Enhancing Data-based Fault Isolation Through Nonlinear Control

Benjamin J. Ohran, David Muñoz de la Peña, and James F. Davis
Dept. of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095

Panagiotis D. Christofides
Dept. of Chemical and Biomolecular Engineering and Dept. of Electrical Engineering, University of California, Los Angeles, CA 90095

DOI 10.1002/aic.11328
Published online December 3, 2007 in Wiley InterScience (www.interscience.wiley.com).

This work focuses on a broad class of nonlinear process systems subject to control actuator faults and disturbances and proposes a method for data-based fault detection and isolation that explicitly takes into account the design of the feedback control law. This method allows isolating specific faults in the closed-loop system; fault detection is done using a purely data-based approach and fault isolation is achieved using the structure of the closed-loop system as induced by an appropriately designed controller. This is achieved through the design of nonlinear model-based state-feedback control laws that decouple the dependency between certain process state variables in the closed-loop system. In this sense, the proposed approach constitutes a departure from the available data-based fault detection and isolation techniques which do not take advantage of the design of the feedback control law to enforce a closed-loop system structure that enhances fault isolation. The theoretical results are demonstrated through simulations of a CSTR and a gas-phase polyethylene reactor. © 2007 American Institute of Chemical Engineers *AIChE J,* 54: 223–241, 2008
Keywords: fault diagnosis, process control

Introduction

Handling abnormal situations is a subject of great importance within the areas of chemical process control and operations. In chemical plant operations, abnormal situations can arise from failures in control systems, equipment and chemical processes. Modern chemical plants that rely on highly automated processes to maintain precise control and efficient production are particularly vulnerable to these failures. Loss of control in a chemical process can lead to the waste of raw materials and energy resources, as well as downtime and production losses. More extreme cases of out of control processes can lead to destruction of process equipment and/or injury to personnel. As process plants become more sophisticated, it is increasingly more important to develop ways of eliminating or mitigating the consequences of such failures. One way to reduce the risk of problems is through early and accurate detection of failures and subsequent control system reconfiguration to achieve optimal plant operation through fault-tolerant control.

Over the past ten years, fault-tolerant control has become an active area of research within control engineering. Many research studies can be found in the field of aerospace control engineering,[1,2,3] as well as within chemical process control.[4,5,6] Fault-tolerant control is based on the assumption that there exist multiple available control configurations in which the closed-loop system can operate. Fault-tolerant control systems utilize this redundancy to reconfigure a failed control system configuration to one that does not rely on the faulty actuator, sensor or controller. The success of any fault-tolerant control method, however, requires the integration of several key components, including: the detection and

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

isolation of faults, multiple available feedback control configurations that stabilize the system and a supervisory switching scheme that controls the transition from the failed configuration to a well-functioning fallback configuration that can ensure closed-loop stability. In this article, the main focus will be on fault detection and isolation (FDI), that is, not only detecting that a control actuator fault or disturbance has occurred, but also diagnosing the underlying cause of the faulty behavior (i.e., pointing exactly to the specific control actuator/sensor that has failed). If a fault is isolated early and accurately, it is more likely that it can be safely dealt with through fault-tolerant control systems (see, for example,[7,8] for more results in this area).

Methods for fault detection and isolation fall into two broad categories: model-based methods and data-based methods. Model-based methods utilize a mathematical model of the process to build, under appropriate assumptions, dynamic filters that use process measurements to compute residuals that relate directly to specific faults; in this way, fault detection and isolation can be accomplished for specific model and fault structures (see, for example,[9,10]). On the other hand, data-based methods are primarily based on process measurements. Analyzing measured data gives a picture of the location and direction of the system in the state-space. It is then possible to extract information about the fault by comparing the location and/or direction of the system in the state-space with past behavior under faulty operation (e.g.,[11,12]), or with expected behavior as predicted by the structure or model of the system. A number of methods applicable to actuator/sensor faults have been developed that process the measured data to reduce their dimension and extract information from the data using principle component analysis (PCA) or partial-least squares (PLS) techniques (e.g.,[13,14,15,16]). These methods reduce the dimensionality of the data by eliminating directions in the state-space with low common-cause variance. Many methods use this reduced space and consequent null space to gain further information about the process behavior, including techniques, such as contribution plots (e.g.,[17]), or multiscale statistical process control using wavelets (e.g.,[18,19,20]). One of the main drawbacks of these data-based methods is that in order to accomplish fault isolation, they commonly require fault-specific historical data that may be costly to obtain. Furthermore, due to the nature of a chemical process, its structure and/or how it is instrumented, in practice, it is often hard to distinguish between regions/directions corresponding to operation in the presence of different faults due to overlap, making fault isolation difficult. For a comprehensive review of model-based and data-based fault detection and isolation methods, the reader may refer to.[10,21]

In most applications, the FDI scheme is designed independently from the feedback control law and is then applied on top of the closed-loop system operating under a feedback control law that is previously designed without consideration of the possible faults that might occur. This is shown in Figure 1a which shows that the independently designed feedback control law and FDI scheme are combined only in the final closed-loop system. The focus of this work is to investigate the possibility of integrating the feedback control design with the data-based FDI scheme. This paradigm shift is illustrated in Figure 1b which demonstrates the idea of designing both

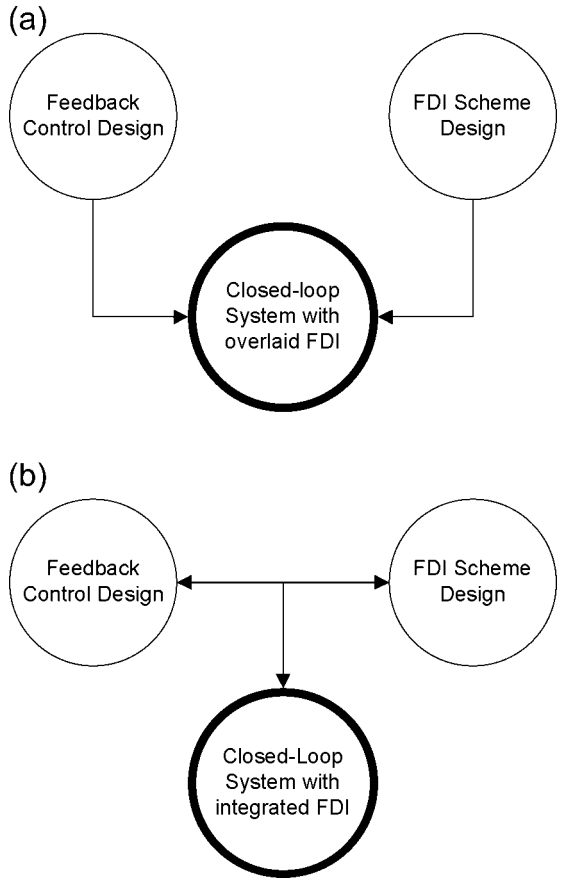

Figure 1. (a) Top: Common methods of fault diagnosis apply the FDI scheme and feedback control law to the closed-loop system independently from each other, and (b) bottom: this work proposes integrating the feedback control law design with the FDI scheme in the closed-loop system.

the feedback control law and the FDI scheme with the other in mind. With the controller design taking into account the FDI scheme, faults may be more easily isolated in the resulting closed-loop system.

The aforementioned considerations motivate the development of a data-based method for fault detection and isolation that utilizes the design of the controller to enhance the isolability of the faults in the closed-loop system. Specifically, it is demonstrated in this work that a data-based FDI scheme is able to isolate a given set of faults if the nonlinear closed-loop system satisfies certain isolability conditions in the presence of common-cause process variation. We explicitly characterize this set of isolability conditions and show that it is possible, under certain conditions on the system structure, to design a feedback control law that guarantees that the closed–loop system satisfies the isolability conditions and that the origin of the closed-loop system is asymptotically stable. This is achieved through the use of appropriate nonlinear control laws that effectively decouple the dependency between certain process state variables. The controller enforces a specific structure on the system that makes fault detection and isolation possible without prior knowledge of system

behavior under faulty operation. The theoretical results are applied to a continuously stirred-tank reactor (CSTR) example and to a polyethylene reactor example. It should also be noted that although the examples given in this article are presented using a specific method for data-based fault diagnosis, the closed–loop system structure enforced by the proposed approach can also be exploited to achieve fault isolation using other data-based fault detection methods.

Preliminaries

Process model

This work focuses on a broad class of nonlinear process systems subject to actuator faults and disturbances with the following state-space description

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

where $x \in \mathbb{R}^n$ denotes the vector of process state variables, $u \in \mathbb{R}^m$ denotes the vector of manipulated input variables, and $d \in \mathbb{R}^p$ denotes the vector of p possible actuator faults or disturbances. Normal operating conditions are defined by $d = 0$. Each component d_k, $k = 1, \ldots, p$ of vector d characterizes the occurrence of a given fault. When fault k occurs, variable d_k can take any value. Therefore, the model of Eq. 1 can include a broad class of possible faults ranging from actuator faults to complex process disturbances and failures. The system under normal operating conditions and zero input has an equilibrium point at the origin, i.e., $f(0,0,0) = 0$.

Before proceeding with the theoretical development, it is important to state that the proposed FDI method brings together model-based analysis and controller design techniques for nonlinear, deterministic ordinary-differential equation systems and statistical data-based fault-diagnosis techniques. These together will be applied to the closed-loop system to diagnose faults that affect the process outside of the region determined by the common-cause process variation. To this end, we will first state the isolability conditions for the closed-loop system that need to be enforced by the appropriate control laws on the basis of the nonlinear deterministic system of Eq. 1. Subsequently, we will introduce additive autocorrelated noise in the right-hand side of Eq. 1 and additive Gaussian noise in the measurements of the vector x to compute the region of operation of the process variable, x, under common-cause variance. Finally, we will demonstrate that the enforcement of an isolable structure in the closed-loop system by an appropriate feedback law allows isolating specific faults whose effect on the closed-loop system leads to sustained process operation outside of the region of common-cause variance.

Throughout this work, the notation $L_f h(x)$ denotes the standard Lie derivative of the scalar function $h(x)$, with respect to the vector function $f(x)$. The notation $L_f^k h(x)$ denotes the k-th order Lie derivative of the scalar function $h(x)$, with respect to the vector function $f(x)$ and $L_g L_f^{k-1} h(x)$ denotes the mixed Lie derivative of the scalar function $h(x)$, with respect to the vector functions $f(x)$ and $g(x)$. Additionally, in order to prove stability of the closed-loop system, it is necessary to utilize the definition of input-to-state stability which uses functions of class $\mathcal{K}$ and $\mathcal{KL}$. Specifically, a function $\gamma : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{K}$ if it is continuous, increasing and zero at zero. A function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{KL}$ if, for each fixed t, the function $\beta(\cdot, t)$ is of class $\mathcal{K}$ and, for each fixed s, the function $\beta(s, \cdot)$ is non-increasing and approaches zero at infinity.

Definition 1:[22] *The system of Eq. 1 with $d(t) = 0$ is said to be input-to-state stable (ISS) with respect to u if there exist functions β of class $\mathcal{KL}$ and γ of class $\mathcal{K}$ such that for each $x_0 \in \mathbb{R}^n$ and for each measurable, bounded input $u(t)$, the solution to Eq. 1 exists for each $t \geq 0$ with $x(0) = x_0$ and satisfies*

$$|x(t)| \leq \beta(|x(0)|, t) + \gamma(||u||), \forall t \geq 0 \tag{2}$$

Under the assumptions of single-fault occurrence and available measurements for all of the process state variables, a data-based fault detection and isolation technique is proposed based on the structure of the system in closed-loop with a state feedback controller $u(x)$. The conditions (denoted as isolability conditions) under which this technique can be applied are provided. The main objective is to design a state feedback controller $u(x)$, such that the origin of the system of Eq. 1 in closed-loop with this controller is asymptotically stable under normal operating conditions, i.e., $d(t) = 0$, and that the closed-loop system satisfies the isolability conditions needed to apply the proposed FDI method. It is shown that for certain systems, the controller can be designed to guarantee that these conditions are satisfied, as well as to stabilize the closed-loop system.

Referring to the assumption that only a single fault occurs at any specific time instance, note that this is a reasonable assumption from a practical point of view. Namely, it is more likely that a single control actuator (e.g., an automatic valve) will fail at a particular time instance during the process operation than it is for two or more control actuators to fail at exactly the same time. Referring to the assumption that measurements of the process state variables are available, note that this assumption is made to simplify the development. In principle, this assumption can be relaxed using model-based state estimator design techniques for nonlinear systems (e.g.,[23]) to construct dynamic systems which yield estimates of the unmeasured states from the output measurements; however, the detailed development of the more general case is outside the scope of this work. Finally, we focus our attention on general actuator faults and disturbances and do not explicitly consider sensor faults since there is a plethora of techniques which address the issue of sensor fault detection (see, for example,[24–29]). With the general way in which the faults d_k are modeled, it is possible to represent virtually any fault because d_k is not restricted in any way and may be any time-varying signal; however, to achieve data-based detection and isolation of the fault d_k in the closed-loop system in the presence of noise in the state equations and measurements (noise which is introduced to model common-cause process variance), $d_k(t)$ should be sufficiently large in a way that is stated precisely in the section titled "Data-based isolation based on a fault signature".

In order to present the FDI method, it is necessary to define the incidence graph of a system and its reduced representation. The following definitions are motivated by standard results in graph theory.[30] This kind of graph-theoretic

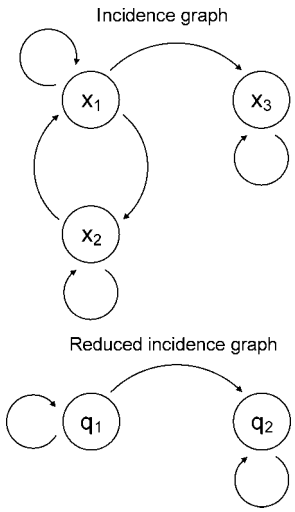

Figure 2. Incidence graph and reduced incidence graph for the system of Eq. 3.

analysis has been applied before in the context of feedback control of nonlinear systems (see, for example,[31]).

Definition 2: *The incidence graph of an autonomous system $\dot{x} = f(x)$ with $x \in \mathbb{R}^n$ is a directed graph defined by n nodes, one for each state, x_i, of the system. A directed arc with origin in node x_i and destination in node x_j exists if and only if $\frac{\partial f_j}{\partial x_i} \neq 0$.*

The incidence graph of a system shows the dependence of the time derivatives of its states. Figure 2 shows the incidence graph of the following system

$$\begin{aligned} \dot{x}_1 &= -2x_1 + x_2 + d_1 \\ \dot{x}_2 &= -2x_2 + x_1 + d_2 \\ \dot{x}_3 &= -2x_3 + x_1 + d_3 \end{aligned} \tag{3}$$

when $d_1 = d_2 = d_3 \equiv 0$. A path from node x_i to node x_j is a sequence of connected arcs that starts at x_i and reaches x_j. A path through more than one arc that starts and ends at the same node is denoted as a loop. States that belong to a loop have mutually dependent dynamics, and any disturbance affecting one of them also affects the trajectories of the rest. The mutual dependence of the dynamics of the states that belong to a given loop makes data-based isolation of faults that affect the system a difficult task. The following definition introduces the reduced incidence graph of an autonomous system. In this graph, the nodes of the incidence graph belonging to a given loop are united in a single node. This allows identifying which states do not have mutually dependant dynamics.

Definition 3: *The reduced incidence graph of an autonomous system $\dot{x} = f(x)$ with $x \in \mathbb{R}^n$ is the directed graph of nodes q_i, where $i = 1, \ldots, N$, that has the maximum number of nodes, N, and satisfies the following conditions:*

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

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

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

In the reduced incidence graph, states that belong to a loop in the incidence graph correspond to a single node. In this way, the states of the system are divided into subsystems that do not have mutually dependent dynamics; that is, there are no loops connecting them. The arcs of the graph indicate if there exists a state corresponding to the origin node that affects a state corresponding to the destination node. Note that the reduced incidence graph can be always obtained, but for strongly coupled systems, it may be defined by a single node; i.e., in the incidence graph there exists a loop that contains all the states of the system. In this case, data-based fault detection and isolation cannot be achieved using the proposed method. In the incidence graph of the system of Eq. 3 there is a loop that contains states x_1 and x_2. The reduced incidence graph of the system of Eq. 3 contains two nodes. Node q_1 corresponds to the states of the loop, that is, $X_1 = \{x_1, x_2\}$. Node q_2 corresponds to $X_2 = x_3$. Figure 2 shows the reduced incidence graph of the system of Eq. 3. It can be seen that in the reduced incidence graph there are no loops.

Remark 1: *In the process model of Eq. 1, process and sensor noise are not explicitly taken into account. However, noise is directly accounted for in the FDI method below by means of appropriate tolerance thresholds in the decision criteria for fault detection and isolation. The thresholds are generated on the basis of operating data and take into account both sensor and process noise, allowing for an appropriate FDI performance even if the process model and the measurements are corrupted by noise. To demonstrate this point, process and sensor noise are included in the two examples included in this work; see the simulation case studies section for details.*

Remark 2: *Due to the complex nature of faults in nonlinear systems, performing fault isolation with data-based methods alone generally leaves an ambiguous picture. On the other hand, it is possible to perform data-based fault isolation of simple faults using data-based FDI methods (this is discussed and demonstrated in[32] using contribution plots). In some cases, historical data from faulty operation will improve isolation capabilities of data-based methods; however, even with this information, due to overlap in the state-space of the regions corresponding to different faults and incomplete fault libraries, it still may be very difficult to isolate faults in nonlinear process systems.*

Data-based fault detection

Data-based methods for fault detection in multivariate systems are well established in statistical process monitoring. This section reviews a standard data-based method of fault detection that will be used in the context of the proposed FDI method.

A common approach to monitoring multivariate process performance is based upon the T^2 statistic introduced by Harold Hotelling.[33] This approach allows multivariate processes to be monitored for a shift in the operating mean $\bar{X}$, using a single test statistic that has a well-defined distribution. The true operating mean can be estimated from past history or

chosen based on the known process. Generally, the true process variance is unknown and must be estimated using sampled data. Hotelling's T^2 statistic tests the hypothesis that the current operating mean is the same as $\bar{X}$ with a certain degree of confidence $\alpha \cdot 100$ %. This is the multivariate generalization of Student's t-distribution. Consider a vector $X \in \mathbb{R}^n$ that is the average of m randomly sampled state measurements. Assuming that X has an n-variate normal distribution with an unknown variance-covariance matrix Σ, the T^2 statistic can be computed using the operating mean $\bar{X}$, estimated from historical data, and the estimated covariance matrix S, estimated from the m measurements contributing to X, as follows

$$T^2 = m(X - \bar{X})^T S^{-1}(X - \bar{X}). \tag{4}$$

Based on the assumption that the measurements in X are normally distributed, the T^2 statistic has the following distribution

$$T^2 \sim \frac{mn}{(m - n + 1)} F(n, m - n + 1) \tag{5}$$

where $F(n,m - n + 1)$ is the F statistic with n and $m - n + 1$ degrees of freedom. An upper control limit (UCL) for the T^2 statistic can be calculated by finding the value T^2_{UCL} on the T^2 distribution for which there is probability α of a greater or equal value occurring, that is, $P(T^2 \geq T^2_{UCL}) = \alpha$

$$T^2_{UCL} = \frac{mn}{(m - n + 1)} F_\alpha(n, m - n + 1) \tag{6}$$

Note that T^2 is a positive quantity and has no lower control limit. With this definition of the UCL, α is the probability of a type I error, or false alarm. This implies that at least once every $1/\alpha$ samples there is expected to be a false alarm or, in other words, the average run length (ARL) is equal to $1/\alpha$. Decreasing the value of α will increase the ARL and thus decrease the likelihood of a Type I error. However, this decreases the power of the statistical test. Power is measured as $1 - \beta$, where β is the probability of a Type II error, which is that a failure has occurred, but is not detected by the test. Because the focus of this work is on failures that cause significant change in the operating point, and assumes a persistent state of failure before declaring a fault, finding the balance between the statistical power of the test, and the likelihood of a false alarm is not considered (see Remark 6 for further discussion on this issue).

In addition to the method presented previously, other methods using Hotelling's T^2 statistic have been established which deviate from the strict definition of the test. In particular, due to the nature of continuous chemical processes, it is sometimes convenient to estimate S from historical data. This assumes that data from future observations will have similar covariance. Methods that use historical data generally have two phases of operation. Phase 1 is for testing during fault-free operation to verify that the process is in control. The following UCL is used for the T^2 statistic in Phase 1[34]

$$T^2_{UCL} = \frac{n(h - 1)(m - 1)}{hm - h - n + 1} F_\alpha(n, hm - h - n + 1) \tag{7}$$

where h is the number of m-sized samples used to evaluate the covariance matrix S from historical data. Phase 2 is for the normal monitoring of a process for faults with the following control limit

$$T^2_{UCL} = \frac{n(h + 1)(m - 1)}{hm - h - n + 1} F_\alpha(n, hm - h - n + 1) \tag{8}$$

Note that when h is large, these limits are nearly identical.

In the context of process monitoring, it is often convenient to use a sample size of $m = 1$ where individual observations are monitored (i.e.,[34,35]). This is commonly used in data-based fault detection and isolation methods (see, for example,[11,14,17,34,35]). In this scenario, the UCL becomes

$$T^2_{UCL} = \frac{(h^2 - 1)n}{h(h - n)} F_\alpha(n, h - n) \tag{9}$$

where h is now the total number of historical measurements used to evaluate the covariance matrix S. In the simulation section of this work, we use both the traditional method of Hotelling's T^2 statistic by monitoring sampled data sets of size m with the corresponding UCL in Eq. 6, where the estimated covariance matrix, S, is evaluated at each step from the m observations, as well as the single observation approach using the control limit from Eq. 9 and the appropriate S based on h historical observations.

The T^2 statistic is widely used for fault detection purposes in multivariate processes and can be used for both the full state vector and the transformed state vector in the reduced PCA space. The T^2 statistic for the full state vector does not provide additional information that can be used for isolating the underlying cause of a fault. In some cases, the T^2 statistics of certain subgroups of the state vector (or functions of it) can be monitored in addition to the full vector to assist in fault isolation. In this situation, the process is decomposed into subsystems, generally based on function, structure and/or behavior allowing fault detection and isolation techniques to be applied to subgroups of sensor measurements. The context of the decomposition itself narrows the detection and isolation focus allowing the application of the T^2 statistic for localized detection. As the focus of the process decomposition context narrows, detection approaches isolation. If the focus is narrowed to a particular process component then detection and isolation become one and the same. Examples of work in which decompositions are used for localized FDI are in[36] and[37]. This idea for data-based isolation using the T^2 statistic for each subsystem is also utilized in the context of the method proposed in the next section.

Remark 3: *Note that the fault detection methods presented in this section will naturally account for process and sensor noise. Thus, the T^2 statistic, which scales the process data by the inverse of the covariance matrix, will be tolerant to the normal amount of process and measurement variation without signalling a fault. However, if the variance of the system were to change during the course of operation, this could signal a fault in the system when using a covariance matrix, S, estimated from historical data. This type of fault will generally not be declared as this work requires a fault large enough to cause persistent failure as discussed in Remark 6.*

Data-based isolation based on a fault signature

Data-based isolation of the underlying cause of a faulty process behavior is, in general, a difficult problem which strongly depends on the structure of the closed–loop system. In systems with multiple possible faults, one-dimensional (1-D) statistics, such as the T^2 statistic presented in the previous section, cannot be used to perform fault isolation when applied globally (i.e. to the entire state vector). To understand this point in the context of a specific example, consider the system of Eq. 3. It can be seen based on the structure of the system, that a fault in d_1, or a fault in d_2 will affect the state trajectories of all three states of the system. In this case, the fault will be readily detected, but the T^2 statistic and the state trajectories will not provide further information with which one can reliably determine whether a fault in d_1 or d_2 had occurred. However, if a failure in d_3 were to occur, it can be seen from the system equations that only the state trajectory of state 3 would be affected. With this particular structure, which is that there is no path from the affected state x_3, to x_1 or x_2, it is possible to isolate the fault d_3 by observing the affected state trajectories at the time of the failure. Thus, it can be seen that under certain conditions, isolation is possible.

The example given previously motivates introducing a set of isolability conditions which guarantee that fault isolation is possible based on the state trajectories affected by a given fault. This will also provide guidelines for the design of control laws that guarantee that these conditions are satisfied. In order to precisely state these conditions, the isolability graph of an autonomous system is defined below.

Definition 4: *The isolability graph of an autonomous system $\dot{x} = f(x,d)$ with $x \in \mathbb{R}^n$, $d \in \mathbb{R}^p$ is a directed graph made of the N nodes of the reduced incidence graph of the system $\dot{x} = f(x,0)$ and p additional nodes, one for each possible fault d_k. The graph contains all the arcs of the reduced incidence graph of the system $\dot{x} = f(x,0)$. 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 $\frac{\partial f_i}{\partial d_k} \neq 0$ for some $x_i \in X_j$.*

Figure 3 shows the isolability graph of the system of Eq. 3. The isolability graph of an autonomous system subject to p faults shows, in addition to the incidence arcs of the reduced incidence graph, which loops of the system are affected by each possible fault. Based on this graph, it is possible to define the signature of a fault.

Definition 5: *The signature of a fault d_k of an autonomous system subject to p faults $\dot{x} = f(x,d)$ with $x \in \mathbb{R}^n$, $d \in \mathbb{R}^p$ 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 $i-th$ component of W^k, denoted W^k_i, is one if there exists a path in the isolability graph from the node corresponding to fault k to the node q_i corresponding to the set of states X_i, or zero otherwise.*

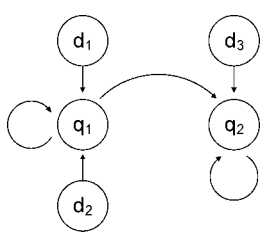

Figure 3. Isolability graph for the system of Eq. 3.

The signature of a fault indicates the set of states that are affected by the fault. If each of the corresponding signatures of the faults is different, then it is possible to isolate the faults using a data-based fault-detection method. Faults d_1 and d_2 in the system of Eq. 3 have the same signature, $W^1 = [1\ 1]^T$, because d_1 and d_2 both directly affect q_1, and there is a path from q_1 to q_2. This implies that both faults affect the same set of states. Therefore, it is not possible to distinguish between them based on the signature. On the other hand, the signature of fault d_3 in the same system is $W^1 = [0\ 1]^T$, because there is no path to q_1 from q_2, which is the node directly affected by d_3. This implies that the states corresponding to node q_1 are effectively decoupled from fault d_3 . This allows distinguishing between a fault in d_3 and a fault in either d_1 or d_2 in the system of Eq. 3, based on the profiles of the state trajectories.

In this work, we propose to design and implement appropriate feedback laws in the closed-loop system that induce distinct signatures for specific faults to allow their isolation. In the next section, we present methods for the design of controllers that enforce an isolable structure in the closed-loop system. In the remainder of this section, we discuss the issue of determination of the fault signatures for the closed-loop system in the absence and presence of noise in the differential equations and measurements. This determination of the fault signature from process measurements will also lead to a characterization of the type of fault signals $d_k(t)$, for which isolation can be achieved when common-cause variation is considered for the closed-loop system (caused by the introduction of noise in the differential equations and measurements). Specifically, referring to the deterministic closed-loop system (i.e., no noise is present in the states or in the measurements), the signature of the fault W^k, for any time-varying signal $d_k(t)$, can be computed directly from the isolability graph, and is independent of the type of time-dependence of $d_k(t)$. In other words, the signal $d_k(t)$ need not satisfy any conditions for its signature to be computed. Once the fault signature is computed, then fault isolation is immediate in the deterministic case by checking whether or not the signature of the system corresponds to a defined fault. However, in the presence of noise in the states and measurements, $d_k(t)$ has to be sufficiently large to have an effect that leads to operation of the process states outside of the range expected, due to common-cause variance. Additionally, this must happen for a sufficiently large period of time to distinguish the fault, based on its signature, from other causes that can lead to violations of the upper control limit for a small period of time. Specifically in the proposed method, the following statistics based on the state trajectories of the system of Eq. 1 in closed-loop with a given feedback controller $u(x)$ in the presence of noise in the states and measurements are monitored:

- T^2 statistic based on the full state x with upper control limit T^2_{UCL}.
- T^2_i statistic with $i = 1, \ldots, N$ based on the states $x_j \in X_i$, where X_i are the sets of states corresponding to each one of the nodes of the reduced incidence graph. To each T^2_i statistic a corresponding upper control limit T^2_{UCLi} is assigned.

The fault detection and isolation procedure then follows the steps given below:

1. A fault is detected if $T^2(t) > T^2_{UCL}\,\forall t\, t_f \le t \le T_P$, where T_P is chosen so that the window $T_P - t_f$ is large enough to allow fault isolation with a desired degree of confidence, and depends on the process time constants and potentially on available historical information of the process behavior.

2. A fault that is detected can be isolated if the signature vector of the fault $W(t_f, T_P)$ can be built as follows

$$T_i^2(t) > T^2_{UCLi}\,\forall t\, t_f \le t \le T_P \rightarrow W_i(t_f, T_P) = 1$$

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

In such a case, fault d_k is detected at time T_P if $W(t_f, T_P) = W^k$. If two or more faults are defined by the same signature, isolation between them is not possible on the basis of the fault signature obtained from the isolability graph.

The conditions in steps 1 and 2 state that the fault $d_k(t)$ has to be sufficiently large in order to be detected and isolated.

Remark 4: *States to which there is not a path from a given fault node to the corresponding subsystem node in the isolability graph are not affected by changes in the value of d_k; thus, they are effectively decoupled from the fault d_k. The FDI method can be applied if the signatures of the closed-loop system faults are different. This is the isolability condition. Note that the signature of a fault depends on the structure of the closed-loop system, in particular, on the isolability graph. For example, if the reduced incidence graph has only one node, isolation is not possible. In the following section, we propose to design the feedback controller $u(x)$ to guarantee that the reduced incidence graph of the closed-loop system has more than one node, that there exist faults with different signatures and that the origin of the closed-loop system is asymptotically stable.*

Remark 5: *The concept of the "signature of a fault" employed in this section can be generalized in the context of monitoring the evolution of a set of variables defined as functions of the state. In particular, given any variable change, the isolability graph can be obtained in the new state space and the signature defined on the basis of the new state variables. In the next section, an example of this idea is provided for input/output linearizable, nonlinear systems where the signature of a fault is given in a partially linearized state-space.*

Remark 6: *The upper control limit is chosen taking into consideration common-cause variance, including process and sensor noise, in order to avoid false alarms. Thus, small disturbances or failures may go undetected if the magnitude and effect of the disturbance is similar to that of the inherent process variance. For this reason, it was stated in the fault detection and isolation procedure that a fault d_k must be "sufficiently large" in order for $T_i^2(t)$ to exceed the threshold $T^2_{UCLi}\,\forall t\, t_f \le t \le T_P$. It is assumed that if a fault d_k is not large enough to cause $T_i^2(t)$ to exceed the threshold $T^2_{UCLi}\,\forall t\, t_f \le t \le T_P$ (where t_f is the time in which $T_i^2(t_f) \ge T^2_{UCL}$ for the first time) then the fault is not "sufficiently large" and its effect on the closed-loop system, from the point of view of faulty behavior, is not of major consequence. Therefore, such a d_k is not considered to be a fault. However, it should be noted that a fault d_k that is large enough to cause the T^2 derived from the full state vector, x, to cross the upper control limit signaling a fault may not be large enough to signal a fault in all of the affected subgroups. In this case, it is possible to have a false isolation. This is investigated in the simulation case studies section. Finally, the condition $T_i^2(t) \not> T^2_{UCLi}\,\forall t\, t_f \le t \le T_P$ allows violation of the UCL in the full state vector and individual subsystems, due to other causes for a short period of time. However, such violations do not modify the fault signature $W(t_f, T_P)$ if T_P is chosen to be sufficiently large.*

Remark 7: *We would like to point out that the isolability conditions are not restrictive from the practical point of view that it is generally possible to induce at least some degree of decoupling within any given system. For example, any system with a relative degree $r \le n$ can be decoupled using the method presented in the section on feedback linearization. Systems, such as this are very common in practice. However, while the isolability conditions can generally be met for one or a few faults in almost any system, it can be difficult to isolate all faults within any given system using this method alone.*

Controller Enhanced Isolation

Enforcing an isolable closed-loop system structure through controller design

In general, control laws are designed without taking into account the FDI scheme that will be applied to the closed-loop system. We propose to design an appropriate nonlinear control law to allow isolation of given faults using the method proposed in the previous section, by effectively decoupling the dependency between certain process state variables to enforce the fault isolability conditions in the closed-loop system. As explained in the previous section, this requires that the structure of the isolability graph of the closed-loop system be such that at least one or more faults be partially decoupled from one or more nodes on the isolability graph. The main idea is to obtain an isolability graph of the closed-loop system which provides a different signature for each fault. This key requirement can be accomplished using a variety of nonlinear control laws. In general providing a systematic procedure to design a controller that guarantees both closed-loop stability and satisfaction of the isolability conditions for any nonlinear process is not possible. The specific form of the controller depends on the structure of the open-loop system and such a controller may not exist. One general procedure that can be followed, however, is to decouple a set of states from the rest. Recursively applying this decoupling technique, appropriate closed-loop isolability graphs can be obtained in certain cases. As an example of this design approach, we first provide a controller that can be applied to nonlinear systems with the following state space description

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + f_{12}(x_1, x_2) + g_1(x_1, x_2)u + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2 \end{aligned} \tag{10}$$

where $x_1 \in \mathbb{R}$, $x_2 \in \mathbb{R}^n$, $u \in \mathbb{R}$, and $g_1(x_1, x_2) \neq 0$ for all $x_1 \in \mathbb{R}$, $x_2 \in \mathbb{R}^n$. With a state feedback controller of the form

$$u(x_1,x_2) = -\frac{f_{12}(x_1,x_2) - v(x_1)}{g_1(x_1,x_2)} \tag{11}$$

the closed-loop system takes the form

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + v(x_1) + d_1 \\ \dot{x}_2 &= f_2(x_1,x_2) + d_2 \end{aligned} \tag{12}$$

where $v(x_1)$ has to be designed in order to achieve asymptotic stability of the origin of the x_1 subsystem when $d_1 = 0$. Note that explicit stabilizing control laws that provide explicitly-defined regions of attraction for the closed-loop system have been developed using Lyapunov techniques for specific classes of nonlinear systems, particularly input-affine nonlinear systems; the reader may refer to[38,39,40,23] for results in this area. The origin of the closed-loop system is asymptotically stable if $\dot{x}_2 = f_2(x_1,x_2)$ is input-to-state stable with respect to x_1. In this case the proposed controller guarantees asymptotic stability of the closed-loop system, as well as different signatures for faults d_1 and d_2. Note that the reduced incidence graph is defined by two nodes corresponding to both states, and the signatures are given by $W^1 = [1\ 1]^T$ and $W^2 = [0\ 1]^T$.

The controller design method discussed previously provides a basic tool for obtaining control laws that provide closed-loop stability and satisfy the isolability constraints. The main idea is to force decoupling in a first controller design step (in this case $u(x)$), and then ensure closed-loop stability in a second (in this case $v(x)$). Additionally, the next section provides a systematic controller design for a particular class of nonlinear systems. This procedure along with the class of systems under consideration are introduced in the following subsection.

Input/output linearizable nonlinear systems

In this subsection, we focus on a class of process systems modeled by single-input single-output nonlinear systems with multiple possible faults which have the following state-space description

$$\begin{aligned} \dot{x} &= f(x) + g(x)u + \sum_{k=1}^{p} w_k(x)d_k \\ y &= h(x) \end{aligned} \tag{13}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}$ is the input, $y \in \mathbb{R}$ is the controlled output, and $d_k \in \mathbb{R}$ represents a possible fault. It is assumed that f, g, h and w_k are sufficiently smooth functions, that is, all necessary derivatives exist and are continuous functions of x, 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 disturbances. As before, this definition of d_k is not restricted by value and may be time-varying, and, thus, it can model a very broad class of faults. The system has an equilibrium point at $x = 0$ when $u(t) = d_k(t) \equiv 0$ and $h(0) = 0$. Note that in general this equilibrium point may correspond to a given set-point of the output.

The main control objective is to design a feedback control law $u(x)$, such that the origin is an asymptotically stable equilibrium point of the closed-loop system, and, moreover, the closed-loop system satisfies the isolability conditions. Feedback linearization is used to accomplish this task. First, it is necessary to review the definition of the relative degree of the output y, with respect to the input u, in the system of Eq. 13.

Definition 6:[41] *Referring to the system of Eq. 13, the relative degree of the output y, with respect to the input u, is the smallest integer, $r \in [1,n]$, for which*

$$\begin{aligned} &L_g L_f^i h(x) = 0,\ i = 0,\ldots,r-2 \\ &L_g L_f^{r-1} h(x) \neq 0. \end{aligned}$$

A system with an input relative degree $r \leq n$ is input-output linearizable. If $r = n$ the entire input-state dynamics can be linearized. If $r < n$, the feedback controller can be chosen so that a linear input-output map is obtained from an external input v, to the output y, even though the state equations are only partially linearized (see also,[41]). To be specific, if the system of Eq. 13 has input relative degree $r < n$, then there exists a coordinate transformation (see[41]) $(\zeta,\ \eta) = T(x)$ such that the representation of the system of Eq. 13 with $d_k = 0$ for all $k = 1,\ \ldots\ ,\ p$ (that is, the system without faults), in the $(\zeta,\ \eta)$ coordinates, takes the form

$$\begin{aligned} \dot{\zeta}_1 &= \zeta_2 \\ &\vdots \\ \dot{\zeta}_{r-1} &= \zeta_r \\ \dot{\zeta}_r &= L_f^r h(x) + L_g L_f^{r-1} g(x) u \\ \dot{\eta}_1 &= \Psi_1(\zeta,\eta) \\ &\vdots \\ \dot{\eta}_{n-r} &= \Psi_{n-r}(\zeta,\eta) \end{aligned} \tag{14}$$

where $y = \zeta_1,\ x = T^{-1}(\zeta,\eta),\ \zeta = [\zeta_1,\ldots\zeta_r]^T$ and $\eta = [\eta_1,\ldots,\eta_{n-r}]^T$. Choosing $u(x)$ in an appropriate way, the dynamics of ζ can be linearized and controlled properly using linear control theory. The stability of the closed-loop system, however, can only be assured if the inverse dynamics $(\dot{\eta} = \Psi(\zeta,\eta))$ satisfy additional stability assumptions. In particular, the inverse dynamics must be input-to-state stable with respect to ζ. If this is the case, then an appropriate control law can be designed for the input-output subsystem that guarantees stability of the entire closed-loop system. In the following theorem, we review one example of an input-output feedback-linearizing controller. The controller presented, under the assumption of no faults, guarantees asymptotic stability of the closed-loop system.

Theorem 1:[41] *Consider the system of Eq. 13 with $d_k = 0$ for all $k = 1,\ \ldots\ ,\ p$ under the feedback law*

$$u(x) = \frac{1}{L_g L_f^{r-1} h(x)} \left[K T_\zeta(x) - L_f^r h(x) \right] \tag{15}$$

where $\zeta = T_\zeta(x)$. Assume K is chosen such that the matrix $A + BK$ has all of its eigenvalues in the lefthand side of the complex plane where

$$A = \begin{bmatrix} 0_{r-1} & I_{r-1} \\ 0 & 0_{r-1}^T \end{bmatrix}, \quad B = \begin{bmatrix} 0_{r-1} \\ 1 \end{bmatrix}.$$

I_{r-1} is the $(r-1) \times (r-1)$ identity matrix, and 0_{r-1} is the $(r-1) \times 1$ zero vector. Then, if the dynamic system $\dot{\eta} = \Psi(\zeta, \eta)$ is locally input-to-state stable (ISS), with respect to ζ, the origin of the closed-loop system is locally asymptotically stable.

We prove that under certain assumptions, if the state-feedback law given in Eq. 15 is used, then the faults of system of Eq. 13 can be isolated into two different groups: those that affect the output and those that do not affect the output. The main idea is that the isolability graph of the closed-loop system in the coordinates (ζ, η) provides different signatures for the faults depending on their relative degree, which is defined later (this definition was introduced in[42] in the context of feedforward/feedback control of nonlinear systems with disturbances, but it is employed here to address a completely different issue).

Definition 7:[42] *Referring to the system of Eq. 13, 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*

$$\begin{aligned} &L_{w_k} L_f^i h(x) = 0, \ i = 0, \ldots, \rho_k - 2 \\ &L_{w_k} L_f^{\rho_k - 1} h(x) \neq 0. \end{aligned} \tag{16}$$

The definition of the relative degree of a fault is analogous to that of the relative degree of the input, but instead of relating the output 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.

To show this point, taking into account Definitions 6 and 7, there exists (see[41]) a coordinate transformation $(\zeta, \eta) = T(x)$, such that the representation of the system of Eq. 13 with $d_j = 0$ for all $d_j \neq d_k$ (that is, the system subject only to fault d_k), in the (ζ, η) coordinates, takes the form (for $\rho_k < r$)

$$\begin{aligned} \dot{\zeta}_1 &= \zeta_2 \\ &\vdots \\ \dot{\zeta}_{r-1} &= \zeta_r \\ \dot{\zeta}_r &= L_f^r h(x) + L_g L_f^{r-1} h(x) u \\ \dot{\eta}_1 &= \Psi_1(\zeta, \eta, d_k) \\ &\vdots \\ \dot{\eta}_{n-r} &= \Psi_{n-r}(\zeta, \eta, d_k) \end{aligned}$$

where $y = \zeta_1, \ x = T^{-1}(\zeta, \eta), \ \zeta = [\zeta_1, \ldots, \zeta_r]^T$ and $\eta = [\eta_1, \ldots, \eta_{n-r}]^T$. Following the definition of the state-feedback law of Eq. 15, the following state-space representation is obtained for ζ

$$\dot{\zeta} = (A + BK)\zeta$$

This dynamical system is independent of d_k. Therefore, the trajectory of the output y is independent of the fault d_k. This result, however, does not hold if the relative degree ρ_k of the fault d_k is equal to or smaller than r. In this case, the coordinate change does not eliminate the dependence of the output on the fault d_k. Applying the same coordinate change $(\zeta, \eta) = T(x)$, the dynamics of the system of Eq. 13 with $d_j = 0$ for all $d_j \neq d_k$ (that is, the system subject to fault d_k), in the (ζ, η) coordinates, takes the form

$$\begin{aligned} \dot{\zeta}_1 &= \zeta_2 + \Phi_1(d_k) \\ &\vdots \\ \dot{\zeta}_{r-1} &= \zeta_r + \Phi_{r-1}(d_k) \\ \dot{\zeta}_r &= L_f^r h(x) + L_g L_f^{r-1} h(x) u + \Phi_r(d_k) \\ \dot{\eta}_1 &= \Psi_1(\zeta, \eta, d_k) \\ &\vdots \\ \dot{\eta}_{n-r} &= \Psi_{n-r}(\zeta, \eta, d_k) \end{aligned}$$

where $y = \zeta_1, \ x = T^{-1}(\zeta, \eta), \ \zeta = [\zeta_1, \ldots, \zeta_r]^T$ and $\eta = [\eta_1, \ldots, \eta_{n-r}]^T$. In this case, when the fault occurs, the output is affected. In summary, if controller of Eq. 15 is used, the possible faults of the system of Eq. 13 are divided into two groups, each with a different signature. When a fault occurs, taking into account whether the trajectory of the output is affected or not, one can determine which group the fault belongs to. Note that if only two faults are defined and $\rho_1 \leq r$ and $\rho_2 > r$, then the fault is automatically isolated.

Remark 8: *The feedback linearizing control laws presented in this subsection are designed to enforce a linear input/output structure in the closed-loop system. Although the external input, $v = K\zeta$, may be designed to stabilize the resulting linear closed-loop system optimally, the total control action u is not optimal with respect to a closed-loop performance index (cost) that includes a penalty on the control action.*

Simulation Case Studies

In this section, the proposed approach for integrated FDI and controller design is applied to two chemical process examples. First, we consider a CSTR and utilize feedback linearization to design a nonlinear controller that yields a closed-loop system for which the isolability conditions hold. Second, we consider a polyethylene reactor and design a nonlinear control law, based on the general method of the first subsection under "Controller enhanced isolation", that yields a closed-loop system for which the isolability conditions hold. In both cases, we demonstrate that data-based fault detection and isolation is achieved under feedback control laws that enforce isolability in the closed-loop system, an outcome that is not possible, in general, when other feedback control designs that do not enforce the required structure are used.

Application to a CSTR example

The first 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

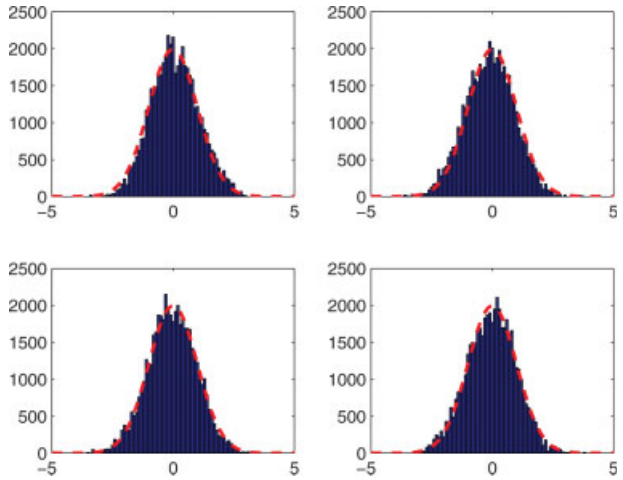

Figure 4. CSTR example.

Distribution of normalized, fault-free operating data compared with a normal distribution of the same mean and variance. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

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

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

$$r_1 = k_{10}e^{\frac{-E_1}{RT}}C_A, \quad r_{-1} = k_{-10}e^{\frac{-E_{-1}}{RT}}C_B$$
$$r_2 = k_{20}e^{\frac{-E_2}{RT}}C_B, \quad r_{-2} = k_{-20}e^{\frac{-E_{-2}}{RT}}C_C$$

where k_{i0} is the pre-exponential factor, and E_i is the activation energy of the i^{th} 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

$$\begin{aligned}
\dot{C}_A &= \frac{F}{V}(C_{A0} - C_A) - r_1 + r_{-1} + d_1 \\
\dot{C}_B &= -\frac{F}{V}C_B + r_1 - r_{-1} - r_2 + r_{-2} \\
\dot{C}_C &= -\frac{F}{V}C_C + r_2 - r_{-2} \\
\dot{T} &= \frac{F}{V}(T_0 - T) + \frac{(-\Delta H_1)}{\rho c_p}(r_1 - r_{-1}) \\
&\quad + \frac{(-\Delta H_2)}{\rho c_p}(r_2 - r_{-2}) + u + d_2
\end{aligned} \tag{17}$$

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, d_1 and d_2 denote faults/disturbances and $u = Q/\rho c_p$ is the manipulated input, where Q is the heat input to the system.

The system of Eq. 17 is modeled with sensor measurement noise and autoregressive process noise. The sensor measurement noise was generated using a zero-mean normal 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 Eq. 17. Because of the dynamic nature of the process and the autocorrelated process noise, it is expected that the state trajectories will be serially correlated. Although the distribution of the state measurements in open-loop operation may not be normal (Gaussian), the influence of feedback control is such that the measurements under closed-loop operation are approximately normal (see[34]). Figure 4 shows the distribution of the state measurements of the closed-loop system of Eq. 17 under the feedback-linearizing control law in fault-free operation over a long period of time compared with a Gaussian distribution. Note that although the long-term distribution is approximated well by a normal distribution, this will not hold true for short-term operation, a point that will affect the choice of test statistic to be applied.

The controlled output y, of the system is defined as the concentration of the desired product C_C. This particular definition of the output, while meaningful from the point of view of regulating the desired product concentration, will be also useful in the context of fault isolation. We consider only faults d_1 and d_2, which represent undesired changes in C_{A0} (disturbance) and T_0/Q (disturbance/actuator fault), respectively. For example, if C_{A0} changes by ΔC_{A0} then $d_1 = \frac{F}{V}\Delta C_{A0}$. These changes may be the consequence of an error in external control loops. In this system, the input u appears in the temperature dynamics, and is of relative degree 2 with respect to the output $y = C_C$. The fault d_1 appears only in the dynamics of C_A, and is of relative degree 3 with respect to the output $y = C_C$. Finally, fault d_2 is of relative degree 2. The values for the parameters of the process model are given in Table 1.

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

$$C_{Cs} = 0.9471\frac{kmol}{m^3}, \; T_s = 312.6K, \; u_s = 0K/s \tag{18}$$

where the subscript s refers to the steady state value at equilibrium. To this end, we consider two different feedback con-

Table 1. CSTR Example Process Parameters

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

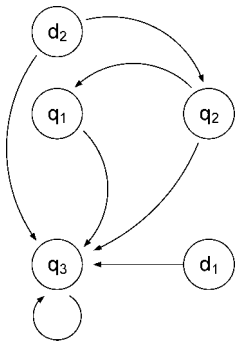

Figure 5. Isolability graph for the system of Eq. 17. $q_1 = \{\zeta_1\}$, $q_2 = \{\zeta_2\}$ and $q_3 = \{\eta\}$.

trollers: a controller based on feedback linearization and a proportional controller (it is important to point out that the conclusions of this simulation study would continue to hold if the proportional controller is replaced by proportional-integral-derivative control, model-predictive control or any other controller that does not achieve decoupling of the controlled output, $y = C_C$, from the fault d_1, in the closed-loop system). The feedback-linearizing controller takes the form of Eq. 15 with

$$K = [-1 \; -1]$$

Note that the state variables are shifted so that the origin represents the desired set point. The proportional controller takes the form

$$u = (T_s - T)$$

In the closed-loop system operating under the feedback-linearizing control law, according to the results of the previous section, faults with a relative degree higher than that of the input (i.e., $\rho_k > 2$) will not affect the output in the event of a failure. Therefore, because d_1 has a relative degree of 3, it will not affect the behavior of the output. Conversely, because fault d_2 is of relative degree 2, its effect cannot be decoupled from the output. This result is illustrated in Figure 5. The nodes in this figure are $q_1 = \zeta_1$, $q_2 = \zeta_2$ and $q_3 = \{\eta_1, \eta_2\}$, where $\zeta_1 = C_C$, $\zeta_2 = \zeta_1$ and $\{\eta_1, \eta_2\}$ are combinations of C_A, C_B and T such that $[\zeta;\eta] = T(C_A, C_B, C_C, T)$ is an invertible transformation. The isolability graph of this system in the transformed coordinates shows that each of the states in the ζ subsystem is a separate node, and that the states in the η subsystem form a single additional node. Although there are multiple nodes in the ζ subsystem, because each is directly affected by d_1, the effect is the same as if they were a single node. Moreover, since there is no path from the η subsystem node to any of the ζ subsystem nodes, and d_2 only affects the η subsystem node directly, the signatures for faults d_1 and d_2 will be unique and thus isolable. Additionally, it should be noted that the trajectory of ζ_1 follows that of the output, C_C, and the ζ subsystem is not affected by the other states. Thus, monitoring the output C_C, as one subsystem, and the remaining states as a second subsystem is equivalent to monitoring the subsystems formed in the transformed space.

The isolability property stated previously, however, does not hold for the closed-loop system under proportional control. In that case, when a fault occurs (whether it be d_1 or d_2), the output is affected by the presence of the fault. These theoretical predictions were tested by simulating the system of Eq. 17 in closed-loop under both proportional control and feedback-linearizing control. In both cases, the system was initially operating at the steady-state of Eq. 18, with a failure appearing at time $t = 0.5$ *hr*.

Based on the structure of the closed-loop system under feedback-linearizing control, the state vector was divided into two subvectors, $X_1 = \{C_C\}$ and $X_2 = \{C_A, C_B, T\}$ as discussed earlier. Hotelling's statistic (Eq. 4) for the full state vector (T^2), and each of the subvectors (T_1^2 and T_2^2) were monitored to detect and evaluate the presence of a fault. Detection was performed based on the T^2 statistic violating the upper control limit T^2_{UCL} defined in Eq. 6 using $m = 10$ randomly sampled measurements at intervals of $\Delta t = -ln(\xi)/W_s$ where ξ is a uniformly distributed random variable from 0 to 1, and W_s is the sample rate of one sample per minute. Similarly, isolation was done based on the detection of a violation of the UCL in T_1^2 and T_2^2, and the known fault signatures computed from the isolability graph $W_1 = [0\ 1]$ and $W_2 = [1\ 1]$. Additionally, the same data was tested with a sample size $m = 1$, and the upper control limits as defined in Eq. 9. In this case a much higher sampling rate was used (20 samples per minute), because there was no need to capture a larger time scale (see Remark 9). As described in the section on data-based fault detection, the method of single observations relies on the covariance matrix S calculated from historical data under common-cause variation only, and the method of $m = 10$ observations uses a covariance matrix S obtained from the new observations being analyzed in each sample.

The closed-loop system was simulated under proportional and feedback-linearizing control. Noise in the states and measurements was included as discussed earlier. A fault in d_1 was introduced as a step change of magnitude 1 $kmol/m^3$ *s*. Figure 6 shows the state trajectories for the closed-loop system under the proportional and the feedback-linearizing controller. Figure 7 shows the T^2 statistics for the system under feedback-linearizing control, calculated from $m = 10$ randomly sampled state measurements using the T^2_{UCL} from Eq. 6 with confidence level $\alpha = 0.001$, and degrees of freedom (3, 8) for T_1^2, (1,10) for T_2^2 and (4,7) for T^2. Also, the data is prone to greater false alarms, because over the short window of 10 observations the trajectories are much more serially correlated, and can be susceptible to almost singular covariance matrices, leading to large T^2 values for small deviations from the mean. Figure 8 shows the T^2 statistic for the same results, calculated instead from individual observations ($m = 1$) using the UCL from Eq. 9 with confidence level $\alpha = 0.01$ and degrees of freedom (3,2997), (1,2999) and (4,2996) for T_1^2, T_2^2 and T^2, respectively. Observe that the moving average of $m = 10$ observations causes a delay in the fault detection time compared to the case where $m = 1$.

In both methods, the T^2 statistic exceeds the upper control limit T^2_{UCL}, signaling a failure, around $t = 0.5$ *hr*. The T_1^2 value remained below its threshold, while the T_2^2 value

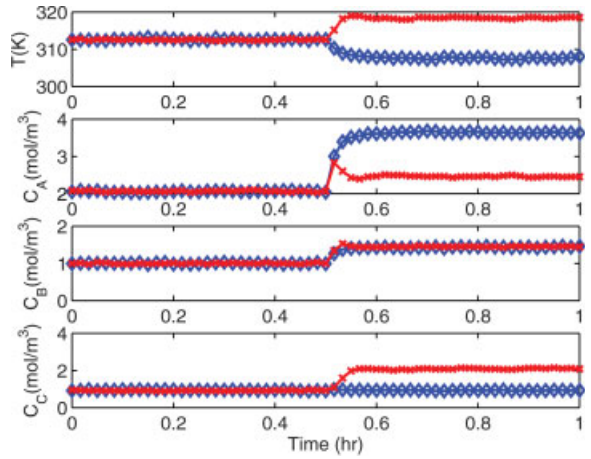

Figure 6. CSTR example.

State trajectories of the closed-loop system under feedback-linearizing (◇) and P (×) control with a fault d_1 at t = 0.5 *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

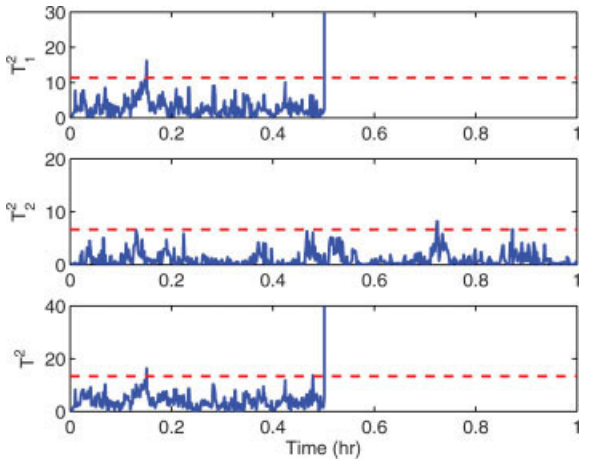

Figure 8. CSTR example.

Closed-loop system under proportional control with sample size m = 10. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at t = 0.5 *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

exceeded T^2_{UCL2}. This shows that the output (subvector 1) was not affected by the failure. In the case of proportional control with a failure in d_1 the T^2 statistic accurately shows that the failure occurred around time t = 0.5 *hr*. Figures 9 and 10 show the results m = 10 and m = 1, respectively. However, in this simulation, all of the state trajectories were affected by the failure resulting in values of T_1^2 and T_2^2 that exceeded the upper control limits. In the case of a failure in d_2, introduced as a step change of magnitude 1 *K/s* both proportional control and feedback-linearizing control show failures in T^2 at t = 0.5 *hr*, as well as in both subsystems T_1^2 and T_2^2 see Figures 11 and 12. Looking at T_1^2 and T_2^2 in Figures 9 and 11, it is clear that fault d_1 did not affect the output, whereas d_2 did. In this situation, where only one fault in each group is considered, it is possible to successfully identify the failure in Figure 9 as d_1. However, for proportional control, all of the states were affected by each failure (see Figures 10 and 12) leaving an unclear picture as to the cause of the fault.

A Monte Carlo simulation study was performed by randomly varying the fault sizes, and the amount of variance in the process and measurement noise in order to verify that the method performs as expected in a broad range circumstances. In total, 500 simulations were run, each with uniformly distributed random values of fault size, process noise variance and sensor noise variance. Only a fault in d_1 was considered with values ranging from 0 to 3 *kmol/m*^{3} *s*. The standard deviation of the process noise σ_p, and the sensor noise σ_m ranged from 0 to twice the values reported in Table 2. A single observation T^2 statistic was used with the associated

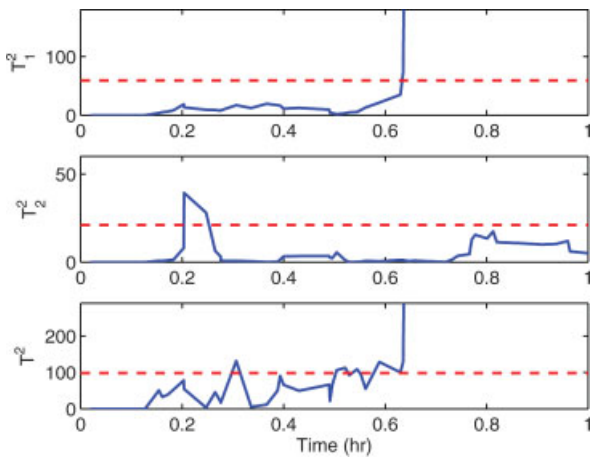

Figure 7. CSTR example.

Closed-loop system under feedback-linearizing control with sample size m = 10. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at t = 0.5 *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

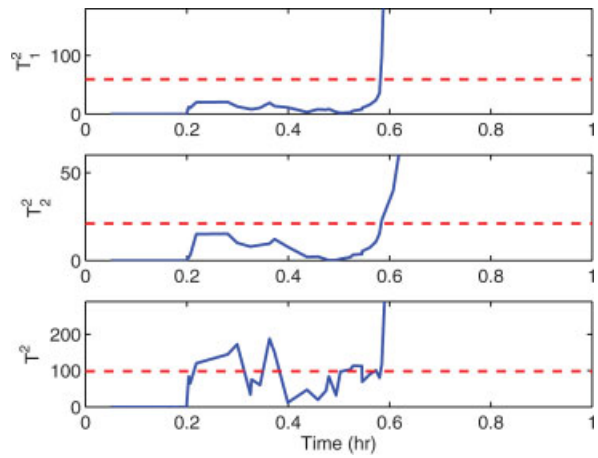

Figure 9. CSTR example.

Closed-loop system under feedback-linearizing control with sample size m = 1. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at t = 0.5 *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

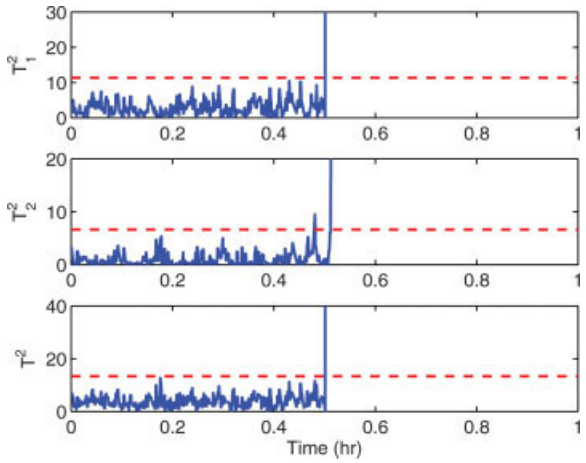

Figure 10. CSTR example.

Closed-loop system under proportional control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

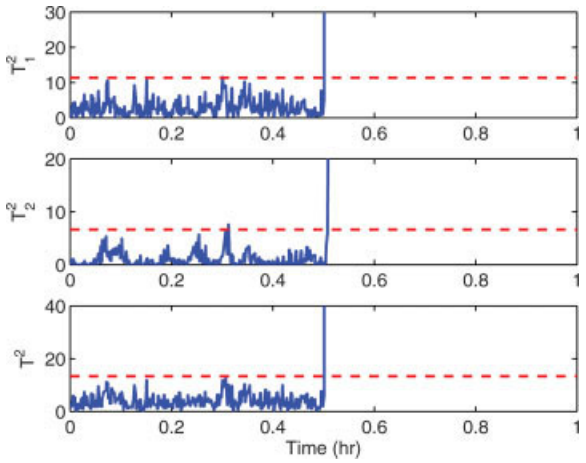

Figure 12. CSTR example.

Closed-loop system under proportional control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_2 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

UCL. The results of these simulations were that from 500 runs, faults were detected when $d_1 > 0.21$, with an average initial detection time of 30.7 min. Out of the 500 runs, a single run was detected by the T^2 statistic but showed no failure in either T_1^2 or T_2^2.

Finally, to follow-up on the point of Remark 8, while the feedback-linearizing controller is not an optimal controller, Figure 13 shows that the control action requested by the feedback-linearizing controller is not excessive and is comparable to that of the control action requested by the proportional controller.

Remark 9: *The simulation results showed that the traditional setting for Hotelling's T^2 statistic which calls for using m randomly sampled observations, and a covariance matrix based on the sampled data was less accurate than the method of individual observations. This is due to the fact that the data is not normally distributed on a short time scale. A small number of observations in a sample can lead to an almost singular S, while the predicted distribution for a large number of observations per sample becomes increasingly narrow. This reveals the fact that the data over a short period are in fact serially correlated. While this could be remedied by using a larger sample time scale, this may become inappropriate due to the need to quickly identify faults. However, the single observation method is a reasonable approach because the individual observations hold to the normal distribution over a long period of time. The probability of exceeding the UCL predicted by Eq. 9 using S estimated from historical data is accurate on a large time-scale and potentially conservative otherwise.*

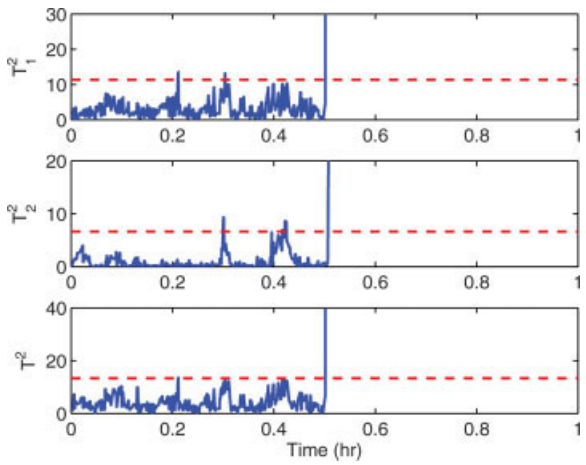

Figure 11. CSTR example.

Closed-loop system under feedback-linearizing control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_2 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

Application to a polyethylene reactor

In this subsection, the proposed method will be demonstrated using a model of an industrial gas phase polyethylene reactor. The feed to the reactor consists of ethylene, comonomer, hydrogen, inerts and catalyst. A recycle stream of unreacted gases flows from the top of the reactor, and is cooled by passing through a water-cooled heat exchanger. Cooling rates in the heat exchanger are adjusted by mixing cold and warm water streams while maintaining a constant total cooling water flow rate through the heat exchanger. Mass balances on hydrogen and comonomer have not been considered in this study because hydrogen and comonomer

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

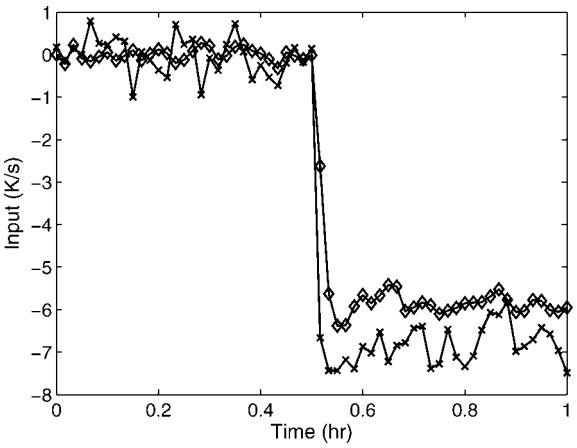

Figure 13. CSTR example.

Manipulated input profiles for both the proportional controller ($\diamond$) and the feedback-linearizing controller ($\times$) with a failure in d_1 at time $t = 0.5$ *hr*.

have only mild effects on the reactor dynamics[44]. A mathematical model for this reactor has the following form ([44])

$$\begin{aligned}
\frac{d[In]}{dt} &= \frac{1}{V_g}\left(F_{In} - \frac{[In]}{[M_1]+[In]}b_t\right)\\
\frac{d[M_1]}{dt} &= \frac{1}{V_g}\left(F_{M_1} - \frac{[M_1]}{[M_1]+[In]}b_t - R_{M1}\right)\\
\frac{dY_1}{dt} &= F_c a_c - k_{d_1}Y_1 - \frac{R_{M1}M_{W_1}Y_1}{B_w} + d_2\\
\frac{dY_2}{dt} &= F_c a_c - k_{d_2}Y_2 - \frac{R_{M1}M_{W_1}Y_2}{B_w} + d_2\\
\frac{dT}{dt} &= \frac{H_f + H_{g1} - H_{g0} - H_r - H_{pol}}{M_r C_{pr} + B_w C_{ppol}} + d_1\\
\frac{dT_{w_1}}{dt} &= \frac{F_w}{M_w}(T_{wi} - T_{w_1}) - \frac{UA}{M_w C_{pw}}(T_{w_1} - T_{g_1})\\
\frac{dT_{g_1}}{dt} &= \frac{F_g}{M_g}(T - T_{g_1}) + \frac{UA}{M_g C_{pg}}(T_{w_1} - T_{g_1}) + d_3
\end{aligned} \tag{19}$$

where

$$\begin{aligned}
b_t &= V_p C_v \sqrt{([M_1]+[In])RRT - P_v}\\
R_{M1} &= [M_1]k_{p0}e^{\frac{-E_a}{R}\left(\frac{1}{T}-\frac{1}{T_f}\right)}(Y_1+Y_2)\\
C_{pg} &= \frac{[M_1]}{[M_1]+[In]}C_{pm1} + \frac{[In]}{[M_1]+[In]}C_{pIn}\\
H_f &= (F_{M_1}C_{pm1} + F_{In}C_{pIn})(T_{feed} - T_f)\\
H_{g1} &= F_g(T_{g_1} - T_f)C_{pg}\\
H_{g0} &= (F_g + b_t)(T - T_f)C_{pg}\\
H_r &= H_{reac}M_{W_1}R_{M1}\\
H_{pol} &= C_{ppol}(T - T_f)R_{M1}M_{W_1}
\end{aligned} \tag{20}$$

The definitions for all the variables used in Eqs. 19–20 are given in Table 3, and their values can be found in Table 4[44] (see also[45]). Under normal operating conditions, the open-loop system behaves in an oscillatory fashion (i.e., the system possesses an open-loop unstable steady-state surrounded by a stable limit cycle). The open-loop unstable steady-state around which the system will be controlled is

$$\begin{aligned}
[In]_{ss} &= 439.7\frac{mol}{m^3} & [M_1]_{ss} &= 326.7\frac{mol}{m^3}\\
Y_{1ss}, Y_{2ss} &= 3.835mol & T_{ss} &= 356.2K\\
T_{g1ss} &= 290.4K & T_{w1ss} &= 294.4K.
\end{aligned}$$

Note that with the given parameters, the dynamics of Y_1, Y_2 are identical and will be reported in the results as a single combined state. In this example, we consider three possible faults d_1, d_2, and d_3 which represent a change in the feed temperature, catalyst deactivation and a change in the recycle gas flow rate, respectively. The manipulated inputs are the feed temperature T_{feed}, and the inlet flow rate of ethylene F_{M1}. The control objective is to stabilize the system at the open-loop unstable steady-state. In addition, in order to apply the proposed FDI scheme, the controller must guarantee that the closed-loop system satisfies the isolability conditions. The open-loop system is highly coupled. If the controller does not impose a specific structure, all the states have mutually dependent dynamics (i.e., they consist of one node in the isolability graph as stated in Definition 5). In this work, we propose to design a nonlinear controller to decouple [In], $[M_1]$ and T from (Y_1, Y_2) and from T_{w1} and T_{g1}. In this way, the resulting closed-loop system consists of three subsystems (i.e., three nodes in the isolability graph) that do not have mutually dependent dynamics. In addition, the signature of

Table 3. Polyethylene Reactor Example Process Variables

a_c	active site concentration of catalyst
b_t	overhead gas bleed
B_w	mass of polymer in the fluidized bed
C_{pml}	specific heat capacity of ethylene
C_v	vent flow coefficient
C_{pw}, C_{pIn}, C_{ppol}	specific heat capacity of water, inert gas and polymer
E_a	activation energy
F_c, F_g	flow rate of catalyst and recycle gas
F_{In}, F_{M_1}, F_w	flow rate of inert, ethylene and cooling water
H_f, H_{g0}	enthalpy of fresh feed stream, total gas outflow stream from reactor
H_{g1}	enthalpy of cooled recycle gas stream to reactor
H_{pol}	enthalpy of polymer
H_r	heat liberated by polymerization reaction
H_{reac}	heat of reaction
$[In]$	molar concentration of inerts in the gas phase
k_{d_1}, k_{d_2}	deactivation rate constant for catalyst site 1, 2
k_{p0}	pre-exponential factor for polymer propagation rate
$[M_1]$	molar concentration of ethylene in the gas phase
M_g	mass holdup of gas stream in heat exchanger
M_rC_{pr}	product of mass and heat capacity of reactor walls
M_w	mass holdup of cooling water in heat exchanger
M_{W1}	molecular weight of monomer
P_v	pressure downstream of bleed vent
R, RR	ideal gas constant, unit of $\frac{J}{mol\cdot K}$, $\frac{m^3\cdot atm}{mol\cdot K}$
T, T_f, T_{feed}	reactor, reference, feed temperature
T_{g1}, T_{w1}	temperature of recycle gas, cooling water stream from exchanger
T_{wi}	inlet cooling water temperature to heat exchanger
UA	product of heat exchanger coefficient with area
V_g	volume of gas phase in the reactor
V_p	bleed stream valve position
y_1, Y_2	moles of active site type 1, 2

each of the three faults is different, and, thus, the fault isolability conditions are satisfied. In order to accomplish this objective, we define the following control laws

$$F_{M1} = u_2 V_g + F_{M1ss}$$
$$T_{feed} = \frac{u_1(M_r C_{pr} + B_W C_{ppol}) + H_{fss}}{F_{M1} C_{pm1} + F_{In} C_{pIn}} + T_f \tag{21}$$

with

$$u_1 = \frac{H_r - H_{rss} + H_{pol} - H_{polss} - H_{g1} + H_{g1ss}}{M_r C_{pr} + B_w C_{ppol}} + v_1$$
$$u_2 = \frac{R_{M1} - R_{M1ss}}{V_g} + v_2 \tag{22}$$

where terms with the subscript *ss* are constants evaluated at the steady state and v_1, v_2 are the external inputs that will allow stabilizing the resulting closed-loop system (see Eq. 23). Under the control law of Eq. 22, the dynamics of the states T and $[M_1]$, take the following form in the closed-loop system

$$\frac{d[M_1]}{dt} = \left[F_{M_1} - \frac{[M_1]}{[M_1] + [In]} b_t - R_{M1ss}\right] \frac{1}{V_g} + v_2$$
$$\frac{dT}{dt} = \frac{H_f + H_{g1ss} - H_{g0} - H_{rss} - H_{polss}}{M_r C_{pr} + B_w C_{ppol}} + v_1 + d_1 \tag{23}$$

It can be seen that these states only depend on $[In]$, $[M_1]$ and T. The closed-loop system under the controller of Eq. 23 has a reduced incidence graph with three nodes q_1, q_2 and q_3 corresponding to the three partially decoupled subsystems $X_1 = \{[In], [M_1], T\}$, $X_2 = \{Y_1, Y_2\}$ and $X_3 = \{T_{g1}, T_{w1}\}$, respectively. The resulting isolability graph for the closed-loop system is shown in Figure 14. This structure leads to each of the three faults d_1, d_2 and d_3 having unique signatures $W^1 = [1\ 1\ 1]^T$, $W^2 = [0\ 1\ 0]^T$ and $W^3 = [0\ 0\ 1]^T$, and allows fault detection and isolation in the closed-loop system using the proposed data-based FDI scheme.

In open-loop operation, the system has an unstable steady-state surrounded by a stable limit-cycle as shown by[45]. In order to understand the stability properties of the entire closed-loop system, the stability of each subsystem around its equilibrium point was investigated assuming that the remaining states were at their equilibrium points. It can be seen that both of the uncontrolled subsystems $X_2 = \{Y_1, Y_2\}$ and $X_3 = \{T_{g1}, T_{w1}\}$ are stable. This implies that to obtain a stable closed-loop system, the control inputs v_1, v_2 have to be designed to stabilize the subsystem $X_1 = \{[In], [M_1], T\}$. In the present example, two PI controllers are implemented that determine v_1 and v_2 to regulate each state independently. By simulation, the PI controllers have been tuned to stabilize the equilibrium of the closed-loop system and achieve a reasonable closed-loop response with regard to requested control action and response time. Note that any controller that stabilizes subsystem X_1 can be used. The main objective is to demonstrate the proposed data-based FDI method. The PI controllers are defined as follows

$$v_1(t) = K_1\left(T_{ss} - T + \frac{1}{\tau_1}\int_0^t (T_{ss} - T)dt\right)$$
$$v_2(t) = K_2([M_1]_{ss} - [M_1] + \frac{1}{\tau_2}\int_0^t ([M_1]_{ss} - [M_1])dt) \tag{24}$$

with $K_1 = 0.005$, $K_1 = 0.0075$, $\tau_2 = 1{,}000$, $\tau_1 = 500$. We will refer to the controller defined by Eqs. 21, 22 and 24 as the "decoupling" controller. Additionally, for comparison purposes, a controller is used that stabilizes the closed-loop system, but does not take into account the isolability conditions of the proposed FDI method. Specifically, two PI controllers will be used to regulate T and M_1. This will be denoted as the "PI-only" control law. The inputs F_{M1} and T_{feed} are defined by Eq. 21, but in this case, u_1 and u_2 are evaluated by applying the PI controllers of Eq. 24, with the same tuning parameters to the states T and M_1.

The PI-only controller stabilizes the equilibrium point under normal operating conditions, however, all the states are mutually dependent, or in other words the reduced incidence graph consists of only one node. This implies that every fault affects all the state trajectories, making isolation of the fault a difficult task. The proposed FDI scheme cannot be applied because the closed-loop system does not satisfy the isolability conditions, i.e., all the system faults have the same signature.

Simulations have been carried out for several scenarios to demonstrate the effectiveness of the proposed FDI scheme in detecting and isolating the three faults d_1, d_2 and d_3. In all the simulations, sensor measurement and process noise were included. The sensor measurement noise trajectory was generated using a sample time of ten seconds, and a zero-mean normal distribution with standard deviation σ_M. 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, with a sample time of ten seconds, 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. The autoregressive process noise is added to the right-hand side of the differential equations for each state and the sensor measurement noise is added to the measurements of each state. Sensor measurement noise and process noise are evaluated independently for each state variable. The process and sensor measurement noise for Y_1 and Y_2 are taken to be

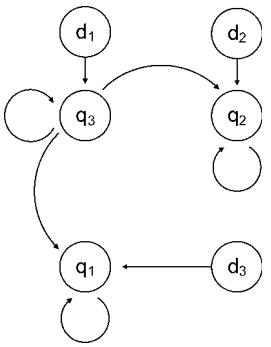

Figure 14. Isolability graph for the system of Eq. 19.

Table 4. Polyethylene Reactor Example Parameters and Units

V_g	=	500	m^3
V_p	=	0.5	
P_v	=	17	atm
B_w	=	$7 \cdot 10^4$	kg
k_{p0}	=	$85 \cdot 10^{-3}$	$\frac{m^3}{mol \cdot s}$
E_a	=	(9000)(4.1868)	$\frac{J}{Kg}$
C_{pw}	=	$(10^3)(4.1868)$	$\frac{J}{Kg \cdot K}$
C_v	=	7.5	$\frac{mol}{atm^{0.5} \cdot s}$
C_{pm1}, C_{pIn}	=	(11)(4.1868), (6.9)(4.1868)	$\frac{J}{mol \cdot K}$
C_{ppol}	=	$(0.85 \cdot 10^3)(4.1868)$	$\frac{J}{kg \cdot K}$
k_{d_1}	=	0.0001	s^{-1}
k_{d_2}	=	0.0001	s^{-1}
M_{W1}	=	$28.05 \cdot 10^{-3}$	$\frac{kg}{mol}$
M_w	=	$3.314 \cdot 10^4$	kg
M_g	=	6060.5	mol
$M_r C_{pr}$	=	$(1.4 \cdot 10^7)(4.1868)$	$\frac{J}{K}$
H_{reac}	=	$(-894.10^3)(4.1868)$	$\frac{J}{kg}$
$U\ A$	=	$(1.14 \cdot 10^6)(4.1868)$	$\frac{J}{K \cdot s}$
F_{In}, F_{M1}, F_g	=	5, 190, 8500	$\frac{mol}{s}$
F_w	=	$(3.11 \cdot 10^5)(18 \cdot 10^{-3})$	$\frac{kg}{s}$
F_c^s	=	$\frac{5.8}{3600}$	$\frac{kg}{s}$
T_f, T_{feed}^s, T_{wi}	=	360, 293, 289.56	K
RR	=	$8.20575 \cdot 10^{-5}$	$\frac{m^3 \cdot atm}{mol \cdot K}$
R	=	8.314	$\frac{J}{mol \cdot K}$
a_c	=	0.548	$\frac{mol}{kg}$
u_1^{max}, u_2^{max}	=	$5.78 \cdot 10^{-4}$, $3.04 \cdot 10^{-4}$	$\frac{K}{s}$, $\frac{mol}{s}$
$[In]_s$	=	439.68	$\frac{mol}{m^3}$
$[M_1]_s$	=	326.72	$\frac{mol}{m^3}$
Y_{1s}, Y_{2s}	=	3.835, 3.835	mol
T_s, T_{w1s}, T_{g1s}	=	356.21, 290.37, 294.36	K

equal. Table 5 provides the values of the noise parameters for each state of the system of Eq. 19. The same assumptions regarding the multivariate normal distribution of the measured process data under closed-loop operation for the CSTR example apply to this example. Figure 15 shows that the distribution of the state measurements over a long period of fault-free operation is approximately Gaussian.

For each failure d_k, two simulations have been carried out. One using the decoupling controller and another using the PI-only controller. Both simulations have been carried out using the same sensor measurement and process noise trajectories. Starting from steady-state, the three different failures with values $d_1 = 10\ \frac{K}{s}$, $d_2 = -0.002\ \frac{mol}{s}$, and $d_3 = 300\ \frac{K}{s}$ were introduced at time $t = 0.5\ hr$. These failures are disturbances in the dynamics of T, Y and T_{g1}, and represent changes in the feed temperature, catalyst deactivation and changes in the recycle gas flow rate, respectively. Figures 16, 18 and 20 show the state trajectories of the closed-loop system under the decoupling controller (solid line), and the PI-only controller (dashed line) for each of the three possible faults. It can be seen that for the PI-only controller, each time a fault occurs, all states deviate from the normal operating region around the equilibrium point. This makes isolation a difficult task. However, the closed-loop state trajectories under the decoupling controller demonstrate that when a given fault occurs, not all state trajectories are affected. The decoupling of some states from given faults allows for the isolation of the faults based on the T_i^2 statistics. Specifically, the state trajectories of the closed-loop system under the decoupling controller were monitored using the T^2 statistic based on all the states of the system of Eq. 19 and the T_i^2 statistic corresponding to each one of the three subsystems X_1, X_2, and X_3. All statistics were monitored using the single-observation method ($m = 1$) with the upper control limit

Table 5. Polyethylene Reactor Noise Parameters

	σ_p	σ_m	ϕ
$[In]$	1E-3	5E-2	0
$[M_1]$	1E-3	5E-2	0.7
Y	1E-3	1E-2	0.7
T	5E-3	5E-2	0.7
T_{g1}	5E-3	5E-2	0.7
T_{w1}	5E-3	5E-2	0.7

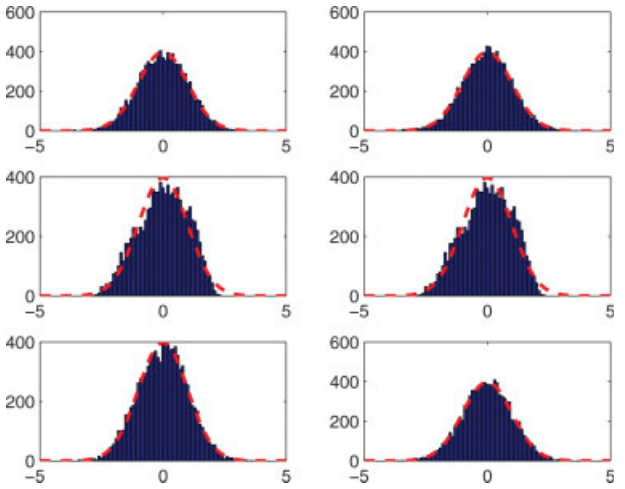

Figure 15. Polyethylene reactor example.

Distribution of normalized, fault-free operating data compared with a normal distribution of the same mean and covariance. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

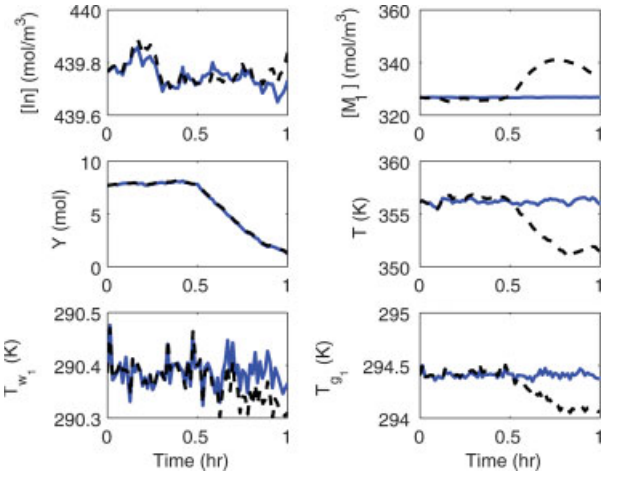

Figure 16. Polyethylene reactor example.

State trajectories of the closed-loop system under decoupling (solid) and PI-only (dashed) controllers with a fault d_2 at $t = 0.5\ hr$. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

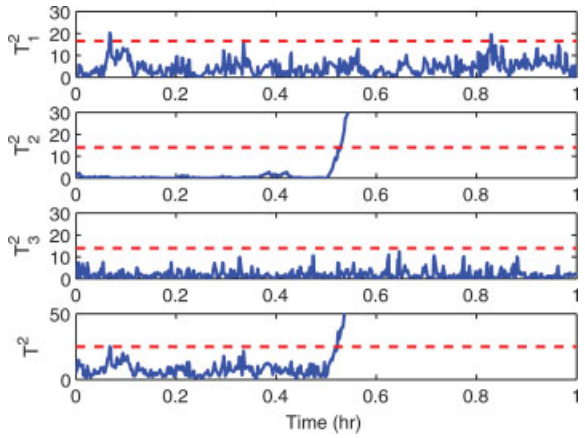

Figure 17. Polyethylene reactor example.

Statistics T^2, T_1^2, T_3^2, and T_3^2 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_2 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

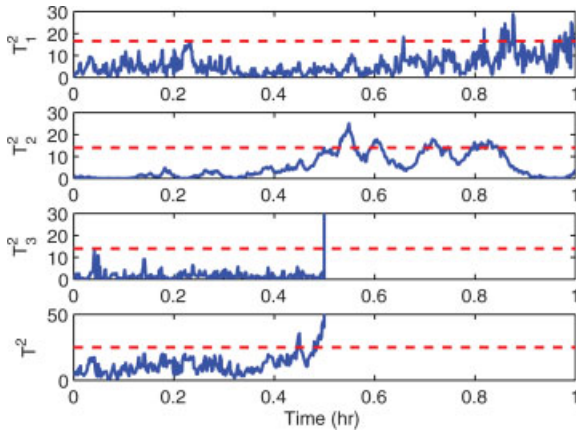

Figure 19. Polyethylene reactor example.

Statistics T^2, T_1^2, T_2^2, and T_3^2 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_3 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

defined in Eq. 9, and the covariance matrix S, obtained from historical observations. As in the CSTR example, simulations were also run using a multiple observation test statistic ($m = 10$). This method showed similar results in terms of fault detection and isolation to the ones of the single observation statistic and these results are not presented here for brevity.

Figures 17, 19 and 21 show the trajectories of T^2, T_1^2, T_2^2 and T_3^2 for each different scenario along with the corresponding upper control limits. Each failure is defined by a unique signature that can be isolated based on the monitored statistics. Figure 17 shows the statistics corresponding to the simulation with a failure in d_2. The signature of d_2 is $W^2 = [0\ 1\ 0]^T$, because the dynamics of the states corresponding to X_1 and X_3 are not affected by fault d_2; that is, there is no path from the node corresponding to d_2 to the nodes corresponding to X_1 and X_2 in the isolability graph of the closed-loop system. Figure 17 clearly shows the fault occurring at time $t = 0.5$ *hr*, and the signature that we would expect; that is, only T_2^2 violates the upper control limit. The state trajectories of this faulty scenario of Figure 16 demonstrates that there is a failure affecting Y starting at $t = 0.5$ *hr*. The failure affects all the state trajectories under PI-only control but affects only Y for the closed-loop system under nonlinear decoupling control. Similarly, a failure in T_{g1} affects only subsystem X_3. The state trajectories of Figure 18 shows that under PI-only control, all of the states are affected, whereas under decoupling control, only the subsystem $X_3 = \{T_{g1}, T_{w1}\}$ is affected. The statistics in Figure 19 show that the signature of the faultis $[0\ 0\ 1]^T = W^3$. The signature of fault d_1 is $W^1 = [1\ 1\ 1]^T$, meaning that this fault affects all the states in the closed-loop system. The state trajectories and the corresponding statistics are shown in Figures 20 and 21. The

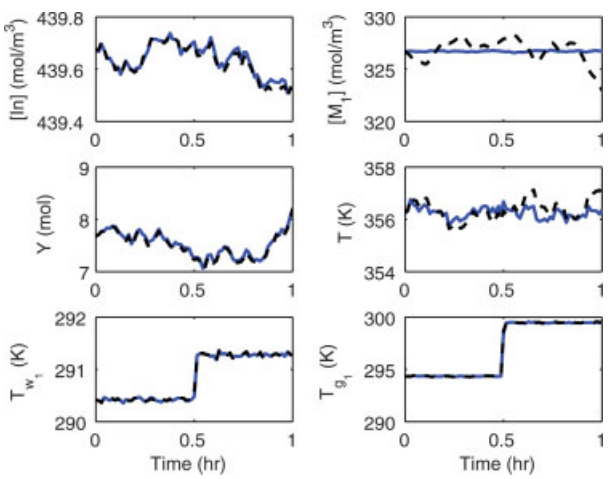

Figure 18. Polyethylene reactor example.

State trajectories of the closed-loop system under the decoupling (solid), and PI-only (dashed) controllers with a fault d_3 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

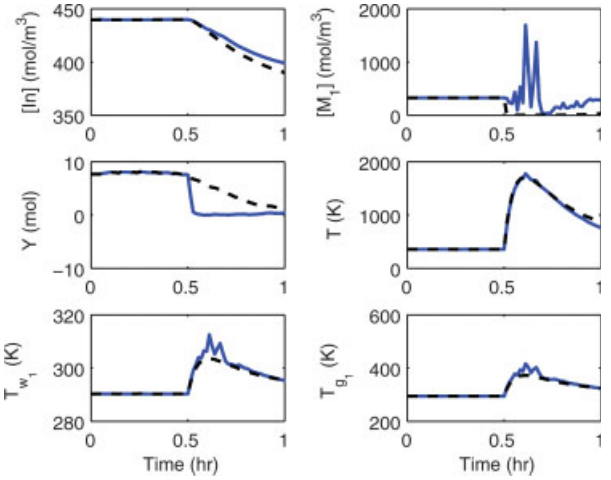

Figure 20. Polyethylene reactor example.

State trajectories of the closed-loop system under the decoupling (solid) and PI-only (dashed) controllers with a fault d_1 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

control action required under the decoupling control law is of comparable magnitude to that of the PI-only controller. Figure 22 shows the manipulated input trajectories for both controllers in the scenario with fault d_2 occurring.

Remark 10: *Although the method of determining faults by monitoring T_i^2 values was used in this example, other FDI methods could benefit from the fact that the enforced structure separates regions of faulty operation. In the case where the desired structure is only partially achieved due to plant-model mismatch or other uncertainties, it may be necessary to utilize more sophisticated methods of fault detection and isolation (e.g., contribution plots or clustering). It should be noted that even an incomplete decoupling will benefit many of these methods as the regions of faulty operation are still at least partially separated.*

Conclusions

This work has proposed a method for integrating the design of the feedback control law with the fault detection and isolation scheme. This approach strengthens existing FDI techniques by enforcing an appropriate structure on the closed-loop system that may separate regions of faulty operation in the state space, such that fault isolation may become possible. This was illustrated through two chemical process examples, a CSTR and a polyethylene reactor. By carefully designing the feedback controller, it was demonstrated that it is possible to enhance the isolability of particular faults. In the CSTR example, feedback linearization was used to achieve the required closed-loop system structure in order to perform fault detection and isolation, whereas in the polyethylene reactor example, a more general approach to nonlinear controller design was used in meeting the required conditions for isolability. Additionally, it was demonstrated that using a data-based method of monitoring the T_i^2 values of the resulting subsystems, it was possible to isolate certain faults due to the enforced closed-loop system structure.

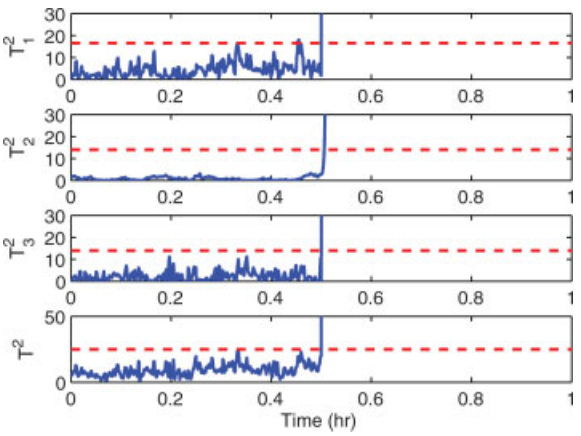

Figure 21. Polyethylene reactor example.

Statistics T^2, T_1^2, T_2^2, and T_3^2 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_1 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

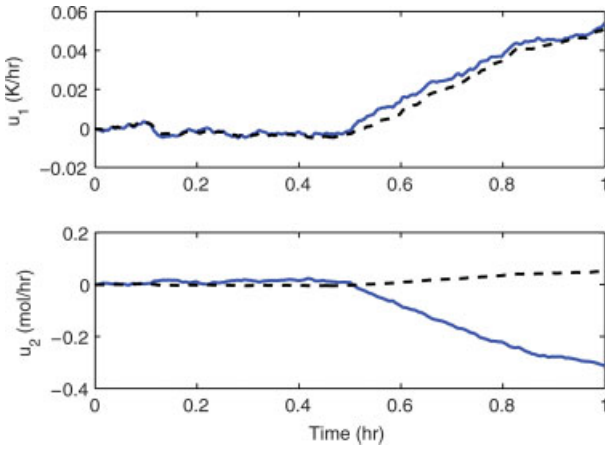

Figure 22. Polyethylene reactor example.

Manipulated input profiles for both decoupling (solid) and PI-only (dashed) control with a fault in d_2 at $t = 0.5$ *hr*. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

Acknowledgments

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

Literature Cited

1. Patton RJ. Fault-Tolerant Control Systems: The 1997 Situation. In: *Proceedings of the IFAC Symposium Safeprocess 1997*. Hull, U.K. 1997:1033–1054.
2. Blanke M, Izadi-Zamanabadi R, Bogh SA, Lunau CP. Fault-tolerant control systems – A holistic view. *Control Eng Practice*. 1997;5:693–702.
3. Zhou DH, Frank PM. Fault Diagnostics and Fault Tolerant Control. *IEEE Trans on Aerospace and Elec Systs*. 1998;34:420–427.
4. Bao J, Zhang WZ, Lee PL. Passivity-based decentralized failure-tolerant control. *Ind & Eng Chem Res*. 2002;41:5702–5715.
5. Mhaskar P, Gani A, Christofides PD. Fault-tolerant process control: Performance-based Reconfiguration and Robustness. *Int J of Robust & Nonlinear Control*. 2006;16:91–111.
6. Mhaskar P, Gani A, McFall C, Christofides PD, Davis JF. Fault-tolerant control of nonlinear systems subject to sensor data losses. *AIChE J*. 2007;53:654–668.
7. Yang GH, Zhang SY, Lam J, Wang J. Reliable control using redundant controllers. *IEEE Trans on Auto Contr*. 1998;43:1588–1593.
8. Mhaskar P, Gani A, El-Farra NH, Christofides PD, Davis JF. Integrated fault-detection and fault-tolerant control of process systems. *AIChE J*. 2006;52:2129–2148.
9. Frank PM. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy–A survey and some new results. *Automatica*. 1990;26:459–474.
10. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN. A review of process fault detection and diagnosis Part I: Quantitative model-based methods. *Comp and Chem Eng*. 2003;27:293–311.
11. Romagnoli JA, Palazoglu A. *Introduction to Process Control*. CRC Press; 2006.
12. Yoon S, MacGregor JF. Fault diagnosis with multivariate statistical models part I: using steady state fault signatures. *J of Process Control*. 2001;11:387–400.
13. MacGregor JF, Kourti T. Statistical process control of multivariate processes. *J of Quality Technol*. 1996;28:409–428.
14. Wise BM, Gallagher NB. The process chemometrics approach to monitoring and fault detection. *J of Process Control*. 1996;6:329–348.
15. Raich A, Çinar A. Statistical process monitoring and disturbance diagnosis in multivariable continuous processes. *AIChE J*. 1996;42:995–1009.

16. Negiz A, Çinar A. Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE J*. 1997;43:2002–2020.
17. Kourti T, MacGregor JF. Multivariate SPC methods for process and product monitoring. *J of Quality Technol*. 1996;28:409–428.
18. Bakshi BR. Multiscale PCA with application to multivariate statistical process monitoring. *AIChE J*. 1998;44:1596–1610.
19. Aradhye HB, Bakshi BR, Strauss RA, Davis JF. Multiscale SPC using wavelets: Theoretical analysis and properties. *AIChE J*. 2003; 49:939–958.
20. Aradhye HB, Bakshi BR, Davis JF, Ahalt SC. Clustering in wavelet domain: A multiresolution ART network for anomaly detection. *AIChE J*. 2004;50:2455–2466.
21. Venkatasubramanian V, Rengaswamy R, Kavuri SN, Yin K. A review of process fault detection and diagnosis Part III: Process history based methods. *Comp and Chem Eng*. 2003;27:327–346.
22. Khalil HK. *Nonlinear Systems*. Macmillan Publishing Company; 1992.
23. Christofides PD, El-Farra NH. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays*. New York: Springer; 2005.
24. Whiteley JR, Davis JF. Knowledge-based interpretation of sensor patterns. *Comp & Chem Eng*. 1992;16:329–346.
25. Mehranbod N, Soroush M, Panjapornpon C. A method of sensor fault detection and identification. *J of Process Control*. 2005;15: 321–339.
26. Whiteley JR, Davis JF. Qualitative interpretation of sensor patterns. *IEEE Expert*. 1992;8:54–63.
27. Rollins DR, Davis JF. Unbiased estimation of gross errors when the covariance matrix is unknown. *AIChE J*. 1993;39:1335–1341.
28. Mehranbod N, Soroush M, Piovoso M, Ogunnaike BA. Probabilistic model for sensor fault detection and identification. *AIChE J*. 2003;49:1787–1802.
29. Dunia R, Qin SJ, Edgar TF, McAvoy TJ. Identification of faulty sensors using principal component analysis. *AIChE J*. 1996;42:2797–2812.
30. Harary F. *Graph Theory*. Perseus Books Publishing, 1969.
31. Daoutidis P, Kravaris C. Structural evaluation of control confiurations for multivariable nonlinear processes. *Chem Eng Sci*. 1991;47: 1091–1107.
32. Yoon S, MacGregor JF. Statistical and causal model-based approaches to fault detection and isolation. *AIChE J*. 2000;46:1813–1824.
33. Hotelling H. Multivariate Quality Control. In: Eisenhart O. *Techniques of Statistical Analysis*. McGraw-Hill; 1947:113–184.
34. Montgomery DC. *Introduction to statistical quality control*. John Wiley & Sons; 1996.
35. Tracy ND, Young JC, Mason RL. Multivariate control charts for individual observations. *J of Quality Technol*. 1992;24:88–95.
36. Prasad PR, Davis JF, Jirapinyo Y, Bhalodia M, Josephson JR. Structuring diagnostic knowledge for large-scale process systems. *Comp and Chem Eng*. 1999;22:1897–1905.
37. MacGregor JF, Jaeckle C, Kiparissides C, Koutoudi M. Process monitoring and diagnosis by multiblock PLS method. *AIChE J*. 1994;40:826–838.
38. El-Farra NH, Christofides PD. Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem Eng Sci*. 2001;56:1841–1868.
39. El-Farra NH, Christofides PD. Bounded robust control of constrained multivariable nonlinear processes. *Chem Eng Sci*. 2003;58:3025–3047.
40. Kokotovic P, Arcak M. Constructive nonlinear control: a historical perspective. *Automatica*. 2001:637–662.
41. Isidori A. *Nonlinear Control Systems: An Introduction*. Berlin-Heidelberg: Springer-Verlag; 1989.
42. Daoutidis P, Kravaris C. Synthesis of feedforward state feedback controllers for nonlinear processes. *AIChE J*. 1989;35:1602–1616.
43. McAuley KB, Macdonald DA, McLellan PJ. Effects of operating conditions on stability of gas-phase polyethylene reactors. *AIChE J*. 1995;41:868–879.
44. Dadebo SA, Bell ML, McLellan PJ, McAuley KB. Temperature control of industrial gas phase polyethylene reactors. *J of Process Control*. 1997;7:83–95.
45. Gani A, Mhaskar P, Christofides PD. Fault-tolerant control of a polyethylene reactor. *J of Process Control*. 2007;17:439–451.

Manuscript received Apr. 20, 2007, and revision received Aug. 17, 2007.