8th International IFAC Symposium on
Dynamics and Control of Process Systems
Preprints Vol.1, June 6-8, 2007, Cancún, Mexico

ENHANCING FAULT ISOLATION THROUGH NONLINEAR CONTROLLER DESIGN

Benjamin J. Ohran [*] **Prashant Mhaskar** [**]
David Muñoz de la Peña [*]
Panagiotis D. Christofides [*,1] **James F. Davis** [*]

[*] *Department of Chemical and Biomolecular Engineering*
University of California, Los Angeles, CA 90095-1592
[**] *Department of Chemical Engineering*
McMaster University, Hamilton On L8S 4L7

Abstract: This work proposes a fault detection and isolation scheme that takes into account, in an explicit way, the design of the feedback control law. This scheme allows isolating specific faults in the closed-loop system using a purely data-based approach without requiring prior knowledge of fault history. This is accomplished through the design of an appropriate nonlinear control law based on feedback linearization that allows isolating given faults by effectively decoupling the dependency between certain process state variables. The results are demonstrated through a continuously stirred tank reactor example.

Keywords: Fault detection and isolation, Fault tolerant control, Process monitoring, Chemical process control

1. INTRODUCTION

Dealing efficiently with process and control system failures is becoming an issue of increasing importance in the context of highly-automated chemical processes. Automation tends to increase vulnerability of the plant to faults that, if not quickly handled, can potentially cause a host of undesired economic, environmental and safety problems. As chemical plants become more automated, there is an increasing need to detect and isolate faults early and accurately to avoid such problems. In this paper, our main focus will be on fault detection and isolation (FDI), that is, not only detecting that a fault has occurred, but also diagnosing the underlying cause of the faulty behavior. If a fault is isolated early, it can be more safely dealt with through fault-tolerant control systems (see, for example, Yang et al. (1998); Bao et al. (2002); Mhaskar et al. (2006) for results in this area).

Methods for process monitoring 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 process faults; in this way fault detection and isolation can be accomplished for specific model and fault structures. On the other hand, data-based methods are based exclusively on process measurements. In the context of fault isolation, data-based methods usually require historical data under faulty operation and perform data-based fault isolation through the use of such techniques as contribution plots (Kourti and MacGregor (1996)). Other methods have been developed that take advantage of the structure of dimensionally reduced data and the consequent residual space created in principle component analysis (PCA) or partial least squares (PLS). Gertler et al. (1999) employ PCA to identify linear relationships in the process data that can then be used with analytical redundancy techniques. Yoon and MacGregor (2001) compare steady-state fault directions in the PCA space with historical fault data. The main drawback of these methods is that they require specific historical data that may be costly to obtain. For a comprehensive review of model-based and data-based fault detection and isolation methods, the reader may refer to Venkatasubramanian et al. (2003b,a).

These methods have had varying degrees of success in detecting and isolating faults, but still leave room for improvement. In particular, most results are based on the premise that the controller is

[1] Corresponding author: pdc@seas.ucla.edu

designed independently of the possible faults that might occur. These works focus on designing a fault detection and isolation scheme for a given closed-loop system where the controller has already been fixed. The present work proposes a novel method that takes into account the design of the feedback control law. This method allows isolating specific faults in the closed-loop system using a purely data-based approach, without requiring prior knowledge of fault history. This is achieved through the design of appropriate nonlinear control laws that allow isolating given faults by effectively decoupling the dependency between certain process state variables. While the achievement of the key requirement, the enforcement of a special structure in the closed-loop system, can be accomplished by a variety of nonlinear control laws, in the present paper we utilize feedback linearization to achieve this task. The results are demonstrated through a continuously stirred tank reactor example.

2. PRELIMINARIES

2.1 Data-Based Detection

Data-based methods for fault detection in multivariate systems are well established in statistical process control. A common approach to monitoring multivariate process performance is based upon Hotelling's T^2 statistic, which allows processes to be monitored using a single variable that gives a well-defined threshold for normal operation. Specifically, given a multivariate state vector x of dimension n, the T^2 statistic (see, for example, Romagnoli and Palazoglu (2006); Kourti and MacGregor (1996)) can be computed using the mean μ and the estimated covariance matrix S of process data obtained under normal operating conditions as follows:

$$T^2 = (x-\mu)^T S^{-1}(x-\mu). \qquad (1)$$

The upper control limit for the T^2 statistic can be calculated using the F distribution, where m is the number of measurements used in estimating the covariance matrix S, according to the formula

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

where $F_\alpha(n, m-n)$ is the upper critical value of the F distribution with $(n, m-n)$ degrees of freedom and significance level α.

In systems where the measurement vector x is of high dimension, it is quite common to perform a dimensionality reduction using PCA or PLS to reduce the number of variables with respect to which T^2 should be computed. Although these methods are useful in reducing the dimensionality of x, and thus the complexity of the fault detection algorithm, we will not discuss or employ them in the present paper; our objective is to simply illustrate how properly designed nonlinear controllers, can lead to enhanced data-based diagnosis and isolation of specific faults. For this same reason, when considering data-based isolation, we do not utilize more standard methods such as contribution plots for the Q-statistic and T^2 statistic as demonstrated in Kourti and MacGregor (1996). Instead we use a plot of the normalized error (Err_i) of the output and each of the states in the system.

$$Err_i = \frac{(x_i - \mu_i)}{s_i} \qquad (3)$$

where μ_i is the mean and s_i is the estimated covariance for each variable. Monitoring the normalized error plot of the output, it is possible to isolate specific faults using the controller-enhanced isolation technique described in the present work. The normalized error plots for the output and each of the states also demonstrate that in the case where the presented technique is not used, it is not clear where the fault lies.

In the proposed scheme, fault detection will be carried out using the T^2 statistic of the state vector (note that we will assume that the state is fully accessible), while fault isolation will be based on the normalized error plot of the output.

2.2 Feedback Linearizable Systems

We assume that the process is modeled by a single-input single-output nonlinear system with multiple faults/disturbances which has the following state-space description

$$\begin{aligned} \dot{x} &= f(x) + g(x)u + \sum_{i \in D} w_i(x) d_i \\ y &= h(x) \end{aligned} \qquad (4)$$

where $x \in R^n$ is the state, $u \in R$ is the input, $y \in R$ is the measured output and $d_i \in R$ represents a possible fault. We assume that f, g, h and w_i are sufficiently smooth functions and that a set D of possible faults has been identified. Each of these faults is characterized by an unknown input to the system d_i that can model sensor errors, actuator failures and disturbances. The system has an equilibrium point at $x = 0$ and $h(0) = 0$. Note that in general this equilibrium point corresponds to a given set-point of the output. Throughout the paper, the notations $L_f^k h(\cdot)$ and $L_g L_f^{k-1} h(\cdot)$ denote the standard k-th order Lie derivative and mixed Lie derivative of a scalar function $h(\cdot)$, with respect to vector functions $f(\cdot)$ and $g(\cdot)$. We assume that the state is fully accessible.

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. We use feedback-linearizing control to accomplish this. Next we consider state feedback control of input-output linearizable systems. To this end, we review the following definition:

Definition 1. (Isidori (1989)). Referring to (4), the relative degree of the output y with respect to the input u is the smallest integer, $r \in [1, n]$, for which

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

A system with relative degree $r \leq n$ is feedback linearizable. If $r = n$ the entire input-state dynamics are linearized. If $r < n$, the feedback controller can be chosen so that a linear input-output map is obtained from the external input to the output, even though the state equations are only partially linearized. In this case, if the inverse dynamics satisfy a given stability condition (in particular, input-to-state stable inverse dynamics), an appropriate control law can be designed for the input-output subsystem that guarantees stability of the entire closed-loop system. To be specific, if system (4) has relative degree $r < n$, then there exists a coordinate transformation (see Isidori (1989)) $(\zeta, \eta) = T(x)$ such that the representation of system (4) with $d_i = 0$ for all $d_i \in D$ (that is, the system without faults), in the (ζ, η) coordinates, takes the form

$$\begin{aligned} \dot{\zeta}_1 &= \zeta_2 \\ &\vdots \\ \dot{\zeta}_{r-1} &= \zeta_r \\ \dot{\zeta}_r &= L_f^r h(x) + L_g L_f^{r-1} g(x) u \\ \dot{\eta}_1 &= \Psi_1(\zeta, \eta) \\ &\vdots \\ \dot{\eta}_{n-r} &= \Psi_{n-r}(\zeta, \eta) \end{aligned} \tag{5}$$

where $y = \zeta_1$, $x = T^{-1}(\zeta, \eta)$, $\zeta = [\zeta_1, \dots, \zeta_r]^T$ and $\eta = [\eta_1, \dots, \eta_{n-r}]^T$. 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 the following theorem, we review one example of an input-output state feedback controller. The controller presented, under the assumption of no faults, guarantees asymptotic stability of the closed-loop system.

Theorem 2. (Isidori (1989)). Consider system (4) with $d_i = 0$ for all $d_i \in D$, under the feedback law

$$u(x) = \frac{1}{L_g L_f^{r-1} h(x)} [K T_\zeta(x) - L_f^r h(x)] \tag{6}$$

where $\zeta = T_\zeta(x)$. Assume K is chosen such that the matrix $A + BK$ has all of its eigenvalues in the left-hand 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.

2.3 Controller Enhanced Isolation

In this section, we prove that under certain assumptions, if the state-feedback law (6) is used, then the faults of system (4) can be isolated into two different groups: those that affect the output and those that do not. We use the following definition of relative degree of a fault (this definition was introduced in Daoutidis and Kravaris (1989) in the context of feedforward/feedback control of nonlinear systems with disturbances but it is employed here to address a completely different problem):

Definition 3. Referring to (4), the relative degree of the output y with respect to the fault d_i, $\rho_i \in [1, n]$, is the smallest integer for which

$$\begin{aligned} L_{w_i} L_f^i h(x) &= 0, \; i = 0, \dots, \rho_i - 2 \\ L_{w_i} L_f^{\rho_i - 1} h(x) &\neq 0. \end{aligned} \tag{7}$$

The definition of relative degree of a fault is analogous to the definition of relative degree of the input, but instead of relating the input to the output, this definition of relative degree relates a particular fault to the output. If a feedback-linearizing controller is used, then the faults can be divided in two different groups: those with a relative degree ρ_i that is greater than the relative degree r and those with a relative degree ρ_i 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. This dependence can be monitored using the normalized error plots.

To show this point, taking into account definitions 1 and 3, there exists (see Isidori (1989)) a coordinate transformation $(\zeta, \eta) = T(x)$ such that the representation of system (4) with $d_j = 0$ for all $d_j \in D - \{d_i\}$ (that is, the system subject only to fault d_i), in the (ζ, η) coordinates, takes the form

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

where $y = \zeta_1$, $x = T^{-1}(\zeta, \eta)$, $\zeta = [\zeta_1, \dots, \zeta_r]^T$ and $\eta = [\eta_1, \dots, \eta_{n-r}]^T$. Following the definition of the state-feedback law (6), the following state-space representation is obtained for ζ:

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

This dynamical system is independent of d_i. Therefore, the trajectory of the output y is independent of the fault d_i. This result, however, does not hold if the relative degree ρ_i of the fault d_i is equal to or smaller than r. In this case, the coordinate change does not eliminate the dependence of the output with the fault. Applying the same coordinate change $(\zeta,\eta) = T(x)$, the dynamics of system (4) with $d_j = 0$ for all $d_j \in D - \{d_i\}$ (that is, the system subject to fault d_i), in the (ζ,η) coordinates, takes the form

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

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 (6) is used, the possible faults of system (4) are divided in 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, that is $D = \{1,2\}$ and $\rho_1 \le r$ and $\rho_2 > r$, then the fault is automatically isolated.

In this work we propose to detect the occurrence of a fault using the T^2 statistic of the full state vector. Once a fault has been detected, the normalized error plot of the output determines whether the output has been affected or not.

Remark 4. There are systems where different outputs can be chosen. Depending on the structure of the system, isolation of a given set of faults can be accomplished by choosing an appropriate output. Note that isolation is done with a purely data-based approach. Even if a model is used to design the controller (which is the case in most control schemes), the isolation of a fault is done only on the basis of the trajectory of the output y.

Remark 5. The proposed approach to fault isolation can also be extended to multiple-input multiple-output systems. In this case, the possible faults can be divided into different groups, depending on whether they affect one, several or none of the system outputs.

3. ILLUSTRATIVE EXAMPLE

We consider a well-mixed continuously stirred tank reactor in which a feed component A is converted to an intermediate species B and finally to the desired product C, according to the reaction scheme

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

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

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

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 T, the temperature of the reactor. Using first principles and standard modeling assumptions, the following mathematical model of the process is obtained

$$
\begin{aligned}
\dot{C_A} &= \frac{F}{V}(C_{A0} - C_A) - r_1 + r_{-1} + d_1 \\
\dot{C_B} &= -\frac{F}{V} C_B + r_1 - r_{-1} - r_2 + r_{-2} \\
\dot{C_C} &= -\frac{F}{V} C_C + r_2 - r_{-2} \qquad (8) \\
\dot{T} &= \frac{F}{V}(T_0 - T) + \frac{(-\Delta H_1)}{\rho c_p}(r_1 - r_{-1}) \\
&\quad + \frac{(-\Delta H_2)}{\rho c_p}(r_2 - r_{-2}) + u + d_2
\end{aligned}
$$

where V is the reactor volume, ΔH_1 and ΔH_2 are the heats of reaction for the first and second steps, ρ is the fluid density, c_p is the fluid heat capacity, d_1 and d_2 are possible faults of the system and $u = Q/\rho c_p$ is the manipulated input, where Q is the heat input to the system. For the purpose of data-based fault detection, system (8) is modeled with autoregressive process noise of the form $w_k = \phi w_{k-1} + \xi_k$ and white sensor noise with a sample time of 1 min. Values of ϕ, the standard deviation of ξ_k, σ_p, and of the white noise, σ_m, are given in Table 2.

Table 1. 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 $[kJ/kg \cdot K]$		

Table 2. Noise Parameters

	σ_m	σ_p	ϕ
C_A	1E-2	1E-3	0.9
C_B	1E-2	1E-3	0.9
C_C	1E-2	1E-3	0.9
T	1E-1	1E-2	0.9

The 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. 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 relative degree 2. The fault d_1 appears only in the dynamics of C_A and is relative degree 3. Finally, fault d_2 is relative degree 2. The values for the constants of the process model are given in Table 1. The control objective is to regulate the system at the equilibrium point

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

To this end, we consider two different feedback controllers: a controller based on input-output 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 PID, MPC or any other controller that does not achieve decoupling of the output from d_1 in the closed-loop system). The feedback-linearizing controller takes the form of (6) 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, faults with a relative degree higher than that of the input will not affect the output in the event of a failure. Therefore d_1, with relative degree 3, will not affect the output. Conversely, because fault d_2 is relative degree 2, it cannot be decoupled from the output. This property does not hold for the closed-loop system under proportional control. In that case, under the presence of a fault (whether in d_1 or d_2), the output is modified. The above statements were tested by simulating system (8) in closed-loop under both proportional control and feedback-linearizing control. In all cases, the system was initially operating at the steady-state with a failure appearing at time $t = 25\ min$.

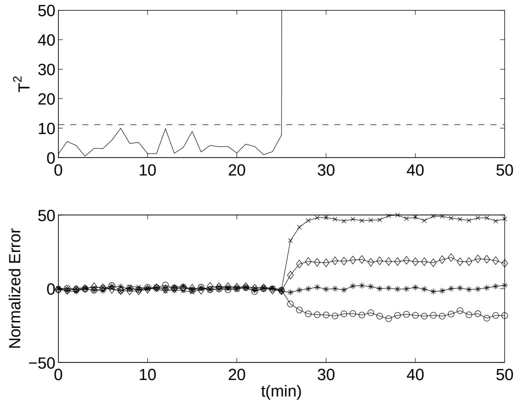

Fig. 1. System under feedback-linearizing control. Upper figure: plot of T^2 (solid) with T_{UCL} (dashed). Lower figure: each state's normalized error, with a failure in d_1 at $t = 25\ min$. T = o, $C_A = \times$, $C_B = \diamond$, $C_C = \star$.

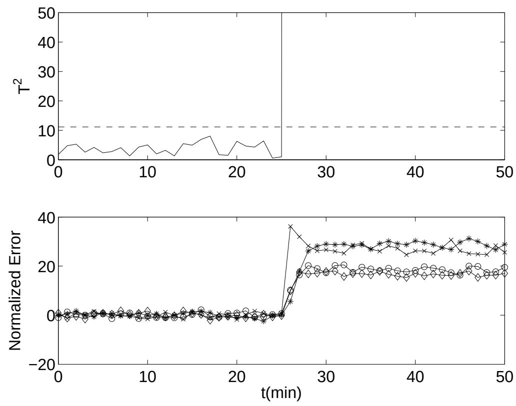

Fig. 2. System under proportional control. Upper figure: plot of T^2 (solid) with T_{UCL} (dashed). Lower figure: each state's normalized error, with a failure in d_1 at $t = 25\ min$. T = o, $C_A = \times$, $C_B = \diamond$, $C_C = \star$.

Failures in d_1 were introduced as a step change of magnitude 1 $kmol/m^3s$ and in d_2 as a step change of magnitude 10 K/s. These faults change the equilibrium point of system (8) to an undesired state. Hotelling's statistic (1) and normalized error plots (3) were used to monitor the closed-loop system.

Simulating the closed-loop system under feedback-linearizing control with a fault in d_1 (see Figure 1), the T^2 statistic shows a failure at $t = 25\ min$. The normalized error plot clearly shows that the output was not affected by the failure. In the case of proportional control with a failure in d_1 (see Figure 2), the T^2 statistic accurately shows that the failure occurred around time $t = 25\ min$. In this simulation, each of the state trajectories was affected by the failure. In the case of a failure in d_2, both proportional control and feedback-linearizing control show failures at $t = 25\ min$ as well as changes in the normalized error plots for all states, see Figures 3, 4.

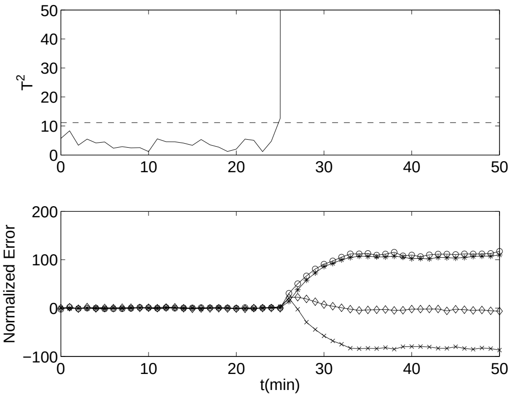

Fig. 3. System under feedback-linearizing control. Upper figure: plot of T^2 (solid) with T_{UCL} (dashed). Lower figure: each state's normalized error, with a failure in d_2 at $t = 25\ min$. $T =$ o, $C_A = \times$, $C_B = \diamond$, $C_C = \star$.

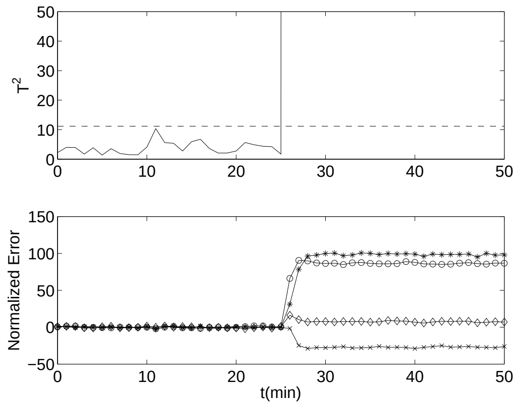

Fig. 4. System under proportional control. Upper figure: plot of T^2 (solid) with T_{UCL} (dashed). Lower figure: each state's normalized error, with a failure in d_2 at $t = 25\ min$. $T =$ o, C_A $= \times$, $C_B = \diamond$, $C_C = \star$.

Looking at the normalized error plot of the output in Figures 1 and 3, it is clear that fault d_1 did not affect the output whereas d_2 did. Fault d_2 is relative degree 2 and thus affects the output, while d_1 is relative degree 3 and does not. In this situation, where we consider only one fault in each group, we can successfully identify the failure in Figure 1 as d_1. However, for proportional control, all of the states were affected by each failure (see Figures 2, 4) leaving an unclear picture as to the cause of the fault. Although prior knowledge of faulty behavior could possibly narrow down the likely fault or even isolate the fault, it is not readily apparent from the recorded data.

The feedback-linearizing controller is not an optimal control scheme. Nonetheless, Figure 5 shows that the requested control action is not excessive and is comparable to the one requested by the proportional controller.

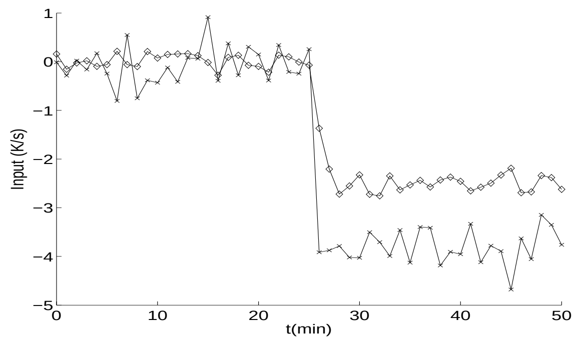

Fig. 5. Manipulated input profiles for both the proportional controller ($\diamond$) and the feedback-linearizing controller ($\times$)

REFERENCES

J. Bao, W. Z. Zhang, and P. L. Lee. Passivity-based decentralized failure-tolerant control. *Ind. & Eng. Chem. Res.*, 41:5702–5715, 2002.

P. Daoutidis and C. Kravaris. Synthesis of feedforward state feedback controllers for nonlinear processes. *AIChE Journal*, 35:1602–1616, 1989.

J. Gertler, L. Weihua, Y. Huang, and T.J. McAvoy. Isolation enhanced prinicpal component analysis. *AIChE Journal*, 45:323–334, 1999.

A. Isidori. *Nonlinear Control Systems: An Introduction.* Springer-Verlag, Berlin-Heidelberg, second edition, 1989.

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

P. Mhaskar, C. McFall, A. Gani, P.D. Christofides, and J.F. Davis. Fault-tolerant control of nonlinear systems: Fault-detection and isolation and controller reconfiguration. Submitted, *Automatica*, 2006.

J.A. Romagnoli and A. Palazoglu. *Introduction to Process Control.* CRC Press, 2006.

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

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

G. H. Yang, S. Y. Zhang, J. Lam, and J. Wang. Reliable control using redundant controllers. *IEEE Transactions on Automatic Control*, 43: 1588–1593, 1998.

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