Chemical Engineering Science 64 (2009) 2370 – 2383

Contents lists available at ScienceDirect

Chemical Engineering Science

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

Data-based fault detection and isolation using feedback control: Output feedback and optimality

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

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

ARTICLE INFO

Article history:
Received 12 September 2008
Received in revised form 22 January 2009
Accepted 11 February 2009
Available online 21 February 2009

Keywords:
Process control
Process monitoring
State estimation
Model predictive control
Fault detection and isolation
Nonlinear process systems

ABSTRACT

This work focuses on data-based fault detection and isolation (FDI) of nonlinear process systems. Working within the framework of controller-enhanced FDI that we recently introduced, we address and solve two unresolved, practical problems. First, we consider the case where only output measurements are available and design appropriate state estimator-based output feedback controllers to achieve controller-enhanced FDI in the closed-loop system. Precise conditions for achieving FDI using output feedback control are provided. Second, we address the problem of controller-enhanced FDI in an optimal fashion within the framework of model predictive control (MPC). We propose an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. Throughout the manuscript, we use a nonlinear chemical process example to demonstrate the applicability and effectiveness of the proposed methods.

1. Introduction

Advanced automation technology has changed the way the chemical process industry operates in many ways. Over the last few decades, advancements in plant operations have led to higher efficiency and improved economics through better control and monitoring of process systems. These technological advances have resulted in process systems becoming increasingly automated, no longer requiring operators to open and close valves in order to manually perform process control. In general, there is a trend towards such "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). Along with the move towards more automated plant operation, improved methods of fault detection, isolation and handling are necessary due to the issues raised by automation itself. Despite the many benefits of automatic process control, increased complexity and instrumentation can cause automated plants to become more susceptible to control system failures. Abnormal situations cost U.S. industries over $20 billion each year (Nimmo, 1995). 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. Fault tolerant control (FTC) is a field that has received a significant amount of attention recently as a means for avoiding disaster in the case of a fault, see for example Mhaskar et al. (2006b, 2007, 2008a), El-Farra (2006) and El-Farra and Ghantasala (2007). FTC attempts to reconfigure a process control system upon detection of a fault, in order to preserve closed-loop system stability and performance. We discuss here active methods of FTC, as opposed to passive methods which rely on robust controller design rather than control system reconfiguration. Specifically, the key elements of a successful FTC system include multiple control configurations with well-defined regions of closed-loop stability, a supervisor that is able to switch between faulty and well-functioning control configurations, and perhaps most importantly, a fast, accurate method for detecting faulty process behavior and isolating its cause. The fault detection and isolation (FDI) problem is the focus of the present work.

FDI methods can generally be divided into two categories: model-based and data-based. Model-based FDI methods generally rely on mathematical models of the process developed either from first principles or from system identification that can be solved in real time. The data generated from the model are compared with measured data from the physical system to create residuals that relate to specific faults. With an accurate process model and under appropriate assumptions, it is possible to accomplish FDI for specific fault structures (see, for example, Frank, 1990; Hammouri et al., 2002;

* 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 © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ces.2009.02.020

Kabore and Wang, 2001; Mhaskar et al., 2008b). Data-based methods, on the other hand, rely on process measurements in order to perform FDI. Analyzing process measurements gives the location and direction of the system trajectory in the state space. It is then possible, particularly for linear process systems, to extract information about the fault by comparing the location and/or direction of the system trajectory in the state space with past faulty behavior (e.g., Romagnoli and Palazoglu, 2006; Yoon and MacGregor, 2001). Several methods have been developed that manipulate the measured data to reduce their dimension and extract information from the data with respect to actuator/sensor faults using principle component analysis (PCA) or partial least squares (PLS) techniques (e.g., MacGregor and Kourti, 1996; Wise and Gallagher, 1996; Raich and Çinar, 1996; Negiz and Çinar, 1997). These methods reduce the dimensionality of the data by eliminating directions in the state space with low common-cause variance. Other methods have been developed that consider the contribution of particular states to the overall shift from normal operation (Kourti and MacGregor, 1996). Some data-based methods take advantage of PCA to find correlations within the data (Gertler et al., 1999). Work has also been done to group data based on process structure or process distinct timescales as in multi-block or multi-scale PCA (Westerhuis et al., 1998; Bakshi, 1998; Aradhye et al., 2003). While many of these methods have been successful in achieving fault detection, fault isolation remains a difficult task, particularly for nonlinear processes where historical data under faulty operation are insufficient to discriminate between faults. For a comprehensive review of model-based and data-based FDI methods, the reader may refer to Venkatasubramanian et al. (2003a, b).

In a previous work (Ohran et al., 2008a), we developed an FDI method that takes advantage of both model-based and data-based approaches. This method brought together elements of model-based controller design and statistical process monitoring. In this method, the controller is designed with the FDI scheme in mind in addition to stability and performance criteria. By enforcing an isolable structure in the closed-loop system, it becomes possible to perform FDI based on statistical evaluation of process measurements. The purpose of the present work is to further develop the approach proposed in Ohran et al. (2008a) by relaxing the requirement of full state feedback control and developing the use of model predictive control (MPC) to optimize the manipulated input cost. Specifically, we first consider the case where only output measurements are available and design appropriate state estimator-based output feedback controllers to achieve controller-enhanced FDI in the closed-loop system. Second, we address the problem of controller-enhanced FDI in an optimal fashion within the framework of MPC. We propose an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. Throughout the manuscript, we use a nonlinear chemical process example to demonstrate the applicability and effectiveness of the proposed methods.

2. Preliminaries

2.1. Process system structure

We consider nonlinear process systems with the following general state-space description:

$$\dot{x} = f(x, u, d) \tag{1}$$

where $x \in \mathbb{R}^n$ is the vector of process state variables, $u \in \mathbb{R}^m$ is the vector of manipulated input variables and $d \in \mathbb{R}^p$ is the vector of p possible actuator faults or disturbances. Vector d is equal to zero when the system is under normal operating conditions. When fault k, with $k = 1, \ldots, p$ occurs, the kth component of vector d, denoted d_k, can take any time-varying value. This model includes a broad class of possible faults. The approach of controller-enhanced FDI was introduced in Ohran et al. (2008a) as a method of dividing the state vector into a number of partially decoupled subvectors. These subvectors can be monitored using measured process data. Based on their responses and the system structure enforced by the decoupling controller, it is possible to discriminate between individual faults or groups of faults. Decoupling into subvectors can be accomplished by using model-based control laws to enforce the appropriate structure (see Section 2.3.1). In order to understand the necessary structure to perform isolation, we review (Ohran et al., 2008a) the definitions of the incidence graph, the reduced incidence graph and the isolability graph.

Definition 1. The incidence graph of the system of equation (1) is a directed graph defined by n nodes, one for each state, x_i, $i = 1, \ldots, n$, of the system. A directed arc with origin in node x_i and destination in node x_j exists if and only if $\partial f_j / \partial x_i \neq 0$.

The arcs in the incidence graph illustrate dependencies within the states of the system. A path through more than one arc that starts and ends at the same node is denoted as a loop. Nodes connected by a loop have mutually dependent dynamics, and any disturbance affecting one of them also affects the rest.

Definition 2. The reduced incidence graph of the system of equation (1) is the directed graph of N nodes, one for each q_i, $i = 1, \ldots, N$, where N is the maximum number of nodes that satisfy the following conditions:

- Each node q_i corresponds to a set of states $X_i = \{x_j\}$. These sets of states are a partition of the state vector of the system, i.e.,

$$\bigcup X_i = \{x_1, \ldots, x_n\}, \quad X_i \bigcap X_j = \emptyset, \quad \forall i \neq j$$

- A directed arc with origin q_i and destination q_j exists if and only if $\partial f_l / \partial x_k \neq 0$ for some $x_l \in X_i$, $x_k \in X_j$.
- There are no loops in the graph.

The reduced incidence graph reveals the partially decoupled subsystems within the structure of the states in x.

Definition 3. The isolability graph of the system of equation (1) is a directed graph made of the N nodes of the reduced incidence graph and p additional nodes, one for each possible fault d_k. In addition, a directed arc with origin in fault node d_k and destination to a state node q_j exists if and only if $\partial f_l / \partial d_k \neq 0$ for some $x_l \in X_j$.

These definitions present the basic dependencies within a state vector. In most nonlinear process systems, the states are fully coupled and the isolability graph contains a single node representing all of the states in the system. However, in systems with partially decoupled dynamics the reduced incidence and isolability graphs demonstrate graphically the subsets of the state vector. Consider a simple example of the following system:

$$\begin{aligned} \dot{x}_1 &= -x_1 + x_2 + d_1 \\ \dot{x}_2 &= x_1 + 2x_2 + d_2 \\ \dot{x}_3 &= -2x_1 + x_3 + d_3 \end{aligned} \tag{2}$$

Because x_1 and x_2 are mutually dependent but are not affected by x_3, they form a partially decoupled subsystem represented by a single node (q_1) in the isolability graph leaving x_3 to form a node by itself (q_2). Fig. 1 shows the isolability graph for the system of equation (2).

With the isolability graph of a system, it is possible to consider fault isolation based upon monitoring the subsystems. For this

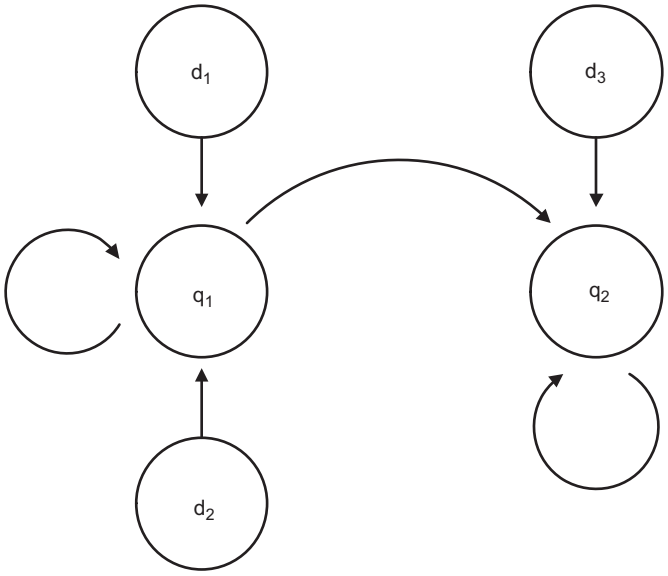

Fig. 1. Isolability graph of the system of equation (2).

purpose, it is necessary to review the definition of a fault signature given below (Ohran et al., 2008a):

Definition 4. The signature of a fault d_k of the system of equation (1) is a binary vector W^k of dimension N, where N is the number of nodes of the reduced incidence graph of the system. The ith component of W^k, denoted W_i^k, is equal to 1 if there exists a path in the isolability graph from the node corresponding to fault d_k to the node q_i corresponding to the set of states X_i, or 0 otherwise.

Using this definition of a fault signature and the isolability graph shown in Fig. 1, it is possible to identify the fault signatures for the three faults considered in the system of equation (2). In this case, the fault d_3 has the signature $W^3 = [0\ 1]^T$ and the two faults d_1 and d_2 have the signature $W^1 = W^2 = [1\ 1]^T$. Thus, based on the fault signatures, it is possible to distinguish between a failure in d_3 from a failure in d_1 or d_2. However, it is not generally possible to discriminate between failures in $d_1$and d_2.

Remark 1. It should be noted that while d_k can model any type of fault, the present approach does not attempt to distinguish between types of faults (e.g., disturbances or actuator faults) that would affect the dynamics of the same state. That is, two faults which affect the system dynamics through the same state are isolated as the same fault in this method (e.g., an inlet temperature disturbance and heat-jacket actuator failure would both affect the reactor temperature dynamics and would thus appear identical in the fault detection scheme). For recent work on discriminating disturbances from actuator failures, see Ghantasala and El-Farra (2009).

Remark 2. There are other approaches in the literature that examine the necessary structural conditions in order to perform model-based fault diagnosis (see, for example, Hammouri et al., 2001; De Persis and Isidori, 2000, 2001). While these approaches are similar to our approach in that they take into consideration the system structure and develop conditions for fault diagnosis, they differ in the fact that they do not enforce the necessary structure for FDI in the closed-loop system via feedback control and use model-based fault diagnosis as opposed to the data-based fault diagnosis approach used in this work.

2.2. Process monitoring

The discussion in the previous subsection focused on deterministic process behavior (i.e., the presence of process/measurement noise was not included in the computation of the fault signature) in which evaluation of the fault signature based on the isolability graph is straightforward and results in a definitive answer. On the other hand, in processes subject to state and measurement noise, it is possible to have false positives and false negatives in determining the effect of a fault on the state trajectories. For this reason, in order to make a comparison between the fault signature based on the deterministic system structure and the process signature based on the actual behavior (computed on the basis of process measurements), it is necessary to use a method of monitoring of the state trajectories that clearly distinguishes normal behavior from faulty behavior and is tolerant to the normal amount of process variation (as computed from historical process data). Additionally, it is assumed that faults of interest will be sufficiently large so that their effect will not be masked by normal process variation.

For the purpose of monitoring whether or not a state has deviated from its normal behavior, we use statistical process monitoring methods. In particular, we use Hotelling's T^2 statistic (Hotelling, 1947), a well established method in statistical process control that monitors multivariate normal (Gaussian) data using a single statistic (Romagnoli and Palazoglu, 2006). Because of its suitability for continuous, serially correlated chemical processes, the method of using single observations is employed (Tracy et al., 1992; Montgomery, 1996). Given a multivariate state vector x of dimension n, the T^2 statistic can be computed using the mean $\bar{x}$ and the estimated covariance matrix S of process data obtained under normal operating conditions (see, for example, Romagnoli and Palazoglu, 2006; Kourti and MacGregor, 1996), as follows:

$$T^2 = (x - \bar{x})^T S^{-1} (x - \bar{x}) \tag{3}$$

The upper control limit (UCL) for the T^2 statistic can be calculated from its distribution, under the assumption that the data are multivariate normal, according to the following formula:

$$T^2_{UCL} = \frac{(h^2 - 1)n}{h(h - n)} F_\alpha(n, h - n) \tag{4}$$

where h is the number of historical measurements used in estimating S, $F_\alpha(n, h-n)$ is the value on the F distribution with $(n, h-n)$ degrees of freedom for which there is probability α of a greater or equal value occurring. Thus, α is the probability of a false alarm. This distribution is based on the assumption that the data are multivariate normal. This requirement is generally a reasonable assumption since even process data that may be serially correlated under open-loop operation are frequently close to normal in the closed-loop system under feedback control on a large time-scale (Montgomery, 1996). The validity of this assumption of normal process data in the closed-loop system has been verified in our previous work (see, for example, Ohran et al. (2008a, b). It has also been verified in the context of the reactor example used in the present paper. Similar results verifying that the closed-loop system data in the reactor example are normal are not given in the present paper for brevity and to avoid redundancy.

The T^2 statistic is used to both detect that a fault has occurred and to provide the system signature that can be compared with the fault signatures defined by the isolability graph. In order to perform these tasks, the T^2 statistic based on the full state vector x with UCL T^2_{UCL} is first used to detect the presence of a fault. Subsequently, the T_i^2 statistic is used to monitor the status of each subset of the state vector with an UCL T^2_{UCLi} where $i=1, \ldots, N$ that is based on each of the

subvectors and their states $x_j \in X_i$. The FDI procedure then follows the steps given below (Ohran et al., 2008a):

1. A fault is detected if $T^2(t) > T^2_{UCL}, \forall t\ t_f \leqslant t \leqslant t_f + T_P$ where t_f is the last time when T^2 crossed the UCL (i.e., after time t_f, T^2 does not return to any values below T^2_{UCL}) and T_P is the fault detection window chosen to be large enough to allow fault isolation with a desired degree of confidence. Choosing T_P depends on the process time constants and potentially on available historical information of past process behavior.
2. Fault isolation can be performed by comparing fault signatures with the process signature $W(t_f, T_P)$ which can be built as follows:

$$T_i^2(t) > T^2_{UCLi}, \quad \forall t\ t_f \leqslant t \leqslant t_f + T_P \rightarrow W_i(t_f, T_P) = 1$$
$$T_i^2(t) \not> T^2_{UCLi}, \quad \forall t\ t_f \leqslant t \leqslant t_f + T_P \rightarrow W_i(t_f, T_P) = 0$$

A fault d_k is isolated at time $t_f + T_P$ if $W(t_f, T_P) = W^k$. If two or more faults are defined by the same signature, further isolation between them is not possible on the basis of the fault signature.

2.3. Controller design for enhanced FDI

2.3.1. Decoupling controller design

The approach to FDI discussed in the previous section can be applied if the signatures of the faults in the closed-loop system are distinct. The uniqueness of a fault depends on the structure of the closed-loop system and the faults considered. In general, complex nonlinear systems are fully coupled (i.e., cannot be broken down into partially decoupled subvectors) and faults cannot be isolated using this method when the controller is designed only to account for closed-loop stability. However, an isolable structure in the closed-loop system may still be achieved through the application of appropriately designed nonlinear control laws. Although many control laws exist that may achieve the desired goal, it is not possible to apply a systematic procedure to controller design that guarantees closed-loop stability and an isolable closed-loop system structure for any nonlinear process. Nonetheless, controller designs can be developed to decouple a particular set of states from the rest of the system in a number of applications. As an example, consider a controller that can be applied to nonlinear systems with the following state-space description:

$$\dot{x}_1 = f_{11}(x_1) + f_{12}(x_1, x_2) + g_1(x_1, x_2)u + d_1$$
$$\dot{x}_2 = f_2(x_1, x_2) + d_2 \tag{5}$$

where $x_1 \in R$, $x_2 \in \mathbb{R}^n$, $u \in \mathbb{R}$ and $g_1(x_1, x_2) \neq 0$ for all $x_1 \in R, x_2 \in \mathbb{R}^n$.

With a nonlinear state feedback controller of the form:

$$u(x_1, x_2) = -\frac{f_{12}(x_1, x_2) - v(x_1)}{g_1(x_1, x_2)} \tag{6}$$

the closed-loop system takes the form

$$\dot{x}_1 = f_{11}(x_1) + v(x_1) + d_1$$
$$\dot{x}_2 = f_2(x_1, x_2) + d_2 \tag{7}$$

where $v(x_1)$ has to be designed in order to achieve asymptotic stability of the origin of the x_1 subsystem when $d_1 = 0$. In this case, the controller of Eq. (6) guarantees asymptotic stability of the closed-loop system, as well as different signatures for faults d_1 and d_2. Note that the closed-loop system in this case can be broken down into two subvectors, each including one state, and the signatures are given by $W^1 = [1\ 1]^T$ and $W^2 = [0\ 1]^T$. If necessary, using multiple controllers allows for more degrees of freedom in breaking up the full state vector into subvectors and allowing fault isolation. Note that in this example, the x_2 subsystem must be input-to-state stable with respect to x_1.

2.3.2. Input/output linearizable nonlinear systems

Input/output linearizable nonlinear systems constitute a special class of nonlinear systems for which it is possible to systematically design nonlinear controllers to achieve controller-enhanced FDI. Specifically, we consider processes modeled by single-input single-output nonlinear systems with multiple possible faults that have the following state-space description:

$$\dot{x} = f(x) + g(x)u + \sum_{k=1}^{p} w_k(x) d_k$$
$$y = h(x) \tag{8}$$

where $x \in \mathbb{R}^n$ is the state vector, $u \in \mathbb{R}$ is the input, $y \in \mathbb{R}$ is the controlled output and $d_k \in R$ represents a possible fault. It is assumed that f, g, h and w_k are sufficiently smooth functions and that a set of p possible faults has been identified. Each of these faults is characterized by an unknown input to the system d_k that can model actuator failures and process faults and disturbances. The value of d_k is not restricted and may be any time-varying fault. The system has an equilibrium point at $x = 0$ when $u(t) \equiv 0$, $d_k(t) \equiv 0$ and $h(0) = 0$. Below, we will use the Lie derivative notation: $L_f h(x)$ is the Lie derivative of the scalar field $h(x)$ with respect to the vector field $f(x)$, $L_f^r h(x)$ is the r-th order Lie derivative and $L_g L_f h(x)$ is a mixed Lie derivative.

The main control objective is to design a feedback control law $u = p_{DC}(x)$ such that the closed-loop system has an asymptotically stable equilibrium point, and the input/output response is linear. Moreover, the closed-loop system must satisfy the isolability conditions by having two or more groups of faults with unique system signatures. To this end, we review the definition of relative degree of the output, y, with respect to the input, u, in the system of equation (8).

Definition 5 (*Isidori, 1989*). Referring to the system of equation (8), the relative degree of the output, y, with respect to the input, u, is the smallest integer, $r \in [1, n]$, for which

$$L_g L_f^i h(x) = 0, \quad i = 0, \ldots, r-2$$
$$L_g L_f^{r-1} h(x) \neq 0$$

If the system of equation (8) has input relative degree $r < n$, then there exists a coordinate transformation (see Isidori, 1989) $(\zeta, \eta) = \Theta(x)$ such that the representation of the system of equation (8) with $d_k = 0$ for all $k = 1, \ldots, p$, in the (ζ, η) coordinates, takes the form

$$\dot{\zeta}_1 = \zeta_2$$
$$\vdots$$
$$\dot{\zeta}_{r-1} = \zeta_r$$
$$\dot{\zeta}_r = L_f^r h(x) + L_g L_f^{r-1} g(x) u$$
$$\dot{\eta}_1 = \Psi_1(\zeta, \eta)$$
$$\vdots$$
$$\dot{\eta}_{n-r} = \Psi_{n-r}(\zeta, \eta) \tag{9}$$

where $y = \zeta_1$, $x = \Theta^{-1}(\zeta, \eta)$, $\zeta = [\zeta_1, \ldots, \zeta_r]^T$ and $\eta = [\eta_1, \ldots, \eta_{n-r}]^T$. Choosing $u = p_{DC}(x)$ in an appropriate way, the dynamics of ζ can be linearized and controlled. The stability of the closed-loop system, however, can only be guaranteed if the inverse dynamics ($\dot{\eta} = \Psi(\zeta, \eta)$) are input-to-state stable with respect to ζ. The feedback-linearizing control law takes the following general form:

$$u(x) = \frac{1}{L_g L_f^{r-1} h(x)} [v(x) - L_f^r h(x)] \tag{10}$$

where $v(x)$ is an external controller for the purpose of stabilizing the system.

If the state-feedback law given in Eq. (10) is used, it can be shown that the faults of the system of equation (8) can be isolated into two different groups: those that affect the output and those that do not affect the output. It is important to note here that the output function, $h(x)$, can be appropriately chosen as a nonlinear combination of the states, x, to aid the task of FDI using a feedback linearizing controller design. The induced structure of the closed-loop system in the transformed coordinates (ζ, η) provides different signatures for the faults depending on their relative degree which is defined below:

Definition 6 (*Daoutidis and Kravaris, 1989*). Referring to the system of equation (8), the relative degree, $\rho_k \in [1, n]$, of the output, y, with respect to the fault d_k is the smallest integer for which

$$L_{w_k} L_f^i h(x) = 0, \quad i = 0, \ldots, \rho_k - 2$$
$$L_{w_k} L_f^{\rho_k - 1} h(x) \neq 0 \tag{11}$$

Analogous to the relative degree of the output with respect to the input, this definition of relative degree relates the output to a particular fault. If a feedback-linearizing controller is used, then the faults can be divided into two different groups: those with a relative degree ρ_k that is greater than the relative degree r and those with a relative degree ρ_k that is less than or equal to r. When a fault occurs, the faults of the first group will not affect the output, y, while those of the latter will. Thus, using the control law in Eq. (10), the possible faults of the system of equation (8) are divided into two groups, each with a different signature. When a fault occurs, taking into account whether the trajectory of the output has deviated from the normal case or not, it is possible to isolate to which group the fault belongs.

Remark 3. Note that in order for the feedback linearizing controller of Eq. (10) to decouple the output from the specific group of faults described above, the first-principles model must match that of the actual process. In a practical application, there is tolerance for some degree of plant-model mismatch that can be accounted for by the fault detection thresholds. In this case, there is not perfect decoupling but the enforcement of near-decoupling in the closed-loop system by the controller that still allows for FDI. On the other hand, large discrepancies between the plant and the model would not allow enforcing the desired structure.

3. Controller-enhanced FDI using output feedback control

In this section, we address the problem of controller-enhanced FDI using output feedback control. Specifically, we discuss the limitations imposed by the availability of measurements of only few state variables and design state estimator-based output feedback control laws that enhance fault isolation in the closed-loop system. We demonstrate an application of our analysis and controller design to a chemical reactor example.

3.1. State estimation

In order to perform controller-enhanced FDI using output feedback control, any unknown process state variable must be quickly and accurately estimated from the available output measurements so that the decoupling state feedback controller designs of Sections 2.3.1 and 2.3.2 can be implemented. The state estimation is performed for the state vector x (or a subset thereof) with the outputs, or measured states, defined as $y = Cx$. In this work, we consider only outputs of the form $y_i = x_i$, $i = 1, \ldots, q < n$. In other words, C is a matrix with one and only one non-zero entry in each row and that entry is equal to unity. This set-up is appropriate in chemical process control applications where measurements of a few states like temperature and concentrations of a few species, like key products, are available, but concentrations of some species are not measured. This set-up also allows obtaining a clear picture of the use of output feedback instead of full state feedback in controller-enhanced FDI. The theory for the state estimator design is based upon a linear system, but can also be applied to nonlinear systems, using a local stability analysis around the operating point (origin). Specifically, the linearized model of the nonlinear system of equation (1) takes the following form:

$$\dot{x} = Ax + Bu + Wd$$
$$y = Cx \tag{12}$$

where A is the Jacobian matrix of the nonlinear system at the operating point, u is the manipulated input vector and d is the fault vector. The matrices B and W can be computed from the linearization of Eq. (1) around the origin. Under the assumption that (A, C) forms an observable pair, each state variable x can be estimated by the following dynamic equation:

$$\dot{\hat{x}} = A\hat{x} + Bu + L(y - C\hat{x}) \tag{13}$$

where $\hat{x}$ is the state estimate and L is the estimator gain that can be chosen so that all the eigenvalues of the matrix $(A - LC)$ are placed at appropriate locations in the left-half of the complex plane to guarantee a desirable rate of convergence of the estimation error to zero. The computation of L can be done using standard pole placement techniques or via a Kalman filtering framework by adding process and measurement noise in the linearized model of Eq. (12). In either case, the linearized state estimation error equation with $d(t) = 0$ takes the form:

$$\dot{e} = (A - LC)e \tag{14}$$

where $e = x - \hat{x}$ is the estimation error. While it is possible to perform state estimation using the full state vector in the state estimator of Eq. (13) when $d(t) \equiv 0$, it becomes necessary to use a reduced-order process model when designing a state estimator-based output feedback controller to enhance FDI. This need for a reduced-order model arises due to faults that affect the state estimator and introduce error into the estimate (i.e., the full state estimation scheme of Eq. (13) works when $d(t) = 0$, but not when $d(t) \neq 0$). Specifically, if the error vector d on the right-hand side of Eq. (12) is nonzero, the new equation for the estimator error becomes $\dot{e} = (A - LC)e + Wd$. Thus, in the presence of a fault, the state estimates no longer converge to their actual values, and the isolable structure attained in the closed-loop system under state feedback control cannot be maintained. However, it is possible in some process systems to perform the state estimation task using a subset of the states that are not directly affected by the expected faults, i.e., effectively eliminating d in the estimation error system. The general structure of the model in Eqs. (12)–(14) remains the same for the reduced-order system, but it is based on a subset of the full state vector, $x_r \subset x$. To mathematically realize this notion, consider a system with the following structure, where time derivatives of the states x_r are not functions of d and include all unknown states to be estimated along with some measured states, and x_d includes the remaining measured states, whose dynamic equations may be functions of d. Specifically, we consider the following decomposition of the vectors and matrices of the linearized system of equation (12)

$$x = \begin{bmatrix} x_r \\ x_d \end{bmatrix}, \quad A = \begin{bmatrix} A_r & A_{rd} \\ A_{dr} & A_d \end{bmatrix}, \quad W = \begin{bmatrix} 0 \\ W_d \end{bmatrix}$$
$$B = \begin{bmatrix} B_r \\ B_d \end{bmatrix}, \quad C = \begin{bmatrix} C_r & 0 \\ 0 & C_d \end{bmatrix}, \quad y = \begin{bmatrix} y_r \\ y_d \end{bmatrix} \tag{15}$$

Provided that the pair (A_r, C_r) is observable, the state estimator based on the reduced-order system then takes the form:

$$\dot{\hat{x}}_r = A_r\hat{x}_r + A_{rd}x_d + B_r u + L_r(y_r - C_r\hat{x}_r) \tag{16}$$

Eq. (16) uses the actual measured values for all of the states in x_d. We can break x_r down further into measured states and unmeasured states, $x_r = [x_{rm}^T \;\; x_{ru}^T]^T$. Note that x_{rm} must include enough measured states independent of d for the system to be observable. Given the restrictions on C, this implies that $y_r = C_r x_r = x_{rm}$ and $C_d = I$ (i.e., $y_d = x_d$). Finally, we define a vector with full state information by combining the measured and estimated data, $\hat{x} = [x_{rm}^T \;\; \hat{x}_{ru}^T \;\; x_d^T]^T$. Note that $\hat{x}_{rm}$ is only used as the driving force for convergence of the state estimator. With these definitions, the reduced-order state estimator of Eq. (16) is not a direct function of d and the dynamics of the estimation error, $e_r = x_r - \hat{x}_r$, take the form $\dot{e}_r = (A_r - L_r C_r)e_r$ which implies that $e_r(t)$ will converge to zero even in the presence of a change in d.

The key requirement is that the states of the reduced-order system must be independent from the faults, or in other words, $\partial f_r/\partial d = 0$. This requires that any unknown states must be independent from the faults as well as that there be enough measured states that can be chosen such that the reduced-order matrices (A_r, C_r) form an observable pair. Although this requirement may seem restrictive, a CSTR example below demonstrates a practical system where the necessary structural requirements to accomplish controller-enhanced FDI using output feedback control are met. It should be noted that while this work uses state observers based upon a pole-placement or a Kalman filtering framework, it may be possible to use other state estimation techniques, such as high-gain observers. The critical point is that the estimators must maintain specific conditions that allow sufficient convergence of the estimation error to zero while in the presence of a fault in order to perform fault isolation. This is demonstrated in the approach laid out above.

Once the estimator gain obtained from the linearized model of the system is calculated, it can then be used to estimate the states of the process using the nonlinear model dynamics. Once again, for the nonlinear system, the state vector, x, decomposes into the one of the reduced-order system (independent of d) and the remaining states, i.e., $x = [x_r^T \;\; x_d^T]^T$ and $f([x_r^T \;\; x_d^T]^T, u, d) = [f_r(x_r, x_d, u)^T f_d(x_r, x_d, u, d)^T]^T$. The nonlinear dynamic equations for the reduced-order system are then combined with the estimator gain and the output error to create a nonlinear state estimator as follows:

$$\dot{\hat{x}}_r = f_r(\hat{x}_r, x_d, u) + L_r(y_r - h_r(\hat{x}_r)) \tag{17}$$

where the measured values are used for the states in x_d, i.e., by assumption $y_d = x_d$. Note that following the previous assumption, $h_r(x_r) = C_r x_r$. Combining the nonlinear state estimator of Eq. (17) with a nonlinear state feedback controller, $u = p_{DC}(x)$, that enforces an isolable structure in the closed-loop system and can be designed following the approaches presented in Sections 2.3.1 and 2.3.2, we obtain the following dynamic nonlinear output feedback controller:

$$\begin{aligned} \dot{\hat{x}}_r &= f_r(\hat{x}_r, x_d, p_{DC}(\hat{x})) + L_r(y_r - C_r\hat{x}_r) \\ u &= p_{DC}(\hat{x}) \end{aligned} \tag{18}$$

Due to the effect of estimation error, it is not possible to achieve complete decoupling. However, it is possible to achieve a near isolable structure that is sufficient for practical purposes. In this sense, we consider a near isolable structure to be one where the closed-loop system under output feedback control can be seen as an $O(e_r)$ regular perturbation of the closed-loop system under state feedback control which is locally exponentially stable and has an isolable structure. Thus, the estimation error can be viewed as a small perturbation error that will be accounted for by the FDI thresholds designed to filter out normal process variation. Theorem 1 summarizes the main analysis and controller design result of this section as well as the closed-loop FDI properties.

Theorem 1. *Consider the closed-loop system of equation* (1) *under the nonlinear output feedback controller of Eq.* (18) *and assume that the pair* (A_r, C_r) *is observable and* L_r *is designed such that the matrix* $(A_r - L_r C_r)$ *has all of its eigenvalues in the left-half of the complex plane. Then, there exist* δ, ε *and* T_y *such that if* f *is continuously differentiable on* $D = \{x \in \mathbb{R}^n \,|\, \|x\|_2 < \delta\}$, *the Jacobian of* f *is bounded and Lipschitz on* D *and* $\max\{\|x(t_0)\|_2, \|\hat{x}_r(t_0)\|_2\} < \delta$ *then* $\|x_r(t) - \hat{x}_r(t)\|_2 < \varepsilon, \forall t > t_0 + T_y$, *and a near isolable structure is enforced in the closed-loop system.*

Proof. Under the control law of Eq. (18), the closed-loop system of Eq. (1) takes the form,

$$\begin{aligned} &\dot{x} = f(x, p_{DC}(\hat{x}), d), \quad y = h(x) \\ &\dot{\hat{x}}_r = f_r(\hat{x}_r, x_d, p_{DC}(\hat{x})) + L_r(y_r - h_r(\hat{x}_r)) \end{aligned} \tag{19}$$

Linearizing the closed-loop system of equation (19) around the equilibrium point (origin) yields,

$$\dot{x} = Ax + Bp_{DC}(\hat{x}), \quad y = Cx \tag{20}$$

$$\dot{\hat{x}}_r = A_r\hat{x}_r + A_{rd}x_d + B_r p_{DC}(\hat{x}) + L_r(y_r - C_r\hat{x}_r) \tag{21}$$

The error between the actual and estimated states of the reduced-order, linearized system is then $e_r = x_r - \hat{x}_r$ with the dynamics $\dot{e}_r = (A_r - L_r C_r)e_r$. Assuming that the pair (A_r, C_r) is observable and that L_r is chosen such that the matrix $A_r - L_r C_r$ has eigenvalues in the left-half of the complex plane, the estimation error, e_r, in the linearized system has exponentially stable dynamics. If the vector field of the nonlinear system, $f(x, p_{DC}(\hat{x}), d)$, is continuously differentiable and the Jacobian matrix is bounded and Lipschitz on $D = \{x \in \mathbb{R}^n \,|\, \|x\|_2 < \delta\}$, then the nonlinear system dynamics are also locally, exponentially stable within some region around the equilibrium point (Khalil, 1992). For some initial condition $\max\{\|x_0\|_2, \|x_{r0}\|_2\} < \delta$, the state estimation error, e_r, will be bounded such that $\|x_r - \hat{x}_r\| < \varepsilon, \; \forall t > t_0 + T_y$, where T_y is a time interval of $O(\varepsilon)$. Thus, the output feedback control approaches state feedback control with error of order ε, i.e., $x_r = \hat{x}_r + O(\varepsilon), \; \forall t > t_0 + T_y$. For sufficiently small ε, this leads to a near isolable structure in the closed-loop system for almost all times since the state feedback controller $p_{DC}(x)$ enforces an isolable structure in the closed-loop system. □

Remark 4. Theorem 1 provides sufficient conditions on the process structure, location of faults and/or disturbances and measurement vector such that controller-enhanced isolation of the type made possible under state feedback control is also possible under output feedback control. The achievement of a near isolable structure refers to the fact that with a sufficiently small ε, the effect of the state estimator error will become increasingly negligible relative to the common-cause variance and the detection threshold for FDI. Thus, even though the state estimate will retain some small amount of error, it will be sufficiently small as to be masked by the normal sensor measurement and process noise which is accounted for in the FDI detection thresholds.

3.2. Application to a CSTR example

The example considered is a well-mixed CSTR in which a feed component A is converted to an intermediate species B and finally to the desired product C, according to the reaction scheme

$$A \underset{}{\overset{1}{\rightleftharpoons}} B \overset{2}{\rightleftharpoons} C$$

Table 1
CSTR example process parameters.

F	1 (m^3/h)
k_{10}	1.0×10^{10} (min^{-1})
k_{-10}	1.0×10^{10} (min^{-1})
k_{20}	1.0×10^{10} (min^{-1})
k_{-20}	1.0×10^{10} (min^{-1})
ΔH_1	-1.0×10^4 (kJ/kmol)
ΔH_2	-0.5×10^4 (kJ/kmol)
C_{A0}	4 (kmol/m^3)
c_p	0.231 (kJ/kg K)
V	1 (m^3)
E_1	6.0×10^4 (kJ/kmol)
E_{-1}	7.0×10^4 (kJ/kmol)
E_2	6.0×10^4 (kJ/kmol)
E_{-2}	6.5×10^4 (kJ/kmol)
R	8.314 (kJ/kmol K)
T_0	300 (K)
ρ	1000 (kg/m^3)

Both steps are elementary, reversible reactions and are governed by the following Arrhenius relationships:

$$r_1 = k_{10}e^{-E_1/RT}C_A, \quad r_{-1} = k_{-10}e^{-E_{-1}/RT}C_B \tag{22}$$

$$r_2 = k_{20}e^{-E_2/RT}C_B, \quad r_{-2} = k_{-20}e^{-E_{-2}/RT}C_C \tag{23}$$

where k_{i0} is the pre-exponential factor and E_i is the activation energy of the ith reaction where the subscripts $1, -1, 2, -2$ refer to the forward and reverse reactions of steps 1 and 2. R is the gas constant, while C_A, C_B and C_C are the molar concentrations of species A, B and C, respectively. The feed to the reactor consists of pure A at flow rate F, concentration C_{A0} and temperature T_0. The state variables of the system include the concentrations of the three main components C_A, C_B, and C_C as well as the temperature of the reactor, T. Using first principles and standard modeling assumptions, the following mathematical model of the process is obtained:

$$\begin{aligned}
\dot{C_A} &= \frac{F}{V}(C_{A0} - C_A) - r_1 + r_{-1} + d_1 \\
\dot{C_B} &= -\frac{F}{V}C_B + r_1 - r_{-1} - r_2 + r_{-2} \\
\dot{C_C} &= -\frac{F}{V}C_C + r_2 - r_{-2} \\
\dot{T} &= \frac{F}{V}(T_0 - T) + \frac{(-\Delta H_1)}{\rho c_p}(r_1 - r_{-1}) + \frac{(-\Delta H_2)}{\rho c_p}(r_2 - r_{-2}) + u + d_2
\end{aligned} \tag{24}$$

where V is the reactor volume, ΔH_1 and ΔH_2 are the enthalpies of the first and second reactions, respectively, ρ is the fluid density, c_p is the fluid heat capacity, $u = Q/\rho c_p$ is the manipulated input, where Q is the heat input to the system, d_1 denotes a disturbance in the inlet concentration and d_2 denotes a fault in the control actuator. The values for the parameters of the process model are given in Table 1.

The system of equation (24) is modeled with sensor measurement noise and autoregressive process noise. The sensor measurement noise was generated using a Gaussian distribution with standard deviation σ_M applied to the measurements of all the process states. The autoregressive process noise was generated discretely as $w_k = \phi w_{k-1} + \xi_k$ where $k = 0, 1, \ldots$ is the discrete time step, ϕ is the autoregressive coefficient and ξ_k is obtained at each sampling step using a zero-mean normal distribution with standard deviation σ_p. Table 2 provides the values of the noise parameters for each state of the system of equation (24). The sampling time interval is $\Delta t_s = 0.1$ min and the fixed numerical integration time interval is $\Delta t_i = 0.001$ min. In this example, the state, C_B, is considered to be unmeasured and is subject to process noise. It should be noted that the open-loop system of equation (24) has fully coupled dynamics. This means that the two faults d_1 and d_2 will be indistinguishable from a data-based perspective because either fault will affect all of the states. Thus, purely data-based FDI is not possible without enforcing an isolable structure in the closed-loop system.

Table 2
CSTR example noise parameters.

	σ_m	σ_p	ϕ
C_A	1E − 2	1E − 2	0.9
C_B	1E − 2	1E − 2	0.9
C_C	1E − 2	1E − 2	0.9
T	1E − 1	1E − 1	0.9

In order to obtain the estimated trajectory for C_B, a state estimator as in Eq. (17) was implemented using the reduced-order system $\hat{x}_r = [\hat{C}_B \ \hat{C}_C]^T$. The process measurements for C_A and T were used in computing the dynamics of $\hat{x}_r$. Note that although C_C is measured, it is used in the reduced-order state estimator so that the reduced-order system is observable. The control input was updated at each sampling interval with the measured values for C_A, T and C_C and the estimated value of $\hat{C}_B$. As discussed in Section 3.1, C_A and T should not be modeled as dynamic states in the estimator since they are directly affected by the faults d_1 and d_2. Therefore, the measured process data of C_A and T must be used in modeling the estimator. Thus, the final form of the state estimator based on the reduced subsystem $\hat{x}_r = [\hat{C}_B \hat{C}_C]^T$ is as given below:

$$\begin{aligned}
\dot{\hat{C}}_B &= -\frac{F}{V}\hat{C}_B + r_1 - r_{-1} - r_2 + r_{-2} + L_1(C_C - \hat{C}_C) \\
\dot{\hat{C}}_C &= -\frac{F}{V}\hat{C}_C + r_2 - r_{-2} + L_2(C_C - \hat{C}_C)
\end{aligned} \tag{25}$$

with

$$r_1 = k_{10}e^{-E_1/RT}C_A, \quad r_{-1} = k_{-10}e^{-E_{-1}/RT}\hat{C}_B$$
$$r_2 = k_{20}e^{-E_2/RT}\hat{C}_B, \quad r_{-2} = k_{-20}e^{-E_{-2}/RT}\hat{C}_C$$

where L is the filter gain obtained using Kalman-filtering theory based on the reduced-order system for the sensor and process noise given in Table 2. The resulting value for L_r is $[L_{r1} \ L_{r2}]^T = [0.0081 \ 0.0559]^T$.

The controlled output of the system, for the purpose of feedback linearization, is defined as the concentration of the desired product $y = h(x) = C_C$ (although, the measured output vector is $y_m = [C_A \ T \ C_C]^T$). We consider only faults d_1 and d_2, which represent undesired changes in C_{A0} (disturbance) and Q (actuator fault), respectively. In this process, the manipulated input u appears in the temperature dynamics and the output, $y = C_C$, has relative degree 2 with respect to u. The fault d_1 appears only in the dynamics of C_A and the output, $y = C_C$, has relative degree 3 with respect to d_1. Finally, the output, $y = C_C$, has relative degree 2 with respect to d_2. Based on the relative degrees of the output with respect to the input and with respect to the faults, under feedback linearizing control the system structure will be such that the state vector can be separated into two subsets: $X_1 = \{C_A, \hat{C}_B, T\}$ and $X_2 = \{C_C\}$. Thus, the fault signature for $d_1 = [1 \ 0]^T$ and for $d_2 = [1 \ 1]^T$. During the simulation, the T^2 for the full state vector is monitored in order to perform fault detection (substituting the estimate $\hat{C}_B$ for the unknown state C_B). Each of the subsystems is monitored to compute the system signature upon detection of a fault. Based on observation of the system dynamic behavior, a fault detection window, T_P, of 1 min is used.

The control objective is to regulate the system at the equilibrium point

$$C_{As} = 2.06\,\text{kmol/m}^3, \quad C_{Bs} = 1.00\,\text{kmol/m}^3, \quad C_{Cs} = 0.937\,\text{kmol/m}^3,$$
$$T_s = 312.6\,\text{K}, \quad u_s = 0\,\text{K/s}. \tag{26}$$

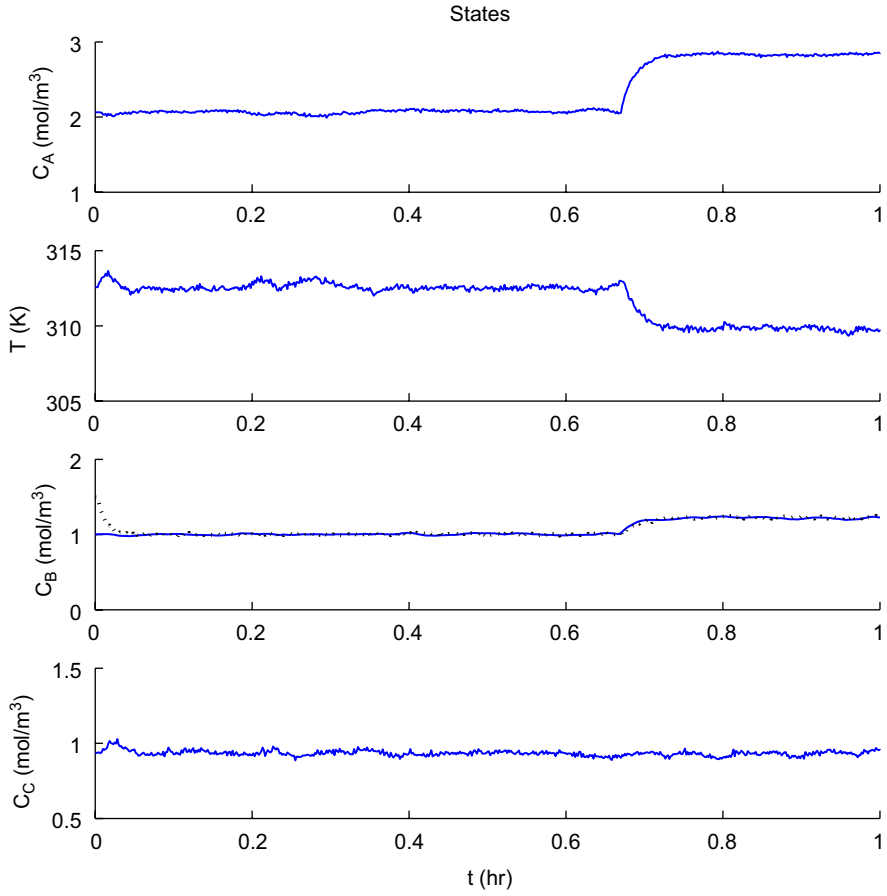

Fig. 2. Plot of measured state values for the CSTR under output feedback decoupling control with fault d_1. C_B shows both actual (solid) and estimated (dotted) values.

where the subscript s refers to the steady state values of the variables. It should be noted that the CSTR system of equation (24) belongs to the class of systems of equation (1) with $x = [C_A - C_{As}, T - T_s, C_B - C_{Bs}, C_C - C_{Cs}]^T$ where C_B is replaced with $\hat{C}_B$ in the definition of $\hat{x}$. This implies that we can apply the output feedback scheme presented using the controlled output $y = C_C$. Using Eq. (10), the feedback-linearizing controller takes the following form:

$$u = \frac{v - L_f^2 h(\hat{x})}{L_g L_f h(\hat{x})} \tag{27}$$

with

$$v = [-2\zeta_1 - 2\zeta_2]$$

where

$$\zeta_1 = C_C$$

$$\zeta_2 = -\frac{F}{V}C_C + r_2 - r_{-2}$$

$$r_2 = k_{20}e^{-E_2/RT}\hat{C}_B, \quad r_{-2} = k_{-20}e^{-E_{-2}/RT}C_C$$

Note that the state variables are in the transformed space and are shifted so that the origin represents the desired set point.

The closed-loop system was simulated for each of the two faults considered. Each simulation was run for a process time of 1 h with the fault occurring at $t = 40$ min. The values for the faults were each zero prior to the fault occurring and took constant values of $d_1 = 1\,\text{kmol/m}^3$ min and $d_2 = 10\,\text{K/min}$ at $t = 40$ min. The state estimator was initialized far from the operating point at $\hat{C}_B(0) = 1.5\,\text{kmol/m}^3$ and $\hat{C}_C(0) = C_C(0) = C_{Cs}$ in order to demonstrate convergence.

Fig. 2 shows the trajectories for each of the states in the simulation with a failure in d_1. The fault is apparent at approximately $t = 40$ min (0.667 h). We can readily see from the state trajectories that the decoupling scheme was effective as evidenced by the fact that the output, C_C, is unaffected by the fault. Also, we see that the state estimator converged relatively quickly at around $t = 3$ min.

For the system with a failure in d_1, Fig. 3 shows the Hotelling's T^2 statistic for the two subvectors X_1 and X_2 as well as for the full state vector. From the graph, we can see that a fault is clearly detected at the expected time $t = 40$ min as shown in the plot of the T^2 statistic for the full state vector (T_3^2). Although there were a few single incidents of data breaching the UCL, none of them represented sustained departures for the length of the fault detection window, T_P. Also note that values above the UCL before $t = 0.1$ h were due to the state estimator not having converged. Upon detection of the fault, the system signature can be computed as $W = [1\ \ 0]^T$ due to the fact that the T^2 statistic for the subvector X_1 exceeded the UCL for a sustained period and the T^2 for the subvector X_2 remained within the bounds of normal operation. Because the system signature matches that of the fault signature for d_1, a fault in d_1 is declared at time $t \approx 41$ min.

In Fig. 4, we see the simulation results for the same system with a failure in d_2. Again, the failure is evident around $t = 40$ min. However, in this case we see that all state trajectories are affected. The process signature obtained from the T^2 statistics in Fig. 5 shows that both subvectors were affected and this process signature matches the fault signature of d_2.

The control action required to decouple and stabilize the system is shown in Fig. 6.

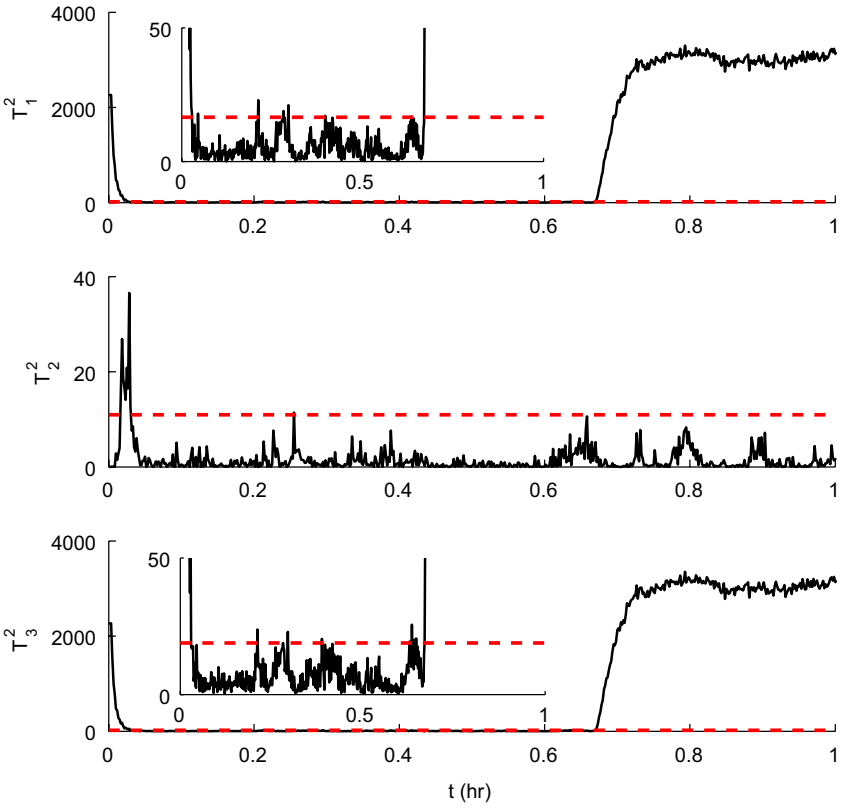

Fig. 3. T^2 statistics for the CSTR under output feedback decoupling control with fault d_1 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

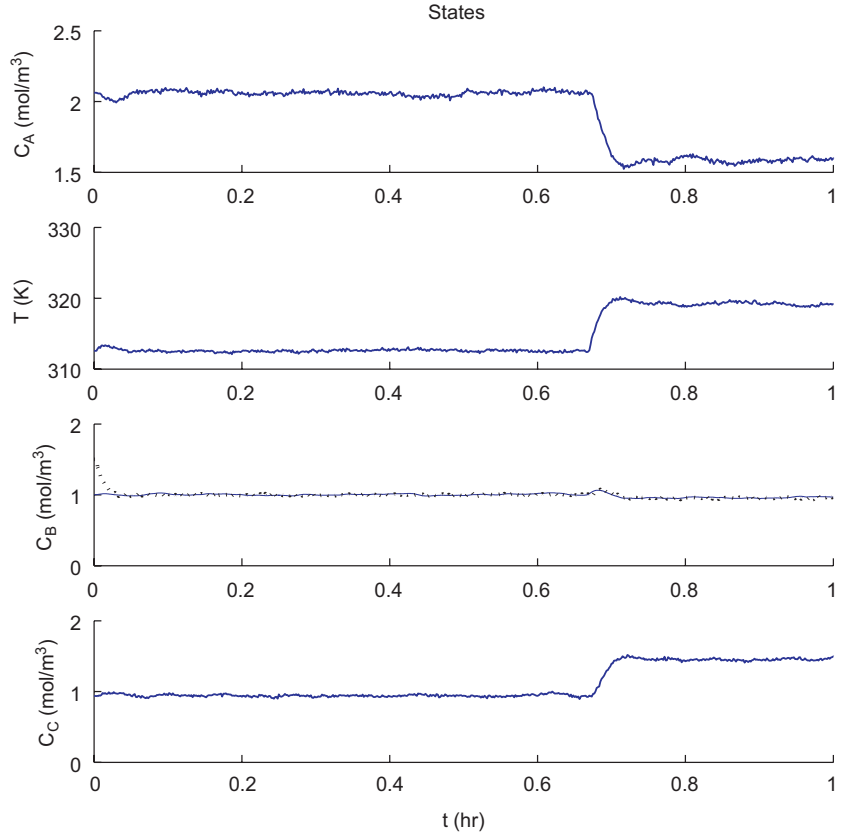

Fig. 4. Plot of measured state values for the CSTR under output feedback decoupling control with fault d_2. C_B shows both actual (solid) and estimated (dotted) values.

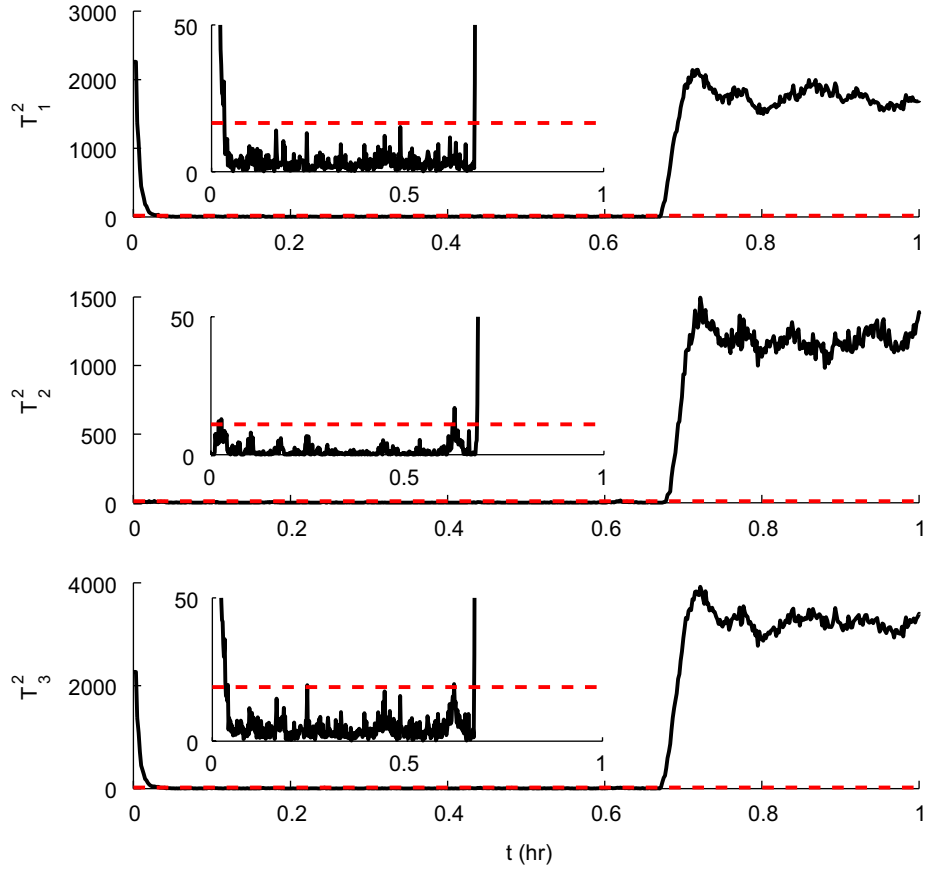

Fig. 5. T^2 statistics for the CSTR under output feedback decoupling control with fault d_2 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

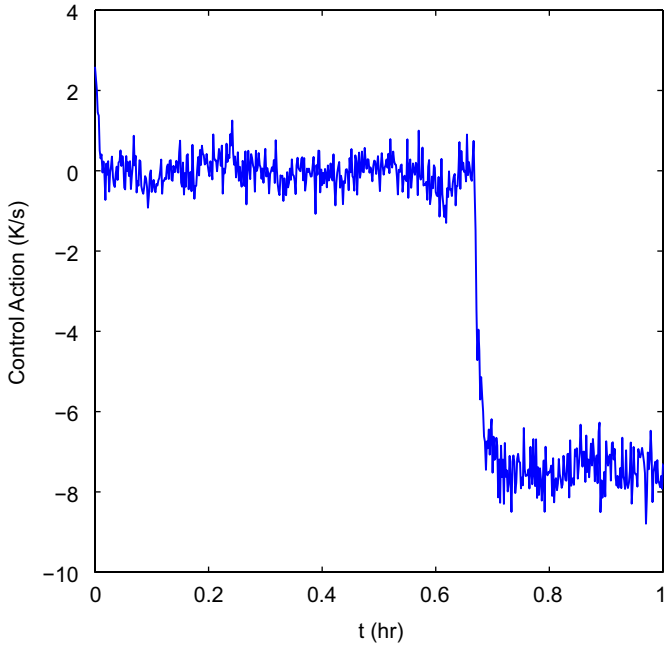

Fig. 6. Manipulated input profile under output feedback decoupling control with fault d_2.

Remark 5. It is important to point out that in the output feedback control formulation presented above, the output measurements are assumed to be continuously available. The reader may refer to McFall et al. (2008) for recent results on model-based FDI using a combination of synchronous and asynchronous measurements.

4. Controller-enhanced FDI using MPC

In addition to addressing the problem of controller-enhanced isolation using output feedback control, we also consider achieving controller-enhanced isolation in an optimal fashion using MPC. We will consider this problem under the assumption that measurements of the full state vector are available, but the extension to the output feedback case is conceptually straightforward by combining the results of the present and previous sections. We will start with the presentation of a general MPC formulation with an appropriate decoupling constraint and continue with an application to the case of input/output linearizable nonlinear systems.

4.1. MPC with isolability constraints

MPC is a popular control strategy that is based on using a process model to optimize controller performance. MPC predicts the future evolution of the system from an initial state at discrete sampling times for a given prediction horizon. These predictions are used to minimize a given cost function by solving a suitable optimization problem. MPC optimizes over the set of discrete manipulated input trajectories with a fixed sampling time and within a fixed prediction horizon (number of sampling time steps). The optimization problem is solved based on a cost function, accounting for input constraints, resulting in a set of optimal control inputs for the given horizon length. To present the proposed MPC formulation, we consider the nonlinear system of equation (1) and assume that we can construct

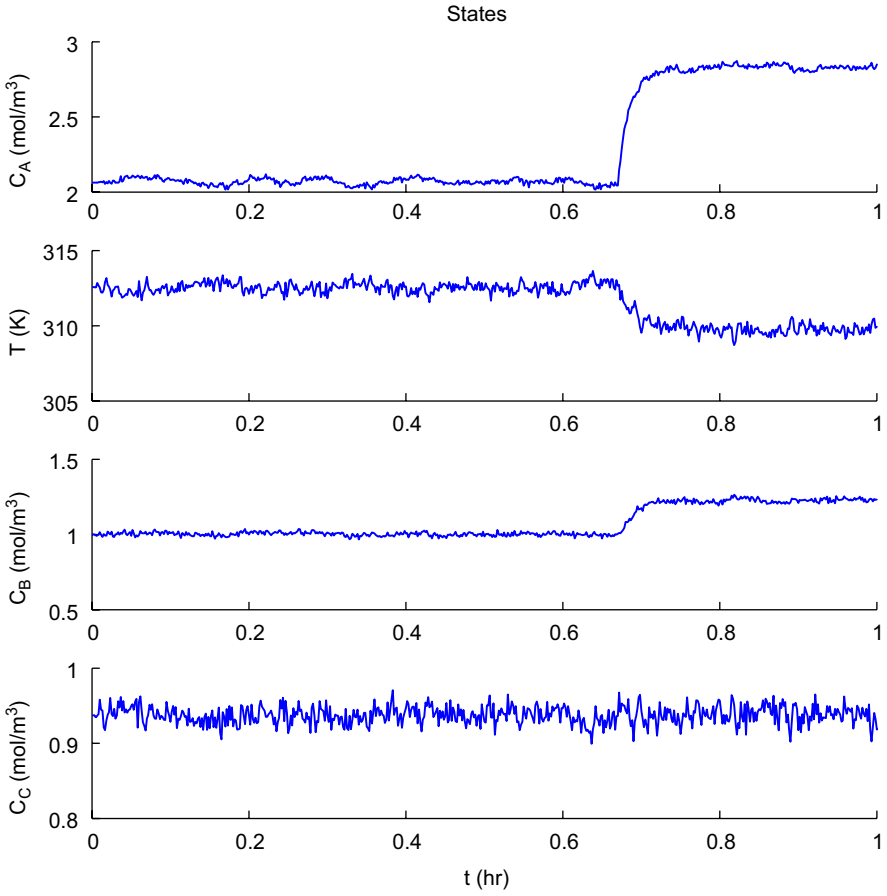

Fig. 7. Plot of measured state values for the CSTR under feedback linearizing MPC with fault d_1.

a nonlinear state feedback control law $u = p_{DC}(x, v)$, using the approaches presented in Sections 2.3.1 and 2.3.2, such that the resulting system

$$\dot{x} = f(x, p_{DC}(x, v), d) = \tilde{f}(x, v, d) \tag{28}$$

has an isolable structure. For the formulation of the MPC optimization problem, we consider the controller $u = p_{DC}(x, v)$ to be applied continuously. This requirement can be relaxed with minimal effect and this issue will be discussed below.

We consider the application of MPC to the system of equation (28). It is important to note that the decoupling controller $u=p_{DC}(x, v)$ should be applied prior to the MPC optimization of the external input, v, and thus, the MPC optimization is performed independently from and does not affect the decoupling controller. In order to define a finite dimensional optimization problem, v is constrained to belong to the family of piece-wise constant functions $S(\Delta)$, with sampling period Δ. The MPC framework can now be used to compute the auxiliary input v_k. Specifically, we consider the following MPC formulation:

$$J = \arg\min_{v_k \in S(\Delta)} \int_{t_k}^{t_k+T_h} (\tilde{x}^T(\tau) R \tilde{x}(\tau) + v_k^T(\tau) Q v_k(\tau))\, d\tau$$

$$\dot{\tilde{x}}(t) = \tilde{f}(\tilde{x}, v_k(t)), \quad \tilde{x}(t_k) = x(t_k) \tag{29}$$

where $\tilde{x}$ is the simulated system to be optimized, R and Q are positive definite matrices that penalize the state and manipulated input cost and T_h is the prediction horizon.

We note the case of input/output linearizable nonlinear systems with two faults/disturbances, (i.e., $d = [d_1 \;\; d_2]^T$) implies that Eq. (28) can be written as

$$\dot{\zeta} = \hat{f}(\zeta, v, d_1)$$

$$\dot{\eta} = \hat{\psi}(\zeta, \eta) + d_2 \tag{30}$$

where $x = \Theta(\zeta, \eta)$ and $\Theta(\zeta, \eta)$ is, in general, a nonlinear coordinate change, and $\hat{f}(\zeta, v, d_1)$, $\hat{\psi}(\zeta, \eta)$ are nonlinear vector functions of appropriate dimensions. The generalization to the case of having more than two faults is conceptually straightforward, yet notationally more involved. With the input/output linearizing control, Eq. (29) can be reduced to

$$J = \arg\min_{v_k \in S(\Delta)} \int_{t_k}^{t_k+T_h} (\tilde{\zeta}^T(\tau) R \tilde{\zeta}(\tau) + v_k^T(\tau) Q v_k(\tau))\, d\tau$$

$$\dot{\tilde{\zeta}}(t) = v_k(t), \quad \tilde{\zeta}(t_k) = \zeta(t_k) \tag{31}$$

where $\tilde{\zeta}$ is the simulated state in the transformed space and the resulting nonlinear controller has the form

$$u(x(t), v_k) = \frac{v_k - L_f^r h(x(t))}{L_g L_f^{r-1} h(x(t))} \tag{32}$$

Using the input/output linearizing controller to induce the necessary structure for fault isolation, MPC is used to compute the external controller in order to maintain stability and optimal performance. Specifically, the external input, v_k, is optimized with respect to the

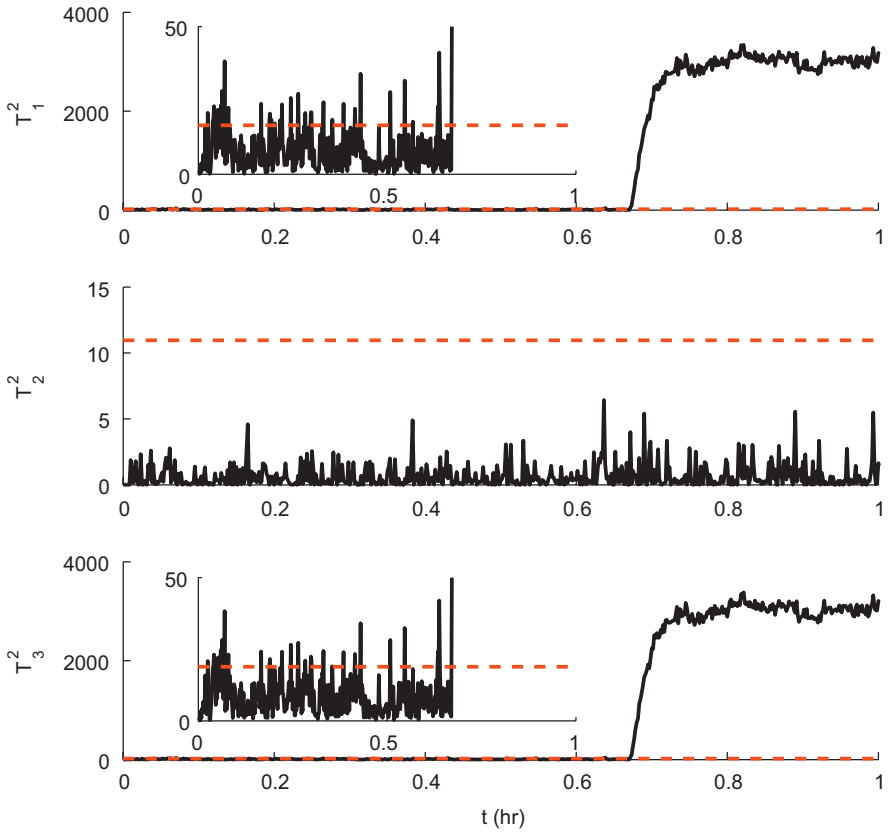

Fig. 8. T^2 statistics for the CSTR under feedback linearizing MPC with fault d_1 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

cost function as a set of discrete control inputs over a sequence of sampling times for a given horizon length. This results in a overall control input that is not optimal with respect to the total cost due to the input/output linearizing component, but is optimal with respect to the extra controller cost needed to stabilize and control the system at the steady state.

Remark 6. It should be noted that the MPC formulation given in equation (31) assumes that the decoupling controller, $u = p_{DC}(x, v)$, is applied continuously. In a practical situation, the decoupling controller will be implemented via sample and hold. Although this introduces error into closed-loop system dynamics, the closed-loop system has a near isolable structure as the hold time, Δ, goes to zero. This is sufficient for near decoupling due to the thresholds implemented for FDI which account for normal process variation (for further results on practical closed-loop stability subject to sample and hold control, see Mhaskar et al., 2005, 2006a). Error introduced by sample-and-hold implementation of the decoupling control law leads, subsequently, to error in the MPC optimization due to plant-model mismatch. Again, this error becomes increasingly small as the hold time, Δ, goes to zero and can be adequately accounted for by the FDI thresholds used.

Remark 7. Referring to the incorporation of stability constraints in MPC, we note that in order to guarantee robust stability of the closed-loop system, MPC controllers generally include a set of stability constraints. This can be accomplished through Lyapunov-based MPC (LMPC) (Mhaskar et al., 2005, 2006a; Muñoz de la Peña and Christofides, 2008) or through terminal constraints in the cost function. Different schemes can be found in the literature, see Mayne et al. (2000) for a review on MPC stability results.

4.2. Application to a CSTR example

The input/output linearizing control law with MPC as the external control input was applied to the chemical reactor example of Section 3. All parameters were the same as in Section 3 including sensor noise and process noise characteristics, faults sizes, fault incident times, system parameters, set points and fault detection time. However, in this simulation, full state feedback is used (i.e., C_A, C_B, C_C and T are measured). The sample and hold time for the MPC controller is the same as the discrete sampling time in Section 3, $\Delta t_s = 0.1$ min, and the numerical integration time step is $\Delta t_i = 0.001$ min. The controller cost function over which the system was optimized used weights of $R = [100\ 0; 0\ 1]$ and $Q = 10$. The horizon length was 10 time steps (1 min). Because of the inherently stable nature of the CSTR dynamics, more robust methods of stabilization were not used as penalizing the state was sufficient in this case.

In Fig. 7, we see the state trajectories for the system under decoupling control with MPC as the external input to optimize system performance. A failure in d_1 with the same magnitude as in Section 3 is introduced at $t = 40$ min. As before, we see that the decoupling control was effective as evidenced by the fact that C_C appears to be unaffected by the fault. Fig. 8 shows the T^2 statistic for the closed-loop system. We note that fault detection occurred based on the statistic for the full state vector, T_3^2, at $t \approx 41$ min. The system signature based on T_1^2 and T_2^2 matches the fault signature for d_1, $W = W^1 = [1\ 0]^T$.

The process simulated with a failure in d_2 and its T^2 statistics are shown in Fig. 9. Again, we see that the closed-loop system signature based on the monitored subsystems matches what is expected based on the isolability graph (i.e., $W = W^2 = [1\ 1]^T$). In this plot, we again

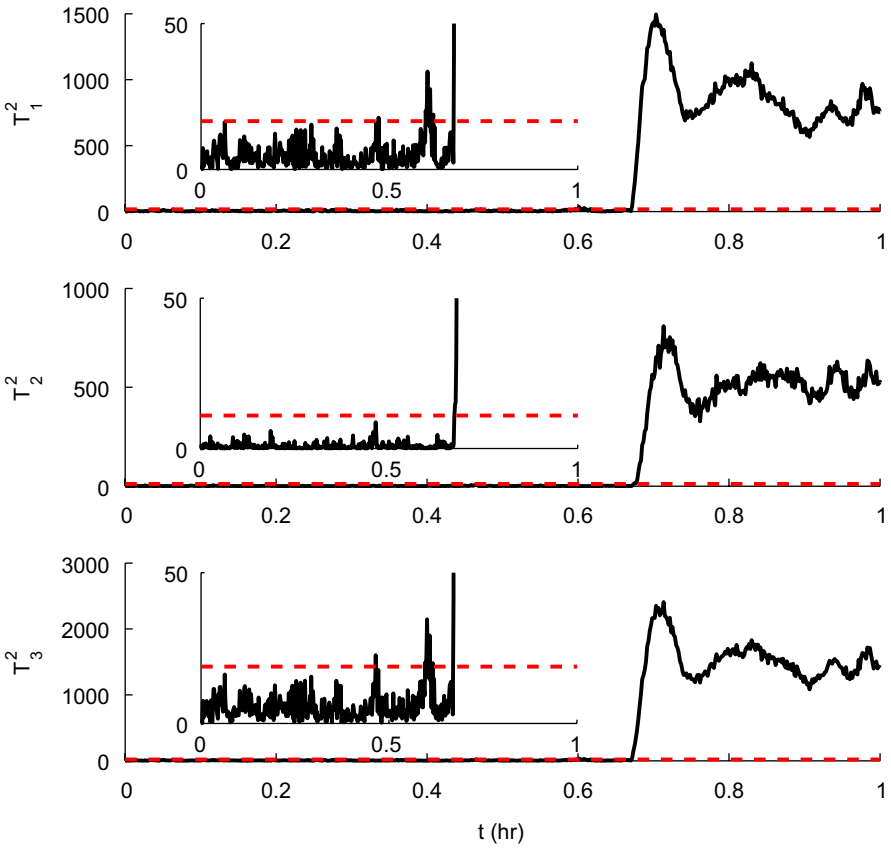

Fig. 9. T^2 statistics for the CSTR under feedback linearizing MPC with fault d_2 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

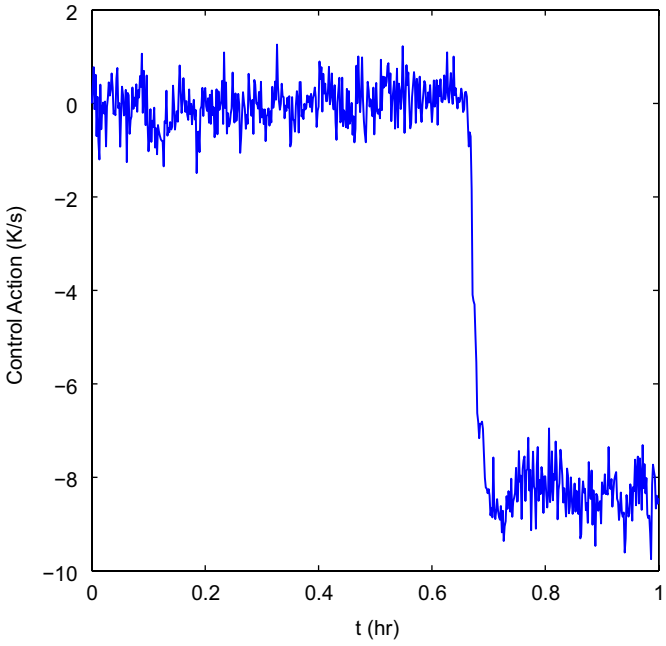

Fig. 10. Manipulated input profile under feedback linearizing MPC with fault d_2.

see temporary violations of the UCL, but none that are sustained for longer than the fault detection window, T_P.

In Fig. 10, we see the control action requested by the feedback linearizing MPC. Based on the cost function used to perform MPC, the costs of two approaches (feedback linearizing control with proportional control and feedback linearizing MPC) were compared. Both controllers were implemented via state feedback. The process was initialized at $x(0)=[C_A(0)=2.06\,\text{kmol/m}^3\ T(0)=312.6\,\text{K}\ C_B(0)=1.00\,\text{kmol/m}^3\ C_C=1.44\,\text{kmol/m}^3]^T$ and was allowed to run for an hour without faults. The total costs of converging to the steady-state for the closed-loop system under feedback linearizing control with proportional control was 19.96 and for the closed-loop system under feedback linearizing MPC was 11.97; as expected, the use of MPC leads to improved overall performance.

5. Conclusions

Building upon our previous work on controller-enhanced FDI (Ohran et al., 2008a), the present work has addressed two previously unresolved, practical problems. Specifically, it was demonstrated that the method of controller-enhanced FDI can be applied to processes where only output measurements are available under appropriate assumptions in the process system structure. We developed an approach where systems with incomplete state measurements can be dealt with using state estimator-based output feedback control. This approach maintains the necessary isolable structure in the closed-loop system in order to perform controller-enhanced FDI. Additionally, we addressed the problem of controller-enhanced FDI in an optimal fashion within the framework of MPC. We proposed an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. The effectiveness of these methods was demonstrated through application to a nonlinear CSTR example.

Acknowledgment

Financial support from NSF, CTS-0529295 is gratefully acknowledged.

References

Aradhye, H.B., Bakshi, B.R., Strauss, R.A., Davis, J.F., 2003. Multiscale SPC using wavelets: theoretical analysis and properties. A.I.Ch.E. Journal 49, 939–958.

Bakshi, B.R., 1998. Multiscale PCA with application to multivariate statistical process monitoring. A.I.Ch.E. Journal 44, 1596–1610.

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.

Daoutidis, P., Kravaris, C., 1989. Synthesis of feedforward state feedback controllers for nonlinear processes. A.I.Ch.E. Journal 35, 1602–1616.

De Persis, C., Isidori, A., 2000. On the observability codistributions of a nonlinear system. Systems and Control Letters 40, 297–304.

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

El-Farra, N.H., 2006. Integrated fault detection and fault-tolerant control architectures for distributed processes. Industrial & Engineering Chemistry Research 45, 8338–8351.

El-Farra, N.H., Ghantasala, S., 2007. Actuator fault isolation and reconfiguration in transport-reaction processes. A.I.Ch.E. Journal 53, 1518–1537.

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.

Gertler, J., Weihua, L., Huang, Y., McAvoy, T., 1999. Isolation enhanced principal component analysis. A.I.Ch.E. Journal 45, 323–334.

Ghantasala, S., El-Farra, N.H., 2009. Robust diagnosis and fault-tolerant control of distributed process over communication networks. International Journal of Adaptive Control and Signal Processing, in press.

Hammouri, H., Kabore, P., Kinnaert, M., 2001. A geometric approach to fault detection and isolation for bilinear systems. IEEE Transactions on Automatic Control 46, 1451–1455.

Hammouri, H., Kabore, P., Othman, S., Biston, J., 2002. Failure diagnosis and nonlinear observer application to a hydraulic process. Journal of the Franklin Institute 339, 455–478.

Hotelling, H., 1947. Multivariate quality control. In: Eisenhart, O. (Ed.), Techniques of Statistical Analysis. McGraw-Hill, pp. 113–184.

Isidori, A., 1989. Nonlinear Control Systems: An Introduction. second ed.. Springer, Berlin, Heidelberg.

Kabore, P., Wang, H., 2001. Design of fault diagnosis filters and fault-tolerant control for a class of nonlinear systems. IEEE Transactions on Automatic Control 46, 1805–1810.

Khalil, H., 1992. Nonlinear Systems. Macmillan Publishing Company,

Kourti, T., MacGregor, J., 1996. Multivariate SPC methods for process and product monitoring. Journal of Quality Technology 28, 409–428.

MacGregor, J., Kourti, T., 1996. Statistical process control of multivariate processes. Journal of Quality Technology 28, 409–428.

Mayne, D.Q., Rawlings, J.B., Rao, C.V., Scokaert, P.O.M., 2000. Constrained model predictive control: stability and optimality. Automatica 36, 789–814.

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 & Engineering Chemistry Research 47, 10009–10019.

Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2005. Predictive control of switched nonlinear systems with scheduled mode transitions. IEEE Transactions on Automatic Control 50, 1670–1680.

Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2006a. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. Systems & Control Letters 55, 650–659.

Mhaskar, P., Gani, A., Christofides, P.D., 2006b. Fault-tolerant process control: performance-based reconfiguration and robustness. International Journal of Robust & Nonlinear Control 16, 91–111.

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

Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2008a. Robust predictive control of switched systems: satisfying uncertain schedules subject to state and control constraints. International Journal of Adaptive Control and Signal Processing 22, 161–179.

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

Montgomery, D.C., 1996. Introduction to Statistical Quality Control. Wiley, New York.

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.

Negiz, A., Çinar, A., 1997. Statistical monitoring of multivariable dynamic processes with state-space models. A.I.Ch.E. Journal 43, 2002–2020.

Nimmo, I., 1995. Adequately address abnormal operations. Chemical Engineering Progress 91, 36–45.

Ohran, B.J., Muñoz de la Peña, D., Christofides, P.D., Davis, J.F., 2008a. Enhancing data-based fault isolation through nonlinear control. A.I.Ch.E. Journal 54, 223–241.

Ohran, B.J., Rau, J., Christofides, P.D., Davis, J.F., 2008b. Plant-wide fault isolation using nonlinear feedback control. Industrial & Engineering Chemistry Research 47, 4220–4229.

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

Romagnoli, J., Palazoglu, A., 2006. Introduction to Process Control. CRC Press, Baco Raton.

Tracy, N.D., Young, J.C., Mason, R.L., 1992. Multivariate control charts for individual observations. Journal of Quality Technology 24, 88–95.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S., Yin, K., 2003a. A review of process fault detection and diagnosis part III: process history based methods. Computers and Chemical Engineering 27, 327–346.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., Kavuri, S., 2003b. A review of process fault detection and diagnosis part I: quantitative model-based methods. Computers and Chemical Engineering 27, 293–311.

Westerhuis, J.A., Kourti, T., MacGregor, J.F., 1998. Analysis of multiblock and hierarchical PCA and PLS models. Journal of Chemometrics 12, 301–321.

Wise, B.M., Gallagher, N.B., 1996. The process chemometrics approach to monitoring and fault detection. Journal of Process Control 6, 329–348.

Yoon, S., MacGregor, J., 2001. Fault diagnosis with multivariate statistical models part I: using steady state fault signatures. Journal of Process Control 11, 387–400.