tag{3}$$

for all $x \in D \subseteq R^{n_x}$ where D is an open neighborhood of the origin. We denote the region Ω_ρ[3] $\subseteq D$ as the stability region of the closed-loop system under the control $u_1 = h_1(x_s)$ and $u_2=0$.

By continuity, the local Lipschitz property assumed for the vector field $f(x, u_1, u_2)$ and the fact that the manipulated inputs u_1 and u_2 are bounded in convex sets, there exists a positive constant M_1 such that

$$|f(x, u_s + \tilde{u}_s, u_a + \tilde{u}_a)| \leq M_1 \tag{4}$$

for all $x \in \Omega_\rho$, $u_s + \tilde{u}_s \in U_1$ and $u_a + \tilde{u}_a \in U_2$.

Remark 4. The assumption that there exists a controller $u_s = h_1(x_s)$ which can stabilize the closed-loop system with $u_a=0$ implies that, in principle, it is not necessary to use the extra input u_a in order to achieve closed-loop stability. However, u_a together with the asynchronous measurements can be used to improve the closed-loop performance achieved only by u_s and continuous measurements. See Section 2.4 for further discussions on the design of two-tier control architecture using continuous and asynchronous measurements. Moreover, the use of u_a brings the potential of FTC for the system without extra backup control configurations. Also see Section 2.5 for further discussion on this issue.

2.4. Two-tier control architecture

In the two-tier control architecture (Liu et al., 2010, 2008), the networked control system decides the trajectory of $u_a(t)$ between successive samples, i.e., for $t \in [t_k, t_{k+1})$ and the local control system decides $u_s(t)$ using the continuously available measurements. In order to take advantage of the model of the system and the asynchronous state measurements, model predictive control (MPC) is used to decide $u_a(t)$. In order to guarantee that the resulting closed-loop system is stable, a Lyapunov-based MPC (LMPC) which includes a contractive constraint is designed. The contractive constraint of the LMPC design is based on the local control system $h_1(x_s(t))$. The LMPC optimization problem is defined as follows:

$$\begin{aligned}
&\min_{u_a \in S(\Delta)} \int_0^{N\Delta} L(x^e(\tau), h_1(x_s^e(\tau)), u_a(\tau))\, d\tau \\
&\quad \dot{x}^e(\tau) = f(x^e(\tau), h_1(x_s^e(\tau)), u_a(\tau)) \\
&\quad \dot{x}^l(\tau) = f(x^l(\tau), h_1(x_s^l(\tau)), 0) \\
&\quad x^l(0) = x^e(0) = x(t_k) \\
&\quad u_a(\tau) \in U_2 \\
&V(x^e(\tau)) \leq V(x^l(\tau)), \quad \forall\ \tau \in [0, N\Delta]
\end{aligned} \tag{5}$$

where $x(t_k)$ is the state obtained from both the measurements of x_s and x_a, $x^e = [x_s^{eT} \quad x_a^{eT}]^T$ is the predicted trajectory of the fault-free system with the input trajectories $u_s(\tau) = h_1(x_s(\tau))$ and $u_a(\tau)$ computed by the LMPC, $x^l = [x_s^{lT} \quad x_a^{lT}]^T$ is the predicted trajectory of the fault-free system for the input trajectory $u_a(\tau) \equiv 0$ for all $\tau \in [0, N\Delta]$, $L(x, u_s, u_a)$ is a positive definite function of the state and the inputs that defines the cost, and N is the prediction horizon. The optimal solution to this optimization problem is denoted $u_a^*(\tau|t_k)$. This signal is defined for all $\tau > 0$ with $u_a^*(\tau|t_k) = 0$ for all $\tau > N\Delta$.

The control inputs of the two-tier control architecture based on the above LMPC of Eq. (5) corresponding to the measurements provided by $x(t)$ are defined as follows:

$$\begin{aligned}
&u_s^L(t|x) = h_1(x_s(t)), \quad \forall t \\
&u_a^L(t|x) = u_a^*(t-t_k|t_k), \quad \forall t \in [t_k, t_{k+1})
\end{aligned} \tag{6}$$

where $u_a^*(t-t_k|t_k)$ is the optimal solution of the LMPC problem at time step t_k with $x_e\ (t_k) = x(t_k)$. This implementation technique takes into account that the local control system uses the continuously available measurements, while the networked control system has to operate in open-loop between consecutive asynchronous measurements.

The closed-loop system of Eq. (2) under the two-tier control architecture with inputs defined by $u_s = u_s^L$ and $u_a = u_a^L$ maintains the same stability region Ω_ρ and asymptotic stability as the local Lyapunov-based control law h_1 (Liu et al., 2010, 2008). This

[2] A continuous function $\alpha : [0,a) \rightarrow [0,\infty)$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\alpha(0)=0$.

[3] We use Ω_r to denote the set $\Omega_r := \{x \in R^{n_x} | V(x) \leq r\}$.

property of the two-tier control architecture will be used in the proof of Theorem 1 in Section 3.

2.5. FTC considerations

In order to carry out FTC, there must be a backup control configuration for the system under consideration. The presence of the networked control action u_a and of the asynchronous measurements x_a brings extra control flexibility to the closed-loop system which can be used to carry out FTC. Specifically, we assume that the control input u_s can be decomposed into two subsets, that is $u_s=[u_{s1}^T \;\; u_{s2}^T]^T$ and there exists a Lyapunov-based control law $h_2(x)=[h_{21}(x)^T \;\; h_{22}(x)^T]^T$ such that when $u_{s1}=h_{21}(x)$ and $u_a=h_{22}(x)$ with $u_{s2}=0$ can asymptotically stabilize the closed-loop system under continuous state measurements satisfying the input constrains on u_s and u_a.

Using converse Lyapunov theorems, this assumption on h_2 implies that there exist functions $\alpha_i'(\cdot), i=1,2,3,4$ of class $\mathcal{K}$ and a continuously differentiable Lyapunov function $V_2(x)$ for the fault-free system of Eq. (2) with $u_{s1}=h_{21}(x)$, $u_a=h_{22}(x)$ and $u_{s2}=0$ that satisfy the following inequalities:

$$\alpha_1'(|x|) \le V_2(x) \le \alpha_2'(|x|)$$

$$\frac{\partial V(x)}{\partial x} f(x,[h_{21}(x)^T \;\; 0^T]^T, h_{22}(x)) \le -\alpha_3'(|x|)$$

$$\left|\frac{\partial V_2(x)}{\partial x}\right| \le \alpha_4'(|x|)$$

$$h_{21}(x) \in U_1, \quad h_{22}(x) \in U_2 \tag{7}$$

for all $x \in D_2 \subseteq R^{n_s+n_a}$ where D_2 is an open neighborhood of the origin. We denote $\Omega_{2,\gamma}$[4] $\subseteq D_2$ as the stability region of the closed-loop fault-free system with $u_s=[h_{21}(x)^T \;\; 0^T]^T$ and $u_a=h_{22}(x)$.

By continuity and the local Lipschitz property assumed for the vector field $f(x,u_s,u_a)$, the fact that the manipulated inputs u_1 and u_2 are bounded in convex sets and the continuous differentiable property of the Lyapunov function V_2, there exist positive constant M_2 and L_x such that

$$|f(x,u_s+\tilde{u}_s,u_a+\tilde{u}_a)| \le M_2 \tag{8}$$

$$\left|\frac{\partial V_2}{\partial x} f(x,u_s,u_a) - \frac{\partial V_2}{\partial x} f(x',u_s,u_a)\right| \le L_x|x-x'| \tag{9}$$

for all $x,x' \in \Omega_{2,\gamma}$, $u_s+\tilde{u}_s \in U_1$ and $u_a+\tilde{u}_a \in U_2$.

Note that, in general, the Lyapunov-based controller h_2 cannot be used as a backup control configuration for FTC because x is not available continuously. We propose to design an LMPC to decide u_a following the LMPC scheme proposed in Muñoz de la Peña and Christofides (2008), which takes into account asynchronous measurements explicitly, as follows:

$$\min_{u_a,u_{s1} \in S(\Delta)} \int_0^{N\Delta} L(x^{e2}(\tau),u_{s1}(\tau),u_a(\tau))\,d\tau \tag{10a}$$

$$\dot{x}^{e2}(\tau) = f(x^{e2}(\tau),[u_{s1}(\tau))^T 0^T]^T,u_a(\tau)) \tag{10b}$$

$$\dot{x}^{l2}(\tau) = f(x^{l2}(\tau),[h_{21}(x_s^{l2}(\tau))^T 0^T]^T,h_{22}(x^{l2}(j\Delta))), \quad \forall \tau \in [j\Delta,(j+1)\Delta) \tag{10c}$$

$$x^{l2}(0)=x^{e2}(0)=\hat{x}(t_k) \tag{10d}$$

$$u_a(\tau) \in U_2 \tag{10e}$$

$$u_{s1}(\tau) \in U_1 \tag{10f}$$

$$V_2(x^{e2}(\tau)) \le V_2(x^{l2}(\tau)), \quad \forall \tau \in [0,N\Delta] \tag{10g}$$

where $\hat{x}(t_k)$ is the state measurement obtained from x_s (t_k) and $x_a(t_k)$, $x^{e2}=[x_s^{e2T} \;\; x_a^{e2T}]^T$ is the predicted trajectory of the fault-free system with the input trajectories u_{s1} and u_a computed by the optimization of Eq. (10), $x^{l2}=[x_s^{l2T} \;\; x_a^{l2T}]^T$ is the predicted trajectory of the fault-free system with the input trajectories $u_s=[h_{21}(x)^T \;\; 0^T]^T$ and $u_a=h_{22}(x)$ applied in a sample-and-hold fashion with $j=0,\ldots,N-1$. The optimal solution to this optimization problem is denoted $u_a^{b,*}(\tau|t_k)$ and $u_{s1}^{b,*}(\tau|t_k)$. The signals are defined for $\tau \in [t_k,t_k+N\Delta]$.

The control inputs of the closed-loop system under the LMPC of Eq. (10) are defined as follows:

$$u_{s1}^b(t|x) = u_{s1}^{b,*}(t-t_k|t_k), \quad \forall t \in [t_k,t_{k+1})$$

$$u_{s2}^b(t|x) = 0, \quad \forall t$$

$$u_a^b(t|x) = u_a^{b,*}(t-t_k|t_k), \quad \forall t \in [t_k,t_{k+1}) \tag{11}$$

The closed-loop system of Eq. (2) under the backup control configuration with inputs defined by $u_{s1}=u_{s1}^b$, $u_{s2}=0$ and $u_a=u_a^b$ maintains the same stability region $\Omega_{2,\gamma}$ as h_2 and provides practical stability of the closed-loop system (Muñoz de la Peña and Christofides, 2008). These properties will be used in the proof of Theorem 2 in Section 3.

Remark 5. The assumption that there exists a Lyapunov-based control law h_2 that can stabilize the closed-loop system by manipulating u_{s1} and u_a implies that when there is a fault in the subset u_{s2} of u_s, we can switch off the actuators associated with u_{s2} and the remaining control actions (i.e., u_{s1} and u_a) can still be able to maintain the closed-loop stability. Further, we note that the proposed backup control configuration is one of the many possible options for FTC; however, under the proposed backup control configuration, stability of the closed-loop system can be proved (see Section 3 and Mhaskar et al., 2008, 2006, for further discussion on these issues).

2.6. FDI using asynchronous measurements

In the two-tier control architecture, full state information is not needed for all times, however, in order to design FDI filters, full state information, obtained via measurement and estimation, is needed. We will first design an observer to provide fault-free estimates for the asynchronous states at any time t. The asynchronous state observer takes the form

$$\dot{\hat{x}}_a = f_a(x_s,\hat{x}_a,u_s^L(\hat{x}),u_a^L(\hat{x})) \tag{12}$$

where $\hat{x}=[x_s^T \;\; \hat{x}_a^T]^T$ and, with a little abuse of notation, we have dropped the time index of the two-tier controller functions and denote $u_s^L(t|x), u_a^L(t|x)$ with $u_s^L(x)$, $u_a^L(x)$, respectively, in order to simplify the FDI definitions. Each time a new asynchronous measurement is received, the estimated states $\hat{x}_a$ are reset to match the true process state; that is, $\hat{x}_a(t_k)=x_a(t_k)$ for all t_k. Utilizing both continuous and asynchronous state measurements, a filter can be defined for each element in the input vector $[u_s^T \;\; u_a^T]^T$ as follows (McFall et al., 2008):

$$\dot{\tilde{x}}_k = f_k(\tilde{X}_k,u_s^L(\tilde{X}_k),u_a^L(\tilde{X}_k)) \tag{13}$$

where $\tilde{x}_k$ is the filter output for the kth state which is directly affected by one of the control inputs, f_k is the kth component of the vector function f and $\tilde{X}_k$ is a state trajectory obtained from the continuous measurements, the estimated and the corresponding filter output as follows $\tilde{X}_k=[\hat{x}_1,\ldots,\tilde{x}_k,\ldots,\hat{x}_{n_s+n_a}]^T$.

The FDI filters only initialized at $t=0$ such that $\tilde{x}_k(0)=\hat{x}_k(0)=x_k(0)$. For each state associated with a filter, the FDI residual can be defined as $r_k(t)=|\hat{x}_k(t)-\tilde{x}_k(t)|$

[4] We use $\Omega_{2,\gamma}$ to denote the set $\Omega_{2,\gamma} := \{x \in R^{n_s+n_a} : V_2(x) \le \gamma\}$.

(Mhaskar et al., 2008; McFall et al., 2008). The objective of the FDI scheme is to detect the fault when an actuator fault has occurred, and then identify which of the m_s+m_a different faults (i.e., $\tilde{u}_j$, $j=1,\ldots,m_s+m_a$) has occurred. Depending on the structure of the system, faults can be classified into different types. A fault $\tilde{u}_j$ is a type I fault if and only if

$$\frac{\partial f_k}{\partial \tilde{u}_j}=0, \quad \forall k \in \{n_s+1,\ldots,n_s+n_a\}$$

where $\tilde{u}_j$ is the j th element in the vector $[\tilde{u}_s^T \;\; \tilde{u}_a^T]^T$. A fault $\tilde{u}_j$ is a type II fault if there exists at least one $k \in \{n_s+1,\ldots,n_s+n_a\}$ such that

$$\frac{\partial f_k}{\partial \tilde{u}_j} \neq 0$$

Because the effects of a type I fault are measured continuously, only the filters of the states directly affected by the fault deviate from normal when a fault occurs. The rest of the filters continue to track the evolution of their corresponding states because the effect of the fault is known and accounted for. This allows for both fault detection and isolation in the case of a type I fault. However, a type II fault affects states that are measured asynchronously, and thus the effects of the fault are not immediately known and cannot be accounted for by the observer $\hat{x}_i$. The error introduced into $\hat{x}_i$ will then propagate into the FDI filters. In order to isolate the possible source of a fault and determine the type of the fault, it is necessary to wait until the residuals of each asynchronous state filters are updated after a new asynchronous measurement is received. In general, multiple residuals may be non-zero, making it impossible to isolate the specific fault.

In order to carry out FTC, all the possible faults should be isolable or at least be grouped by the subset of inputs they may affect. In the present work, we consider systems in which only a known set of inputs affect the asynchronous states, hence, when a type II fault is detected, the fault is known to belong to the set allowing for a FTC to be implemented. Specifically, we assume that for every element u_j, $j \in \{1,\ldots,m_s\}$ in the input vector u_s, the relative degree of x_k with respect to u_j is not equal to 1 for all $k \in \{n_s+1,\ldots,n_s+n_a\}$. This assumption implies that the elements in the local control system (i.e., u_s) only affect directly the continuously available state x_s and hence the local control system cannot generate type II faults. When a type I occurs it can be detected and isolated; on the other hand, when a type II fault occurs, although the exact actuator that has failed is unknown, it belongs to the networked control system. This property allows us to carry out FTC in the two-tier control architecture as discussed in Section 3, by shutting down the faulty actuator or subset of actuators and activating an alternative non-faulty control configuration.

3. Monitoring and FTC

In this section, we look at the monitoring and FTC of the closed-loop system under the two-tier control architecture. The structure of this integrated system is shown graphically in Fig. 1. In general, an FTC switching rule may be employed to orchestrate the reconfiguration of the control system in the event of control system failure. This rule determines which of the backup control loops can be activated, in the event that the main control loop fails, in order to preserve closed-loop stability.

As discussed in Section 2.6, type I faults in actuators can be detected and isolated for both local and networked control systems, and type II faults can be grouped to networked control system. When there is a fault in the networked control system actuators (i.e., fault in u_a), no matter what type the fault is, if the fault can be detected and isolated in a reasonable time frame, we can shut down the networked control system (i.e., let $u_a=0$) and leave the local control system in action alone. Note that in this switching rule, when there is a fault in u_a, the whole networked control system is shut down. This switching rule ensures the closed-loop stability because the local control system $u_s=h_1$ can stabilize the closed-loop system. Theorem 1 below describes the switching rules and the stability properties of the closed-loop system when there is an actuator fault in the networked control system actuators.

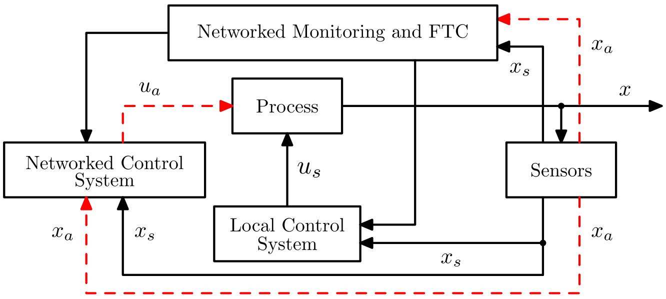

Fig. 1. Two-tier control strategy with integrated monitoring and FTC.

In general, when there is an actuator fault in the local control system, it is impossible to carry out FTC unless there is another backup control system. However, in the two-tier control architecture, because the networked control system brings extra control flexibility into the whole system, it is possible in some cases to carry out FTC without activating new control actuators. The assumption that there exists a Lyapunov-based control law h_2, manipulating u_{s1} and u_a, that asymptotically stabilizes the closed-loop system ensures that FTC can be carried out without other backup control systems when there are faults in the subset u_{s2} of the local control system. When there is a fault in u_{s2}, it must be a type I fault and can be detected and isolated. In this case, the proposed FTC strategy is to shut down the control actions of u_{s2} and reconfigure the rest of the local control system and the networked LMPC once the fault is isolated. Theorem 2 below states the switching rule and reconfiguration strategy for this case. However, when there is a fault in the subset u_{s1} of u_s, it is impossible to carry out FTC because of the lack of backup control configurations within the two-tier control architecture and class of nonlinear systems considered.

The proposed FTC switching rules for the system of Eq. (2) within the two-tier control architecture are summarized as follows:

1. When a fault in u_a is detected at t_f^a, the proposed FTC switching rule is:

$$u_a(t)=\begin{cases} u_a^L(x), & t<t_f^a \\ 0, & t\geq t_f^a \end{cases}$$

$$u_s(t)=h_1(x_s), \quad \forall t \tag{14}$$

2. When a fault in u_{s2} is detected at t_f^s, the proposed FTC switching rule is:

$$u_a(t)=\begin{cases} u_a^L(x), & t<t_f^s \\ u_a^b(x), & t\geq t_f^s \end{cases}$$

$$u_s(t)=\begin{cases} h_1(x_s), & t<t_f^s \\ \begin{bmatrix} u_{s1}^b(x) \\ 0 \end{bmatrix}, & t\geq t_f^s \end{cases} \tag{15}$$

In what follows, we give sufficient conditions under which the above switching rules of Eqs. (14) and (15) guarantee stability of the closed-loop system. The sufficient conditions are provided in Theorems 1 and 2. In order to state Theorems 1 and 2, we need the following propositions.

Proposition 1 (*c.f.* Liu et al., 2010). *Consider the Lyapunov functions* $V(\cdot)$, $V_2(\cdot)$ *of system* (2). *There exists quadratic functions* $f_V(\cdot)$ *and* $f_{V_2}(\cdot)$ *such that*

$$V(x) \le V(x') + f_V(|x - x'|)$$

$$V_2(x'') \le V_2(x''') + f_{V_2}(|x'' - x'''|) \tag{16}$$

for all $x, x' \in \Omega_\rho$ *and* $x'', x'' \in \Omega_{2,\gamma}$.

This proposition bounds the difference between the magnitudes of the Lyapunov functions $V(x)$ and $V_2(x)$ of two different states in the Ω_ρ and $\Omega_{2,\gamma}$, respectively.

Proposition 2 (*c.f.* Muñoz de la Peña and Christofides, 2008). *Consider the sampled trajectory* $\hat{x}$ *of the fault-free system of Eq.* (2) *in closed-loop with the Lyapunov-based control law* h_2 *applied in a sample-and-hold fashion. Let* $\Delta, \varepsilon_s > 0$ *and* $\gamma > \gamma_s > 0$ *satisfy*

$$-\alpha_3'(\alpha_2'^{-1}(\gamma_s)) + \alpha_4'(\alpha_1'^{-1}(\gamma))L_x M_2 \Delta \le -\varepsilon_s/\Delta \tag{17}$$

Then, if $\gamma_{\min} < \gamma$ *where*

$$\gamma_{\min} = \max\{V_2(\hat{x}(t+\Delta)) : V_2(\hat{x}(t)) \le \gamma_s\} \tag{18}$$

and $\hat{x}(0) \in \Omega_{2,\gamma}$, *the following inequality holds*:

$$V_2(\hat{x}(k\Delta)) \le \max\{V_2(\hat{x}(0)) - k\varepsilon_s, \gamma_{\min}\} \tag{19}$$

Proposition 2 ensures that if the fault-free system of Eq. (2) under the control law $h_2(x)$ implemented in a sample-and-hold fashion starts in $\Omega_{2,\gamma}$, then it is ultimately bounded in $\Omega_{2,\gamma_{\min}}$.

Theorem 1. *Consider system* (2) *in closed-loop under the two-tier control architecture of Eq.* (6). *If* $0 < \rho_0 < \rho$ *and* $x(t_0) \in \Omega_{\rho_0}$ *where* t_0 *is the initial time, and a fault in* u_a *is detected at time* t_f^a, *if the following condition is satisfied*:

$$f_V(M_1 \Delta_{\max}) \le \rho - \rho_0 \tag{20}$$

then the switching rule of Eq. (14) *guarantees that the state of the closed-loop system* $x(t)$ *is maintained in* Ω_ρ *for all* t *and* $x(t)$ *converges to the origin asymptotically after* t_f^a.

Proof. A fault can only be detected when a new asynchronous measurement is received after the fault occurred. In order to prove the closed-loop stability, we will prove that $V(x)$ is always bounded in the stability region Ω_ρ of h_1 when the condition of Eq. (20) is satisfied. Assume an asynchronous measurement is received at t_k, a fault in u_a occurs at t_f and is detected and isolated when a new asynchronous measurement is received at t_f^a, which implies $t_k \le t_f \le t_f^a$.

According to the switching rule (14), from t_0 to t_f, the closed-loop system (2) is controlled under the two-tier control architecture based on h_1. Following from the stability property of the two-tier control architecture (Liu et al., 2010), if $x(t_0) \in \Omega_{\rho_0}$, the state of the closed-loop system will converge to the origin asymptotically which implies the state of the closed-loop system at t_f will be still maintained in Ω_{ρ_0}, that is, $x(t_f) \in \Omega_{\rho_0}$.

From Eq. (4), the following inequality can be written:

$$|\dot{x}| = |f(x, h_1, u_a + \tilde{u}_a)| \le M_1.$$

From this inequality, we can get the following bound on the difference between $x(t_f)$ and $x(t_f^a)$:

$$|x(t_f^a) - x(t_f)| \le M_1(t_f^a - t_f) \tag{21}$$

By Proposition 1 and the inequality of Eq. (21), we know that

$$V(x(t_f^a)) \le V(x(t_f)) + f_V(M_1(t_f^a - t_f)) \tag{22}$$

After applying the switching rule (14) at t_f^a, the closed-loop system will be controlled by the local Lyapunov-based control law h_1. In order to maintain the stability of the closed-loop system, $x(t_f^a)$ must be inside the stability region of h_1, that is, $x(t_f^a) \in \Omega_\rho$. From the inequality of Eq. (22) and the above reasoning, the following inequality must be satisfied:

$$V(x(t_f)) + f_V(M_1(t_f^a - t_f)) \le \rho$$

Moreover, this inequality needs to hold for the worst case, that is, $V(x(t_f)) = \rho_0$ and $t_f^a - t_f = \Delta_{\max}$, which leads to the following inequality:

$$f_V(M_1 \Delta_{\max}) \le \rho - \rho_0$$

which is the condition of Eq. (20).

After t_f^a, the closed-loop system will be controlled under the local control system h_1. This implies that $x(t)$ will converge to the origin asymptotically after t_f^a because h_1 renders the closed-loop system asymptotically stable. This proves that $x(t)$ of the closed-loop system is always maintained in Ω_ρ and converges asymptotically to the origin after t_f^a under the switching rule of Eq. (14). □

Theorem 1 above gives sufficient conditions under which the switching rule of Eq. (14) guarantees the stability of the closed-loop system in the presence of an actuator fault in u_a. Below Theorem 2 gives sufficient conditions under which the switching rule of Eq. (15) guarantees the stability of the closed-loop system in the presence of an actuator fault in u_{s2}.

Theorem 2. *Consider system* (2) *in closed-loop under the two-tier control architecture of Eq.* (6). *Let* $\Delta, \varepsilon_s > 0$ *and* $\gamma > \gamma_s > 0$ *satisfy the condition of Eq.* (17). *If* $N\Delta \ge \Delta_{\max}$, $x(t_0) \in \Omega_{\rho_0}$ *where* t_0 *is the initial time and a fault in* $u_{s\ 2}$ *is detected and isolated at time* t_f^s, *and if* $x(t_f^s) \in \Omega_{2,\gamma}$, *then the switching rule of Eq.* (15) *guarantees that the state of the closed-loop system* $x(t)$ *is ultimately bounded in* $\Omega_{2,\gamma_{\min}}$.

Proof. Assume an asynchronous measurement is received at t_k, a fault in $u_{s\ 2}$ occurs at t_f and is detected and isolated when a new asynchronous measurement is received at t_f^s, which implies $t_k \le t_f \le t_f^s$. According to the switching rule of Eq. (15), from t_0 to t_f, the closed-loop system of Eq. (2) is controlled under the two-tier control architecture with u_s=$h_1(x_s)$ and u_a=u_a^L. Following from the asymptotic stability property of the two-tier control architecture of Eq. (6), if $x(t_0) \in \Omega_{\rho_0}$, the state of the closed-loop system will converge to the origin asymptotically.

According to the switching rule of Eq. (15), after t_f^s, the closed-loop system will be controlled with u_s=$[u_{s1}^{bT} \quad 0^T]^T$ and u_a=u_a^b. If $N\Delta \ge \Delta_{\max}$ and $x(t_f^s) \in \Omega_{2,\gamma}$, following the results in Muñoz de la Peña and Christofides (2008), we can prove that the closed-loop system state $x(t)$ is ultimately bounded in $\Omega_{2,\gamma_{\min}}$. This proves Theorem 2. □

Remark 6. The switching rule of Eq. (15) implies that when there is a fault in u_{s2}: (a) the networked control system needs to be reconfigured following the LMPC of Eq. (10), and (b) the reconfigured networked control system needs to determine both u_a and u_{s1}. In this case, only the state measurements obtained from x_s and x_a at time instants t_k are utilized. If h_{21} only depends on the continuously-measured state x_s, (i.e., $h_{21}(x)$=$h_{21}(x_s)$), in order to take advantage of all the available measurements, we can use h_{21} to determine u_{s1} and use the networked LMPC of Eq. (10) to optimize u_a; this means that in the optimization problem of

LMPC of Eq. (10), we let $u_{s1}=h_{21}$. This point will be demonstrated in the process example of Section 4. Finally, we note that when a fault in u_{s1} is detected at t_f^s, there is no guarantee that closed-loop system stability can be maintained via FTC.

4. Application to a reactor-separator process

4.1. Process description and modeling

The process considered in this study is a three vessel, reactor-separator system consisting of two continuously stirred tank reactors (CSTRs) and a flash tank separator (see Fig. 2). A feed stream to the first CSTR contains the reactant, *A*, which is converted into the desired product, *B*. Species *A* can also react into an undesired side-product, *C*. The solvent does not react and is labeled as *D*. The effluent of the first CSTR along with additional fresh feed makes up the inlet to the second CSTR. The reactions $A \rightarrow B$ and $A \rightarrow C$ (referred to as 1 and 2, respectively) take place in the two CSTRs in series before the effluent from CSTR 2 is fed to a flash tank. The overhead vapor from the flash tank is condensed and recycled to the first CSTR, and the bottom product stream is removed. All three vessels are assumed to have static holdup. The dynamic equations describing the behavior of the system, obtained through material and energy balances under standard modeling assumptions, are given below:

$$\frac{dT_1}{dt} = \frac{F_{10}}{V_1}(T_{10}-T_1)+\frac{F_r}{V_1}(T_3-T_1)+\frac{-\Delta H_1}{\rho Cp}k_1e^{-E_1/RT_1}C_{A1} + \frac{-\Delta H_2}{\rho Cp}k_2e^{-E_2/RT_1}C_{A1}+\frac{Q_1}{\rho C_pV_1} \tag{23a}$$

$$\frac{dC_{A1}}{dt} = \frac{F_{10}}{V_1}(C_{A10}-C_{A1})+\frac{F_r}{V_1}(C_{Ar}-C_{A1})-k_1e^{-E_1/RT_1}C_{A1}-k_2e^{-E_2/RT_1}C_{A1} \tag{23b}$$

$$\frac{dC_{B1}}{dt} = \frac{-F_{10}}{V_1}C_{B1}+\frac{F_r}{V_1}(C_{Br}-C_{B1})+k_1e^{-E_1/RT_1}C_{A1} \tag{23c}$$

$$\frac{dC_{C1}}{dt} = \frac{-F_{10}}{V_1}C_{C1}+\frac{F_r}{V_1}(C_{Cr}-C_{C1})+k_2e^{-E_2/RT_1}C_{A1} \tag{23d}$$

$$\frac{dT_2}{dt} = \frac{F_1}{V_2}(T_1-T_2)+\frac{(F_{20}+\Delta F_{20})}{V_2}(T_{20}-T_2)+\frac{-\Delta H_1}{\rho Cp}k_1e^{-E_1/RT_2}C_{A2} + \frac{-\Delta H_2}{\rho Cp}k_2e^{-E_2/RT_2}C_{A2}+\frac{Q_2}{\rho C_pV_2} \tag{23e}$$

$$\frac{dC_{A2}}{dt} = \frac{F_1}{V_2}(C_{A1}-C_{A2})+\frac{(F_{20}+\Delta F_{20})}{V_2}(C_{A20}-C_{A2}) -k_1e^{-E_1/RT_2}C_{A2}-k_2e^{-E_2/RT_2}C_{A2} \tag{23f}$$

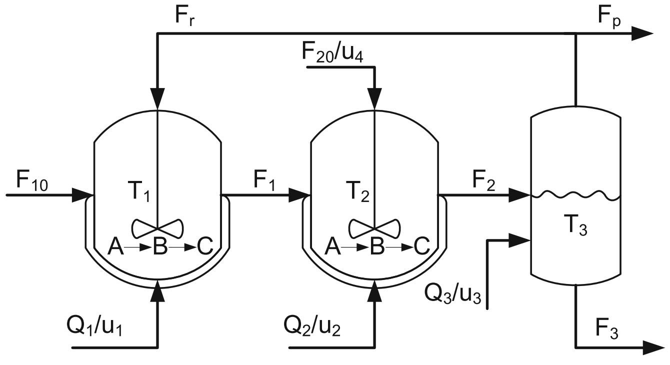

Fig. 2. Two CSTRs and a flash tank with recycle stream.

$$\frac{dC_{B2}}{dt} = \frac{F_1}{V_2}(C_{B1}-C_{B2})-\frac{(F_{20}+\Delta F_{20})}{V_2}C_{B2}+k_1e^{-E_1/RT_2}C_{A2} \tag{23g}$$

$$\frac{dC_{C2}}{dt} = \frac{F_1}{V_2}(C_{C1}-C_{C2})-\frac{(F_{20}+\Delta F_{20})}{V_2}C_{C2}+k_2e^{-E_2/RT_2}C_{A2} \tag{23h}$$

$$\frac{dT_3}{dt} = \frac{F_2}{V_3}(T_2-T_3)-\frac{H_{vap}F_r}{\rho CpV_3}+\frac{Q_3}{\rho C_pV_3} \tag{23i}$$

$$\frac{dC_{A3}}{dt} = \frac{F_2}{V_3}(C_{A2}-C_{A3})-\frac{F_r}{V_3}(C_{Ar}-C_{A3}) \tag{23j}$$

$$\frac{dC_{B3}}{dt} = \frac{F_2}{V_3}(C_{B2}-C_{B3})-\frac{F_r}{V_3}(C_{Br}-C_{B3}) \tag{23k}$$

$$\frac{dC_{C3}}{dt} = \frac{F_2}{V_3}(C_{C2}-C_{C3})-\frac{F_r}{V_3}(C_{Cr}-C_{C3}) \tag{23l}$$

The definitions for the variables used in Eq. (23) can be found in Table 1, with the parameter values given in Table 2. Each of the tanks has an external heat input.

The model of the flash tank separator operates under the assumption that the relative volatility for each of the species remains constant within the operating temperature range of the flash tank. This assumption allows calculating the mass fractions in the overhead based upon the mass fractions in the liquid portion of the vessel. It has also been assumed that there is a negligible amount of reaction taking place in the separator. The following algebraic equations model the composition of the overhead stream relative to the composition of the liquid holdup

Table 1
Process variables.

C_{A1}, C_{A2}, C_{A3}	Concentration of *A* in vessels 1, 2, 3
C_{B1}, C_{B2}, C_{B3}	Concentration of *B* in vessels 1, 2, 3
C_{C1}, C_{C2}, C_{C3}	Concentration of *C* in vessels 1, 2, 3
C_{Ar}, C_{Br}, C_{Cr}	Concentration of *A*, *B*, *C* in the recycle
T_1, T_2, T_3	Temperatures in vessels 1, 2, 3
T_{10}, T_{20}	Feed stream temp. to vessels 1, 2
F_1, F_2, F_3	Effluent flow rate from vessels 1, 2, 3
F_{10}, F_{20}	Feed stream flow rate to vessels 1, 2
C_{A10}, C_{A20}	Concentration of *A* in the feed stream to vessels 1, 2
F_r	Recycle flow rate
V_1, V_2, V_3	Volume of vessels 1, 2, 3
u_1, u_2, u_3, u_4	Manipulated inputs
E_1, E_2	Activation energy for reactions 1, 2
k_1, k_2	Pre-exponential values for reactions 1, 2
ΔH_1, ΔH_2	Heats of reaction for reactions 1, 2
H_{vap}	Heat of vaporization
α_A, α_B, α_C, α_D	Relative volatilities of *A*, *B*, *C*, *D*
MW_A, MW_B, MW_C	Molecular weights of *A*, *B*, and *C*
C_p, R	Heat capacity and gas constant

Table 2
Parameter values.

T_{10}=300, T_{20}= 300	K
F_{10} = 5, F_{20}=5, F_r = 1.9	m^3/h
C_{A10} = 4, C_{A20}=3	kmol/m^3
V_1=1.0, V_2=0.5, V_3=1.0	m^3
E_1=5*E*4, E_2 = 5.5*E*4	kJ/kmol
k_1=3*E*6, k_2= 3*E*6	1/h
$\Delta H_1 = -5E4$, $\Delta H_2 = -5.3 \times 10^4$	kJ/kmol
H_{vap}=5	kJ/kmol
C_p = 0.231	kJ/kg K
R = 8.314	kJ/kmol K
$\rho = 1000$	kg/m^3
$\alpha_A = 2$, $\alpha_B = 1$, $\alpha_C = 1.5$, $\alpha_D = 3$	Unitless
MW_A = 50, MW_B = 50, MW_C = 50	kg/kmol

in the flash tank:

$$C_{Ar}=\frac{\alpha_A C_{A3}}{K},\quad C_{Br}=\frac{\alpha_B C_{B3}}{K},\quad C_{Cr}=\frac{\alpha_C C_{C3}}{K}$$

$$K=\alpha_A C_{A3}\frac{MW_A}{\rho}+\alpha_B C_{B3}\frac{MW_B}{\rho}+\alpha_C C_{C3}\frac{MW_C}{\rho}+\alpha_D x_D \rho \tag{24}$$

where x_D is the mass fraction of the solvent in the flash tank liquid holdup and is found from a mass balance.

The system of Eq. (23) is modeled with sensor measurement noise and Gaussian process noise. The sensor measurement noise is generated using a zero-mean normal distribution with standard deviation 10^{-1} for the temperature states and 10^{-2} for the nine concentration states. Noise is also applied to each measurement with a frequency of $\Delta_m=0.001$ h. The process noise is generated similarly, with a zero-mean normal distribution and with the same standard deviation values. Process noise is added to the right-hand side of the ODEs in the system of Eq. (23) and changes with a frequency of $\Delta_w=0.001$ h.

We assume that the measurements of temperatures T_1, T_2 and T_3 are available continuously and the measurements of the species concentration C_{Ai}, C_{Bi} and C_{Ci}, i=1,2,3 are available asynchronously at time instants t_k with an average frequency of W=10 measurements per hour. The measurement times $\{t_{k\geq 0}\}$ are modeled as a Poisson process with the time between measurements $\Delta_a=\min\{-\log(\xi/W),\Delta_{\max}\}$ where ξ is a uniformly distributed random number between 0 and 1 and $\Delta_{\max}=0.05$ h which is the maximum time interval between two successive asynchronous species concentration measurements.

The manipulated inputs to the process are the heat inputs to the three vessels Q_1, Q_2 and Q_3 and the change of the inlet flow rate ΔF_{20} to the second tank. The process has one unstable and two stable steady states and the operating set point is the unstable steady state:

$$x_s=[369.5\ \ 3.318\ \ 0.172\ \ 0.042\ \ 435.3\ \ 2.751\ \ 0.446\ \ 0.111\ \ 435.3\ \ 2.882\ \ 0.497\ \ 0.120]^T \tag{25}$$

The process of Eq. (23) belongs to the class of nonlinear systems described by Eq. (2) where the deviation of the actual state from the steady-state x is the state, u_s=$[u_1\ \ u_3\ \ u_2]^T$=$[Q_1\ \ Q_3\ \ Q_2]^T$ and $u_a=u_4=\Delta F_{20}$ are the manipulated inputs which are subject to the constraints $|u_i|\leq 10^6$ kJ/h ($i=1,2,3$) and $|u_4|\leq 4.998\ \mathrm{m}^3/\mathrm{h}$.

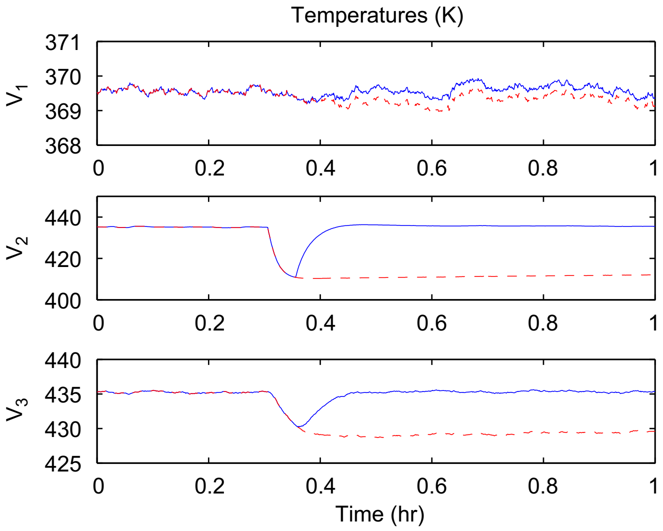

Fig. 3. Temperature trajectories in each vessel with a fault in the networked control actuator (u_4 = 4.998 m^3/h) at t = 0.3 h. Dashed lines represent trajectories without FTC and solid lines represent trajectories with FTC.

The local control system consists of the three heat input actuators operating under three PI controllers that control the three heat input actuators (i.e., h_1=$[u_1\ \ u_2\ \ u_3]^T$) with proportional gains K_{p1}=K_{p2}=K_{p3}=8000 and integral times $\tau_{I1}=\tau_{I2}=\tau_{I3}=10$, respectively. These PI controllers can asymptotically stabilize the closed-loop process at the desired steady-state. A quadratic Lyapunov function $V(x)$=x^TPx with P=$diag[10\ \ 10^3\ \ 10^3\ \ 10^3\ \ 10\ \ 10^3\ \ 10^3\ \ 10^3\ \ 10\ \ 10^3\ \ 10^3\ \ 10^3]$ is used. Based on the PI controllers and the Lyapunov function $V(x)$, an LMPC of the form given in Eq. (5) is designed as the networked control system to manipulate the change of the inlet flow rate to the second tank (i.e., u_4) taking advantage of the asynchronous concentration measurements to improve the closed-loop performance. The cost function $L(x, u_s, u_a)$ used in the networked LMPC is quadratic and takes the form $L(x,u_s,u_a)$=$x^T\,Q_c\,x+R_c\,u_a^2$, where Q_c=P, R_c=10. The horizon for the optimization problem is N=5 with $\Delta=0.01$ h so that $N\Delta\geq\Delta_{\max}$. At each asynchronous measurement time, the networked LMPC optimization problem is solved again and implemented over the length of the horizon or until a new asynchronous concentration measurement becomes available.

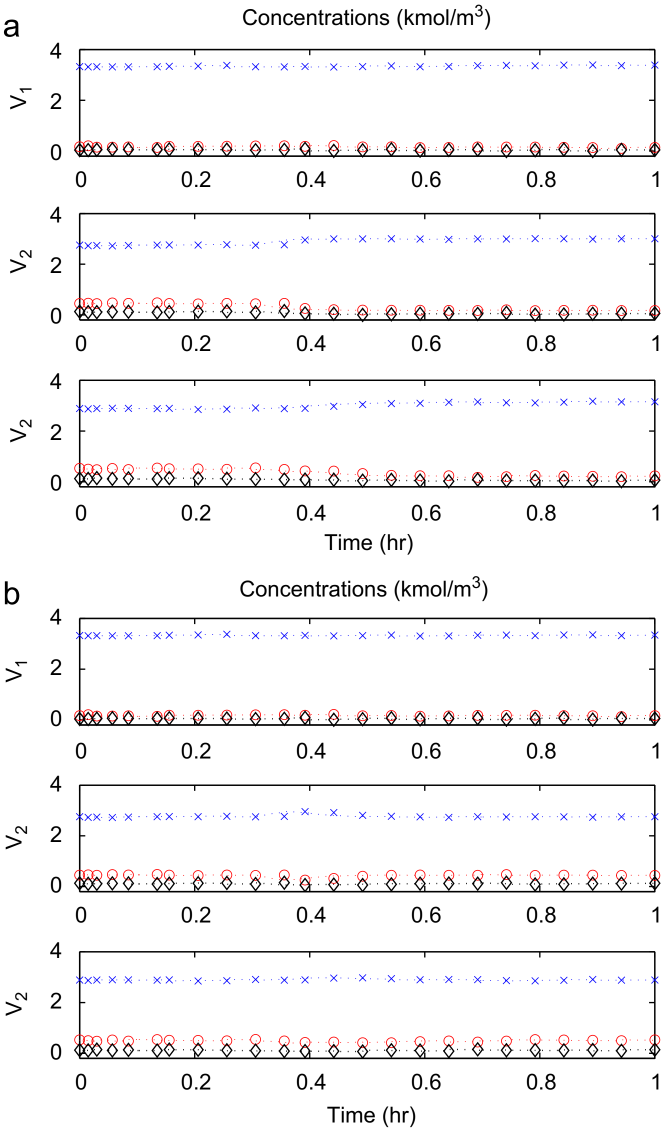

Fig. 4. Asynchronous concentration measurements (C_A= ×, C_B = o, $C_C=\diamond$) in each vessel (V 1, V 2, V 3) with a fault in the networked control actuator (u_4 = 4.998 m^3/h) at t = 0.3 h. Dotted lines represent observer trajectories. (a) No FTC is implemented; (b) FTC is implemented.

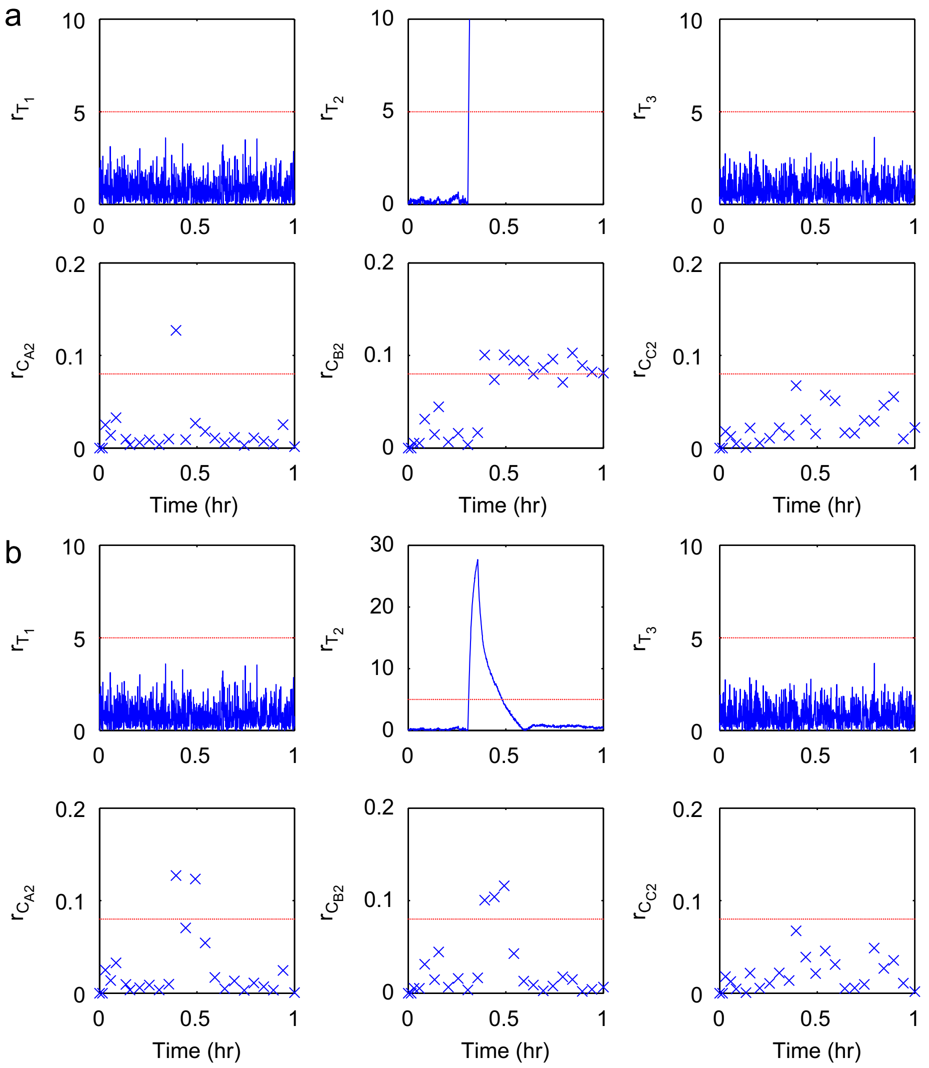

Fig. 5. FDI filter residuals for temperatures (T_1, T_2, T_3) and concentration (C_{A2}, C_{B2}, C_{C2}) with a fault in the networked control actuator (u_4 = 4.998 m^3/h) at t = 0.3 h. (a) No FTC is implemented; (b) FTC is implemented.

In order to perform FDI for the reactor-separator system, we construct the asynchronous state observers of the form of Eq. (12), where $\hat{C}_{Ai}$, $\hat{C}_{Bi}$, and $\hat{C}_{Ci}, i=1,2,3$ are the asynchronous observer states. Each observer state is reset to its actual value each time a new asynchronous measurement becomes available at time t_k. The observer states provide estimates for the concentration states between measurements allowing the computation of FDI filter residuals.

Actuator fault-detection and isolation for the system in closed-loop with the primary configuration is accomplished by generating FDI filters for the four manipulated inputs as in Eq. (13). In addition, the FDI residuals take the following form:

$$r_{T_i,\max} = |T_i(t) - \tilde{T}_i(t)|, \quad i=1,2,3$$

$$r_{C_{i2},\max} = |\hat{C}_{i2}(t_k) - \tilde{C}_{i2}(t_k)|, \quad i=A,B,C \tag{26}$$

Due to sensor measurement and process noise, the residuals will be non-zero even without a fault. This necessitates the use of fault detection thresholds so that a fault is declared only when a residual exceeds a specific threshold value, $r_{i,\max}$. This threshold value is chosen to avoid false alarms due to process and sensor measurement noise, but should still be sensitive enough to detect faults in a timely manner so that effective FTC can be performed. The threshold values used for each residual in the numerical simulations are as follows:

$$r_{T_i} = 5K, \quad i=1,2,3$$

$$r_{C_{i2}} = 0.08\,\text{kmol/m}^3, \quad i=A,B,C$$

Note that because only the networked control system affects the asynchronously sampled states, when a concentration residual exceeds its corresponding threshold, a fault in the networked control system can be declared.

With respect to the decomposition of the input space for FTC purposes, the inputs of the process u_s can be decomposed into $u_{s1}=[u_1 \quad u_3]^T$ and $u_{s2}=u_2$. Furthermore, it was verified that for specific process under consideration there exists a controller design $h_2=[u_1 \quad u_3 \quad u_4]^T$ with u_1, u_3 controlled by the same PI controllers introduced before in this section and u_4 controlled by another PI controller based on the measurement of T_2 with the proportional gain $K_{p4}=-0.3$ and the integral time $\tau_{I4}=10$, that can stabilize the process at the operating steady-state. The control design h_2 can also stabilize the closed-loop system asymptotically with continuous measurements and u_2=0. Based on this h_2-controller, a new LMPC can be designed and used for FTC purposes following Eq. (10) with $u_{s\ 1}$ determined by the PI controllers, which means that only u_4 is optimized by this LMPC (see also Remark 6), to stabilize the process. In the design of this LMPC, the same Lyapunov function is used, that is, $V_2=V$.

4.2. FTC for networked control system

In this subsection, we consider FTC for the process when there is a fault in the actuator associated with u_4. Specifically, we consider a fault which renders the actuator keeps ΔF_{20} at the maximum (i.e., $u_4=4.998\,\mathrm{m}^3/\mathrm{h}$). Because ΔF_{20} affects both asynchronously and continuously measured state directly, a fault in ΔF_{20} can be declared when two or more of the residuals in r_{T_2}, $r_{C_{A2}}$, $r_{C_{B2}}$ and $r_{C_{C2}}$ are greater than the corresponding thresholds and r_{T_1}, r_{T_3} are found to be less than their respective thresholds at an asynchronous sampling time t_k.

We first simulate the process with the fault without implementing FTC. The fault is introduced at time $t=0.3$ h. The state trajectories of the process are shown in Fig. 3 (dashed lines) and Fig. 4(a) when no FTC is implemented. From Figs. 3 and 4(a), we see that without implementing FTC, the state of the process cannot be maintained at the desired steady-state. The residuals in Fig. 5(a) shows that the fault is detected at $t=0.310$ h when $r_{T2} > r_{T2,\max}$. It can then be isolated when the next asynchronous measurement is received at $t_k=0.356$ h and $r_{T2} > r_{T2,\max}$ and $r_{C_{B2}} > r_{C_{B2,\max}}$.

In contrast to the above scenario, we run the same simulation again, but upon isolation of the fault we carry out the switching rule of Eq. (14) and the networked control system is switched off. The state trajectories of the process are shown in Fig. 3 (solid lines) and Fig. 4(b). From Figs. 3 and 4(b), we see that the state trajectories show the initial deviation from steady-state followed by a return to the steady-state as the fault is isolated at $t=0.356$ h and the networked control system is switched off (see Fig. 5(b) for the corresponding residuals).

4.3. FTC for local control system

In this subsection, we consider FTC for the process when there is a fault in the heat input actuator to vessel 2 which renders $Q_2=0$ (i.e., $u_2=0$ kJ/h). Since Q_2 only affects the continuous available measurement T_2 directly, a fault in Q_2 can be claimed when $r_{T2} > r_{T2,\max}$ and the other residuals are found to be less than their respective thresholds at an asynchronous sampling time t_k.

We first simulate the process with the failure without implementing FTC nor updating the LMPC in the networked control system. The fault is also introduced at time $t=0.3$ h. The state trajectories of the process are shown in Figs. 6 (dashed lines) and 7(a). From Figs. 6 and 7(a), we see that without implementing FTC, the state of the process cannot be maintained at the required steady-state. The residuals in Fig. 8(a) show that the fault is detected at $t=0.432$ h when $r_{T2} > r_{T2,\max}$. It can then be isolated when the next asynchronous measurement is received at $t_k=0.442$ h.

In contrast to the above scenario, we carry out the same simulation again, but upon isolation of the fault we implement the switching rule of Eq. (15) and reconfigure the networked control system to reflect the failed actuator. In this case, despite the failed actuator, the networked control system is able to stabilize the process after reconfiguration. Figs. 6 (solid lines) and 7(b) show the temperature and concentration profiles for the process. The temperature trajectories show the initial deviation from the steady-state as the fault is first introduced followed by a

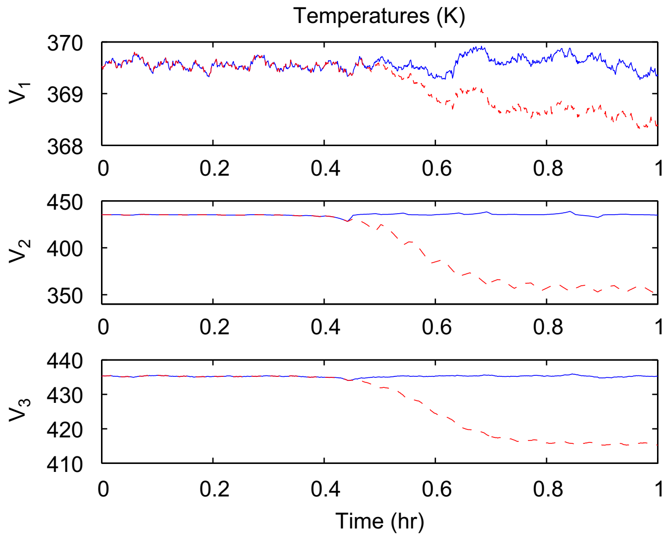

Fig. 6. Temperature trajectories in each vessel with an actuator failure in the heat input to vessel 2 at t = 0.3 h. Dashed lines represent trajectories without FTC and solid lines represent trajectories with FTC.

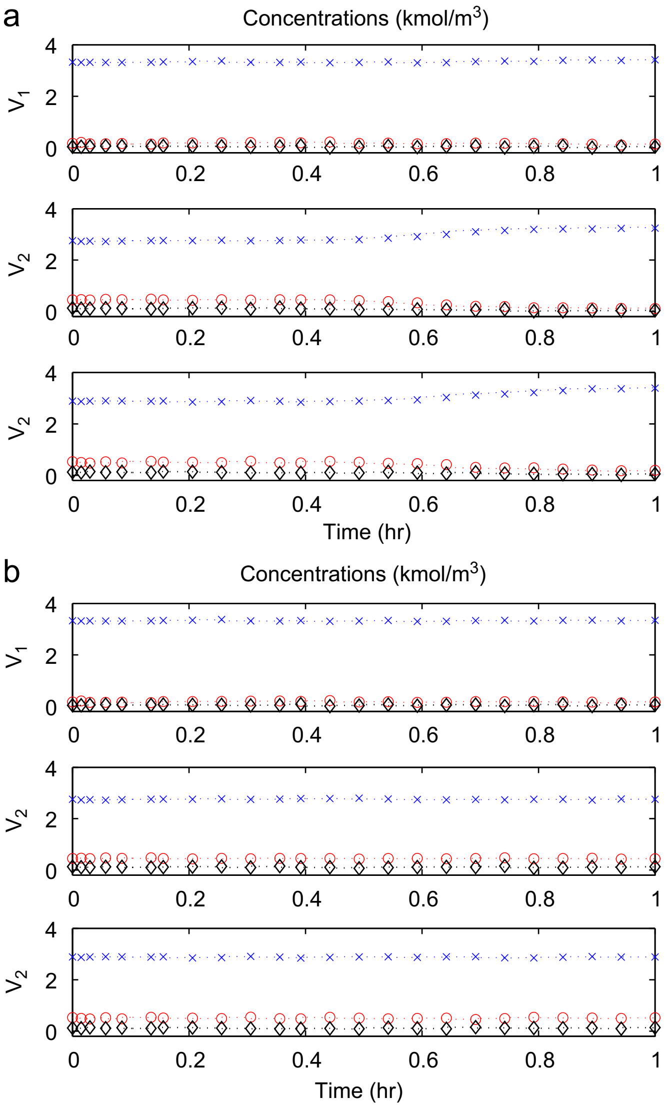

Fig. 7. Asynchronous concentration measurements ($C_A=\times$, C_B=o, $C_C=\diamond$) in each vessel ($V\,1$, $V\,2$, $V\,3$) with an actuator failure in the heat input to vessel 2 (u_2=0) at t=0.3 h. Dotted lines represent observer trajectories. (a) No FTC is implemented; (b) FTC is implemented.

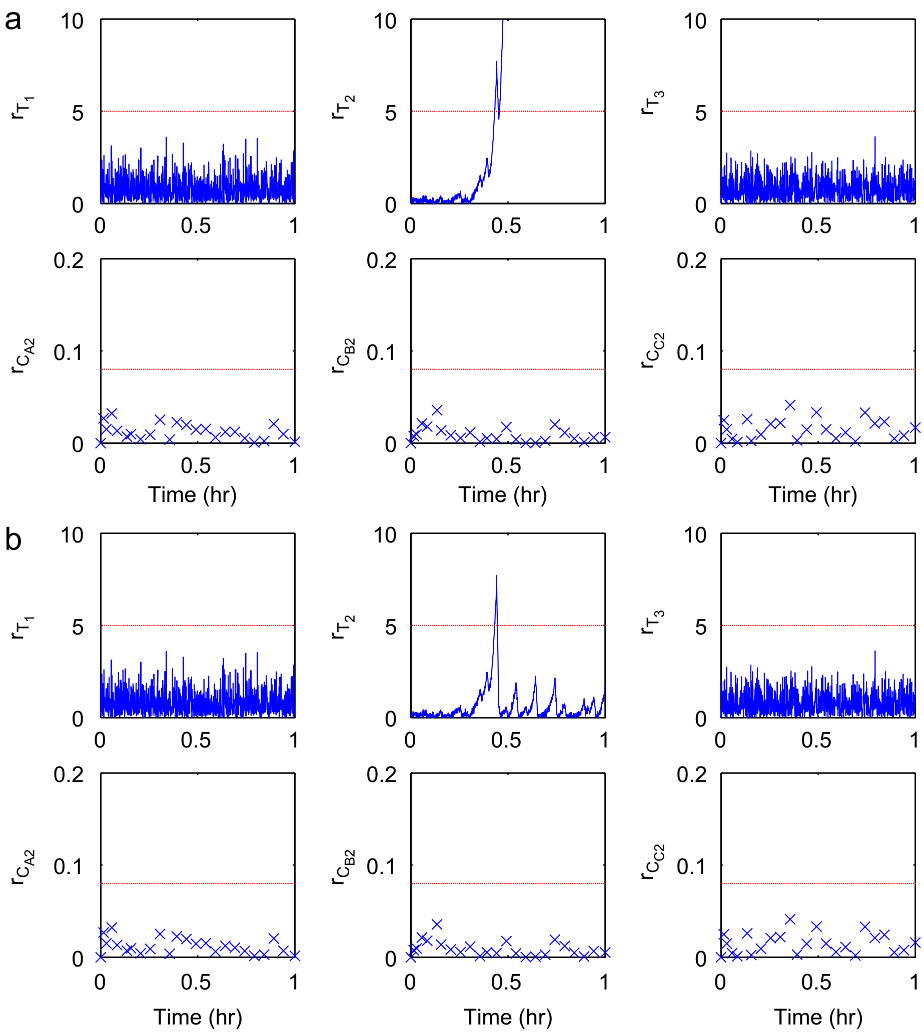

Fig. 8. FDI filter residuals for temperatures (T_1, T_2, T_3) and concentration (C_{A2}, C_{B2}, C_{C2}) with an actuator failure in the heat input to vessel 2 (u_2 = 0) at t = 0.3 h. (a) No FTC is implemented; (b) FTC is implemented.

return to steady-state as the fault is detected at t=0.432 h, isolated at t=0.442 h and the switching rule of Eq. (15) is implemented (see Fig. 8(b) for the corresponding residuals).

5. Conclusions

In this work, we studied the monitoring and reconfiguration of two-tier control systems applied to a general nonlinear processes in the presence of control actuator faults. Specifically, a general class of nonlinear process systems was first considered and was controlled by a two-tier control system integrating a local control system using continuous sensing/actuation with a networked control system using asynchronous sensing/actuation. To deal with control actuator faults that may occur in the closed-loop system and eliminate the ability of the two-tier control system to stabilize the process, a FDI/FTC system was designed which detects and isolates actuator faults and determines how to reconfigure the two-tier control system to handle the actuator faults and ensure closed-loop stability. The FDI/FTC system uses continuous measurements of process variables like temperature and asynchronous measurements of variables like species concentrations. The method was demonstrated using a reactor-separator process consisting of two continuously stirred tank reactors and a flash tank separator with recycle stream.

References

Christofides, P.D., Davis, J.F., El-Farra, N.H., Clark, D., Harris, K.R.D., Gipson, J.N., 2007. Smart plant operations: vision, progress and challenges. A.I.Ch.E. Journal 53, 2734–2741.

Davis, J.F., 2007. Report from NSF Workshop on Cyberinfrastructure in Chemical and Biological Systems: Impact and Directions (see ⟨http://www.oit.ucla.edu/nsfci/NSFCIFullReport.pdf⟩ for the pdf file of this report).

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

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.

Garcia, E.A., Frank, P.M., 1997. Deterministic nonlinear observer-based approaches to fault diagnosis: a survey. Control Engineering Practice 5, 663–670.

Lin, Y., Sontag, E.D., Wang, Y., 1996. A smooth converse Lyapunov theorem for robust stability. SIAM Journal on Control and Optimization 34, 124–160.

Liu, J., Muñoz de la Peña, D., Ohran, B., Christofides, P.D., Davis, J.F., 2008. A two-tier architecture for networked process control. Chemical Engineering Science 63, 5394–5409.

Liu, J., Muñoz de la Peña, D., Ohran, B.J., Christofides, P.D., Davis, J.F., 2010. A two-tier control architecture for nonlinear process systems with continuous/asynchronous feedback. International Journal of Control 83, 257–272.

Massera, J.L., 1956. Contributions to stability theory. Annals of Mathematics 64, 182–206.

McFall, C., Muñoz de la Peña, D., Ohran, B., Christofides, P.D., Davis, J.F., 2008. Fault detection and isolation for nonlinear process systems using asynchronous measurements. Industrial and Engineering Chemistry Research 47, 10009–10019.

Mhaskar, P., Gani, A., El-Farra, N.H., Christofides, P.D., Davis, J.F., 2006. Integrated fault-detection and fault-tolerant control of process systems. A.I.Ch.E. Journal 52, 2129–2148.

Mhaskar, P., Gani, A., McFall, C., Christofides, P.D., Davis, J.F., 2007. Fault-tolerant control of nonlinear process systems subject to sensor faults. A.I.Ch.E. Journal 53, 654–668.

Mhaskar, P., McFall, C., Gani, A., Christofides, P., Davis, J., 2008. Isolation and handling of actuator faults in nonlinear systems. Automatica 44, 53–62.

Montestruque, L.A., Antsaklis, P.J., 2003. On the model-based control of networked systems. Automatica 39, 1837–1843.

Montestruque, L.A., Antsaklis, P.J., 2004. Stability of model-based net-worked control systems with time-varying transmission times. IEEE Transactions on Automatic Control 49, 1562–1572.

Muñoz de la Peña, D., Christofides, P.D., 2008. Lyapunov-based model predictive control of nonlinear systems subject to data losses. IEEE Transactions on Automatic Control 53, 2076–2089.

Nešić, D., Teel, A.R., 2004a. Input–output stability properties of networked control systems. IEEE Transactions on Automatic Control 49, 1650–1667.

Nešić, D., Teel, A.R., 2004b. Input-to-state stability of networked control systems. Automatica 40 (12), 2121–2128.

Neumann, P., 2007. Communication in industrial automation—What is going on? Control Engineering Practice 15, 1332–1347

Ohran, B., de la Peña, D.M., Christofides, P.D., Davis, J.F., 2008. Enhancing data-based fault isolation through nonlinear control. A.I.Ch.E. Journal 53, 2734–2741.

Raich, A., Çinar, A., 1996. Statistical process monitoring and disturbance diagnosis in multivariable continuous processes. A.I.Ch.E. Journal 42, 995–1009.

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

Sun, Y., El-Farra, N.H., 2008. Quasi-decentralized model-based networked control of process systems. Computers and Chemical Engineering 32, 2016–2029.

Walsh, G., Ye, H., Bushnell, L., 2002. Stability analysis of networked control systems. IEEE Transactions on Control Systems Technology 10 (3), 438–446.

Ydstie, E.B., 2002. New vistas for process control: integrating physics and communication networks. A.I.Ch.E. Journal 48, 422–426.