UNIVERSITY OF CALIFORNIA

Los Angeles

Data-based Fault Detection and Isolation for Nonlinear Process Systems Using Feedback Control

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Chemical Engineering

by

Benjamin J. Ohran

2009

The dissertation of Benjamin J. Ohran is approved.

Tsu-Ci Tsao

Tsu-Chin Tsao

Gerassimos Orkoulas

James F. Davis

P. D. Christofide

Panagiotis D. Christofides, Committee Chair

University of California, Los Angeles

2009

Contents

List of Figures

List of Tables

ACKNOWLEDGEMENTS

Chapter 2 is a version of B. J. Ohran, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Enhancing data-based fault isolation through nonlinear control. *AIChE Journal*, 54, 223–241, 2008.

Chapter 3 is a version of B. J. Ohran, J. Rau, P. D. Christofides and J. F. Davis. Plant-wide fault isolation using nonlinear feedback control. *Industrial & Engineering Chemistry Research*, 47, 4220–4229, 2008

Chapter 4 is a version of B. J. Ohran, J. Liu, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Data-based fault detection and isolation using feedback control: Output feedback and optimality. *Chemical Engineering Science*, in press, 2009.

Chapter 5 is a version of C. McFall, D. Muñoz de la Peña, B. J. Ohran, P. D. Christofides and J. F. Davis. Fault-detection and isolation for nonlinear process systems using asynchronous measurements. *Industrial & Engineering Chemistry Research*, 47, 10009–10019, 2008.

I would like to acknowledge the contributions of Jinfeng Liu, David Muñoz de la Peña, Panagiotis D. Christofides and James F. Davis to Chapter 6.

Financial support from NSF, CBET-0652131, and from UCLA Graduate Division, Doctoral Dissertation Year Fellowship for Benjamin J. Ohran, is gratefully acknowledged.

I would like to thank my advisors, Panagiotis D. Christofides and James F. Davis, for their direction and support.

I would like to thank my wife and children for their patience and encouragement.

VITA

October 1, 1978	Born, Zurich, Switzerland
2003	Visiting Researcher Åbo Akademi Turku, Finland
2003	Process Engineering Intern Celanese Chemical Pampa, Texas
2004	Bachelor of Science, Chemical Engineering Brigham Young University Provo, Utah
2005	Software Developer Quomation Insurance Services Provo, Utah
2006–2008	Teaching Assistant Department of Chemical Engineering University of California, Los Angeles
2008	Teaching Assistant of the Year Award Department of Chemical Engineering University of California, Los Angeles
2008	Dissertation Year Fellowship Department of Chemical Engineering University of California, Los Angeles

PUBLICATIONS AND PRESENTATIONS

1. Liu, J., D. Muñoz de la Peña, B. J. Ohran, P. D. Christofides and J. F. Davis. A two-tier architecture for networked process control. *Chemical Engineering Science*, 63, 5349–5409, 2008.

2. Liu., J., D. Muñoz de la Peña, B. J. Ohran, P. D. Christofides and J. F. Davis. A two-tier control architecture for nonlinear process systems with continuous/asynchronous feedback. *Proceedings of the American Control Conference*, in press, St. Louis, MO,

2009.

3. Lundmark, D., B. J. Ohran, C. Mueller and M. Hupa. Simulation of BFBCs fired with biofuel mixtures A CFD based modelling concept *Proceedings of the 46th IEA FBC Meeting*, Jacksonville, FL, 2003.

4. McFall, C., B. J. Ohran, P. D. Christofides and J. F. Davis. Fault-detection and isolation and fault-tolerant control of nonlinear process systems using asynchronous measurements *AIChE Annual Meeting*, Philadelphia, PA, 2008.

5. McFall, C., D. Muñoz de la Peña, B. J. Ohran, P. D. Christofides and J. F. Davis. Fault-detection and isolation of a polyethylene reactor using asynchronous measurements. *Proceedings of the American Control Conference*, in press, St. Louis, MO, 2009.

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

7. Ohran, B. J., D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Data-based fault detection and isolation using feedback control: Output feedback and optimality. *AIChE Annual Meeting*, Philidelphia, PA, 2008.

8. Ohran, B. J., D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Enhancing data-based fault isolation through feedback control. *AIChE Annual Meeting*, Salt Lake City, UT, 2007.

9. Ohran, B. J., D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Enhancing data-based fault isolation through nonlinear control. *AIChE Journal*, 54, 223–241, 2008.

10. Ohran, B. J., D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Enhancing data-based fault isolation through nonlinear control: Application to a polyethylene reactor. *Proceedings of the American Control Conference*, 3299–3306, Seattle, WA, 2008.

11. Ohran, B. J., J. Liu, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Data-based fault detection and isolation using feedback control: Output feedback and optimality. *Chemical Engineering Science*, 64, 2370–2383, 2009.

12. Ohran, B. J., J. Liu, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Data-based fault detection and isolation using output feedback control. *Proceedings of the IFAC International Symposium on Advanced Control of Chemical Processes*, in press, Istanbul, Turkey, 2009.

13. Ohran, B. J., J. Rau, P. D. Christofides and J. F. Davis. Controller enhanced fault detection and isolation in a reactor-separator system. *Proceedings of the American Control Conference*, 1499–1506, Seattle, WA, 2008.

14. Ohran, B. J., M. M. Choi and L. L. Baxter. A comprehensive 3-D CFD bed model *Advanced Combustion Engineering Research Center Conference*, Provo, UT, 2004.

15. Ohran, B. J., M. M. Choi, S. Kær and L. L. Baxter. Comprehensive, three-dimensional CFD model of a reacting char bed *Proceedings of the International Chemical Recovery Conference*, Charleston, SC, 2004.

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

17. Ohran, B. J., P. Mhaskar, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Enhancing fault isolation through nonlinear controller design. *Proceedings of 8th IFAC Symposium on Dynamics and Control of Process Systems*, 81–86, Cancun, Mexico, 2007.

18. Ohran, B. J., P. Mhaskar, D. Muñoz de la Peña, P. D. Christofides and J. F. Davis. Uniting data-based fault-diagnosis and model-based controller design techniques for enhanced fault isolation. *AIChE Annual Meeting*, San Francisco, CA, 2006.

ABSTRACT OF THE DISSERTATION

Data-based Fault Detection and Isolation
for Nonlinear Process Systems Using Feedback Control

by

Benjamin J. Ohran

Doctor of Philosophy in Chemical Engineering
University of California, Los Angeles, 2009
Professor Panagiotis D. Christofides, Chair

Handling abnormal situations, like control actuator, measurement sensor and control system faults, is a subject of great importance in the chemical and process industries since abnormal situations account annually for at least $20 billion in lost revenue in the US alone. Modern chemical plants that rely on highly automated processes to maintain robust operation and efficient production are particularly vulnerable to these faults. 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 but more importantly it may lead to personnel injury or death. However, the existing paradigm to plant operations deals with the key tasks of designing control systems and monitoring schemes for detecting faults separately, thereby liming its applicability since it does not take advantage of an efficient integration of these tasks.

This dissertation will present a paradigm shift to the existing approach of designing control systems and monitoring schemes in that it proposes to design control systems that are stabilizing, robust and optimal yet, they also lead to closed-loop system structures that facilitate fault isolation. To present our new method of controller-enhanced isolation, we will focus on a broad class of nonlinear process systems subject to control actuator faults and disturbances. The method allows isolating faults in the closed-loop system by designing

nonlinear model-based control laws that decouple the dependency between certain process state variables 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. We will discuss extensions of the basic framework to deal with the issues of limited state measurements, controller optimality and networked implementation. We will present examples of large-scale process systems to demonstrate the effectiveness and benefits of the proposed method.

Chapter 1

Introduction

1.1 Background on fault detection and isolation and fault-tolerant control

Advanced automation technology has changed the way the chemical process industry operates in many ways. Over the last few decades, advancements in plant operations have led to higher efficiency and improved economics through better control and monitoring of process systems. These technological advances have resulted in process systems becoming increasingly automated, no longer requiring operators to open and close valves in order to manually perform process control. In general, there is a trend towards “smart” plants that are capable of highly automated control with decision making at the plant level taking into account environmental, health, safety and economic considerations [7]. Along with the move towards more automated plant operation, improved methods of fault detection, isolation and handling are necessary due to the issues raised by automation itself. Despite the many benefits of automatic process control, increased complexity and instrumentation can cause automated plants to become more susceptible to control system failures. Abnormal situations cost U.S. industries over $20 billion each year [54]. As part of the continuing improvements to process monitoring and control, it is important to design systems capable of detecting and handling such process or control system abnormalities.

Over the past ten years, fault-tolerant control has become an active area of research within control engineering as a means for avoiding disaster in the case of a fault, see for example, [44, 46, 18, 21, 43]. Many research studies can be found in the field of aerospace control engineering [56, 5, 73] as well as within chemical process control [4, 44, 46]. Fault-tolerant control is based upon the assumption that there exist multiple available control configurations under which the closed-loop system can operate. Using this redundancy, fault tolerant control attempts to reconfigure a process control system upon detection of a fault, in order to preserve closed-loop system stability and performance. This work addresses active methods of FTC, as opposed to passive methods which rely on robust controller design rather than control system reconfiguration. The key elements of a successful FTC system include multiple control configurations with well-defined regions of closed-loop stability, a supervisor that is able to switch between faulty and well-functioning control configurations, and perhaps most importantly, a fast, accurate method for detecting faulty process behavior and isolating its cause.

In this work, the main focus will be on fault detection and isolation, 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, [70, 45] 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, [22, 65]). 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., [60, 72]) or with expected behavior as predicted by the structure or model of the system. Several methods have been developed that process the measured data to reduce their dimension and extract information from the data with respect to actuator/sensor faults using principle component analysis (PCA) or partial least squares (PLS) techniques (e.g., [35, 69, 58, 53]). 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 as well as about actuator/sensor faults, including techniques such as contribution plots (e.g., [31]) or multi-scale statistical process control using wavelets (e.g., [3, 2, 1]). 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 the 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 [65, 64].

In general, most of the FDI methods mentioned thus far rely on measurements that are continuously or synchronously sampled, and they do not account for measurements that arrive asynchronously. Recently, research has been done on the topic of feedback control with asynchronous measurements [46, 51]. These efforts provide a starting framework for control subject to asynchronous measurements, but they do not include FDI. Because it is common in chemical processes to encounter states that are measurable, but only on an asynchronous or infrequent basis, the issue of FDI in such systems is also addressed. The issue of asynchronous sensor measurements also motivates, in general, a discussion of networked monitoring and control systems that take advantage of these additional measurements. Although there are many works in the literature focusing on the analysis and design of networked control systems [52, 62, 48, 49], from a control design standpoint, augmenting preexisting, local control networks with additional networked sensors and actuators poses a number of challenges including the feedback of additional measurements that may be asynchronous and/or delayed, for example, additional species concentrations or particle size distribution measurements. In a previous work [32], we introduced a two-tier control architecture for nonlinear process systems with both continuous and asynchronous sensing and/or actuation. This class of systems arises naturally in the context of process control systems based on point-to-point wired links integrated with networked wired/wireless communication and utilizing multiple heterogeneous measurements (e.g., temperature and concentration). In this architecture, the local, pre-existing control system uses continuous sensing and actuation and an explicit control law (for example, the local controller may be a classical controller, like a proportional-integral-derivative controller, or a nonlinear controller designed via geometric or Lyapunov-based control methods for which an explicit formula for the calculation of the control action is available). In addition, a networked control system was designed using Lyapunov-based model predictive control to profit from both the continuous and the asynchronous measurements as well as from additional networked control actuators. The two-tier control architecture preserves the stability properties of the local control system while improving the closed-loop performance.

1.2 Dissertation objectives and structure

The objective of this dissertation is to present novel methods of fault detection and isolation within the framework of fault-tolerant control and the "smart plant" paradigm. This is accomplished through the development of a data-based fault detection and isolation technique using feedback control, a model-based approach to fault detection and isolation in systems with asynchronously measured states and integration of asynchronous, model-based fault detection and isolation methods with fault-tolerant control and two-tier control. These techniques allow for quick, accurate fault detection and isolation in nonlinear process systems subject to process and control system failures. This information can then potentially be used for logic-based switching between the faulty control configuration and any well-functioning redundant configurations in a fault-tolerant control scheme. These methods are developed theoretically and demonstrated through numerical simulation.

The structure of this dissertation is as follows: first, the method of data-based fault detection and isolation using feedback control is developed in Chapter 2. Specifically, it is demonstrated in this chapter 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. This set of isolability conditions is explicitly characterized and it is shown 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 continuous stirred tank reactor (CSTR) example and to a polyethylene reactor example.

Chapter 3 further extends the results of Chapter 2 to a plant-wide setting with a multiple-input multiple-output reactor-reactor-separator system. The focus of this chapter is to demonstrate in a plant-wide setting the fault detection and isolation that integrates model-based controller design with data-based fault detection in order to perform fault isolation. The work demonstrates that the achievement of fault isolation across multiple coupled units is possible through feedback control. Additionally the effects of process and sensor measurement noise on the ability to detect and accurately isolate faults are investigated through a Monte-Carlo simulation study. The results from the nonlinear control simulation are compared with a conventional (proportional-integral) feedback controller to demonstrate that without the isolable structure induced by feedback control the faults are otherwise indistinguishable without prior knowledge of fault history.

Chapter 4 considers the issues of output-feedback control and optimal control in the setting of data-based FDI using feedback control. The purpose this chapter is to further develop the approach proposed in Chapter 2 by relaxing the requirement of full state feedback control and developing the use of model predictive control to optimize the manipulated input cost. Specifically, we first consider the case where only output measurements are available and design appropriate state estimator-based output feedback controllers to achieve controller-enhanced fault detection and isolation in the closed-loop system. Second, we address the problem of controller-enhanced FDI in an optimal fashion within the framework of model predictive control (MPC). We propose an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. Throughout the chapter, a nonlinear chemical process example is used to demonstrate the applicability and effectiveness of the proposed methods.

The goal of chapter 5 is to develop an FDI scheme that will allow fault tolerant control to take place when process measurements are available at asynchronous time instants. First, an FDI scheme that employs model-based techniques is proposed that allows for the isolation of faults. This scheme employs model-based FDI filters similar to those found in [47] in addition to observers that estimate the fault free evolution of asynchronously measured states during time intervals in which their measurements are not available. Specifically, the proposed FDI scheme provides detection and isolation of any fault that enters into the differential equation of only synchronously measured states, and grouping of faults that enter into the differential equation of any asynchronously measured state. For a fully coupled process system, fault detection occurs shortly after a fault takes place, and fault isolation, limited by the arrival of asynchronous measurements, occurs when asynchronous measurements become available. Once the FDI methodology has provided the system supervisor with a fault diagnosis, the supervisor takes appropriate action to seamlessly reconfigure the system to an alternative control configuration that will enforce the desired operation. Applications of the proposed asynchronous FDI and FTC framework to a polyethylene reactor simulation [37] are presented.

Chapter 6 focuses on the monitoring and reconfiguration of a two-tier networked control system for a chemical process in the presence of control actuator faults. Specifically, a chemical process system is considered and is controlled by a two-tier networked control system integrating a local control system using continuous sensing/actuation with a networked control system using asynchronous sensing/actuation. To deal with control actuator faults that may occur in the closed-loop system, a networked fault detection and isolation (FDI) and fault-tolerant control (FTC) system is designed which detects and isolates actuator faults and determines how to reconfigure the two-tier networked control system to handle the actuator faults. The FDI/FTC system uses continuous measurements of process variables like temperatures and asynchronous measurements of variables like concentrations. The method is demonstrated using a reactor-separator process consisting of two continuous stirred tank reactors and a flash tank separator with recycle stream.

Chapter 2

Controller enhanced fault detection and isolation

2.1 Introduction

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 2.1(a) 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 chapter is to investigate the possibility of integrating the feedback control design with the data-based FDI scheme. This paradigm shift is illustrated in Figure 2.1(b) which demonstrates the idea of designing both 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 above considerations motivate the development of a data-based method of 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

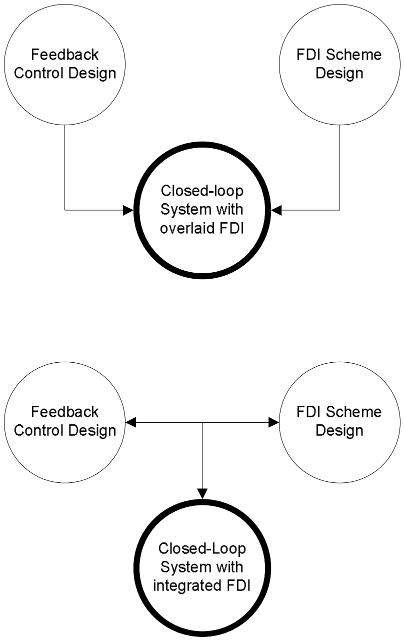


Figure 2.1: (a) (top) Common methods of fault diagnosis apply the FDI scheme and feedback control law to the closed-loop system independently from each other. (b) (bottom) This work proposes integrating the feedback control law design with the FDI scheme in the closed-loop system.

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 continuous stirred tank reactor (CSTR) example and to a polyethylene reactor example. It should also be noted that although the examples given in this chapter 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.

2.2 Preliminaries

2.2.1 Process model

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

$$\dot{x} = f(x, u, d) \tag{2.1}$$

where $x \in R^n$ denotes the vector of process state variables, $u \in R^m$ denotes the vector of manipulated input variables and $d \in R^p$ 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.2.1 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 that 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.2.1. Subsequently, we will introduce additive autocorrelated noise in the right-hand side of Eq.2.1 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 *[29]: The system of Eq.2.1 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.2.1 exists for each $t \geq 0$ with $x(0) = x_0$ and satisfies*

$$|x(t)| \leq \beta(|x(0)|, t) + \gamma(||u||), \ \forall t \geq 0. \tag{2.2}$$

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.2.1 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 logical 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 single time instance during the process operation than it is that two or more control actuators will fail at exactly the same instance of 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 by using model-based state estimator design techniques for nonlinear systems (e.g., [8]) to construct dynamic systems which yield estimates of the unmeasured states from the output measurements; however, the detailed development of the results for this case is outside the scope of the present 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, [67, 39, 68, 59, 40, 17]). Note that 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 [26]. This kind of graph-theoretic analysis has been applied before in the context of feedback control of nonlinear systems (see, for example, [11]).

Definition 2*: The incidence graph of an autonomous system $\dot{x} = f(x)$ with $x \in R^n$ 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

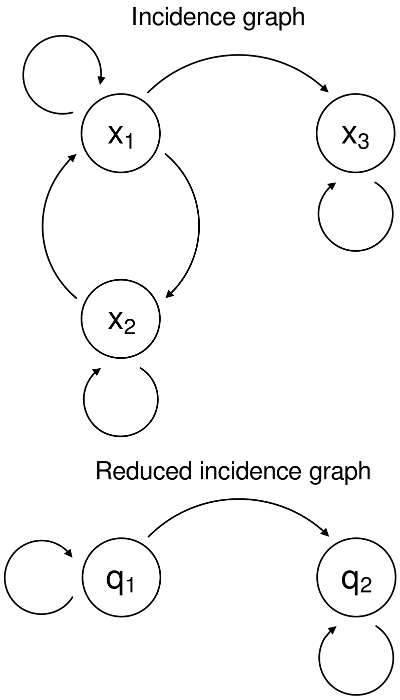


Figure 2.2: Incidence graph and reduced incidence graph for the system of Eq.2.3.

states. Figure 2.2 shows the incidence graph of the following system:

$$\begin{aligned} \dot{x}_1 &= -2x_1 + x_2 + d_1 \\ \dot{x}_2 &= -2x_2 + x_1 + d_2 \\ \dot{x}_3 &= -2x_3 + x_1 + d_3 \end{aligned} \tag{2.3}$$

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 $x \in R^n$ is the directed graph of nodes q_i, where $i = 1, ..., N$, 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.2.3 there is a loop that contains states x_1 and x_2. The reduced incidence graph of the system of Eq.2.3 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 2.2 shows the reduced incidence graph of the system of Eq.2.3. It can be seen that in the reduced incidence graph there are no loops.

Remark 1: *In the process model of Eq.2.1, process and sensor noise are not explicitly taken into account. However, noise is indirectly 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 Section 2.5 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 [71] 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.*

2.2.2 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 [27]. 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:

$$T^2 = m(X - \bar{X})^T S^{-1}(X - \bar{X}). \tag{2.4}$$

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

$$T^2 \sim \frac{mn}{(m - n + 1)} F(n, m - n + 1) \tag{2.5}$$

where $F(n, m - n + 1)$ is the F distribution 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, $P(T^2 \geq T^2_{UCL}) = \alpha$.

$$T^2_{UCL} = \frac{mn}{(m - n + 1)} F_\alpha(n, m - n + 1) \tag{2.6}$$

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 above, 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 [50]:

$$T^2_{UCL} = \frac{n(h-1)(m-1)}{hm-h-n+1} F_\alpha(n, hm-h-n+1) \tag{2.7}$$

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:

$$T^2_{UCL} = \frac{n(h+1)(m-1)}{hm-h-n+1} F_\alpha(n, hm-h-n+1) \tag{2.8}$$

Note that when h is large, these limits are nearly identical. In addition, it is often convenient to use a sample size of $m = 1$ where individual observations are monitored (i.e., [50, 63]). This is commonly used in data-based fault detection and isolation methods (see, for example, [60, 31, 50, 69, 63]). In this scenario, the UCL becomes:

$$T^2_{UCL} = \frac{(h^2-1)n}{h(h-n)} F_\alpha(n, h-n) \tag{2.9}$$

where h is now the total number of historical measurements used to evaluate the covariance matrix S. In the simulation section of this chapter, 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.2.6 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.2.9 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 [57] and [34]. This idea for data-based isolation using the T^2 statistic for each subsystem is also utilized in the context of the proposed method in the next section.

Remark 3: *Note that the methods of fault detection 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.*

2.3 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 statistics such as the T^2 statistic presented in the previous section cannot be used to perform fault isolation when applied globally. To understand this point in the context of a specific example, consider the system of Eq.2.3. It can be seen based upon 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

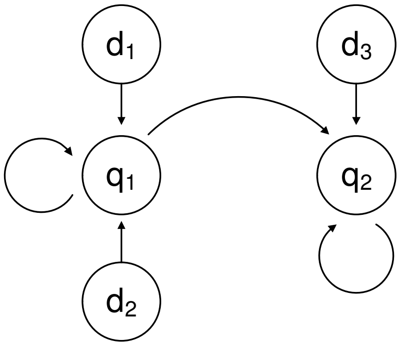


Figure 2.3: Isolability graph for the system of Eq.2.3.

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 above 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 $x \in R^n$, $d \in R^p$ 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 $\frac{\partial f_l}{\partial d_k} \neq 0$ for some $x_l \in X_j$.*

Figure 2.3 shows the isolability graph of the system of Eq.2.3. 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 $x \in R^n$, $d \in R^p$ 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_i^k, 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.*

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.2.3 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 states and upon detection of a fault with the signature $W^1 = [1\ 1]^T$, it is not possible to distinguish between them based upon 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.2.3 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 for a sufficiently large period of time to allow isolation of 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.2.1 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_i^2 statistic with $i = 1, \dots, N$ 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_i^2 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 $T^2(t) > T^2_{UCL}$, $\forall t \, t_f \leq t \leq T_P$, 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:

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

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

   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 above 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_{UCLi}^2, $\forall t,\ t_f \leq t \leq T_P$. It is assumed that if a fault d_k is not large enough to cause $T_i^2(t)$ to exceed the threshold T_{UCLi}^2, $\forall t,\ t_f \leq t \leq T_P$ (where t_f is the time in which $T_i^2(t_f) \geq T_{UCL}^2$ 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* $T_i^2(t) \not> T_{UCLi}^2$, $\forall t,\ t_f \leq t \leq T_P$, *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 a practical point of view. These conditions are not restrictive in the sense 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* $r \leq n$ *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.*

2.4 Controller enhanced isolation

2.4.1 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 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. The achievement of this key requirement can be accomplished by 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:

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + f_{12}(x_1, x_2) + g_1(x_1, x_2)u + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2 \end{aligned} \tag{2.10}$$

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

$$u(x_1, x_2) = -\frac{f_{12}(x_1, x_2) - v(x_1)}{g_1(x_1, x_2)} \tag{2.11}$$

the closed-loop system takes the form

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + v(x_1) + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2 \end{aligned} \tag{2.12}$$

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 [19, 20, 30, 8] 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 above 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.

2.4.2 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

$$\begin{aligned} \dot{x} &= f(x) + g(x)u + \sum_{k=1}^{p} w_k(x)d_k \\ y &= h(x) \end{aligned} \tag{2.13}$$

where $x \in R^n$ is the state, $u \in R$ is the input, $y \in R$ is the controlled output and $d_k \in R$ represents a possible fault. It is assumed that f, g, h and w_k are sufficiently smooth functions, 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 $u(t) = 0$, $d_k(t) \equiv 0$ 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.2.13.

Definition 6 *[28]: Referring to the system of Eq.2.13, 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, [28]). To be specific, if the system of Eq.2.13 has input relative degree $r < n$, then there exists a coordinate transformation (see [28]) $(\zeta, \eta) = T(x)$ such that the representation of the system of Eq.2.13 with $d_k = 0$ for all $k = 1, ..., p$ (that is, the system without faults), in the (ζ, η) coordinates, takes the form

$$\begin{aligned}
\dot{\zeta}_1 &= \zeta_2 \\
&\vdots \\
\dot{\zeta}_{r-1} &= \zeta_r \\
\dot{\zeta}_r &= L_f^r h(x) + L_g L_f^{r-1} g(x) u \\
\dot{\eta}_1 &= \Psi_1(\zeta, \eta) \\
&\vdots \\
\dot{\eta}_{n-r} &= \Psi_{n-r}(\zeta, \eta)
\end{aligned} \tag{2.14}$$

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 *[28]: Consider the system of Eq.2.13 with $d_k = 0$ for all $k = 1, ..., p$ under the feedback law*

$$u(x) = \frac{1}{L_g L_f^{r-1} h(x)} [K T_\zeta(x) - L_f^r h(x)] \tag{2.15}$$

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.

We prove that under certain assumptions, if the state-feedback law given in Eq.2.15 is used, then the faults of system of Eq.2.13 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 below (this definition was introduced in [10] 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 *[10]: Referring to the system of Eq.2.13, 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*

$$\begin{aligned} &L_{w_k} L_f^i h(x) = 0, \ i = 0, \ldots, \rho_k - 2 \\ &L_{w_k} L_f^{\rho_k - 1} h(x) \neq 0. \end{aligned} \tag{2.16}$$

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 [28]) a coordinate transformation $(\zeta, \eta) = T(x)$ such that the representation of the system of Eq.2.13 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

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

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.2.15, 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.2.13 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.2.15 is used, the possible faults of the system of Eq.2.13 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.*

2.5 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 example 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 example 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.

2.5.1 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

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

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

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

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

$$\begin{aligned} \dot{C_A} &= \tfrac{F}{V}(C_{A0} - C_A) - r_1 + r_{-1} + d_1 \\ \dot{C_B} &= -\tfrac{F}{V} C_B + r_1 - r_{-1} - r_2 + r_{-2} \\ \dot{C_C} &= -\tfrac{F}{V} C_C + r_2 - r_{-2} \\ \dot{T} &= \tfrac{F}{V}(T_0 - T) + \tfrac{(-\Delta H_1)}{\rho c_p}(r_1 - r_{-1}) + \tfrac{(-\Delta H_2)}{\rho c_p}(r_2 - r_{-2}) + u + d_2 \end{aligned} \tag{2.17}$$

Table 2.1: 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	$0.231\ [kJ/kg \cdot K]$		

Table 2.2: 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

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.2.17 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 2.2 provides the values of the noise parameters for each state of the system of Eq.2.17. 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 opera-

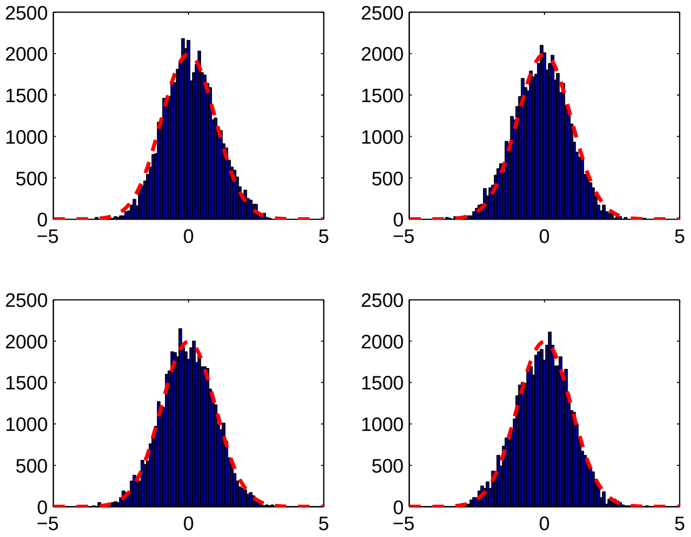


Figure 2.4: CSTR example. Distribution of normalized, fault-free operating data compared with a normal distribution of the same mean and variance.

tion are approximately normal (see [50]). Figure 2.4 shows the distribution of the state measurements of the closed-loop system of Eq.2.17 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 2.1.

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

$$C_{Cs} = 0.9471\frac{kmol}{m^3},\ T_s = 312.6K,\ u_s = 0K/s. \tag{2.18}$$

where the subscript s refers to the steady state value at equilibrium. To this end, we consider two different feedback controllers: 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.2.15 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 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 2.5. 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

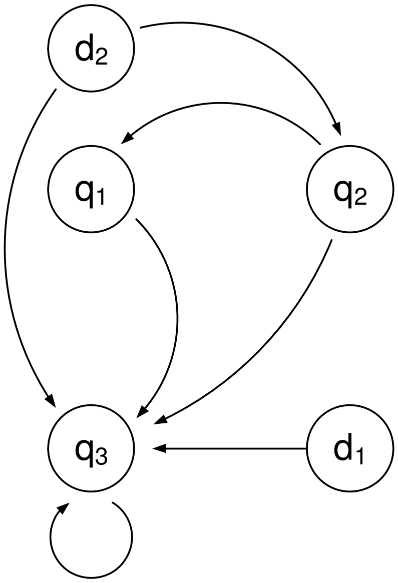


Figure 2.5: Isolability graph for the system of Eq.2.17. $v1 = \{\zeta_1\}$, $v2 = \{\zeta_2\}$ and $v3 = \{\eta\}$.

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 above, 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.2.17 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.2.18 with a failure appearing at time $t = 0.5\ hr$.

Based upon 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 above. Hotelling's statistic (Eq.2.4) 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

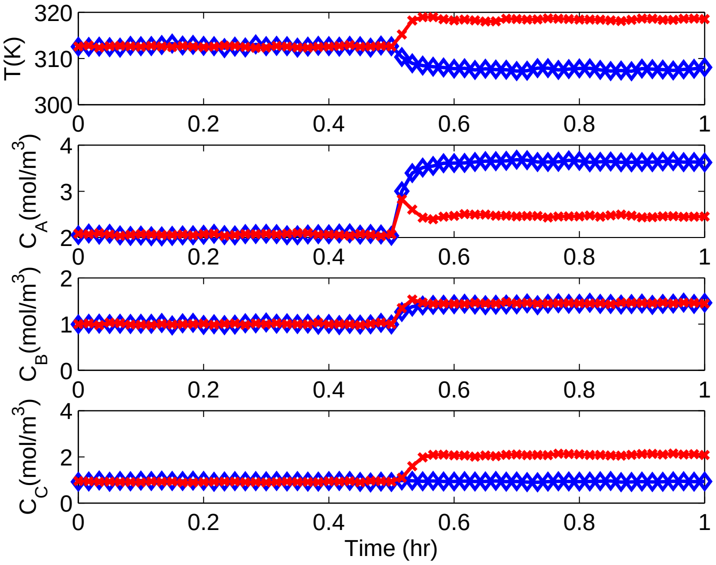


Figure 2.6: CSTR example. State trajectories of the closed-loop system under feedback-linearizing ($\diamond$) and P ($\times$) control with a fault d_1 at $t = 0.5hr$.

T^2_{UCL} defined in Eq.2.6 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 1 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.2.9. 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 above. A fault in d_1 was introduced as a step change of magnitude 1 $kmol/m^3s$. Figure 2.6 shows the state trajectories for the closed-loop system under the proportional and the feedback-linearizing

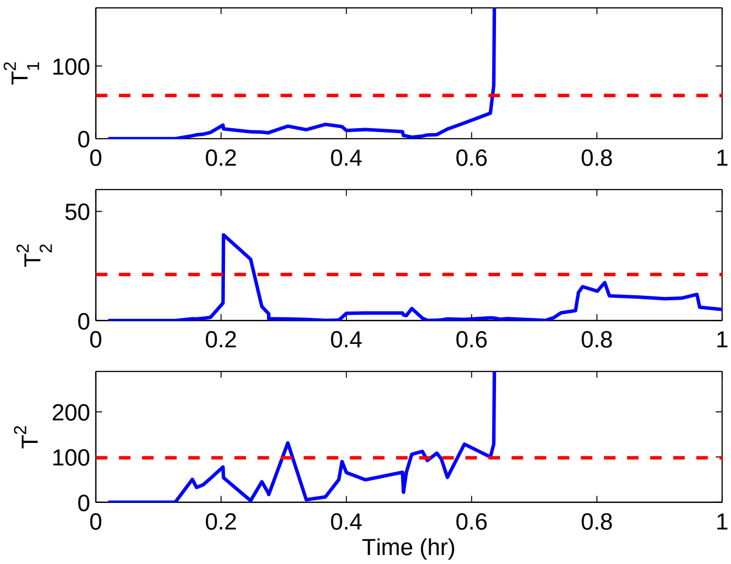


Figure 2.7: CSTR example. Closed-loop system under feedback-linearizing control with sample size $m = 10$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at $t = 0.5\ hr$.

controller. Figure 2.7 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.2.6 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 2.8 shows the T^2 statistic for the same results, calculated instead from individual observations ($m = 1$) using the UCL from Eq.2.9 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 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

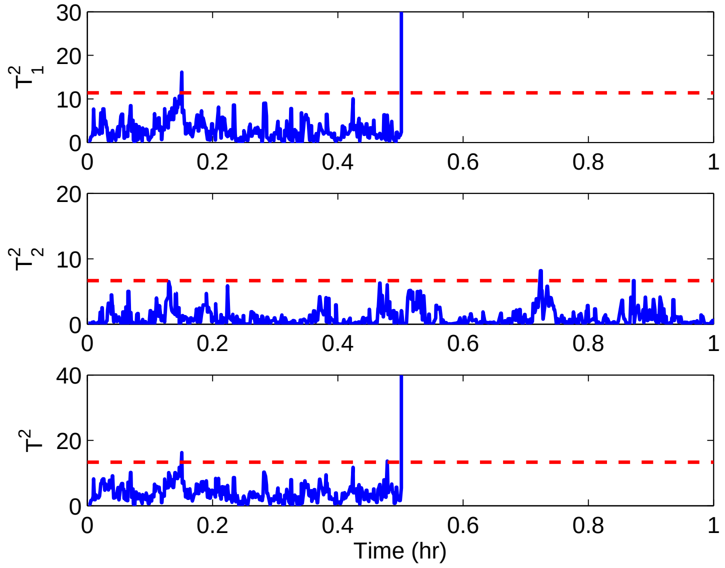


Figure 2.8: CSTR example. Closed-loop system under feedback-linearizing control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at $t = 0.5$ hr.

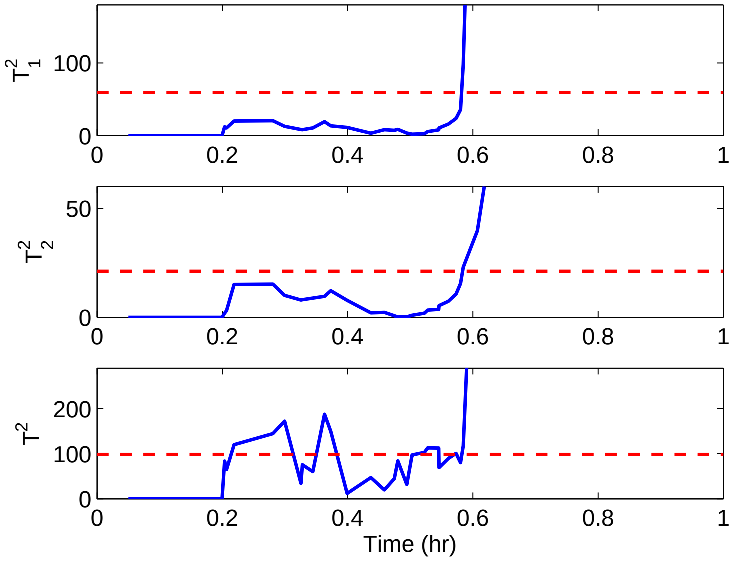


Figure 2.9: CSTR example. Closed-loop system under proportional control with sample size $m = 10$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at $t = 0.5$ hr.

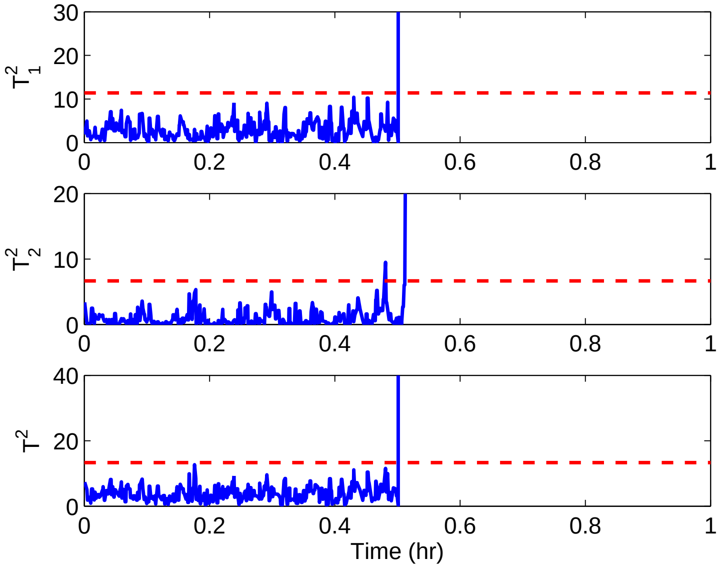


Figure 2.10: CSTR example. Closed-loop system under proportional control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_1 at $t = 0.5$ hr.

that the failure occurred around time $t = 0.5$ hr. Figures 2.9 and 2.10 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 2.11 and 2.12. Looking at T_1^2 and T_2^2 in Figures 2.8 and 2.11, 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 2.8 as d_1. However, for proportional control, all of the states were affected by each failure (see Figures 2.10 and 2.12) 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

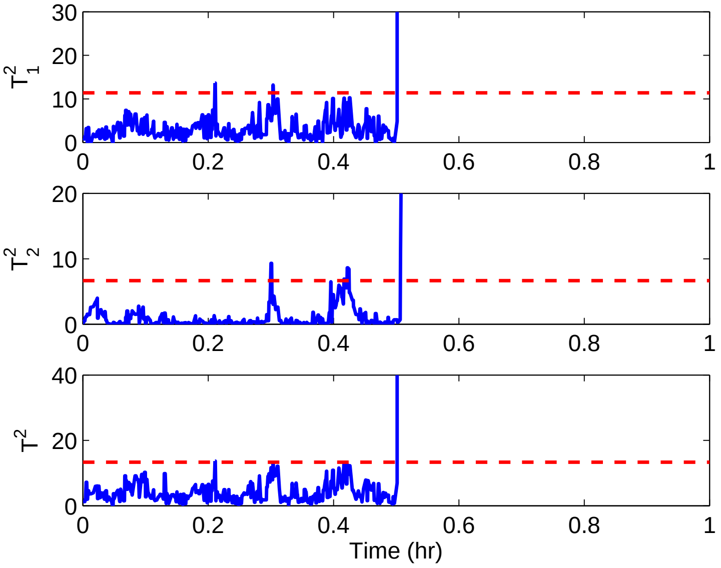


Figure 2.11: CSTR example. Closed-loop system under feedback-linearizing control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_2 at $t = 0.5$ hr.

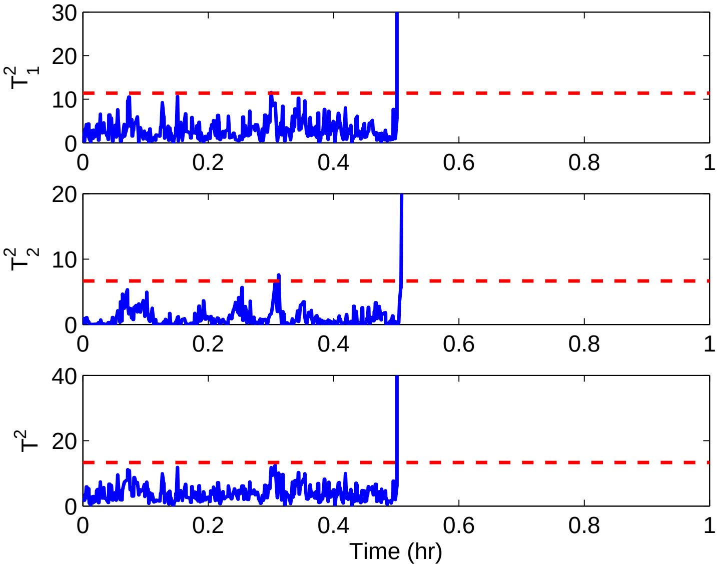


Figure 2.12: CSTR example. Closed-loop system under proportional control with sample size $m = 1$. Statistics T^2, T_1^2 and T_2^2 (solid) with T_{UCL} (dashed) with a failure in d_2 at $t = 0.5$ hr.

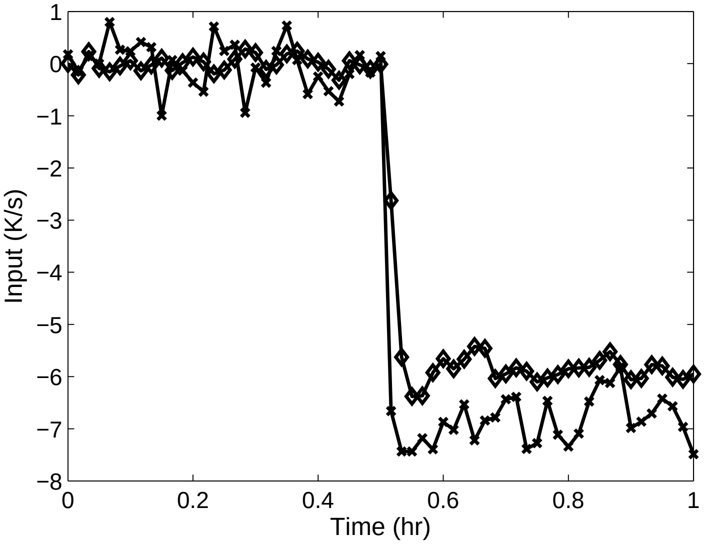


Figure 2.13: CSTR example. Manipulated input profiles for both the proportional controller ($\diamond$) and the feedback-linearizing controller ($\times$) with a failure in d_1 at time $t = 0.5\ hr$

and sensor noise variance. Only a fault in d_1 was considered with values ranging from 0 to 3 $kmol/m^3s$. 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 2.2. A single observation T^2 statistic was used with the associated 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 $30.7min$. 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 2.13 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 upon 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 timescale. A small number of observations in a sample can lead to an almost singular S, while on the* *other hand, the predicted distribution for a large number of observations per sample becomes increasingly narrow which 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 timescale, 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.*

2.5.2 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 have only mild effects on the reactor dynamics [37]. A mathematical model for this reactor has the following form ([9]):

$$\begin{aligned}
\frac{d[In]}{dt} &= \frac{1}{V_g}(F_{In} - \frac{[In]}{[M_1]+[In]}b_t) \\
\frac{d[M_1]}{dt} &= \frac{1}{V_g}(F_{M_1} - \frac{[M_1]}{[M_1]+[In]}b_t - R_{M1}) \\
\frac{dY_1}{dt} &= F_c a_c - k_{d_1}Y_1 - \frac{R_{M1}M_{W_1}Y_1}{B_w} + d_2 \\
\frac{dY_2}{dt} &= F_c a_c - k_{d_2}Y_2 - \frac{R_{M1}M_{W_1}Y_2}{B_w} + d_2 \\
\frac{dT}{dt} &= \frac{H_f + H_{g1} - H_{g0} - H_r - H_{pol}}{M_r C_{pr} + B_w C_{ppol}} + d_1 \\
\frac{dT_{w_1}}{dt} &= \frac{F_w}{M_w}(T_{wi} - T_{w_1}) - \frac{UA}{M_w C_{pw}}(T_{w_1} - T_{g_1}) \\
\frac{dT_{g_1}}{dt} &= \frac{F_g}{M_g}(T - T_{g_1}) + \frac{UA}{M_g C_{pg}}(T_{w_1} - T_{g_1}) + d_3
\end{aligned} \tag{2.19}$$

where

$$
\begin{aligned}
b_t &= V_p C_v \sqrt{([M_1]+[In])RRT - P_v} \\
R_{M1} &= [M_1] k_{p0} e^{\frac{-E_a}{R}(\frac{1}{T}-\frac{1}{T_f})}(Y_1+Y_2) \\
C_{pg} &= \frac{[M_1]}{[M_1]+[In]} C_{pm1} + \frac{[In]}{[M_1]+[In]} C_{pIn} \\
H_f &= (F_{M_1} C_{pm1} + F_{In} C_{pIn})(T_{feed} - T_f) \\
H_{g1} &= F_g (T_{g_1} - T_f) C_{pg} \\
H_{g0} &= (F_g + b_t)(T - T_f) C_{pg} \\
H_r &= H_{reac} M_{W_1} R_{M1} \\
H_{pol} &= C_{ppol}(T - T_f) R_{M1} M_{W_1}
\end{aligned}
\tag{2.20}
$$

The definitions for all the variables used in Eqs.2.19-2.20 are given in Table 2.3 and their values can be found in Table 2.4 (see [9, 23]). 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

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

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).

Table 2.3: 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_{pm1}	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_{W_1}	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_{g_1}, T_{w_1}	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

Table 2.4: 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	$=$	$(9000)(4.1868)$	$\frac{J}{mol}$
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_{W_1}	$=$	$28.05 \cdot 10^{-3}$	$\frac{kg}{mol}$
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}	$=$	$(-894 \cdot 10^3)(4.1868)$	$\frac{J}{kg}$
UA	$=$	$(1.14 \cdot 10^6)(4.1868)$	$\frac{J}{K \cdot s}$
F_{In}, F_{M_1}, 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_{1_s}, Y_{2_s}	$=$	3.835, 3.835	mol
T_s , $T_{w_{1_s}}$, $T_{g_{1_s}}$	$=$	356.21, 290.37, 294.36	K

In the present 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 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:

$$\begin{aligned} F_{M1} &= u_2 V_g + F_{M1ss} \\ T_{feed} &= \frac{u_1(M_r C_{pr} + B_W C_{ppol}) + H_{fss}}{F_{M1} C_{pm1} + F_{In} C_{pIn}} + T_f \end{aligned} \tag{2.21}$$

with

$$\begin{aligned} u_1 &= \frac{H_r - H_{rss} + H_{pol} - H_{polss} - H_{g1} + H_{g1ss}}{M_r C_{pr} + B_w C_{ppol}} + v_1 \\ u_2 &= \frac{R_{M1} - R_{M1ss}}{V_g} + v_2 \end{aligned} \tag{2.22}$$

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.2.23) below. Under the control law of Eq.2.22, the dynamics of the states, T and $[M_1]$, take the following form in the closed-loop system:

$$\begin{aligned} \frac{d[M_1]}{dt} &= (F_{M_1} - \frac{[M_1]}{[M_1] + [In]} b_t - R_{M1ss}) \frac{1}{V_g} + v_2 \\ \frac{dT}{dt} &= \frac{H_f + H_{g1ss} - H_{g0} - H_{rss} - H_{polss}}{M_r C_{pr} + B_w C_{ppol}} + v_1 + d_1 \end{aligned} \tag{2.23}$$

It can be seen that these states only depend on $[In]$, $[M_1]$ and T. The closed-loop system under the controller of Eq.2.21 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 2.14. 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

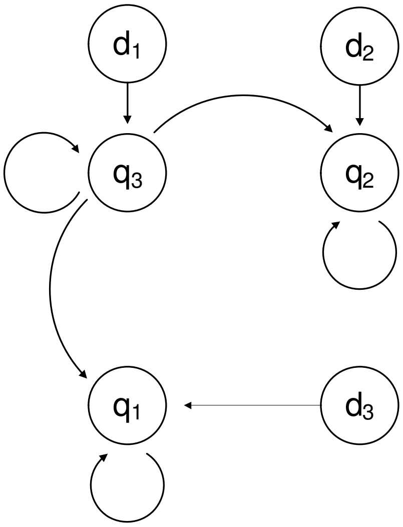


Figure 2.14: Isolability graph for the system of Eq.2.19.

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 with a limit-cycle as shown by [23]. 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:

$$\begin{aligned} v_1(t) &= K_1(T_{ss} - T + \frac{1}{\tau_1}\int_0^t (T_{ss} - T)dt) \\ v_2(t) &= K_2([M_1]_{ss} - [M_1] + \frac{1}{\tau_2}\int_0^t ([M_1]_{ss} - [M_1])dt) \end{aligned} \tag{2.24}$$

Table 2.5: 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

with $K_1 = 0.005,\ K_1 = 0.0075,\ \tau_2 = 1000,\ \tau_1 = 500$. We will refer to the controller defined by Eqs.2.21, 2.22 and 2.24 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.2.21, but in this case, u_1 and u_2 are evaluated by applying the PI controllers of Eq.2.24 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

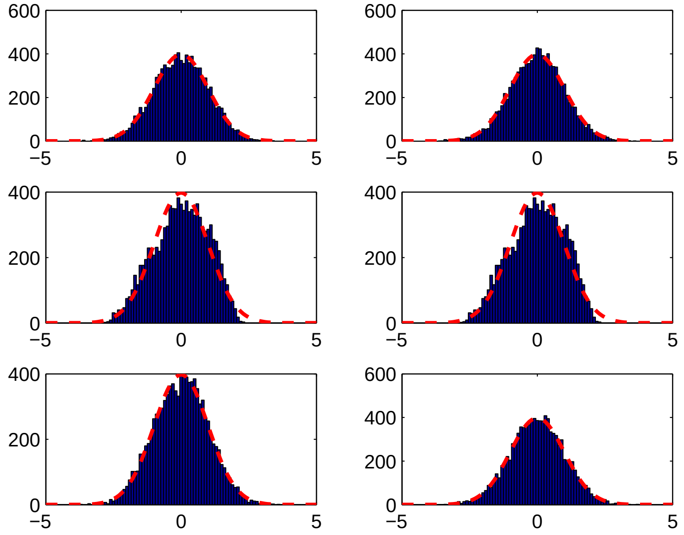


Figure 2.15: Polyethylene reactor example. Distribution of normalized, fault-free operating data compared with a normal distribution of the same mean and covariance.

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 equal. Table 2.5 provides the values of the noise parameters for each state of the system of Eq.2.19. 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 2.15 shows 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 $t = 0.5hr$. 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 2.16, 2.17 and 2.18 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,

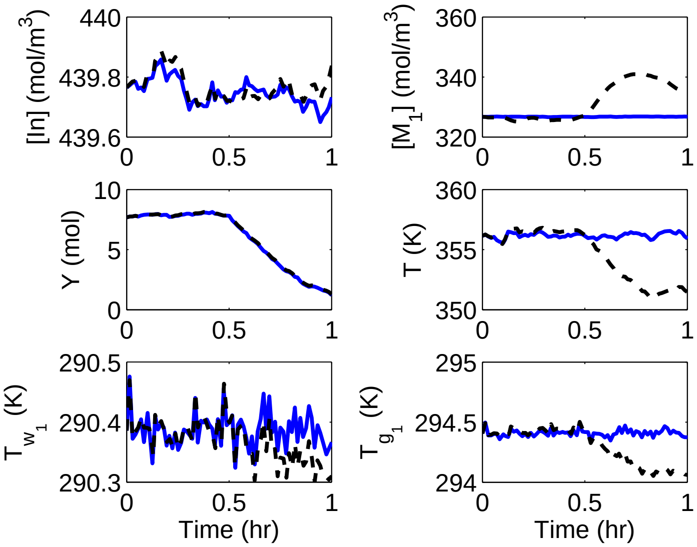


Figure 2.16: Polyethylene reactor example. State trajectories of the closed-loop system under decoupling (solid) and PI-only (dashed) controllers with a fault d_2 at $t = 0.5\ hr$.

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.2.19 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 defined in Eq.2.9 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 are not presented here for brevity.

Figures 2.19, 2.20 and 2.21 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 2.19 shows

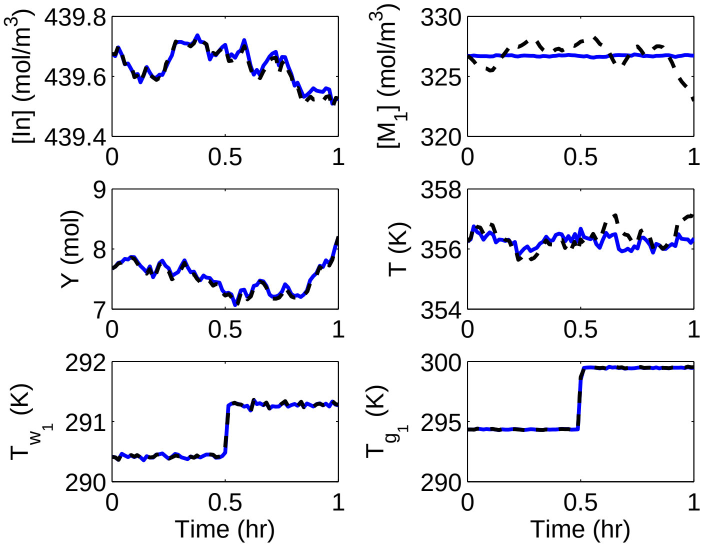


Figure 2.17: Polyethylene reactor example. State trajectories of the closed-loop system under the decoupling (solid) and PI-only (dashed) controllers with a fault d_3 at $t = 0.5hr$.

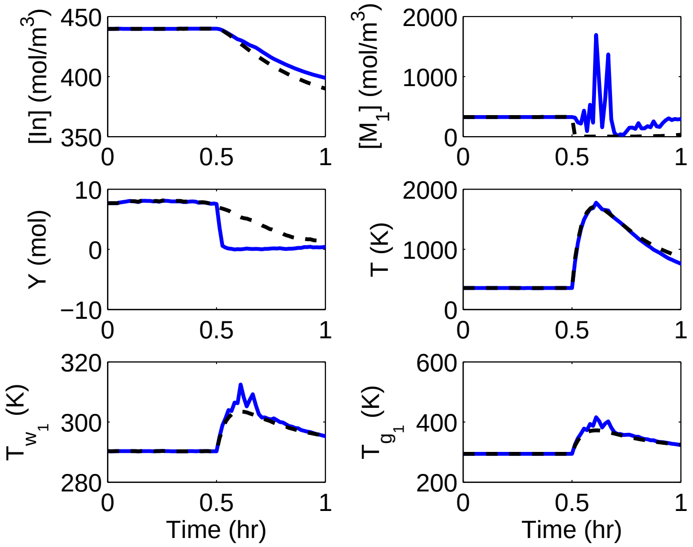


Figure 2.18: Polyethylene reactor example. State trajectories of the closed-loop system under the decoupling (solid) and PI-only (dashed) controllers with a fault d_1 at $t = 0.5\ hr$.

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 2.19 clearly shows the fault occurring at time $t = 0.5hr$ 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 2.16 demonstrates that there is a failure affecting Y starting at $t = 0.5hr$. 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 2.17 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 2.20 show that the signature of the fault is $[0\ 0\ 1]^T = W^3$. 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 2.18 and 2.21. The control action required under the decoupling control law is on the same order of magnitude as that of the PI-only controller. Figure 2.22 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.*

2.6 Conclusions

This chapter has proposed a method for integrating the design of the feedback control law with the fault detection and isolation scheme. This approach strengthens existing

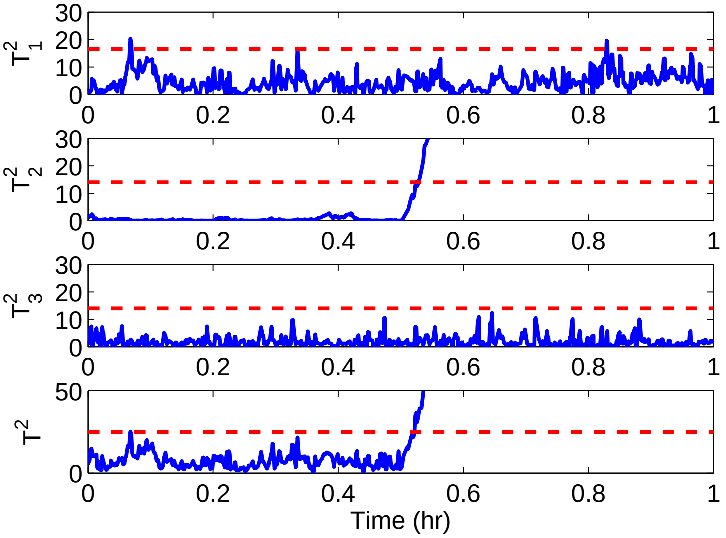


Figure 2.19: Polyethylene reactor example. Statistics T^2, T^2_1, T^2_2, and T^2_3 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_2 at $t = 0.5$ hr.

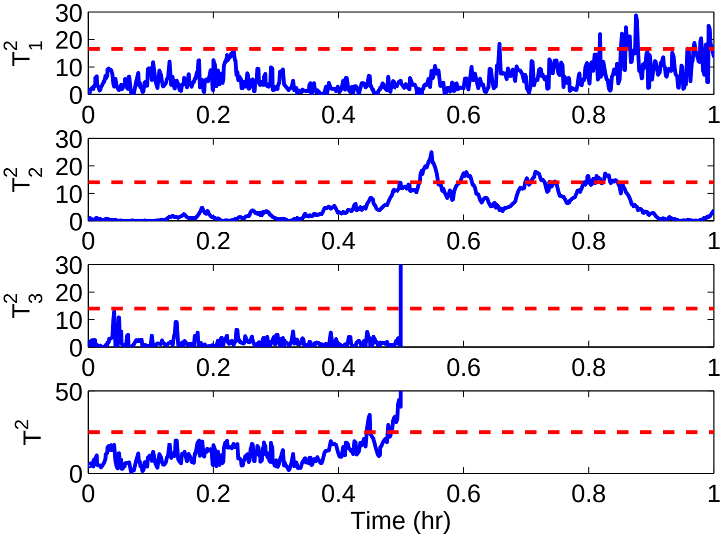


Figure 2.20: Polyethylene reactor example. Statistics T^2, T^2_1, T^2_2, and T^2_3 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_3 at $t = 0.5$ hr.

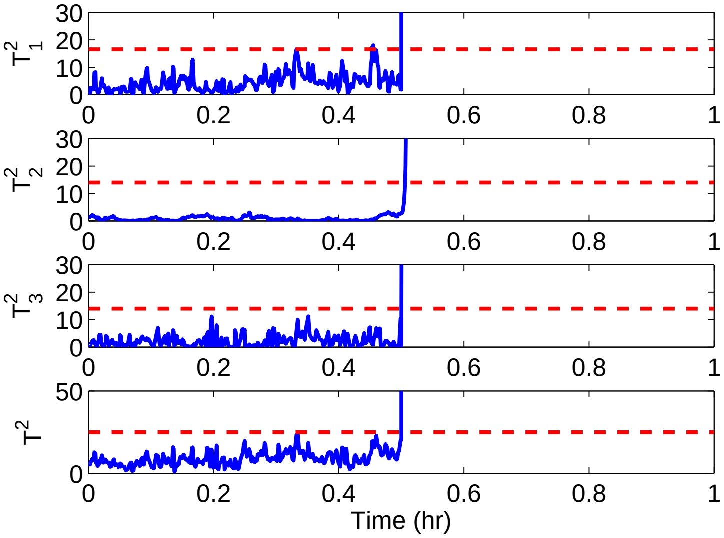


Figure 2.21: Polyethylene reactor example. Statistics T^2, T_1^2, T_2^2, and T_3^2 (solid) with T_{UCL} (dashed) of the closed-loop system under the decoupling controller with a failure in d_1 at $t = 0.5\ hr$.

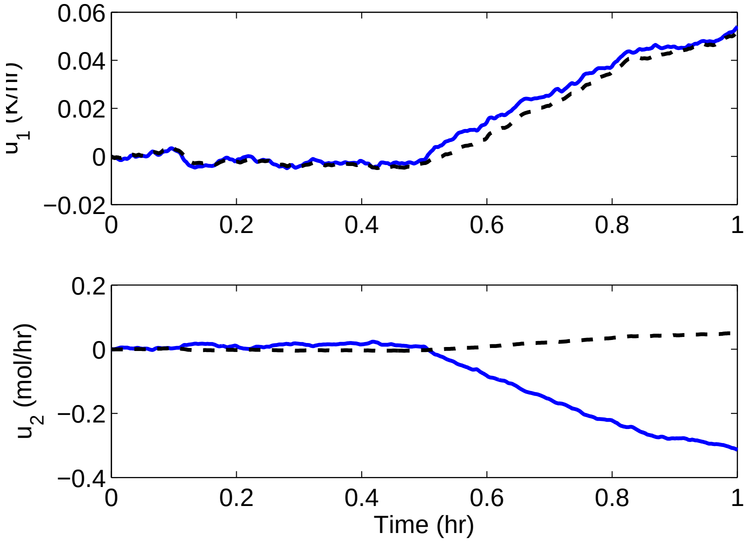


Figure 2.22: Polyethylene reactor example. Manipulated input profiles for both decoupling (solid) and PI-only (dashed) control with a fault in d_2 at $t = 0.5hr$.

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 example and a polyethylene reactor example. 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.

Chapter 3

Plant-wide FDI

3.1 Introduction

This chapter further extends the results of Chapter 2 to a plant-wide setting with a multiple-input multiple-output reactor-reactor-separator system. The focus of this chapter is to demonstrate in a plant-wide setting the fault detection and isolation that integrates model-based controller design with data-based fault detection in order to perform fault isolation. The work demonstrates that the achievement of fault isolation across multiple coupled units is possible through feedback control. Additionally the effects of process and sensor measurement noise on the ability to detect and accurately isolate faults are investigated through a Monte-Carlo simulation study. The results from the nonlinear control simulation are compared with a conventional (proportional-integral) feedback controller to demonstrate that without the isolable structure induced by feedback control the faults are otherwise indistinguishable without prior knowledge of fault history.

3.2 Preliminaries

3.2.1 Fault signatures

The objective of this chapter is to demonstrate the method proposed in Chapter 2 of controller enhanced fault detection and isolation in a multi-unit setting. Controller enhanced

FDI was introduced in Chapter 2 as a method of dividing the state vector into a number of partially decoupled subvectors which can be monitored for their individual responses to particular faults in the system using process measurements only. Based on their responses and the system structure imposed by the model-based controllers, it is possible to discriminate between individual faults or groups of faults. Dividing the state vector into partially decoupled subvectors is accomplished by using model-based control laws to enforce an appropriate structure. Based on this structure, faults affecting the system produce a unique response as observed in the state trajectories. The responses of the subvectors are monitored for out-of-control behavior using standard process monitoring methods that take into account the acceptable level of variation under normal operating conditions (i.e., common cause variation). Thus, this approach brings together model-based controller design techniques and data-based statistical process monitoring for diagnosing faults. To better understand the structure that must be enforced in order to perform fault isolation, we review the definitions of the incidence graph, the reduced incidence graph and the isolability graph in the context of nonlinear deterministic systems.

Definition 8 *The incidence graph of an autonomous system $\dot{x} = f(x)$ with $x \in R^n$ is a directed graph defined by n nodes, one for each state, x_i, $i = 1, \ldots, n$, of the system. A directed arc with origin in node x_i and destination in node x_j exists if and only if $\frac{\partial f_j}{\partial x_i} \neq 0$.*

Definition 9 *The reduced incidence graph of an autonomous system $\dot{x} = f(x)$ with $x \in R^n$ is the directed graph of nodes q_i, where $i = 1, ..., N$, 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.*

The incidence graph of a system shows the time derivative dependencies between the states. By reducing fully coupled states to a single node, the reduced incidence graph reveals any partially decoupled subsystems that may exist. With the structure of the subsystems revealed, it is beneficial to look at how faults affect each of the subsystems as shown in an isolability graph.

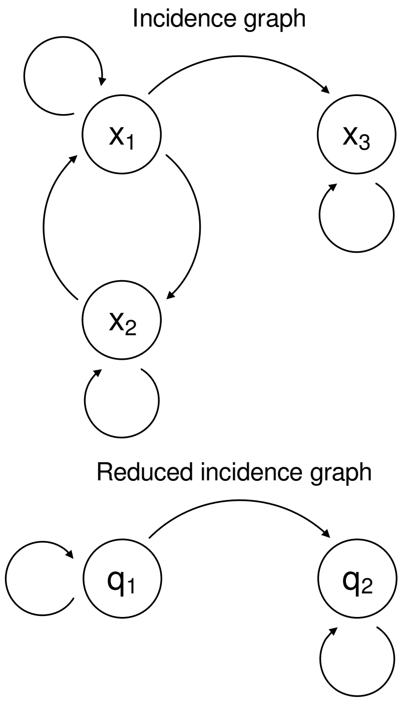
Definition 10 *The isolability graph of an autonomous system $\dot{x} = f(x, d)$ with $x \in R^n$, $d \in R^p$ is a directed graph made of the N nodes of the reduced incidence graph of the system $\dot{x} = f(x, 0)$ and p additional nodes, one for each possible fault d_k. The graph contains all the arcs 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 $\frac{\partial f_l}{\partial d_k} \neq 0$ for some $x_l \in X_j$.*

These definitions are convenient in presenting the basic dependencies within a state vector. Although this graphical approach has the advantage of visualizing the system structure, it may be noted that it is also possible to understand the structure a system and its faults using the definition of relative degree [28]. This approach has been used previously in other FDI papers [47, 55].

In most complex systems, the states are fully coupled and the isolability graph contains a single node representing all of the states in the system. However, in systems with partially decoupled dynamics this demonstrates graphically the partially independent subsets of the state vector. Consider, for example, the following system:

$$\begin{aligned}
\dot{x}_1 &= x_1 + x_2 + u + d_1 \\
\dot{x}_2 &= -x_2 + x_1 + d_2 \\
\dot{x}_3 &= x_1 - x_2 - x_3 + d_3
\end{aligned} \tag{3.1}$$

Figure 3.1 shows the incidence and reduced incidence graphs for the system of Eq.3.1. Because x_1 and x_2 are mutually dependent but are not affected by x_3, they form a partially decoupled subsystem represented by a single node (q_1) in the reduced incidence graph leaving x_3 to form a node by itself (q_2). Figure 3.2 shows the effect of each of the faults in the isolability graph for the system of Eq.3.1. With the isolability graph of a system,


Incidence graph

Reduced incidence graph

Figure 3.1: Incidence and reduced incidence graphs for the system of Eq.3.1.

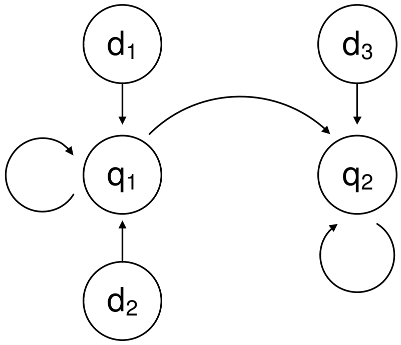


Figure 3.2: Isolability graph of the system of Eq.3.1.

it is possible to consider fault isolation based upon monitoring the subsystems. For this purpose, it is necessary to review the definition of a fault signature given below (see also, Chapter 2).

Definition 11 *The signature of a fault d_k of an autonomous system subject to p faults $\dot{x} = f(x, d)$ with $x \in R^n$, $d \in R^p$ 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_i^k, is equal to 1 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; W_i^k is equal to 0 otherwise.*

Using this definition of a fault signature and the isolability graph shown in Figure 3.2, it is possible to identify the fault signatures for the three faults considered in the system of Eq.3.1. In this case, because the node $q_2 = \{x_3\}$ does not affect the node $q_1 = \{x_1, x_2\}$, the fault d_3 has the signature $W^3 = [0\ 1]$ and the two faults d_1 and d_2 which affect q_1 and q_2 have the signature $W^1 = W^2 = [1\ 1]$. Based on this, it is expected that a failure in d_1 or d_2 will affect all of the states, whereas a failure in d_3 is expected to affect only those in q_2. In this regard, it is possible to distinguish between a failure in d_3 from a failure in d_1 or d_2 based on the system response. However, it is not generally possible to discriminate between a failure in d_1 and d_2.

Remark 11 *The process model for the system of Eq.3.1 does not explicitly account for process and sensor noise. Likewise, the isolability graph and associated fault signatures are developed for the deterministic case. However, noise is accounted for in the process monitoring method given in the next section by means of appropriate tolerance thresholds (computed using historical process data) in the decision criteria for fault detection and isolation. The thresholds are based on historical, fault-free operating data and take into account both sensor and process noise present under normal operating conditions. This allows for appropriate FDI performance even if the process model and the measurements are corrupted by noise.*

3.2.2 Process monitoring

The discussion in the previous subsection focused on deterministic process behavior in which evaluation of the fault signature based on the isolability graph is straight-forward. On the other hand, in processes subject to state and measurement noise, it is possible to have false positives and false negatives in determining the affect of a fault on the state trajectories. In the simulation results section of this chapter, autocorrelated noise is added to the process dynamic equations and white sensor noise is added to process measurements. For this reason, in order to make a comparison between the fault signature based on the expected response of the system from the isolability graph and the system signature based on the actual behavior (computed on the basis of process measurements), it is necessary to use a method of monitoring the state trajectories that clearly distinguishes normal behavior from faulty behavior and is tolerant to the normal amount of process variation (as computed from process historical data). Additionally, it is assumed that faults of interest will be sufficiently large so that their effect will not be masked by normal process variation; faults whose influence on the closed-loop system behavior over a large time window is within the normal common-cause process variation do not have a significant effect on the process. These types of faults are generally inconsequential and do not need to be handled via fault-tolerant control schemes.

For the purpose of process monitoring, we use Hotelling's T^2 statistic, a well established method in statistical process control that monitors multivariate data using a single statistic [60]. Because of its suitability for continuous, serially correlated chemical processes, the method of using single observations is employed [63, 50]. The T^2 statistic is computed using the multivariate state vector (or subset of the state vector) $x \in R^n$, the expected or desired mean $\bar{x}$ (the normal operating point) and the estimated covariance matrix S obtained using h historical measurements of the system under normal operation:

$$T^2 = (x - \bar{x})^T S^{-1} (x - \bar{x}) \tag{3.2}$$

The upper control limit for the T^2 statistic is obtained from its distribution and is computed using the following equation:

$$T^2_{UCL} = \frac{(h^2-1)n}{h(h-n)} F_\alpha(n, h-n) \tag{3.3}$$

where $F_\alpha(n, h-n)$ is the value from the F distribution with $(n, h-n)$ degrees of freedom corresponding to a confidence level α. The T^2 statistic is used to both detect that a fault has occurred as well as provide the system signature that can be compared with the fault signatures defined by the isolability graph. In order to perform these tasks, the T^2 statistic based on the full state vector x with upper control limit T^2_{UCL} is first used to detect the presence of a fault. Subsequently, the T^2_i statistic is used to monitor the status of each subset of the state vector with an upper control limit T^2_{UCLi} where $i = 1, \ldots, N$ that is based on each of the nodes q_i and their corresponding states $x_j \in X_i$.

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

1. A fault is detected if $T^2(t) > T^2_{UCL}, \; \forall t, \; t_f \leq t \leq T_P$ where t_f is the first time T^2 crosses the UCL and 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. Choosing T_P depends on the process time constants and potentially on available historical information on 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:

   $$T^2_i(t) > T^2_{UCLi}, \; \forall t, \; t_f \leq t \leq T_P \rightarrow W_i(t_f, T_P) = 1.$$

   $$T^2_i(t) \not> T^2_{UCLi}, \; \forall t, \; t_f \leq t \leq T_P \rightarrow W_i(t_f, T_P) = 0.$$

   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.

It should be noted that the method of fault detection discussed here makes no assumption regarding the time-scale of the fault. In general, both abrupt and slowly developing faults will be detected and isolated. However, slowly developing faults are more likely to be subject to false isolation if the fault is diagnosed before becoming sufficiently large as discussed in Remark 12. To minimize such effects, it is important to adjust the detection window T_P, based on the individual system dynamics. For information regarding fault detection time see [16, 15, 14]. Additionally, it should be noted that the detection and isolation method discussed here requires no significant real-time computation other than computing the T^2 statistics which require only minimal computation time.

Remark 12 *In the data-based fault detection and isolation method presented above, the upper control limit is chosen based on common-cause variance, including process and sensor noise, in order to minimize false alarms. Additionally, to further avoid false alarms, a period of persistent failure is required, $T_P - t_f$. For these reasons, small disturbances or failures are likely to go undetected if the magnitude and effect of the disturbance is on the same level as that of the inherent process variance. Specifically, in order to declare a fault, d_k must be sufficiently large in order for $T_i^2(t)$ to exceed the threshold T^2_{UCLi} $\forall t$ $t_f \leq t \leq T_P$. Clearly, faults that do not meet the criteria for declaring a fault are, from the point of view of faulty behavior, not of major consequence. However, it should be noted that there is the probability (albeit low) that there is a fault d_k that is large enough to signal a fault in the full state vector, x, but is not 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 results section by simulating the closed-loop system a large number of times with randomly varying fault sizes in a Monte-Carlo type simulation.*

3.2.3 Controller design

The approach to fault detection and isolation discussed in the previous two sections can be applied if the signatures of the faults in the closed-loop system are distinct. The uniqueness of a fault depends on the structure of the closed-loop system as shown in the isolability graph. In general, complex nonlinear systems are fully coupled and faults cannot be isolated using this method when the controller is designed only with closed-loop stability in mind. Despite this being the case for most open-loop systems, an isolable structure in the closed-loop system can still be achieved through the application of appropriately designed nonlinear control laws. Although many control laws exist that will achieve the desired goal, it is not possible to apply a systematic procedure to controller design that guarantees closed-loop stability and an isolable closed-loop system structure for any nonlinear process. The specific form of the controller depends on the structure of the open-loop system and it is possible that such a controller may not exist. Nonetheless, a general approach can be applied to decouple a particular set of states from the rest of the system in a number of applications. As an example, consider a controller that can be applied to nonlinear systems with the following state space description:

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + f_{12}(x_1, x_2) + g_1(x_1, x_2)u + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2 \end{aligned} \tag{3.4}$$

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

$$u(x_1, x_2) = -\frac{f_{12}(x_1, x_2) - v(x_1)}{g_1(x_1, x_2)} \tag{3.5}$$

the closed-loop system takes the form

$$\begin{aligned} \dot{x}_1 &= f_{11}(x_1) + v(x_1) + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2 \end{aligned} \tag{3.6}$$

where $v(x_1)$ has to be designed in order to achieve asymptotic stability of the origin of the x_1 subsystem when $d_1 = 0$. In this case the 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 $W^2 = [0\ 1]^T$. If necessary, using multiple controllers allows for more degrees of freedom in breaking up the full state vector into subvectors.

As an example, this is demonstrated with the system of Eq.3.1. Consider a controller added to the right-hand side of the dynamic equation for the state x_1 of the form:

$$u = -x_2 + v$$

where v is an external controller that may be used for stabilizing the system. With this controller, the closed-loop system takes the form:

$$\begin{aligned} \dot{x}_1 &= x_1 + d_1 + v \\ \dot{x}_2 &= -x_2 + x_1 + d_2 \\ \dot{x}_3 &= x_1 - x_2 - x_3 + d_3 \end{aligned} \tag{3.7}$$

Since there are no longer loops in the system, the reduced incidence graph is now equivalent to the incidence graph having three nodes (one for each state). Consequently, it becomes possible to distinguish between faults d_1 and d_2 in addition to d_3 using the method described above. This method will be applied to the reactor-separator system described in the next section. Note that the controller design outlined above does not take into consideration optimality criteria beyond the tuning of the external controller v. It is likely that the nonlinear feedback control law that enforces an isolable structure will incur additional cost compared with a control law designed for optimality. In the simulation results section, this issue is addressed by comparing the nonlinear feedback controller with a conventional PI controller to show that the cost incurred for enabling fault isolation in the closed-loop system is not excessive.

Remark 13 *It is important to note that it is possible to extend the state feedback controller design to an output feedback controller design, which uses a high-gain observer operating at a fast time-scale to achieve state estimation, to enforce a near-isolable structure in the closed-loop system. The reader may refer to [20, 6, 8] for results on high-gain observer based output feedback control. However, the detailed development of this approach is outside of the scope of the present chapter.*

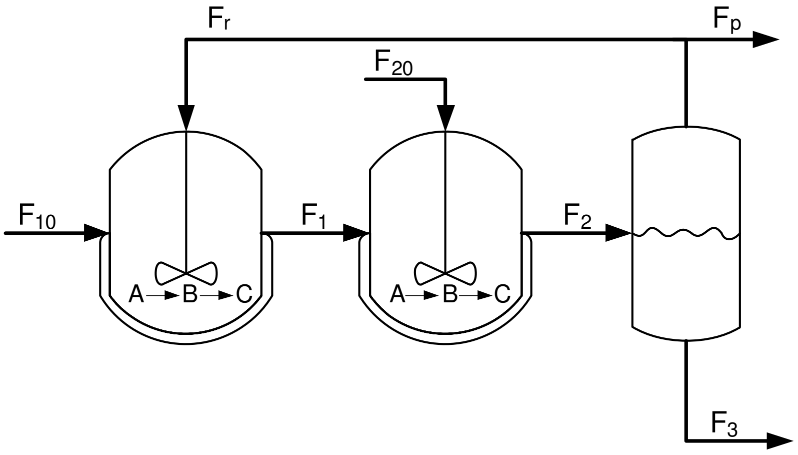


Figure 3.3: Reactor-separator system with recycle.

3.3 Reactor-separator process

3.3.1 Process description and modeling

The process considered in this study is a three vessel, reactor-separator system consisting of two continuous stirred tank reactors (CSTRs) and a flash tank separator (see Figure 3.3). A feed stream to the first CSTR contains the reactant A which is converted into the desired product B. The desired product can then further react into an undesired side-product C. The effluent of the first CSTR along with additional fresh feed makes up the inlet to the second CSTR. The reactions $A \to B$ and $B \to C$ (referred to as 1 and 2, respectively) take place in the two CSTRs in series before the effluent from CSTR 2 is fed to a flash tank. The overhead vapor from the flash tank is condensed and recycled to the first CSTR, and the bottom product stream is removed. A small portion of the overhead is purged before being recycled to the first CSTR. All three vessels are assumed to have static holdup. The dynamic equations describing the behavior of the system, obtained through material and energy balances under standard modeling assumptions, are given below.

$$
\begin{aligned}
\frac{dx_{A1}}{dt} &= \frac{F_{10}}{V_1}(x_{A10} - x_{A1}) + \frac{F_r}{V_1}(x_{Ar} - x_{A1}) - k_1 e^{\frac{-E_1}{RT_1}} x_{A1} \\
\frac{dx_{B1}}{dt} &= \frac{F_{10}}{V_1}(x_{B10} - x_{B1}) + \frac{F_r}{V_1}(x_{Br} - x_{B1}) + k_1 e^{\frac{-E_1}{RT_1}} x_{A1} - k_2 e^{\frac{-E_2}{RT_1}} x_{B1} \\
\frac{dT_1}{dt} &= \frac{F_{10}}{V_1}(T_{10} - T_1) + \frac{F_r}{V_1}(T_3 - T_1) + \frac{Q_1}{\rho C p V_1} + \frac{-\Delta H_1}{Cp} k_1 e^{\frac{-E_1}{RT_1}} x_{A1} \\
&\quad + \frac{-\Delta H_2}{Cp} k_2 e^{\frac{-E_2}{RT_1}} x_{B1} + u_1 \\
\frac{dx_{A2}}{dt} &= \frac{F_1}{V_2}(x_{A1} - x_{A2}) + \frac{F_{20}}{V_2}(x_{A20} - x_{A2}) - k_1 e^{\frac{-E_1}{RT_2}} x_{A2} \\
\frac{dx_{B2}}{dt} &= \frac{F_1}{V_2}(x_{B1} - x_{B2}) + \frac{F_{20}}{V_2}(x_{B20} - x_{B2}) + k_1 e^{\frac{-E_1}{RT_2}} x_{A2} - k_2 e^{\frac{-E_2}{RT_2}} x_{B2} \qquad (3.8) \\
\frac{dT_2}{dt} &= \frac{F_1}{V_2}(T_1 - T_2) + \frac{F_{20}}{V_2}(T_{20} - T_2) + \frac{Q_2}{\rho C p V_2} + \frac{-\Delta H_1}{Cp} k_1 e^{\frac{-E_1}{RT_2}} x_{A2} \\
&\quad + \frac{-\Delta H_2}{Cp} k_2 e^{\frac{-E_2}{RT_2}} x_{B2} + u_2 \\
\frac{dx_{A3}}{dt} &= \frac{F_2}{V_3}(x_{A2} - x_{A3}) - \frac{F_r + F_p}{V_3}(x_{Ar} - x_{A3}) \\
\frac{dx_{B3}}{dt} &= \frac{F_2}{V_3}(x_{B2} - x_{B3}) - \frac{F_r + F_p}{V_3}(x_{Br} - x_{B3}) \\
\frac{dT_3}{dt} &= \frac{F_2}{V_3}(T_2 - T_3) + \frac{Q_3}{\rho C p V_3}
\end{aligned}
$$

The definitions for the variables used in Eq.3.8 can be found in Table 3.1, with the parameter values given in Table 3.2. Each of the tanks has an external heat input. In both CSTRs, the heat input is a manipulated variable for controlling the reactors at the appropriate operating temperature. These are the only control actuators considered in the system. The model of the flash tank separator operates under the assumption that the relative volatility for each of the species remains constant within the operating temperature range of the flash tank. This assumption allows calculating the mass fractions in the overhead based upon the mass fractions in the liquid portion of the vessel. It has also been assumed that there is a negligible amount of reaction taking place in the separator. The following algebraic equations model the composition of the overhead stream relative to the composition of the liquid holdup in the flash tank:

Table 3.1: Process Variables

x_{A1}, x_{A2}, x_{A3}	mass fractions of A in vessels 1, 2, 3
x_{B1}, x_{B2}, x_{B3}	mass fractions of B in vessels 1, 2, 3
x_{C1}, x_{C2}, x_{C3}	mass fractions of C in vessels 1, 2, 3
x_{Ar}, x_{Br}, x_{Cr}	mass fractions of A, B, C in the recycle
T_1, T_2, T_3	temperatures in vessels 1, 2, 3
T_{10}, T_{20}	feed stream temp. to vessels 1, 2
F_1, F_2, F_3	effluent flow rate from vessels 1, 2, 3
F_{10}, F_{20}	feed stream flow rate to vessels 1, 2
F_r, F_p	flow rates of the recycle and purge
V_1, V_2, V_3	volume of vessels 1, 2, 3
u_1, u_2	manipulated inputs
E_1, E_2	activation energy for reactions 1, 2
k_1, k_2	pre-exponential values for reactions 1, 2
ΔH_1, ΔH_2	heats of reaction for reactions 1, 2
α_A, α_B, α_C	relative volatilities of A, B, C
Q_1, Q_2, Q_3	heat input into vessels 1, 2, 3
C_p, R	heat capacity and gas constant

$$\begin{aligned}
x_{Ar} &= \frac{\alpha_A x_{A3}}{\alpha_A x_{A3} + \alpha_B x_{B3} + \alpha_C x_{C3}} \\
x_{Br} &= \frac{\alpha_B x_{B3}}{\alpha_A x_{A3} + \alpha_B x_{B3} + \alpha_C x_{C3}} \\
x_{Cr} &= \frac{\alpha_C x_{C3}}{\alpha_A x_{A3} + \alpha_B x_{B3} + \alpha_C x_{C3}}
\end{aligned} \tag{3.9}$$

The open-loop system of Eq.3.8 is fully coupled and is represented by a single node in the reduced incidence graph. However, using appropriately designed model-based nonlinear state feedback control laws for the manipulated inputs u_1 and u_2, it is possible to separate the closed-loop system into four nodes in the isolability graph. Consider the following nonlinear control laws which decouple the full state vector into 4 subvectors [8]:

$$\begin{aligned}
u_1 &= \frac{F_r}{V_1}(T_{3ss} - T_3) - \frac{-\Delta H_1}{Cp} k_1 e^{\frac{-E_1}{RT_1}} (x_{A1} - x_{A1ss}) - \frac{-\Delta H_2}{Cp} k_2 e^{\frac{-E_2}{RT_1}} (x_{B1} - x_{B1ss}) + v_1 \\
u_2 &= -\frac{-\Delta H_1}{Cp} k_1 e^{\frac{-E_1}{RT_2}} (x_{A2} - x_{A2ss}) - \frac{-\Delta H_2}{Cp} k_2 e^{\frac{-E_2}{RT_2}} (x_{B2} - x_{B2ss}) + v_2
\end{aligned} \tag{3.10}$$

where the subscript ss refers to values at the steady state, or set point. The terms v_1 and v_2 are external controllers used to stabilize the system and achieve offset-free output tracking

Table 3.2: Parameter Values

$T_{10} = 300$, $T_{20} = 300$	K
$F_{10} = 1.4 \cdot 10^{-3}$, $F_{20} = 1.4 \cdot 10^{-3}$	$\frac{m^3}{s}$
$F_r = 1.4 \cdot 10^{-2}$, $F_p = 1.4 \cdot 10^{-3}$	$\frac{m^3}{s}$
$V_1 = 1.0$, $V_2 = 0.5$, $V_3 = 1.0$	m^3
$E_1 = 5 \cdot 10^4$, $E_2 = 6 \cdot 10^4$	$\frac{J}{mol}$
$k_1 = 2.77 \cdot 10^3$, $k_2 = 2.510^3$	$\frac{1}{s}$
$\Delta H_1 = -6 \cdot 10^4$, $\Delta H_2 = -7 \cdot 10^4$	$\frac{J}{mol}$
$C_p = 4.2 \cdot 10^3$	$\frac{J}{kgK}$
$R = 8.314$	$\frac{J}{molK}$
$\rho = 1000$	$\frac{kg}{m^3}$
$Q_1 = 3.5 \cdot 10^5$, $Q_2 = 4.5 \cdot 10^5$, $Q_3 = 3.5 \cdot 10^5$	$\frac{J}{s}$
$\alpha_A = 3.5$, $\alpha_B = 1$, $\alpha_C = 0.5$	unitless

and are defined, according to standard proportional-integral control formulas, as follows:

$$\begin{aligned} v_1(t) &= K_1(T_{1ss} - T_1 + \frac{1}{\tau_{I1}} \int_0^t (T_{1ss} - T_1)dt) \\ v_2(t) &= K_2(T_{2ss} - T_2 + \frac{1}{\tau_{I2}} \int_0^t (T_{2ss} - T_2)dt) \end{aligned} \tag{3.11}$$

where K_1, K_2 are the proportional controller gains and τ_{I1} and τ_{I2} are the integral time constants. The closed-loop system operating under the control laws defined in Eqs.3.10-3.11 decouples T_1 from x_{A1}, x_{B1} and T_3 and T_2 from x_{A2} and x_{B2}. The four subgroups created by the controller of Eqs.3.10-3.11 are $q_1 = \{T_1\}$, $q_2 = \{T_2\}$, $q_3 = \{T_3\}$ and $q_4 = \{x_{A1}, x_{A2}, x_{A3}, x_{B1}, x_{B2}, x_{B3}\}$. The resulting isolability graph is shown in Figure 3.4. From the isolability graph the fault signatures can be defined as follows:

$$\begin{aligned} W^1 &= [1; 1; 1; 1] \\ W^2 &= [0; 1; 1; 1] \\ W^3 &= [0; 0; 1; 0] \\ W^4 &= [0; 0; 0; 1] \end{aligned} \tag{3.12}$$

The four faults shown in Figure 3.4 are those that will be considered in this example. They represent failures in the heat inputs to each of the tanks (faults d_1, d_2, d_3) and a

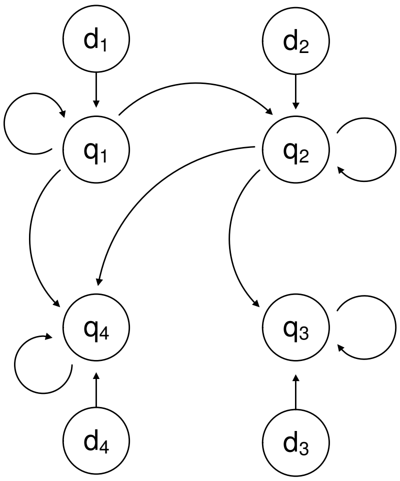


Figure 3.4: Isolability graph for the reactor-separator system.

feed stream concentration disturbance in species A in the inlet to CSTR 1 (d_4). These are added to the right-hand side of the dynamic equations for T_1, T_2, T_3 and x_{A1}. Note that the FDI approach used places no restrictions on the fault d_i, which can represent any time-varying signal. Thus, faults may be additive or parametric and can represent any fault (e.g., time-varying biases, actuator failures, disturbances, process parameter failures).

For comparison purposes, in the simulation results, a PI controller with the form given in Eq.3.11 is used. This control law is used for comparing the isolability of faults, using process measurements only, in the closed-loop system under PI-only control and in the closed-loop system under the nonlinear feedback control which enforces the isolable structure. Although a PI controller is used for comparison in this chapter, any controller that does not enforce an isolable structure in the closed-loop system would yield similarly indistinguishable faults. Additionally, the PI-only controller will be used to evaluate the additional cost incurred by the nonlinear feedback controller in order to enforce an isolable structure in the closed-loop system.

3.3.2 Simulation results

The model presented in Section 3.3.1 was numerically simulated using a standard Runge-Kutta integration method. The system was modeled with both process and sensor noise.

The sensor measurement noise was generated as Gaussian distributed random noise with standard deviation σ_m and was added to the state measurement at a sample rate of 0.1 sample/second. Noisy measurements were used in updating the feedback control law described in Eqs.3.10-3.11 on the same interval. Process noise was added to the right-hand side of each equation in the system of ODEs found in Eq.3.8. Process noise was generated as autocorrelated noise of the form $w_k = \phi w_{k-1} + \xi_k$ where $k = 0, 1, \ldots$ is the discrete time step of 1 second, w_k is a normally distributed random variable with standard deviation σ_p and ϕ is the autocorrelation factor. Table 3.3 contains the parameters used in generating the noise. The sensor measurement and process noise were generated independently for each state in the system. For purposes of fault detection, a window of 30 seconds was used in declaring a fault (i.e., $T_P - t_f = 30\ sec$).

The controllers were designed as shown in Eqs.3.10-3.11 using control parameters $K_1 = K_2 = \frac{0.01}{sec}$ and $\tau_{I1} = \tau_{I2} = 300 sec$. The PI controllers shown for comparison used the same parameters. The system was controlled at the set point values of $T_{1ss} = 436.8\ K$ and $T_{2ss} = 433.9\ K$. In all cases, the system was initially at steady-state and was simulated for 30 min fault-free and for 30 min after the occurrence of the fault. The four faults were introduced as added terms on the right-hand side of the ODEs in Eq.3.8; only a single fault was applied in each simulation. The values $d_1 = 1\frac{K}{s}$, $d_2 = 2\frac{K}{s}$, $d_3 = 1\frac{K}{s}$ and $d_4 = -2 \cdot 10^{-3}\frac{1}{s}$ were added to the dynamic equations for T_1, T_2, T_3 and x_{A1}, respectively. These represent changes in the heat input (actuator/valve failures) for faults d_1, d_2 and d_3 and an inlet concentration disturbance in species A for fault d_4. However, these faults could also be thought of as any general faults as the development of this method does not limit the values that d can take.

Four simulation scenarios were carried out, one for each fault, to demonstrate the method of detecting and isolating faults in the closed-loop system. In order to apply the method of fault detection and isolation presented in Section 3.2, the data should be multivariate normal and fit the T^2 distribution under closed-loop operation. Figure 3.5 demonstrates that the measurements from each of the states closely approximates a Gaussian distribution. The distribution for the measured T^2 values is shown in Figure 3.6. Again we see that the measured statistic closely approximates the predicted distribution, however, in this case

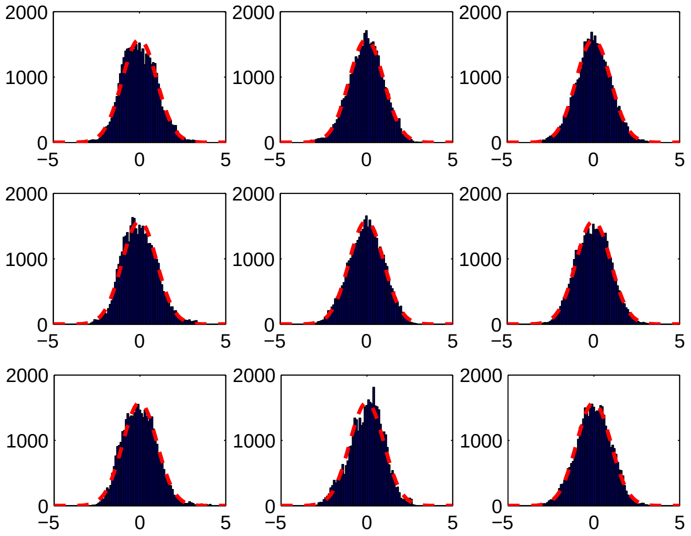


Figure 3.5: Normalized histogram plots of each of the system states compared with a normal distribution (dashed) for a large number of measurements during fault-free operation under nonlinear feedback control.

the fit is less exact due to correlation between states. Nonetheless, the distribution is reasonably close. If necessary, the upper control limit can be adjusted upward to provide a more conservative limit if false alarms are problem.

Figure 3.7 shows the trajectories of the mass fractions in each of the tanks and the recycle stream for the simulation in closed-loop operation under the nonlinear feedback controller with a failure in d_1. The effects of the failure at time $t = 0.5$ hr are visible in the plot. The temperature trajectories for each of the tanks is shown in Figure 3.8 along with the control action requested. Once the failure is detected at $t = 0.5$ hr, the T_i^2 plots are used to determine the fault signature for the system. Figure 3.9 shows the T^2 statistic results for the four subsets of the state vector as well as for the full state vector. The fault is detected at time $t = 0.5$ hr by the full T^2 and is isolated based on the four T_i^2 corresponding to the subsets. Based on the T_i^2 plots the signature of the system in this case is $W = [1; 1; 1; 1] \equiv W^1$. Thus, the fault is correctly isolated as one affecting the states in $q_1 = T_1$, or d_1. Note that although the process data are serially correlated on a short timescale, this was compensated for by using a large amount of historical data for

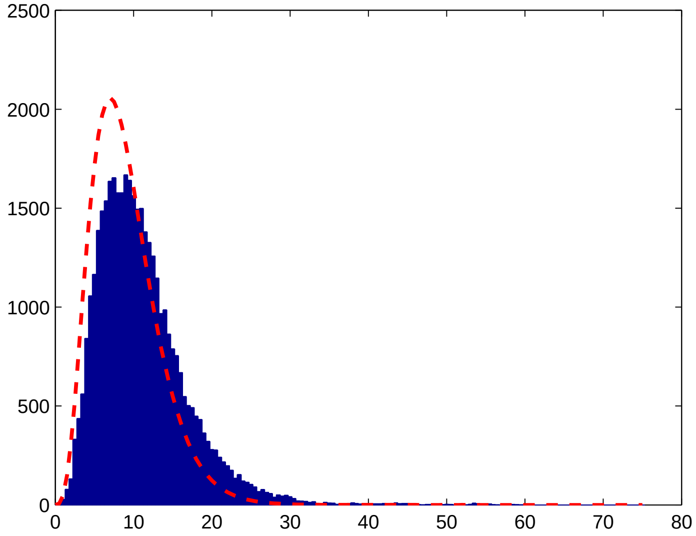


Figure 3.6: Histogram of T^2 statistic for the full state vector compared with the expected T^2 distribution (dashed) for a large number of measurements during fault-free operation under nonlinear feedback control.

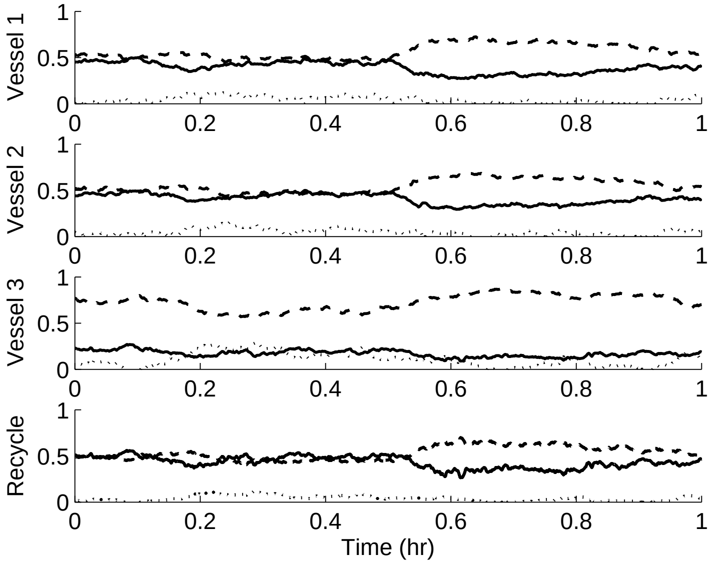


Figure 3.7: Plots of the mass fractions x_A (solid), x_B (dashed) and x_C (dotted) for the system under nonlinear feedback control with a failure in d_1 at $t = 0.5$ hr.

Table 3.3: Noise Parameters

	σ_m	σ_p	ϕ
x_{A1}	1E-3	1E-3	0.7
x_{B1}	1E-3	1E-3	0.7
T_1	1E-3	1E-2	0.7
x_{A2}	1E-3	1E-3	0.7
x_{B2}	1E-3	1E-3	0.7
T_2	1E-3	1E-2	0.7
x_{A3}	1E-3	1E-3	0.7
x_{B3}	1E-3	1E-3	0.7
T_3	1E-3	1E-2	0.7

estimating S. Additionally, it has been found that feedback control makes the closed-loop system data more normally distributed (see [50]). Thus, the assumption that the data are multivariate normal for applying the T^2 statistic is reasonable. This was also confirmed in Figures 3.5-3.6. The simulation with a failure in d_1 was repeated using only a PI controller for comparison. The states were similarly all affected by fault d_1 (see Figure 3.10) and the control action requested was of comparable magnitude with that of the nonlinear feedback controller (see Figure 3.11). This demonstrates that the control action requested by the nonlinear feedback control law to enforce an isolable structure is not excessive in this case. For the PI controller, the states of the closed-loop system are all fully coupled and thus the state trajectories will all be affected by any fault, making it impossible to distinguish between faults on the basis of process measurements. The simulation with a failure in d_2, below, demonstrates this point.

Figure 3.12 shows the T^2 results for the simulation in closed-loop operation under the nonlinear feedback controller with a failure in d_2 occurring at $t = 0.5$ hr. Note that although there may be a brief violation of the upper control limit (e.g., at approximately $t = 0.2$ hr in Figure 3.12), this is not declared as a fault nor is it a false alarm since a fault is declared only after a persistent state of failure lasting at least 30 seconds to avoid such situations. Once the fault is declared around time $t = 0.5$ hr the signature of the system can be determined from the T_i^2 plots which show $W = [0; 1; 1; 1] \equiv W^2$. For the PI-only controller, all of the states were affected as they were in the case with a failure in d_1; however, the case with the nonlinear feedback controller designed to enforce an isolable

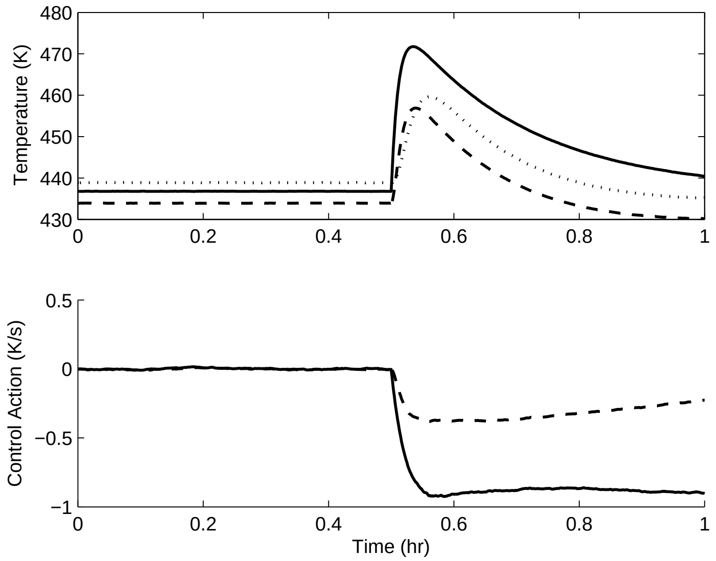


Figure 3.8: (top) Temperature trajectories for T_1 (solid), T_2 (dashed) and T_3 (dotted) for the system under nonlinear feedback control with a failure in d_1 at $t = 0.5$ hr. (bottom) Control action requested for the same system for u_1 (solid) and u_2 (dashed).

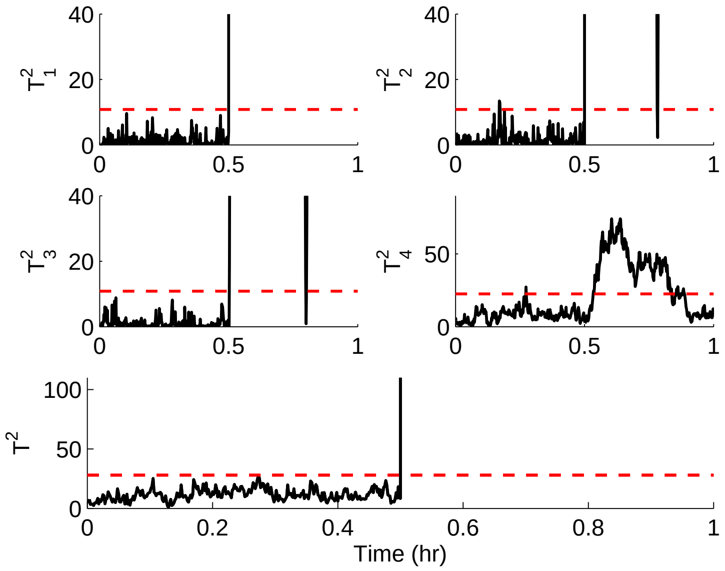


Figure 3.9: Plots of the T^2 statistic (solid) with the corresponding T^2_{UCL} (dashed) for each of the subsystems and for the full state vector under nonlinear feedback control with a failure in d_1 at $t = 0.5$ hr.

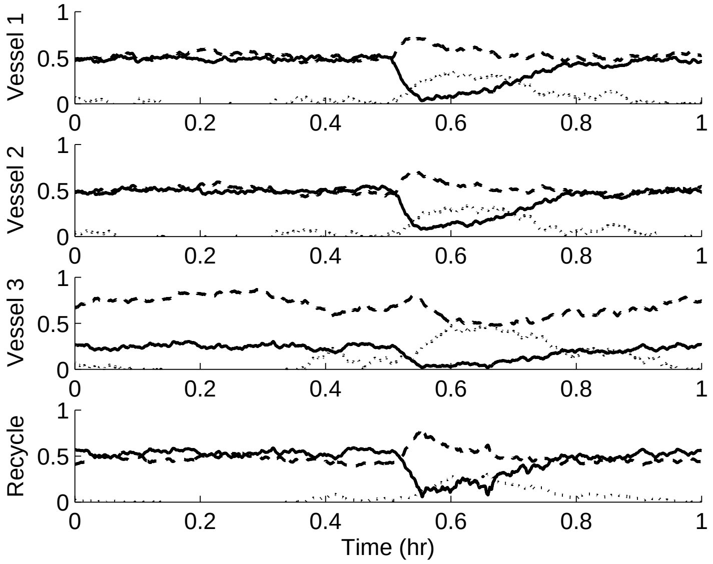


Figure 3.10: Plots of the mass fractions x_A (solid), x_B (dashed) and x_C (dotted) for the system under PI control with a failure in d_1 at $t = 0.5\ hr$.

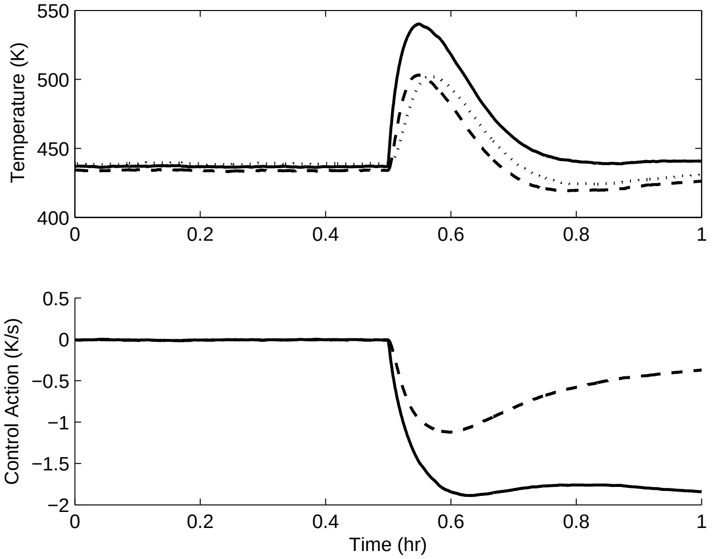


Figure 3.11: (top) Temperature trajectories for T_1 (solid), T_2 (dashed) and T_3 (dotted) for the system under PI-only control with a failure in d_1 at $t = 0.5\ hr$. (bottom) Control action requested for the same system for u_1 (solid) and u_2 (dashed).

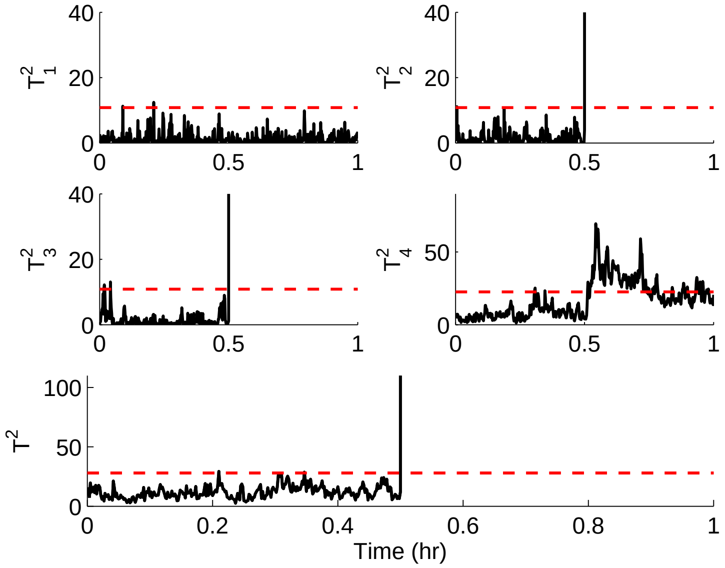


Figure 3.12: Plots of the T^2 statistic (solid) with the corresponding T^2_{UCL} (dashed) for each of the subsystems and for the full state vector under nonlinear feedback control with a failure in d_2 at $t = 0.5\ hr$.

structure correctly shows that T_1 is decoupled from the fault, making it possible to identify. Figure 3.13 shows a comparison of the temperature plots for the PI-only controller and the nonlinear feedback controller to illustrate this point. The plot in Figure 3.13 (top) shows that under PI-only control all of the temperature trajectories are affected (as well as the mass fraction trajectories, however, these have been omitted for brevity) whereas under the nonlinear feedback controller, the unique response can be identified in Figure 3.13 (bottom) by the fact that the T_1 trajectory is unchanged.

The T^2 plots for the system under nonlinear feedback control with a failure in d_3 are shown in Figure 3.14. This also shows the expected behavior corresponding to the fault signatures defined in Eq.3.12; that is, the fault affected only the temperature of the flash tank and did not influence the other states. The PI comparison (omitted) showed similar results as before in that all states were affected and a fault could not be isolated based on measured data. Finally, note that for the system under nonlinear feedback control with a failure in d_4 (see Figure 3.15), the fault signature only shows that the fault affects the dynamics of the states in $q_4 = \{x_{A1}, x_{A2}, x_{A3}, x_{B1}, x_{B2}, x_{B3}\}$. In this case the fault signature

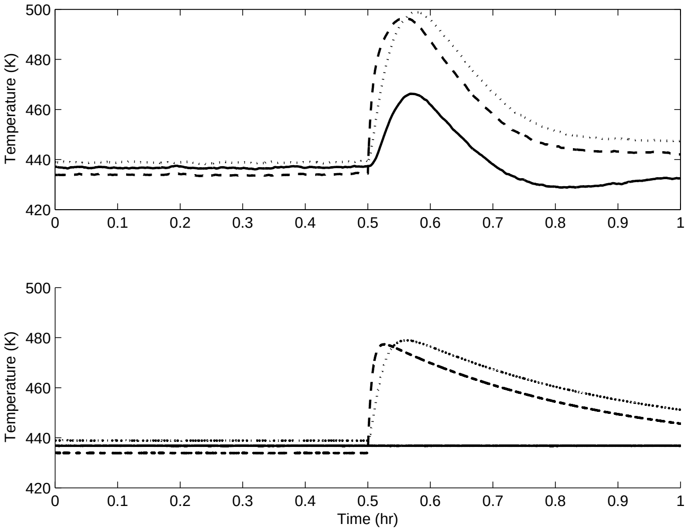


Figure 3.13: Temperature trajectories for T_1 (solid), T_2 (dashed) and T_3 (dotted) for the system with a failure in d_2 at $t = 0.5\ hr$ under PI-only (top) and nonlinear feedback control (bottom).

indicates that there is a fault in d_4, but is unable to distinguish between any of the faults that directly affect the states within this set.

As mentioned in Remark 12, it is possible that faults of intermediate size can be detected but not accurately isolated due to the states being on the threshold of detection and/or possible small gain effects of the directly affected subsystem on another. This was tested in the present model by randomly varying the fault sizes of each of the four faults between 0 and twice the value used in the prior 4 simulations. Each fault was tested over 500 simulations to determine how large of a fault is necessary to detect and isolate the fault accurately. Table 3.4 shows the results for these simulations. The results present the range of values for which faults were either undetected, falsely isolated or correctly isolated as well as the number of simulations for which the faults values fell within the indicated range.

As shown in Table 3.4, faults d_1 and d_2 had a range of values for which false isolations occurred. This was largely due to the fact that the temperatures had a relatively small gain effect on the mass fractions. This can be compensated for, partially, by increasing the upper control limit of the statistical test for fault detection (T^2_{UCL} for the full state vector).

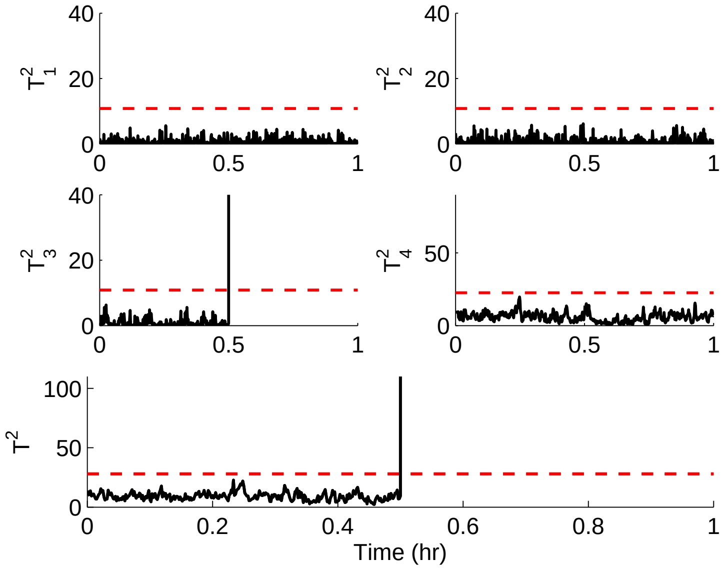


Figure 3.14: Plots of the T^2 statistic (solid) with the corresponding T^2_{UCL} (dashed) for each of the subsystems and for the full state vector under nonlinear feedback control with a failure in d_3 at $t = 0.5$ hr.

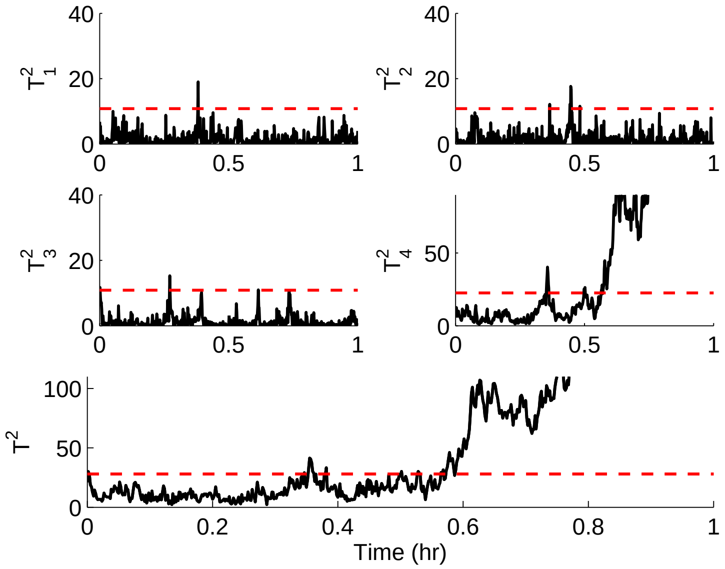


Figure 3.15: Plots of the T^2 statistic (solid) with the corresponding T^2_{UCL} (dashed) for each of the subsystems and for the full state vector under nonlinear feedback control with a failure in d_4 at $t = 0.5$ hr.

Table 3.4: Fault sizes and results from the Monte-Carlo Simulation Study

Undetected	(count)	False Isolation	(count)	Correct Isolation	(count)
$0 < d_1 < 0.014$	(10)	$0.027 < d_1 < 0.50$	(121)	$0.52 < d_1 < 2$	(369)
$0 < d_2 < 0.022$	(3)	$0.036 < d_2 < 1.49$	(192)	$1.53 < d_2 < 4$	(101)
$0 < d_3 < 0.014$	(10)		(0)	$0.027 < d_3 < 2$	(490)
$0 < -d_4 < 0.0012$	(165)		(0)	$0.0012 < -d_4 < 0.002$	(335)

While this makes the FDI scheme less sensitive, this reduces both the incidence of false alarms and false isolations.

3.4 Conclusions

This work has demonstrated the application of a model-based nonlinear controller designed to enforce an isolable structure in the closed-loop system of a multi-unit reactor-separator chemical process. Fault detection and isolation were performed using statistical process monitoring techniques and information based upon the imposed closed-loop system structure. This was demonstrated through numerical simulation studies of the closed-loop system in the presence of four different faults. It was shown that by decoupling faults of interest from certain states, it was possible to achieve unique system responses to each of the four faults allowing fault isolation based on process measurements only. These results were compared with a conventional PI controller and were thoroughly tested for susceptibility to false isolation through a Monte-Carlo simulation study of 500 runs for each of the four fault scenarios.

Chapter 4

Controller-enhanced FDI:Output feedback and Optimality

4.1 Introduction

This chapter considers the issues of output-feedback control and optimal control in the setting of data-based FDI using feedback control. The purpose this chapter is to further develop the approach proposed in Chapter 2 by relaxing the requirement of full state feedback control and developing the use of model predictive control to optimize the manipulated input cost. Specifically, we first consider the case where only output measurements are available and design appropriate state estimator-based output feedback controllers to achieve controller-enhanced fault detection and isolation in the closed-loop system. Second, we address the problem of controller-enhanced FDI in an optimal fashion within the framework of model predictive control (MPC). We propose an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. Throughout the chapter, a nonlinear chemical process example is used to demonstrate the applicability and effectiveness of the proposed methods.

4.2 Preliminaries

4.2.1 Process system structure

In this chapter, we consider nonlinear process systems with the following general state-space description:

$$\dot{x} = f(x, u, d) \tag{4.1}$$

where $x \in R^n$ is the vector of process state variables, $u \in R^m$ is the vector of manipulated input variables and $d \in R^p$ is the vector of p possible actuator faults or disturbances. Vector d is equal to zero when the system is under normal operating conditions. When fault k, with $k = 1, ..., p$ occurs, the k^{th} component of vector d, denoted d_k, can take any time-varying value. This model includes a broad class of possible faults. The approach of controller enhanced FDI was introduced in Chapter 2 as a method of dividing the state vector into a number of partially decoupled subvectors. These subvectors can be monitored using measured process data. Based on their responses and the system structure enforced by the decoupling controller, it is possible to discriminate between individual faults or groups of faults. Decoupling into subvectors can be accomplished by using model-based control laws to enforce the appropriate structure (see subsection 4.2.3.) In order to understand the necessary structure to perform isolation, we review the definitions of the incidence graph, the reduced incidence graph and the isolability graph.

Definition 12 *The incidence graph of the system of Eq.4.1 is a directed graph defined by n nodes, one for each state, x_i, $i = 1 \ldots n$, of the system. A directed arc with origin in node x_i and destination in node x_j exists if and only if $\frac{\partial f_j}{\partial x_i} \neq 0$.*

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

Definition 13 *The reduced incidence graph of the system of Eq.4.1 is the directed graph of N nodes, one for each q_i, $i = 1 \ldots N$, where N is the maximum number of nodes that* *satisfy the following conditions:*

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

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

- *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.*

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

Definition 14 *The isolability graph of the system of Eq.4.1 is a directed graph made of the N nodes of the reduced incidence graph and p additional nodes, one for each possible fault d_k. In addition, a directed arc with origin in fault node d_k and destination to a state node q_j exists if and only if $\frac{\partial f_l}{\partial d_k} \neq 0$ for some $x_l \in X_j$.*

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

$$\begin{aligned}
\dot{x}_1 &= -x_1 + x_2 + d_1 \\
\dot{x}_2 &= x_1 + 2x_2 + d_2 \\
\dot{x}_3 &= -2x_1 + x_3 + d_3
\end{aligned} \tag{4.2}$$

Because x_1 and x_2 are mutually dependent but are not affected by x_3, they form a partially decoupled subsystem represented by a single node (q_1) in the isolability graph leaving x_3 to form a node by itself (q_2). Figure 4.1 shows the isolability graph for the system of Eq.4.2.

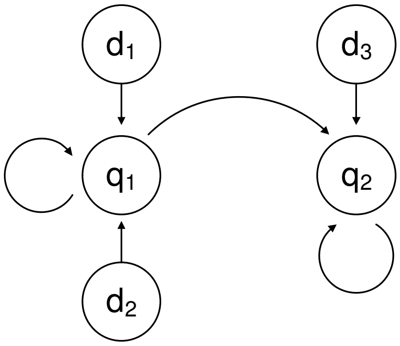


Figure 4.1: Isolability graph of the system of Eq.4.2.

With the isolability graph of a system, it is possible to consider fault isolation based upon monitoring the subsystems. For this purpose, it is necessary to review the definition of a fault signature given below:

Definition 15 *The signature of a fault d_k of the system of Eq.4.1 is a binary vector W^k of dimension N, where N is the number of nodes of the reduced incidence graph of the system. The i^{th} component of W^k, denoted W_i^k, is equal to 1 if there exists a path in the isolability graph from the node corresponding to fault d_k to the node q_i corresponding to the set of states X_i, or 0 otherwise.*

Using this definition of a fault signature and the isolability graph shown in Figure 4.1, it is possible to identify the fault signatures for the three faults considered in the system of Eq.4.2. In this case, the fault d_3 has the signature $W^3 = [0\ 1]^T$ and the two faults d_1 and d_2 have the signature $W^1 = W^2 = [1\ 1]^T$. Thus, based on the fault signatures, it is possible to distinguish between a failure in d_3 from a failure in d_1 or d_2. However, it is not generally possible to discriminate between failures in d_1 and d_2.

Remark 14 *It should be noted that while d_i can model any type of fault, the present approach does not attempt to distinguish between types of faults (e.g., disturbances or actuator faults) that would affect the dynamics of the same state. That is, two faults which affect the system dynamics through the same state are isolated as the same fault in this method (e.g., an inlet temperature disturbance and heat-jacket actuator failure would both affect the reactor temperature dynamics and would thus appear identical in the fault detection scheme).*

For recent work on discriminating disturbances from actuator failures, see [24].

Remark 15 *There are other approaches in the literature that examine the necessary structural conditions in order to perform model-based fault diagnosis (see, for example, [25, 12, 13]). While these approaches are similar to our approach in that they take into consideration the system structure and develop conditions for fault diagnosis, they differ in the fact that they do not enforce the necessary structure for fault detection and isolation in the closed-loop system via feedback control and use model-based fault diagnosis as opposed to the data-based fault diagnosis approach used in this work.*

4.2.2 Process monitoring

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

For the purpose of monitoring whether or not a state has deviated from its normal behavior, we use statistical process monitoring methods. In particular, we use Hotelling's T^2 statistic [27], a well established method in statistical process control that monitors multivariate normal (Gaussian) data using a single statistic [60]. Because of its suitability for continuous, serially correlated chemical processes, the method of using single observations is employed [63, 50]. Given a multivariate state vector x of dimension n, the T^2 statistic can be computed using the mean $\bar{x}$ and the estimated covariance matrix S of process data obtained under normal operating conditions (see, for example, [60, 31]), as follows:

$$T^2 = (x - \bar{x})^T S^{-1} (x - \bar{x}). \tag{4.3}$$

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

$$T^2_{UCL} = \frac{(h^2 - 1)n}{h(h - n)} F_\alpha(n, h - n) \tag{4.4}$$

where h is the number of historical measurements used in estimating S, $F_\alpha(n, h - n)$ is the value on the F distribution with $(n, h - n)$ degrees of freedom for which there is probability α of a greater or equal value occurring. Thus, α is the probability of a false alarm. This distribution is based on the assumption that the data are multivariate normal. This requirement is generally a reasonable assumption since even process data that may be serially correlated under open-loop operation are frequently close to normal in the closed-loop system under feedback control on a large time-scale [50]. The validity of this assumption of normal process data in the closed-loop system has been verified in Chapter 2. It has also been verified in the context of the reactor example used in the present chapter. Similar results verifying that the closed-loop system data in the reactor example are normal are not given in the present chapter for brevity and to avoid redundancy.

The T^2 statistic is used to both detect that a fault has occurred and to provide the system signature that can be compared with the fault signatures defined by the isolability graph. In order to perform these tasks, the T^2 statistic based on the full state vector x with upper control limit T^2_{UCL} is first used to detect the presence of a fault. Subsequently, the T^2_i statistic is used to monitor the status of each subset of the state vector with an upper control limit T^2_{UCLi} where $i = 1, \ldots, N$ that is based on each of the subvectors and their states $x_j \in X_i$. The fault detection and isolation procedure then follows the steps given below:

1. A fault is detected if $T^2(t) > T^2_{UCL}$ $\forall t$ $t_f \leq t \leq t_f + T_P$ where t_f is the last time

when T^2 crossed the UCL (i.e., after time t_f, T^2 does not return to any values below T^2_{UCL})) and T_P is the fault detection window chosen to be large enough to allow fault isolation with a desired degree of confidence. Choosing T_P depends on the process time constants and potentially on available historical information of past process behavior.

2. Fault isolation can be performed by comparing fault signatures with the process signature $W(t_f, T_P)$ which can be built as follows:

$$T_i^2(t) > T^2_{UCLi} \; \forall t \; t_f \leq t \leq t_f + T_P \rightarrow W_i(t_f, T_P) = 1.$$
$$T_i^2(t) \ngtr T^2_{UCLi} \; \forall t \; t_f \leq t \leq t_f + T_P \rightarrow W_i(t_f, T_P) = 0.$$

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

4.2.3 Controller design for enhanced FDI

Decoupling controller design

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

$$\begin{aligned}\dot{x}_1 &= f_{11}(x_1) + f_{12}(x_1, x_2) + g_1(x_1, x_2)u + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2\end{aligned} \tag{4.5}$$

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

$$u(x_1, x_2) = -\frac{f_{12}(x_1, x_2) - v(x_1)}{g_1(x_1, x_2)} \tag{4.6}$$

the closed-loop system takes the form

$$\begin{aligned}\dot{x}_1 &= f_{11}(x_1) + v(x_1) + d_1 \\ \dot{x}_2 &= f_2(x_1, x_2) + d_2\end{aligned} \tag{4.7}$$

where $v(x_1)$ has to be designed in order to achieve asymptotic stability of the origin of the x_1 subsystem when $d_1 = 0$. In this case, the controller of Eq.4.6 guarantees asymptotic stability of the closed-loop system, as well as different signatures for faults d_1 and d_2. Note that the closed-loop system in this case can be broken down into two subvectors, each including one state, and the signatures are given by $W^1 = [1\ 1]^T$ and $W^2 = [0\ 1]^T$. If necessary, using multiple controllers allows for more degrees of freedom in breaking up the full state vector into subvectors and allowing fault isolation. Note that in this example, the x_2 subsystem must be input-to-state stable with respect to x_1.

Input/output linearizable nonlinear systems

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

$$\begin{aligned}\dot{x} &= f(x) + g(x)u + \sum_{k=1}^{p} w_k(x)d_k \\ y &= h(x)\end{aligned} \tag{4.8}$$

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

The main control objective is to design a feedback control law $u = p_{DC}(x)$ such that the closed-loop system has an asymptotically stable equilibrium point, and the input/output response is linear. Moreover, the closed-loop system must satisfy the isolability conditions by having two or more groups of faults with unique system signatures. To this end, we review the definition of relative degree of the output, y, with respect to the input, u, in the system of Eq.4.8.

Definition 16 *[28]: Referring to the system of Eq.4.8, the relative degree of the output, y, with respect to the input, u, is the smallest integer, $r \in [1, n]$, for which*

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

If the system of Eq.4.8 has input relative degree $r < n$, then there exists a coordinate transformation (see [28]) $(\zeta, \eta) = \Theta(x)$ such that the representation of the system of Eq.4.8

with $d_k = 0$ for all $k = 1, ..., p$, in the (ζ, η) coordinates, takes the form

$$\begin{array}{rcl}\dot{\zeta}_1 & = & \zeta_2 \\ & \vdots & \\ \dot{\zeta}_{r-1} & = & \zeta_r \\ \dot{\zeta}_r & = & L_f^r h(x) + L_g L_f^{r-1} g(x) u \\ \dot{\eta}_1 & = & \Psi_1(\zeta, \eta) \\ & \vdots & \\ \dot{\eta}_{n-r} & = & \Psi_{n-r}(\zeta, \eta)\end{array} \tag{4.9}$$

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

$$u(x) = \frac{1}{L_g L_f^{r-1} h(x)} [v(x) - L_f^r h(x)] \tag{4.10}$$

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

If the state-feedback law given in Eq.4.10 is used, it can be shown that the faults of the system of Eq.4.8 can be isolated into two different groups: those that affect the output and those that do not affect the output. It is important to note here that the output function, $h(x)$, can be appropriately chosen as a nonlinear combination of the states, x, to aid the task of fault detection and isolation using a feedback linearizing controller design. The induced structure of the closed-loop system in the transformed coordinates (ζ, η) provides different signatures for the faults depending on their relative degree which is defined below:

Definition 17 *[10]: Referring to the system of Eq.4.8, the relative degree, $\rho_k \in [1, n]$, of the output, y, with respect to the fault d_k is the smallest integer for which*

$$\begin{array}{l} L_{w_k} L_f^i h(x) = 0, \; i = 0, \ldots, \rho_k - 2 \\ L_{w_k} L_f^{\rho_k - 1} h(x) \neq 0. \end{array} \tag{4.11}$$

Analogous to the relative degree of the output with respect to the input, this definition of relative degree relates the output to a particular fault. If a feedback-linearizing controller is used, then the faults can be divided into two different groups: those with a relative degree ρ_k that is greater than the relative degree r and those with a relative degree ρ_k that is less than or equal to r. When a fault occurs, the faults of the first group will not affect the output, y, while those of the latter will. Thus, using the control law in Eq.4.10, the possible faults of the system of Eq.4.8 are divided into two groups, each with a different signature. When a fault occurs, taking into account whether the trajectory of the output has deviated from the normal case or not, it is possible to isolate to which group the fault belongs.

Remark 16 *Note that in order for the feedback linearizing controller of Eq.4.10 to decouple the output from the specific group of faults described above, the first-principles model must match that of the actual process. In a practical application, there is tolerance for some degree of plant-model mismatch that can be accounted for by the fault detection thresholds. In this case, there is not perfect decoupling but the enforcement of near-decoupling in the closed-loop system by the controller that still allows for fault detection and isolation. On the other hand, large discrepancies between the plant and the model would not allow enforcing the desired structure.*

4.3 Controller enhanced FDI using output feedback control

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

4.3.1 State estimation

In order to perform controller enhanced FDI using output feedback control, any unknown process state variable must be quickly and accurately estimated from the available output measurements so that the decoupling state feedback controller designs of subsections 4.2.3 and 4.2.3 can be implemented. The state estimation is performed for the state vector x (or a subset thereof) with the outputs, or measured states, defined as $y = Cx$. In this chapter, we consider only outputs of the form $y_i = x_i$, $i = 1, \ldots, q < n$. In other words, C is a matrix with one and only one non-zero entry in each row and that entry is equal to unity. This set-up is appropriate in chemical process control applications where measurements of a few states like temperature and concentrations of a few species, like key products, are available, but concentrations of some species are not measured. This set-up also allows obtaining a clear picture of the use of output feedback instead of full state feedback in controller enhanced FDI. The theory for the state estimator design is based upon a linear system, but can also be applied to nonlinear systems, using a local stability analysis around the operating point (origin). Specifically, the linearized model of the nonlinear system of Eq.4.1 takes the following form:

$$\begin{aligned} \dot{x} &= Ax + Bu + Wd \\ y &= Cx \end{aligned} \tag{4.12}$$

where A is the Jacobian matrix of the nonlinear system at the operating point, u is the manipulated input vector and d is the fault vector. The matrices B and W can be computed from the linearization of Eq.4.1 around the origin. Under the assumption that (A, C) forms an observable pair, each state variable x can be estimated by the following dynamic equation:

$$\dot{\hat{x}} = A\hat{x} + Bu + L(y - C\hat{x}) \tag{4.13}$$

where $\hat{x}$ is the state estimate and L is the estimator gain that can be chosen so that all the eigenvalues of the matrix $(A - LC)$ are placed at appropriate locations in the left-half of the complex plane to guarantee a desirable rate of convergence of the estimation error to zero. The computation of L can be done using standard pole placement techniques or via a Kalman filtering framework by adding process and measurement noise in the linearized model of Eq.4.12. In either case, the linearized state estimation error equation with $d(t) = 0$ takes the form:

$$\dot{e} = (A - LC)e. \tag{4.14}$$

where $e = x - \hat{x}$ is the estimation error. While it is possible to perform state estimation using the full state vector in the state estimator of Eq.4.13 when $d(t) \equiv 0$, it becomes necessary to use a reduced-order process model when designing a state estimator-based output feedback controller to enhance FDI. This need for a reduced-order model arises due to faults that affect the state estimator and introduce error into the estimate (i.e., the full state estimation scheme of Eq.4.13 works when $d(t) = 0$, but not when $d(t) \neq 0$). Specifically, if the error vector d on the right-hand side of Eq.4.12 is nonzero, the new equation for the estimator error becomes $\dot{e} = (A - LC)e + Wd$. Thus, in the presence of a fault, the state estimates no longer converge to their actual values, and the isolable structure attained in the closed-loop system under state feedback control cannot be maintained. However, it is possible in some process systems to perform the state estimation task using a subset of the states that are not directly affected by the expected faults, i.e., effectively eliminating d in the estimation error system. The general structure of the model in Eqs.4.12-4.14 remains the same for the reduced-order system, but it is based on a subset of the full state vector, $x_r \subset x$. To mathematically realize this notion, consider a system with the following structure, where time derivatives of the states x_r are not functions of d and include all unknown states to be estimated along with some measured states, and x_d includes the remaining measured states, whose dynamic equations may be functions of d. Specifically, we consider the following decomposition of the vectors and matrices of the linearized system of Eq.4.12

$$\begin{aligned} x &= \begin{bmatrix} x_r \\ x_d \end{bmatrix}, \quad A = \begin{bmatrix} A_r & A_{rd} \\ A_{dr} & A_d \end{bmatrix}, \quad W = \begin{bmatrix} 0 \\ W_d \end{bmatrix} \\ B &= \begin{bmatrix} B_r \\ B_d \end{bmatrix}, \quad C = \begin{bmatrix} C_r & 0 \\ 0 & C_d \end{bmatrix}, \quad y = \begin{bmatrix} y_r \\ y_d \end{bmatrix}. \end{aligned} \tag{4.15}$$

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

$$\dot{\hat{x}}_r = A_r\hat{x}_r + A_{rd}x_d + B_ru + L_r(y_r - C_r\hat{x}_r) \tag{4.16}$$

Eq.4.16 uses the actual measured values for all of the states in x_d. We can break x_r down further into measured states and unmeasured states, $x_r = [x_{rm}^T \; x_{ru}^T]^T$. Note that x_{rm} must include enough measured states independent of d for the system to be observable. Given the restrictions on C, this implies that $y_r = C_rx_r = x_{rm}$ and $C_d = I$ (i.e., $y_d = x_d$). Finally, we define a vector with full state information by combining the measured and estimated data, $\hat{x} = [x_{rm}^T \; \hat{x}_{ru}^T \; x_d^T]^T$. Note that $\hat{x}_{rm}$ is only used as the driving force for convergence of the state estimator. With these definitions, the reduced-order state estimator of Eq.4.16 is not a direct function of d and the dynamics of the estimation error, $e_r = x_r - \hat{x}_r$, take the form $\dot{e}_r = (A_r - L_rC_r)e_r$ which implies that $e_r(t)$ will converge to zero even in the presence of a change in d.

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

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

$$\dot{\hat{x}}_r = f_r(\hat{x}_r, x_d, u) + L_r(y_r - h_r(\hat{x}_r)) \tag{4.17}$$

where the measured values are used for the states in x_d, i.e., by assumption $y_d = x_d$. Note that following the previous assumption, $h_r(x_r) = C_r x_r$. Combining the nonlinear state estimator of Eq.4.17 with a nonlinear state feedback controller, $u = p_{DC}(x)$, that enforces an isolable structure in the closed-loop system and can be designed following the approaches presented in subsections 4.2.3 and 4.2.3, we obtain the following dynamic nonlinear output feedback controller:

$$\begin{aligned} \dot{\hat{x}}_r &= f_r(\hat{x}_r, x_d, p_{DC}(\hat{x})) + L_r(y_r - C_r\hat{x}_r) \\ u &= p_{DC}(\hat{x}) \end{aligned} \tag{4.18}$$

Due to the effect of estimation error, it is not possible to achieve complete decoupling. However, it is possible to achieve a near isolable structure that is sufficient for practical purposes. In this sense, we consider a near isolable structure to be one where the closed-loop system under output feedback control can be seen as an $O(e_r)$ regular perturbation of the closed-loop system under state feedback control which is locally exponentially stable and has an isolable structure. Thus, the estimation error can be viewed as a small perturbation error that will be accounted for by the FDI thresholds designed to filter out normal process variation. Theorem 2 below summarizes the main analysis and controller design result of this section as well as the closed-loop FDI properties.

Theorem 2 *Consider the closed-loop system of Eq.4.1 under the nonlinear output feedback controller of Eq.4.18 and assume that the pair (A_r, C_r) is observable and L_r is designed such that the matrix $(A_r - L_rC_r)$ has all of its eigenvalues in the left-half of the complex plane. Then, there exist δ, ϵ and T_y such that if f is continuously differentiable on $D = \{x \in R^n| \ \|x\|_2 < \delta\}$, the Jacobian of f is bounded and Lipschitz on D and*

$\max\{\|x(t_0)\|_2, \|\hat{x}_r(t_0)\|_2\} < \delta$ *then* $\|x_r(t) - \hat{x}_r(t)\|_2 < \epsilon,\ \forall t > t_0 + T_y$*, and a near isolable structure is enforced in the closed-loop system.*

Proof: Under the control law of Eq.4.18, the closed-loop system of Eq.4.1 takes the form,

$$\begin{aligned} \dot{x} &= f(x, p_{DC}(\hat{x}), d), \quad y = h(x) \\ \dot{\hat{x}}_r &= f_r(\hat{x}_r, x_d, p_{DC}(\hat{x})) + L_r(y_r - h_r(\hat{x}_r)). \end{aligned} \tag{4.19}$$

Linearizing the closed-loop system of Eq4.19 around the equilibrium point (origin) yields,

$$\dot{x} = Ax + Bp_{DC}(\hat{x}), \quad y = Cx \tag{4.20}$$

$$\dot{\hat{x}}_r = A_r\hat{x}_r + A_{rd}x_d + B_r p_{DC}(\hat{x}) + L_r(y_r - C_r\hat{x}_r). \tag{4.21}$$

The error between the actual and estimated states of the reduced-order, linearized system is then $e_r = x_r - \hat{x}_r$ with the dynamics $\dot{e}_r = (A_r - L_rC_r)e_r$. Assuming that the pair (A_r, C_r) is observable and that L_r is chosen such that the matrix $A_r - L_rC_r$ has eigenvalues in the left-half of the complex plane, the estimation error, e_r, in the linearized system has exponentially stable dynamics. If the vector field of the nonlinear system, $f(x, p_{DC}(\hat{x}), d)$, is continuously differentiable and the Jacobian matrix is bounded and Lipschitz on $D = \{x \in R^n |\ \|x\|_2 < \delta\}$, then the nonlinear system dynamics are also locally, exponentially stable within some region around the equilibrium point [29]. For some initial condition $max\{\|x_0\|_2, \|x_{r0}\|_2\} < \delta$, the state estimation error, e_r, will be bounded such that $\|x_r - \hat{x}_r\| < \epsilon\ \forall t > t_0 + T_y$, where T_y is a time interval of $O(\epsilon)$. Thus, the output feedback control approaches state feedback control with error of order ϵ, i.e., $x_r = \hat{x}_r + O(\epsilon)\ \forall t > t_0 + T_y$. For sufficiently small ϵ, this leads to a near isolable structure in the closed-loop system for almost all times since the state feedback controller $p_{DC}(x)$ enforces an isolable structure in the closed-loop system. **QED**

Remark 17 *Theorem 2 provides sufficient conditions on the process structure, location of faults and/or disturbances and measurement vector such that controller-enhanced isolation of the type made possible under state feedback control is also possible under output feedback control. The achievement of a near isolable structure refers to the fact that with a sufficiently* *small ϵ, the effect of the state estimator error will become increasingly negligible relative to the common-cause variance and the detection threshold for FDI. Thus, even though the state estimate will retain some small amount of error, it will be sufficiently small as to be masked by the normal sensor measurement and process noise which is accounted for in the FDI detection thresholds.*

4.3.2 Application to a CSTR example

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

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

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

$$\begin{aligned} r_1 &= k_{10} e^{\frac{-E_1}{RT}} C_A, \;\; r_{-1} = k_{-10} e^{\frac{-E_{-1}}{RT}} C_B && (4.22) \\ r_2 &= k_{20} e^{\frac{-E_2}{RT}} C_B, \;\; r_{-2} = k_{-20} e^{\frac{-E_{-2}}{RT}} C_C && (4.23) \end{aligned}$$

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

Table 4.1: 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	$0.231\ [kJ/kg \cdot K]$		

model of the process is obtained

$$\begin{aligned}
\dot{C_A} &= \tfrac{F}{V}(C_{A0} - C_A) - r_1 + r_{-1} + d_1 \\
\dot{C_B} &= -\tfrac{F}{V}C_B + r_1 - r_{-1} - r_2 + r_{-2} \\
\dot{C_C} &= -\tfrac{F}{V}C_C + r_2 - r_{-2} \\
\dot{T} &= \tfrac{F}{V}(T_0 - T) + \tfrac{(-\Delta H_1)}{\rho c_p}(r_1 - r_{-1}) + \tfrac{(-\Delta H_2)}{\rho c_p}(r_2 - r_{-2}) + u + d_2
\end{aligned} \tag{4.24}$$

where V is the reactor volume, ΔH_1 and ΔH_2 are the enthalpies of the first and second reactions, respectively, ρ is the fluid density, c_p is the fluid heat capacity, $u = Q/\rho c_p$ is the manipulated input, where Q is the heat input to the system, d_1 denotes a disturbance in the inlet concentration and d_2 denotes a fault in the control actuator. The values for the parameters of the process model are given in Table 4.1.

The system of Eq.4.24 is modeled with sensor measurement noise and autoregressive process noise. The sensor measurement noise was generated using a Gaussian distribution with standard deviation σ_M applied to the measurements of all the process states. The autoregressive process noise was generated discretely as $w_k = \phi w_{k-1} + \xi_k$ where $k = 0, 1, \ldots$ is the discrete time step, ϕ is the autoregressive coefficient and ξ_k is obtained at each sampling step using a zero-mean normal distribution with standard deviation σ_p. Table 4.2 provides the values of the noise parameters for each state of the system of Eq.4.24. The sampling time interval is $\Delta t_s = 0.1\ min$ and the fixed numerical integration time interval

Table 4.2: 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

is $\Delta t_i = 0.001\ min$. In this example, the state, C_B, is considered to be unmeasured and is subject to process noise. It should be noted that the open-loop system of Eq.4.24 has fully coupled dynamics. This means that the two faults d_1 and d_2 will be indistinguishable from a data-based perspective because either fault will affect all of the states. Thus, purely data-based FDI is not possible without enforcing an isolable structure in the closed-loop system.

In order to obtain the estimated trajectory for C_B, a state estimator as in Eq.4.17 was implemented using the reduced-order system $\hat{x}_r = [\hat{C}_B\ \hat{C}_C]^T$. The process measurements for C_A and T were used in computing the dynamics of $\hat{x}_r$. Note that although C_C is measured, it is used in the reduced-order state estimator so that the reduced-order system is observable. The control input was updated at each sampling interval with the measured values for C_A, T and C_C and the estimated value of $\hat{C}_B$. As discussed in subsection 4.3.1, C_A and T should not be modeled as dynamic states in the estimator since they are directly affected by the faults d_1 and d_2. Therefore, the measured process data of C_A and T must be used in modeling the estimator. Thus, the final form of the state estimator based on the reduced subsystem $\hat{x}_r = [\hat{C}_B\ \hat{C}_C]^T$ is as given below:

$$\begin{aligned}\dot{\hat{C}}_B &= -\tfrac{F}{V}\hat{C}_B + r_1 - r_{-1} - r_2 + r_{-2} + L_1(C_C - \hat{C}_C)\\ \dot{\hat{C}}_C &= -\tfrac{F}{V}\hat{C}_C + r_2 - r_{-2} + L_2(C_C - \hat{C}_C)\end{aligned} \tag{4.25}$$

with

$$\begin{aligned}r_1 &= k_{10}e^{\frac{-E_1}{RT}}C_A,\ \ r_{-1} = k_{-10}e^{\frac{-E_{-1}}{RT}}\hat{C}_B\\ r_2 &= k_{20}e^{\frac{-E_2}{RT}}\hat{C}_B,\ \ r_{-2} = k_{-20}e^{\frac{-E_{-2}}{RT}}\hat{C}_C\end{aligned}$$

where L is the filter gain obtained using Kalman-filtering theory based on the reduced-order system for the sensor and process noise given in Table 4.2. The resulting value for L_r is $[L_{r1}\ L_{r2}]^T = [0.0081\ 0.0559]^T$.

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

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

$$C_{As} = 2.06\frac{kmol}{m^3},\ C_{Bs} = 1.00\frac{kmol}{m^3},\ C_{Cs} = 0.937\frac{kmol}{m^3},\ T_s = 312.6K,\ u_s = 0K/s. \quad (4.26)$$

where the subscript s refers to the steady state values of the variables. It should be noted that the CSTR system of Eq.4.24 belongs to the class of systems of Eq.4.1 with $x = [C_A - C_{As},\ T - T_s,\ C_B - C_{Bs},\ C_C - C_{Cs}]^T$ where C_B is replaced with $\hat{C}_B$ in the definition of $\hat{x}$. This implies that we can apply the output feedback scheme presented using the controlled output $y = C_C$. Using Eq.4.10, the feedback-linearizing controller takes the following form:

$$u = \frac{v - L_f^2 h(\hat{x})}{L_g L_f h(\hat{x})} \quad (4.27)$$

with

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

where

$$\begin{aligned}
\zeta_1 &= C_C \\
\zeta_2 &= -\tfrac{F}{V}C_C + r_2 - r_{-2} \\
r_2 &= k_{20}e^{\frac{-E_2}{RT}}\hat{C}_B, \;\; r_{-2} = k_{-20}e^{\frac{-E_{-2}}{RT}}C_C.
\end{aligned}$$

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

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

Figure 4.2 shows the trajectories for each of the states in the simulation with a failure in d_1. The fault is apparent at approximately $t = 40\ min$ $(0.667hr)$. We can readily see from the state trajectories, that the decoupling scheme was effective as evidenced by the fact that the output, C_C, is unaffected by the fault. Also, we see that the state estimator converged relatively quickly at around $t = 3\ min$.

For the system with a failure in d_1, Figure 4.3 shows the Hotelling's T^2 statistic for the two subvectors X_1 and X_2 as well as for the full state vector. From the graph, we can see that a fault is clearly detected at the expected time $t = 40\ min$ as shown in the plot of the T^2 statistic for the full state vector (T_3^2). Although there were a few single incidents of data breaching the upper control limit, none of them represented sustained departures for the length of the fault detection window, T_P. Also note that values above the upper control limit before $t = 0.1hr$ were due to the state estimator not having converged. Upon detection of the fault, the system signature can be computed as $W = [1\ 0]^T$ due to the fact that the T^2 statistic for the subvector X_1 exceeded the upper control limit for a sustained period and the T^2 for the subvector X_2 remained within the bounds of normal operation.

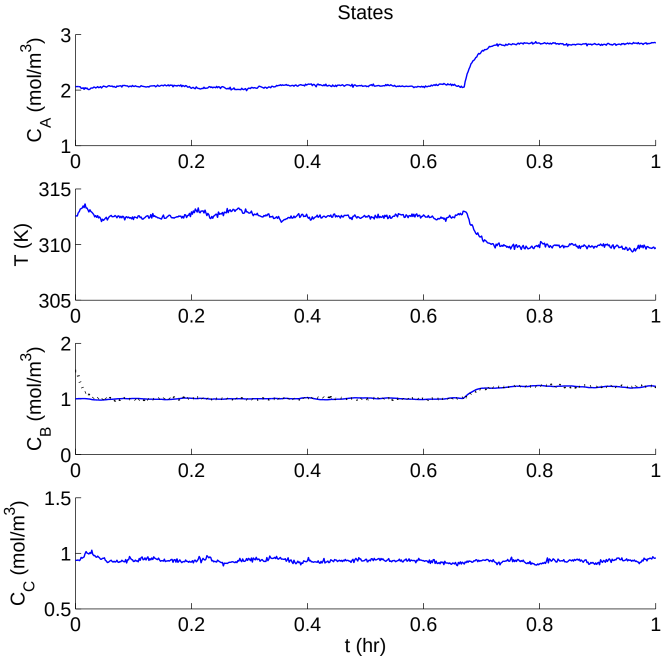


Figure 4.2: Plot of measured state values for the CSTR under output feedback decoupling control with fault d_1. C_B shows both actual (solid) and estimated (dotted) values.

Because the system signature matches that of the fault signature for d_1, a fault in d_1 is declared at time $t \approx 41$ min.

In Figure 4.4, we see the simulation results for the same system with a failure in d_2. Again, the failure is evident around $t = 40$ min. However, in this case we see that all state trajectories are affected. The process signature obtained from the T^2 statistics in Figure 4.5 shows that both subvectors were affected and this process signature matches the fault signature of d_2.

The control action required to decouple and stabilize the system is shown in Figure 4.6.

Remark 18 *It is important to point out that in the output feedback control formulation presented above, the output measurements are assumed to be continuously available. The reader may refer to [38] for recent results on model-based fault detection and isolation using a combination of synchronous and asynchronous measurements.*

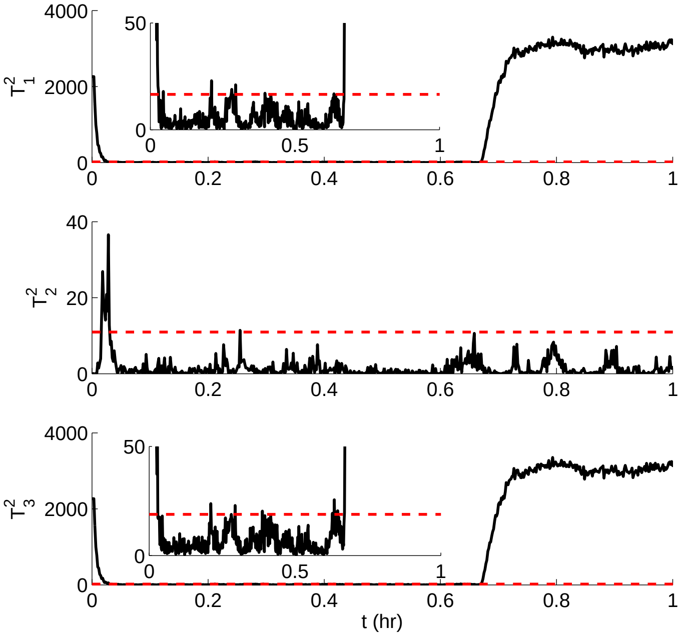


Figure 4.3: T^2 statistics for the CSTR under output feedback decoupling control with fault d_1 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

4.4 Controller enhanced FDI using model predictive control

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

4.4.1 MPC with isolability constraints

Model predictive control is a popular control strategy that is based on using a process model to optimize controller performance. MPC predicts the future evolution of the system from

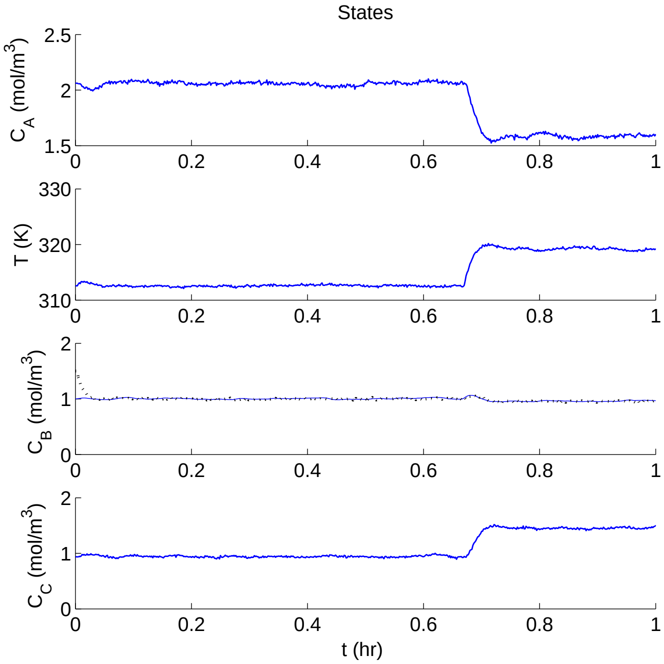


Figure 4.4: Plot of measured state values for the CSTR under output feedback decoupling control with fault d_2. C_B shows both actual (solid) and estimated (dotted) values.

an initial state at discrete sampling times for a given prediction horizon. These predictions are used to minimize a given cost function by solving a suitable optimization problem. MPC optimizes over the set of discrete manipulated input trajectories with a fixed sampling time and within a fixed prediction horizon (number of sampling time steps). The optimization problem is solved based on a cost function, accounting for input constraints, resulting in a set of optimal control inputs for the given horizon length. To present the proposed MPC formulation, we consider the nonlinear system of Eq.4.1 and assume that we can construct a nonlinear state feedback control law $u = p_{DC}(x, v)$, using the approaches presented in subsections 4.2.3 and 4.2.3, such that the resulting system

$$\dot{x} = f(x, p_{DC}(x, v), d) = \tilde{f}(x, v, d) \tag{4.28}$$

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

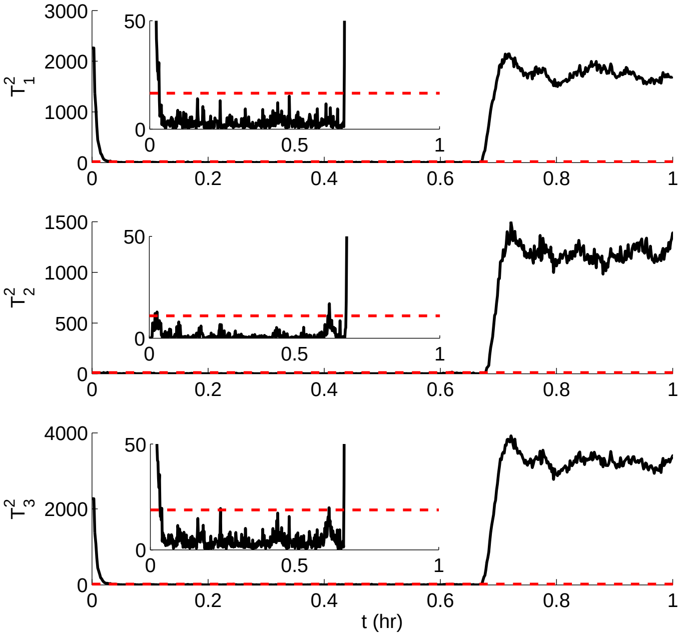


Figure 4.5: T^2 statistics for the CSTR under output feedback decoupling control with fault d_2 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

We consider the application of MPC to the system of Eq.4.28. It is important to note that the decoupling controller $u = p_{DC}(x, v)$ should be applied prior to the MPC optimization of the external input, v, and thus, the MPC optimization is performed independently from and does not affect the decoupling controller. In order to define a finite dimensional optimization problem, v is constrained to belong to the family of piece-wise constant functions $S(\Delta)$, with sampling period Δ. The MPC framework can now be used to compute the auxiliary input v_k. Specifically, we consider the following MPC formulation:

$$\begin{gathered}\min_{v_k \in S(\Delta)} \int_{t_k}^{t_k+T_h} (\tilde{x}^T(\tau)R\tilde{x}(\tau) + v_k^T(\tau)Qv_k(\tau))d\tau \\ \text{s.t.} \;\; \dot{\tilde{x}}(t) = \tilde{f}(\tilde{x}, v_k(t)), \;\; \tilde{x}(t_k) = x(t_k)\end{gathered} \tag{4.29}$$

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

We note the case of input/output linearizable nonlinear systems with two faults, (i.e.,

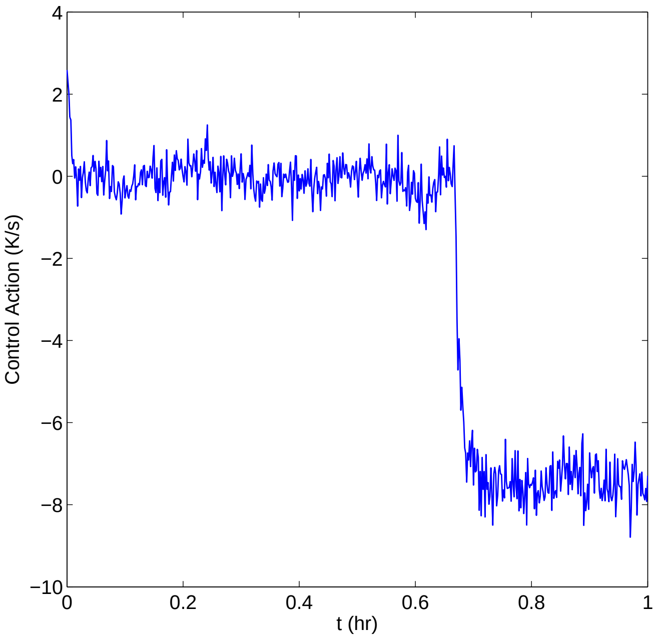


Figure 4.6: Manipulated input profile under output feedback decoupling control with fault d_2.

$d = [d_1\ d_2]^T$) implies that Eq.4.28 can be written as:

$$\begin{aligned} \dot{\zeta} &= \hat{f}(\zeta, v, d_1) \\ \dot{\eta} &= \hat{\psi}(\zeta, \eta) + d_2 \end{aligned} \tag{4.30}$$

where $x = \Theta(\zeta, \eta)$ and $\Theta(\zeta, \eta)$ is, in general, a nonlinear coordinate change, and $\hat{f}(\zeta, v, d_1)$, $\hat{\psi}(\zeta, \eta)$ are nonlinear vector functions of appropriate dimensions. The generalization to the case of having more than two faults is conceptually straightforward, yet notationally more involved. With the input/output linearizing control, Eq.4.29 can be reduced to

$$\begin{gathered} \min_{v_k \in S(\Delta)} \int_{t_k}^{t_k+T_h} (\tilde{\zeta}^T(\tau) R \tilde{\zeta}(\tau) + v_k^T(\tau) Q v_k(\tau)) d\tau \\ \text{s.t.} \quad \dot{\tilde{\zeta}}(t) = v_k(t), \quad \tilde{\zeta}(t_k) = \zeta(t_k) \end{gathered} \tag{4.31}$$

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

$$u(x(t), v_k) = \frac{v_k - L_f^r h(x(t))}{L_g L_f^{r-1} h(x(t))}. \tag{4.32}$$

Using the input/output linearizing controller to induce the necessary structure for fault isolation, MPC is used to compute the external controller in order to maintain stability and optimal performance. Specifically, the external input, v_k, is optimized with respect to the cost function as a set of discrete control inputs over a sequence of sampling times for a given horizon length. This results in a overall control input that is not optimal with respect to the total cost due to the input/output linearizing component, but is optimal with respect to the extra controller cost needed to stabilize and control the system at the steady state.

Remark 19 *It should be noted that the MPC formulation given in Eq.4.31 assumes that the decoupling controller,* $u = p_{DC}(x, v)$*, is applied continuously. In a practical situation, the decoupling controller will be implemented via sample and hold. Although this introduces error into closed-loop system dynamics, the closed-loop system has a near isolable structure as the hold time,* Δ*, goes to zero. This is sufficient for near decoupling due to the thresholds implemented for FDI which account for normal process variation (for further results on practical closed-loop stability subject to sample and hold control, see [41, 42].) Error introduced by sample-and-hold implementation of the decoupling control law leads, subsequently, to error in the MPC optimization due to plant-model mismatch. Again, this error becomes increasingly small as the hold time,* Δ*, goes to zero and can be adequately accounted for by the FDI thresholds used.*

Remark 20 *Referring to the incorporation of stability constraints in MPC, we note that in order to guarantee robust stability of the closed-loop system, MPC controllers generally include a set of stability constraints. This can be accomplished through Lyapunov-based MPC (LMPC) [41, 42, 51] or through terminal constraints in the cost function. Different schemes can be found in the literature, see [36] for a review on MPC stability results.*

4.4.2 Application to a CSTR example

The input/output linearizing control law with MPC as the external control input was applied to the chemical reactor example of Section 4.3. All parameters were the same as in Section 4.3 including sensor noise and process noise characteristics, faults sizes, fault incident times, system parameters, set points and fault detection time. However, in this simulation, full state feedback is used (i.e., C_A, C_B, C_C and T are measured). The sample and hold time for the MPC controller is the same as the discrete sampling time in Section 4.3, $\Delta t_s = 0.1\ min$, and the numerical integration time step is $\Delta t_i = 0.001\ min$. The controller cost function over which the system was optimized used weights of $R = [100\ 0;\ 0\ 1]$ and $Q = 10$. The horizon length was 10 time steps (1 min). Because of the inherently stable nature of the CSTR dynamics, more robust methods of stabilization were not used as penalizing the state was sufficient in this case.

In Figure 4.7, we see the state trajectories for the system under decoupling control with MPC as the external input to optimize system performance. A failure in d_1 with the same magnitude as in Section 4.3 is introduced at $t = 40\ min$. As before, we see that the decoupling control was effective as evidenced by the fact that C_C appears to be unaffected by the fault. Figure 4.8 shows the T^2 statistic for the closed-loop system. We note that fault detection occurred based on the statistic for the full state vector, T_3^2, at $t \approx 41\ min$. The system signature based on T_1^2 and T_2^2 matches the fault signature for d_1, $W = W^1 = [1\ 0]^T$.

The process simulated with a failure in d_2 and its T^2 statistics are shown in Figure 4.9. Again, we see that the closed-loop system signature based on the monitored subsystems matches what is expected based on the isolability graph (i.e., $W = W^2 = [1\ 1]^T$). In this plot, we again see temporary violations of the upper control limit, but none that are sustained for longer than the fault detection window, T_P.

In Figure 4.10, we see the control action requested by the feedback linearizing MPC. Based on the cost function used to perform MPC, the costs of two approaches (feedback linearizing control with proportional control and feedback linearizing MPC) were compared. Both controllers were implemented via state feedback. The process was initialized at $x(0) = [C_A(0) = 2.06 kmol/m^3\ T(0) = 312.6K\ C_B(0) = 1.00 kmol/m^3\ C_C = 1.44 kmol/m^3]^T$ and

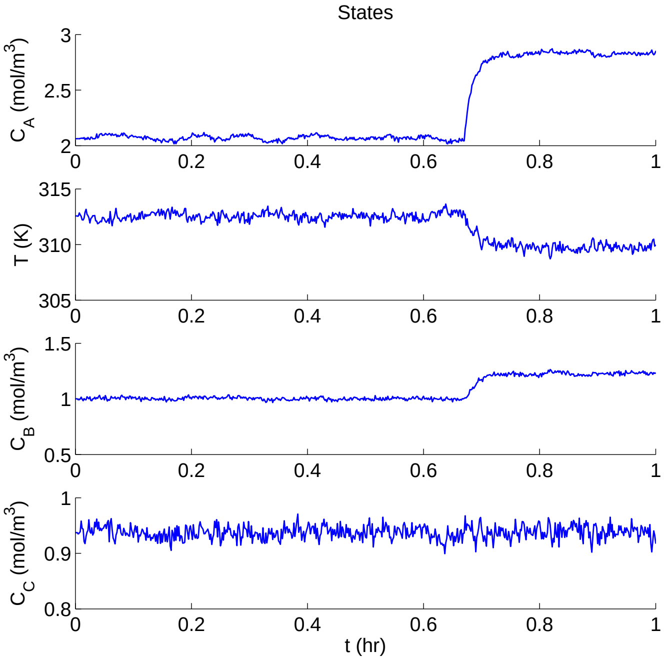


Figure 4.7: Plot of measured state values for the CSTR under feedback linearizing MPC with fault d_1.

was allowed to run for an hour without faults. The total costs of converging to the steady-state for the closed-loop system under feedback linearizing control with proportional control was 19.96 and for the closed-loop system under feedback linearizing MPC was 11.97; as expected, the use of MPC leads to improved overall performance.

4.5 Conclusions

Building upon our work on controller-enhanced FDI presented in Chapter 2, the present chapter has addressed two previously unresolved, practical problems. Specifically, it was demonstrated that the method of controller-enhanced FDI can be applied to processes where only output measurements are available under appropriate assumptions in the process system structure. We developed an approach where systems with incomplete state measurements can be dealt with using state estimator-based output feedback control. This approach maintains the necessary isolable structure in the closed-loop system in order to

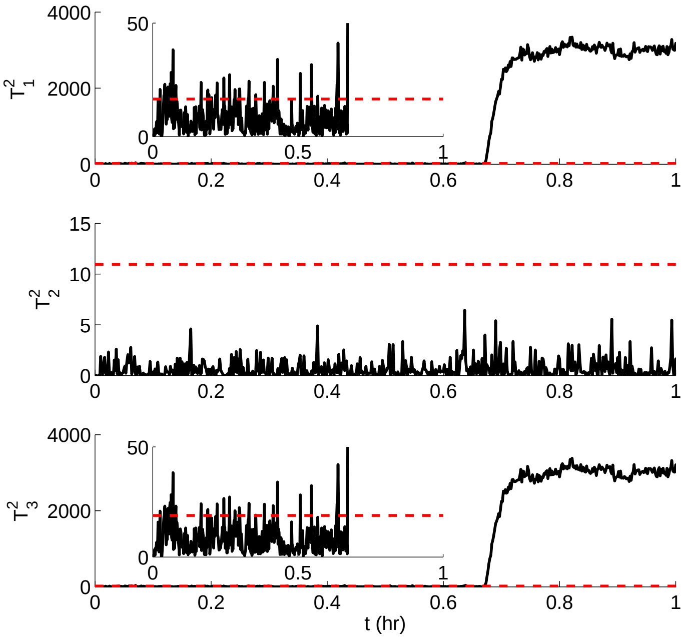


Figure 4.8: T^2 statistics for the CSTR under feedback linearizing MPC with fault d_1 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

perform controller-enhanced FDI. Additionally, we addressed the problem of controller-enhanced FDI in an optimal fashion within the framework of MPC. We proposed an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. The effectiveness of these methods was demonstrated through application to a nonlinear CSTR example.

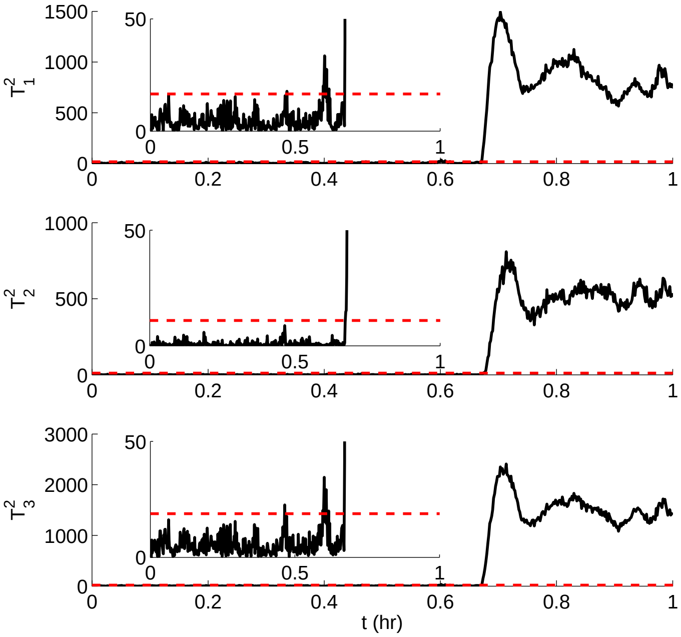


Figure 4.9: T^2 statistics for the CSTR under feedback linearizing MPC with fault d_2 for the subsystem X_1 (T_1^2), the subsystem X_2 (T_2^2) and the full system x (T_3^2).

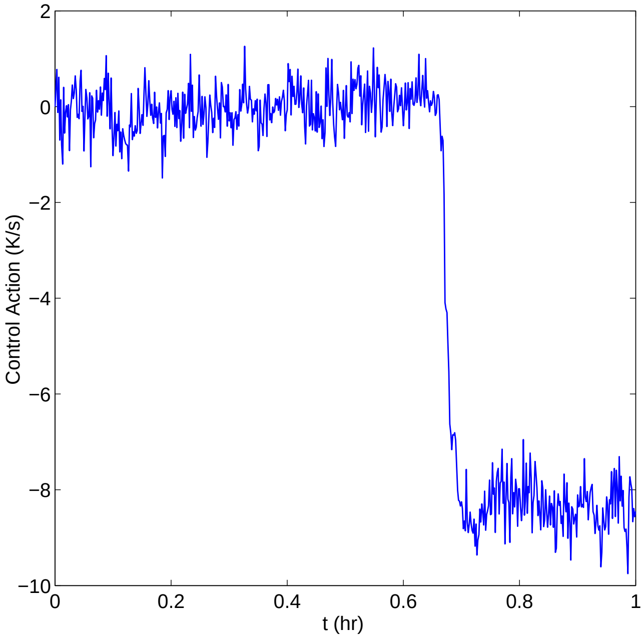


Figure 4.10: Manipulated input profile under feedback linearizing MPC with fault d_2.

Chapter 5

FDI using Asynchronous Measurements

5.1 Introduction

The goal of this chapter is to develop an FDI scheme that will allow fault tolerant control to take place when process measurements are available at asynchronous time instants. First, an FDI scheme that employs model-based techniques is proposed that allows for the isolation of faults. This scheme employs model-based FDI filters similar to those found in [47] in addition to observers that estimate the fault free evolution of asynchronously measured states during time intervals in which their measurements are not available. Specifically, the proposed FDI scheme provides detection and isolation of any fault that enters into the differential equation of only synchronously measured states, and grouping of faults that enter into the differential equation of any asynchronously measured state. For a fully coupled process system, fault detection occurs shortly after a fault takes place, and fault isolation, limited by the arrival of asynchronous measurements, occurs when asynchronous measurements become available. Once the FDI methodology has provided the system supervisor with a fault diagnosis, the supervisor takes appropriate action to seamlessly reconfigure the system to an alternative control configuration that will enforce the desired operation. Applications of the proposed asynchronous FDI and FTC framework to a polyethylene reactor simulation [37] are presented.

5.2 FDI using asynchronous measurements: Problem formulation and solution

5.2.1 Class of nonlinear systems

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

$$\begin{aligned} \dot{x}_s &= f_s(x_s, x_a, u, d) \\ \dot{x}_a &= f_a(x_s, x_a, u, d) \end{aligned} \tag{5.1}$$

where $x_s \in R^{n_s}$ denotes the set of state variables that are sampled synchronously, $x_a \in R^{n_a}$ denotes the set of state variables that are sampled asynchronously, $u \in R^{n_u}$ denotes the input and $d \in R^p$ is a model of the set of p possible faults. The faults are unknown and d_j, $j = 1 \dots p$, can take any value. The state of the full system is given by the vector

$$x = \begin{bmatrix} x_s \\ x_a \end{bmatrix} \in R^{n_s+n_a}$$

Using this definition for x, the system of Eq.5.1 can be written in the following equivalent compact form

$$\dot{x} = f(x, u, d) \tag{5.2}$$

We assume that f is a locally Lipschitz vector function and that $f(0, 0, 0) = 0$. This means that the origin is an equilibrium point for the fault-free system with $u(t) \equiv 0$. Moreover, we assume that the fault-free system ($d_i(t) \equiv 0$ for all t) has an asymptotically stable equilibrium at the origin $x = 0$ for a given feedback control function $h : R^{n_s+n_a} \rightarrow R^{n_u}$ which satisfies $h(0) = 0$.

5.2.2 Modeling of asynchronous measurements

The system of Eq.5.1 is controlled using both sampled synchronous and asynchronous measurements. We assume that each state $x_{s,i}$, $i = 1 \dots n_s$ is sampled continuously (i.e., at intervals of fixed size $\Delta > 0$ where Δ is a sufficiently small positive number). Each state $x_{a,i}$, $i = n_s + 1, \dots, n_s + n_a$, is sampled asynchronously and is only available at time instants $t_{k,i}$ where $t_{k,i}$ is a random increasing sequence of times. A controller design that takes advantage of the asynchronous measurements must take into account that it will have to operate without complete state information between asynchronous samples. This class of systems arises naturally in process control, where process variables such as temperature, flow, or concentration have to be measured. In such a case, temperature and flow measurements can be assumed to be available continuously. Concentration measurements, however, are available at an asynchronous sampling rate.

If there exists a non-zero probability that the system operates in open-loop for a period of time large enough for the state to leave the stability region or even diverge to infinity (i.e., finite escape time), it is not possible to provide guaranteed stability properties. In order to study the stability properties in a deterministic framework, we consider systems where there is a limit on the maximum number of consecutive sampling times in which measurements of $x_{a,i}$ are not available, i.e.

$$\max(t_{k+1,i} - t_{k,i}) \leq \Delta_M$$

This bound on the maximum period of time in which the loop is open has been also used in other works in the literature [66, 52, 46] and allows us to study deterministic notions of stability.

5.2.3 Asynchronous state observer

An observer that takes advantage of both synchronous and asynchronous measurements can be constructed to estimate the fault-free evolution of asynchronous states between consecutive measurements. The observer states are updated by setting the observer state equal to the measurement each time a new asynchronous measurement becomes available at $t_{k,i}$. The asynchronous state observer takes the form

$$\dot{\hat{x}}_a = f_a(x_s, \hat{x}_a, u, 0) \tag{5.3}$$

with $\hat{x}_{a,i}(t_{k,i}) = x_{a,i}(t_{k,i})$ for all $t_{k,i}$; that is, each time a new asynchronous measurement is received, the estimated states $\hat{x}_{a,i}$ with $i = n_s + 1, \ldots, n_s + n_a$ are reset to match the true process state. The information generated by this observer provides a fault-free estimate for each asynchronous state at any time t and allows for the design of non-linear control laws that utilize full state information. Using the estimated states, the control input applied to the system is given by $u = h(\hat{x})$ where $\hat{x} = [x_s^T \ \hat{x}_a^T]^T$.

This control input is defined for all times because it is based on both the synchronous states and the estimated asynchronous states. We assume that Δ_M is small enough to guarantee that the system in closed-loop with this control scheme is practically stable, see [66, 52, 46] for details on similar stability results.

5.2.4 Design of fault-detection and isolation filter

In this section we construct fault-detection and isolation (FDI) filters that will automatically identify the source of a failure in a timely manner. Utilizing both synchronous state measurements, $\hat{x}_i(t)$, $i = 1, \ldots, n_s$, and asynchronous state estimates, $\hat{x}_i(t)$, $i = n_s + 1, \ldots, n_s + n_a$, the following $n_s + n_a$ filters are defined [47]:

$$\dot{\tilde{x}}_i = f_i(\hat{x}_1 \ldots \tilde{x}_i \ldots \hat{x}_{n_s+n_a}, h(\hat{x}_1 \ldots \tilde{x}_i \ldots \hat{x}_{n_s+n_a}), 0) \tag{5.4}$$

where $\tilde{x}_i$ is the filter output for the i^{th} state in $\hat{x}$ and f_i is the i^{th} component of the vector function f. The FDI filters are only initialized at $t = 0$ such that $\tilde{x}(0) = \hat{x}(0)$. For each state in $\hat{x}$, the FDI residual can be defined as

$$r_i(t) = |\hat{x}_i(t) - \tilde{x}_i(t)|, \ i = 1, \ldots, n_s + n_a.$$

The synchronous residuals $r_i(t)$ with $i = 1, \dots, n_s$ are computed continuously because $\hat{x}_i(t)$ with $i = 1, \dots, n_s$ is known for all t. On the other hand, the asynchronous residuals $r_i(t)$, $i = n_s + 1, \dots, n_s + n_a$, are computed only at times $t_{k,i}$ when a new asynchronous measurement of $\hat{x}_i(t)$, $i = n_s + 1, \dots, n_s + n_a$, is received. These FDI filters operate by essentially predicting the fault-free evolution of each individual state, accounting for faults that enter the system when the predicted evolution of the state diverges from the measured evolution [47].

The dynamics of the synchronous states and asynchronous observers, $\hat{x}$, and the FDI filters, $\tilde{x}_i$, are identical to those of the system of Eq.5.1 when there are no disturbances or noise acting on the system. When the states are initialized as $\hat{x}(0) = \tilde{x}(0) = x(0)$ both the observer and filter states will track the true process states. For faults affecting the synchronous states, when a fault, d_j, occurs, only the residual corresponding to the affected state, r_i, will become nonzero. This is the case when the $f_s(x_s, x_a, h(x), d)$ vector field has a structure such that type I faults are isolable; see [47] for a precise determination of such a structure. In the case with faults affecting asynchronously measured states, at least one r_i will become non-zero when a fault occurs. However, faults that affect asynchronous states cause the asynchronous observer $\hat{x}_a$ to diverge from the true process state x_a between consecutive measurements, and any FDI filter states that are a function of $\hat{x}_a$ will no longer accurately track the corresponding true process states. When such a fault occurs more than one residual value may become nonzero.

Continuous measurements for asynchronous states are not available, thus the FDI filters in Eq.5.4 cannot always completely isolate all failures. We consider two classes of faults. Type I faults are faults that only affect states that are measured continuously; that is, d_j is a type I fault if

$$\frac{\partial f_i}{\partial d_j} = 0, \quad \forall i = n_s + 1, \dots, n_s + n_a.$$

Type II faults affect at least one asynchronous state; that is, d_j is a type II fault if there exists at least one $i = n_s + 1, \dots, n_s + n_a$ such that

$$\frac{\partial f_i}{\partial d_j} \neq 0.$$

The FDI filter will detect and isolate a type I fault d_j because the asynchronous state observers will track the asynchronous states accurately (i.e., the effect of the fault $d_j(t)$ on an asynchronous observer state is accounted for through the synchronous states, so $d_j(t)$ is accounted for in the observer of Eq.5.3 and hence the FDI filter). A type II fault enters the system in the differential equation of a state that is sampled asynchronously. The effect of type II faults cannot be accounted for by the observer $\hat{x}_i$, and such a fault will cause $\hat{x}_i$ to no longer track x_i and will eventually affect other coupled filter states as well. Strict isolation cannot take place for a type II fault. The FDI filter will detect and partially isolate disturbances in this case because the asynchronous state observers will diverge from the asynchronous states (i.e., the effect of the fault $d_j(t)$ on an asynchronous observer state is unmeasured and unaccounted for, thus the observer in Eq.5.3 does not track the disturbed state). In other words, if a type I fault occurs, then it can be detected and isolated. If a type II fault occurs, then this fault can be grouped to the subset of type II faults.

A fault is detected at time t_f if there exists a residual i such that $r_i(t_f) > r_{i,max}$, where $r_{i,max}$ is an appropriate threshold chosen to account for process and sensor noise. In order to isolate the possible source of the fault, it is necessary to wait until the residuals of all the asynchronous state filters are updated after t_f to determine if the fault is type I or type II. The residual of each asynchronous state filter $\tilde{x}_i$ is updated at time

$$t_i(t_f) = \min_k t_{k,i} |\; t_{k,i} > t_f.$$

If $r_i(t_i(t_f)) \leq r_{i,max}$ with $i = n_s + 1, \ldots, n_s + n_a$, then the fault occurred at time t_f is a type I fault and can be appropriately isolated. Otherwise, the fault belongs to the set of type II faults.

Consider that a synchronous residual r_i indicates a fault at time t_f. In this case the fault could have two possible causes, a type I or type II fault. In order to determine the true cause of this fault, one has to wait for the complete set of asynchronous measurements to arrive after t_f. When all the asynchronous measurements arrive and if all the residuals of the asynchronous states are smaller than the threshold, then the fault can be attributed to a type I fault. If any asynchronous measurement arrives and the corresponding residual indicates a fault, then the fault is type II. Note that when an asynchronous residual indicates a fault, we can also conclude that the fault is type II. When the fault is type II it has been detected, and it is possible to narrow the fault source down to the set of faults that enter the differential equations of asynchronous states.

When the fault can be attributed to a type I fault and it has been detected and isolated, then automated fault tolerant (FTC) control action can be initiated. For example, when a fault event that is due to a manipulated input failure (i.e., an actuator failure) is detected and isolated, fault tolerant control methods can be initiated [47]. In general an FTC switching rule may be employed that orchestrates the re-configuration of the control system in the event of control system failure. This rule determines which of the backup control loops can be activated, in the event that the main control loop fails, in order to preserve closed-loop stability. Owing to the limitations imposed by input constraints on the stability region for each control configuration, switching from a malfunctioning configuration to a well-functioning, but randomly selected, backup configuration will not preserve closed-loop stability if the state of the system, at the time of failure, lies outside the stability region of the chosen backup configuration. In this case, stabilization using this configuration requires more control action than is allowed by its constraints. This observation motivates the development of switching logic, which is to switch to the control configuration for which the closed-loop state resides within the stability region at the time of control failure. Without loss of generality, let the initial actuator configuration be $k(0) = 1$ and let t_d be the time when this failure has been isolated, then the switching rule given by

$$k(t) \ = \ j \ \forall \, t \geq t_d \, if \ \ x(t_d) \ \in \ \Omega(u_j^{max}) \tag{5.5}$$

for some $j \in \{2, 3, \cdots, N\}$ guarantees closed-loop asymptotic stability, where $\Omega(u_j^{max})$ is the stability region for the j^{th} control configuration. The implementation of the above switching law requires monitoring the closed-loop state trajectory with respect to the stability regions associated with the various fall-back configurations. The reader may refer to [23] for application of FTC to a polyethylene reactor with constraints on the manipulated inputs. In this work we consider a control law without constraints on the manipulated inputs, and the primary control configuration with a faulty actuator will be deactivated in favor of a fully functional fall-back control configuration where the fall-back configuration can guarantee global stability of the closed-loop system. This integrated FDI/FTC reconfiguration allows for seamless fault-recovery in the event of an actuator failure. Section 5.3 demonstrates integrated FDI/FTC for the polyethylene reactor.

5.3 Application to a polyethylene reactor

5.3.1 Process and measurement modeling

The proposed model-based asynchronous FDI and FTC method will be demonstrated using a model of an industrial gas phase polyethylene reactor. The feed to the reactor consists of ethylene ($[M_1]$), comonomer, hydrogen, inerts ($[In]$) and catalyst (Y). 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 have only mild effects on the reactor dynamics [37]. A mathematical model for this reactor has the following form [9]:

$$\begin{aligned}
\frac{d[In]}{dt} &= \frac{1}{V_g}(F_{In} - \frac{[In]}{[M_1]+[In]}b_t) \\
\frac{d[M_1]}{dt} &= \frac{1}{V_g}(F_{M_1} - \frac{[M_1]}{[M_1]+[In]}b_t - R_{M1}) + d_4 \\
\frac{dY_1}{dt} &= F_c a_c - k_{d_1}Y_1 - \frac{R_{M1}M_{W_1}Y_1}{B_w} + d_2 \\
\frac{dY_2}{dt} &= F_c a_c - k_{d_2}Y_2 - \frac{R_{M1}M_{W_1}Y_2}{B_w} + d_2 \\
\frac{dT}{dt} &= \frac{H_f + H_{g1} - H_{g0} - H_r - H_{pol}}{M_r C_{pr} + B_w C_{ppol}} + Q + d_1 \\
\frac{dT_{w_1}}{dt} &= \frac{F_w}{M_w}(T_{wi} - T_{w_1}) - \frac{UA}{M_w C_{pw}}(T_{w_1} - T_{g_1}) \\
\frac{dT_{g_1}}{dt} &= \frac{F_g}{M_g}(T - T_{g_1}) + \frac{UA}{M_g C_{pg}}(T_{w_1} - T_{g_1}) + d_3
\end{aligned} \tag{5.6}$$

where

$$\begin{aligned}
b_t &= V_p C_v \sqrt{([M_1]+[In])RRT - P_v} \\
R_{M1} &= [M_1]k_{p0}e^{\frac{-E_a}{R}(\frac{1}{T}-\frac{1}{T_f})}(Y_1+Y_2) \\
C_{pg} &= \frac{[M_1]}{[M_1]+[In]}C_{pm1} + \frac{[In]}{[M_1]+[In]}C_{pIn} \\
H_f &= (F_{M_1}C_{pm1} + F_{In}C_{pIn})(T_{feed} - T_f) \\
H_{g1} &= F_g(T_{g_1} - T_f)C_{pg} \\
H_{g0} &= (F_g + b_t)(T - T_f)C_{pg} \\
H_r &= H_{reac}M_{W_1}R_{M1} \\
H_{pol} &= C_{ppol}(T - T_f)R_{M1}M_{W_1}
\end{aligned} \tag{5.7}$$

The definitions for all the variables used in (5.6) and (5.7) are given in Table 5.1 and their values can be found in [9] (see also [23]). 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

$$\begin{array}{ll}
[In]_{ss} = 439.7\frac{mol}{m^3} & [M_1]_{ss} = 326.7\frac{mol}{m^3} \\
Y_{ss} = 7.67mol & T_{ss} = 356.2K \\
T_{g1ss} = 290.4K & T_{w1ss} = 294.4K.
\end{array}$$

where T, T_{g1} and T_{w1} are the temperatures of the reactor, recycle gas after cooling and exit-stream cooling water, respectively. In this example, we consider four possible faults, d_1, d_2, d_3, and d_4 which represent a heat jacket fault, catalyst deactivation, a change in the recycle gas flow rate, and ethylene consumption, respectively. The primary manipulated input for these studies is the heat input, Q, and the fall-back manipulated input is the feed temperature, T_{feed}. A fall-back manipulated input is required to maintain desired system performance in the presence of failure in the primary control configuration.

Simulations have been carried out for several scenarios to demonstrate the effectiveness of the proposed FDI scheme in detecting and isolating the four faults d_1, d_2, d_3, and d_4

in the presence of asynchronous measurements. The temperature measurements (T, T_{g_1}, T_{w_1}) are all assumed to be available synchronously, while the concentration measurements ($[In]$, $[M_1]$, Y) arrive at asynchronous intervals. In all the simulations, sensor measurement and process noise are 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. Table 5.2 provides the values of the noise parameters for each state of the system. The length of time between consecutive asynchronous measurements is generated randomly based on a Poisson process. The time when the system will receive the next asynchronous measurement of the i^{th} state is given by $t_{k+1,i} = t_{k,i} + \Delta_a$ where $\Delta_a = -ln(\xi)/W_a$ and $\xi \in (0, 1)$ is a random variable chosen from a uniform probability distribution and $W_a = 0.003\ s^{-1}$ is the mean rate of asynchronous sampling. There is an upper bound limiting the time between consecutive measurements such that $\Delta_a \leq \Delta_M = 1200\ s$. This value of Δ_M is small enough to provide practical closed-loop stability around the desired equilibrium point for the polyethylene reactor. An increasing sequence of measurement arrival times is generated independently for each asynchronously measured state.

5.3.2 Design of the asynchronous state observers

To perform FDI for the polyethylene reactor system we need to construct the asynchronous state observers of the form in Eq.5.3. The asynchronous state observers for this system

Table 5.1: 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_{pm1}	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_{W_1}	molecular weight of monomer
P_v	pressure downstream of bleed vent
Q	Heat added/removed by heating jacket
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_{g_1}, T_{w_1}	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

Table 5.2: Polyethylene reactor noise parameters

	σ_p	σ_m	ϕ
$[In]$	1E-4	5E-2	0
$[M_1]$	1E-4	5E-2	0.7
Y	1E-4	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

have the form:

$$\begin{aligned}
\frac{d[\hat{In}]}{dt} &= \frac{1}{V_g}(F_{In} - \frac{[\hat{In}]}{[\hat{M_1}]+[\hat{In}]}\hat{b}_t) \\
\frac{d[\hat{M_1}]}{dt} &= \frac{1}{V_g}(F_{M_1} - \frac{[\hat{M_1}]}{[\hat{M_1}]+[\hat{In}]}\hat{b}_t - \hat{R}_{M1}) \\
\frac{d\hat{Y}}{dt} &= F_c a_c - k_{d_1}\hat{Y} - \frac{\hat{R}_{M1} M_{W_1} Y}{B_w} \\
\hat{b}_t &= V_p C_v \sqrt{([\hat{M_1}]+[\hat{In}])RRT(t) - P_v} \qquad (5.8) \\
\hat{R}_{M1} &= [\hat{M_1}] k_{p0} e^{\frac{-E_a}{R}(\frac{1}{T(t)}-\frac{1}{T_f})}(\hat{Y}) \\
[\hat{In}](t_{k,[In]}) &= [In](t_{k,[In]}) \\
[\hat{M_1}](t_{k,[M_1]}) &= [M_1](t_{k,[M_1]}) \\
\hat{Y}(t_{k,Y}) &= Y(t_{k,Y})
\end{aligned}$$

where $[\hat{In}]$, $[\hat{M_1}]$, and $\hat{Y}$ are the asynchronous observer states. Each asynchronous observer state is initialized each time new measurement information becomes available at the times $t_{k,i}$. The observer states provide estimates for the asynchronous states between consecutive measurements allowing the computation of control actions and FDI residuals at each time.

5.3.3 Design of the state feedback controller

The control objective is to stabilize the system at the open-loop unstable steady state. A nonlinear Lyapunov-based feedback controller that enforces asymptotic stability of the closed-loop system is synthesized using the method proposed in [61] (see also [19]). This is a single input controller that utilizes synchronous measurements as well as observer states.The polyethylene reactor dynamics belong to the following class of non-linear systems:

$$\dot{x}(t) = f(x(t)) + g_1(x(t))u_1(t) + g_2(x(t))u_2(t) + w(x(t))d(t) \tag{5.9}$$

where

$$x(t) = \begin{bmatrix} [In] - [In]_{ss} \\ [M_1] - [M_1]_{ss} \\ Y - Y_{ss} \\ T - T_{ss} \\ T_{g1} - T_{g1ss} \\ T_{w1} - T_{w1ss} \end{bmatrix}$$

and

$$u_1(t) = Q,\ u_2(t) = T_{feed}.$$

Consider the quadratic control Lyapunov function $V(x) = x^T P x$ where

$$P = 1 \times 10^{-2}\ diag[0.5\ 0.5\ 0.5\ 1\ 0.005\ 0.005].$$

The values of the weighting matrix P are chosen to account for the different range of numerical values for each state. The following feedback laws [61] asymptotically stabilize the open-loop and possibly unstable steady-state of the nominal system (i.e., $d(t)) \equiv 0$)

$$h_i(x) = \begin{cases} \frac{L_fV + \sqrt{L_fV^2 + Lg_iV^4}}{-L_{g_i}V} & \text{if } L_{g_i}V \neq 0 \\ 0 & \text{if } L_{g_i}V = 0 \end{cases},\ i = 1, 2. \tag{5.10}$$

where L_fV and $L_{g_i}V$ denote the Lie derivatives of the scalar function V with respect to the vectors fields f and g_i respectively.

In the simulations, the primary control configuration is given by

$$u_1(t) = h_1(\hat{x}(t))$$

and the fall-back control configuration is given by

$$u_2(t) = h_2(\hat{x}(t))$$

where

$$\hat{x}(t) = \begin{bmatrix} [\hat{In}] - [In]_{ss} \\ [\hat{M_1}] - [M_1]_{ss} \\ \hat{Y} - Y_{ss} \\ T - T_{ss} \\ T_{g1} - T_{g1ss} \\ T_{w1} - T_{w1ss} \end{bmatrix}.$$

5.3.4 Design of FDI/FTC scheme

Fault detection and isolation for the system in closed-loop with the primary configuration is accomplished by generating FDI filters as in Eq.5.4., and for the polyethylene system the FDI filters take the following form:

$$\begin{aligned}
\frac{d[\tilde{In}]}{dt} &= \frac{1}{V_g}(F_{In} - \frac{[\tilde{In}]}{[\hat{M_1}] + [\tilde{In}]}\tilde{b}_t^{[In]}) \\
\frac{d[\tilde{M_1}]}{dt} &= \frac{1}{V_g}(F_{M_1} - \frac{[\tilde{M_1}]}{[\tilde{M_1}] + [\hat{In}]}\tilde{b}_t^{[M_1]} - \tilde{R}_{M1}^{[M_1]}) \\
\frac{d\tilde{Y}}{dt} &= F_c a_c - k_{d_1}\tilde{Y} - \frac{\tilde{R}_{M1}^{Y} M_{W_1}\tilde{Y}}{B_w} \\
\frac{d\tilde{T}}{dt} &= \frac{H_f + \tilde{H}_{g1}^T - \tilde{H}_{g0}^T - \tilde{H}_r^T - \tilde{H}_{pol}^T}{M_r C_{pr} + B_w C_{ppol}} + h_1(\hat{x}(t)) \\
\frac{d\tilde{T}_{w_1}}{dt} &= \frac{F_w}{M_w}(T_{wi} - \tilde{T}_{w_1}) - \frac{UA}{M_w C_{pw}}(\tilde{T}_{w_1} - T_{g_1}) \\
\frac{d\tilde{T}_{g_1}}{dt} &= \frac{F_g}{M_g}(T - \tilde{T}_{g_1}) + \frac{UA}{M_g \tilde{C}_{pg}}(T_{w_1} - \tilde{T}_{g_1})
\end{aligned} \tag{5.11}$$

where

$$\begin{aligned}
\tilde{b}_t^{[In]} &= V_p C_v \sqrt{([\hat{M}_1] + [\tilde{I}n])RRT - P_v} \\
\tilde{b}_t^{[M_1]} &= V_p C_v \sqrt{([\tilde{M}_1] + [\hat{I}n])RRT - P_v} \\
\tilde{b}_t^{[T]} &= V_p C_v \sqrt{([\hat{M}_1] + [\hat{I}n])RR\tilde{T} - P_v} \\
\tilde{R}_{M1}^{[M_1]} &= [\tilde{M}_1] k_{p0} e^{\frac{-E_a}{R}(\frac{1}{T} - \frac{1}{T_f})} (\hat{Y}) \\
\tilde{R}_{M1}^{Y} &= [\hat{M}_1] k_{p0} e^{\frac{-E_a}{R}(\frac{1}{T} - \frac{1}{T_f})} (\tilde{Y}) \\
\tilde{R}_{M1}^{T} &= [\hat{M}_1] k_{p0} e^{\frac{-E_a}{R}(\frac{1}{\tilde{T}} - \frac{1}{T_f})} (\hat{Y}) \\
\tilde{C}_{pg} &= \frac{[\hat{M}_1]}{[\hat{M}_1] + [\hat{I}n]} C_{pm1} + \frac{[\hat{I}n]}{[\hat{M}_1] + [\hat{I}n]} C_{pIn} \\
\tilde{H}_{g1}^{T} &= F_g (T_{g_1} - T_f) \tilde{C}_{pg} \\
\tilde{H}_{g0}^{T} &= (F_g + \tilde{b}_t^{T})(\tilde{T} - T_f) \tilde{C}_{pg} \\
\tilde{H}_{r}^{T} &= H_{reac} M_{W_1} \tilde{R}_{M1}^{T} \\
\tilde{H}_{pol}^{T} &= C_{ppol} (\tilde{T} - T_f) \tilde{R}_{M1}^{T} M_{W_1}
\end{aligned} \tag{5.12}$$

In addition, the FDI residuals take the following form:

$$\begin{aligned}
r_{[In]} &= |[\widehat{In}](t_k) - [\tilde{I}n](t_k)| \\
r_{[M_1]} &= |[\hat{M}_1](t_k) - [\tilde{I}n](t_k)| \\
r_Y &= |\hat{Y}(t_k) - \tilde{Y}(t_k)| \\
r_T &= |T - \tilde{T}| \\
r_{T_{g_1}} &= |T_{g_1} - \tilde{T}_{g_1}| \\
r_{T_{w_1}} &= |T_{w_1} - \tilde{T}_{w_1}|.
\end{aligned} \tag{5.13}$$

In the case with measurement and process noise, the residuals will be nonzero even without a failure event. This motivates the use of detection thresholds such that a fault is declared when a residual exceeds a specific threshold value, $r_{i,max}$ (note that a different threshold value can be used for each residual). This threshold value must be selected to avoid false alarms due to process and measurement noise, but it should also be sensitive enough (small enough) to detect faults in a timely manner so that efficient FTC action can be initiated.

The threshold values used for each residual in the numerical simulations can be seen as the dashed lines in Figures 5.3, 5.6, 5.9, and 5.12.

If the fault can be isolated to d_1 (i.e., r_T exceeds $r_{T,max}$ at $t = t_f$, while $r_i(t_i(t_f)) \leq r_{i,max}$ with $i = [In], [M_1], Y$), then one can invoke fault tolerant control methods to handle actuator failures by activation of a fall-back control configuration. In the simulation studies, it is assumed that a fall-back configuration, where the fall-back manipulated input $u_2 = T_{feed}$, is available. The control law of Eq.5.10 enforces stability when the control actuator is functioning properly, thus switching to the operational fall-back configuration will guarantee stability in the case of failure of the primary control configuration, $u_1 = Q$.

5.3.5 Closed-loop process simulation results

This section consists of four simulation studies, each examining one of the faults d_1, d_2, d_3, or d_4. The first simulation considers a fault, d_1, on the heating jacket which is the primary manipulated input. In this case the simulation includes fault tolerant control that automatically reconfigures the plant so that the fall-back manipulated input, $u_2 = T_{feed}$, is activated to maintain stability. Specifically, the supervisory control element will deactivate the primary control configuration, u_1 and activate the fall-back configuration u_2 when $r_T > r_{T,max}$ and $r_i(t_i(t_f)) \leq r_{i,max}$ with $i = [In], [M_1], Y$. This specific fault signature corresponds to a type I fault that can be isolated to d_1. The reader may refer to [23] to obtain more information on FTC and reconfiguration rules for a polyethylene reactor with constraints on the manipulated inputs that give rise to stability regions. This work does not consider constraints on the manipulated inputs, hence, the fall-back configuration can guarantee stability from anywhere in the state space because the closed-loop system under the fall-back control configuration is globally asymptotically stable. The remaining simulation studies explore faults that disturb the system, but do not arise from actuator failures. Since they are not caused by actuation component malfunctions these failures cannot be resolved simply by actuator reconfiguration. However, these simulations demonstrate quick detection and isolation in the presence of asynchronous measurements that enables the operator to take appropriate and focused action in a timely manner.

For the fault d_1 a simulation study has been carried out to demonstrate the proposed asynchronous fault detection and isolation and fault tolerant control method. The sequence of asynchronous measurements for this scenario is shown in Figure 5.1. This first simulation uses the primary control configuration in which Q is the manipulated input and has a fall-back configuration, in which T_{feed} is the manipulated input, available in case of a fault in d_1. A fault takes place where $d_1 = 1\ K/s$ at $t = 0.5\ hr$ representing a failure in the heating jacket, Q. At this time the synchronous states in Figure 5.2 all move away from the equilibrium point. Additionally, as asynchronous measurements become available, it is clear the asynchronous states also move away from the equilibrium point after the failure. It is unclear from the state information alone what caused this faulty behavior. However, if the FDI residuals in Figure 5.3 are examined, it is clear that the residual r_T that is associated with the manipulated input Q, violates its threshold at $t_f = 0.5003\ hr$. The fault is detected upon this threshold violation. However, isolation cannot take place until one new measurement for each asynchronous state becomes available. At $t = 0.5944\ hr$ all three required asynchronous measurements have arrived, and the asynchronous residuals remain below their thresholds, hence $r_i(t_i(t_f)) \leq r_{i,max}$ with $i = [In], [M_1], Y$. This signals that this is a type I fault that can be isolated to d_1. At this time, the system is reconfigured to the fall-back configuration where T_{feed} is the manipulated input, and the resulting state trajectory, shown as the dotted line in Figure 5.2, moves back to the desired operating point. The manipulated input for this scenario can be seen in Figure 5.4 where the solid line is the manipulated input without detection and reconfiguration, and the dotted line represents the input after FDI and reconfiguration.

The second simulation demonstrates the proposed asynchronous model-based fault-detection and isolation method when a type II fault occurs. The sequence of asynchronous measurements for this scenario are found in Figure 5.5. This simulation uses the primary control configuration in which Q is the manipulated input. A fault takes place where $d_2 = -0.001\ mol/s$ at $t = 0.5\ hr$ representing a catalyst deactivation event. After the failure, two synchronous states in move away from the equilibrium point (see [38] for additional figures). Additionally, as asynchronous measurements become available it can be seen that asynchronous states also move away from the equilibrium point after the failure.

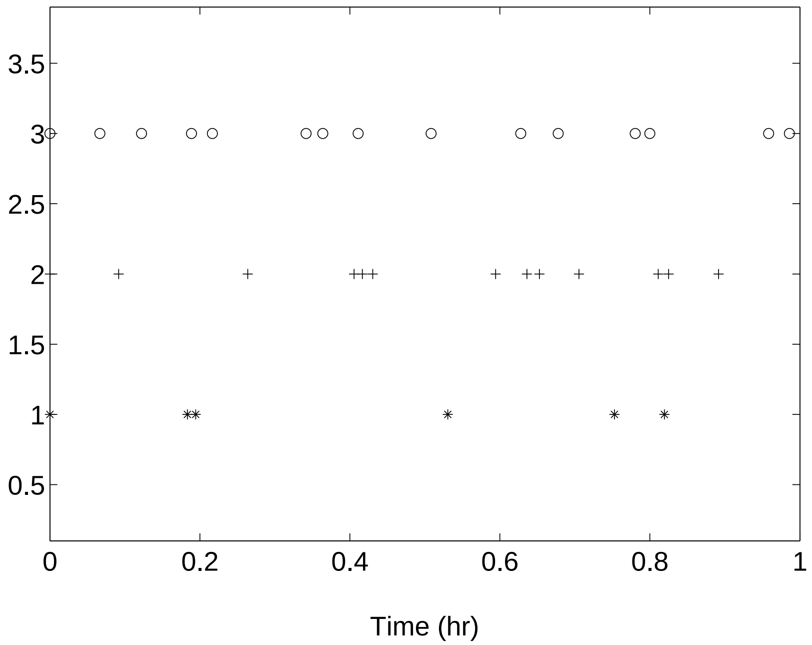


Figure 5.1: Asynchronous sampling times $t_{k,[In]}$ (star), $t_{k,[M_1]}$ (cross), and $t_{k,Y}$ (circle) with a fault d_1 at $t = 0.5$ hr.

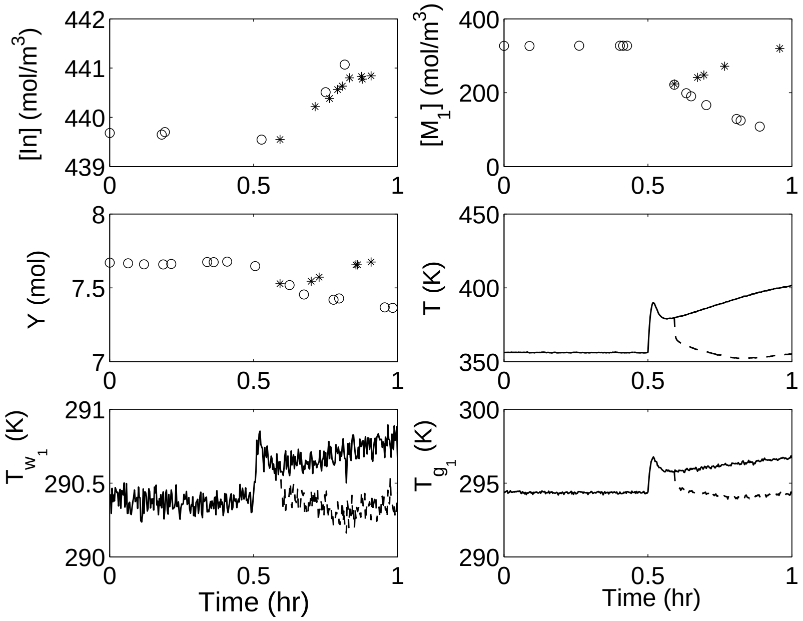


Figure 5.2: State trajectories of the closed-loop system without fault-tolerant control (circle/solid) and with appropriate fault detection and isolation and fault-tolerant control where the fall-back control configuration is activated (star/dotted) with a fault d_1 at $t = 0.5$ hr.

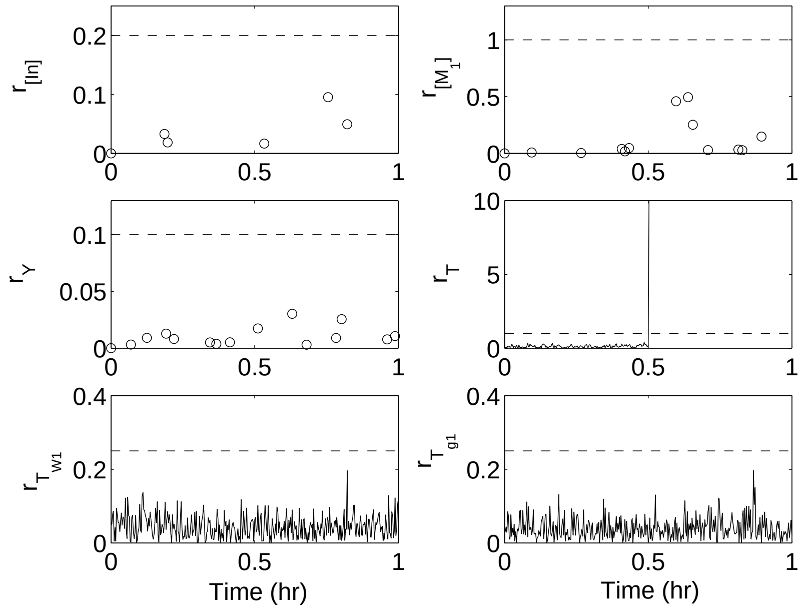


Figure 5.3: Fault-detection and isolation residuals for the closed-loop system with a fault d_1 at $t = 0.5$ hr. The fault is detected immediately, but isolation occurs at $t = 0.59$ hr when all three asynchronous states have reported a residual below their detection threshold. This signals a type I fault, and we can isolate the source of this fault as d_1.

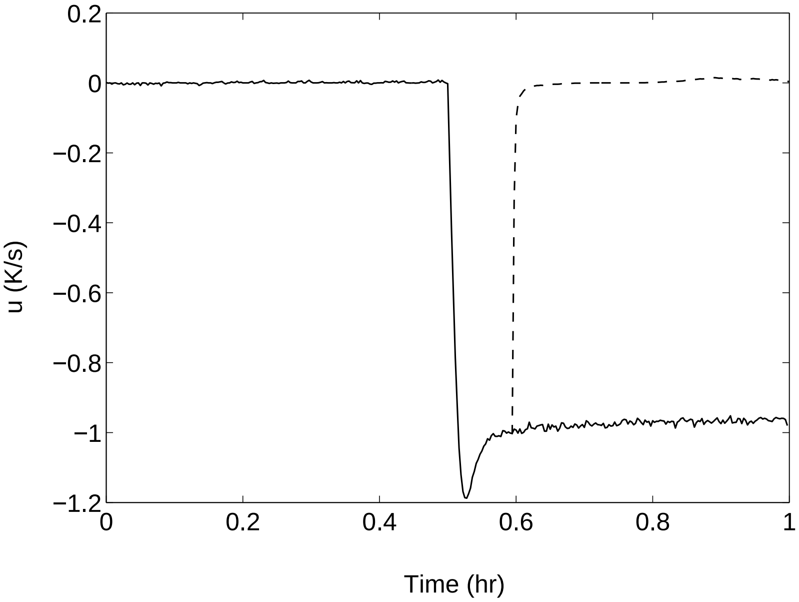


Figure 5.4: Manipulated input for the closed-loop system without fault-tolerant control (solid) and with appropriate fault-tolerant control where the fall-back control configuration is activated (dotted) with a fault d_1 at $t = 0.5$ hr.

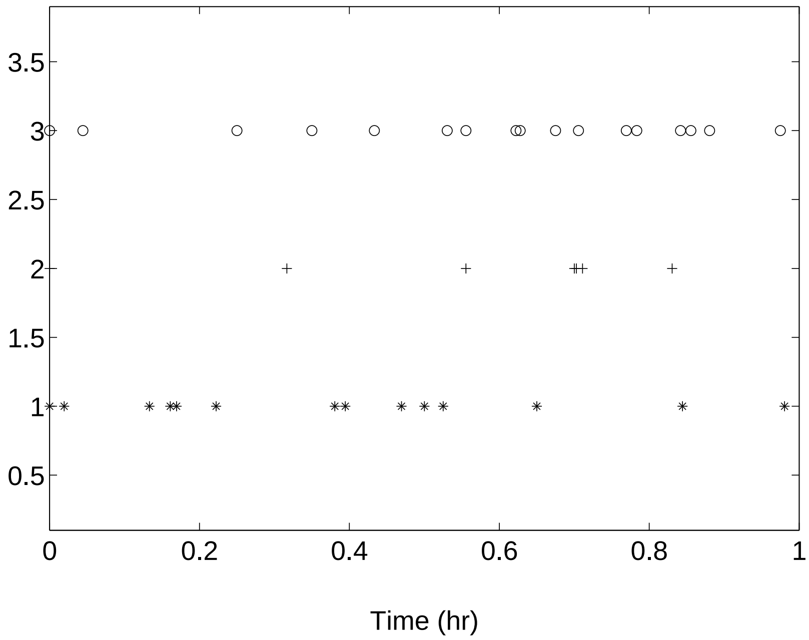


Figure 5.5: Asynchronous sampling times $t_{k,[In]}$ (star), $t_{k,[M_1]}$ (cross), and $t_{k,Y}$ (circle) with a fault d_2 at $t = 0.5\ hr$.

It is unclear from the state information alone what caused this faulty behavior. However, if the FDI residuals in Figure 5.6 generated by (5.13) are examined, it is clear that the residuals $r_{[M_1]}$, r_Y,and r_T violate their thresholds. The fault is detected upon the first threshold violation (r_Y at $t = 0.5333\ hr$). When the residual associated with Y exceeds the threshold this signals that the fault is type II and entered the system in the differential equation of an asynchronous state. When the fault is type II it cannot be isolated. However, such a fault can be grouped in the subset of faults that enter into the differential equation of an asynchronous state, (i.e., the group of type II faults, specifically, d_2 or d_4). At this time, the system operator can utilize the above partial isolation to examine the plant and determine the exact source of the failure. The manipulated input for this scenario can be seen in Figure 5.7.

The third simulation study examines FDI in the presence of a type I fault, d_3, representing a change in the recycle gas flow rate. The sequence of asynchronous measurements for this scenario are found in Figure 5.8. This simulation study uses the primary control configuration in which Q is the manipulate input, and a fault takes place where $d_3 = 300\ K/s$

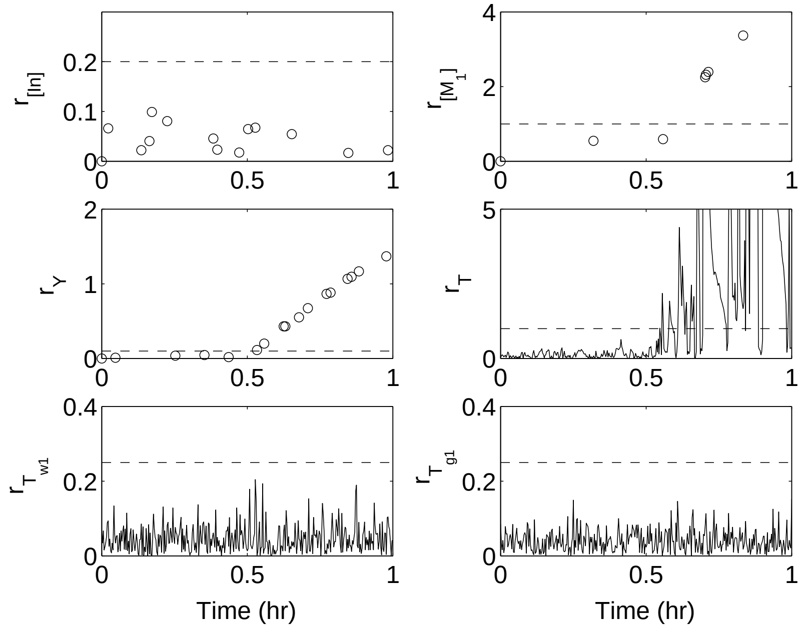


Figure 5.6: Fault-detection and isolation residuals for the closed-loop system with a fault d_2 at $t = 0.5$ hr. The fault is detected when residual for Y exceeds the threshold. Subsequently, T and $[M_1]$ exceed their thresholds. When any asynchronous residual violates the threshold this indicates that the fault is in the set of type II faults; d_2 or d_4.

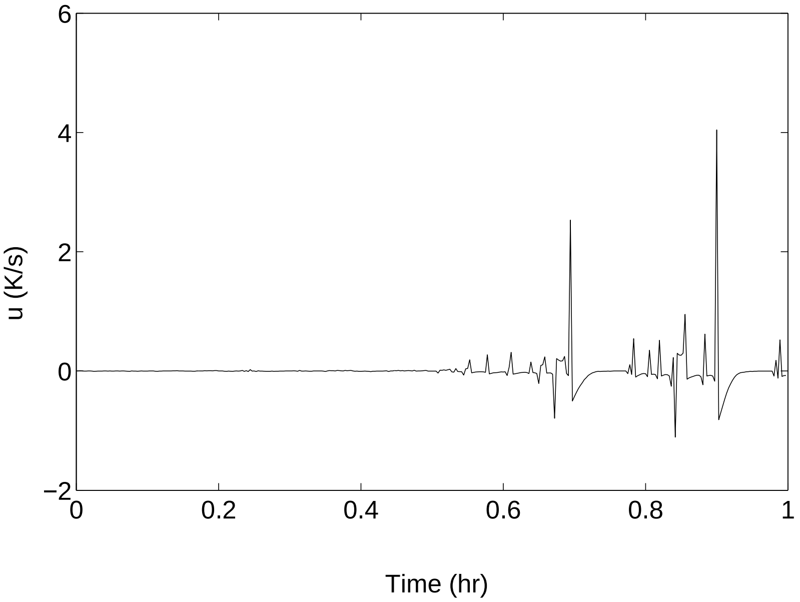


Figure 5.7: Manipulated input for the closed-loop system with a fault d_2 at $t = 0.5$ hr.

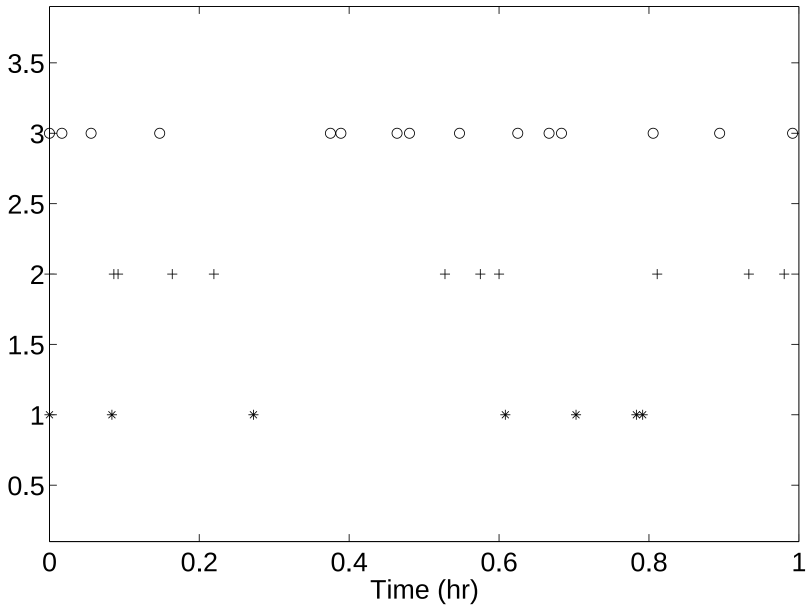


Figure 5.8: Asynchronous sampling times $t_{k,[In]}$ (star), $t_{k,[M_1]}$ (cross), and $t_{k,Y}$ (circle) with a fault d_3 at $t = 0.5$ hr.

at $t = 0.5$ hr. At this time the synchronous states all move away from the equilibrium point (see [38] for additional figures). Additionally, as asynchronous measurements become available it is observed that the asynchronous states also move away from the equilibrium point after the failure. It is unclear from the state information alone what caused this faulty behavior. However, if the FDI residuals in Figure 5.9 are examined, the residual associated with T_{g1}, violates its threshold at $t = 0.5003$ hr. The fault is detected upon this threshold violation. However, isolation cannot take place until one new measurement for each asynchronous state becomes available. At $t = 0.6086$ hr all three required asynchronous measurements have become available, and the residuals signal a type I fault, allowing the isolation of the fault to d_3. The manipulated input for this scenario can be seen in Figure 5.10.

The final simulation study demonstrates the proposed asynchronous model-based fault-detection and isolation method when a type II fault occurs. The sequence of asynchronous measurements for this scenario are found in Figure 5.11 This simulation uses the primary control configuration in which Q is the manipulated input. A fault takes place where $d_4 = -0.2$ mol/s at $t = 0.5$ hr representing unexpected monomer consumption. After

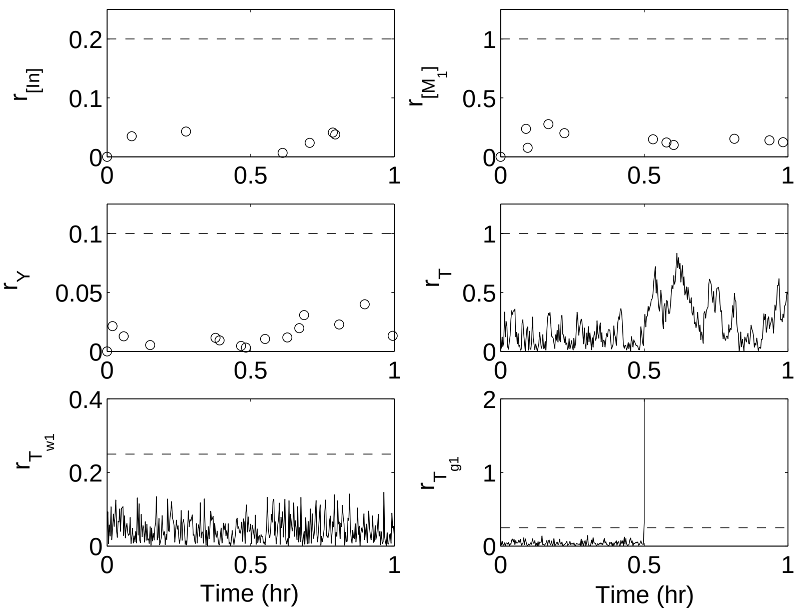


Figure 5.9: Fault-detection and isolation residuals for the closed-loop system with a fault d_3 at $t = 0.5\ hr$. A fault is detected immediately when residual for T_{g1} exceeds the threshold. Subsequently, none of the asynchronous residuals exceed their thresholds, indicating that the fault source can be isolated as d_3.

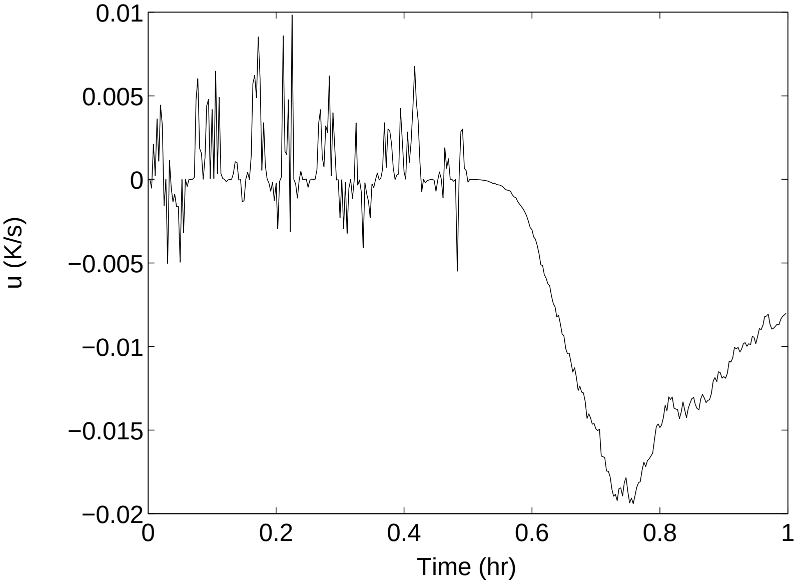


Figure 5.10: Manipulated input for the closed-loop system with a fault d_3 at $t = 0.5\ hr$.

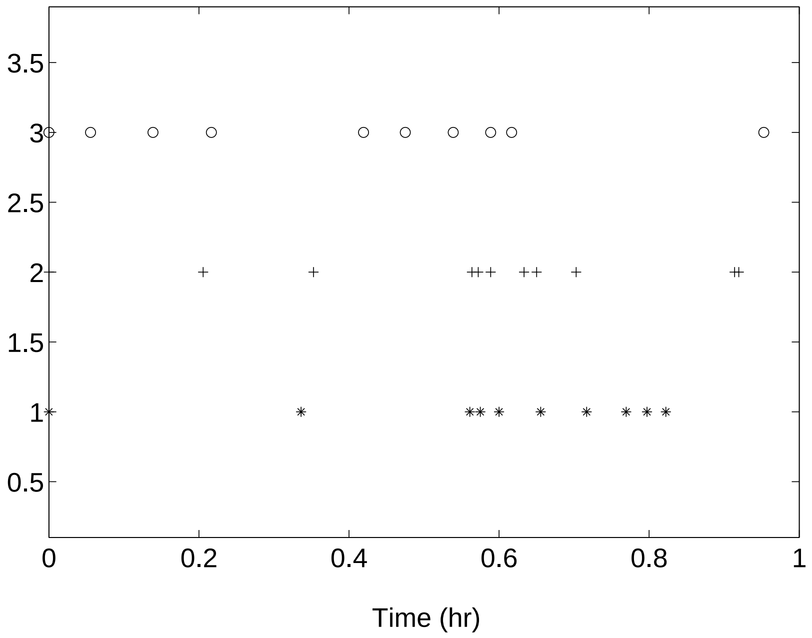


Figure 5.11: Asynchronous sampling times $t_{k,[In]}$ (star), $t_{k,[M_1]}$ (cross), and $t_{k,Y}$ (circle) with a fault d_4 at $t = 0.5\ hr$.

the failure the synchronous states diverge from their desired values (see [38] for additional figures). Additionally, as asynchronous measurements become available it can be seen that asynchronous states also diverge after the failure. It is unclear from the state information alone what caused this faulty behavior. However, if the FDI residuals in Figure 5.12 are examined, the residuals $r_{[In]}$, $r_{[M_1]}$, r_T,and $r_{T_{g1}}$ violate their thresholds. The fault is detected upon the first threshold violation ($r_{[M_1]}$ at $t = .05667\ hr$). When the residual $r_{[M_1]}$ exceeds the threshold this signals that a type II fault has occurred. When a type II fault occurs it cannot be isolated. As in the second simulation, such a fault can be grouped in the subset of type II faults d_2 or d_4. At this time, the system operator can utilize the partial isolation to examine the plant and determine the exact source of the failure. The manipulated input for this scenario can be seen in Figure 5.13.

5.4 Conclusions

This chapter addressed the application of fault detection and isolation and fault-tolerant control in a polyethylene reactor system where several process measurements were not

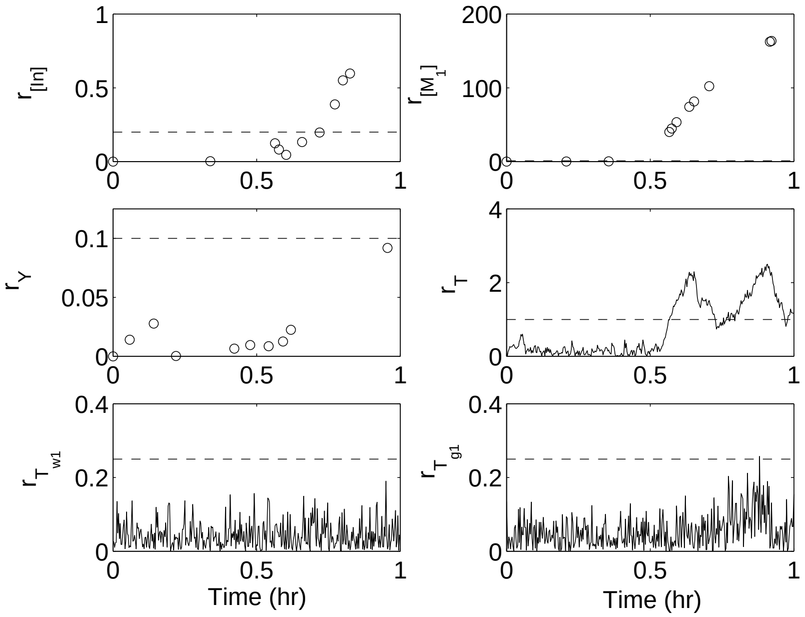


Figure 5.12: Fault-detection and isolation residuals for the closed-loop system with a fault d_4 at $t = 0.5$ hr. The fault is detected when residual for $[M_1]$ exceeds the threshold. Subsequently, T and $[In]$ exceed their thresholds. When any asynchronous residual violates the threshold this indicates the fault is in the set of type II faults; d_2 or d_4.

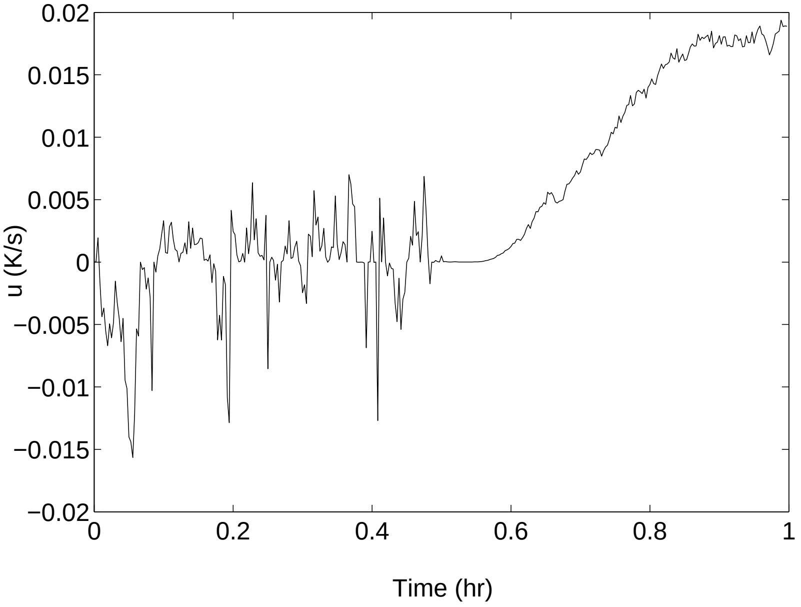


Figure 5.13: Manipulated input for the closed-loop system with a fault d_4 at $t = 0.5$ hr.

available synchronously. First, an FDI scheme that employs model-based techniques was introduced that allowed for the isolation of faults. This scheme employed model-based FDI filters in addition to observers that estimate the fault-free evolution of asynchronously measured states during times when they are unmeasured. Specifically, the proposed FDI scheme provided detection and isolation for a type I fault where the fault entered into the differential equation of only synchronously measured states, and grouping of type II faults where the fault entered into the differential equation of any asynchronously measured state. The detection occurred shortly after a fault took place, and the isolation, limited by the arrival of asynchronous measurements, occurred once all of the asynchronous measurements became available. Once the FDI methodology provided the system supervisor with a fault diagnosis, the supervisor took appropriate action to seamlessly reconfigure the polyethylene reactor system to an alternative control configuration that enforced the desired operation.

Chapter 6

Networked Monitoring and Fault Tolerant Control

6.1 Introduction

This chapter focuses on the monitoring and reconfiguration of a two-tier networked control system for a chemical process in the presence of control actuator faults. Specifically, a chemical process system is considered and is controlled by a two-tier networked control system integrating a local control system using continuous sensing/actuation with a networked control system using asynchronous sensing/actuation. To deal with control actuator faults that may occur in the closed-loop system, a networked fault detection and isolation (FDI) and fault-tolerant control (FTC) system is designed which detects and isolates actuator faults and determines how to reconfigure the two-tier networked control system to handle the actuator faults. The FDI/FTC system uses continuous measurements of process variables like temperatures and asynchronous measurements of variables like concentrations. The method is demonstrated using a reactor-separator process consisting of two continuous stirred tank reactors and a flash tank separator with recycle stream.

6.2 Preliminaries

6.2.1 Class of nonlinear systems

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

$$\begin{aligned}\dot{x}_s &= f_s(x_s, x_a, u_s, u_a, d) \\ \dot{x}_a &= f_a(x_s, x_a, u_s, u_a, d),\end{aligned} \tag{6.1}$$

where $x_s \in R^{n_s}$ denotes the set of state variables that are sampled synchronously, $x_a \in R^{n_a}$ denotes the set of state variables that can only be sampled asynchronously, $u_s \in \ R^{m_s}$ denotes the inputs computed from only synchronous measurements, $u_a \in \ R^{m_a}$ denotes inputs computed from synchronous and asynchronous measurements and $d \in R^p$ is a model of the set of p possible faults. The faults are unknown and d_j, $j = 1, \ldots, p$, can take any value. The states of the full system are given by the vector

$$x = \begin{bmatrix} x_s \\ x_a \end{bmatrix} \in R^{n_s+n_a}.$$

Using this definition for x, the system of Eq.6.1 can be written in the following equivalent compact form

$$\dot{x} = f(x, u_s, u_a, d). \tag{6.2}$$

We assume that f is a locally Lipschitz vector function and that $f(0, 0, 0, 0) = 0$. This means that the origin is an equilibrium point for the fault-free system ($d \equiv 0$ for all t) with $u_s \equiv 0$ and $u_a \equiv 0$. Moreover, we assume that there exists an output feedback controller $u_s(x_s(t))$ that renders the origin $x = 0$ of the fault-free system asymptotically stable with $u_a \equiv 0$.

6.2.2 Modeling of asynchronous measurements

The system of Eq.6.1 is controlled using both sampled synchronous and asynchronous measurements. We assume that each state in x_s is sampled continuously (i.e., at intervals of fixed size $\Delta > 0$ where Δ is a sufficiently small positive number). Each state in x_a is sampled asynchronously and is only available at some time instants t_k where $\{t_{k\geq 0}\}$ is a random increasing sequence of times. A controller design that takes advantage of the asynchronous measurements must take into account that it will have to operate in open loop when new asynchronous measurements are unavailable. This class of systems arises naturally in process control, where process variables such as temperature, flow, or concentration have to be measured. In such a case, temperature and flow measurements can be assumed to be available continuously. Concentration measurements, however, are available at an asynchronous sampling rate. This model is also of interest for systems controlled through a hybrid communication network in which wireless sensors are used to add redundancy to existing working control loops (which use point-to-point wired communication links and continuous measurements), because wireless communication is often subject to data losses due to interference.

Since there exists a non-zero probability that the system operates in open-loop for a period of time large enough for the state to leave the stability region or even diverge to infinity (i.e., finite escape time), it is not possible to provide guaranteed stability properties. In order to maintain reasonable stability and system performance, we consider systems where there is a limit on the maximum length of times in which measurements of x_a are not available, i.e.

$$\max(t_{k+1} - t_k) \leq \Delta_M.$$

This bound on the maximum period of time in which the loop is open has been also used in other works in the literature [66, 52, 46]. Note that this bound is also required for fault detection and isolation systems which take advantage of asynchronous measurements to detect faults within a reasonable time frame.

6.2.3 Two-tier control architecture

The continuous measurements $x_s(t)$ can be used to design a continuous output-feedback controller $u_s(x_s(t))$ to stabilize the system. The control system based only on the continuous measurements $x_s(t)$ is called the local control system. This controller is able to stabilize the system, however, it does not profit from the extra information provided by $x_a(t)$.

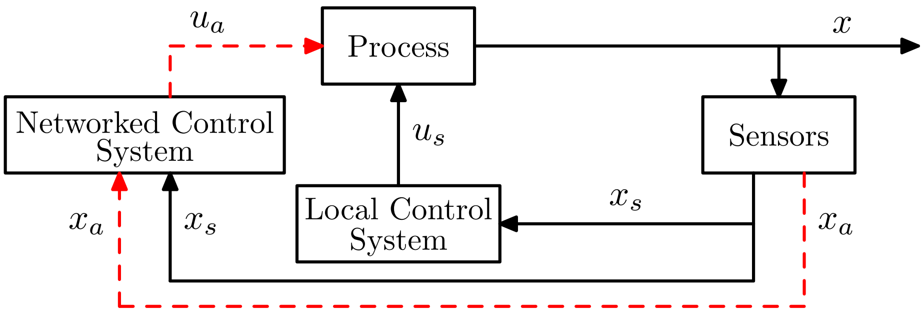


Figure 6.1: Two-tier control strategy (solid lines denote dedicated point-to-point, wired communication links and continuous sensing/actuation; dashed lines denote networked (wired/wireless) communication and/or asynchronous sampling/actuation).

The main objective of the two-tier control architecture [32, 33] is to improve the performance of the closed-loop system using the information provided by $x_a(t)$ while guaranteeing that the stability properties of the local control system $u_s(x_s(t))$ are maintained. This is done by defining a controller (networked control system) based on the full state measurements x obtained from both the synchronous (x_s) and asynchronous (x_a) measurements at time steps t_k. In the two-tier control architecture, the networked control system decides the trajectory of $u_a(t)$ between successive samples, i.e., for $t \in [t_k, t_{k+1})$ and the local control system decides $u_s(t)$ using the continuously available measurements. Figure 6.1 shows a schematic of the two-tier control architecture.

In order to take advantage of the model of the system and the asynchronous state measurements, model predictive control (MPC) is used to decide u_a. The main idea is the following: at each time instant t_k that a new state measurement $x(t_k)$ is obtained, an open-loop finite horizon optimal control problem is solved and an optimal input trajectory is obtained. This input trajectory is implemented until a new set of measurements arrives at time t_{k+1}. If the time between two consecutive measurements is longer than the prediction horizon, u_a is set to zero until a new set of measurements arrives and the optimal control problem is solved again. In order to define a finite dimensional optimization problem, u_a is constrained to belong to the family of piece-wise constant functions with sampling period Δ_c, $S(\Delta_c)$. In order to guarantee that the resulting closed-loop system is stable, a Lyapunov-based MPC (LMPC) which includes a contractive constraint is designed. The contractive constraint of the networked control system LMPC design is based on the local control system $u_s(x_s(t))$. The LMPC optimization problem is defined as follows:

$$
\begin{aligned}
\min_{u_a \in S(\Delta_c)} & \int_0^{N\Delta} L(x^e(\tau), u_s(x_s^e(\tau)), u_a(\tau)) d\tau \\
& \dot{x}^e(\tau) = f(x^e(\tau), u_s(x_s^e(\tau)), u_a(\tau), 0) \\
& \dot{x}^l(\tau) = f(x^l(\tau), u_s(x_s^l(\tau)), 0, 0) \\
& x^l(0) = x^e(0) = x(t_k) \\
& V(x^e(\tau)) \leq V(x^l(\tau)) \ \forall \ \tau \in [0, N\Delta_c]
\end{aligned}
\tag{6.3}
$$

where $x(t_k)$ is the state obtained from both the measurements of x_s and x_a, $x^e = [x_s^{eT} \ x_a^{eT}]^T$ is the predicted trajectory of the nominal system for the input trajectory computed by the LMPC, $x^l = [x_s^{lT} \ x_a^{lT}]^T$ is the predicted trajectory of the nominal system for the input trajectory $u_a(\tau) \equiv 0$ for all $\tau \in [0, N\Delta_C]$, $L(x, u_s, u_a)$ is a positive definite function of the state and the inputs that defines the cost, and N is the prediction horizon. This optimization problem does not depend on the uncertainty and assures that the system in closed-loop with the networked control system maintains the stability properties of the local control system. The optimal solution to this optimization problem is denoted $u_a^*(\tau|t_k)$. This signal is defined for all $\tau > 0$ with $u_a^*(\tau|t_k) = 0$ for all $\tau > N\Delta_C$.

The control inputs of the two-tier control architecture based on the above LMPC of Eq.6.3 corresponding to the measurements provided by $x(t)$ are defined as follows:

$$
\begin{aligned}
& u_s^L(t|x(t)) = u_s(x_s(t)), \ \forall t \\
& u_a^L(t|x(t)) = u_a^*(t - t_k|t_k), \ \forall t \in [t_k, t_{k+1})
\end{aligned}
\tag{6.4}
$$

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

6.2.4 FDI using asynchronous measurements

An observer that takes advantage of both synchronous and asynchronous measurements can be constructed to estimate the fault-free evolution of asynchronous states between consecutive measurements. The observer states are updated by setting the observer state equal to the measurement each time a new asynchronous measurement becomes available at t_k. The asynchronous state observer takes the form

$$\dot{\hat{x}}_a \quad = \quad f_a(x_s, \hat{x}_a, u_s^L(\hat{x}), u_a^L(\hat{x}), 0) \tag{6.5}$$

where $\hat{x} = [x_s^T \hat{x}_a^T]^T$ and, with a little abuse of notation, we have dropped the time index of the two-tier controller functions and denote $u_s^L(t|x(t)), u_a^L(t|x(t))$ with $u_s^L(x), u_a^L(x)$ respectively in order to simplify the FDI definitions. Each time a new asynchronous measurement is received, the estimated states $\hat{x}_a$ are reset to match the true process state; that is, $\hat{x}_a(t_k) = x_a(t_k)$ for all t_k. The information generated by this observer provides a fault-free estimate for each asynchronous state at any time t and allows for the design of non-linear FDI filters that utilize full state information.

Utilizing both synchronous and asynchronous state measurements, the following $n_s + n_a$ filters are defined [47]:

$$\dot{\tilde{x}}_i \quad = \quad f_i(\tilde{X}_i, u_s^L(\tilde{X}_i), u_a^L(\tilde{X}_i), 0), \forall i = 1, \ldots, n_s + n_a \tag{6.6}$$

where $\tilde{x}_i$ is the filter output for the i^{th} state, f_i is the i^{th} component of the vector function f and $\tilde{X}_i$ is a state trajectory obtained from the synchronous measurements, the estimated and the corresponding filter output as follows:

$$\tilde{X}_i = [\hat{x}_1 \ldots \tilde{x}_i \ldots \hat{x}_{n_s+n_a}]^T.$$

Note that in Eq.6.6, it is necessary to compute a separate LMPC optimization problem for each state in which the LMPC control input (i.e., u_a^L) appears in the state's dynamic equation. The FDI filters are only initialized at $t = 0$ such that $\tilde{x}(0) = \hat{x}(0)$. For each state in $\hat{x}$, the FDI residual can be defined as [47, 38]:

$$r_i(t) = |\hat{x}_i(t) - \tilde{x}_i(t)|, \; i = 1 \ldots, n_s + n_a.$$

The synchronous residuals $r_i(t)$ with $i = 1, \ldots, n_s$ are computed continuously because $\hat{x}_i(t)$ with $i = 1, \ldots, n_s$ is known for all t. On the other hand, the asynchronous residuals $r_i(t)$, $i = n_s + 1, \ldots, n_s + n_a$, are computed only at times t_k when a new asynchronous measurement of $\hat{x}_i(t)$, $i = n_s + 1, \ldots, n_s + n_a$, is received. Under no-fault conditions ($d \equiv 0$) with $\hat{x}(0) = \tilde{x}(0) = x(0)$, both the observer and filter states will track the true process states. In this case the dynamics of the synchronous states and asynchronous observers, $\hat{x}$, and the FDI filters, $\tilde{x}$, are identical and $r_i(t) = 0; i = 1, \ldots, n_s$.

When a fault d_j occurs, one or more residuals will be affected. For faults affecting the synchronous states, only the residual corresponding to the affected state, r_i, will become nonzero. This is the case when the $f_s(x_s, x_a, u_s, u_a, d)$ vector field has a structure such that faults are isolable (see [47]). The following formal definition describes the class of faults d_j that are type I:

$$\frac{\partial f_i}{\partial d_j} = 0, \forall i = n_s + 1, \ldots, n_s + n_a.$$

On the other hand, faults that affect asynchronous states cause the asynchronous observer $\hat{x}_a$ to diverge from the true process state x_a between consecutive measurements. Any FDI filter states that are a function of $\hat{x}_a$ will no longer accurately track the corresponding true process states. When such a fault occurs, more than one residual value may become nonzero. These faults are labeled type II if they affect at least one asynchronous state; that is, d_j is a type II fault if there exists at least one $i = n_s + 1, \ldots, n_s + n_a$ such that

$$\frac{\partial f_i}{\partial d_j} \neq 0.$$

Because the effects of a type I fault are measured synchronously, only the filters of the states directly affected by the fault deviate from normal. Other filters continue to track because the effect of the fault is known and accounted for. This allows for both fault detection and isolation in the case of a type I fault. However, a type II fault affects states that are measured asynchronously, and thus the effects of the fault are not immediately known and cannot be accounted for by the observer $\hat{x}_i$. The error introduced into $\hat{x}_i$ will then propagate into the FDI filters. In this scenario, multiple residuals may exceed their fault detection threshold, making it impossible to isolate the specific fault. Although it is

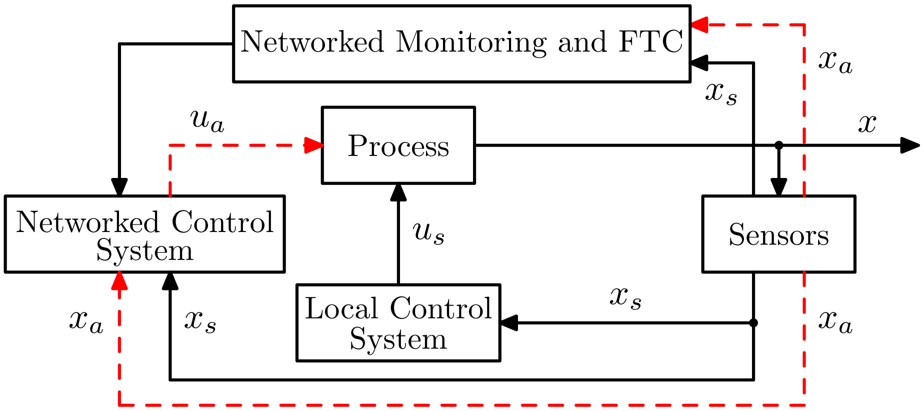


Figure 6.2: Two-tier control strategy with integrated networked monitoring and fault-tolerant control (solid lines denote dedicated point-to-point, wired communication links and continuous sensing/actuation; dashed lines denote networked (wired/wireless) communication and/or asynchronous sampling/actuation).

impossible to isolate the specific fault, we are still able to group the fault as type II.

A fault is detected at time t_f, if there exists a residual i such that $r_i(t_f) > r_{i,max}$, where $r_{i,max}$ is an appropriate threshold chosen to account for process and sensor noise. In order to isolate the source of the fault, it is necessary to wait until the residuals of all the asynchronous state filters are updated at time $t_k > t_f$ to determine if the fault is type I or type II. If $r_i(t_k) \leq r_{i,max}$ with $i = n_s + 1, \ldots, n_s + n_a$, then the fault occurred at time t_f is a type I fault and can be appropriately isolated. Otherwise, the fault belongs to the set of type II faults.

When the fault can be attributed to a type I fault and it has been detected and isolated, then automated fault tolerant control action can be initiated. In general an FTC switching rule may be employed that orchestrates the re-configuration of the control system in the event of control system failure. This rule determines which of the backup control loops can be activated, in the event that the main control loop fails, in order to preserve closed-loop stability. In this work, we look at the closed-loop system under the two-tier control architecture where, upon detection and isolation of actuator faults, the networked control system can be reconfigured to maintain stability of the plant. The structure of this integrated system is shown graphically in Figure 6.2. By updating the model used in the networked control system, it becomes possible to preserve system stability in the presence

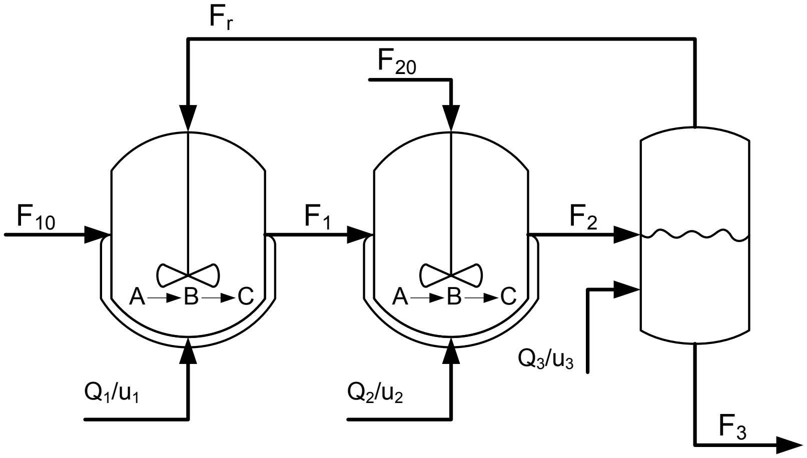


Figure 6.3: Two CSTRs and a flash tank with recycle stream.

of an actuator fault.

6.3 Application to a reactor-separator process

6.3.1 Process description and modeling

The process considered in this study is a three vessel, reactor-separator system consisting of two continuous stirred tank reactors (CSTRs) and a flash tank separator (see Figure 6.3). A feed stream to the first CSTR contains the reactant, A, which is converted into the desired product, B. Species A can also react into an undesired side-product, C. The solvent does not react and is labeled as D. The effluent of the first CSTR along with additional fresh feed makes up the inlet to the second CSTR. The reactions $A \to B$ and $B \to C$ (referred to as 1 and 2, respectively) take place in the two CSTRs in series before the effluent from CSTR 2 is fed to a flash tank. The overhead vapor from the flash tank is condensed and recycled to the first CSTR, and the bottom product stream is removed. All three vessels are assumed to have static holdup. The dynamic equations describing the behavior of the system, obtained through material and energy balances under standard modeling assumptions, are given

Table 6.1: Process Variables

C_{A1}, C_{A2}, C_{A3}	concentration of A in vessels 1, 2, 3
C_{B1}, C_{B2}, C_{B3}	concentration of B in vessels 1, 2, 3
C_{C1}, C_{C2}, C_{C3}	concentration of C in vessels 1, 2, 3
C_{Ar}, C_{Br}, C_{Cr}	concentration of A, B, C in the recycle
T_1, T_2, T_3	temperatures in vessels 1, 2, 3
T_{10}, T_{20}	feed stream temp. to vessels 1, 2
F_1, F_2, F_3	effluent flow rate from vessels 1, 2, 3
F_{10}, F_{20}	feed stream flow rate to vessels 1, 2
F_r	recycle flow rate
V_1, V_2, V_3	volume of vessels 1, 2, 3
u_1, u_2, u_3, u_4	manipulated inputs
E_1, E_2	activation energy for reactions 1, 2
k_1, k_2	pre-exponential values for reactions 1, 2
ΔH_1, ΔH_2	heats of reaction for reactions 1, 2
H_{vap}	heat of vaporization
α_A, α_B, α_C, α_D	relative volatilities of A, B, C, D
MW_A, MW_B, MW_C	molecular weights of A, B, C
C_p, R	heat capacity and gas constant

below.

$$
\begin{aligned}
\frac{dT_1}{dt} &= \frac{F_{10}}{V_1}(T_{10}-T_1)+\frac{F_r}{V_1}(T_3-T_1)+u_1+\frac{-\Delta H_1}{\rho Cp}k_1e^{\frac{-E_1}{RT_1}}C_{A1}+\frac{-\Delta H_2}{\rho Cp}k_2e^{\frac{-E_2}{RT_1}}C_{A1}\\
\frac{dC_{A1}}{dt} &= \frac{F_{10}}{V_1}(C_{A10}-C_{A1})+\frac{F_r}{V_1}(C_{Ar}-C_{A1})-k_1e^{\frac{-E_1}{RT_1}}C_{A1}-k_2e^{\frac{-E_2}{RT_1}}C_{A1}\\
\frac{dC_{B1}}{dt} &= \frac{-F_{10}}{V_1}C_{B1}+\frac{F_r}{V_1}(C_{Br}-C_{B1})+k_1e^{\frac{-E_1}{RT_1}}C_{A1}\\
\frac{dC_{C1}}{dt} &= \frac{-F_{10}}{V_1}C_{C1}+\frac{F_r}{V_1}(C_{Cr}-C_{C1})+k_2e^{\frac{-E_2}{RT_1}}C_{A1}\\
\frac{dT_2}{dt} &= \frac{F_1}{V_2}(T_1-T_2)+\frac{F_{20}}{V_2}(T_{20}-T_2)+u_2+\frac{-\Delta H_1}{\rho Cp}k_1e^{\frac{-E_1}{RT_2}}C_{A2}+\frac{-\Delta H_2}{\rho Cp}k_2e^{\frac{-E_2}{RT_2}}C_{A2}\\
\frac{dC_{A2}}{dt} &= \frac{F_1}{V_2}(C_{A1}-C_{A2})+\frac{F_{20}}{V_2}(C_{A20}-C_{A2})-k_1e^{\frac{-E_1}{RT_2}}C_{A2}-k_2e^{\frac{-E_2}{RT_2}}C_{A2}+u_4\\
\frac{dC_{B2}}{dt} &= \frac{F_1}{V_2}(C_{B1}-C_{B2})-\frac{F_{20}}{V_2}C_{B2}+k_1e^{\frac{-E_1}{RT_2}}C_{A2}\\
\frac{dC_{C2}}{dt} &= \frac{F_1}{V_2}(C_{C1}-C_{C2})-\frac{F_{20}}{V_2}C_{C2}+k_2e^{\frac{-E_2}{RT_2}}C_{A2}\\
\frac{dT_3}{dt} &= \frac{F_2}{V_3}(T_2-T_3)-\frac{H_{vap}F_r}{\rho CpV_3}+u_3\\
\frac{dC_{A3}}{dt} &= \frac{F_2}{V_3}(C_{A2}-C_{A3})-\frac{F_r}{V_3}(C_{Ar}-C_{A3})\\
\frac{dC_{B3}}{dt} &= \frac{F_2}{V_3}(C_{B2}-C_{B3})-\frac{F_r}{V_3}(C_{Br}-C_{B3})\\
\frac{dC_{C3}}{dt} &= \frac{F_2}{V_3}(C_{C2}-C_{C3})-\frac{F_r}{V_3}(C_{Cr}-C_{C3}).
\end{aligned}
\tag{6.7}
$$

The definitions for the variables used in Eq.6.7 can be found in Table 6.1, with the parameter values given in Table 6.2. Each of the tanks has an external heat input.

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

$$\begin{aligned}&C_{Ar} = \frac{\alpha_A C_{A3}}{K},\ C_{Br} = \frac{\alpha_B C_{B3}}{K},\ C_{Cr} = \frac{\alpha_C C_{C3}}{K}\\ &K = \alpha_A C_{A3}\frac{MW_A}{\rho} + \alpha_B C_{B3}\frac{MW_B}{\rho} + \alpha_C C_{C3}\frac{MW_C}{\rho} + \alpha_D x_D \rho\end{aligned} \tag{6.8}$$

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

The system of Eq.6.7 is modeled with sensor measurement noise and gaussian process noise. The sensor measurement noise is generated using a zero-mean normal distribution with standard deviation 10^{-1} for the temperature states and 10^{-2} for the 9 concentration states. Noise is applied to each measurement of the synchronous states and to the continuous measurements of the temperatures with a frequency of $\Delta_m = 0.01hr$. The process noise is generated similarly, with a zero-mean normal distribution and with the same standard deviation values. Process noise is added to the right-hand side of the ODEs in the system of Eq.6.7 and changes with a frequency of $\Delta_w = 0.01hr$.

In all three vessels, the heat input is a manipulated variable for controlling the reactors at the appropriate operating temperature. The system has 1 unstable and 2 stable steady states. The operating set point is the unstable steady state,

$$T_1 = 369.5K, \quad T_2 = 435.3K, \quad T_3 = 435.3K. \tag{6.9}$$

The local control system consists of the three heat input actuators (i.e., u_1, u_2 and u_3) oper-

Table 6.2: Parameter Values

$T_{10} = 300$, $T_{20} = 300$	K
$F_{10} = 5$, $F_{20} = 5$, $F_r = 1.9$	$\frac{m^3}{hr}$
$V_1 = 1.0$, $V_2 = 0.5$, $V_3 = 1.0$	m^3
$E_1 = 5E4$, $E_2 = 5.5E4$	$\frac{kJ}{kmol}$
$k_1 = 3E6$, $k_2 = 3E6$	$\frac{1}{hr}$
$\Delta H_1 = -5E4$, $\Delta H_2 = -5.3 \cdot 10^4$	$\frac{kJ}{kmol}$
$H_{vap} = 5$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$
$R = 8.314$	$\frac{kJ}{kmolK}$
$\rho = 1000$	$\frac{kg}{m^3}$
$\alpha_A = 2$, $\alpha_B = 1$, $\alpha_C = 1.5$, $\alpha_D = 3$	unitless
$MW_A = 50$, $MW_B = 50$, $MW_C = 50$	$\frac{kg}{kmol}$

ating under identical PI control laws with the proportional gain $K_p = 100$ and the integral time $\tau_I = 1$. In addition, there is a networked control system governing the inlet concentration of A in the fresh feed into the second CSTR (i.e., u_4). The networked control system is an LMPC controller of the form given in Eq.6.3. The cost function L is quadratic and takes the form $L = x^T Q x + R u_a^2$, where $Q = diag[10\ 10^3\ 10^3\ 10^3\ 10\ 10^3\ 10^3\ 10^3\ 10\ 10^3\ 10^3\ 10^3]$ and $R = 1$. The horizon for the optimization problem is $N = 5$ with $\Delta_C = 0.01hr$.

All of the concentration measurements in the system are obtained asynchronously at time instants t_k with an average frequency of $W = 10$ measurements per hour. The measurement times are modeled as a Poisson process with the time between measurements $\Delta_a = \min\{-log(\xi/W), \Delta_M\}$ where ξ is a uniformly distributed random number between 1 and 0 and $\Delta_M = 0.05hr$. At each asynchronous measurement time, the LMPC optimization problem was solved again and implemented over the length of the horizon or until a new set of measurements becomes available.

In order to perform FDI for the reactor-separator system we construct the asynchronous state observers of the form in Eq.6.5, where $\hat{C}_{Ai}$, $\hat{C}_{Bi}$, and $\hat{C}_{Ci}$, $i = 1, 2, 3$ are the asynchronous observer states. Each observer state is reset to its actual value each time a new set of asynchronous measurements becomes available at time t_k. The observer states provide estimates for the concentration states between measurements allowing the computation of

FDI filter residuals.

Fault detection and isolation for the system in closed-loop with the primary configuration is accomplished by generating FDI filters as in Eq.6.6. In addition, the FDI residuals take the following form:

$$\begin{aligned} r_{T_i} &= |T_i(t) - \tilde{T}_i(t)|, \quad i = 1,2,3 \\ r_{C_{Ai}} &= |\hat{C}_{Ai}(t_k) - \tilde{C}_{Ai}(t_k)|, \quad i = 1,2,3 \\ r_{C_{Bi}} &= |\hat{C}_{Bi}(t_k) - \tilde{C}_{Bi}(t_k)|, \quad i = 1,2,3 \\ r_{C_{Ci}} &= |\hat{C}_{Ci}(t_k) - \tilde{C}_{Ci}(t_k)|, \quad i = 1,2,3 \end{aligned} \tag{6.10}$$

Due to sensor measurement and process noise, the residuals will be nonzero even without a fault. This necessitates the use of fault detection thresholds so that a fault is declared only when a residual exceeds a specific threshold value, $r_{i,max}$. This threshold value is chosen to avoid false alarms due to process and sensor measurement noise, but should still be sensitive enough to detect faults in a timely manner so that effective fault-tolerant control can be performed. The threshold values used for each residual in the numerical simulations can be seen as the dashed lines in Figures 6.6 and 6.10.

6.3.2 Simulation results

With the present reactor-separator model that takes advantage of asynchronous concentration measurements in an augmented sensor network to both perform FDI and two-tier control, in the presence of an actuator fault, it is possible to reconfigure the networked control system to stabilize the system and maintain control. In this simulation example, we consider a failure in the heat input actuator to vessel 2. Once the fault has been detected (when $r_{T_2} > r_{T_2,max}$ at $t = t_f$) and isolated (when the other residuals are found to be less than their respective thresholds at $t_k > t_f$), it is possible to update the LMPC control law to reflect the failed actuator. If the time between asynchronous measurements is short enough and the horizon long enough, the system can be stabilized and continue to operate under the fall-back control configuration. In addition to this example, we first simulate the system with a failure in the heat input actuator to vessel 2 without updating the LMPC model in the networked control system, in order to show that without performing FDI and FTC, the system becomes unstable.

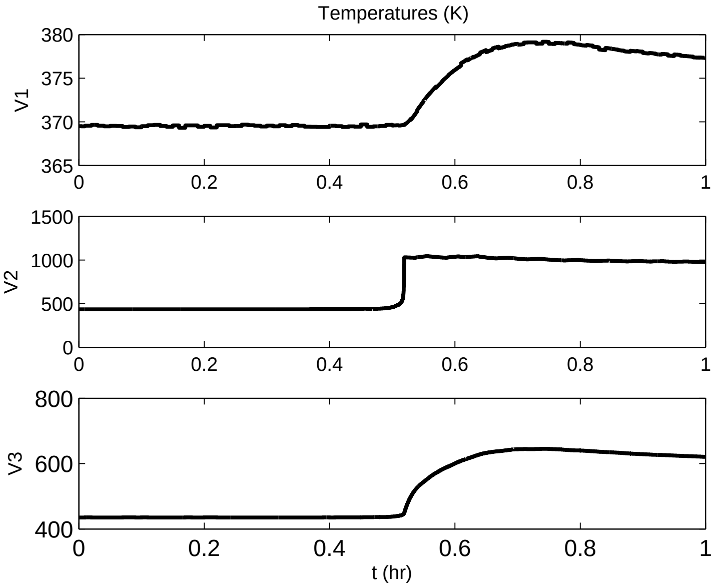


Figure 6.4: Temperature trajectories in each vessel with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$ and FTC. No fault tolerant control implemented.

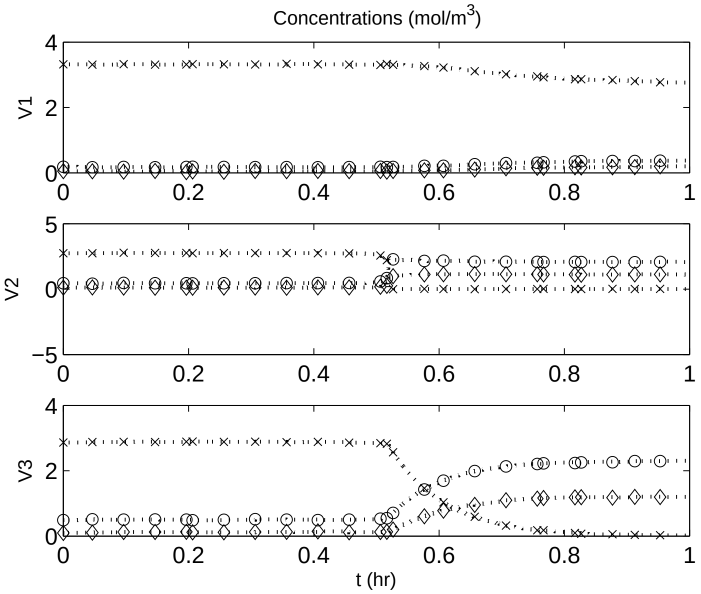


Figure 6.5: Asynchronous concentration measurements (C_A=x, C_B =o, C_C = $\diamond$) in each vessel (V1, V2, V3) with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$. Dotted lines represent observer trajectories. No fault tolerant control implemented.

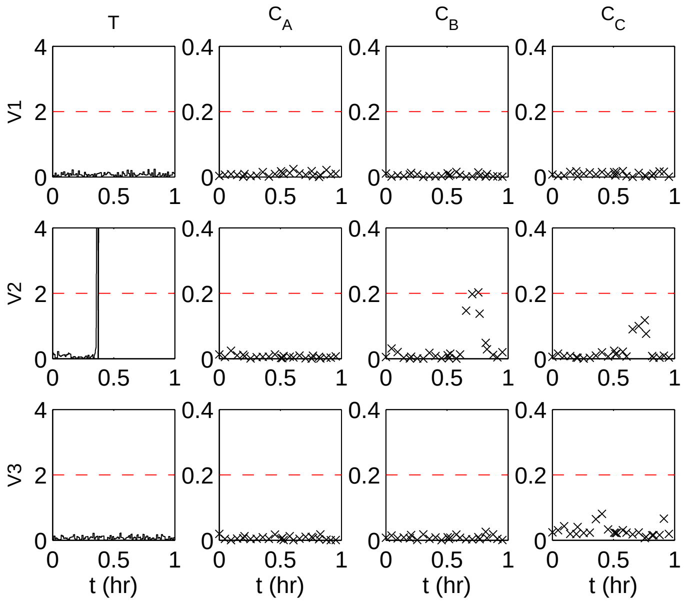


Figure 6.6: FDI filter residuals for temperature (T) and concentration(C_A, C_B, C_C) in each vessel (V1, V2, V3) with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$. Fault is detected at $t = 0.36hr$ and isolated at $t_k = 0.41hr$, but no fault tolerant control is implemented.

The system of Eq.6.7, along with the asynchronous state observers and FDI filters, is simulated in closed-loop operation with the three local PI controllers and the LMPC controller for 1 hour. The system is subject to both sensor measurement and process noise as well as a control actuator failure in the heat input to vessel 2, introduced at time $t = 0.3hr$ ($u_2 = 0$ for all $t > 0.3hr$). Figures 6.4 and 6.5 show the state trajectories for the system when the networked control system is not modified, resulting in an unstable system. The residuals in Figure 6.6 shows that the fault is detected at $t = 0.36hr$ when $r_{T_2} > r_{T_2,max}$. It can then be isolated when the next asynchronous measurement is received at $t_k = 0.41hr$. We see that without updating the networked control system (i.e., the model used in the LMPC optimization problem), the process becomes unstable and cannot be controlled by the networked control system due to plant model mismatch. The manipulated input profile for the networked control system is shown in Figure 6.7.

In contrast to the above scenario, we run the same simulation again, but upon isolation of the fault we reconfigure the networked control system to reflect the failed actuator. In this case, despite the failed actuator, the networked control system is able to stabilize

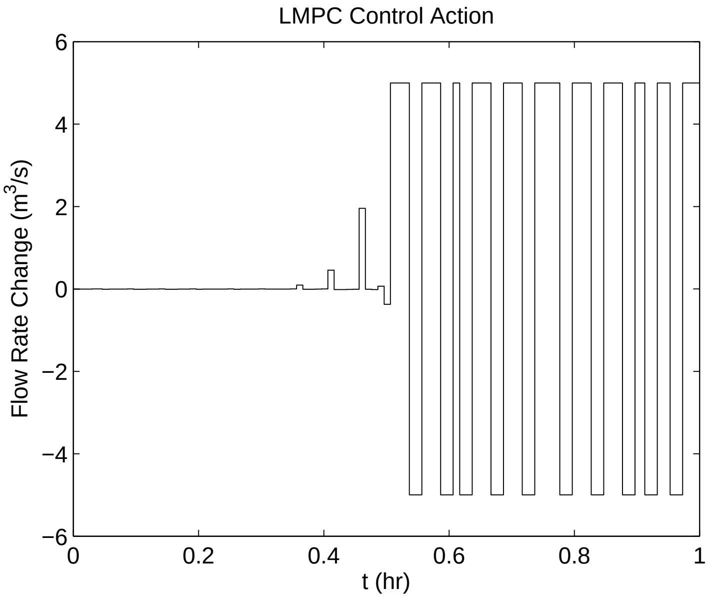


Figure 6.7: Manipulated input profile for the networked control system with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$. No fault tolerant control implemented.

the system. Figures 6.8 and 6.9 show the temperature and concentration profiles for the system with a failure in the heat input to vessel 2. The temperature trajectories show the initial deviation from steady-state as the fault is first introduced followed by a return to steady-state as the fault is detected at $t = 0.38$, isolated at $t = 0.46$ and the back-up controller configuration implemented in the networked control system (see Figure 6.10). The manipulated input profile in Figure 6.11 shows that once the fault is isolated, a large amount of control action is needed to return to steady-state, after which a minimal amount of control input is required to maintain system stability.

6.4 Conclusions

In this work, we studied the monitoring and reconfiguration of a networked control system applied to a chemical process system in the presence of control actuator faults. To deal with control actuator faults that may occur in the closed-loop system, a networked fault detection and isolation (FDI) and fault-tolerant control (FTC) system was designed which detects and isolates actuator faults and determines how to reconfigure the networked control

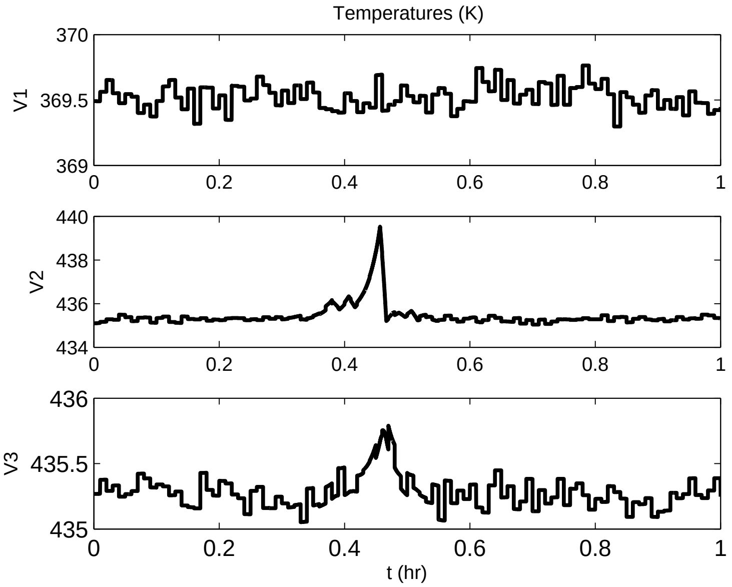


Figure 6.8: Temperature trajectories in each vessel with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$ and fault tolerant control upon fault isolation.

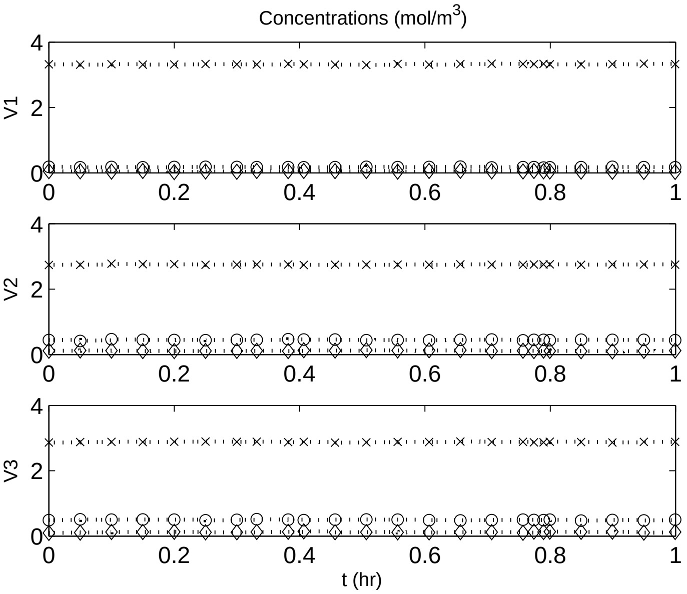


Figure 6.9: Asynchronous concentration measurements (C_A=x, C_B =o, C_C = $\diamond$) in each vessel (V1, V2, V3) with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$ and fault tolerant control upon fault isolation. Dotted lines represent observer trajectories.

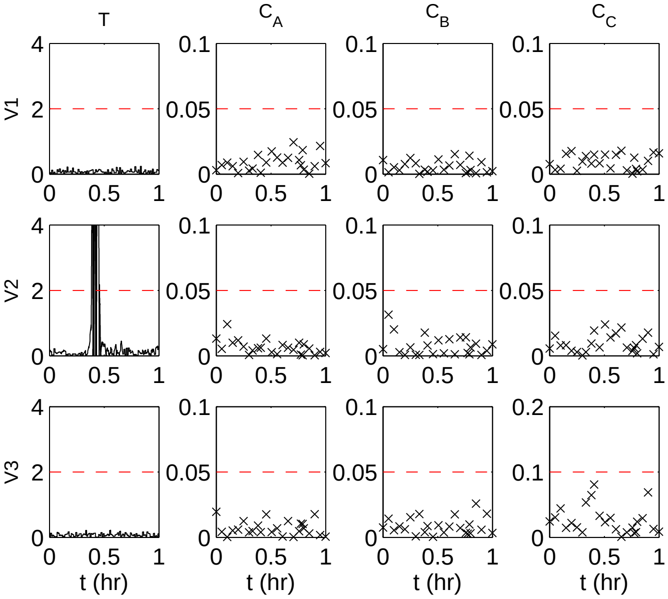


Figure 6.10: FDI filter residuals for temperature (T) and concentration(C_A, C_B, C_C) in each vessel (V1, V2, V3) with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$. Fault is detected at $t = 0.38hr$ and isolated at $t_k = 0.46hr$. Fault tolerant control implemented at time of isolation, $t_k = 0.48hr$.

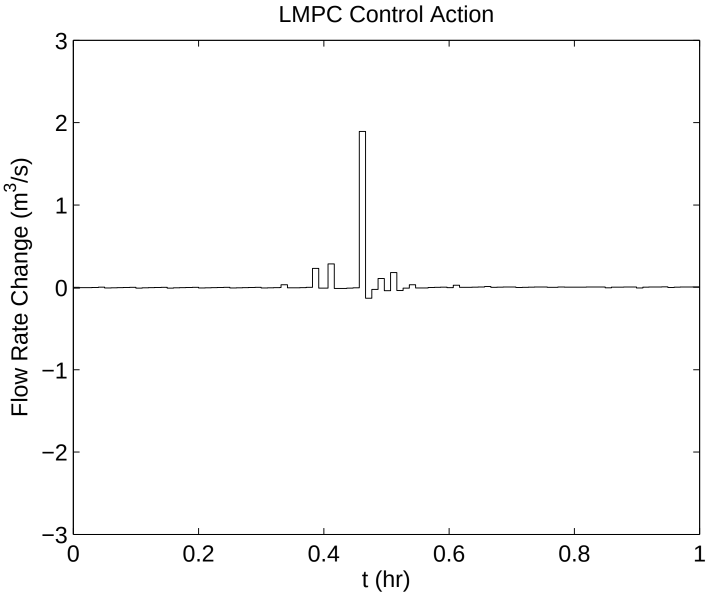


Figure 6.11: Manipulated input profile for the networked control system with an actuator failure in the heat input to vessel 2 at $t = 0.3hr$ and fault tolerant control upon fault isolation.

system to handle the actuator faults. The networked FDI/FTC method was demonstrated using a reactor-separator process consisting of two continuous stirred tank reactors and a flash tank separator with recycle stream.

Chapter 7

Conclusions

This dissertation developed a novel approach to data-based fault detection and isolation in nonlinear process systems through the use of feedback control. Taking into account the fault detection and isolation scheme when designing the feedback control law, it was shown that by considering the system structure and the structure of potential faults affecting the system, it is possible to enforce an isolable structure in the closed-loop system of a nonlinear process. These results were extended to include the cases of output feedback control and optimal control. Further work in the area of fault detection and isolation included model-based FDI using asynchronous measurements as well as an approach to networked monitoring and fault-tolerant control that integrates a two-tier control architecture with asynchronous FDI in order to perform fault-tolerant control. Specifically, in Chapter 2 a method of enforcing the necessary structure in order to perform FDI was developed, and the conditions in which this is possible were clearly outlined. In a CSTR example, feedback linearization was used to achieve the required closed-loop system structure in order to perform fault detection and isolation. In a 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.

Chapter 3 demonstrated the application of the data-based FDI method using feedback control laid out in Chapter 2 to a multi-unit reactor-separator chemical process. Fault detection and isolation were performed using statistical process monitoring techniques and information based upon the imposed closed-loop system structure. This was demonstrated through numerical simulation studies of the closed-loop system in the presence of four different faults. It was shown that by decoupling faults of interest from certain states, it was possible to achieve unique system responses to each of the four faults, allowing fault isolation based on process measurements only. These results were compared with a conventional PI controller and were thoroughly tested for susceptibility to false isolation through a Monte-Carlo simulation study of 500 runs for each of the four fault scenarios.

Chapter 4 built upon the work in Chapters 2-3 in controller-enhanced FDI by addressing two previously unresolved, practical problems. In this chapter, we developed an approach where systems with incomplete state measurements could be dealt with using state estimator-based output feedback control. This approach maintains the necessary isolable structure in the closed-loop system in order to perform controller-enhanced FDI. Additionally, we addressed the problem of controller-enhanced FDI in an optimal fashion within the framework of MPC. We proposed an MPC formulation that includes appropriate isolability constraints to achieve FDI in the closed-loop system. The effectiveness of these methods was demonstrated through application to a nonlinear CSTR example.

In a shift from the previous chapters, Chapter 5 used model-based FDI to address the problem of FDI and FTC when some of the process measurements are not available synchronously. This scheme employed model-based FDI filters in addition to observers that estimate the fault-free evolution of asynchronously measured states during times when they are unmeasured. We presented applications of the proposed asynchronous FDI and FTC framework to a polyethylene reactor simulation.

Finally, in Chapter 6, we studied the monitoring and reconfiguration of a networked control system applied to a chemical process system in the presence of control actuator faults. To deal with control actuator faults that may occur in the closed-loop system, a networked fault detection and isolation (FDI) and fault-tolerant control (FTC) system was designed which detects and isolates actuator faults and determines how to reconfigure the networked control system to handle the actuator faults. The networked FDI/FTC method was demonstrated using a reactor-separator process consisting of two continuous stirred tank reactors and a flash tank separator with recycle stream.

Bibliography

[1] H. B. Aradhye, B. R. Bakshi, J. F. Davis, and S. C. Ahalt. Clustering in wavelet domain: A multiresolution ART network for anomaly detection. *AIChE Journal*, 50:2455–2466, 2004.

[2] H. B. Aradhye, B. R. Bakshi, R. A. Strauss, and J. F. Davis. Multiscale SPC using wavelets: Theoretical analysis and properties. *AIChE Journal*, 49:939–958, 2003.

[3] B. R. Bakshi. Multiscale PCA with application to multivariate statistical process monitoring. *AIChE Journal*, 44:1596–1610, 1998.

[4] J. Bao, W. Z. Zhang, and P. L. Lee. Passivity-based decentralized failure-tolerant control. *Industrial & Engineering Chemistry Research*, 41:5702–5715, 2002.

[5] M. Blanke, R. Izadi-Zamanabadi, S. A. Bogh, and C. P. Lunau. Fault-tolerant control systems – a holistic view. *Control Engineering Practice*, 5:693–702, 1997.

[6] P. D. Christofides. Robust output feedback control of nonlinear singularly perturbed systems. *Automatica*, 36:45–52, 2000.

[7] P. D. Christofides, J. F. Davis, N. H. El-Farra, D. Clark, K. R. D. Harris, and J. N. Gipson. Smart plant operations: Vision, progress and challenges. *AIChE Journal*, 53:2734–2741, 2007.

[8] P. D. Christofides and N. H. El-Farra. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays,* 446 pages. Springer, New York, 2005.

[9] S. A. Dadebo, M. L. Bell, P. J. McLellan, and K. B. McAuley. Temperature control of industrial gas phase polyethylene reactors. *Journal of Process Control*, 7:83–95, 1997.

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

[11] P. Daoutidis and C. Kravaris. Structural evaluation of control confiurations for multivariable nonlinear processes. *Chemical Engineering Science*, 47:1091–1107, 1991.

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

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

[14] M. A. Demetriou. Utilization of lmi methods for fault tolerant control of a flexible cable with faulty actuators. In *Proceedings of the 40th IEEE Conference on Decision and Control*, volume 2, pages 1885–1890, Florida, 2001.

[15] M. A. Demetriou and A. Armaou. Robust detection and accommodation of incipient component faults in nonlinear distributed processes. In *Proceedings of the American Control Conference*, New York, 2007.

[16] M. A. Demetriou, K. Ito, and R. C. Smith. Adaptive monitoring and accommodation of nonlinear actuator faults in positive real infinite dimensional systems. *IEEE Transactions on Automatic Control*, 2007.

[17] R. Dunia, S. J. Qin, T. F. Edgar, and T. J. McAvoy. Identification of faulty sensors using principal component analysis. *AIChE Journal*, 42:2797–2812, 1996.

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

[19] N. H. El-Farra and P. D. Christofides. Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chemical Engineering Science*, 56:1841–1868, 2001.

[20] N. H. El-Farra and P. D. Christofides. Bounded robust control of constrained multivariable nonlinear processes. *Chemical Engineering Science*, 58:3025–3047, 2003.

[21] N. H. El-Farra and S. Ghantasala. Actuator fault isolation and reconfiguration in transport-reaction processes. *AIChE Journal*, 53:1518–1537, 2007.

[22] P. M. Frank. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy–a survey and some new results. *Automatica*, 26:459–474, 1990.

[23] A. Gani, P. Mhaskar, and P. D. Christofides. Fault-tolerant control of a polyethylene reactor. *Journal of Process Control*, 17:439–451, 2007.

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

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

[26] F. Harary. *Graph Theory.* Perseus Books Publishing, 1969.

[27] H. Hotelling. Multivariate quality control. In O. Eisenhart, editor, *Techniques of Statistical Analysis*, pages 113–184. McGraw-Hill, 1947.

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

[29] H. K. Khalil. *Nonlinear Systems.* Macmillan Publishing Comapny, 1992.

[30] P. Kokotovic and M Arcak. Constructive nonlinear control: a historical perspective. *Automatica*, pages 637–662, 2001.

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

[32] J. Liu, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis. A two-tier control architecture for nonlinear process systems with continuous/asynchronous feedback. In *Proceedings of the American Control Conference*, 2009.

[33] J. Liu, D. Muñoz de la Peña, B. J. Ohran, P. D. Christofides, and J. F. Davis. A two-tier architecture for networked process control. *Chemical Engineering Science*, 63:5349–5409, 2008.

[34] J. F. MacGregor, C. Jaeckle, C. Kiparissides, and M. Koutoudi. Process monitoring and diagnosis by multiblock PLS method. *AIChE Journal*, 40:826–838, 1994.

[35] J. F. MacGregor and T. Kourti. Statistical process control of multivariate processes. *Journal of Quality Technology*, 28:409–428, 1996.

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

[37] K. B. McAuley, D. A. Macdonald, and P. J. McLellan. Effects of operating conditions on stability of gas-phase polyethylene reactors. *AIChE Journal*, 41:868–879, 1995.

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

[39] N. Mehranbod, M. Soroush, and C. Panjapornpon. A method of sensor fault detection and identification. *Journal of Process Control*, 15:321–339, 2005.

[40] N. Mehranbod, M. Soroush, M. Piovoso, and B. A. Ogunnaike. Probabilistic model for sensor fault detection and identification. *AIChE Journal*, 49:1787–1802, 2003.

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

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

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

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

[45] P. Mhaskar, A. Gani, N. H. El-Farra, P. D. Christofides, and J. F. Davis. Integrated fault-detection and fault-tolerant control of process systems. *AIChE Journal*, 52:2129–2148, 2006.

[46] P. Mhaskar, A. Gani, C. McFall, P. D. Christofides, and J. F. Davis. Fault-tolerant control of nonlinear process systems subject to sensor faults. *AIChE Journal*, 53:654–668, 2007.

[47] P. Mhaskar, C. McFall, A. Gani, P.D. Christofides, and J. F. Davis. Isolation and handling of actuator faults in nonlinear systems. *Automatica*, 44:53–62, 2008.

[48] L. A. Montestruque and P. J. Antsaklis. On the model-based control of networked systems. *Automatica*, 39:1837–1843, 2003.

[49] L. A. Montestruque and P. J. Antsaklis. Stability of model-based net-worked control systems with time-varying transimission times. *IEEE Trans. Automat. Control*, 49:1562–1572, 2004.

[50] D. C. Montgomery. *Introduction to statistical quality control.* John Wiley & Sons, 1996.

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

[52] D. Nešić and A. R. Teel. Input-to-state stability of networked control systems. *Automatica*, 40:2121–2128, 2004.

[53] A. Negiz and A. Çinar. Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE Journal*, 43:2002–2020, 1997.

[54] I. Nimmo. Adequately address abnormal operations. *Chem. Eng. Prog.*, 91:36–45, 1995.

[55] B. J. Ohran, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis. Enhancing data-based fault isolation through nonlinear control. *AIChE Journal*, 53:2734–2741, 2008.

[56] R. J. Patton. Fault-tolerant control systems: The 1997 situation. In *Proceedings of the IFAC Symposium Safeprocess*, pages 1033–1054, Hull, United Kingdom, 1997.

[57] P. R. Prasad, J. F. Davis, Y. Jirapinyo, M. Bhalodia, and J.R. Josephson. Structuring diagnostic knowledge for large-scale process systems. *Computers and Chemical Engineering*, 22:1897–1905, 1999.

[58] A. Raich and A. Çinar. Statistical process monitoring and disturbance diagnosis in multivariable continuous processes. *AIChE Journal*, 42:995–1009, 1996.

[59] D. R. Rollins and J. F. Davis. Unbiased estimation of gross errors when the covariance matrix is unknown. *AIChE Journal*, 39:1335–1341, 1993.

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

[61] E. Sontag. A 'universal' construction of Arstein's theorem on nonlinear stabilization. *System and Control Letters*, pages 117–123, 1989.

[62] M. Tabbara, D. Nesic, and A. R. Teel. Stability of wireless and wireline networked control systems. *IEEE Transactions on Automatic Control*, 52:1615–1630, 2007.

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

[64] 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, 2003.

[65] 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, 2003.

[66] G. Walsh, H. Ye, and L. Bushnell. Stability analysis of networked control systems. *IEEE Transactions on Control Systems Technology*, 10:438–446, 2002.

[67] J. R. Whiteley and J. F. Davis. Knowledge-based interpretation of sensor patterns. *Computers & Chemical Engineering*, 16:329–346, 1992.

[68] J. R. Whiteley and J. F. Davis. Qualitative interpretation of sensor patterns. *IEEE Expert*, 8:54–63, 1992.

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

[70] 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.

[71] S. Yoon and J. F. MacGregor. Statistical and causal model-based approaches to fault detection and isolation. *AIChE Journal*, 46:1813–1824, 2000.

[72] 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.

[73] D. H. Zhou and P. M. Frank. Fault diagnostics and fault tolerant control. *IEEE Transactions on Aerospace and Electronic Systems*, 34:420–427, 1998.